

The Integrated Energy and Communication Systems Architecture

Volume IV: Technical Analysis

*Appendix D:
Technologies, Services, and Best Practices*

EPRI Project Manager

Joe Hughes

Cosponsor

Electricity Innovation Institute Consortium for Electric Infrastructure to Support a Digital
Society (CEIDS)

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

ORGANIZATIONS THAT PREPARED THIS DOCUMENT

General Electric Company led by GE Global Research (Prime Contractor)

Significant Contributions made by

EnerNex Corporation

Hypertek

Lucent Technologies (Partner)

Systems Integration Specialists Company, Inc.

Utility Consulting International (Partner)

ORDERING INFORMATION

Requests for copies of this report should be directed to EPRI Orders and Conferences, 1355 Willow Way, Suite 278, Concord, CA 94520. Toll-free number: 800.313.3774, press 2, or internally x5379; voice: 925.609.9169; fax: 925.609.1310.

Electric Power Research Institute and EPRI are registered service marks of the Electric Power Research Institute, Inc. EPRI. ELECTRIFY THE WORLD is a service mark of the Electric Power Research Institute, Inc. All other trademarks are the property of their respective owners.

Copyright © 2002, 2003, 2004 Electric Power Research Institute, Inc. All rights reserved.

CITATIONS

This document describes research sponsored by EPRI and Electricity Innovation Institute.

The publication is a corporate document that should be cited in the literature in the following manner:

THE INTEGRATED ENERGY AND COMMUNICATION SYSTEMS ARCHITECTURE, EPRI, Palo Alto, CA and Electricity Innovation Institute, Palo Alto, CA: 2003 {Product ID Number.

Table of Contents

1.	Technologies	1-1
1.1	Energy Industry-Specific Technologies.....	1-1
1.1.1	Utility Field Device Related Data Exchange Technologies	1-1
1.1.1.1	IEC60870-5 - Telecontrol Protocol.....	1-1
1.1.1.1.1	IEC60870-5 Part 101 - Serial Telecontrol Protocol	1-1
1.1.1.1.2	IEC60870-5 Part 104 - Telecontrol Protocol over TCP/IP.....	1-2
1.1.1.2	DNP.....	1-2
1.1.1.2.1	DNP Serial Protocol.....	1-2
1.1.1.2.2	DNP3 Protocol over TCP/IP	1-3
1.1.1.3	IEC61334 - Distribution PLC.....	1-3
1.1.1.4	ISO 9506 MMS - Manufacturing Messaging Specification	1-3
1.1.1.5	IEC61850 Substation Automation.....	1-4
1.1.1.5.1	IEC61850 - Substation Automation Communications	1-4
1.1.1.5.2	IEC61850 Part 7-2 - GSE (GOOSE and GSSE)	1-5
1.1.1.5.3	IEC61850 Part 7-2 - SMV (Sampled Measured Values)	1-5
1.1.1.5.4	IEC61850 Part 7-2 - Abstract Common Services Interface (ACSI).....	1-6
1.1.1.5.5	IEC61850 Parts 7-3 and 7-4 - Substation Object Modeling.....	1-7
1.1.1.5.6	IEC61850 Part 6 - Substation Configuration Language.....	1-8
1.1.1.5.7	IEC61850 Power Quality Object Models.....	1-9
1.1.1.6	IEC62350 - Object Models for Distributed Energy Resources (DER).....	1-9
1.1.1.7	IEC62349 - Hydro Power Plant Object Models	1-10
1.1.1.8	IEC61400-25 for Wind Power Object Models	1-10
1.1.1.9	Fieldbus	1-10
1.1.1.10	PROFIBUS.....	1-11
1.1.1.11	ModBus	1-11
1.1.1.11.1	ModBus.....	1-11
1.1.1.11.2	ModBus TCP/IP	1-12
1.1.1.11.3	ModBus Plus	1-12
1.1.1.12	IEEE 1451 Standard for a Smart Transducer Interface for Sensors and Actuators	1-12
1.1.1.13	Digital Time Division Command/Response Multiplex Data Bus, MIL-STD-1553	1-12
1.1.1.14	IEEE C37.94 - Standard for N x 64 kbps Optical Fiber Interfaces between Teleprotection and Multiplexer Equipment.....	1-13
1.1.1.15	C37.111-1999 IEEE COMTRADE Standard (Common Format for Transient Data Exchange) for Power Systems.....	1-13
1.1.1.16	IEEE 1159.3 - Power Quality Data Interchange Format (PQDIF).....	1-13
1.1.2	IEEE Guides for Communications in Power Systems	1-14
1.1.2.1	487-2000 - IEEE Recommended Practice for the Protection of Wire-Line Communication Facilities Serving Electric Supply Locations.....	1-14
1.1.2.2	643-1980 (R1992) - IEEE Guide for Power-Line Carrier Applications.....	1-14
1.1.2.3	1138-1994 - IEEE Standard Construction of Composite Fiber Optic Ground Wire (OPGW) for Use on Electric Utility Power Lines	1-14
1.1.2.4	C37.93-1987 (R1992) IEEE Guide for Power System Protective Relay Applications of Audio Tones Over Telephone Channels.....	1-14
1.1.2.5	1390-1995 IEEE Standard for Utility Telemetry Service Architecture for Switched Telephone Network	1-15
1.1.3	Utility Control Center Related Data Management Technologies.....	1-15
1.1.3.1	IEC 60870-6 (ICCP).....	1-15
1.1.3.2	IEC 61970 - CIM, CIM Extensions, and GID.....	1-16
1.1.3.2.1	IEC 61970 Part 3 - Common Information Model (CIM)	1-16
1.1.3.2.2	CIM Extensions for Market Operations	1-17
1.1.3.2.3	IEC 61970 Part 4 - Generic Interface Definition (GID).....	1-17
1.1.3.3	OPC.....	1-18

1.1.3.3.1	OPC Data Access (DA).....	1-18
1.1.3.3.2	OPC Historic Data Access (HDA).....	1-19
1.1.3.3.3	OPC Alarming and Eventing.....	1-19
1.1.3.3.4	OPC Command.....	1-19
1.1.3.4	IEC61968 SIDM System Interfaces for Distribution Management.....	1-19
1.1.3.5	IEC62325 on Framework for Energy Market Communications.....	1-20
1.1.3.6	NERC e-tagging.....	1-20
1.1.3.7	NAESB OASIS for Market Transactions.....	1-22
1.1.3.8	OPEN GIS.....	1-22
1.1.3.9	OAG.....	1-23
1.1.3.10	MultiSpeak.....	1-23
1.1.4	Customer Interface Data Management Technologies.....	1-23
1.1.4.1	IEC62056 - Data Exchange for Meter Reading, Tariff, and Load Control.....	1-23
1.1.4.2	ANSI C12.19 (Meter Tables).....	1-24
1.1.4.3	AEIC Guidelines.....	1-24
1.1.4.4	ASHRAE SSPC135 BACnet.....	1-24
1.1.4.5	GPC-20 XML Modeling for HVAC.....	1-24
1.1.4.6	CEBus® based on EIA 600.....	1-25
1.1.4.7	UPnP.....	1-25
1.1.4.8	Controller Area Network (CAN).....	1-25
1.1.5	Customer Automated Meter Reading (AMR) Technologies.....	1-26
1.1.5.1	1390.2-1999 IEEE Automatic Meter Reading via Telephone - Network to Telemetry Interface Unit.....	1-26
1.1.5.2	1390.3-1999 IEEE Standard for Automatic Meter Reading via Telephone - Network to Utility Controller.....	1-26
1.1.5.3	ANSI C12.18 (PSEM, Optical port).....	1-26
1.1.5.4	ANSI C12.21 (POTS).....	1-27
1.1.5.5	ANSI C12.22 (EPSEM).....	1-27
1.1.5.6	Broadband over Power Line (BPL).....	1-27
1.1.6	Customer Site In-Building Technologies.....	1-28
1.1.6.1	Home PNA.....	1-28
1.1.6.2	HomePlug.....	1-28
1.1.6.3	Zigbee Spec.....	1-28
1.2	Communications Industry Technologies.....	1-29
1.2.1	Access Technologies.....	1-29
1.2.1.1	Public Internet.....	1-29
1.2.1.2	Private Intranet.....	1-29
1.2.1.3	Data over Voice Lines.....	1-29
1.2.1.4	Digital Subscriber Line (DSL) Technologies.....	1-30
1.2.1.4.1	Asymmetric Digital Subscriber Line (ADSL) and Digital Subscriber Line (DSL)...	1-31
1.2.1.4.2	High Data-Rate Digital Subscriber Line (HDSL).....	1-31
1.2.1.4.3	Single-Line Digital Subscriber Line (SDSL).....	1-32
1.2.1.4.4	Very high data rate Digital Subscriber Line (VDSL).....	1-32
1.2.1.4.5	Wireless Digital Subscriber Line (WDSL).....	1-32
1.2.1.4.6	Rate-Adaptive DSL (RADSL).....	1-32
1.2.1.4.7	G.Lite/DSL Lite/Universal ADSL.....	1-33
1.2.1.5	Cable Modems - DOCSIS.....	1-33
1.2.1.6	Fiber in the Loop (FITL).....	1-33
1.2.1.7	Hybrid Fiber Coax (HFC).....	1-33
1.2.2	Networking Technologies.....	1-35
1.2.2.1	Internet Protocol Version V4 (IPv4).....	1-35
1.2.2.2	Internet Protocol Version 6 (IPv6).....	1-35
1.2.2.3	Routing Protocols.....	1-35
1.2.2.3.1	Unicast Routing.....	1-36
1.2.2.3.2	Multicast Routing.....	1-36
1.2.2.3.3	Open Shortest Path First (OSPF) Routing Protocol.....	1-36

1.2.2.3.4	Intermediate System to Intermediate System (ISIS) Routing Protocol.....	1-37
1.2.2.3.5	Routing Information Protocol (RIP).....	1-37
1.2.2.3.6	Border Gateway Protocol (BGP).....	1-37
1.2.2.3.7	Host extensions for IP multicasting.....	1-37
1.2.2.3.8	Internet Group Management Protocol (IGMP)	1-38
1.2.2.3.9	Distance Vector Multicast Routing Protocol (DVMRP).....	1-38
1.2.2.3.10	Multicast Open Shortest Path (MOSPF) routing protocol.....	1-38
1.2.2.3.11	Protocol Independent Multicast-Sparse Mode (PIM-SM).....	1-39
1.2.2.3.12	Core-Based Tree (CBT) multicast routing	1-39
1.2.3	IP-based Transport Protocols	1-39
1.2.3.1	Transmission Control Protocol (TCP).....	1-39
1.2.3.2	User Datagram Protocol (UDP).....	1-39
1.2.3.3	Stream Control Transmission Protocol (SCTP)	1-40
1.2.3.4	Datagram Congestion Control Protocol (DCCP)	1-40
1.2.3.5	Real-Time Transport Protocol (RTP)	1-40
1.2.4	Application Layer Protocols	1-41
1.2.4.1	Hypertext Transfer Protocol (HTTP)	1-41
1.2.4.2	File Transfer Protocol (FTP)	1-41
1.2.4.3	Trivial File Transfer Protocol (TFTP).....	1-41
1.2.4.4	TELNET Protocol	1-42
1.2.4.5	Domain Name System (DNS) protocol.....	1-42
1.2.4.6	Dynamic Host Configuration Protocol (DHCP).....	1-42
1.2.4.7	URI.....	1-42
1.2.4.8	World Wide Web (WWW).....	1-43
1.2.4.9	Web Browser.....	1-43
1.2.4.10	Microsoft COM+.....	1-43
1.2.4.11	SNTP (Network Time Protocol).....	1-44
1.2.4.12	CSV files	1-44
1.2.5	Link Layer and Physical Technologies	1-44
1.2.5.1	LAN/MAN Technologies.....	1-44
1.2.5.2	IEEE 802 MAC Addresses.....	1-44
1.2.5.3	IEEE 802.3aez Standards	1-45
1.2.5.4	IEEE 802.1p and IEEE 802.1q (VLAN)	1-45
1.2.5.5	IEEE 802.1d Spanning Tree Protocol (STP).....	1-45
1.2.5.6	IEEE 802.1w Rapid Spanning Tree Protocol (RSTP).....	1-45
1.2.5.7	IEEE 802.17 - Resilient Packet Ring (RPR)	1-46
1.2.5.8	LAN interconnection technologies.....	1-46
1.2.5.9	Ethernet	1-46
1.2.5.10	Hubs/Repeaters.....	1-46
1.2.5.11	Bridges/Switches.....	1-46
1.2.5.12	Routers	1-47
1.2.5.13	V series Modems.....	1-47
1.2.5.14	Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1.....	1-47
1.2.5.15	X series Data Network	1-48
1.2.5.16	Frame Relay	1-48
1.2.5.17	Point-to-Point Protocol (PPP)	1-49
1.2.5.18	Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH)....	1-49
1.2.5.19	Asynchronous Transfer Mode (ATM).....	1-50
1.2.6	Wireless Technologies	1-50
1.2.6.1	3rd Generation Cellular Wireless	1-50
1.2.6.2	Universal Mobile Telecommunication System (UMTS).....	1-50
1.2.6.3	Code-Division Multiple Access 2000 (CDMA-2000).....	1-51
1.2.6.4	TDMA Cellular Wireless - IS-136	1-51
1.2.6.5	CDMA Cellular Wireless - IS-95	1-51
1.2.6.6	Cellular Digital Packet Data (CDPD).....	1-51
1.2.6.7	Global System for Mobile Communication (GSM)	1-51

1.2.6.8	Short Message Service (SMS).....	1-52
1.2.6.9	Global Positioning System (GPS)	1-52
1.2.6.10	Trunked Mobile Radio (TMR, TETRA, Project25)	1-52
1.2.6.11	IEEE 802.11 Wireless Local Area Network (WLAN)	1-54
1.2.6.12	IEEE 802.15 Wireless Personal Area Network (PAN)	1-54
1.2.6.13	Bluetooth Special	1-54
1.2.6.14	IEEE 802.16 Broadband Wireless Access Standards	1-55
1.2.6.15	Multiple Address (MAS) Radio	1-55
1.2.6.16	Spread Spectrum Radio System	1-56
1.2.6.17	Satellite Leased Channels and VSAT.....	1-58
1.2.6.18	Paging Systems	1-58
1.2.6.19	Radio Frequency Identification (RFID)	1-59
1.2.7	Quality-of-Service-enabling Technologies	1-60
1.2.7.1	Multi-Protocol Label Switching (MPLS).....	1-60
1.2.7.2	Differentiated Services (DiffServ)	1-60
1.2.7.3	Integrated Services (IntServ).....	1-60
1.2.8	Virtual Private Networking Technologies.....	1-61
1.2.8.1	Layer 3 VPNs	1-61
1.2.8.2	Layer 2 VPNs.....	1-61
1.2.8.3	PPTP.....	1-61
1.2.9	Computer Systems Related Technologies.....	1-62
1.2.9.1	CORBA and CORBA Services	1-62
1.2.9.2	Web Services.....	1-62
1.2.9.2.1	Web Services Technologies	1-62
1.2.9.2.2	Universal Description, Discovery, and Integration (UDDI).....	1-62
1.2.9.2.3	XML Protocol/Simple Object Access Protocol (SOAP).....	1-63
1.2.9.2.4	Web Services Description Language (WSDL).....	1-63
1.2.9.2.5	Web Services Business Process Execution Language (WS-BPEL).....	1-63
1.2.9.2.6	Web Services Architecture Including Reliable Messaging	1-64
1.2.9.3	Enterprise Java Beans (EJB)	1-64
1.2.9.4	IEEE 1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems	1-64
1.2.9.5	GUID.....	1-65
1.2.9.6	9834-1 Procedures for the operation of OSI Registration Authorities	1-65
1.2.10	General Internet and De Facto Data Management Technologies.....	1-65
1.2.10.1	Simple Mail Transfer Protocol (SMTP).....	1-65
1.2.10.2	Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME.....	1-66
1.2.10.3	Post Office Protocol version 3 (POP3).....	1-66
1.2.10.4	Internet Message Access Protocol version 4 (IMAP4).....	1-66
1.2.10.5	ANSI/ISO/IEC 8632-1, 2, 3, 4 - Computer Graphics Metafile (CGM).....	1-67
1.2.10.6	ISO/IEC 11179 Parts 1 - 6 Metadata Registries	1-67
1.2.10.7	Meta Object Facility (MOF).....	1-69
1.2.10.8	XML Metadata Interchange (XMI).....	1-69
1.2.10.9	Common Warehouse Model (CWM)	1-69
1.2.10.10	American Standard Code for Information Interchange (ASCII)	1-69
1.2.10.11	Hypertext Markup Language (HTML).....	1-70
1.2.10.12	eXtensible Markup Language (XML).....	1-70
1.2.10.13	RDF	1-71
1.2.10.14	XML Schema (xIs).....	1-71
1.2.10.15	XPath.....	1-71
1.2.10.16	XSLT.....	1-71
1.2.10.17	XQuery	1-72
1.2.10.18	ANSI/ISO/IEC 9075 - Structured Query Language (SQL).....	1-72
1.2.11	eCommerce Related Data Management Technologies.....	1-72
1.2.11.1	Universal Business Language (UBL).....	1-72
1.2.11.2	ebXML.....	1-73

1.2.11.2.1	ebXML.....	1-73
1.2.11.2.2	ebXML Collaboration Protocol Profiles (CPPA).....	1-73
1.2.11.2.3	ebXML Messaging.....	1-73
1.2.11.2.4	ebXML Registry.....	1-73
1.2.11.3	ISO/IEC JTC 1 SC32 - ISO/IEC 15944-1:2002 Information technology -- Business agreement semantic descriptive techniques -- Part 1: Operational aspects of Open-EDI for implementation.....	1-74
1.2.11.4	EAN.UCC Identification Numbers	1-74
1.2.11.5	EAN.UCC Universal Bar Codes	1-74
1.2.11.6	10303 Standard Exchange for Product Data (STEP).....	1-75
1.3	Security Technologies.....	1-75
1.3.1	Policy and Framework Related Technologies.....	1-75
1.3.1.1	ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management	1-75
1.3.1.2	ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework	1-76
1.3.1.3	ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems.....	1-76
1.3.1.4	FIPS PUB 112 Password Usage.....	1-76
1.3.1.5	FIPS PUB 113 Computer Data Authentication	1-77
1.3.1.6	RFC 2196 Site Security Handbook	1-77
1.3.1.7	RFC 2401 Security Architecture for the Internet Protocol.....	1-77
1.3.1.8	RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	1-77
1.3.2	General Security Technologies	1-78
1.3.2.1	PKI - Public Key Infrastructure (X.509)	1-78
1.3.2.2	Kerberos	1-78
1.3.2.3	FIPS 140-2 Security Requirements for Cryptographic Modules.....	1-78
1.3.2.4	FIPS 197 for Advanced Encryption Standard (AES)	1-79
1.3.2.5	Role-Based Access Control.....	1-79
1.3.2.6	PKCS.....	1-80
1.3.2.7	FIPS 186 Digital Signatures Standard (DSS).....	1-80
1.3.2.8	Intrusion Detection Technologies.....	1-80
1.3.2.9	Intrusion Prevention Systems (IPS).....	1-81
1.3.2.10	Service Level Agreements (SLA)	1-81
1.3.3	Media and Network Layer Technologies	1-82
1.3.3.1	Secure IP Architecture (IPSec).....	1-82
1.3.3.2	IEEE 802.11i Security for Wireless Networks (WPA2)	1-82
1.3.3.3	Remote Authentication Dial In User Service (RADIUS).....	1-82
1.3.3.4	ATM Security.....	1-83
1.3.3.5	AGA-12 Cryptographic Protection of SCADA Communications General Recommendations	1-83
1.3.4	Transport Layer Security Technologies	1-83
1.3.4.1	Transport Layer Security (TLS)/Secure Sockets Layer (SSL)	1-84
1.3.5	Application Layer Security Technologies.....	1-84
1.3.5.1	RFC 2228 FTP Security Extensions.....	1-84
1.3.5.2	Internet Mail Extensions	1-84
1.3.5.3	RFC 2086 IMAP4 ACL extension	1-85
1.3.5.4	SNMP Security.....	1-85
1.3.5.5	RFC 1305 Network Time Protocol (Version 3) Specification, Implementation	1-85
1.3.5.6	IEC 62351-3 Security for Profiles including TCP/IP	1-86
1.3.5.7	IEC 62351-4 Security for Profiles including MMS (ISO-9506)	1-86
1.3.5.8	IEC 62351-5 Security for IEC 60870-5 and Derivatives.....	1-86
1.3.5.9	IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles	1-86
1.3.6	XML Related Technologies	1-86
1.3.6.1	OASIS Security Assertion Markup Language (SAML).....	1-86

1.3.6.2	OASIS Extensible Access Control Markup Language (XACML).....	1-87
1.3.6.3	XML Key Management Specification (XKMS).....	1-87
1.3.6.4	Secure XML.....	1-87
1.4	Network and Enterprise Management Technologies.....	1-88
1.4.1	Network Management Technologies.....	1-88
1.4.1.1	Simple Network Management Protocol (SNMP).....	1-88
1.4.1.2	Remote Network Monitor (RMON).....	1-88
1.4.1.3	OSI Network Management Model and CMIP.....	1-89
1.4.1.4	Telecommunications Management Network (TMN) - M series.....	1-90
1.4.1.5	Transaction Language 1 (TL1).....	1-90
1.4.1.6	IEC 62351-7 Objects for Network Management.....	1-90
1.4.2	Web-based Network Management.....	1-91
1.4.2.1	Web-based Enterprise Management (WBEM).....	1-91
1.4.2.2	Policy-based Management Technologies.....	1-91
1.4.3	System Engineering Related Data Management Technologies.....	1-91
1.4.3.1	DoD Joint Technical Architecture.....	1-92
1.4.3.2	MIL-STD-499.....	1-92
2.	Common Services.....	2-1
2.1	Security Services.....	2-1
2.1.1	Common Security Services.....	2-1
2.1.1.1	Audit Common Service.....	2-1
2.1.1.2	Authorization for Access Control.....	2-3
2.1.1.3	Confidentiality.....	2-11
2.1.1.4	Credential Conversion.....	2-16
2.1.1.5	Credential Renewal Service.....	2-18
2.1.1.6	Delegation Service.....	2-21
2.1.1.7	Firewall Traversal.....	2-22
2.1.1.8	Identity Establishment Service.....	2-24
2.1.1.9	Identity Mapping Service.....	2-32
2.1.1.10	Information Integrity Service.....	2-33
2.1.1.11	Inter-Domain Security.....	2-33
2.1.1.12	Non-repudiation.....	2-34
2.1.1.13	Path Routing and QOS Service.....	2-35
2.1.1.14	Security Policies.....	2-36
2.1.1.15	Policy Exchange.....	2-42
2.1.1.16	Privacy Service.....	2-43
2.1.1.17	Profile Service (User Profile Service).....	2-43
2.1.1.18	Quality of Identity Service.....	2-44
2.1.1.19	Security against Denial-of-Service.....	2-46
2.1.1.20	Security Assurance Management.....	2-47
2.1.1.21	Security Protocol Mapping.....	2-48
2.1.1.22	Security Service Availability Discovery Service.....	2-48
2.1.1.23	Setting and Verifying User Authorization.....	2-49
2.1.1.24	Single Sign On Service.....	2-49
2.1.1.25	Trust Establishment Service.....	2-49
2.1.1.26	User and Group Management.....	2-50
2.2	Network and System Management Services.....	2-50
2.2.1	Enterprise Management Services.....	2-50
2.2.1.1	Inventory Management.....	2-50
2.2.1.2	Communication System/Network Discovery.....	2-50
2.2.1.3	Routing Management.....	2-50
2.2.1.4	Traffic Management.....	2-51
2.2.1.5	Traffic Engineering.....	2-51
2.2.1.6	System/Network Health-Check Analysis.....	2-51
2.2.1.7	System/Network Fault Diagnosis.....	2-51
2.2.1.8	System/Network Fault Correcting.....	2-52

2.2.1.9	Service Level Agreement (SLA) Determination and Maintenance.....	2-52
2.2.1.10	System/Network Performance Analysis.....	2-52
2.2.1.11	System/Network Performance Diagnosis.....	2-52
2.2.1.12	Performance Tuning/Correction.....	2-52
2.2.1.13	Accounting and/or Billing.....	2-53
2.3	Data Management Common Services.....	2-53
2.3.1	Data Management Common Services.....	2-53
2.3.1.1	Distributed Data Management Service.....	2-53
2.3.1.2	Object Management Service.....	2-53
2.3.1.3	Address and Naming Management.....	2-53
2.3.1.4	Generic Eventing And Subscription.....	2-54
2.3.1.5	Alarm Detection/Reporting.....	2-54
2.3.1.6	Instrumentation and Monitoring Service.....	2-54
2.3.1.7	Measurement Data Logging Service.....	2-54
2.3.1.8	Remote Control.....	2-55
2.3.1.9	Network Time.....	2-55
2.3.1.10	File Transfer.....	2-55
2.4	Common Platform Services.....	2-55
2.4.1	Common Platform Services.....	2-55
2.4.1.1	Component Registry Service.....	2-55
2.4.1.2	Component Lookup Service.....	2-55
2.4.1.3	Component Discovery Service.....	2-55
2.4.1.4	Component Initialization and Termination.....	2-55
2.4.1.5	Storage.....	2-56
2.4.1.6	Resource Management.....	2-56
2.4.1.7	Transactions.....	2-56
2.4.1.8	Checkpoint and Recovery.....	2-56
2.4.1.9	Workflow Service.....	2-56
3.	Best Practices.....	3-1
3.1	Data Management Best Practices.....	3-1
3.1.1	Data Management Best Practices.....	3-1
3.1.1.1	Unified Modeling Language (UML).....	3-1
3.1.1.2	Alternate Communication Channels.....	3-5
3.1.1.3	Backup Data Sources.....	3-6
3.1.1.4	Backup Databases.....	3-6
3.1.1.5	Backup Sites.....	3-6
3.1.1.6	Metadata Files and Databases.....	3-7
3.1.1.7	Object Modeling Techniques for IEC61850-based Devices.....	3-7
3.1.1.8	Quality Flagging.....	3-8
3.1.1.9	Time Stamping.....	3-9
3.1.1.10	Validation of Source Data and Data Exchanges.....	3-9
3.1.1.11	Data Update Management.....	3-10
3.1.1.12	Management of Time-Sensitive Data Flows and Timely Access to Data by Multiple Different Users.....	3-10
3.1.1.13	Management of Data Consistency and Synchronization across Systems.....	3-11
3.1.1.14	Management of Data and Object Naming.....	3-11
3.1.1.15	Management of Data Formats in Data Exchanges.....	3-11
3.1.1.16	Management of Transaction Integrity (backup and rollback capability).....	3-12
3.1.1.17	Management of Data Accuracy.....	3-12
3.1.1.18	Management of Data Acquisition.....	3-12
3.1.1.19	Management of Manual Data Entry.....	3-13
3.1.1.20	Data Storage and Access Management.....	3-13
3.1.1.21	Data Consistency across Multiple Systems.....	3-14
3.1.1.22	Database Maintenance Management.....	3-14
3.1.1.23	Data Backup and Logging Management.....	3-15
3.1.1.24	Application Management.....	3-15

3.1.2	Enterprise (Network and System) Management Best Practices	3-15
3.1.2.1	Analysis of the Integration of Enterprise Management and Power Systems	3-15
3.2	Security Best Practices	3-16
3.2.1	Security Policy	3-16
3.2.1.1	General Security Policy Process	3-17
3.2.1.1.1	Security Policy Development Process	3-17
3.2.1.1.2	Security Policy Coverage Requirements	3-17
3.2.1.1.3	Security Risk Assessment/Analysis of Assets	3-18
3.2.1.1.4	Implementation of Security Policies	3-18
3.2.1.1.5	Analysis and Re-Analysis of Security Policies	3-18
3.2.1.2	PKI Infrastructure Policy and Issues	3-19
3.2.1.3	Specific Policy Issues and Recommendations per Service	3-22
3.2.1.3.1	Audit Service and Non-Repudiation	3-22
3.2.1.3.2	Credentials and User Accounts	3-22
3.2.1.3.3	User and Group Account Management	3-25
3.2.1.4	Security Training	3-27
3.2.1.5	Impact of Security Policy for Credential Renewal on Availability	3-28
3.2.2	Security Frameworks and Policy Documents	3-28
3.2.2.1	ISO/IEC Security Best Practices	3-28
3.2.2.2	ISO/IEC 10164-8:1993 Information technology -- Open Systems Interconnection -- Systems Management: Security audit trail function	3-28
3.2.2.3	ISO/IEC 18014-1:2002 Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework	3-28
3.2.2.4	ISO/IEC 18014-2:2002 Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens	3-29
3.2.2.5	ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens	3-29
3.2.2.6	ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework	3-29
3.2.2.7	ISO JTC1 SC37 SD 2 - Harmonized Biometric Vocabulary	3-29
3.2.2.8	Federal Security Best Practices	3-30
3.2.2.9	CICSI 6731.01 Global Command and Control System Security Policy	3-30
3.2.2.10	FIPS PUB 112 Password Usage	3-30
3.2.2.11	FIPS PUB 113 Computer Data Authentication	3-30
3.2.2.12	IETF Security Best Practices Internet Requests for Comments (RFCs)	3-31
3.2.2.13	RFC 1102 Policy routing in Internet protocols	3-31
3.2.2.14	RFC 1322 A Unified Approach to Inter-Domain Routing	3-31
3.2.2.15	RFC 1351 SNMP Administrative Model	3-31
3.2.2.16	RFC 2008 Implications of Various Address Allocation Policies for Internet Routing	3-31
3.2.2.17	RFC 2196 Site Security Handbook	3-32
3.2.2.18	RFC 2276 Architectural Principles of Uniform Resource Name Resolution	3-32
3.2.2.19	RFC 2350 Expectations for Computer Security Incident Response	3-32
3.2.2.20	RFC 2386 A Framework for QoS-based Routing in the Internet	3-32
3.2.2.21	RFC 2401 Security Architecture for the Internet Protocol	3-33
3.2.2.22	RFC 2505 Anti-Spam Recommendations for SMTP MTAs	3-33
3.2.2.23	RFC 2518 HTTP Extensions for Distributed Authoring - WEBDAV	3-33
3.2.2.24	RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	3-34
3.2.2.25	RFC 2725 Routing Policy System Security	3-34
3.2.2.26	RFC 2775 Internet Transparency	3-34
3.2.2.27	RFC 2993 Architectural Implications of NAT	3-34
3.2.2.28	RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	3-35
3.2.2.29	Other Security Best Practices	3-35
3.2.2.30	21 CFR Part 11 Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application	3-35

3.2.2.31	ISA-99 Integrating Electronic Security into the Manufacturing and Control Systems Environment	3-35
3.2.2.32	EPRI 100898 Scoping Study on Security Processes and Impacts	3-35
3.2.2.33	EPRI 100174 Communication Security Assessment for the United States Electric Utility Infrastructure	3-36
3.2.2.34	NIST SP 500-166 Computer Viruses and Related Threats: A Management Guide	3-36
3.2.2.35	Radius Protocol Security and Best Practices	3-36
4.	Security Documents	4-1
4.1	Security Technology Documents	4-1
4.1.1	ISO/IEC Documents on Security Technologies	4-1
4.1.1.1	ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics	4-1
4.1.1.2	ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols	4-1
4.1.1.3	ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V	4-1
4.1.1.4	ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange	4-1
4.1.1.5	ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages	4-2
4.1.1.6	ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers	4-2
4.1.1.7	ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)	4-2
4.1.1.8	ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands	4-2
4.1.1.9	ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes	4-3
4.1.1.10	ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards	4-3
4.1.1.11	ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods	4-3
4.1.1.12	ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application	4-3
4.1.1.13	ISO 9735-9:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 9: Security key and certificate management message (message type-KEYMAN)	4-4
4.1.1.14	ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework	4-4
4.1.1.15	ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks	4-4
4.1.1.16	ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)	4-5
4.1.1.17	ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control	4-5
4.1.1.18	ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview	4-5
4.1.1.19	ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework	4-6
4.1.1.20	ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework	4-7
4.1.1.21	ISO/IEC 10181-4:1997 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework	4-8

4.1.1.22	ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle	4-9
4.1.1.23	ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management.....	4-9
4.1.1.24	ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems.....	4-9
4.1.1.25	ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security.....	4-9
4.1.1.26	ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security.....	4-9
4.1.1.27	ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security	4-10
4.1.1.28	ISO/IEC 13888-1:1997 Information technology -- Security techniques -- Non-repudiation -- Part 1: General.....	4-10
4.1.1.29	ISO/IEC 13888-2:1998 Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques.....	4-11
4.1.1.30	ISO/IEC 13888-3:1997 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques.....	4-11
4.1.1.31	ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode.....	4-12
4.1.1.32	ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements.....	4-13
4.1.1.33	ISO/IEC 15408-3:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements	4-14
4.1.1.34	ISO/IEC 17799:2000 Information technology -- Code of practice for information security management	4-14
4.1.1.35	ISO JTC1 SC37 1.37.19784.1 BioAPI - Biometric Application Programming Interface	4-14
4.1.1.36	ISO JTC1 SC37 1.37.19794 - Biometric Data Interchange Format	4-15
4.1.1.37	ISO JTC1 SC37 1.37.19794.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data	4-15
4.1.1.38	ISO JTC1 SC37 1.37.19794.4 Biometric Data Interchange Format - Part 4: Finger Image Data	4-15
4.1.1.39	ISO JTC1 SC37 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data	4-15
4.1.2	Federal Documents on Security Technologies.....	4-15
4.1.2.1	FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES).....	4-15
4.1.3	IETF Internet Requests for Comments (RFCs) on Security Technologies	4-16
4.1.3.1	STD 13 Domain Name System	4-16
4.1.3.2	RFC 1004 Distributed-protocol authentication scheme	4-16
4.1.3.3	RFC 1013 X Window System Protocol, version 11: Alpha update April 1987	4-16
4.1.3.4	RFC 1034 Domain names - concepts and facilities.....	4-16
4.1.3.5	RFC 1040 Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication	4-17
4.1.3.6	RFC 1423 Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers.....	4-17
4.1.3.7	RFC 1221 Host Access Protocol (HAP) Specification - Version 2.....	4-17
4.1.3.8	RFC 1305 Network Time Protocol (Version 3) Specification, Implementation	4-18
4.1.3.9	RFC 1352 SNMP Security Protocols	4-18
4.1.3.10	RFC 1507 DASS - Distributed Authentication Security Service	4-18
4.1.3.11	RFC 1579 Firewall-Friendly FTP	4-19
4.1.3.12	RFC 1591 Domain Name System Structure and Delegation.....	4-19
4.1.3.13	RFC 1608 Representing IP Information in the X.500 Directory	4-19
4.1.3.14	RFC 1612 DNS Resolver MIB Extensions	4-19
4.1.3.15	RFC 1826 IP Authentication Header.....	4-20
4.1.3.16	RFC 1827 IP Encapsulating Security Payload (ESP).....	4-20

4.1.3.17	RFC 1919 Classical versus Transparent IP Proxies	4-20
4.1.3.18	RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)	4-21
4.1.3.19	RFC 1968 The PPP Encryption Control Protocol (ECP)	4-21
4.1.3.20	RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms	4-21
4.1.3.21	RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME	4-22
4.1.3.22	RFC 2086 IMAP4 ACL extension	4-22
4.1.3.23	RFC 2093 Group Key Management Protocol (GKMP) Specification	4-22
4.1.3.24	RFC 2228 FTP Security Extensions.....	4-22
4.1.3.25	RFC 2230 Key Exchange Delegation Record for the DNS.....	4-23
4.1.3.26	RFC 2244 ACAP -- Application Configuration Access Protocol	4-23
4.1.3.27	RFC 2246 The TLS Protocol Version 1.0	4-23
4.1.3.28	RFC 2313 PKCS #1: RSA Encryption Version 1.5	4-23
4.1.3.29	RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5	4-24
4.1.3.30	RFC 2356 Sun's SKIP Firewall Traversal for Mobile IP	4-24
4.1.3.31	RFC 2406 IP Encapsulating Security Payload (ESP).....	4-25
4.1.3.32	RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0.....	4-25
4.1.3.33	RFC 2440 OpenPGP Message Format	4-25
4.1.3.34	RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP).....	4-25
4.1.3.35	RFC 2409 The Internet Key Exchange (IKE)	4-26
4.1.3.36	RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile.....	4-26
4.1.3.37	RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols	4-26
4.1.3.38	RFC 2511 Internet X.509 Certificate Request Message Format	4-27
4.1.3.39	RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	4-27
4.1.3.40	RFC 2535 Domain Name System Security Extensions.....	4-27
4.1.3.41	RFC 2543 SIP: Session Initiation Protocol	4-27
4.1.3.42	RFC 2547 BGP/MPLS VPNs.....	4-27
4.1.3.43	RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OSCP.....	4-28
4.1.3.44	RFC 2592 Definitions of Managed Objects for the Delegation of Management Script... ..	4-28
4.1.3.45	RFC 2744 Generic Security Service API Version 2 : C-bindings	4-28
4.1.3.46	RFC 2764 A Framework for IP Based Virtual Private Networks	4-29
4.1.3.47	RFC 2753 A Framework for Policy-based Admission Control.....	4-29
4.1.3.48	RFC 2797 Certificate Management Messages over CMS	4-29
4.1.3.49	RFC 2817 Upgrades to TLS within HTTP/1.1	4-29
4.1.3.50	RFC 2818 HTTP over TLS (HTTPS)	4-30
4.1.3.51	RFC 2820 Access Control Requirements for LDAP.....	4-30
4.1.3.52	RFC 2865 Remote Authentication Dial In User Service (RADIUS)	4-30
4.1.3.53	RFC 2869 RADIUS Extensions	4-30
4.1.3.54	RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering....	4-30
4.1.3.55	RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms.....	4-31
4.1.3.56	RFC 2888 Secure Remote Access with L2TP.....	4-31
4.1.3.57	RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0.....	4-31
4.1.3.58	RFC 2946 Telnet Data Encryption Option.....	4-32
4.1.3.59	RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements	4-32
4.1.3.60	RFC 2979 Behavior of and Requirements for Internet Firewalls	4-32
4.1.3.61	RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0	4-32
4.1.3.62	RFC 2986 PKCS #10: Certification Request Syntax Specification Version 1.7	4-32
4.1.3.63	RFC 3053 IPv6 Tunnel Broker.....	4-33
4.1.3.64	RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS).....	4-33
4.1.3.65	RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	4-33
4.1.3.66	RFC 3369 Cryptographic Message Syntax (CMS)	4-34
4.1.3.67	RFC 3370 Cryptographic Message Syntax (CMS) Algorithms	4-34

4.1.3.68	RFC 3401 Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS.....	4-34
4.1.3.69	RFC 3402 Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm .	4-34
4.1.3.70	RFC 3403 Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database.....	4-34
4.1.3.71	RFC 3404 Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI).....	4-35
4.1.3.72	RFC 3405 Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures.....	4-35
4.1.3.73	RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).....	4-35
4.1.3.74	RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1.....	4-35
4.1.3.75	RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.....	4-36
4.1.3.76	RFC 3761 The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM).....	4-36
4.1.4	Other Security Technologies.....	4-37
4.1.4.1	IEEE Documents on Security Technologies.....	4-37
4.1.4.1.1	IEEE 802.11b Web Encryption Protocol.....	4-37
4.1.4.1.2	IEEE 802.11i Security for Wireless Networks (WPA2).....	4-37
4.1.4.1.3	IEEE Personal and Private Information (PAPI) draft standard.....	4-37
4.1.4.2	RSA Documents on Security Technologies.....	4-37
4.1.4.2.1	RSA PKCS #8 Private-Key Information Syntax Standard.....	4-37
4.1.4.2.2	RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.....	4-37
4.1.4.3	OASIS Documents on Security Technologies.....	4-38
4.1.4.3.1	OASIS Security for Grid Services.....	4-38
4.1.4.3.2	OASIS Attribute Profiles for SAML 2.0.....	4-38
4.1.4.3.3	OASIS SAML 2.0: Security Assertion Markup Language Version 2.0.....	4-38
4.1.4.3.4	OASIS Security Assertion Markup Language (SAML) V2.0.....	4-38
4.1.4.3.5	OASIS Authentication Context.....	4-38
4.1.4.3.6	Web Services Policy Framework (WS-Policy).....	4-39
4.1.4.3.7	Web Services Policy Assertions Language (WS-PolicyAssertions).....	4-39
4.1.4.3.8	Web Services Policy Attachment (WS-PolicyAttachment).....	4-39
4.1.4.3.9	OASIS Extensible Access Control Markup Language (XACML).....	4-39
4.1.4.4	World Wide Web Consortium (W3C) Documents on Security Technologies.....	4-39
4.1.4.4.1	WC3 XML Key Management Specification (XKMS 2.0) Bindings.....	4-39
4.1.4.4.2	W3C The Platform for Privacy Preferences 1.1 (P3P1.1) SpecificationW3C Working Draft 27 April 2004.....	4-40
4.1.4.5	Miscellaneous Security Technologies.....	4-40
4.1.4.5.1	AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.....	4-40
4.1.4.5.2	ANSI INCITS 359-2004 Role Based Access Control (RBAC).....	4-40
4.1.4.5.3	BCP 65 Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures.....	4-41
4.1.4.5.4	EPRI 1002596 ICCP TASE.2 Security Enhancements.....	4-41
4.1.4.5.5	NERC Certificate Policy for the Energy Market Access and Reliability Certificate (eMARC) Program Version 2.4.....	4-41
4.1.4.5.6	NIST GSC-IS The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1.....	4-41
4.1.4.5.7	NISTIR 6529 Common Biometric File Format (CBEFF).....	4-41
4.1.4.5.8	Semantic Web Pervasive Computing Standard Ontology (PERVASIVE-SO) Guide -- Describing User Profile and Preferences.....	4-42
4.1.4.5.9	Smart Card Alliance Smart Card Primer.....	4-42
4.1.4.5.10	Smart Card Alliance Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology.....	4-42

4.1.4.5.11 Smart Card Alliance Government Smart Card Handbook	4-42
4.1.4.5.12 WebDAV Access Control Extensions to WebDAV.....	4-43
4.1.4.5.13 WPA WI-FI Protected Access.....	4-43
4.1.4.5.14 WPA2 WI-FI Protected Access Version 2	4-43
4.1.4.5.15 TMN PKI - Digital certificates and certificate revocation lists profiles.....	4-43

List of Figures

<i>Figure 1: Example of SSL/TLS Tunnel for Firewall Transversal</i>	2-23
<i>Figure 2: Estimated Smart Card Storage Costs</i>	2-29
<i>Figure 3: General trend is security vulnerabilities (extracted from EPRI Report 1008988)</i>	2-39
<i>Figure 4: Simplified diagram of Public/Private Key encryption and Digital Signature</i>	2-40
<i>Figure 5: General trend is security vulnerabilities (extracted from EPRI Report 1008988)</i>	3-19
<i>Figure 6: Simplified diagram of Public/Private Key encryption and Digital Signature</i>	3-20

List of Tables

<i>Table 1: Relevant Standards/Specifications relevant to the Audit Service</i>	2-3
<i>Table 2: Typical Physical Access Control Strategies</i>	2-5
<i>Table 3: Physical Security Strategies vs. Security Services Provided</i>	2-6
<i>Table 4: References regarding Computational Resource Access Control</i>	2-9
<i>Table 5: Relevant Computational Resource Access Control Standards/Specifications</i>	2-9
<i>Table 6: References relating to Access Control for Informational Resources</i>	2-11
<i>Table 7: Reference Relevant to Encryption Technology</i>	2-13
<i>Table 8: Encryption Related Specifications/Standards</i>	2-14
<i>Table 9: Digital Certificate Related Specifications/Standards</i>	2-15
<i>Table 10: References and Specifications regarding Credential Conversion</i>	2-17
<i>Table 11: Relevant Specification regarding Credential Renewal</i>	2-19
<i>Table 12: Relevant Specifications for the Delegation Service</i>	2-21
<i>Table 13: References regarding Firewall Transversal</i>	2-23
<i>Table 14: Relevant Specifications regarding Firewall Transversal</i>	2-24
<i>Table 15: General References Regarding Identity Establishment and Identity Infrastructure</i>	2-25
<i>Table 16: Relevant Specifications regarding Identification Frameworks</i>	2-26
<i>Table 17: Relevant Standards Concerning Smart Cards</i>	2-27
<i>Table 18: Public Key Infrastructure (PKI) Related Specification/Standards</i>	2-29
<i>Table 19: Relevant Specifications for Digital Signatures</i>	2-31
<i>Table 20: Relevant References regarding Biometrics</i>	2-31
<i>Table 21: Relevant Specification regarding Biometrics and Smart Cards</i>	2-32
<i>Table 22: Relevant Specification regarding non-repudiation</i>	2-34
<i>Table 23: Relevant Specifications for the Path Routing Service</i>	2-36
<i>Table 24: Relevant Specification regarding Policy Exchange</i>	2-42
<i>Table 25: References Regarding Privacy</i>	2-43
<i>Table 26: Relevant Specification regarding Privacy</i>	2-43
<i>Table 27: Relevant Specifications regarding the Profile Service</i>	2-44
<i>Table 28: References Relating to Quality of Identity</i>	2-44
<i>Table 29: Relevant Specification for the Quality of Identity Service</i>	2-45
<i>Table 30: Relevant Specifications regarding Denial-of-Service</i>	2-47
<i>Table 31: Relevant Specifications regarding Security Assurance</i>	2-47
<i>Table 32: Potentially Relevant Specifications in regards to Security Capability Discovery</i>	2-48
<i>Table 33: Recommended Minimum Password size</i>	3-24
<i>Table 34: Relevant Articles concerning User and Group Account Management</i>	3-26

This page left intentionally blank.

1. Technologies

The technologies, services and best practices in this appendix were analyzed for the requirements that they fulfill and the IECSA environments that they are recommended to participate in. These interrelationships are best visualized as hyperlinks in the web version of the deliverable set. The source data can be found in the UML model and attached here as a Microsoft Excel file. Click the paperclip icon in the margin to the right to view this data file.



1.1 Energy Industry-Specific Technologies

1.1.1 Utility Field Device Related Data Exchange Technologies

1.1.1.1 IEC60870-5 - Telecontrol Protocol

1.1.1.1.1 IEC60870-5 Part 101 - Serial Telecontrol Protocol

URL: http://trianglemicroworks.com/mailman/listinfo/iec60870-5_trianglemicroworks.com

IEC60870-5 Part 101 was developed by IEC TC57 in WG03 as a 3-layer communications protocol standard for use by utilities for SCADA. It was designed primarily to meet the needs of real-time exchange of data between compute-constrained devices over media-constrained communication channels (typically less than 1200 bps). This protocol is widely used in Europe and other countries, but is not typically used within the United States or Canada. In these two countries, a variation of IEC60870-5 Part 101 was developed, called DNP.

Additional information on IEC60870-5 Part 101 can be obtained from the IEC

IEC TC57 Working Group 3 was one of the first organizations formed with the goal of developing a common protocol for the utility industry. It initially focused on producing an extremely reliable data link layer protocol for slow serial links. This data link layer was designed to be used in either balanced point-to-point links or unbalanced multi-drop links, with several levels of reliability which were thoroughly characterized in the annexes of the following two specifications:

- 60870-5-1 Transmission Frame Formats
- 60870-5-2 Link Transmission Procedures

The next three specifications from WG3 described in general terms the most common utility application protocol functions used by proprietary protocols at the time. These functions included such features as initialization, select-before-operate and direct controls, accumulator freezing, report-by-exception, periodic reporting, remote parameter setting, and file transfer.

- 60870-5-3 General Structure of Application Data
- 60870-5-4 Definition and Coding of Application Information Elements
- 60870-5-5 Basic Application Functions

These specifications defined the protocol in general terms only. For the details of the protocol implementation, WG3 defined several companion standards, each designed for a different application area, and selecting different a subset of features from the earlier five standards.

- 60870-5-101 Telecontrol (referred to as SCADA in North America)
- 60870-5-102 Load Profiling (energy measurement through accumulators)
- 60870-5-103 Protection Equipment (monitoring and control of relays)

These companion standards were three-layer serial protocols only, with no networking capabilities. With the advent of WANs in distribution automation, WG3 developed a standard mechanism for implementing IEC 60870-5-101 over Internet protocols:

- 60870-5-104 Telecontrol over TCP/IP

Although the 60870-5 companion standards can technically be used within a substation, TC57 has designated IEC 61850 (Working Groups 10, 11 and 12) as the primary standard within substations, while 60870-5 is to be used for telecontrol (to remote sites) only.

WG3 recently released a revised edition of the original 101 companion standard and is currently investigating security solutions for the IEC 60870-5 protocols along with Working Group 15.

Keywords: Protocol, Standard, Monitoring, Control, Protection, Physical layer, Data link layer, Application layer, LAN, WAN, Serial, High reliability, Power industry

1.1.1.1.2 IEC60870-5 Part 104 - Telecontrol Protocol over TCP/IP

URL: http://trianglemicroworks.com/mailman/listinfo/iec60870-5_trianglemicroworks.com

IEC60870-5 Part 104 was developed by **IEC TC57** in WG03 as an international standard, by placing **IEC60870-5 Part 101** over the TCP/IP Protocol stack. This permits networking of the communications for monitoring and controlling field devices through **SCADA**. This has made it less useful for compute constrained devices and media-constrained communications, but has made it significantly more useful for less constrained environments. It is equivalent to **DNP** when it runs over the TCP/IP.

A complete description of the 60870-5 parts can be found in IEC60870-5 Part 101 Description.

Keywords: Protocol, Standard, Monitoring, Control, Protection, Physical layer, Data link layer, Application layer, Serial, Power industry

1.1.1.2 DNP

1.1.1.2.1 DNP Serial Protocol

URL: <http://www.dnp.org>

DNP was developed as a three-layer asynchronous protocol suitable for use on slow serial links and radios, so like IEC 60870-5 it is strongly focused on compactness, data integrity and reliability in noisy environments. It incorporates the best features of the many proprietary protocols that preceded it, such as select-before-operate and direct controls, accurately timestamped data, broadcasting, freezing accumulators, scan groups, and report-by-exception. It also supports features that were very advanced for the time it was created, including spontaneous reporting, multiple masters, peer-to-peer communications, floating-point data, wild-card requests, file transfer, limited self-description, and vendor-extension.

Keywords: protocol, monitoring, control, SCADA, substations, field device, pole-top, serial, wireless, data link layer, application layer, multi-drop, bridging, broadcast, water utility, power utility, reliability, availability, de facto standard, open systems, consortia

1.1.1.2.2 DNP3 Protocol over TCP/IP

URL: <http://www.dnp.org>

In 2000, the DNP Technical Committee defined a specification for carrying DNP3 over TCP/IP and UDP/IP. Because the WAN/LAN version is essentially the serial DNP3 encapsulated, this makes it possible to connect serial DNP3 devices to WAN/LAN DNP3 devices using terminal servers, IP packet radios, CDPD modems, and other networking technologies without requiring the access devices to have knowledge of DNP3. DNP3 is often referred to as a SCADA protocol, but was intended for use in all areas of utility communications.

The DNP Technical Committee continues to add features to the protocol, with a mandate of maintaining backward compatibility with existing devices. Recent additions include double-bit status inputs and "attribute" objects that aid in self-description of the device. The committee is working on an XML schema for description of a DNP3 implementation, and network security features for authentication and encryption.

DNP3 Serial may use the same security technologies as those being developed by IEC TC57 WG15 for IEC60870-5 Part 101.

DNP3 WAN/LAN may use the same security technologies as those being developed by IEC TC57 WG15 for IEC60870-5 Part 104.

Advantages/Strengths: DNP is widely used within North America, and increasingly in other countries.

Disadvantages/Weaknesses: DNP does not support object models.

Keywords: LAN, WAN, local area network, wide area network, TCP/IP, UDP/IP, CDPD

1.1.1.3 IEC61334 - Distribution PLC

URL: <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=1187>

The IEC61334 Distribution PLC standard, Distribution Line Message Specification (DLMS), is used primarily for retrieving metering information using the IEC62056 metering standard over distribution power line carrier. The two most relevant documents for the DLMS User Association have reached the status of International Standards. Both were created by WG9.

- IEC 61334-4-41, 1996-03, Distributed Automation Using Distribution Line Carrier Systems Part 4: Data Communication Protocols; Section 4: Application Protocol; Clause 1: Distribution Line Message Specification (DLMS)
- IEC 61334-6 (2000-06), Distribution automation using distribution line carrier systems - Part 6: A-XDR encoding rule: Defines a set of encoding rules that may be used to derive the specification of a transfer syntax for values of types defined in the DLMS core standard using the ASN.1 notation (see IEC 61334-4-41).

Keywords: Power Line Carrier

1.1.1.4 ISO 9506 MMS - Manufacturing Messaging Specification

URL: http://www.nettedautomation.com/standardization/ISO/TC184/SC5/WG2/mms_intro/

MMS (Manufacturing Message Specification) is a messaging system for modeling real devices and functions and for exchanging information about the real device, and exchanging process data - under real-time conditions - and supervisory control information between networked devices and/or computer applications. MMS is an international standard (ISO 9506) that is developed and

maintained by the ISO Technical Committee 184 (TC184) - Industrial Automation - of the International Organization for Standardization (ISO).

The object models and messaging services provided by MMS are generic enough to be appropriate for a wide variety of devices, applications, and industries. Whether the device is a Programmable Logic Controller (PLC) or a robot, the MMS object models, services, and messages are identical. Similarly, applications as diverse as material handling, fault annunciation, energy management, electrical power distribution control, inventory control, and deep space antenna positioning in industries as varied as automotive, aerospace, petrochemical, electric utility, office machinery and space exploration have put MMS to useful work.

Keywords: ISO 9506 MMS – Manufacturing Messaging Specification
MMS, ISO 9506, Manufacturing Messaging Specification, UCA, IEC61850, services, CASM, Object Oriented services, ACSI Mapping

1.1.1.5 IEC61850 Substation Automation

1.1.1.5.1 IEC61850 - Substation Automation Communications

URL: <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=1188>

Working Groups 10 focuses on communications within substations, as opposed to distributed Telecontrol, which was the focus of Working Group 3, or communications between control centers, as in Working Group 7. Communications within the substation was divided into three levels: station, process, and unit. Initially each Working Group handled a different part of the architecture, but in later years they formed joint task forces to address mutual issues. The initial specifications focused on a “top-down” approach, characterizing the interactions between substation components at a requirements level:

- 61850-1 Introduction and Overview
- 61850-2 Glossary
- 61850-3 General Requirements
- 61850-4 System and Product Management
- 61850-5 Communications Requirements

WG 10 also have within their scope the task of developing a standard file format for exchanging information between proprietary configuration tools for substation devices. This standard is based on Extensible Markup Language (XML), and draws on the data modeling concepts found in the other parts of IEC 61850, and the capability of the IEC 61850 protocols to “self-describe” the data to be reported by a particular device.

- 61850-6 Substation Configuration Language

At about the time when the requirements parts of the work were approaching completion, WGs 10-12 became aware of the work that the Electrical Power Research Institute (EPRI) and the Utility Communications Architecture (UCA®) Forum had completed on UCA, especially on developing a standard set of services and data models for intra-substation communications. This work was incorporated into IEC 61850, with some significant modifications, in the following specifications:

- 61850-7-1 Principles and Models
- 61850-7-2 Abstract Communications Service Interface
- 61850-7-3 Common Data Classes (Object Models)

- 61850-7-4 Compatible Logical Node Classes and Data Classes (Object Models)

Most of the IEC 61850 specifications describe the protocol in a very abstract manner, and only the last parts of the standard describes “Specific Communication Service Mapping” onto a particular set of protocols. The initial protocol profiles for IEC 61850 are nearly identical to those developed for IEC 60870-6 (TASE.2) between substations, using the Manufacturing Message Specification (MMS) and both Internet and OSI protocol stacks. These are mainly full 7-layer profiles, but there are also high-speed profiles used directly over Ethernet (IEEE 802.x) LANs for “process bus” and protection tripping. The profiles are described in:

- 61850-8 Protocol Mapping

The initial intent was that IEC 61850 would be a superset of UCA 2.0 and that devices implementing the two protocol suites could interoperate

Another significant contribution of IEC 61850 is a high-speed protocol Ethernet-based protocol to be used for communications between “smart transformers” and higher level devices, to permit several different devices to simultaneously receive sampled waveform values from a given transformer in real-time:

- 61850-9 Sampled Measured Values

Parts 7.1, 7.2, 7.3, 7.4, and 9.1 of 61850 have become International Standards with the remaining protocol pieces reaching International Standard status in 2003 to early 2004. The final work in IEC 61850 will be to develop test procedures for verifying conformance to the protocol:

- 61850-10 Certification Test Procedures

1.1.1.5.2 IEC61850 Part 7-2 - GSE (GOOSE and GSSE)

URL: <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=1188>

GOOSE and GSE define a high-speed Ethernet-based protocol to be used for communications between protection devices. They are defined in Part 7-2.

The Goose and GSE services are used for fast multicast communication between a publisher and one or more subscribers. The abstract services are used for such operations as (for example) protection event notification. The most important abstract services (SendGooseMessage) in this group map onto short, connectionless stacks, although some of the administrative services (querying about dataset definitions, etc.) use full Two-Party associations.

Keywords: Generic Object Oriented Substation Event, GOOSE, Generic Sub-Station Event, UCA, IEC61850, high-speed Relay to Relay communications, binary messaging, analog data messaging, priority, virtual LAN, Ethernet communications

1.1.1.5.3 IEC61850 Part 7-2 - SMV (Sampled Measured Values)

URL: <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=1188>

SMV (Sampled Measured Values) is a service that provides streaming data for PTs and CTs. It is defined in Part 7-2 as one of the Abstract Common Services.

Keywords: Process Bus, digitized sample data, remote input/output, data synchronization, 100MB Ethernet, Optical CT/PT Interface

1.1.1.5.4 IEC61850 Part 7-2 - Abstract Common Services Interface (ACSI)

URL: <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=1188>

Communication Services are the **Verbs**. They provide the actions, such as sending and receiving data, reporting data when some event occurs, logging data, and other “actions”. In SA, there are two types of communication services: Abstract Communication Services, which must be mapped to a particular protocol (such as MMS or OPS); and PICOM, which is a unique set of services for protection relaying.

IEC61850-7-2 defines a set of abstract communication services that addresses the basic requirements for the process of exchanging information. These services include:

- Association services, where a logical connection is made between two entities, such as a substation master with a new IED. In addition, multi-cast associations are also handled. This group of services handles establishing connections, deliberate breaking connections, aborting connections (usually due to some error condition), and managing unexpected broken connections.
- Get, which requests information to be sent, including Get Logical Device Directory, Get Logical Node Directory, Get Data Values, Get Data Values Directory, and others. This service is used to monitor information.
- Set, which sends information to be used or stored, including Set Data Values. This service is used for control commands, setting parameters, and writing descriptions
- Data Sets, where data values are grouped into sets for efficient transmittal. Data Sets can be manually created as well as automatically created and deleted.
- Report Control, which manages the reporting of Data Sets upon request, at a particular periodicity (e.g. integrity scan), and upon the occurrence of pre-specified events, such as data change (e.g. closed to tripped status), quality change (e.g. a problem causes data to be invalid), data update (e.g. an accumulator value is “frozen” periodically), or integrity scan mismatch (e.g. the integrity scan indicates a different status value from the value that was last reported).
- Log Control, which manages logging and journaling of information, such as sequence of events
- Substitution Values, which manages the substitution of values if these are indicated in the Data Object classes
- GSE Messages, which handle special ultra-high-speed messaging to multiple destinations, typically for protective relaying.
- Select-Before-Operate Control, which implements the safety mechanisms used by most switch-related control commands. This procedure basically consists of: an originator of the control command first issuing a select of the control point, the receiver then performing a select and reporting the results back to the originator, the originator then issuing an execute command which the receiver performs only if it receives the execute command within a pre-specified time from the originator.
- Time Management, which handles the synchronization of time across all interconnected nodes.
- File Transfer, which handles the transfer of files between entities, without treating them as data objects. This capability supports the uploading of new applications into the IEDs and other servers.

Of these services, most are taken care of automatically by the basic communications software. The key services that are important for the substation engineer to become involved with are the Data Sets. Basic Data Sets are pre-defined: each Logical Node has an associated Data Set of all its data. However, these may not be appropriate for all users, therefore, the substation engineer

should help define the data groupings, based on substation requirements as well as other user and software application requirements.

Although clearly initial Data Sets must be defined, they can be changed at any time. Therefore, one of the requirements from the vendors must be an HMI (human-machine interface) tool that permits the easy definition and modification of these Data Sets.

Piece of Information for COMmunications (PICOM) is a term defined by CIGRE WG34.04 to describe the information passed between Logical Nodes. The components of a PICOM are:

- Data, meaning the actual data items sent from one LN to another LN
- Type of data, meaning its format
- Performance of the information exchange

The PICOMs are used primarily to define what data needs to be exchanged between protective relaying IEDs. The detailed exchange parameters of PICOMs should be part of a protective relaying vendor's package; however, the substation engineer will need to specify very precisely what protection events should trigger what actions.

The abstract objects and communication services have to be "mapped" to real-world bits and bytes, in other words, to actual communication protocols.

IEC61850 currently has two protocol mapping specified, namely, the GSE protocol for transmissions between very high speed devices (such as protection relays) and MMS over the TCP/IP suite of protocols. However, the OM-DA object models can also be transmitted using some other mappings to protocol profiles, although some protocols can manage objects better than others. For instance, MMS and XML (over any lower layer network protocols) can utilize the object models completely. However, XML does not specify the communication services (when to send, triggered by what, etc.). So an underlying service capability must be added, most of which do not handle some of the more powerful services like data sets.

The initial protocol profiles for IEC 61850 are nearly identical to those developed for IEC 60870-6 (TASE.2) between substations, using the Manufacturing Message Specification (MMS) and both Internet and OSI protocol stacks. These are mainly full 7-layer profiles, but there are also high-speed profiles used directly over Ethernet (IEEE 802.x) LANs for "process bus" and protection tripping.

Keywords: Protocol, ACSI, Abstract Common Services Interface, CASM, Common Services, interoperability, Specific Communication Service Mappings, SCSM

1.1.1.5.5 IEC61850 Parts 7-3 and 7-4 - Substation Object Modeling

IEC61850 Parts 7-3 and 7-4 comprise the Substation Object Models. These two Parts of the IEC 61850 specifications describe the object models as abstract objects, and only the last parts of the standard describes "Specific Communication Service Mapping" onto a particular set of protocols.

Object Models (OM) are Nouns with pre-defined names and pre-defined data structures. Objects are the data that is exchanged among different devices and systems.

The figure below illustrates Object Models. The OM rests on top of the SM services model and the CP communications protocols.

It should be noted that new object models are continually being developed. Specifically, work is under way to add a suite of Power Quality object models to deal with sag, swell, harmonics, snapshots, and a variety of averaged values.

The OM structure from the bottom up is described below:

- Standard Data Types: common digital formats such as Boolean, integer, and floating point.
- Common Attributes: predefined common attributes that can be reused by many different objects, such as the Quality attribute. These common attributes are defined in IEC61850-7-3 clause 6.
- Common Data Classes (CDCs): predefined groupings building on the standard data types and predefined common attributes, such as the Single Point Status (SPS), the Measured Value (MV), and the Controllable Double Point (DPC). In essence, these CDCs are used to define the type or format of Data Objects. These CDCs are defined in IEC61850-7-3 clause 7.
- Data Objects (DO): predefined names of objects associated with one or more Logical Nodes. Their type or format is defined by one of the CDCs. They are listed only within the Logical Nodes. An example of a DO is “Auto” defined as CDC type SPS. It can be found in a number of Logical Nodes. Another example of a DO is “RHZ” defined as a SPC (controllable single point), which is found only in the RSYN Logical Node.
- Logical Nodes (LN): predefined groupings of Data Objects that serve specific functions and can be used as “bricks” to build the complete device. Examples of LNs include MMXU, which provides all electrical measurements in 3-phase systems (voltage, current, watts, vars, power factor, etc.); PTUV for the model of the voltage portion of under voltage protection; and XCBR for the short circuit breaking capability of a circuit breaker. These LNs are described in IEC61850-7-4 clause 5.
- Logical Devices (LD): the device model composed of the relevant Logical Nodes. For instance, a circuit breaker could be composed of the Logical Nodes: XCBR, XSWI, CPOW, CSWI, and SMIG. Logical Devices are not directly defined in any of the documents, since different products and different implementations can use different combinations of Logical Nodes for the same Logical Device. However, many examples are given in IEC61850-5.

Keywords: Protocol, Substation Object Mapping, Object Modeling, Substation Object Mapping, Common Data Classes, Basic communication structure, abstract definitions, common attribute types, data attribute

1.1.1.5.6 IEC61850 Part 6 - Substation Configuration Language

Abstract configuration languages provide a mechanism for describing how real-world components are actually connected to each other. Two such configuration languages have been defined to date in the utility industry:

- Substation Configuration Language SCL for the configuration of equipment within substations
- Common Information Model (CIM) for the overall configuration of the power system, from corporate ownership through the lines, substations, and feeders, down to the customer sites.

The concept of a **configuration language** is that the configuration of the substation can be modeled electronically using object models, not just the data in the substation. This model of the substation configuration allows applications to “learn” how all the devices within a substation are actually interconnected both electrically and from an information point of view.

The Substation Configuration Language (SCL), IEC61850 Part 6, defines the interrelationship of the substation equipment to each other and to the substation itself. Although the substation object

models define each of the devices in the substation, these device models do not define how the models are interrelated. Therefore Part 6 was developed to provide a tool for defining the substation configuration.

The SCL uses a standard file format for exchanging information between proprietary configuration tools for substation devices. This standard is based on Extensible Markup Language (XML), and draws on the data modeling concepts found in the other parts of IEC 61850, and the capability of the IEC 61850 protocols to "self-describe" the data to be reported by a particular device.

An effort is underway to "harmonize" this configuration language with the similar object models of the Common Information Model (CIM). The work to do this is also still under development through the IEC. However, when it is completed, it may become very important in future more sophisticated functions that would benefit from having substation configuration information available and updated electronically.

Even if this configuration language is not immediately used within a utility's operations, it should be required from the appropriate substation automation vendor, probably the vendor of the substation master.

Keywords: Protocol, Substation Configuration Language, SCL, XML, IED configuration, schema, substation automation system, communication system configuration data

1.1.1.5.7 IEC61850 Power Quality Object Models

IEC TC57 WG10 is currently developing object models for power quality.

1.1.1.6 IEC62350 - Object Models for Distributed Energy Resources (DER)

URL: <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=2613>

Object models for Distributed Energy Resources (DER) are being developed in the IEC TC57 WG17 and for Wind Turbines, in IEC TC88 WG25, to become international standards for communicating with DER systems. These object models are based as much as possible on the IEC61850 object modeling concepts and core components. In particular they use existing Common Data Classes (CDCs) and Logical Nodes (LNs) where these meet the requirements. They only add new CDCs and LNs where these are necessary for the unique characteristics of DER devices and systems.

The scope of the DER object modeling is illustrated in the Figure 1 below, while Figure 2 provides a list of the DER object models. In 2003 a draft of the DER object document was submitted to the IEC as a starting draft for the DER object models, and the first meeting of the WG was held in April 2004.

Working Group 17 is tasked with making recommendations and standards for communication with Distributed Energy Resource Devices. The development of the standard is requirements driven but through participation of WG members familiar with IEC 61850, a high degree of re-use and compatibility with IEC 61850 is anticipated.

Advantages/Strengths

The DER object models meet the IECSCA High Level Concepts of using abstract information modeling as a core method. These object models will support interoperability among the many stakeholders that need to exchange information with DER systems. These include the DER Owners, Marketers, Distribution System Operators, DER Operators, Distribution System Maintenance, and DER Device Maintenance personnel.

Disadvantages/Weaknesses

At this time (early 2004) object models for only three DER device types have been developed as drafts. The DER object models are only in draft form, and still require significant review by the IEC working groups.

Keywords: DER, Distributed Energy Resources, ADA, Advanced Distribution Automation, Object Models, Distributed Resources, DR, distributed generation, alternative energy, Logical Nodes, LN, CDC, distribution system

1.1.1.7 IEC62349 - Hydro Power Plant Object Models

URL: <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=2614>

IEC TC57 WG18 is tasked with making recommendations and standards for communication with hydroelectric power plants. The development of the standard is requirements-driven but through participation of WG members familiar with IEC 61850, a high degree of re-use and compatibility with IEC 61850 is anticipated.

Keywords: Hydroelectric power plants, object models, turbine models, IEC61850, CDC, Logical Nodes, Object Models

1.1.1.8 IEC61400-25 for Wind Power Object Models

URL: <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=2199>

IEC TC88 WG25 is tasked with writing a communications standard for the wind power industry. The standard will facilitate communications among a collection of wind machines and other equipment within a wind power plant (WPP) as well as with equipment and systems external to the WPP. The development of the standard (IEC 61400-25) is requirements driven but through participation of WG members familiar with IEC 61850, a high degree of re-use and compatibility with IEC 61850 is anticipated. It is expected that Web Services, rather than ISO 9506 MMS, will be used as the protocols to exchange the data.

Keywords: Wind Power Plants, WPP, web services, IEC61850, object models, CDC

1.1.1.9 Fieldbus

URL: <http://www.fieldbus.org>

The non-profit Fieldbus Foundation promotes and maintains a popular local-area “bus” communications specification for use in industrial automation, particularly in instrumentation and control. This specification is known as “Foundation Fieldbus”, distinguished from the generic term “fieldbus” which may apply to several different technologies.

Foundation Fieldbus is a three-layer protocol suite plus object model specifications, known as “function blocks” defined above the application layer. It includes self-description in the form of “Device Description” (DD) files that use a standard (non-XML) language specific to Foundation Fieldbus.

The data link layer is listed among several technologies complying IEC61158: “Digital Data Communication for Measurement and Control - Fieldbus for use in Industrial Control Systems”.

The data link layer uses a “deterministic bus scheduler” to control access to the bus using token passing. The application layer, the Fieldbus Message Specification (FMS) uses a publish/subscribe model and resembles the Manufacturing Message Specification (MMS) that is the core of IEC61850.

The standard Foundation Fieldbus physical layer is a multi-drop 31.25Kbps, “intrinsically safe” physical layer known as H1. H1 networks may be accessed from Ethernet networks through a “Linking Device” using a “High Speed Ethernet (HSE)” profile that includes TCP/IP, UDP/IP and SNMP, or devices may support only HSE. The HSE specification pays special attention to redundancy in Ethernet LANs.

Keywords: Industrial automation, LAN, WAN, Multi-drop, Serial, Physical layer, Data link layer, Application layer, Gateway, Information model

1.1.1.10 PROFIBUS

URL: <http://www.profibus.org>

The non-profit PROFIBUS User Organization, as a part of the worldwide organization PROFIBUS International, promotes and maintains a set of extremely popular specifications for local-area “bus” communications in industrial and process automation. PROFIBUS is also frequently used in power systems devices. The current PROFIBUS is actually PROFIBUS DP (Decentralized Periphery), which replaces an earlier PROFIBUS FMS (Fieldbus Message Specification). PROFIBUS FMS resembled the current IEC61850 profile, while DP is a much more compact protocol suite.

The core of PROFIBUS DP is a data link layer that is simultaneously token-passing (between master devices) and polled (from masters to slaves), enabling deterministic bus access with high bandwidth utilization. The data link layer comes in several options and operates over a variety of physical layers. It is usually implemented in hardware. The approved physical media include RS485, RS485-IS (Intrinsically Safe), Manchester-coded Bus, Powered (MBP), and fiber optics, at rates from 9600bps to 12Mbps.

To aid in interoperability, the PROFIBUS User Organization has defined several application layer profiles dedicated to specific uses such as factory automation, process automation, and motion control.

PROFIBUS is listed among several “field buses” conforming to IEC 61158: “Digital Data Communication for Measurement and Control - Fieldbus for use in Industrial Control Systems” and IEC 61784: “Profile Sets for Continuous and Discrete Manufacturing Relative to Fieldbus Use in Industrial Control Systems”.

Access to PROFIBUS networks and data from IP-based Ethernet networks is achieved through PROFINet gateways, which use an object-oriented application layer using DCOM and XML over TCP/IP.

Keywords: Industrial automation, LAN, WAN, Multi-drop, Serial, Physical layer, Data link layer, Application layer, Gateway, Information model

1.1.1.11 ModBus

1.1.1.11.1 ModBus

URL: <http://www.modbus.org>

MODBUS® Protocol is a messaging structure developed by Modicon® in 1979, used to establish master-slave/client-server communication between intelligent devices. It is a de facto standard and a widely used network protocol in the industrial manufacturing environment.. It is implemented by hundreds of vendors on thousands of different devices in order to transfer

discrete/analog I/O and register data between control devices. In the power industry, it is used predominantly within substations.

Keywords: Modbus, Modicon, Modbus RTU, RS-485, register based, serial communications, PLC, interface for distributed automation, master-slave

1.1.1.11.2 ModBus TCP/IP

URL: [http:// www.modbus.org](http://www.modbus.org)

An open MODBUS® TCP/IP specification was developed in 1999 in order to provide a networking version of ModBus. It is based on Ethernet and TCP/IP.

Keywords: Modbus, Ethernet, TCP/IP, Modbus application layer, function codes, register mapping, interface for distributed automation, Modicon, multi-master

1.1.1.11.3 ModBus Plus

URL: [http:// URL: http://www.modicon.com/opennetworking/modbus/](http://www.modicon.com/opennetworking/modbus/)

MODBUS PLUS is a protocol using a Token Ring network topology with a physical access based on a transmission speed to 1 Mb/s. The ModBus Plus protocol uses MODBUS messaging for the application layer, and the HDLC protocol for the network layer.

Keywords: Modbus Plus, peer to peer, token exchange, high speed, EIA/TIA/RS-485, multi-master, point to point, self-healing

1.1.1.12 IEEE 1451 Standard for a Smart Transducer Interface for Sensors and Actuators

URL: <http://ieee1451.nist.gov>

The objective of this project is to develop a smart transducer interface standard, where a transducer is defined as a sensor or an actuator. This standard is intended to make it easier for transducer manufacturers to develop smart devices and to interface those devices to networks, systems, and instruments by incorporating existing and emerging sensor- and networking technologies. There are four working groups, each addressing a different area:

- P1451.1 - Common object model for smart transducers along with interface specifications for the components of the model. Published as IEEE 1541.1-1999.
- P1451.2 - Smart transducer interface module (STIM), a transducer electronic data sheet (TEDS), and a digital interface to access the data. Published as IEEE 1451.2-1997.
- P1451.3 - Digital communication interface for distributed multidrop systems. In progress.
- P1451.4 - Mixed-mode communication protocol for smart transducers. In progress.

Keywords: Protocol, Multi-drop, Sensors, Standard, Pending standard

1.1.1.13 Digital Time Division Command/Response Multiplex Date Bus, MIL-STD-1553

URL: <http://assist.daps.dla.mil/docimages/0001/86/42/1553B.PD0>

"MIL-STD-1553 is a military standard that defines the electrical and protocol characteristics for a data bus. A data bus is used to provide a medium for the exchange of data and information between various systems. It is similar to what the personal computer and office automation industry has dubbed a Local Area Network (LAN)."

MIL-STD-1553 is master / slave redundant bus protocol for achieving command and control (SCADA) in a military device environment. It provides for deterministic exchange between nodes on the bus of information. Multiple bus masters may exist on the bus and can compete for the right to master the bus at any given time. There is a substantial effort in this standard to support high availability of services and graceful degradation due to failure of bus nodes and segments.

Keywords: MIL-STD-1553, Time division multiplex, Command/response, LAN, SCADA, Deterministic communications

1.1.1.14 IEEE C37.94 - Standard for N x 64 kbps Optical Fiber Interfaces between Teleprotection and Multiplexer Equipment

URL: <http://standards.ieee.org/>

This Standard describes the communication interconnection details for directly connecting digital relays into digital multiplexers via a pair of fiber optic fibers. The variable "N" (where N = 1,2...12) describes a multiple of 64 kilobit per second connections at which the communication link is to operate (from 64,000 bps up to 768,000 bps). Requirements for both physical connection and the communications timing are also included. Primary applications include digital current differential relay communications and substation to substation relay communications.

Keywords: teleprotection, multiplexer, multimode optical fiber, alarm indication signal, bit error rate, cyclic redundancy check, loss of signal, remote defect indication, unit interval, loss of frame

1.1.1.15 C37.111-1999 IEEE COMTRADE Standard (Common Format for Transient Data Exchange) for Power Systems

URL: <http://standards.ieee.org/>

COMTRADE provides a common format for the data files and exchange medium needed for the interchange of various types of fault, test, or simulation data is defined. Sources of transient data are described, and the case of diskettes as an exchange medium is recommended. Issues of sampling rates, filters, and sample rate conversions for transient data being exchanged are discussed. Files for data exchange are specified, as is the organization of the data.

Keywords: Configuration file, Data file, Header file, Transient data

1.1.1.16 IEEE 1159.3 - Power Quality Data Interchange Format (PQDIF)

URL: <http://grouper.ieee.org/groups/1159/3/index.html>

PQDIF is a recommended practice for a file format suitable for exchanging power quality related measurement and simulation data in a vendor independent manner. Appropriate definitions and event categories were developed by various task forces under the IEEE Standards Coordinating Committee 22 (SC22) on Power Quality and the IEEE 1159 Working Group on Power Quality Monitoring. A variety of simulation, measurement and analysis tools for power quality engineers are now available from many vendors. Generally, the data created, measured, and analyzed by these tools are incompatible between vendors. The 1159.3 file format provides a common ground that all vendors could export to, import from to allow the end user maximum flexibility in choice of tool and vendor. 1159.3 is considered a significant superset of the data interchange provided by the IEEE COMTRADE format (C37.111-1191)

Keywords: PQDIF, COMTRADE, Power quality, Data exchange

1.1.2 IEEE Guides for Communications in Power Systems

1.1.2.1 487-2000 - IEEE Recommended Practice for the Protection of Wire-Line Communication Facilities Serving Electric Supply Locations

URL: <http://standards.ieee.org/>

Specifies methods for electrically protecting wire-line communication circuits entering electric supply locations such as substations. This document covers: the electric supply location environment; protection apparatus; services types, reliability, service performance objective classifications, and transmission considerations; protection theory and philosophy; protection configurations; installation and inspection; and safety.

Keywords: Physical layer, Substations, Media

1.1.2.2 643-1980 (R1992) - IEEE Guide for Power-Line Carrier Applications

URL: <http://standards.ieee.org/>

This is a general guide for users of communications carrier equipment as applied on power-transmission lines. It discusses general characteristics of PLC and provides procedures for calculating channel performance. It discusses various PLC components and procedures for selecting frequencies.

Keywords: Physical layer, Power line carrier, Media

1.1.2.3 1138-1994 - IEEE Standard Construction of Composite Fiber Optic Ground Wire (OPGW) for Use on Electric Utility Power Lines

URL: <http://standards.ieee.org/>

This standard specifies the construction, components, mechanical and electrical performance, installation guidelines, acceptance criteria, test requirement and methods for composite overhead ground wire with optical fibers, commonly known as OPGW. The IEEE reaffirmed this standard in 2002.

Keywords: Physical layer, Fiber optic, Media

1.1.2.4 C37.93-1987 (R1992) IEEE Guide for Power System Protective Relay Applications of Audio Tones Over Telephone Channels

URL: <http://standards.ieee.org/>

This is a tutorial and reference guide to understanding communications between protective relays using audio signals over leased telephone channels. It discusses the characteristics of leased lines in general and provides specific examples of several offerings available at the time of publishing.

Keywords: Physical layer, Media, Audio, Protection signal

1.1.2.5 1390-1995 IEEE Standard for Utility Telemetry Service Architecture for Switched Telephone Network

URL: <http://standards.ieee.org>

Description: This standard describes a utility telemetry service architecture operated over the telephone network. The architecture described is a basic transport architecture capable of supporting many different applications. The text is described in terms of a utility meter reading application, but any enhanced service provider (ESP) communication can be transported. Telemetry calls may be initiated by either the utility/service provider (outbound) or the telemetry interface unit (TIU)/CPE (inbound) on the end user's premise.

Keywords:

1.1.3 Utility Control Center Related Data Management Technologies

1.1.3.1 IEC 60870-6 (ICCP)

URL: <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=1186>

The IEC60870-6 Telecontrol Application Service Element 2 (TASE.2) protocol (informally known as the InterControl Center Communications Protocol (ICCP)) was developed by IEC TC57 WG07 for data exchange over Wide Area Networks (WANs) between a utility control center and other control centers, other utilities, power plants and substations.

TASE.2 (ICCP) is used in almost every utility for inter-control center communications between SCADA and/or EMS systems. It is supported by most vendors of SCADA and EMS systems.

Since it was first developed in the mid 1990's before object models had been developed for SCADA applications, TASE.2 (ICCP) was not designed to support the transfer of different types of object models, beyond those defined in Part 802.

The TASE.2 protocol allows for data exchange over Wide Area Networks (WANs) between a utility control center and other control centers, other utilities, power plants and substations.

- 60870-6-503 Services and Protocol - This part of IEC 60870 defines a mechanism for exchanging time-critical data between control centers. In addition, it provides support for device control, general messaging and control of programs at a remote control center. It defines a standardized method of using the ISO 9506 Manufacturing Message Specification (MMS) services to implement the exchange of data. The definition of TASE.2 consists of three documents. This part of IEC 60870 defines the TASE.2 application modeling and service definitions.
- 60870-6-602 Transport Protocols - This Technical Report describes the Transport Profiles for the IEC 60870-6 Series over WAN with Reference to International Standardized Profiles (ISP's) used by distributed SCADA/EMS applications in control centers, power plants and substations. The Transport Profiles use virtually any standard or de-facto standard (including TCP/IP) connection-mode and connectionless-mode network services over any type of transmission media.
- 60870-6-702 Profiles - This specification defines the Application Profile (Layers 5-7) for use with ICCP. It is needed for vendors implementing protocol stacks that support the ICCP application layer. Most users of ICCP will not be concerned with this specification.
- 60870-6-802 Object Model - This part of IEC 60870 proposes object models from which to define object instances. The object models represent objects for transfer. The local system may not maintain a copy of every attribute of an object instance.

Keywords:

1.1.3.2 IEC 61970 - CIM, CIM Extensions, and GID

1.1.3.2.1 IEC 61970 Part 3 - Common Information Model (CIM)

URL: <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=1634>

The Common Information Model (CIM) is an abstract model that represents all the major power system objects in an electric utility enterprise, including some organizational and ownership aspects, but focusing on power system connectivity. The “instantiation” of a CIM power system model (conversion from an abstract model into a specific configuration of a specific utility’s power system) provides the information that is typically needed by power flow topology models used by multiple applications, such as the EMS and DMS Network Analysis applications. This model includes public classes and attributes for these objects, as well as the relationships between them.

The CIM was initially developed under the aegis of EPRI as the Control Center API (CCAPI) research project (RP-3654-1) project. It is currently undergoing standardization through the IEC TC57 WG13, as the document IEC 61970. The following descriptions of the CCAPI concepts are derived from excerpts from the introduction to the IEC document and other submissions to the IEC.

The purpose of the CIM is to produce standard interface specifications for "plug-in" applications for an electric utility power control center Energy Management System (EMS) or other system performing the same or similar functions. A "plug-in" application is defined to be software that may be installed on a system with minimal effort and no modification of source code. This standard facilitates installation of the same application program on different platforms by reducing the efforts currently required.

- 61970-1 Guidelines and General Requirements - This part of the standard, IEC 61970-1, provides a set of guidelines and general infrastructure capabilities needed for the application of the EMSAPI interface standards. This part describes the reference model that provides the framework for the application of the other parts of the EMSAPI standards. This reference model is based on component technology that places the focus of the standards on component interfaces for information exchange between applications in a control center environment. The model is also applicable to similar information exchanges between control center applications and systems external to the control center environment, such as Distribution Management Systems (DMS).
- 61970-2 Glossary
- 61970-3 Information Model - This part of the standard, IEC 61970-301, defines the CIM Base set of packages, which provides a logical view of the physical aspects of Energy Management System information. Part IEC 61970-302 defines the financial and energy scheduling logical view. Part IEC 61970-303 defines the SCADA logical view. The CIM is an abstract model that represents all the major objects in an electric utility enterprise typically needed to model the operational aspects of a utility. This model includes public classes and attributes for these objects, as well as the relationships between them.
- 61970-5 Interface Technology Mapping. Since the Level 1 CIS documents are independent by design of the underlying infrastructure technology, they must be mapped to specific technologies for implementation purposes. To ensure interoperability, there must be a standard mapping for each interface to each technology. For example, if Java is the chosen implementation technology, then there needs to be a standard mapping of the publishing and event subscription services specified in the Level 2 CIS document to Java services.

Keywords: Object modeling, UML, Enterprise VP, Computational VP

1.1.3.2.2 CIM Extensions for Market Operations

URL:

Some work sponsored by EPRI is undertaking the development of CIM-based object models for Market Operations. The exact future of these object models is unclear at this time.

Keywords:

1.1.3.2.3 IEC 61970 Part 4 - Generic Interface Definition (GID)

URL:

The Generic Interface Definition (GID) is part of IEC61970 and comprises Part 4

- 61970-4 Component Interfaces - The purpose of the Part 4 CIS documents is to specify the interfaces that a component shall use to facilitate integration with other independently developed components. Although typical applications and functions are identified in Annex B to assist in defining the types of information that must be transferred, the purpose is not to attempt to define components per se. The component vendors should be free to package different collections of component interfaces into component packages while still remaining compliant with the EMSAPI standards.
- 401 - Part 401 provides a framework for the specification of the Level 1 Functional Requirements documents. It explains the separation of these specifications into two major groups. One group of standards defines the generic services that a component can use for exchanging information with another component or for accessing public data. The other group defines the information content of messages that a component or system exchanges with other components. Part 401 provides an overview of the generic services defined for the CIS standards. These specifications describe in narrative terms with text, Unified Modeling Language (UML) notation, and Interface Definition Language (IDL), the interface functionality that is standardized. These specifications define the generic services that can be used by any application to exchange information with another application or for public data access. It also provides a roadmap to explain the contents of each of the specifications in this series and the underlying industry de facto standards that are incorporated.
- 402 - These base services incorporate the following industry de facto standards. 402 Includes IECTC57 Namespace - a mechanism by which the CIM is presented via TC 57 API's. That is, it is essentially an agreement on how to communicate the CIM hierarchies via an OPC/DAIS API.
- 403 - Generic Data Access. This part contains the API services that are needed to access public data based on the CIM organization of information. In other words, a client can access data maintained by another component (either an application or database) or system without any knowledge of the logical schema used for internal storage of the data. Knowledge of the CIM is sufficient. This request and reply-oriented service is intended for synchronous, non-real time access of complex data structures as opposed to high-speed data access of SCADA data, for example, which is provided by Part 404, High Speed Data Access. An example where Request and Reply would be used is for bulk data access of a persistent store to initialize a State Estimator application with the current state of a transmission network, and then storage of the results with notification.

- 404 - High Speed Data Access. This part contains the API services needed for high-speed access of simple data structures, where multiple instances are typically accessed as a data group and need to be efficiently mapped to variables in the client memory space. Typically data groups will be predefined and then published at either periodic intervals or upon change, although it is also possible to use this API with a request and reply data exchange pattern for these same data groups.
- 405 - Generic Eventing and Subscription. This part contains the API services needed for a general-purpose capability to publish and subscribe to events and alarms. This includes the ability to publish and subscribe to topics. It also supports the event “send and forget” data exchange pattern, where events are simply published once, with no knowledge on the part of the server of the intended recipients. An example application is for alarms, where the server capability to publish alarm events and the client capability to subscribe to selected alarms is needed.
- 407 - Time Series Data Access. . This part contains the API services needed for access time series data. This includes the ability for request/reply as well as publish/subscribe oriented exchanges.

Keywords:

1.1.3.3 OPC

URL: www.opcfoundation.org

OPC is a foundation dedicated to open connectivity in industrial automation and the enterprise systems that support industry. To this aim, OPC has created a series of open standards specifications with the goal of assuring interoperability. Based on fundamental standards and technology of the general computing market, the OPC Foundation adapts and creates specifications that fill industry-specific needs. OPC will continue to create new standards as needs arise and to adapt existing standards to utilize new technology. There are currently seven standards specifications completed or in development, of which the following four are the most important to the power industry.

1.1.3.3.1 OPC Data Access (DA)

URL: www.opcfoundation.org

OPC is a foundation dedicated to open connectivity in industrial automation and the enterprise systems that support industry. To this aim, OPC has created a series of open standards specifications with the goal of assuring interoperability. Based on fundamental standards and technology of the general computing market, the OPC Foundation adapts and creates specifications that fill industry-specific needs. OPC will continue to create new standards as needs arise and to adapt existing standards to utilize new technology. There are currently seven standards specifications completed or in development.

At a high level, an OPC Data Access Server is comprised of several objects: the server, the group, and the item. The OPC server object maintains information about the server and serves as a container for OPC group objects. The OPC group object maintains information about itself and provides the mechanism for containing and logically organizing OPC items. The OPC Groups provide a way for clients to organize data. For example, the group might represent items in a particular operator display or report. Data can be read and written. Exception based connections can also be created between the client and the items in the group and can be enabled and disabled as needed. An OPC client can configure the rate that an OPC server should provide the

data changes to the OPC client. IEC TC57 WG13's Part 403 High Speed Data Access is based on OPC DA.

Keywords: Computational VP, Widespread usage

1.1.3.3.2 OPC Historic Data Access (HDA)

URL: www.opcfoundation.org

Historical engines today produce an added source of information that must be distributed to users and software clients that are interested in this information. Currently most historical systems use their own proprietary interfaces for dissemination of data. There is no capability to augment or use existing historical solutions with other capabilities in a plug-n-play environment. This requires the developer to recreate the same infrastructure for their products, as all other vendors have had to develop independently with no interoperability with any other systems.

Keywords: Computational VP, Widespread usage

1.1.3.3.3 OPC Alarming and Eventing

URL: www.opcfoundation.org

These interfaces provide the mechanisms for OPC Clients to be notified of the occurrence of specified events and alarm conditions. They also provide services that allow OPC Clients to determine the events and conditions supported by an OPC Server, and to obtain their current status. Events can consist of XML messages, thus OPC Alarming and Eventing can provide a generic client/server oriented publish/subscribe API.

Keywords: Computational VP, Widespread usage

1.1.3.3.4 OPC Command

URL: www.opcfoundation.org

This specification describes interfaces which are implemented by any OPC Servers (e.g. Data Access, Alarm & Event, Batch) with a need for commands, and which provide the mechanisms for OPC Clients to be notified of the occurrence of specified command state and result information. These interfaces also provide services that allow OPC Clients to determine the commands supported.

The basis for the execution of an OPC command is the Finite State Machine (FSM). The FSM is an object that precisely describes the behavior of the command in terms of states, transitions, transition conditions, events, and actions. This provides the mechanism to convey information about the method and sequence of the command's execution. The FSM includes the triggering stimulus and resulting actions related to each state transition within the process as well as status and error data associated with resultant states.

Keywords: Computational VP, Limited usage

1.1.3.4 IEC61968 SIDM System Interfaces for Distribution Management

URL: <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=1635>

IEC TC57 WG14 is developing a set of documents that identify and establish requirements for standard interfaces of a Distribution Management System (DMS) based on an interface

architecture. These documents will define interfaces for the major elements of Distribution Management Systems. Subsequent standards will be developed in accordance with the interfaces defined in this task.

- Part 1 - Interface Architecture and General Requirement
- Part 2 - Glossary
- Part 3 - Interface Standards for Network Operation
- Part 4 - Interface Standards for Records and Asset Management
- Part 5 - Interface Standards for Operational Planning and Optimization
- Part 6 - Interface Standards for Maintenance and Construction
- Part 7 - Interface Standards for Network Extension Planning
- Part 8 - Interface Standards for Customer Inquiry
- Part 9 - Interface Standards for Meter Reading and Control
- Part 10 - Interface Standard for Systems External to, But Supportive of, Distribution Management
- Part 11 - Common Information Model

Keywords: SIDM, TC57, DMS, Meter reading, Network extension planning, Enterprise VP

1.1.3.5 IEC62325 on Framework for Energy Market Communications

URL: [<urls>](#)

The main purpose of the IEC62325 document on Market Transactions is to provide energy market specific requirements and technology *independent* guidelines to show how to use Internet technologies in energy markets as an alternative to EDIFACT, X12 or proprietary e-business solutions using the Internet or Extranets based on TCP/P. The explanations given are not intended as a textbook and are only introductory for better understanding. This document provides for energy markets:

- A description of the energy market specific environment
- The definition of the application requirements for e-business
- An example of the energy market structure
- An introduction in the modeling mythology
- Network examples
- A general assessment of communication security

Keywords: Market Operations

1.1.3.6 NERC e-tagging

URL: <http://reg.tsin.com/Tagging/e-tag/Tagging%20Essentials.pdf>

The electronic Transaction Information System (TIS) implemented by NERC is a process of electronically communicating a request for, securing approval of, and recording an energy transaction via the Internet. The process is more commonly referred to as Electronic Tagging, or ETAG.

The scheduling of energy transfers has historically been done on a coordinated basis between control areas. The path chosen, where more than one adjacent control area was involved, was arranged in a sequential manner from control area to control area (contract path). However, since electricity follows the laws of physics and not economics, some of the energy transferred would flow through other systems not involved in the “contract path”, resulting in what are called “parallel flows” on those systems.

The shortcomings of the contract path approach were known to utilities from its inception. However, the limitations were acceptable because the transfers were limited and small in nature. As energy transfers became more numerous and complex, however, the parallel flows on systems off the contract path began to cause serious economic and operational problems. Many utilities began experiencing overloads on their transmission lines without any idea of the source of the additional flows. Firm and non-firm energy schedules had to be canceled, resulting in lost revenues, because the origin of non-compensated flows was unknown.

NERC has implemented a Transaction Information System (TIS) in an effort to provide system operators with the identity of the source of parallel flows impacting their systems. Each energy transaction is identified through a “tag” and its impact on the transmission grid calculated utilizing power transfer distribution factors in a process called the Interchange Distribution Calculator (IDC). This calculation generally is performed “after the fact” in case of an overload, and not before the transaction is initiated. The object is to provide a rational and economically equitable basis for curtailing transactions. While minimizing the need for curtailments, the process does not, however, eliminate the need for them.

The first attempt to secure energy transaction information was by means of an Excel spreadsheet-based tag entry and retrieval system, which utilized faxes and Internet e-mail to transport tags between parties involved in a transaction. However, e-mail had inherent problems with timely delivery of the tag information and the concern that multiple copies of the tag were distributed and sometimes corrupted or changed. At the same time the specification of the tag information was not rigorous and thus the data could be interpreted in different ways.

What was needed was an electronic system, which would ensure that tags get sent, received, and approved in a timely, reliable manner. Such a system would take full advantage of automation of processes such as data validation and reduce the need for operator intervention.

In its November, 1998 resolution adopting the Constrained Path Method (CPM) as the basis for determining interchange transaction curtailment priorities as part of the Transmission Line Loading Relief (TLR) procedure, the NERC Operating Committee directed that such an electronic system be developed. A document, Electronic Tagging - Functional Specifications, was subsequently produced by the NERC Transaction Information System Working Group. The document describes the functional requirements and detailed technical specifications for the implementation of ETAG. The document did not specify the type of software or graphical interfaces to be used, leaving these up to the vendor community. Numerous vendors are currently offering ETAG products and a list of them can be found on the NERC website.

Keywords: NERC, Reliability, Constrained Paths, Line Loading Relief, Etaging

1.1.3.7 NAESB OASIS for Market Transactions

URL: http://www.naesb.org/weq/weq_ess_oasis_2_doc.asp

OASIS (Open Access Same-Time Information System) was mandated by FERC, and specifies the methods and information that must be exchanged between Market Participants and Market Operators for market transactions in the wholesale electric industry, including provisions for both a physical and financial rights market.

OASIS Phase I was developed under the aegis of NERC (the “How Group”), and is basically implemented as a Web Server that accepts the strictly defined OASIS templates as the mechanism to exchange the required data. Although this has worked well, it is very limited in its capabilities. Therefore, NAESB’s OSC group has started the development of OASIS Phase II.

OASIS II is specifically meant to refer to a set of common, standardized business functionality and associated supporting electronic communication interfaces implemented between cooperating entities (e.g., market participants, market operators, etc.), and is not meant to correspond to any one or group of specific systems that implement that interface. The primary scope of OASIS II is to define the functionality of these systems and the communications standards to exchange data among these systems and the users of these systems.

- The OASIS II Use Cases, which will describe all in-scope business processes, business objects, and their associated logic.
- The OASIS II Requirements, which will support the Use Cases by detailing specific requirements and metrics
- The OASIS II Structural Design, which will describe the technical architecture and how functionality will be staged for deployment
- The OASIS II Implementation Plan, which will indicate the order and timeline of how the stages will be specified, developed, and deployed
- The OASIS II Standards and Communications Protocols, which will describe the data exchanges between the various OASIS systems and their associated business logic, and
- The OASIS II Business Practices Standards, which will indicate North-American standards to be considered when utilizing the OASIS Phase II system.

Keywords: Market operations, Market Participants, NERC, NAESB

1.1.3.8 OPEN GIS

URL: [<urls>](#)

The vision of OpenGIS® is a world in which everyone benefits from geographic information and services made available across any network, application, or platform. Approximately 80% of business and government information has some reference to location, but until recently the power of geographic or spatial information and location has been underutilized as a vital resource for improving economic productivity, decision-making, and delivery of services. We are an increasingly distributed and mobile society. Our technologies, services, and information resources must be able to leverage location, (i.e., my geographic position right now) and the spatial information that helps us visualize and analyze situations geographically.

Products and services that comply with OGC's open interface specifications enable users to freely exchange and apply spatial information, applications and services across networks, different platforms and products.

Keywords:

1.1.3.9 OAG

URL: <http://www.openapplications.org/>

The Open Applications Group is a non-profit consortium focusing on best practices and processes based on XML content for eBusiness and Application Integration. The primary focus of this group is integration related to Enterprise Resource Planning applications such as SAP®, Oracle®, and PeopleSoft®. The technical work of the Open Applications Group is divided into two types of projects, Content and Technical. The Content work is comprised of defining the business processes, their messages, and the data dictionary. The Technical work is comprised of XML design, development, UML repository work, and application architecture. The design of the Business Object Document (BOD) includes a noun, which corresponds to an object handle, and a verb, which corresponds to a method. This design enables a supplier to affect a virtual object wrapper around their system.

Keywords: Computational VP, Limited usage

1.1.3.10 MultiSpeak

URL: <http://www.multispeak.org>

MultiSpeak® is a specification for the exchange of data among software applications commonly applied in small electric utilities, such as electric cooperatives. Software providers may use the specification to write interfaces that will enable the interchange of information with other software that supports MultiSpeak. The MultiSpeak Initiative is a collaborative effort of the National Rural Electric Cooperative Association (NRECA) along with over 120 software providers and consultants that serve electric utilities. The Initiative was formed to foster the development of cost-effective, interoperable software products for electric utilities.

MultiSpeak makes use of the XML technologies to construct simple data models for exchange of utility information. A significant deployment of this technology has been implemented in some utilities.

Keywords: Multispeak, XML, NRECA, Enterprise VP, Computational VP

1.1.4 Customer Interface Data Management Technologies

1.1.4.1 IEC62056 - Data Exchange for Meter Reading, Tariff, and Load Control

URL: <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=886>

The purpose of IEC62056 is to establish standards, by reference to other ISO/OSI Standards, necessary for data exchanges by different communication media, for automatic meter reading, tariff and load control, and consumer information. The media can be distribution line carrier (DLC), telephone (including ISDN), radio, or other electrical or optical system. Any of these media may be used for local or remote data exchange.

- IEC 62056-61: Object identification system (OBIS)
- IEC 62056-62: Interface classes

Keywords: AMR, COSEM, DLMS, Xdlms, Meter, HDLC, OBIS, Computational VP

1.1.4.2 ANSI C12.19 (Meter Tables)

URL: <http://www.nertec.com>
http://strategis.ic.gc.ca/epic/internet/inmc-mc.nsf/vwGeneratedInterE/h_lm02133e.html

The ANSI C12 SC17 committee develops standards for the exchange of metering data over various communications networks. Due to co-development of these standards with Measurement Canada, this represents the sole SDO effort in North America developing standards for communications with revenue meters.

ANSI C12.19 provides the data model of the meter. Recent work by the C12.19 committee has produced a mapping of this data model to XML and XMLSchema (note: this is a preliminary draft work in progress: see contribution TF9906-029-9.doc, titled "Table and End-device Description Language Using XML. and Schemas", on the ANSI C 12 SC17 C12.19 web site)

Keywords: ANSI, XML, XML schema, C12,19, Meter tables

1.1.4.3 AEIC Guidelines

URL: [AEICGuidelinesforImplementationofANSIC12.19-1997"UtilityIndustryEndDeviceDataTables"](#)

ANSI C12.19 provides for the flexible description of a revenue meter. This document describes some implementation agreements that will allow utilities to acquire compliant and interoperable meters that follow that standard. In this document are various choices amongst the large options space of the C12.19 standard to reduce variability of the access to commonly used information without constraining the availability of manufacturer custom information.

Keywords: AEIC, ANSI C12,19, Meter, Implementation agreement, Enterprise VP

1.1.4.4 ASHRAE SSPC135 BACnet

URL: <http://www.bacnet.org/>

ANSI/ASHRAE® Standard 135-2001 (Including ANSI/ASHRAE Addenda 135a, 135b, 135c, 135d, and 135e), BACnet® Building Automation and Control Networks, BACnet

The standard for BACnet was first completed in 1995 and revised in 2001. It defines how devices within a building or campus can interact electronically to support collaborative building automation services for principally energy controls, security, and access. BACnet is being used as the standard communications protocol for the building automation system, BAS, device in the simulation.

Keywords: SSPC135, HVAC, Refrigeration, Heating, Air-conditioning, ASHRAE, In-building

1.1.4.5 GPC-20 XML Modeling for HVAC

URL:

“To establish a common data exchange format for the description of commodity data and HVAC&R information VIA the standard XML (extensible Markup Language) formatting language. Data types would include catalog definitions in areas such as, but not limited to, chillers, air-handling units, fans, pumps, fittings, controls, as well as analytical or operations, building performance data.”

Keywords: XML, ASHRAE, In-building

1.1.4.6 CEBus® based on EIA 600

URL: http://www.ce.org/standards/standards_listing.asp?id=prod_cat&id2=100&name=CEBus%20Products

CEBus® is a non-proprietary open protocol based upon an open standard (EIA 600), designed for use within buildings over their existing 120 v, 60 Hz power lines as well as infrared, coaxial, and rf physical layers. CEBus permits appliances and other devices to communicate with every other CEBus device over the in-house powerline without the need for new wires. Some CEBus devices can be installed without the need for a central controller, which enables CEBus devices to be used to provide solutions for many simple automation problems. Alternatively CEBus devices can be networked with a central controller for larger and more extensive automation projects.

CEBus products can be used for retrofitting an existing house or building using the existing powerlines because they do not require any additional wiring to be installed.

Note that CEBus, actively developed in the 1990's is presently not being aggressively pursued in marketplace with products and services.

Keywords: CEBus, CAL, Power line carrier, RF, IR, COAX, In-building, Association

1.1.4.7 UPnP

URL: <http://www.upnp.org/>

Universal Plug and Play (UPnP™) is a set of implementation agreements and specifications for the use of SOAP-based XML messages to achieve home automation actions.

“The Universal Plug and Play Forum is an industry initiative designed to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. As a group, we are leading the way to an interconnected lifestyle.”

Keywords: UPNP, Home automation, SOAP, XML, In-building, Forum

1.1.4.8 Controller Area Network (CAN)

URL: <http://www.can-cia.de/can/>

Controller Area Network (CAN) is a serial bus system especially suited to interconnect smart devices to build smart systems or sub-systems. The attributes of a Controller Area Network (CAN) are:

- the multi-master capabilities that allow building smart and redundant systems without the need of a valuable master,
- the broadcast messaging that is the first piece of the guarantee for 100% data integrity as any device within the network uses the very same information,

- the sophisticated error detecting mechanism and the retransmission of faulty messages which is the second piece of the guarantee for 100% data integrity,
- the availability of more than 50 controllers from low-cost devices to high-end chips from more than 15 manufacturers,
- and the availability of CAN for the next 15 years as its use within the European automotive industry and the decision for CAN from the US and Japan automotive industry is guaranteed.”

CAN is a ubiquitous protocol devised for monitoring and control in automotive applications. However, due to its small footprint and other technical attributes, it has found applications in many areas requiring interaction between sensors and controls. Virtually every manufacturer of embedded micro controller provides devices with built-in CAN interfaces. In this regard it is probably only second in commonality to a UARTs and I2C as a means of device communications.

DeviceNet™ is a related and similar protocol that differs in higher layers from CAN.

CAN was standardized as ISO 11898.

In the year 1992, some companies founded the non-profit trade-association CiA in order to provide technical, product and marketing information with the aim of fostering CAN's image and providing a path for future developments of the CAN protocol. 411 companies (December 2002) have joined the non-profit organization, which develops and supports various CAN-based higher-layer protocols

Keywords: DeviceNet, CAN, Controller Area Network In-building, Automotive, Association

1.1.5 Customer Automated Meter Reading (AMR) Technologies

1.1.5.1 1390.2-1999 IEEE Automatic Meter Reading via Telephone - Network to Telemetry Interface Unit

URL: <http://standards.ieee.org>

Define a standard for the communications interface between the telephone network and the device at the customer premise. The device at the customer premise is identified as a Telemetry Interface Unit (TIU) and may provide an interface between the network and devices at the customer premise such as utility meters, alarm devices, control switches and other devices to be determined.

Keywords: Telephone network, Utility controller, AMR

1.1.5.2 1390.3-1999 IEEE Standard for Automatic Meter Reading via Telephone - Network to Utility Controller

URL: <http://standards.ieee.org>

This document will provide a standardized device interface to promote a multi-vendor environment.

Keywords: Telephone network, Utility controller, AMR, Computational VP

1.1.5.3 ANSI C12.18 (PSEM, Optical port)

URL: <http://>

ANSI C12.18 provides a description of basic transport of C12.19 data over a point-to-point optical link.

Keywords: Metering, meters, Optical port; psem

1.1.5.4 ANSI C12.21 (POTS)

URL: <http://>

ANSI C12.21 provides for the transport of C12.19 data over plain old telephone system, POTS. The standard describes the means of interaction with typical dial-up modems.

Keywords: Metering, meters, Plain old telephone service, Telephone system, Remote data access

1.1.5.5 ANSI C12.22 (EPSEM)

URL: <http://>

ANSI C12.22 provides for the transport of C12.19 data over “any network”. Included in this standard, currently in development, is a standard means of encryption and authentication of metering data using a slightly modified version of STASE-ROSE.

This committee has tackled some of the key requirements of dealing with large volume deployments of revenue critical devices over heterogeneous networks. Some of these requirements are:

- Incorporation of authentication and encryption features in huge quantity, low-cost devices
- Self describing data model of complex meter data
- XMLSchema, XML based translation of meter Description and meter data
- Traceable, scaleable, and globally unique identifiers for corporate entities, communications, and devices.
- Routing of messages over heterogeneous networks (with different addressing schemes and owners) without carrying routing information in every packet.
- Audit trail verification of configuration changes in end devices with economic consequences

Keywords: Metering, meters, AMR meter network optical-port, PSEM, EPSEM, “Meter Tables” STASE-ROSE, Objectid, Information Model

1.1.5.6 Broadband over Power Line (BPL)

URL: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci953137,00.html

Broadband over Power Line (BPL) is a technology that allows Internet data to be transmitted over utility power lines. (BPL is also sometimes called Power-line Communications or PLC.) In order to make use of BPL, subscribers use neither a phone, cable, nor satellite connection. Instead, a subscriber installs a modem that plugs into an ordinary wall outlet and pays a subscription fee similar to those paid for other types of Internet service.

BPL works by modulating high-frequency radio waves with the digital signals from the Internet. These radio waves are fed into the utility grid at specific points. They travel along the wires and pass through the utility transformers to subscribers' homes and businesses. Little, if any, modification is necessary to the utility grid to allow transmission of BPL. This mode has not yet been widely deployed in the United States, but it has been implemented in a few other countries, with varying results. The Federal Communications Commission (FCC) is currently working on a set of rules according to which BPL may be implemented in the United States. If it is put into use, BPL will be an unlicensed service, and will be governed by rules similar to those that apply to cordless telephones, television remote controls, and other consumer electronic devices.

Some people say BPL represents an ideal solution for people in rural areas. But many engineers, along with officials in the National Telecommunications and Information Administration (NTIA) and the Federal Emergency Management Administration (FEMA), fear that BPL will interfere with fire, police, shortwave, land mobile, and other radio systems important to national security.

Amateur radio operators have voiced their concerns as well. BPL subscribers may also be adversely affected by the electromagnetic fields that radio transmitters generate in the course of their normal and licensed operations. The utility power lines are not shielded, as is coaxial cable, and some of the frequencies suggested for BPL operation lie within the spectra assigned to essential wireless services.

1.1.6 Customer Site In-Building Technologies

1.1.6.1 Home PNA

URL: <http://www.homepna.org/>

The Home Phone Network Alliance - HomePNA has created specifications and devices to allow high-speed, reliable networking (LAN) technology that uses the existing phone wires in a home to share a single Internet connection with several PCs as well as voice and video. Version 3.0 of their specification has just been released that allow for operating speeds from 128 to 240 Mbps operation. HomePNA also allows for "deterministic" traffic by allocating time slots in the message for certain messages.

Keywords: HomePNA, Home automation, Phoneline networking, In-building, Association

1.1.6.2 HomePlug

URL: http://www.homeplug.org/index_basic.html

"The HomePlug Powerline Alliance is a not-for-profit corporation established to provide a forum for the creation of open specifications for high-speed home power line networking products and services. The alliance is open to all companies that sign the adopter/participant agreement and make a small dues payment."

Keywords: PLC, Power line carrier, Home automation, In-building, Association

1.1.6.3 Zigbee Spec

URL: http://www.zigbee.org/zigbee_new/index.asp

"The ZigBee™ Alliance is an association of companies working together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard."

Zigbee is an emerging standard being introduced as IEEE 802.15.4. It has the following design requirements:

- Data rates of 250 kb/s, 40 kb/s and 20 kb/s.
- Star or Peer-to-Peer operation.
- Support for low latency devices.
- CSMA-CA channel access.
- Dynamic device addressing.
- Fully handshaked protocol for transfer reliability.
- Low power consumption.
- Frequency Bands of Operation
- 16 channels in the 2.4GHz ISM band
- 10 channels in the 915MHz ISM band
- 1 channel in the European 868MHz band.

Keywords: Zigbee, RF, Monitoring, Control, IEEE, IEEE 802, Pending standard

1.2 Communications Industry Technologies

1.2.1 Access Technologies

1.2.1.1 Public Internet

URL: http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212370,00.html

The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers). It was conceived by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1969 and was first known as the ARPANET. The original aim was to create a network that would allow users of a research computer at one university to be able to "talk to" research computers at other universities. A side benefit of ARPANet's design was that, because messages could be routed or rerouted in more than one direction, the network could continue to function even if parts of it were destroyed in the event of a military attack or other disaster.

Today, the Internet is a public, cooperative, and self-sustaining facility accessible to hundreds of millions of people worldwide. Physically, the Internet uses a portion of the total resources of the currently existing public telecommunication networks. Technically, what distinguishes the Internet is its use of a set of protocols called TCP/IP (for Transmission Control Protocol/Internet Protocol). Two recent adaptations of Internet technology, the intranet and the extranet, also make use of the TCP/IP protocol.

Keywords: Internet, TCP/IP

1.2.1.2 Private Intranet

URL: <http://www.strom.com/pubwork/intranetp.html>
<http://www.intrack.com/intranet/wpapers1.cfm>

Most corporations have implemented corporate networks that utilize the same technologies as the public Internet. These private networks are often called Intranets to distinguish them from the Internet.

Keywords: Internet, Intranet

1.2.1.3 Data over Voice Lines

URL: <http://www2.rad.com/networks/1994/modems/modem.htm>
<http://www.techtutorials.info/hdmodems.html>
http://www.rad.com/RADCnt/MediaServer/3656_ldv-2.pdf
http://www.vocal.com/data_sheets/v925.html

Voice-grade telephone connections (standard 3 kHz voice circuits) are made either by dialing by the user or by being wired in the telephone company's central office and remain connected until the service is discontinued. The latter kind is called a private line, leased line or dedicated line. The user usually pays a fixed fee every month for this service. The leased line is a point-to-point circuit, with both end points identified to the telephone company. The user has no knowledge of

where or how the circuit is routed between the two end-points, unless the telephone company is specifically requested to provide diversity for security and availability purposes.

Point-to-point circuits are cost effective for high-speed communication between two devices, but are more expensive when compared to dial-up applications where the circuit is connected and charged only for the duration of the connection. Low speed point-to-point voice-grade circuits are known in the industry as 3002 circuits. Voice-grade circuits can carry uncompressed data from the slowest speed up to 19.2 kbps. Higher speeds (up to 56 kbps) can be carried with data compression.

Digital circuits or Digital Data Services (DDS) can carry data at 2.4, 4.8, 9.6, 19.2, 56, and 64Kbps. Digital circuits are not technically voice-grade, but they can be used to carry either voice or data. Slow speed leased lines have been used extensively by utilities to provide quick connections to various facilities and devices that cannot otherwise be reached in a structured network or telecommunications scheme.

Main Features of Technology

Technology	3 kHz bandwidth telephone voice circuit
Operation	Low speed, limited by bandwidth and circuit quality
Capacity	Usually dedicated to one modem per line for most applications, but multi-drop connections to multiple RTUs are common
Coverage	As far as phone company phones lines can reach
Data rate	Up to 64kbps with special line conditioning
Power	Terminal equipment to provide
Regulatory	None required

Key Advantages

Coverage	Telephone company circuits reach most locations within the United States and can be installed rapidly
Maintenance	Telephone company provides all maintenance
Interference	Phone company usually guarantees the performance of the line
Availability	Phone company usually guarantees the availability of the line along with time to repair
Security	Each line is dedicated and not shared with others, but eavesdropping is relatively easy
Cost	Phone company is responsible for the line, so no installation and maintenance costs

Key Disadvantages

Reliability/availability	User has no control over line reliability and availability. Situation has worsened since de-regulation because a single line may have multiple carriers, which makes it difficult to trouble-shoot problems and hold one carrier responsible
Data rate	Low data rates
Cost	Recurring charges, high installation cost if remote site does not have nearby phone facility

Keywords: Physical layer

1.2.1.4 Digital Subscriber Line (DSL) Technologies

URL: <http://www.dslforum.org/>
<http://www.t1.org/t1e1/t1e1.htm>

ADSL was first standardized in 1995 by the American National Standards Institute as T1.413, and then by the ITU in 1999 as G.992.1. ADSL can transmit data at speeds up to 8 megabits per second ("Mbps") downstream and up to 640 Kbps upstream. In 1999, the ITU also standardized a

lower speed version of ADSL, known as G.Lite or G.992.2. G.Lite can transmit data at speeds up to 1.5 Mbps downstream and up to 512 Kbps upstream without using special filtering equipment required by full-rate ADSL.

In 2002, the ITU standardized a new family of ADSL standards known as ADSL2 or G.992.3 and G.992.4. These standards provide numerous improvements over previous ADSL standards, including line diagnostics, power management, power cutback, reduced framing, and on-line reconfiguration. In January 2003, the ITU standardized an extension of ADSL2 known as ADSL2+ or G.992.5. ADSL2+ builds upon the ADSL2 standard by increasing achievable data rates to speeds of up to 25 Mbps upstream on phone lines as long as 3,000 feet (20 Mbps out to 5,000 feet). Reach-Extended ADSL2 (RE-ADSL2) - the new ADSL2 Annex L standard - was ratified by the ITU in October 2003. Annex L proposes new power spectral density (PSD) masks that can result in a significant increase in ADSL's reach.

The DSL Forum is a consortium of networking, computing, and service provider companies that promote the development and worldwide acceptance of the Digital Subscriber Line family of technologies.

Committee T1 is sponsored by the Alliance for Telecommunications Industry Solutions (ATIS) and accredited by the American National Standards Institute (ANSI) to create network interconnections and interoperability standards for the United States. Within T1, T1E1 is concerned with Interfaces, Power, and Protection of networks. The T1E1.4 working group (DSL Transmission) addresses high-speed bi-directional digital transport via metallic facilities. The work of this group focuses on the physical layer transceiver functionality.

1.2.1.4.1 Asymmetric Digital Subscriber Line (ADSL) and Digital Subscriber Line (DSL)

URL: <http://www.dslforum.org/>

Asymmetric Digital Subscriber Line (ADSL) is the formal name for what is being commonly called Digital Subscriber Line (DSL). ADSL/DSL is the most commonly available DSL modem technology, and is currently being implemented to connect residential customers to the Internet. ADSL converts existing twisted-pair telephone lines into access paths for Plain Old Telephone System (POTS) voice telephone circuits plus simultaneous high speed data communications. ADSL transmit two separate data streams with much more bandwidth devoted to the downstream than upstream leg. ADSL has a range of downstream speeds depending on distance. For up to 9000, 12000, 16000, 18000 feet, the speed is 8.448, 6.312(DS2), 2.048(E1), and 1.544 (T1) Mbps respectively. The upstream speeds range from 16 kbps to 640 kbps.

ADSL modems provide data rates consistent with North American T-1 line 1.544 Mbps and European E1 2.048 Mbps digital hierarchies and can be purchased with various speed ranges and capabilities. The minimum configuration provides 1.5 or 2.0 Mbps downstream and a 16 kbps duplex channel; higher speed configurations provide rates of 6.1 Mbps and 64 kbps duplex. Products with downstream rates up to 8 Mbps and duplex rates up to 640 kbps are available today. ADSL modems accommodate Asynchronous Transfer Mode (ATM) transport with variable rates and compensation for ATM overhead, as well as IP protocols. The modulation technique used is Quadrature Amplitude Modulation (QAM). ADSL is officially ITU-T standard G-992.1.

Keywords: Modem, serial, high speed, physical layer, Access Technology, Asynchronous

1.2.1.4.2 High Data-Rate Digital Subscriber Line (HDSL)

URL: <http://www.dslforum.org/>

High Data-Rate Digital Subscriber Line (HDSL) is a bidirectional and symmetrical transmission system that allows the transport of signals with a bit rate of 1.544 Mbps or 2.048 Mbps on the copper twisted pairs of an access network.

The HDSL system uses echo cancellation technique for the separation of the directions of transmission, so that one twisted pair can carry both directions. Two different options for the line code are recommended, the Pulse Amplitude Modulation 2B1Q and the Carrierless Amplitude/Phase Modulation (CAP). CAP is applicable for 2.048 Mbps only, while for 2B1Q two different frames for 1.544 Mbps and 2.048 Mbps are defined. The 2B1Q for 2.048 Mbps caters for both duplex transmission on a single pair and parallel transmission on two or three-pairs. This allows for the distribution of the signal to several pairs and for reduction of the symbol rate and an increase of the line length. CAP is defined for one- or two-pairs only and the 1.544 Mbps 2B1Q for two-pairs only. HDSL is an ITU-T recommendation G.991.1

Keywords: Modem, serial, high speed, physical layer, Access Technology

1.2.1.4.3 Single-Line Digital Subscriber Line (SDSL)

URL: <http://www.dslforum.org/>

Single-Line Digital Subscriber Line (SDSL) is single-line version of HDSL, transmitting T1/E1 signals over a single twisted pair, so that a single line can support telephone line and T1/E1 at the same time. It fits the market for residence connection, which must often work over a single telephone line. However, SDSL will not reach much beyond 10,000 feet. At the same distance, ADSL reaches rates above 6 Mbps.

Keywords: Modem, serial, high speed, physical layer, Access Technology

1.2.1.4.4 Very high data rate Digital Subscriber Line (VDSL)

URL: <http://www.dslforum.org/>

VDSL, also called VASDL or BDSL, has data rates higher than ADSL but over shorter lines. The downstream speeds are expected to be at 12.96 (1/4 STS1), 25.82 (1/2 STS-1) and 51.84 (STS-1) Mbps for 4500, 3000 and 1000 feet of wire respectively. Upstream rates fall within a suggested range from 1.6 Mbps to 2.3 Mbps.

Keywords: Modem, serial, high speed, physical layer, Access Technology

1.2.1.4.5 Wireless Digital Subscriber Line (WDSL)

URL: <http://www.dslforum.org/>

Wireless Digital Subscriber Line (WDSL) leaps past the last mile stranglehold from the local telephone company with leading edge wireless technology. WDSL high speed Internet service is delivered to users via radio spectrum - utilizing fixed wireless technologies such as MMDS or 802.11. Hence, unlike other forms of DSL, WDSL is a shared medium. Downstream speeds typically start at 384kbps-1.5M and upstream at 128kbps.

Keywords: Modem, serial, high speed, physical layer, Access Technology, wireless

1.2.1.4.6 Rate-Adaptive DSL (RADSL)

URL: <http://www.dslforum.org/>

Rate-Adaptive DSL (RADSL) is an ADSL technology from Westell in which software is able to determine the rate at which signals can be transmitted on a given customer phone line and adjust the delivery rate accordingly. Westell's FlexCap2 system uses RADSL to deliver from 640 Kbps to 2.2 Mbps downstream and from 272 Kbps to 1.088 Mbps upstream over an existing line.

Keywords: Modem, serial, high speed, physical layer, Access Technology, adaptive

1.2.1.4.7 G.Lite/DSL Lite/Universal ADSL

URL: <http://www.dslforum.org/>

Most DSL technologies require that a signal splitter be installed at a home or business, requiring the expense of a phone company visit and installation. However, it is possible to manage the splitting remotely from the central office. This is known as splitterless DSL, "DSL Lite," G.Lite (by PTTs and Compaq®, Intel®, and Microsoft®), or Universal ADSL and has recently been made an ITU-T standard; G.992.2. G.Lite used DMT modulation.

Keywords: Modem, serial, high speed, physical layer, Access Technology, asynchronous, splitterless

1.2.1.5 Cable Modems - DOCSIS

URL: <http://www.cablemodem.com/>

Cable Modem Standards and Specifications

J-series - Transmission of television, sound program and other multimedia signals

Cable-Modem.net -- The Basics of Broadband

The CableLabs Cable Modem project, also known as DOCSIS (Data Over Cable Service Interface Specification), defines interface requirements for cable modems involved in high-speed data distribution over cable television system networks. The CableHome project is developing the interface specifications to extend cable-based services to network devices within the home. The project will address issues such as device interoperability, Quality of Service, and network management.

Cable modems can operate at higher speeds than regular modems because they are connected via coaxial cable instead of a phone line. Coax has much higher bandwidth than telephone cable, which is limited to 3 kHz. In North America Cable modems adhere to the Data Over Cable Service Interface Specification (DOCSIS) standard, also released as ITU-T J.112. In Europe, both J.112 and a competing standard called EuroModem are used.

Keywords: Cable, Modem, high speed, physical layer, Access Technology, CATV, Home networking

1.2.1.6 Fiber in the Loop (FITL)

URL: <http://www.mynetwatchman.com/kb/IFITL/ifitlintro.htm>
<http://www.martin-group.com/solutions/engineering/FITL.asp>
<http://www.telcordia.com/services/testing/integrated-access/gr/fitl/>
<http://glossary.westnetinc.com/?ID=%09%092233>

There are many architectures for deploying "fiber in the loop", where "loop" refers to the "subscriber loop", the last length of cable between a network provider and a subscriber. FITL architectures vary from deploying fiber feeder plant (between central office and remote terminal site); fiber-to-the-curb (FITC); and, ultimately fiber-to-the-home (FITH) where the optical network unit (ONU) is located at each home. Hybrid Fiber Coax (HFC) architectures have emerged to reduce implementation costs.

Keywords: physical layer, high speed, Fiber to the home, Fiber to the curb, Access.

1.2.1.7 Hybrid Fiber Coax (HFC)

URL: http://www.iec.org/online/tutorials/hfc_tele/

HFC architecture uses fiber to carry voice, video and data from the headend or central office to the optical node serving a neighborhood. At the optical node, downstream optical signal is converted to an electrical signal and carried via coax to drops at customer locations where a service unit separates video, data and telephony signals for direct connection to customer

devices (televisions, computers, telephones, etc.). A single optical node will typically support a number of coaxial distribution feeds. Noise on the uplink direction within an HFC network is an issue. HFC networks mainly provide asymmetrical services - i.e. broadcast services from the cable operator to the subscriber - with a limited return path. Due to the popularity of bi-directional services such as Video-on-Demand, high-speed Internet and Voice over IP, cable operators have begun plant upgrades that provide these services. Many CATV networks use HFC.

Main Features of Technology

Technology	A combination of fiber cable and coaxial cable for distributing signal
Bandwidth	Broadband
Operation	A local CATV company usually provides fiber cable, say, to the curbside (FTTC) of a residence. The fiber then connects with a coaxial cable inside the residence. This is how cable TV is delivered to the home from the CATV headend. The same concept applies to delivering data to a commercial or industrial customer's facility if it already has CATV connection. At the CATV headend, current technology calls for using a cable modem to feed data traffic into the PSTN network or other public network
Capacity	Depends upon the design of the system; fiber capacity is limited by end equipment; coaxial by need to support both TV and data downloads
Coverage	Same as cable TV
Data rate	The theoretical size of the cable link is very large-a total of some 735 MHz usable bandwidth. HFC divides the total bandwidth into a downstream (to the home) band and an upstream (to the hub) band. The downstream band typically occupies 50-750 MHz, while the upstream band typically occupies from 5-40 MHz
No. of channels	Slow speed devices can be groomed into higher speed channels by using CATV multiplex equipment at the fiber node
Multiplexing	Data can be multiplexed with video via the CATV network
Power	CATV provides the necessary powering of the local equipment
Regulatory	No licensing required

Key Advantages

Coverage	Takes advantage of existing cable TV network and eliminates the need for any new infrastructure
Interference	None
Security	Very difficult to be tapped into by others
Reliability	Very high because it is a cabled system. Question is how well will the provider support the network
Cost	Radio frequency components required for cable modem operation are inexpensive

Key Disadvantages

Data rate	The medium is designed primarily for downstream communication (TV)
Upstream channel	5-50MHz bandwidth and is usually noisy, needs filtering and cannot support higher speed data Service providers do not make upstream channel robust due to lack of use Will be shared in the future and may become overloaded due to heavy traffic
Cost	If remote device is not located near a TV connection point, may need extensive premise re-wiring

Keywords: physical layer, high speed, Fiber optic, Coax, Access, CATV

1.2.2 Networking Technologies

1.2.2.1 Internet Protocol Version V4 (IPV4)

URL: <http://www.ietf.org/rfc/rfc791.txt>

IPV4 is the current version of the Internet Protocol (IP), which is the Internet's most basic protocol and is responsible for carrying data from a source to a destination. It is a Network layer protocol in the TCP/IP protocol suite.

IP is a connectionless, datagram protocol that provides two basic functions: addressing and fragmentation. Connectionless means that the internet protocol treats each internet datagram as an independent entity unrelated to any other internet datagram. There are no connections or logical circuits (virtual or otherwise). IP can segment a message into smaller packets, which are sent across the Internet (or other network) to the destination, where the IP layer there reassembles the message. The fragmentation of the datagram packet by IP is known as IP fragmentation. Whenever the IP layer receives a datagram packet to send, it first finds the local interface on which the datagram is to be sent on (routing). Then IP sends a query to that interface to obtain its maximum transmission unit (MTU). If the size of the datagram packet to be transmitted is greater than the MTU of the interface, IP performs fragmentation on the packet. Fragmentation can take place anywhere; i.e., it can be done at the host or at any intermediate router. Techniques to discover the path MTU can be found in RFC 1191 and RFC 1981. IPv4's current addressing consists of a 32-bits address field. IPv4 is documented in **RFC 791**, and IP broadcasting procedures are discussed in **RFC 919**.

The Internet Protocol defines (1) the address scheme and convention, (2) the packet format as well as the (3) control and management functions to be supported by the compatible devices including gateways, routers, and end-hosts.

Keywords: Internet, network layer, addressing.

1.2.2.2 Internet Protocol Version 6 (IPV6)

URL: <http://www.ietf.org/rfc/rfc2460.txt>

IP version 6 (IPv6) [RFC 2460], developed by the Internet Area of IETF, is a new version of the Internet Protocol, designed as a successor to IP version 4 (IPv4) [RFC-791]. The primary changes are (i) extension of the IP address from 32 bytes (IPv4) to 128 bytes (IPv6) to enable more addressable nodes, (ii) flow labeling, (iii) header simplification, and (iv) more support for extensions and options. Support of security services such as message authentication and encryption is also required for any implementation of IPv6.

Advantages/Strengths: IPv6 has increased address space and other advantages over IPv4.

Disadvantages/Weaknesses: Because of the enormous investment in IPv4, and the limited additional benefits of IPv6, IPv6 has not yet been implemented widely, and not much progress has been made in convincing vendors of the need to convert from V4 to V6.

Keywords: Internet, network layer, addressing.

1.2.2.3 Routing Protocols

1.2.2.3.1 Unicast Routing

URL: <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnras/html/unicastrouting.asp>
<http://www.cs.bu.edu/techreports/pdf/2002-018-routing-tradeoffs.pdf>

Unicast is communication between a single sender and a single receiver over a network. The term exists in contradistinction to multicast, communication between a single sender and multiple receivers, and anycast, communication between any sender and the nearest of a group of receivers in a network. An earlier term, *point-to-point* communication, is similar in meaning to unicast. The new Internet Protocol version 6 (IPv6) supports unicast as well as anycast and multicast.

Keywords: Internet, Routing, Interior Gateway Protocol, intra-domain

1.2.2.3.2 Multicast Routing

URL: <http://ntrg.cs.tcd.ie/undergrad/4ba2/multicast/antony/>
<http://www.cisco.com/warp/public/614/17.html>

Multicast is communication between a single sender and multiple receivers on a network. Typical uses include the updating of mobile personnel from a home office and the periodic issuance of online newsletters. Together with anycast and unicast, multicast is one of the packet types in the Internet Protocol Version 6 (IPv6).

An mrouter, or multicast router, is a router program that distinguishes between multicast and unicast packets and determines how they should be distributed along the Multicast Internet (sometimes known as the Multicast Backbone or MBone). Using an appropriate algorithm, an mrouter tells a switching device what to do with the multicast packet.

Mrouters currently make up "islands" on the MBone separated by unicast routers. Thus, an mrouter can disguise multicast packets so that they can cross unicast routers. This is done by making each multicast packet look like a unicast packet; the destination address is the next mrouter. This process is called IP tunneling.

There are two multicast routing protocols that mrouters use to distribute multicast packets. They are dense-mode routing and sparse-mode routing. The protocol used is determined by available bandwidth and the distribution of end users over the network. If the network has many end users and there is enough bandwidth, dense-mode routing is used. However, if bandwidth is limited and users are thinly distributed, sparse-mode routing is used.

Keywords: Internet, Routing, Interior Gateway Protocol, intra-domain

1.2.2.3.3 Open Shortest Path First (OSPF) Routing Protocol

URL: <http://www.ietf.org/rfc/rfc2328.txt>
<http://www.ietf.org/internet-drafts/draft-katz-yeung-ospf-traffic-09.txt>

Open Shortest Path First (OSPF) [RFC 2328] is a link-state routing protocol designed to be run internally to a single Autonomous System. Each OSPF router maintains an identical database describing the Autonomous System's topology. From this database, a routing table is calculated by constructing a shortest-path tree. OSPF extensions for IPv6 [RFC 2740], and traffic engineering are areas that need to be also considered.

Keywords: Internet, Routing, Interior Gateway Protocol, intra-domain

1.2.2.3.4 Intermediate System to Intermediate System (ISIS) Routing Protocol

URL: <http://www.iso.org> ; <http://www.iech.ch>
<http://www.ietf.org/rfc/rfc1195.txt>

OSI Intermediate System (IS) to Intermediate System routing is a protocol used to exchange information between Level 1 (intra-domain) routing devices in an OSI network. The OSI Intra-Domain IS-IS Routing Protocol may be used as an interior gateway protocol (IGP) to support TCP/IP as well as OSI. This allows a single routing protocol to be used to support pure IP environments, pure OSI environments, and dual environments. A specification has been developed by the IS-IS working group of the Internet Engineering Task Force. The OSI IS-IS protocol has reached a mature state, and is ready for implementation and operational use. The most recent version of the OSI IS-IS protocol is contained in ISO DP 10589 [1]. The proposed standard for using IS-IS for support of TCP/IP will therefore make use of this version (with a minor bug correction, as discussed in Annex B). We expect that future versions of this proposed standard will upgrade to the final International Standard version of IS-IS when available.

Keywords: Internet, Routing, Interior Gateway Protocol, intra-domain

1.2.2.3.5 Routing Information Protocol (RIP)

URL: <http://www.ietf.org/rfc/rfc2453.txt>

Routing Information Protocol (RIP) is used to exchange routing information among routers (gateways) and other hosts in the Internet. With the advent of OSPF and IS-IS, there are those who believe that RIP is obsolete. While it is true that the newer IGP routing protocols are far superior to RIP, RIP does have some advantages. Primarily, in a small network, RIP has very little overhead in terms of bandwidth used and configuration and management time. RIP is also very easy to implement, especially in relation to the newer IGPs. Additionally, there are many, many more RIP implementations in the field than OSPF and IS-IS combined. It is likely to remain that way for some years yet.

With the advent of OSPF and IS-IS, there are those who believe that RIP is obsolete. While it is true that the newer IGP routing protocols are far superior to RIP, RIP does have some advantages. Primarily, in a small network, RIP has very little overhead in terms of bandwidth used and configuration and management time. RIP is also very easy to implement, especially in relation to the newer IGPs. Additionally, there are many, many more RIP implementations in the field than OSPF and IS-IS combined. It is likely to remain that way for some years yet.

Keywords: Internet, Routing, Interior Gateway Protocol, intra-domain

1.2.2.3.6 Border Gateway Protocol (BGP)

URL: <http://www.ietf.org/rfc/rfc1771.txt>

Border Gateway Protocol 4 (BGP-4) [RFC 1771] from IETF Inter-Domain Routing working group is an inter-Autonomous System routing protocol exchanging network reachability information with other BGP systems. This information is used to construct a graph of AS connectivity from which routing loops may be pruned and some policy decisions at the AS level may be enforced. It is similar to IDRP ["Information Processing Systems - Telecommunications and Information Exchange between Systems - Protocol for Exchange of Inter-domain Routing Information among Intermediate Systems to Support Forwarding of ISO 847 PDUs", ISO/IEC IS10747, 1993].

Keywords: Internet, Routing, Inter-domain, External Gateway Protocol

1.2.2.3.7 Host extensions for IP multicasting

URL: <http://www.ietf.org/rfc/rfc1112.txt>

This standard specifies the extensions required of a host IP implementation to support IP multicasting, where a "host" is any Internet host or gateway other than those acting as multicast routers.

Keywords: Internet, multicast, host configuration

1.2.2.3.8 Internet Group Management Protocol (IGMP)

URL: <http://www.ietf.org/rfc/rfc3376.txt>

The Internet Group Management Protocol (IGMP) is used by IPv4 systems (hosts and routers) to report their IP multicast group memberships to any neighboring multicast routers. Note that an IP multicast router may itself be a member of one or more multicast groups, in which case it performs both the "multicast router part" of the protocol (to collect the membership information needed by its multicast routing protocol) and the "group member part" of the protocol (to inform itself and other, neighboring multicast routers of its memberships). IGMP is also used for other IP multicast management functions, using message types other than those used for group membership reporting.

Keywords: Internet, multicast, group management.

1.2.2.3.9 Distance Vector Multicast Routing Protocol (DVMRP)

URL: <http://www.ietf.org/rfc/rfc1075.txt>

DVMRP is a distance-vector-style routing protocol for routing multicast datagrams through an internet. It is derived from the Routing Information Protocol (RIP), and implements multicasting as described in RFC-1054. DVMRP is an interior gateway protocol; suitable for use within an autonomous system, but not between different autonomous systems. DVMRP is not currently developed for use in routing non multicast datagrams, so a router that routes both multicast and unicast datagrams must run two separate routing processes.

Keywords: Internet, routing, multicast, Intra-domain, Interior Gateway Protocol

1.2.2.3.10 Multicast Open Shortest Path (MOSPF) routing protocol

URL: <http://www.ietf.org/rfc/rfc1584.txt>

MOSPF provides enhancements to the OSPF protocol to enable the routing of IP multicast datagrams. With MOSPF, an IP multicast packet is routed based both on the packet's source and its multicast destination (commonly referred to as source/destination routing). The multicast extensions are built on top of OSPF Version 2. The extensions have been implemented so that a multicast routing capability can be introduced piecemeal into an OSPF Version 2 routing domain. Some of the OSPF Version 2 routers may run the multicast extensions, while others may continue to be restricted to the forwarding of regular IP traffic (unicasts).

Keywords: Internet, routing, multicast, Intra-domain, Interior Gateway Protocol

1.2.2.3.11 Protocol Independent Multicast-Sparse Mode (PIM-SM)

URL: <http://www.ietf.org/rfc/rfc2362.txt>

PIM-SM is a protocol for efficiently routing to multicast groups that may span wide-area (and inter-domain) internets. It is named Protocol Independent Multicast--Sparse Mode (PIM-SM) because it is not dependent on any particular unicast routing protocol, and because it is designed to support sparse multicast groups within the network.

Keywords: Internet, routing, multicast.

1.2.2.3.12 Core-Based Tree (CBT) multicast routing

URL: <http://www.ietf.org/rfc/rfc2189.txt>

<http://www.ietf.org/rfc/rfc2201.txt>

The Core-Based Tree (CBT) protocol is a network layer multicast routing protocol that builds and maintains a shared delivery tree for a multicast group. The sending and receiving of multicast data by hosts on a subnetwork conforms to the traditional IP multicast service model. CBT is suited to inter- and intra-domain multicast routing in the Internet. CBT may use a separate multicast routing table, or it may use that of an underlying unicast routing, to establish paths between senders and receivers.

Keywords: Internet, routing, multicast.

1.2.3 IP-based Transport Protocols

1.2.3.1 Transmission Control Protocol (TCP)

URL: <http://www.ietf.org/rfc/rfc793.txt>

Transmission Control Protocol (TCP) [RFC 793] is a connection-oriented, reliable transport protocol and part of the TCP/IP protocol suite. It provides the reliability not provided by IP, by adding various timeouts, sequence checking, and checksum features. However, it does not provide recovery services after an error. This is partly because it was originally designed to provide communication services between humans and computers, so that humans could always perform the recovery effort (e.g. just hit the Reload button on your browser).

TCP performs multiplexing, demultiplexing, and error detection (but not recovery). It operates at the Transport Layer in the OSI model and is defined in a number of the below listed RFCs, a host-to-host protocol, provides reliable, connection-oriented data transmission. TCP's congestion control mechanism reacts to network congestion by reducing its transmission window. Various enhancement work on TCP is discussed in the Transport Area working group of the IETF.

Keywords: Internet, Reliable, Transport, Protocol

1.2.3.2 User Datagram Protocol (UDP)

URL: <http://www.ietf.org/rfc/rfc793.txt>

User Data Protocol (UDP) [RFC 768] is a no-frills, bare-bones connectionless transport protocol that enables an application to send individual messages to other applications. Delivery is not guaranteed, and messages may not be delivered in the same order as they were sent. It is preferable to TCP for delay-sensitive, real-time applications.

UDP is part of the TCP/IP protocol suite. UDP is connectionless because it sends data without ever establishing a connection and it provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It is used primarily for broadcasting messages over a network. Applications using UDP includes; e.g., DNS, SNMP, TFTP, RIP, DHCP, BOOTP.

Keywords: Internet, datagram, Transport, Protocol

1.2.3.3 Stream Control Transmission Protocol (SCTP)

URL: <http://www.ietf.org/rfc/rfc2960.txt>

Stream Control Transmission Protocol is designed to transport PSTN signaling messages over IP networks, but is capable of broader applications. SCTP is a reliable transport protocol operating on top of a connectionless packet network such as IP. It offers the following services to its users: (1) acknowledged error-free non-duplicated transfer of user data, (2) data fragmentation to conform to discovered path MTU size, (3) sequenced delivery of user messages within multiple streams, (4) with an option for order-of-arrival delivery of individual user messages, (5) optional bundling of multiple user messages into a single SCTP packet, and most importantly (6) support network-level fault tolerance through supporting of multi-homing at either or both ends of an association. The design of SCTP includes appropriate congestion avoidance behavior and resistance to flooding and masquerade attacks.

Keywords: Internet, datagram, Transport, Protocol

1.2.3.4 Datagram Congestion Control Protocol (DCCP)

URL: <http://www.ietf.org/internet-drafts/draft-ietf-dccp-spec-06.txt>

The Datagram Congestion Control Protocol (DCCP) implements a congestion-controlled, unreliable flow of unicast datagrams suitable for use by applications such as streaming media, Internet telephony, and on-line games.

Keywords: Internet, datagram, Transport, Protocol

1.2.3.5 Real-Time Transport Protocol (RTP)

URL: <http://www.ietf.org/rfc/rfc1889.txt>

Real-time Transport Protocol (RTP) [RFC 1889], provides end-to-end network transport functions for real-time applications, such as audio, video or simulation data, over multicast or unicast network services. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services. The data transport is augmented by a control protocol (RTCP) to allow monitoring of the data delivery and to provide minimal control and identification functionality. RTP and RTCP are independent of the underlying transport and network layers.

Keywords: Internet, Real-time, Transport, Protocol, video, audio, multicast

1.2.4 Application Layer Protocols

1.2.4.1 Hypertext Transfer Protocol (HTTP)

URL: <http://www.ietf.org/rfc/rfc1945.txt>
<http://www.ietf.org/rfc/rfc1945.txt>

The Hypertext Transfer Protocol (HTTP) is an application-level protocol with the lightness and speed necessary for distributed, collaborative, hypermedia information systems. It is a generic, stateless, object-oriented protocol that can be used for many tasks, such as name servers and distributed object management systems, through extension of its request methods (commands). A key feature of HTTP is the typing of data representation, allowing systems to be built independently of the data being transferred.

HTTP has been in use by the World-Wide Web global information initiative since 1990. Most recently, it is also used as one of the key transport protocols to support Web Services.

Keywords: Internet, transport, file transfer, protocol

1.2.4.2 File Transfer Protocol (FTP)

URL: <http://www.ietf.org/rfc/rfc959.txt>

The File Transfer Protocol (FTP) is an application layer protocol used to copy files from one computer to another. It belongs to the TCP/IP protocol suite and is defined in RFC959 with updates in RFC2228, RFC2640, and RFC2773.

FTP can be used directly by a user at a terminal or by a program. Although it has been around for a very long time (Internet-speaking-wise), it is still very frequently used to upload or download files over the Internet or Intranet networks. FTP uses the Telnet protocol on the control connection.

Keywords: Internet, datagram, Transport, Protocol, file transfer

1.2.4.3 Trivial File Transfer Protocol (TFTP)

URL: <http://www.ietf.org/rfc/rfc1350.txt>

Trivial File Transfer Protocol (TFTP) is a simple protocol to transfer files, and therefore was named the Trivial File Transfer Protocol or TFTP. It has been implemented on top of the Internet User Datagram protocol (UDP or Datagrams) so it may be used to move files between machines on different networks implementing UDP. (This should not exclude the possibility of implementing TFTP on top of other datagram protocols.) It is designed to be small and easy to implement. Therefore, it lacks most of the features of a regular FTP. The only thing it can do is read and write files (or mail) from/to a remote server. It cannot list directories, and currently has no provisions for user authentication. It is commonly used during the initial bootstrap or firmware download/upgrades of devices which lack a persistent local storage, e.g. a diskless workstation etc, within a trusted environment.

Keywords: Internet, datagram, Transport, Protocol, file transfer

1.2.4.4 TELNET Protocol

URL: <http://www.ietf.org/rfc/rfc0854.txt>

The TELNET Protocol provides a fairly general, bi-directional, eight-bit byte oriented communications facility. Its primary goal is to allow a standard method of interfacing terminal devices and terminal-oriented processes to each other. The protocol may also be used for terminal-terminal communication ("linking") and process-process communication (distributed computation). A TELNET connection uses a TCP connection to transmit data with interspersed TELNET control information.

Keywords: Internet, reliable, terminal access.

1.2.4.5 Domain Name System (DNS) protocol

URL: <http://www.ietf.org/rfc/rfc1035.txt>

The Domain Name System (DNS) provides a mechanism for naming resources in such a way that the names are usable in different hosts, networks, protocol families, internets, and administrative organizations. The Domain Name System is a mixture of functions and data types that are an official protocol and functions and data types. Since the domain system is intentionally extensible, new data types and experimental behavior should always be expected in parts of the system beyond the official protocol. The official protocol parts include standard queries, responses and the Internet class RR data formats (e.g., host addresses).

Keywords: Internet, datagram, naming, address resolution.

1.2.4.6 Dynamic Host Configuration Protocol (DHCP)

URL: <http://www.ietf.org/rfc/rfc2131.txt>
<http://www.ietf.org/rfc/rfc3315.txt>

The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options such as the IP address of the default gateway for the host. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts.

Keywords: Internet, addressing, host configuration.

1.2.4.7 URI

URL: http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci214160,00.html

To paraphrase the World Wide Web Consortium, Internet space is inhabited by many points of content. A URI (Uniform Resource Identifier; pronounced YEW-AHR-EYE) is the way you identify any of those points of content, whether it be a page of text, a video or sound clip, a still or animated image, or a program. The most common form of URI is the Web page address, which is a particular form or subset of URI called a Uniform Resource Locator (URL). A URI typically describes:

- The mechanism used to access the resource
- The specific computer that the resource is housed in
- The specific name of the resource (a file name) on the computer

The URI rules of syntax, set forth in the Internet Engineering Task Force (IETF) Request for Comments 1630, apply for all Internet addresses.

Keywords:

1.2.4.8 World Wide Web (WWW)

URL: http://searchcrm.techtarget.com/sDefinition/0,,sid11_gci213391,00.html

A technical definition of the World Wide Web is: all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP). A broader definition comes from the organization that Web inventor Tim Berners-Lee helped found, the World Wide Web Consortium (W3C ®):

"The World Wide Web is the universe of network-accessible information, an embodiment of human knowledge."

Keywords: Internet, WWW

1.2.4.9 Web Browser

URL: [<urls>](#)

Any computer software program for reading hypertext. Note 1: Browsers are usually associated with the Internet and the World Wide Web (WWW). Note 2: A browser may be able to access information in many formats, and through different services including HTTP and FTP. From T1 Glossary 2000: Glossary of Telecommunications Terms.

Any computer software, such as Netscape® Navigator® or Microsoft Internet Explorer®, that can be used to view documents on the Internet. Web browsers interpret the HTML computer language and display Web text and images. Not all Web browsers interpret HTML the same way. Thus, the exact same file may display differently when viewed on different Web browsers. Browsers are often referred to as "client software."

Keywords: Browser, Internet, IE, Netscape

1.2.4.10 Microsoft COM+

URL: http://searchwin2000.techtarget.com/sDefinition/0,,sid1_gci211825,00.html

COM+ is an extension of Component Object Model (COM), Microsoft's strategic building block approach for developing application programs. COM+ is both an object-oriented programming architecture and a set of operating system services. It adds to COM a new set of system services for application components while they are running, such as notifying them of significant events or ensuring they are authorized to run. COM+ is intended to provide a model that makes it relatively easy to create business applications that work well with the Microsoft Transaction Server (MTS) in a Windows NT® or subsequent system.

Among the services provided by COM+ are:

- An event registry that allows components to publish the possibility of an event and other components to subscribe to be notified when the event takes place. For example, when a sales transaction is completed, it could trigger an event that would allow other programs to be notified for subsequent processing.
- The interception of designated system requests for the purpose of ensuring security
- The queues of asynchronously received requests for a service

Keywords: Microsoft

1.2.4.11 SNTP (Network Time Protocol)

URL: [<urls>](mailto:urls)

SNTP (Simple Network Time Protocol) functionality is used on the Internet to synchronize systems over a network by analyzing round-trip time delays statistically. Its accuracy is dependent upon the type of network involved and variability of the time delays in traversing the network.

SNTP is readily available as an Internet protocol and is therefore a relatively inexpensive mechanism to synchronize systems, so long as slight time variations are acceptable.

SNTP is not as accurate as GPS

Keywords:

1.2.4.12 CSV files

URL: http://searchdatabase.techtarget.com/sDefinition/0,,sid13_gci213871,00.html

In computers, a CSV (comma-separated values) file contains the values in a table as a series of ASCII text lines organized so that each column value is separated by a comma from the next column's value and each row starts a new line. A CSV file is a way to collect the data from any table so that it can be conveyed as input to another table-oriented application such as a relational database application. Microsoft Excel, a leading spreadsheet or relational database application, can read CSV files. A CSV file is sometimes referred to as a flat file.

Keywords:

1.2.5 Link Layer and Physical Technologies

1.2.5.1 LAN/MAN Technologies

URL: <http://standards.ieee.org/regauth/oui/index.shtml>

The IEEE 802.* is a family of standards for use in Local Area Networks (LAN) and Metropolitan Area Networks (MAN). These extremely popular and widely used standards describe the physical and data link layers, and also include various management aspects of the protocol family: bridging and management, logical link control, etc. Technologies in this family include Carrier Sense Multiple Access (Commonly known as Ethernet, although 802.3 is slightly different than original Ethernet), Token Ring, Token Bus, Security, Wireless LAN, Personal Area Networks, etc.

Keywords: LAN, MAN, Physical layer, Data Link layer.

1.2.5.2 IEEE 802 MAC Addresses

URL: <http://>

The Media Access Control (MAC) address is a globally unique address typically stored in a network card. It is defined as "a hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the data link layer of the OSI Reference Model is divided into two sublayers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. The MAC layer interfaces directly with the network media. Consequently, each different type of network media requires a different MAC layer. On networks that do not conform to the IEEE 802

standards but do conform to the OSI Reference Model, the node address is called the Data Link Control (DLC) address." The IEEE serves as the registration authority for reserving IEEE 802 MAC Addresses. Because they are globally unique numbers, IEEE 802 MAC Addresses are often used for other purposes, and are referred to as Organizationally Unique Identifiers (OUIs).

Keywords: Media access control layer, Data link layer, Address

1.2.5.3 IEEE 802.3aez Standards

URL: <http://>

A supplement to 802.3, the "Ethernet" carrier sense multiple access with collision avoidance (CSMA/CD) standard, 802.3aez defines Gigabit Ethernet (GbE) standards. The IEEE 802.3z formalized Gigabit Ethernet (GbE). Two versions exist, both of which are compatible with 10/100 Mbps Ethernet. Shared GbE, also known as 1000Base-T, essentially is a higher speed version of 10/100Base-T, with the shared bus running at 1 Gbps. IEEE 802.3a and 802.3e define the standards for the 10 GbE. While GbE is backward compatible with 10/100 Mbps Ethernet, there are a few differences beyond raw speed, and it does require upgrading.

Keywords: protocol, data link layer, LAN, Ethernet, Gigabit, high speed

1.2.5.4 IEEE 802.1p and IEEE 802.1q (VLAN)

URL: <http://>

These standards define tags that extend the 802.3 (Ethernet) frame to include a 3-bit priority indicator (802.1p) and a 12-bit Virtual LAN (VLAN) identifier (802.1q). The 3-bit priority indicator can be used to prioritize the treatment of frames within the network, e.g. scheduling priority within an Ethernet switch, buffer-allocation quota etc. The VLAN tags partition a physical LAN into multiple logical LANs to enhance administration, security as well performance of the logical LANs.

Keywords: VLAN, priority, Ethernet

1.2.5.5 IEEE 802.1d Spanning Tree Protocol (STP)

URL: <http://>

Spanning Tree Protocol (STP) is a protocol and associated algorithm for selecting links between Ethernet switches to be disabled or blocked to guarantee that there are no loops in the network. If a link fails, STP will automatically detect the failure and unblock links to restore service.

Keywords: Spanning Tree protocol, reconfiguration, restoration, loop prevention.

1.2.5.6 IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)

URL: <http://>

Rapid Spanning Tree Protocol (RSTP) is a protocol extending 802.1d to a message-based protocol that allows much faster restoration and reconfiguration.

Keywords: Spanning Tree protocol, reconfiguration, restoration, loop prevention.

1.2.5.7 IEEE 802.17 - Resilient Packet Ring (RPR)

URL: <http://>

The IEEE 802.17 working group is defining a Resilient Packet Ring access protocol for LAN, MAN and WAN to transfer data at rates of many gigabit per second.

Keywords: high-availability, high-speed, LAN, MAN, WAN, physical layer, data link layer.

1.2.5.8 LAN interconnection technologies

This is the set of the technologies that can be used to extend the range of a LAN by interconnecting multiple LAN segments together.

1.2.5.9 Ethernet

URL: <http://standards.ieee.org/getieee802/802.3.html>
<http://grouper.ieee.org/groups/802/3/ae/index.html>

Ethernet is a LAN technology first developed by Xerox®, and refined by DEC and Intel (DIX). The access mechanism is Collision Sense Multiple Access with Collision Detection (CSMA/CD). Ethernet was standardized by the IEEE in the IEEE 802.3 standard. Today the term Ethernet includes 10, 100 (Fast), and 1000 (Gigabit) Mbps Ethernet technologies. Development of 10 Gbps Ethernet is in progress in the IEEE 802.3ae 10Gb/s Ethernet Task Force. Ethernet is the most common LAN technology with 88% of the installed base and 98% of all new purchases being Ethernet.

1.2.5.10 Hubs/Repeaters

URL: <http://>

Hubs/ Repeaters interconnect multiple LAN segments at the physical layer by repeating an incoming signal at one of its port to all other ports in a bit-by-bit manner, to result in a single broadcast/collision domain. As such, it cannot be used to interconnect different types of LAN technologies, e.g. between a 10BT and a 100BT Ethernet segments. Manual care is required in order to avoid the formation of loops within the hubbed network topology.

Keywords: LAN interconnection, loop.

1.2.5.11 Bridges/Switches

URL: <http://>

Bridges/Switches interconnect multiple LAN segments/ hosts/ gateways at the data link layer. Most bridges/switches also provide MAC address learning features that can reduce the unnecessary broadcast of frames and thus collisions across all of the LAN segments/hosts to be interconnected. They can also be used to interconnect different types of LAN technologies, e.g. between a 10BT and a 100BT Ethernet segments. 802.1d Spanning Tree Protocol is usually run by bridges/switches to automatically eliminate the formation of loops within the interconnected LAN.

Keywords: LAN interconnection, bridging, switching, loop.

1.2.5.12 Routers

URL: <http://>

Routers interconnect multiple LAN segments/ hosts/ gateways at the network layer. Routers forward packets between its ports according to the router table it holds. The routing table is populated either via manual configuration or by running routing protocols amongst the routers and possibly the end-hosts.

Keywords: LAN interconnection, routing, packet forwarding.

1.2.5.13 V series Modems

URL: <http://www.itu.int>

The ITU-T developed a series of modem standards, prefaced by letter "V" (e.g., V.22, V.25, V.32, V.33, V.34, V.42, V.90), that are fairly mature. These standards vary on parameters such as synchronous/asynchronous transmission, 2-wire/4-wire, half/full duplex, error correction and data compression abilities. They provide data rates of 4.8 to 56 kbps. V.34, one of the more commonly used standards, provides up to 28.8 kbps and falls back to lower speed for compatibility. V.90, the latest modem standard, provides a rate of up to 56 kbps.

Keywords: physical layer, serial, Modem, high reliability, high speed, Compression, Error correction.

1.2.5.14 Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1

URL: <http://www.itu.int>
<http://www.itu.int>

Digital signal X is based on the ANSI T1.107 guidelines. Digital Signal X is a term for the series of standard digital transmission rates or levels based on DS0, a transmission rate of 64 Kbps, the bandwidth normally used for one telephone voice channel. Both the North American T-carrier system and the European E-carrier systems of transmission operate using the DS series as a base multiple. The digital signal is what is carried inside the carrier system, typically via time division multiplexing. DS0 is the base for the digital signal X series. DS1, used as the signal in the T-1 carrier, is 24 DS0 (64 Kbps) signals transmitted using pulse-code modulation (PCM) and time-division multiplexing (TDM). DS2 is four DS1 signals multiplexed together to produce a rate of 6.312 Mbps. DS3, the signal in the T-3 carrier, carries a multiple of 28 DS1 signals or 672 DS0s or 44.736 Mbps. Telecom companies have developed transmission services which are essentially a T1 line with some of the channels turned off. This is to target towards the niche of cost-sensitive customers. Typical speeds for fractional T1's are 256, 384, 512 and 768kbps.

Main Features of Technology

Technology	Frame based transmission over high-speed T1 circuits. Equivalent to X.25 without network layer functions (node-to-node error checking)
Operation	Allows customers to select port speed and request permanent virtual circuit (PVC) with committed information rate (CIR)
Bandwidth	Amount of bandwidth is adjusted to meet application, but limited
Capacity	Up to capacity of T1 and multiple T1s
Coverage	Same as that provided by LECs (local exchange carriers)
Data rate	For each customer, port speed and CIR from 16Kbps to 256Kbps or higher, up to the limit of the T1 or fractional T1 installed
No. of channels	PVC, typically 64 channels per T1
Regulatory	None

Key Advantages

Capacity	Multiple T1s can be provided rapidly by telecommunications providers
Coverage	Very broad coverage for most areas, as provided by LEC
Data rate	Committed information rate (CIR)
Access	Faster network access without latency resulting from node-to-node error checking (in X.25 network)

Key Disadvantages

Cost	Cost of local access circuit can be high if the location of the carrier's POP (point-of-presence) is not in the same city
Access	End devices need to perform error checking and request for re-transmission should error be found. This may slow down overall data transmission Network congestion may cause frames to be discarded and will require re-transmission.

Keywords: time division multiplexing, digital signal hierarchy, transmission.

1.2.5.15 X series Data Network

URL: <http://>

The ITU-T developed a series of data networking standards, designated by the prefix "X", some of which have become extremely popular. The X.25 standard, for example, and its High-level Data Link Control (HDLC) data link layer, were so widespread that they have served as the basis for many of the other technologies described in this Guide. A more recent example is the International version of the Frame Relay Standards.

Frame relay is a widely used, mature packet technology used mainly for wide-area network (WAN) services. Frame relay provides connection-oriented, data link layer communication with the addition of packet relaying, based on the assumption of low noise links and high-speed processors. The Frame Relay Forum is an association that promotes the development and use of this technology. Frame relay was developed as a part of the Integrated Services Digital Network (ISDN) framework, and is specified in many X-series ITU-T standards. Parts are also specified in ITU I.122 and Q.922.

Keywords: Packet-switched networking, data link layer.

1.2.5.16 Frame Relay

URL: <http://www.frforum.com/>

Frame Relay is a technology that has been around since 1990. It evolved out of the older X.25 packet technology and is the packet part of ISDN and defined in I.122. Frame Relay is a simplified form of Packet Switching similar in principle to X.25 in which synchronous frames of data are routed to different destinations depending on header information.

The main differences between Frame Relay and X.25 are that X.25 guarantees data integrity (error detection) and network managed flow control at the cost of some network delays. Frame Relay switches packets much faster end-to-end, but there is no guarantee of data integrity. Instead, it is up to the end devices to check for and correct errors. .

Keywords: Interoperability, network layer, data link layer, Privately-owned WAN services, Public Network Services

1.2.5.17 Point-to-Point Protocol (PPP)

URL: <http://www.ietf.org/rfc/rfc1661.txt>

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP is comprised of three main components:

- A method for encapsulating multi-protocol datagrams.
- A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.
- A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

Keywords: data link layer, multiprotocol, encapsulation, link control, network control.

1.2.5.18 Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH)

URL: <http://www.ansi.org>
<http://webstore.ansi.org/ansidocstore/default.asp>

Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH) are two virtually identical standards that specify synchronous data transmission over a fiber optic network. They are a **physical layer** technology designed to provide a universal transmission and multiplexing scheme, with transmission rates in the gigabit per second range, and a sophisticated operations and management system.

SONET, primarily used in the US and Japan, is published by **ANSI T1.105, 117 and 119**. while SDH, the international version, is published by the by **ITU-T** (G.707, 708, 709, and 783). The most commonly used speed categories are shown in the table below.

Optical Level	Electrical Level	Line Rate (Mbps)	SDH Equivalent	Capacity
OC-1	STS-1	51.840	-	28 DS1s (T-1) or 1 DS3 (T-3)
OC-3	STS-3	155.520	STM-1	84 DS1s or 3 DS3s or 1 E4
OC-12	STS-12	622.080	STM-4	336 DS1s or 12 DS3s or 4 E4
OC-48	STS-48	2488.320	STM-16	1344 DS1s or 48 DS3s or 16 E4
OC-192	STS-192	9953.280	STM-64	5376 DS1s or 192 DS3s or 64 E4
OC-768	STS-768	39813.12	STM-256	21504 DS1s or 768 DS3s or 256 E4

OC = Optical Carrier, STS = Synchronous Transport Signal, STM = Synchronous Transport Module

SONET data rates are from OC-1 (51+ Mbps) to OC-768 (768 times OC-1). OC-1 is one-third the STM-1 rate of SDH. Aside from ANSI, other forums such as SONET Interpretability Forum (SIF), ATM Forum (for ATM over SONET) and IETF (for Packet Over SONET, POS) work or have worked on various aspects of SONET. One of the very important aspects of SONET is the restoration work that has gone into it and has made networks as resilient as they are to failures. SONET is typically deployed in dual redundant ring topologies. SONET offers the ability to provide protection from physical and logical failures in the ring in 50 ms based on the automatic protection-switching (APS) standard.

Keywords: media, fiber optic, physical layer

1.2.5.19 Asynchronous Transfer Mode (ATM)

URL:

Asynchronous Transfer Mode (ATM) is a means of digital communications that is capable of very high speeds (currently up to 40 Gbps using SONET/OC-768). It is used for the transport of voice, video, data, and images. ATM is an ITU-T standard for cell relay. Information is conveyed in small, fixed-size cells. ATM is the world's most widely deployed backbone technology. ATM has been widely adopted because of its flexibility in supporting the broadest array of technologies, including DSL, IP Ethernet, Frame Relay, SONET/SDH and wireless platforms. ATM can be used both for WANs and LANs.

ATM itself consists of a series of layers. The first layer - known as the Application Adaptation Layer (AAL) - holds the bulk of the transmission. This 48-byte payload divides the data into different types. The ATM layer contains five bytes of additional information, referred to as overhead. This section directs the transmission. Lastly, the physical layer attaches the electrical elements and network interfaces.

Keywords: Physical Layer, WAN

1.2.6 Wireless Technologies

1.2.6.1 3rd Generation Cellular Wireless

URL: <http://www.3gpp.org>
<http://www.3gpp2.org>

3G cellular standards are developed by the by the Third-Generation Partnership Project (3GPP), a joint venture of several standard organizations such as the European Telecommunications Standards Institute (ETSI), ANSI, and the Alliance for Telecommunications Industry Solutions (ATIS) Committee T1. The 3GPP is based on the ITU's International Mobile Telecommunications 2000 (IMT-2000) initiative. The characteristics of a 3G wireless standard, motivated by mobility and use of Internet are: (i) support all mobile applications, (ii) support both packet-switched (PS) and circuit-switched (CS) data transmission, and (iii) offer high data rates up to 2 Mbps. The most important IMT-2000 proposals are the UMTS and CDMA-2000 (discussed in next two sections). These standards cover both the air interface and the core network solution. The main effort of 3GPP is to facilitate convergence of 3G networks, providing seamless global roaming between the different modes of CDMA 3G.

Keywords: Cellular, Third generation, wireless, telephony

1.2.6.2 Universal Mobile Telecommunication System (UMTS)

URL: <http://www.3gpp.org>

UMTS, also called Wideband Code Division Multiple Access (W-CDMA), is a successor to the widely used Global System for Mobile communication (GSM). UMTS air interface transmission differs from GSM, however, in being based on CDMA rather than TDMA. UMTS provides the following service types: (i) conversational class (voice, video telephony, video gaming), (ii) streaming class (multimedia, video on demand, webcast), (iii) interactive class (web browsing, network gaming, database access), and (iv) background class (email, SMS, downloading).

Keywords: wireless, cellular, telephony, third generation, physical layer, link layer, spread-spectrum

1.2.6.3 Code-Division Multiple Access 2000 (CDMA-2000)

URL: <http://www.3gpp2.org>

CDMA-2000 is family of third-generation cellular wireless standards based on the second-generation IS95 CDMA standard. It was developed by the Third Generation Partnership Project 2 (3GPP2). It consists of:

- 3G1xEV-DO (Evolution-DataOnly), also called High Data Rate (HDR), can serve up to 2 Mbps, downlink, to a single user.
- 3G1xEV-DV (Evolution-Data & Voice) is also an efficient version of CDMA technology for both voice and data.

Keywords: wireless, cellular, telephony, third generation, physical layer, link layer

1.2.6.4 TDMA Cellular Wireless - IS-136

URL: <http://www.tiaonline.org/>

Time Division Multiple Access (TDMA), developed by the ANSI-accredited Telecommunications Industry Association (TIA), is digital transmission technology that allocates unique time slots to each user within each channel. The two major (competing) systems that split the cellular market are TDMA and CDMA. Because of its adoption by the European standard GSM, and the Japanese Digital Cellular (JDC), TDMA and its variants are currently the technology of choice throughout the world. However, third-generation wireless networks will use CDMA, not TDMA.

Keywords: physical layer, Cellular, Wireless, TDMA

1.2.6.5 CDMA Cellular Wireless - IS-95

URL: <http://www.tiaonline.org/>

Code Division Multiple Access (CDMA) for Spread Spectrum, has become the technology of choice for the future generation of wireless systems. IS-95 based CDMA system developed by the ANSI-accredited Telecommunications Industry Association (TIA) have been widely deployed in the U.S. IS-95 evolves to CDMA-2000 for third-generation cellular systems.

Keywords: physical layer, Cellular, Wireless, Spread Spectrum

1.2.6.6 Cellular Digital Packet Data (CDPD)

URL: <http://www.tiaonline.org/>

CDPD, developed by ANSI-accredited Telecommunications Industry Association (TIA), is a packet data service, defined as an overlay network for the cellular TDMA network. By reusing cellular frequency spectrum, transport connection and antenna systems, CDPD can be made available on existing networks. CDPD is an open specification, supports both IP and CLNP, and is advertised to provide a data rate of up to 19.2 kbps.

Keywords: physical layer, network layer, transport layer, WAN, wireless, cellular, TDMA.

1.2.6.7 Global System for Mobile Communication (GSM)

URL: <http://www.gsmworld.com>
<http://www.etsi.org>

Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a

common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz. GSM is using Time Division Multiple Access (TDMA) wireless technology and many countries outside of Europe have joined the GSM partnership.

Keywords: physical layer, Cellular, wireless, TDMA.

1.2.6.8 Short Message Service (SMS)

URL: <http://www.gsmworld.com>
<http://www.etsi.org>

Short message service (SMS) is a wireless service that enables the transmission of textual messages between mobile subscribers and external systems such as electronic mail, paging, and voice-mail systems. SMS is available initially on digital wireless networks based on GSM, code division multiple access (CDMA), and time division multiple access (TDMA) standards.

Keywords: physical layer, Wireless, Messaging.

1.2.6.9 Global Positioning System (GPS)

URL: http://www.colorado.edu/geography/gcraft/notes/gps/gps_f.html

GPS, or the Global Positioning System, offers a way to determine time to a precision of better than a few hundred nanoseconds almost anywhere on the surface of the earth. It also offers real-time position fix with an accuracy of 3 to 100 meters on a 24-hour per day basis. GPS is developed and operated by the US Department of Defense. The GPS system consists of 24 satellites, orbiting the earth at an altitude of about 10,900 miles and at an inclination of 55 degrees. The orbits are distributed around the earth in such a way that at least 4 satellites are always visible from virtually any point on the surface of the earth. This provides a means of precisely determining the position of the user in longitude, latitude, and altitude. GPS uses Spread Spectrum signals to perform measurements.

Advantages/Strengths

GPS devices can be directly connected to equipment to provide extremely accurate time synchronization and time-stamps. For equipment where time synchronization and time-stamping accuracy is paramount, GPS is preferred over the alternative of SNTP (Simple Network Time Protocol) functionality, which is used to synchronize systems over a network by analyzing round-trip time delays statistically.

Disadvantages/Weaknesses

GPS devices, although decreasing in price, are still too expensive for every type of device requiring some level of time synchronization.

Keywords: time synchronization, Position, Spread Spectrum

1.2.6.10 Trunked Mobile Radio (TMR, TETRA, Project25)

URL: <http://www.tetramou.com>
<http://www.etsi.org>
<http://www.project25.org>
<http://www.apcointl.org>

Trunking refers to the automatic and dynamic sharing of a small number of radio channels among a large number of radio users. Trunked Mobile Radio promises greater airtime efficiency, ease of use and higher availability, compared to other technologies. A TMR system efficiently distributes

message traffic among available channels and reduces queuing time. Large organizations, such as local governments (or utilities) that need to establish their own dedicated radio network typically select a trunked radio scheme. TMR systems offer privacy, wide-area dispatch, economical infrastructure, and more efficient use of radio spectrum. TMR is primarily talk-group based and enables access to multiple facilities by multiple users. TMR services take place in a one-to-many or one-to-one application.

The majority of trunked radio systems are proprietary. However, the TERrestrial Trunked Radio system (TETRA) is an open digital trunked radio standard defined by the European Telecommunications Standardization Institute (ETSI). The TETRA Memorandum of Understanding (MoU) was established in December 1994 to create a forum for discussion, promotion and development of the standard.

The Association of Public Safety Communications Officials (APCO) Project25 developed the 102 series of technical specifications for digital, land mobile radio communications systems. The process was led by a users' Steering Committee, and the standardization work was done by the Telecommunications Industry Association. The result is a suite of ANSI/EIA/TIA standards, TIA/EIA Interim Standards, and TIA Telecommunications System Bulletins. Although Project25 originally was an initiative of public safety, the resultant documents are usable in any application for digital, land mobile applications. Projrct25 work includes key attributes: (i) backward compatibility with existing systems, (ii) scalable trunked and conventional capabilities from single channel to regional trunking, (iii) spectral efficiently from 12.5 kHz to 6.25 kHz, and (iv) interoperability between neighboring systems.

Main Features of Technology

Technology	Radio
Frequency	800 MHz range
Bandwidth	25KHz/12.5KHz
Operation	Can be configured as single site, voted or simulcast system. all channels are shared and automatically switched.
Capacity	Better utilization of frequencies or channels, hence more capacity, by allowing users to share all available channels for voice and data, i.e. trunking
Coverage	Coverage can be extended through use of repeaters, voting receivers and simulcast
Data rate	2.2Kbps throughput low due to call setup delay and small bandwidth
No of Channels	Multiple frequencies or channels, typically 10-20 channels per system
Modulation method	FSK, PSK
Power	Repeater station 50-100W, control station 10-40W, mobile 10-30W
Regulatory	Frequency licensing required

Key Advantages

Capacity	Better utilization of frequencies by users sharing all channels
Coverage	Can extend coverage by using repeaters
Interference	Licensed frequencies protect mobile units against outside interference
Reliability/Availability	Reliability is better because network is more fault-tolerant. Availability is definitely better than mobile radio because more channels are available and different configurations can be used to improve system performance.
Cost	Relatively high due to more sophisticated trunking equipment

Key Disadvantages

Data rate	2.2kbps but low throughput
-----------	----------------------------

Regulatory	Trunking frequencies require licensing and the process is time consuming
------------	--

Keywords: wireless, mobile, radio, physical layer

1.2.6.11 IEEE 802.11 Wireless Local Area Network (WLAN)

URL: <http://www.wirelessethernet.org/OpenSection/index.asp>

This standard provides wireless connectivity to mobile or portable equipment within a LAN area. The IEEE 802.11 standard specifies both the physical (PHY) and medium access control (MAC) layers of the network. The physical layer can use either direct sequence spread spectrum, frequency hopping spread spectrum, or infrared (IR) pulse position modulation. The MAC layer specifies CSMA/CA protocol. Security is one of the major concerns of wireless LANs in general and this technology in particular. IEEE 802.11a and 802.11b have data rate of 55 and 11 Mbps respectively. IEEE 802.11b is currently in widespread use. Wireless Fidelity (WIFI) Alliance certifies interoperability of WIFI technology product using 802.11b.

Keywords: LAN, wireless, Physical layer, MAC layer, spread-spectrum, infrared, mobile computing.

1.2.6.12 IEEE 802.15 Wireless Personal Area Network (PAN)

URL:

The IEEE 802.15 family of standards address Personal Area Networks or short distance wireless networks. Such WPANs include wireless networking of portable and mobile computing devices such as PCs, Personal Digital Assistants (PDAs), peripherals, cell phones and consumer electronics. The goal of this standards group is to publish standards and recommended practices that have broad market applicability and deal with the coexistence and interoperability of other wired and wireless networking solutions. Bluetooth is one of the technologies adopted by this group.

Keywords: Personal, LAN, wireless, Physical layer, MAC layer, data link layer, mobile computing.

1.2.6.13 Bluetooth Special

URL: <http://www.bluetooth.com/>

Bluetooth® is a standard and specification for low-cost, short range radio links between mobile PCs, mobile phones and other portable devices. The technology allows users to form wireless connections between various communication devices, in order to transmit real-time voice and data communications. It overlaps in functionality with IEEE 802.11. It has been adopted by IEEE 802.15, the Wireless Personal Area Network (PAN) group;. The Bluetooth Special Interest Group (SIG) is a trade association dedicated to the development and promotion of this technology.

Keywords: Wireless, LAN

1.2.6.14 IEEE 802.16 Broadband Wireless Access Standards

URL: <http://www.ieee802.org/16/>

The IEEE 802.16 Working Group on Broadband Wireless Access Standards develops standards and recommended practices to support the development and deployment of broadband Wireless Metropolitan Area Networks. IEEE 802.16 is a unit of the IEEE 802 LAN/MAN Standards Committee. IEEE 802.16 addresses the "first-mile/last-mile" connection in wireless metropolitan area networks. It focuses on the efficient use of bandwidth between 10 and 66 GHz (the 2 to 11 GHz region with PMP and optional Mesh topologies by the end of 2002) and defines a medium access control (MAC) layer that supports multiple physical layer specifications customized for the frequency band of use. A closely related body, WiMAX is comprised of companies who are committed to the open interoperability of all products used for broadband wireless access. The purpose of WiMAX is to promote deployment of broadband wireless access networks by using a global standard and certifying interoperability of products and technology. WiMAX supports IEEE 802.16 standard and propose and promote access profiles for IEEE 802.16 standard. It also certifies interoperability levels both in network and the cell.

Keywords: wireless, Physical layer, MAC layer, MAN, data link layer.

1.2.6.15 Multiple Address (MAS) Radio

URL: <http://www.micronetcom.com/mas.htm>

MAS radio has gained popularity in recent years due to its flexibility, reliability and compact size. A basic MAS radio link consists of a master radio transmitter/receiver unit and multiple remote radio transmitter/receiver units. A master unit can access or poll multiple units via a pair of transmit/receive frequencies. The master unit is set up always ready to transmit and receive in order to keep delay due to transmitter keying to a minimum. Each remote unit is set up always in the listening mode until it is polled and then ready to transmit. Each remote unit has a unique address so no two units will try to answer the poll at the same time. This eliminates any contention among the remotes to transmit to the master. The frequency pair used by MAS requires to be licensed by the FCC and the same pair can be re-used elsewhere in the system as long as it does not cause any interference.

For performance reasons, there is a limit to the number of remotes that can be polled by one master radio. This limit is determined by the time delay in the poll and the handshaking required in the response, the data transmission rate and the data collection time set by the system. So, for a large service area, many master radios will need to be used to cover groups of remote units each located in or near a utility owned facility. For difficult-to-reach locations due to topography or limitation of line-of-sight, the same MAS radio can be used as a repeater radio to allow signal transmission over or around large obstructions.

Typically each master radio is located at a site where there is an existing connection to the utility's control center where data is collected for the entire system. This can be a microwave site or fiber optic network node in a network. MAS radio is the preferred communication medium and has been used widely by utilities for SCADA (supervisory control and data acquisition) systems and DA (distribution automation) systems.

Main Features of Technology

Technology	Radio
Frequency	895 to 960 MHz transmit/receive frequency pair
Bandwidth	25kHz for existing frequencies, 12.5kHz for new frequencies
Operation	Requires line-of-sight, point-to-multipoint for master and remote radios
Capacity	Can be expanded by using more master radios, but will be limited by

	how fast remotes can be polled and system scan period allowed
Coverage	Each link is typically 15km
Data rate	Up to 4.8kbps, can be increased to 9.6Kbps but coverage will be reduced
No. of channels	Minimum separation between adjacent channels is 25kHz for previous frequency allocations and 12.5KHz for new frequency allocations
Multiplexing/modulation method	Frequency shift keying (FSK)
Power	5W master, 1W remote
Regulatory	Frequency licensing required

Key Advantages

Capacity	Capacity is limited by data speed and system scan time. Also, limited by the number of masters that can be physically installed in the system (location, topography, etc.)
Coverage	Can typically reach 15 km, can be extended by using repeaters
Data rate	Up to 9.6kbps (with reduced coverage)
Reliability	Can be improved with remote diagnostics, warm standby equipment and redundant architecture
Interference	Licensed frequencies provide some protection against interference by others
Cost	Relatively low

Key Disadvantages

Operation	Line-of-sight to remotes prone to obstruction
Regulatory	Licensing is time consuming and may not be possible due to lack of available frequencies

Keywords: Wireless, LAN

1.2.6.16 Spread Spectrum Radio System

URL: <http://www.conformity.com/0008emc1.html>
<http://grouper.ieee.org/groups/802/11/main.html>
<http://www.sss-mag.com/ss.html>

To avoid having to operate with allocated frequencies from the FCC, a different type of radio known as spread spectrum (SS) radio is used in point to multipoint radio systems. The configuration of the master and remote radios is exactly the same as that for the MAS. The only difference is that FCC Part 15 Rules allow these radios to operate without the need for a license in the 902-928MHz frequency band. To meet the FCC criteria, the radios must operate at low power and must continually hop over a range of frequencies (typically 64 or more), staying on one frequency only for a short fixed period (typically 250 ms). Special processing built into the radio allows the radio to recover data in its original format while continually changing frequencies.

Two spread spectrum modulation techniques are commonly used to achieve spread spectrum. One technique uses the direct sequence method in which the carrier is modulated by a digital code that runs much faster than the modulation rate. With digital data, this means that each bit of data can be spread over a wide frequency band, resulting in less power and a more limited transmission range of typically 3 to 5 miles. The other technique uses the frequency hopping method in which a digital code also moves a carrier but it runs much slower than the modulation

rate. Thus, frequency hopping allows a block of data to be transmitted in the span of, say, 250 milliseconds on one frequency before it switches to another frequency.

When SS radio is used for MAS type application, the coverage is often less because of the low power restriction. Line-of-sight is still required for optimal coverage. However, the ability to operate with unlicensed frequencies is very attractive to potential users because it allows installation to be done quickly without licensing delay. For this reason, SS radio is often used as last-mile connections to a main communication system and, in such an application, the line-of-sight requirement is not as stringent and reliable communication can be achieved even if trees, buildings or terrain obstruct the path. However, each obstruction does reduce the RF (radio frequency) strength. When operating in the unlicensed spread spectrum band, interference is considered normal because there will be many users using the same frequencies. The primary effect is somewhat lower communication throughput. A number of remedies can be used to improve radio performance.

Main Features of Technology

Technology	Radio
Frequency	900 MHz range or 2.4 GHz range
Bandwidth	12.5kHz for 900MHz, 20MHz for 2.4GHz
Operation	In point-to-multipoint configuration, one master radio can poll multiple remote radios but can also operate point-to-point (last mile connection)
Capacity	Limited by data rate and system scan time (same as MAS)
Coverage	5-8 km for direct sequence spread spectrum radio, 16-24 km for frequency hopping spread spectrum radio, can be extended by using repeaters
Data rate	Up to 19.2Kbps for 900MHz radio, T1/E1 (1.544Mbps/2.408Mbps) for 2.4GHz radio
No. of Channels	Typically 50 or more
Multiplexing/modulation method	Spreading of frequencies by direct sequence or frequency hopping techniques
Modulation	OQPSK (offset quadrature phase shift keying)
Power	low 0.1W to 1W
Regulatory	No licensing required for frequencies but directional antenna gain, antenna height, number of hopping frequencies and max. dwell time on each frequency are regulated

Key Advantages

Capacity	In point-to-multipoint system, one master radio can poll multiple remote radios and capacity is limited only by data speed and system scan time
Coverage	5-8 km or 16-24 km
Data rate	Up to 19.2Kbps for 900 MHz, T1 or E1 for 2.4GHz
Reliability	Increased by choosing unobstructed transmission path, using redundant hardware, loop-back diagnostics and forward error correction code
Interference	Designed to operate in environment where interference exists. Interference to others is limited by low power and frequent frequency changes
Security	Spread spectrum techniques provide significant security against eavesdropping, replay, spoofing, denial of service, and interception of information
Regulatory	No licensing required in USA
Cost	Relatively low

Key Disadvantages

Operation	Line-of-sight makes medium prone to obstruction but some obstruction can be tolerated
-----------	---

Keywords: wireless, LAN, frequency hopping, direct sequence,

1.2.6.17 Satellite Leased Channels and VSAT

URL: <http://www.gvf.org/>

A satellite circuit has five elements - two terrestrial links, an uplink, a downlink, and a satellite repeater. The satellite itself consists of six subsystems: physical structure, transponder, attitude control apparatus, power supply, telemetry equipment, and station-keeping apparatus. Earth stations vary from simple, inexpensive receive-only stations to elaborate two-way communications stations.

An earth station includes microwave relay equipment, terminating multiplex equipment, and a satellite communications controller. The relay equipment is different from terrestrial microwave in that the transmitter has a much higher power output and very large antennas (up to 30m in diameter for GEO earth stations) are used. The satellite communications controller apportions the satellite's bandwidth, processes signals for satellite transmission, and interconnects the earth station's radio equipment to terrestrial circuits.

Satellites employ several techniques to increase the traffic carrying capacity and to provide access, namely: FDMA (frequency division multiple access), TDMA (time division multiple access), and DAMA (demand assigned multiple access). The $\frac{1}{4}$ second time delay between two earth stations is noticeable in voice communication circuits. Data communication circuits that use a block transmission protocol will drop to an unacceptably low throughput via a satellite because a station can transmit a new block only after the receiver acknowledges the preceding block.

Several satellite-based services are available. The one most often used by utilities is called Very Small Aperture Terminal (VSAT) that uses a very small transmitting antenna (0.6 to 3.8 meter), and is star-connected with a hub at the center of the network and with dedicated lines running to the host computer. The hub has a large antenna aimed at the satellite. The hub is very expensive and is usually owned by the VSAT vendor. TDMA and spread spectrum technologies are the most common ways of allocating access to the hub by the VSATS. VSAT provides bandwidth as high as T1/E1 or as low as what the customer needs for video, voice and data. CONSAT and GTE have formed a partnership that allows air passengers to make air telephone calls via satellite.

Generally, these systems operate in the Ku-band and C-band frequencies. Ku-band based networks are used primarily in Europe and North America and utilize the smaller sizes of VSAT antennas. C-band, used extensively in Asia, Africa and Latin America, require larger antenna.

VSAT networks come in various shapes and sizes ranging from point-to-point, point-to-multipoint, and on demand for thousands of sites based on a dedicated facility located at their own site. Mesh systems have traditionally been somewhat smaller in size than star systems - 5 to 30 sites used to be a good rule of thumb - but since prices have come down, some networks now comprise as many as several hundred or even thousands of sites.

Keywords: Wireless, satellite, broadband, very small aperture terminal

1.2.6.18 Paging Systems

URL: <http://www.braddye.com/newsletters/4apr2003.html>

A paging network is a collection of paging terminals, system controllers, transmitters, receivers and data links, all carefully engineered to make sure the paging system has optimal coverage and response capabilities with minimal interference. Some paging systems are land-based, while some rely on satellites for large-area coverage.

Like cellular systems, virtually all of the paging networks involve more than one transmitter. Paging networks, especially those that support one-way subscriber devices, rely on simulcast capability to blanket an area. Several transmitters must send the same message over a wide area using the same frequency. This is very different from the cell-based targeted delivery methods used in cellular systems. Paging carriers use the same infrastructure to support both one-way and two-way subscribers.

Not all of the paging infrastructures support single transmitter or cell-based targeted message delivery. Paging systems are store-and-forward systems. They accept messages for delivery to paging devices and store them for a brief period before delivery.

Paging terminals interface to the Public Switched Telephone Network (PSTN) to permit subscribers to dial up and send pages from their telephones. To support alphanumeric messaging, many terminals support access to alpha entry devices that may include PCs or other specialized terminals and through a dial-up modem connection. With the advent of Internet e-commerce, paging terminals also accept messages from new sources such as email and the World Wide Web. Infrastructure suppliers and other vendors usually develop the gateways that translate between the Internet protocols and the paging protocols supported by the paging terminals.

In a paging system, the system controllers perform the tasks of queuing, batching, encoding, and scheduling messages received from paging terminals for delivery to transmitter sites. The most valuable resource available to paging carriers is their RF (radio frequency) spectrum. Therefore, the system controller plays a significant role in optimizing the use of this scarce resource by implementing sophisticated scheduling algorithms, both for inbound and outbound RF channels.

The networks used to connect paging terminals to each other, paging terminals to system controllers, and system controllers to transmitters and receivers can be very complex. These can be wire-line networks that consist of digital links such as T1/E1, analog lines, and frame relay networks. Wireless networks may also include satellite, microwave, or radio.

Generally, paging systems are highly reliable, unless a solar storm or electronic problem causes the satellite to fail.

Keywords: Paging

1.2.6.19 Radio Frequency Identification (RFID)

URL: <http://www.usingrfid.com/>

RFID (radio frequency identification) is a technology that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum to uniquely identify an object, animal, or person. RFID is coming into increasing use in industry as an alternative to the bar code. The advantage of RFID is that it does not require direct contact or line-of-sight scanning. An RFID system consists of three components: an antenna and transceiver (often combined into one reader) and a transponder (the tag). The antenna uses radio frequency waves to transmit a signal that activates the transponder. When activated, the tag transmits data back to the antenna. The data is used to notify a programmable logic controller that an action should occur. The action could be as simple as raising an access gate or as complicated as interfacing with a database to carry out a monetary transaction. Low-frequency RFID systems (30 KHz to 500 KHz) have short transmission ranges (generally less than six feet). High-frequency RFID systems (850 MHz to 950 MHz and 2.4 GHz to 2.5 GHz) offer longer transmission ranges (more than 90 feet). In general, the higher the frequency, the more expensive the system.

RFID is sometimes called dedicated short range communication (DSRC).

Keywords: RF, ID, RFID

1.2.7 Quality-of-Service-enabling Technologies

1.2.7.1 Multi-Protocol Label Switching (MPLS)

URL: <http://www.ietf.org/rfc/rfc3031.txt>

In an Multi-protocol Label Switching (MPLS) [RFC 3031] network, incoming packets are assigned a "label" by a label edge router (LER) and forwarded along a label switch path (LSP) where each label switch router (LSR) makes forwarding decisions based on the contents of the label. Label Switch Paths (LSPs) are established by network operators for reasons such as to guarantee a certain level of performance, to route around network congestion, or to create IP tunnels for network-based virtual private networks (VPN). LSPs are similar to circuit-switched paths in ATM or Frame Relay networks, except that they are not dependent on a particular Layer 2 technology. An LSP can be established that crosses multiple Layer 2 transports such as ATM, Frame Relay or Ethernet. Thus, one of the true promises of MPLS is the ability to create end-to-end circuits, with specific performance characteristics, across any type of transport medium, eliminating the need for overlay networks or Layer 2 only control mechanism. Ongoing work includes MPLS restoration and GMPLS, an extension of MPLS to be used for configuring paths in optical switches, TDM multiplexers, and SONET add-drop multiplexers.

Keywords: Internet, Forwarding, QoS, data link layer switching, Protocol

1.2.7.2 Differentiated Services (DiffServ)

URL: <http://www.ietf.org/rfc/rfc3260.txt>

Differentiated services (DiffServ) [RFC 3260] include enhancements to IP to enable scalable service discrimination. IP packets are classified and marked to receive a particular per-hop forwarding behavior on nodes along their path using the field [DSFIELD]. Network resources are allocated to traffic streams by service provisioning policies which govern how traffic is marked and conditioned upon entry to a differentiated services-capable network, and how that traffic is forwarded within that network.

Keywords: Internet, Integrated Service, QoS, Scalability

1.2.7.3 Integrated Services (IntServ)

URL: <http://www.ietf.org/rfc/rfc1633.txt>, <http://www.ietf.org/rfc/rfc2205.txt>

Integrated Services (IntServ) [RFC 1633] Working Group was setup in response to the growing demand for an Integrated Services Internet defining several service classes that, if supported by the routers, can provide certain QoS commitments for a data flow through a network path. By contrast best-effort traffic entering a router will receive no such service commitment. The level of QoS provided by these enhanced QoS classes is programmable per-flow. Resources can be reserved by network management procedures or using protocols such as Resource reSerVation Protocol (RSVP) [RFC 2205].

Keywords: Internet, Integrated Service, QoS, Reservation, Scalability, network layer

1.2.8 Virtual Private Networking Technologies

1.2.8.1 Layer 3 VPNs

URL: <http://www.ietf.org/html.charters/l3vpn-charter.html>

Extensions to IP-based routing infrastructure to support Virtual Private Networks.

Specific mainstream L3VPN technologies include:

- BGP/MPLS-based IP VPNs (RFC 2547bis),
- IP VPNs using Virtual-Routers (<http://www.ietf.org/internet-drafts/draft-ietf-ppvpn-vpn-vr-03.txt>)
- CE-based VPNs using IPSEC

Keywords:

1.2.8.2 Layer 2 VPNs

URL: <http://www.ietf.org/html.charters/l2vpn-charter.html>

Technologies under definition by the IETF Layer 2 VPN working group and elsewhere such as ATM Forum which include:

- Virtual Private LAN Service (VPLS)

L2 service that emulates LAN across an IP and an MPLS-enabled IP network, allowing standard Ethernet devices communicate with each other as if they were connected to a common LAN segment.

- Virtual Private Wire Service (VPWS)

L2 service that provides L2 point-to-point connectivity (e.g. Frame Relay DLCI, ATM VPI/VCI, point-to-point Ethernet) across an IP and an MPLS-enabled IP network.

- IP-only L2 VPNs

L2 service across an IP and an MPLS-enabled IP network, allowing standard IP devices to communicate with each other as if they were connected to a common LAN segment or a point-to-point circuit.

- LAN-emulation-over-ATM (LANE)

emulates LAN across an ATM-based network.

Keywords:

1.2.8.3 PPTP

URL: <http://www.ietf.org/html.charters/l2vpn-charter.html>

Microsoft, 3Com®, and several other companies have developed the Point-to-Point Tunneling Protocol (PPTP) and Microsoft has extended Windows NT to support it. PPTP and Layer 2 Tunneling Protocol, proposed by Cisco Systems®, are among the most likely proposals as the basis for a new Internet Engineering Task Force(IETF) standard. Generally, there are three computers involved in every PPTP deployment:

- .PPTP client
- Network access server

- PPTP server

A typical deployment of PPTP starts with a remote or mobile PPTP client that needs access to a private enterprise LAN by using a local Internet Service Provider (ISP). The client connects to a network access server (NAS) at the ISP facility using PPP connection. Network access servers are also referred to as front-end processors (FEPs), dial-in servers, or point-of-presence (POP) servers. Once connected, the client can send and receive packets over the Internet or any other network using the TCP/IP protocol. Virtual Private LAN Service (VPLS)

Keywords:

1.2.9 Computer Systems Related Technologies

1.2.9.1 CORBA and CORBA Services

URL: http://www.omg.org/technology/documents/formal/corba_iiop.htm

Although MDA can target every middleware platform and will map to all with significant market buy-in, CORBA® plays a key role as a target platform because of its programming language-, operating system-, and vendor-independence.

Keywords: Computational VP, Widespread usage

1.2.9.2 Web Services

1.2.9.2.1 Web Services Technologies

URL: <http://www.ws-i.org>

The term Web services describes a standardized way of integrating Web-based applications using the XML, SOAP, WSDL and UDDI open standards over an Internet protocol backbone. XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available and UDDI is used for listing what services are available. Used primarily as a means for businesses to communicate with each other and with clients, Web services allow organizations to communicate data without intimate knowledge of each other's IT systems behind the firewall.

Unlike traditional client/server models, such as a Web server/Web page system, Web services do not provide the user with a GUI. Web services instead share business logic, data and processes through a programmatic interface across a network. The applications interface, not the users. Developers can then add the Web service to a GUI (such as a Web page or an executable program) to offer specific functionality to users.

Web services allow different applications from different sources to communicate with each other without time-consuming custom coding, and because all communication is in XML, Web services are not tied to any one operating system or programming language. For example, Java® can talk with Perl, Windows applications can talk with UNIX® applications.

Keywords: Enterprise VP, Computational VP,

1.2.9.2.2 Universal Description, Discovery, and Integration (UDDI)

URL: www.uddi.org

The Universal Description, Discovery, and Integration (UDDI) protocol is one of the major building blocks required for successful Web services. UDDI creates a standard interoperable platform that enables companies and applications to quickly, easily, and dynamically find and use Web services over the Internet. UDDI also allows operational registries to be maintained for different purposes in different contexts. UDDI is a cross-industry effort driven by major platform and software providers, as well as marketplace operators and e-business leaders within the OASIS standards consortium.

Keywords: Computational VP, Limited usage

1.2.9.2.3 XML Protocol/Simple Object Access Protocol (SOAP)

URL: <http://www.w3.org/2000/xml/Group/>

Description: SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses. SOAP can potentially be used in combination with a variety of other protocols; however, the only bindings defined in this document describe how to use SOAP in combination with HTTP and HTTP Extension Framework.

Keywords: Limited usage

1.2.9.2.4 Web Services Description Language (WSDL)

URL: <http://www.w3.org/TR/wsdl>

WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate, however, the only bindings described in this document describe how to use WSDL in conjunction with SOAP 1.1, HTTP GET/POST, and MIME.

Keywords: Computational VP, Limited usage

1.2.9.2.5 Web Services Business Process Execution Language (WS-BPEL)

URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsbpel

The purpose of the Web Services Business Process Execution Language TC is to continue work on the business process language published in the Business Process Execution Language for Web Services (BPEL4WS) specification in August 2002. Continuing the approach and design used in BPEL4WS, the work of the BPEL TC will focus on specifying the common concepts for a business process execution language which form the necessary technical foundation for multiple usage patterns including both the process interface descriptions required for business protocols and executable process models. It is explicitly not a goal of the TC to specify bindings to specific

hardware/software platforms and other mechanisms required for a complete runtime environment for process implementation.

Keywords: Enterprise VP, Computational VP, Limited usage

1.2.9.2.6 Web Services Architecture Including Reliable Messaging

URL: <http://www.w3.org/2002/ws/arch/>

The Web Services Architecture document describes the Web services reference architecture, and where appropriate, identifies candidate technologies that have been determined to meet the functionality requirements defined within the architecture. The Web services reference architecture identifies the functional components, defines the relationships among those components, and establishes a set of constraints upon each to affect the desired properties of the overall architecture.

Keywords: Architectural framework

1.2.9.3 Enterprise Java Beans (EJB)

URL: <http://java.sun.com/j2ee/>

J2EE technology and its component based model simplify enterprise development and deployment. The J2EE platform manages the infrastructure and supports the Web services to enable development of secure, robust and interoperable business applications. The J2EE platform is the foundation technology of the Sun ONE platform and Sun's Web services strategy. Technologies included in J2EE are:

- Java API for XML Processing (JAXP)
- Java API for XML Registries (JAXR)
- Java API for XML-Based Remote Procedure Call (JAX-RPC)
- SOAP with Attachments API for Java (SAAJ)
- Java Message Service (JMS)
- JavaServer Pages
- Java Servlets
- JDBCTM
- J2EE Connector Architecture
- J2EE Deployment Specification
- J2EE Management Specification
- Transactions

Keywords: Enterprise VP, Widespread usage

1.2.9.4 IEEE 1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems

URL: <http://ieee1588.nist.gov>

From the "Scope" section of the standard: "This standard defines a protocol enabling precise synchronization of clocks in measurement and control systems implemented with technologies such as network communication, local computing and distributed objects. The protocol will be applicable to systems communicating by local area networks supporting multicast messaging

including but not limited to Ethernet. The protocol will enable heterogeneous systems that include clocks of various inherent precision, resolution and stability to synchronize. The protocol will support system-wide synchronization accuracy in the sub-microsecond range with minimal network and local clock computing resources. The default behavior of the protocol will allow simple systems to be installed and operated without requiring the administrative attention of users.” It is intended to address time synchronization requirements not met by other technologies such as the Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP). It defines an architecture of time servers and time gateways, some of which may be embedded in networking devices such as switches and routers. Published as IEEE 1588-2002.

Keywords: Protocol, Time synchronization, Multicast, Application layer, Routing, Bridging, Standard

1.2.9.5 GUID

URL: www.opengroup.org

Many utility system use Globally Unique Identifiers (GUIDs) to identify objects, interfaces and their instances. The concept of a GUID was originally conceived by the Open Software Foundation (now called The Open Group) for their Distributed Computing Environment (DCE). The GUID is a unique value in both space and time. It is generated on your development machine by a standard OSF DCE algorithm. It is this DCE algorithm that allows rapid development of COM+ objects without requiring use of namespace partitions. COM+ provides a tool called GUIDGEN that generates a unique GUID based on spatial and temporal information.

Keywords: Widespread usage

1.2.9.6 9834-1 Procedures for the operation of OSI Registration Authorities

URL: http://web.ansi.org/other_services/registration_programs/reg_org.aspx?menuid=10

A registration service provides an unambiguous organization identifier. The service conforms to ITU X.660|ISO/IEC 9834-1, which describes a hierarchy of registration authorities. Information objects are unambiguously identified by constructed names composed of one component from each level of the Registration Authority hierarchy under which the information object is registered. This name is unique, since each component along the path through the hierarchy from the root to the registered object is guaranteed to be unique within the scope of the Registration Authority assigning that name component. The ANSI organization name registration service assigns one name component. ANSI maintains a database that is searched with every new registration request to ensure that duplicate identifiers are never registered.

A formal procedure has been developed within ANSI to administer this process. These procedures specify the syntax of names assigned by this Registration Authority, describe the way in which applications for Organization names are handled, including mechanisms for assuring the assigning of unique names at this level in the hierarchy, and provide for the assignment of Organization names. The procedure is available from the Registration Coordinator

Keywords: Data management

1.2.10 General Internet and De Facto Data Management Technologies

1.2.10.1 Simple Mail Transfer Protocol (SMTP)

URL: <http://www.ietf.org/rfc/rfc0821.txt>

The Simple Mail Transfer Protocol (SMTP) was developed by the IETF for transferring e-mail reliably and efficiently across the Internet. SMTP is independent of the particular transmission subsystem and requires only a reliable ordered data stream channel. An important feature of SMTP is its capability to relay mail across transport service environments. A transport service provides an inter process communication environment (IPCE). An IPCE may cover one network, several networks, or a subset of a network. It is important to realize that transport systems (or IPCEs) are not one-to-one with networks. A process can communicate directly with another process through any mutually known IPCE. Mail is an application or use of inter process communication. Mail can be communicated between processes in different IPCEs by relaying through a process connected to two (or more) IPCEs. More specifically, mail can be relayed between hosts on different transport systems by a host on both transport systems.

Keywords: Mail, Email, Internet, Protocol, Application layer

1.2.10.2 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME

URL: <http://www.ietf.org/rfc/rfc2045.txt>,
<http://www.ietf.org/rfc/rfc2311.txt>

Multipurpose Internet Mail Extensions (MIME) [RFC2045-RFC2049] is a supplementary protocol and an extension to **SMTP**. Originally designed for only e-mail and SMTP as an encoding method for sending non-**ASCII** files through e-mail servers, today MIME has been adopted to also support a way to send non-html documents over the **World Wide Web**. MIME provides a way for non-text information to be encoded as ASCII text. This encoding is known as base64. Web servers now must be configured for MIME types to serve those types of files. Most e-mail clients automatically handle MIME now and the process is transparent to the user.

The Secure/MIME (S/MIME) is an IETF specification [RFC 2311], to send and receive secure MIME data, providing the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption).

Keywords: Security, Mail, E-mail, Encoding, Internet, Protocol, Application layer

1.2.10.3 Post Office Protocol version 3 (POP3)

URL: <http://ietf.org/rfc/rfc1939.txt>

On certain types of smaller nodes in the Internet it is often impractical to maintain a message transport system (MTS). For example, a workstation may not have sufficient resources (cycles, disk space) in order to permit a SMTP server and associated local e-mail delivery system to be kept resident and continuously running. Similarly, it may be expensive (or impossible) to keep a personal computer interconnected to an IP-style network for long amounts of time.

The Post Office Protocol - Version 3 (POP3) is intended to permit a workstation to dynamically access a mail-drop on a server host in a useful fashion. POP3 is not intended to provide extensive manipulation operations of e-mail on the server; normally, e-mail is downloaded and then deleted. A more advanced (and complex) protocol is IMAP4.

POP3 is defined in RFC1939.

Keywords: Mail, Internet, Protocol, Application layer

1.2.10.4 Internet Message Access Protocol version 4 (IMAP4)

URL: <http://ietf.org/rfc/rfc2060.txt>

The Internet Message Access Protocol, Version 4 rev1 (IMAP4) allows a client to access and manipulate electronic e-mail messages on a server. IMAP4 permits manipulation of remote message folders, called "mailboxes", in a way that is functionally equivalent to local mailboxes. IMAP4 also provides the capability for an offline client to resynchronize with the server.

IMAP4 includes operations for creating, deleting, and renaming mailboxes; checking for new messages; permanently removing messages; setting and clearing flags; parsing; searching; and selective fetching of message attributes, texts, and portions thereof. Messages in IMAP4 are accessed by the use of numbers. These numbers are either message sequence numbers or unique identifiers. IMAP4 supports a single server. IMAP4 does not specify a means of posting mail; this function is handled by an e-mail transfer protocol such as SMTP. The IMAP4 protocol assumes a reliable data stream such as provided by TCP.

IMAP4 is defined in RFC2060.

Keywords: Mail, E-mail, Internet, Protocol, Application layer

1.2.10.5 ANSI/ISO/IEC 8632-1, 2, 3, 4 - Computer Graphics Metafile (CGM)

URL: <http://web.ansi.org/default.asp>

The Computer Graphics Metafile (CGM) standard is used in printing and graphics art applications that are either developed or acquired for government use. It is strongly recommended when one or more of the following situations exist. Graphics metafile is maintained at a central facility for a decentralized system that employs graphics devices of different makes and models that must utilize the data. Graphics metafile is required to preserve picture data when conversion or migration from one graphics system to another is necessary and the two systems are not necessarily compatible. Graphics metafile is intended for information interchange between a source system and a target system that are not necessarily compatible.

CGM provides portability of graphics data among different software systems, graphical devices, and computer graphics installations. Data interchange standard that defines a neutral computer-interpretable representation of 2D graphical (pictorial) information in a manner that is independent from any particular application or system.

The four parts of the standard are: Part 1, Functional specification; Part 2, Character encoding; Part 3, Binary encoding; and Part 4, Clear text encoding.

Keywords: Graphics, Metafile

1.2.10.6 ISO/IEC 11179 Parts 1 - 6 Metadata Registries

URL: <http://metadata-stds.org/11179/>

Humans are aware of things or ideas that exist through their properties. Data represents the properties of these things or ideas. A data element is the construct by which we consider the thing or idea, one of its properties, and the possible representations of the property as data. A value domain specifies how a data element is represented, i.e., is the set of allowed values for that data element. Specification of data elements, value domains, and related data entities involves documenting relevant characteristics of each. Data that has been carefully specified greatly enhances its usefulness and shareability across systems and organizations. Sharing data involves the ability to locate and retrieve desired data and to exchange the data with others. When data elements and value domains are well documented according to ISO/IEC 11179 and the documentation is managed in a metadata registry (MDR), finding and retrieving them from disparate databases as well as sending and receiving them via electronic communications are made easier.

The documentation and harmonization of data elements used in communications through automated information processing systems is an ongoing and essential activity. The success of this activity and its application throughout the world is of vital importance if international communications among governments, businesses, and scientific communities are to be improved. The primary data sharing and harmonization problems addressed by the development of ISO/IEC 11179 include, but are not limited to the following:

- There is a lack of mechanisms for enabling global data acquisition and interchange, particularly across application areas;
- Unique global identifiers for data elements and value domains currently do not exist;
- Documentation of data element characteristics is inadequate to support fully automated sharing of data, including locating, retrieving, and exchanging the data;
- There is a lack of uniform guidance for identification, development, and description of data elements and value domains;
- Finding and retrieving a specific data element or value domain among thousands or millions is difficult or impossible;
- No universal means for organizing data elements and value domains exists;
- While data is sometimes standardized within an organization, there are few common data standards between organizations;
- Exchange of data among organizations results in a proliferation of customized data interchange representations;
- Data definitions and descriptions are not sufficiently precise to support reuse or multiple users of data;
- Current inventory structures for reducing logical data redundancies are inadequate;
- Global implementation of electronic data interchange including the use of XML (eXtensible Markup Language) is impeded by a lack of well-specified data elements and value domains.

The six parts are:

- **Part 1: Framework**, introduces and discusses fundamental ideas of data elements, value domains, data element concepts, conceptual domains, and classification schemes essential to the understanding of this set of standards and provides the context for associating the individual parts of ISO/IEC 11179.
- **Part 2: Classification**, provides a conceptual model for managing classification schemes. There are many structures used to organize classification schemes and there are many subject matter areas that classification schemes describe. So, this Part also provides a two-faceted classification for classification schemes themselves.
- **Part 3: Registry Metamodel and Basic Attributes**, specifies a conceptual model for a metadata registry. It is limited to a set of basic attributes for data elements, data element concepts, value domains, conceptual domains, classification schemes, and other related classes, called administered items. The basic attributes specified for data elements in ISO/IEC 11179-3:1994 are provided in this revision.
- **Part 4: Formulation of Data Definitions**, provides guidance on how to develop unambiguous data definitions. A number of specific rules and guidelines are presented in ISO/IEC 11179-4 that specify exactly how a data definition should be formed. A precise, well-formed definition is one of the most critical requirements for shared understanding of an administered item; well-formed definitions are imperative for the exchange of information. Only if every user has a common and exact understanding of the data item can it be exchanged trouble-free.
- **Part 5: Naming and Identification Principles**, provides guidance for the identification of administered items. Identification is a broad term for designating, or identifying, a

particular data item. Identification can be accomplished in various ways, depending upon the use of the identifier. Identification includes the assignment of numerical identifiers that have no inherent meanings to humans; icons (graphic symbols to which meaning has been assigned); and names with embedded meaning, usually for human understanding, that are associated with the data item's definition and value domain.

- **Part 6: Registration**, provides instruction on how a registration applicant may register a data item with a central Registration Authority and the allocation of unique identifiers for each data item. Maintenance of administered items already registered is also specified in this document.

Keywords: Widespread usage

1.2.10.7 Meta Object Facility (MOF)

URL: <http://www.omg.org/mof/>

MOF defines the common meta-model for all of Object Management Group (OMG)'s modeling specifications. Thus, the MOF allows derived specifications to work together in a natural way. The MOF also defines a standard repository for meta-models and, therefore, models (since a meta-model is just a special case of a model).

Keywords:

1.2.10.8 XML Metadata Interchange (XMI)

URL: <http://www.omg.org/xmi/>

XMI defines an XML-based interchange format for UML metamodels and models (since a metamodel is just a special case of a model), by standardizing XML document formats and DTDs. In so doing, it also defines a mapping from UML to XML.

Keywords:

1.2.10.9 Common Warehouse Model (CWM)

URL: <http://www.omg.org/cwm/>

The CWM standardizes a complete, comprehensive metamodel that enables data mining across database boundaries at an enterprise and goes well beyond. Like a UML profile but in data space instead of application space, it forms the MDA mapping to database schemas. The product of a cooperative effort between OMG and the Meta-Data Coalition (MDC), the CWM does for data modeling what UML does for application modeling.

Keywords:

1.2.10.10 American Standard Code for Information Interchange (ASCII)

URL: <http://nvl.nist.gov/pub/nistpubs/sp958-lide/172-173.pdf>

A code for information exchange between computers made by different companies; a string of 7 binary digits represents each character; used in most microcomputers

Keywords: Widespread usage

1.2.10.11 Hypertext Markup Language (HTML)

URL: <http://www.w3.org/MarkUp/>

The coding language used to create Hypertext documents for use on the World Wide Web. HTML looks a lot like old-fashioned typesetting code, where you surround a block of text with codes that indicate how it should appear. The "hyper" in Hypertext comes from the fact that in HTML you can specify that a block of text, or an image, be linked to another file on the Internet. HTML files are meant to be viewed using a "Web Browser". HTML is loosely based on a more comprehensive system for markup called SGML.

Keywords: Widespread usage

1.2.10.12 eXtensible Markup Language (XML)

URL: <http://www.w3.org/XML/>

The eXtensible Markup Language (XML) is an application profile or restricted form of SGML, and has become a very widely used system for defining data formats. Its goal is to enable generic SGML to be served, received, and processed on the Web in the way that is now possible with HTML. XML has been designed for ease of implementation and for interoperability with both SGML and HTML.

It is called extensible because it is not a fixed format like HTML (a single, predefined markup language). Instead, XML is actually a 'meta-language' - a language for describing other languages - that allows for the design of customized markup languages for limitless different types of documents.

XML is defined by W3C at W3C: eXtensible Markup Language (XML). The base specifications are XML 1.0, and Namespaces.

XML describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them. By construction, XML documents are conforming SGML documents. XML documents are made up of storage units called entities, which contain either parsed or unparsed data. Parsed data is made up of characters, some of which form character data, and some of which form markup. Markup encodes a description of the document's storage layout and logical structure. XML provides a mechanism to impose constraints on the storage layout and logical structure.

XML provides a very rich system to define complex documents and data structures such as invoices, molecular data, news feeds, glossaries, inventory descriptions, real estate properties, etc. As long as a programmer has the XML definition for a collection of data (often called a "schema") then they can create a program to reliably process any data formatted according to those rules.

A number of technologies and initiatives are being created around or using XML, some of them include; **XHTML**, **CSS**, **XSL**, **DOM**, **SOAP**, **UDDI**, **WSDL**, **ebXML**, and **BizTalk**.

Keywords: Widespread usage

1.2.10.13 RDF

URL: <http://www.w3.org/RDF/>

RDF is a basic language for writing metadata using XML; a foundation that provides a robust flexible architecture for processing metadata on the Internet. RDF will retain the capability to exchange metadata between application communities, while allowing each community to define and use the metadata that best serves their needs

Keywords: Limited usage

1.2.10.14 XML Schema (xIs)

URL: http://www.w3schools.com/schema/schema_intro.asp

XML Schemas are used to create metadata models using XML as the formal for describing the data attributes. The purpose of an XML Schema is to use XML to define the legal building blocks of an XML document, just like a DTD.

An XML Schema:

- defines elements that can appear in a document
- defines attributes that can appear in a document
- defines which elements are child elements
- defines the order of child elements
- defines the number of child elements
- defines whether an element is empty or can include text
- defines data types for elements and attributes
- defines default and fixed values for elements and attributes

XML Schemas express shared vocabularies and allow machines to carry out rules made by people. They provide a means for defining the structure, content and semantics of XML documents.

Keywords: Widespread usage

1.2.10.15 XPath

URL: <http://www.w3.org/TR/xpath>

XPath, a language for selecting an XML document's parts, lets you treat an XML document like a file system. XPath queries start with a current element or attribute (much like a current directory within a file system) and let you specify other nodes relative to your location.

Keywords: Widespread usage

1.2.10.16 XSLT

URL: <http://www.w3.org/Style/XSL/>

XSLT (Extensible Stylesheet Language Transformations) converts any XML document into another XML, HTML, or plaintext document. Some developers find XSLT difficult to grasp because it is a rule-based language, not primarily a procedural or object-based language (although with effort you can make it work in a procedural way). With XSLT, you specify a set of rules—called templates—that describe how the output document should be created

Keywords: Widespread usage

1.2.10.17 XQuery

URL: <http://www.w3.org/XML/Query>

This document proposes a query language syntax for XML documents, called XQuery. Such a query language has quite different requirements than traditional languages; much more different than is commonly appreciated. Many past proposals have taken a basically relational query language (typically SQL), and modified it by the addition of a few constructs: typically a "contains" operator and some features for matching strings within text chunks against regular expressions, or against word-roots. Such features, while needed, are not enough. The hard problem arises because the most basic design principles of relational databases, do not hold for XML documents.

Keywords: Computational VP, Limited usage

1.2.10.18 ANSI/ISO/IEC 9075 - Structured Query Language (SQL)

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=26196&ICS1=35&ICS2=60&ICS3=>

Structured Query Language (SQL) is widely recognized as the most portable way of requesting information from relational databases, and is used as one of the main access routes for all such databases, and for certain classes of object oriented databases.

The scope of the SQL language is the definition of data structure and the operations on data stored in that structure. Parts 1, 2 and 11 encompass the minimum requirements of the language. Others parts define extensions.

ISO/IEC 9075-14:2003 defines ways in which Database Language SQL can be used in conjunction with XML. It defines ways of importing and storing XML data in an SQL database, manipulating it within the database and publishing both XML and conventional SQL-data in XML form.

Keywords: Widespread usage

1.2.11 eCommerce Related Data Management Technologies

1.2.11.1 Universal Business Language (UBL)

URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ubl

The purpose of the UBL Technical Committee is to develop a standard library of XML business documents (purchase orders, invoices, etc.) by modifying an already existing library of XML

schemas to incorporate the best features of other existing XML business libraries. The TC will then design a mechanism for the generation of context-specific business schemas through the application of transformation rules to the common UBL source library.

Keywords: Limited usage

1.2.11.2 ebXML

1.2.11.2.1 ebXML

URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-iic

ebXML (Electronic Business XML) is a project to use the Extensible Markup Language (XML) to standardize the secure exchange of business data. Among other purposes, ebXML would encompass and perhaps replace a familiar standard called Electronic Data Interchange (EDI). ebXML is designed to enable a global electronic marketplace in which enterprises of any size, and in any location, could safely and securely transact business through the exchange of XML-based messages. The United Nations body for Trade Facilitation and Electronic Business Information Standards (UN/CEFACT) and the Organization for the Advancement of Structured Information Standards (OASIS) launched the project as a joint initiative. Its membership includes 75 companies, including major IT vendors and trade associations throughout the world.

Because ebXML relies on the Internet's existing standards such as HTTP, TCP/IP, MIME, SMTP, FTP, UML, and XML, it can be implemented and deployed on virtually any computing platform. The use of existing standards gives ebXML the advantage of being relatively inexpensive and easy to use.

Keywords: Enterprise VP, Computational VP, Limited usage

1.2.11.2.2 ebXML Collaboration Protocol Profiles (CPPA)

URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-cppa

Collaboration Protocol Profiles (CPPs) and Collaboration Protocol Agreements (CPAs), define a business partner's technical capabilities to engage in electronic business collaborations with other partners, and the technical agreement between two (or more) partners to engage in electronic business collaboration.

Keywords: Enterprise VP, Limited usage

1.2.11.2.3 ebXML Messaging

URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-msg

ebXML Messaging provides technology for the transport, routing and packaging of business transactions using Internet technologies.

Keywords: Limited usage

1.2.11.2.4 ebXML Registry

URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=regrep

ebXML Registries is intended to include one or more specifications for interoperable registries and repositories for SGML- and XML-related entities.

Keywords: Limited usage

1.2.11.3 ISO/IEC JTC 1 SC32 - ISO/IEC 15944-1:2002 Information technology -- Business agreement semantic descriptive techniques -- Part 1: Operational aspects of Open-EDI for implementation

URL: http://www.iso.ch/iso/en/ittf/PubliclyAvailableStandards/c033322_ISO_IEC_15944-1_2002%28E%29.zip

Standardization in the field of generic information technology standards for open electronic data interchange needed to attain global interoperability among the information technology systems used by organizations. Such interoperability is viewed from both business and information technology perspectives. Within this context the scope includes: 1 methodology and framework for identification and modeling of business activities through business scenarios and their components, such as roles, information bundles, and semantic components; 2 identification and specification of formal description techniques for describing classes of business requirements and their contextual and semantic specifications; 3 identification and specification of formal description techniques for developing business scenarios and their components; 4 identification and specification of information technology services and service interfaces for accomplishing business transactions; 5 identification and specification of facilities to manage business scenarios and their.

Keywords: Computational VP, Widespread usage

1.2.11.4 EAN.UCC Identification Numbers

URL: <http://www.ean-int.org/index800.html>

EAN.UCC ID's are unique : a world wide unique number is allocated. They are non-significant : the EAN.UCC identification number in itself is the key to access a database, which contains precise information on the unit. They are multi-industry and international: their non-significance enables their use in all sectors, and their uniqueness permits their use across borders. They are secure : EAN.UCC identification numbers include a check digit for secure data capture.

Keywords: Widespread usage

1.2.11.5 EAN.UCC Universal Bar Codes

URL: <http://www.ean-int.org/index800.html>

UPC - The Universal Product Code (UPC) barcode has been used in the retail industry in the US and Canada since 1973. UCC-12 is another name for the UPC-A standard. UPC-A consists of 12 numbers and UPC-E consists of 12 numbers that are compressed into 8 numbers for small packages.

UCC - The Universal Code Council creates standards for multi-industry product identification. UCC12 is another name for the UPC-A standard.

EAN - The European Article Numbering System (EAN) is a superset of U.P.C. EAN-13 consists of 13 numbers and EAN-8 consists of 8 digits for small packages. EAN14 is a different barcode type created with ITF or Code 128.

ISBN and Bookland - The EAN-13 barcode for a book or periodical is generated from the ISBN number assigned to it. When encoding ISBN in an EAN-13 barcode, the ISBN number is preceded by the number 978 and the ISBN check digit is not used. When the ISBN number is encoded in the EAN-13 barcode in this way it is often called Bookland. A 5 digit add-on barcode is optional and can contain the price of the book or periodical.

ISSN - is a standard for encoding data in an EAN13 barcode. When encoding ISSN in an EAN-13 barcode, the ISSN number is preceded by the number 977 and the ISSN check digit is not used. A two digit number, usually the number "00" (a 2 digit price code) is added to the end, and then the normal EAN check digit is added. Periodicals may have a two digit add on representing the issue number.

JAN - codes are the same as the EAN13 codes, except the first two characters are set to "49".

Add-on Barcodes - an additional barcode can be created just to the right of the symbol to encode additional information. These barcodes are either 2 or 5 digits in length.

EAN-14 is a barcode type created with ITF or Code 128.

UCC128 or EAN128 is a barcode type created with Code 128.

Barcodes are assigned in the US by: <http://www.uc-council.org/>

Keywords: Widespread usage

1.2.11.6 10303 Standard Exchange for Product Data (STEP)

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=20579&ICS1=25&ICS2=40 &ICS3=40>

STEP provides a representation of product information along with the necessary mechanisms and definitions to enable product data to be exchanged. It applies to the representation of product information, including components and assemblies; the exchange of product data, including storing, transferring, accessing, and archiving. STEP is being developed by a broad range of industries to provide extensive support for modeling, automated storage schema generation, life-cycle support, plus many more data management facilities.

Keywords: Computational VP, Widespread usage

1.3 Security Technologies

1.3.1 Policy and Framework Related Technologies

The following technologies are recommended to be part of the policy establishment process.

1.3.1.1 ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management

URL: <http://www.iso.ch>

Establishes user requirements for the service definition needed to support the security audit trail reporting function, defines the service provided by the security audit trail reporting function, specifies the protocol that is necessary in order to provide the service, defines the relationship between the service and management notifications, defines relationships with other systems management functions, specifies conformance requirements.

Keywords: Security, Audit, Non-Repudiation

1.3.1.2 ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework

URL: <http://www.iso.ch>

1. identifies the objective of a time-stamping authority;
2. describes a general model on which time-stamping services are based;
3. defines time-stamping services;
4. defines the basic protocols of time-stamping;
5. specifies the protocols between the involved entities.

Keywords: Audit, Non-Repudiation, Security, time-stamp

1.3.1.3 ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems

URL: <http://www.iso.ch>

Provides guidance to the creation of a robust audit and alarming framework that is critical for intrusion detection.

Keywords: Audit, Non-Repudiation, Security

1.3.1.4 FIPS PUB 112 Password Usage

URL: <http://www.itl.nist.gov/fipspubs/fip112.htm>
<http://csrc.nist.gov/publications/fips/fips112/fip112-2.pdf>

The document specifies basic security criteria for two different uses of passwords in an ADP (Automated Data Processing) system, (1) personal identity authentication and (2) data access authorization. It establishes the basic criteria for the design, implementation and use of a password system in those systems where passwords are used. It identifies fundamental ADP management functions pertaining to passwords and specifies some user actions required to satisfy these functions. In addition, it specifies several technical features that may be implemented in an ADP system in order to support a password system. An implementation schedule is established for compliance with the Standard. Numerous guidelines are provided in the Appendices for managers and users seeking to comply with the Standard.

Although dated 1985 (hence the use of the obsolete term ADP), this is an excellent discussion of passwords.

Keywords: Identity Establishment, Policy, Authorization for Access Control, Credential Renewal, Security

1.3.1.5 FIPS PUB 113 Computer Data Authentication

URL: [http:// http://www.itl.nist.gov/fipspubs/fip113.htm](http://http://www.itl.nist.gov/fipspubs/fip113.htm)
<http://www.dice.ucl.ac.be/crypto/standards/fips/fips113/fip113.pdf>

This publication specifies a standard to be used by Federal organizations that require that the integrity of computer data be cryptographically authenticated. In addition, it may be used by any organization whenever cryptographic authentication is desired. Cryptographic authentication of data during transmission between electronic components or while in storage is necessary to maintain the integrity of the information represented by the data. The standard specifies a cryptographic authentication algorithm for use in ADP (Automated Data Processing) systems and networks. The authentication algorithm makes use of the Data Encryption Standard (DES) cryptographic algorithm as defined in Federal Information Processing Standard 46 (FIPS PUB 46).

Keywords: Keywords Information Integrity, Confidentiality, Privacy, Authorization for Access Control, Setting and Verifying User Authorization, Encryption, Spoof, Security

1.3.1.6 RFC 2196 Site Security Handbook

URL: [http:// http://www.ietf.org/rfc/rfc2196.txt](http://http://www.ietf.org/rfc/rfc2196.txt)

This handbook is a guide to developing computer security policies and procedures for sites that have systems on the Internet. The purpose of this handbook is to provide practical guidance to administrators trying to secure their information and services. The subjects covered include policy content and formation, a broad range of technical system and network security topics, and security incident response.

Keywords: Keywords Policy, Security

1.3.1.7 RFC 2401 Security Architecture for the Internet Protocol

URL: <http://www.ietf.org/rfc/rfc2401.txt>

This memo specifies the base architecture for IPsec compliant systems. The goal of the architecture is to provide various security services for traffic at the IP layer, in both the IPv4 and IPv6 environments. This document describes the goals of such systems, their components and how they fit together with each other and into the IP environment. It also describes the security services offered by the IPsec protocols, and how these services can be employed in the IP environment. This document does not address all aspects of IPsec architecture.

Keywords: Keywords Policy, Security, Encryption, Path Routing and QOS, Confidentiality, Encryption, Security

1.3.1.8 RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

URL: <http://www.ietf.org/rfc/rfc2527.txt>

The purpose of this document is to establish a clear relationship between certificate policies and CPSs, and to present a framework to assist the writers of certificate policies or CPSs with their

tasks. In particular, the framework identifies the elements that may need to be considered in formulating a certificate policy or a CPS. The purpose is not to define particular certificate policies or CPSs, per se.

Keywords: Keywords Policy, Identity Establishment, Identity Mapping, Credential Renewal, Spoof, Security

1.3.2 General Security Technologies

1.3.2.1 PKI - Public Key Infrastructure (X.509)

URL: <http://www.ietf.org/rfc/rfc2459.txt>
<http://www.ietf.org/rfc/rfc2587.txt>
<http://www.ietf.org/rfc/rfc3039.txt>
<http://www.ietf.org/rfc/rfc3161.txt>
<http://www.ietf.org/rfc/rfc2585.txt>

The PKIX working group develops Internet standards to support X.509-based Public Key Infrastructure (PKI). X.509 is an ITU-T or ISO/IEC/ITU standard certificate format. PKIX has produced documents such as, RFC 2459, which profiled X.509 version 3 certificates and version 2 CRLs for use in the Internet, RFC 2587 on LDAP v2 for certificate and CRL storage, and RFC 3039 on the Public Key Infrastructure Qualified Certificates Profile. The Time-Stamp Protocol (RFC 3161), Certificate Management Messages over CMS (RFC 2797), and the use of FTP and HTTP for transport of PKI operations (RFC 2585) are representative of the expanded scope of PKIX, as these are not profiles of ITU PKI, but new protocols developed in the working group.

Keywords: Internet, Security, Protocol, PKI, authentication

1.3.2.2 Kerberos

URL: <http://www.ietf.org/rfc/rfc1510.txt>
<http://www.ietf.org/rfc/rfc2400.txt>

Kerberos network authentication system [RFC 1510] verifies the identities of principals, (e.g., a workstation user or a server) on an open (unprotected) network. Kerberos performs authentication as a trusted third-party authentication service by using conventional cryptography. Currently the Kerberos working group is working on improving the interoperability of these systems while improving security. The working group on Kerberized Internet Negotiation of Keys facilitates centralized key management for IPsec security associations as defined in RFC 2400. Participating systems will use the Kerberos architecture as defined in RFC 1510 (and its successors) for key management.

Keywords: Security, authentication.

1.3.2.3 FIPS 140-2 Security Requirements for Cryptographic Modules

URL: <http://csrc.nist.gov/cryptval/140-2.htm>
<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

Accredited Cryptographic Modules Testing (CMT) laboratories perform validation testing of cryptographic modules: devices that perform encryption, decryption, authentication etc. Cryptographic modules are tested against requirements found in FIPS PUB 140-2, Security Requirements for Cryptographic Modules [PDF]. These security requirements cover 11 areas related to the design and implementation of a cryptographic module. Within most areas, a cryptographic module receives a security level rating (1-4, from lowest to highest), depending on what requirements are met. For instance, a lower rating may indicate that a device will show evidence that it has been tampered with, while a higher rating may indicate the device is resistant to tampering. For other areas that do not provide for different levels of security, a cryptographic module receives a rating that reflects fulfillment of all of the requirements for that area.

Keywords: security, physical layer, standard, encryption

1.3.2.4 FIPS 197 for Advanced Encryption Standard (AES)

URL: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. AES replaces the earlier DES and is intended to be less processor-intensive to implement in software.

Keywords: Security, Standard, Encryption,

1.3.2.5 Role-Based Access Control

URL: <http://csrc.nist.gov/rbac/>

One of the most challenging problems in managing large networked systems is the complexity of security administration. Today, security administration is costly and prone to error because administrators usually specify access control lists for each user on the system individually. Role based access control (RBAC) is a technology that is attracting increasing attention, particularly for commercial applications, because of its potential for reducing the complexity and cost of security administration in large networked applications. Since the publication of the Ferraiolo-Kuhn model for RBAC in 1992, most information technology vendors have incorporated RBAC into their product line, and the technology is finding applications in areas ranging from health care to defense, in addition to the mainstream commerce systems for which it was designed.

With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs, and assigning employees to the proper roles. Complexities introduced by mutually exclusive roles or role hierarchies are handled by the RBAC software, making security administration easier.

Keywords: Security, data management, user interface, transaction management, security analysis, proposed standard, computer industry

1.3.2.6 PKCS

URL: <http://www.rsa.com/>

The Public-Key Cryptography Standards (PKCS) is a set of standards for public-key cryptography, developed by RSA Laboratories in cooperation with an informal consortium, originally including Apple®, Microsoft, DEC, Lotus®, Sun and MIT. PKCS has been cited by the OIW (OSI Implementers' Workshop) as a method for implementation of OSI standards. PKCS is compatible with PEM but extends beyond PEM. For example, where PEM can only handle ASCII data, PKCS is designed for binary data as well. PKCS is also compatible with the ITU-T X.509 standard. The published standards are PKCS #1, #3, #5, #6, #7, #8, #9, #10, and #11

Keywords: Security, PKI, PEM

1.3.2.7 FIPS 186 Digital Signatures Standard (DSS)

URL: [FIPS 186 - \(DSS\), Digital Signature Standard](#)

A Digital Signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

Keywords: Authentication, Non-repudiation

1.3.2.8 Intrusion Detection Technologies

URL: [No specific](#)

There are no authoritative technologies that are available today. However, the closest is the Communication in the Common Intrusion Detection Framework (CDIF). The developing specification is available from:

<http://gost.isi.edu/cidf/drafts/communication.txt>

The following are key attributes of an integrated intrusion detection technology/framework:

- A detection framework must be able to communicate over the wire in a standardized manner.
- An intrusion detection technology must be able to securely contact the proper peer components.

There must be a mechanism to locate peer components in a secure manner.

There must be a mechanism for verifying each partner's authenticity and access privileges.

- Additionally, an intrusion detection technology should integrate with the audit framework/technology.

Keywords:

1.3.2.9 Intrusion Prevention Systems (IPS)

URL: [No Specific](#)

Traditionally, firewalls and anti-virus programs try to block attacks, and intrusion detection systems (IDSs) identify attacks as they occur. Such techniques are crucial to network security, but have limitations. A firewall can stop attacks by blocking certain port numbers, but it does little to analyze traffic that uses allowed port numbers. IDSs can monitor and analyze traffic that passes through open ports, but do not prevent attacks.

Keywords: Firewall, Intrusion detection

1.3.2.10 Service Level Agreements (SLA)

URL: [No Specific](#)

A service level agreement (SLA) is a contract between a network service provider and a customer that specifies, usually in measurable terms, what services the network service provider will furnish, and what performance levels will be met by these services. A network service provider may be an external company or another department within the customer's company. Some metrics that SLAs may specify include:

- What percentage of the time services will be available
- The number of users that can be served simultaneously
- Specific performance benchmarks to which actual performance will be compared, such as available bandwidth, average and peak response times, number and duration of permanent and temporary failures, mean time to repair/correct a failure, percent of messages lost or requiring retransmission, etc.
- The schedule for notification in advance of network changes that may affect users
- Help desk response time for various classes of problems and areas of expertise
- Dial-in access availability
- Usage statistics that will be provided

Advantages/Strengths

SLAs are beneficial to both user and provider, and should be negotiated as part of the original agreement. Otherwise, the user may not know exactly what the provider is promising, and may have false expectations, leading to dissatisfaction with the provider. At the same time, the provider must understand the user's expectations so that these can be priced fairly, and possibly negotiated to a mutually satisfactory level. Sometimes providers will want to establish a "base line" period where SLAs are measured and then negotiated. In many cases, this request is reasonable, especially if provider has little to no understanding of a specific environment and the implication of performance requirements.

Disadvantages/Weaknesses

However, if SLAs are agreed to after a provider is already providing the service, the users are in a weaker position to require the needed performance, unless they can easily and inexpensively find and contract with an alternative provider.

Keywords: Security policy

1.3.3 Media and Network Layer Technologies

1.3.3.1 Secure IP Architecture (IPSec)

URL: <http://www.ietf.org/rfc/rfc2401.txt>

IPSec [RFC2401], developed by the IETF Security Area, is designed to provide interoperable, cryptographically based network layer security for IPv4 and IPv6. The set of security services, provided at the IP layer, includes access control, connectionless integrity, data origin authentication, protection against replays, confidentiality (encryption), and limited traffic flow confidentiality. These are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols. The set of IPsec protocols employed in any context, and the ways in which they are employed, will be determined by the security and system requirements of users, applications, and sites/organizations. These mechanisms are designed to be algorithm-independent, which permits selection of different sets of algorithms without affecting the other parts of the implementation. A standard set of default algorithms is specified to facilitate interoperability.

Keywords: Internet, Security, network layer, Protocol, access control, integrity, authentication, confidentiality

1.3.3.2 IEEE 802.11i Security for Wireless Networks (WPA2)

URL: <http://standards.ieee.org/reading/ieee/std/lanman/drafts/P802.11i.pdf>

The IEEE 802.11i protocol is the update to 802.11 security that includes all of the interim measures found in WPA (Wi-Fi Protected Access), and also adds a longer, strong encryption key using AES and fast handoff through quick reauthentication among access points.

Keywords: Keywords Confidentiality, Policy, Authorization for Access Control, Encryption, Security

1.3.3.3 Remote Authentication Dial In User Service (RADIUS)

URL: <http://www.ietf.org/rfc/rfc2865.txt>

The RADIUS authentication protocol [RFC 2865] carries authentication, authorization, and configuration information between a Network Access Server (Client of RADIUS), which needs to authenticate its links and a shared RADIUS Authentication Server. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information. A RADIUS proxy may act as a server to one or more RADIUS authentication clients, while simultaneously acting as an authentication client to one or more authentication servers.

Keywords: Security, authentication, authorization

1.3.3.4 ATM Security

URL: <http://www.ietf.org/rfc/rfc2684.txt>

ATM Forum has specified procedures to provide security for user plane, control plane and services [af-sec-0100.002]. The goals of the specification are to define an infrastructure that: (i) support multiple algorithms and key lengths, (ii) provides interoperability between those who support the specification, (iii) provides the ability to negotiate new algorithms, (iv) maintains compatibility with devices that do not support security, (v) is scalable to large number of users, (vi) separates authentication and integrity from confidentiality.

The primary mechanism for accomplishing this is through protocol encapsulation, which is the RFC that has been referenced.

Keywords: Confidentiality, Eavesdropping, Security

1.3.3.5 AGA-12 Cryptographic Protection of SCADA Communications General Recommendations

URL: <http://www.aga.org>

The American Gas Association (AGA) represents almost 200 local utilities that deliver natural gas to homes in the USA. These utilities are part of the critical infrastructure and rely on SCADA networks to control the operations. AGA, in conjunction with the Gas Technology Institute (GTI) and other industry groups, created AGA 12 to develop cyber security standards and protocols for the industry.

AGA 12 has taken a unique approach to focus on securing the communications link between field devices and the control servers or control center. While there certainly is a risk of data insertion and modification in the communication channel, it may not be the most likely or even easiest avenue of attack on a SCADA system.

The first Technical Report, TR-1, defines an add-on encryption module that also could be integrated into an RTU or PLC. Oddly enough, the most recent version includes significantly less technical detail and removed the SCADA Link Security (SLS) protocol defined in Appendix K. If you are interested in AGA 12, Digital Bond recommends you look at Appendix K of the March 2003 version. Note: hit cancel when the login request appears and the document will load.

The big hole in TR-1 is key management, which is to be addressed at a later date. This is a significant issue given the number of encryptors that would be deployed in a SCADA system. Until key management is addressed AGA 12-1 encryptors can be considered a proof of concept solution at best.

The best news on the AGA 12 front is sample implementation code exists. Andrew Wright of Cisco's Critical Infrastructure Assurance Group (CIAG) has written and documented the code. There are also good technical papers on the security of the protocol available through Andrew's ScadaSafe site.

Keywords: Confidentiality, Authorization for Access Control, Policy, Eavesdropping, Security

1.3.4 Transport Layer Security Technologies

1.3.4.1 Transport Layer Security (TLS)/Secure Sockets Layer (SSL)

URL: <http://www.ietf.org/rfc/rfc2246.txt>

The Transport Layer Security (TLS) [RFC 2246] is based on Secure Socket Layer (SSL) protocol ["The SSL 3.0 Protocol", Netscape Communications Corp., Nov 18, 1996.]. TLS/SSL provides privacy and data integrity between two communicating applications. TLS is application protocol independent.

SSL is a Public Key Infrastructure (PKI) based protocol used for authenticated and encrypted communication between clients and servers. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

The SSL protocol runs above **TCP/IP** and below higher-level protocols such as **HTTP** or **IMAP**. It uses **TCP/IP** on behalf of the higher-level protocols, and in the process allows an SSL-enabled server to authenticate itself to an SSL-enabled client, allows the client to authenticate itself to the server, and allows both machines to establish an encrypted connection. SSL has recently been succeeded by **Transport Layer Security (TLS)**, which is based on SSLv3, but is not interoperable with SSL.

The TLS protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol, on top of some reliable transport protocol (e.g., TCP), provides security with private and reliable connection. The TLS Handshake Protocol provides connection security such that (i) The peer's identity can be authenticated using asymmetric, or public key, cryptography, (ii) The negotiation of a shared secret is secure: the negotiated secret is unavailable to eavesdroppers, and (iii) The negotiation is reliable: no attacker can modify the negotiation communication without being detected by the parties to the communication.

Keywords: Internet, Security, Protocol, transport layer, Integrity, Confidentiality

1.3.5 Application Layer Security Technologies

1.3.5.1 RFC 2228 FTP Security Extensions

URL: <http://www.ietf.org/rfc/rfc2228.txt>

This document defines extensions to the FTP specification STD 9, RFC 959, "FILE TRANSFER PROTOCOL (FTP)" (October 1985). These extensions provide strong authentication, integrity, and confidentiality on both the control and data channels with the introduction of new optional commands, replies, and file transfer encodings.

Keywords: Keywords Encryption, Authorization for Access Control, Integrity, Confidentiality, Security

1.3.5.2 Internet Mail Extensions

URL: <http://www.ietf.org/rfc/rfc2045.txt>
<http://www.ietf.org/rfc/rfc1040.txt>

<http://www.ietf.org/rfc/rfc1423.txt>
<http://www.ietf.org/rfc/rfc2505.txt>

Multipurpose Internet Mail Extensions (MIME) [RFC2045-RFC2049] extends the format of Internet mail to allow non-US ASCII textual messages, non-textual messages, multi-part message bodies, and non-US ASCII information in the headers. The Secure/MIME (S/MIME) working group is developing specifications, e.g., [RFC 2311], to send and receive secure MIME data, providing the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption).

Keywords: Confidentiality, Authorization for Access Control, Policy, Spoof, Eavesdropping, Security

1.3.5.3 RFC 2086 IMAP4 ACL extension

URL: <http://www.ietf.org/rfc/rfc2086.txt>

Provides Access Control List (ACL) ability to IMAP applications.

Keywords: Keywords Authorization for Access Control, Setting and Verifying User Accounts, Policy, Un-authorized access, Security

1.3.5.4 SNMP Security

URL: <http://www.ietf.org/rfc/rfc1351.txt>
<http://www.ietf.org/rfc/rfc3411.txt>
<http://www.ietf.org/rfc/rfc3414.txt>

Provides administrative models, access control lists, and user based (e.g. role based) models that should be used when deploying SNMP.

Keywords: Keywords Authorization for Access Control, Setting and Verifying User Accounts, Policy, Un-authorized access, Security

1.3.5.5 RFC 1305 Network Time Protocol (Version 3) Specification, Implementation

URL: <http://www.ietf.org/rfc/rfc1305.txt>

This document describes Version 3 of the Network Time Protocol (NTP). It supersedes Version 2 of the protocol described in RFC-1119 dated September 1989. However, it neither changes the protocol in any significant way nor obsoletes previous versions or existing implementations. The main motivation for the new version is to refine the analysis and implementation models for new applications at much higher network speeds to the gigabit-per-second regime and to provide for the enhanced stability, accuracy and precision required at such speeds. In particular, the sources of time and frequency errors have been rigorously examined and error bounds established in order to improve performance, provide a model for correctness assertions and indicate timekeeping quality to the user. The revision also incorporates two new optional features, (1) an algorithm to combine the offsets of a number of peer time servers in order to enhance accuracy and (2) improved local-clock algorithms that allow the poll intervals on all synchronization paths to be substantially increased in order to reduce network overhead. It also adds recommendations in regards to security.

Keywords: Keywords Authorization for Access Control, Policy, Spoof, Security

1.3.5.6 IEC 62351-3 Security for Profiles including TCP/IP

URL:

IEC62351-3 is a developing standard that specifies how to use Transport Layer Security in order to secure IEC TC57 protocols and their derivatives.

Keywords:

1.3.5.7 IEC 62351-4 Security for Profiles including MMS (ISO-9506)

URL:

IEC 62351-4 is a developing standard that specifies how to secure the ISO-9506 (MMS) protocol. It references IEC 62351-3 and adds application level authentication ability. It has applicability in securing IEC 60870-6 TASE.2 (ICCP) and IEC 61850.

Keywords:

1.3.5.8 IEC 62351-5 Security for IEC 60870-5 and Derivatives

URL:

IEC 62351-5 is a developing standard that specifies how to secure the IEC 60870-5 and its derivatives (e.g. DNP) protocols. It references IEC 62351-3 and adds application level authentication ability.

Keywords:

1.3.5.9 IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles

URL:

IEC 62351-6 is a developing standard that specifies how to secure all the communication profiles specified within IEC 61850. It references IEC 62351-5 and adds additional security extensions to provide security for Generic Object Oriented Substation Event (GOOSE), Generic Substation Status Event (GSSE), and Sampled Measured Values (SMV) profiles.

Keywords:

1.3.6 XML Related Technologies

1.3.6.1 OASIS Security Assertion Markup Language (SAML)

URL: <http://www.oasis-open.org/committees/download.php/2290/oasis-sstc-saml-1.0.zip>

Security Assertion Markup Language (SAML) is an XML-based framework standard from OASIS for ensuring that transmitted communications are secure. SAML defines mechanisms to exchange authentication, authorization and non-repudiation information, allowing single sign on capabilities for Web services.

SAML allows a user to log on once for affiliated but separate Web sites. SAML is designed for business-to-business (B2B) and business-to-consumer (B2C) transactions.

SAML specifies three components: assertions, protocol, and binding.

Assertion. There are three assertions: authentication, attribute, and authorization. *Authentication assertion* validates the user's identity. *Attribute assertion* contains specific information about the user. And *authorization assertion* identifies what the user is authorized to do.

Protocol. *Protocol* defines how SAML asks for and receives assertions.

Binding. *Binding* defines how SAML message exchanges are mapped to Simple Object Access Protocol (SOAP) exchanges. SAML works with multiple protocols including Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP) and also supports SOAP, BizTalk®, and Electronic Business XML (ebXML). The Organization for the Advancement of Structured Information Standards (OASIS) is the standards group for SAML.

Keywords: Security exchange, authentication, authorization, non-repudiation, single sign-on

1.3.6.2 OASIS Extensible Access Control Markup Language (XACML)

URL: <http://xml.coverpages.org/xacml-schema-policy-v15.pdf>

The objective of XACML is to provide a mechanism for policy exchange by defining a language capable of expressing policy statements for a wide variety of information systems and devices.

Keywords:

1.3.6.3 XML Key Management Specification (XKMS)

URL: <http://www.w3.org/TR/xkms2/>

XML Key Management Specification (XKMS) specifies protocols for distributing and registering public keys, suitable for use in conjunction with the W3C Recommendations for XML Signature [XML-SIG] and XML Encryption [XML-Enc]. The XML Key Management Specification (XKMS) comprises two parts — the XML Key Information Service Specification (X-KISS) and the XML Key Registration Service Specification (X-KRSS).

Keywords:

1.3.6.4 Secure XML

URL: <http://www.oasis-open.org/committees/download.php/6539/sstc-saml-authn-context-2.0-draft-04a-diff.pdf>

URL: <http://xml.coverpages.org/ws-policyV11.pdf>

URL: <http://xml.coverpages.org/ws-policyassertionsV11.pdf>

URL: <http://xml.coverpages.org/ws-policyattachmentV11.pdf>

URL: <http://xml.coverpages.org/xacml-schema-policy-v15.pdf>

URL: <http://www.w3.org/TR/xkms2/>

There is no single technology that can be called Secure XML. In general, this aggregate technology addresses the use of XML to perform policy exchange, perform authentication, and perform key management in a robust and secure fashion.

Most of these XML exchanges would typically be performed with SOAP and encryption would be supplied by TLS or HTTPS (not listed in the URLs).

Keywords:

1.4 Network and Enterprise Management Technologies

1.4.1 Network Management Technologies

1.4.1.1 Simple Network Management Protocol (SNMP)

URL: <http://www.ietf.org/rfc/rfc1157.txt>, <http://www.ietf.org/rfc/rfc2576.txt>,
<http://www.ietf.org/rfc/rfc3411.txt>

Simple Network Management Protocol (SNMP) [RFC 1157], by IETF Operations and Management Area, is a protocol that enables management stations to configure, monitor, and receive trap (alarm) messages from network devices. The SNMP framework consists of (i) a data definition language, (ii) definitions of management information (the Management Information Base, or MIB), and (iii) a protocol definition, security and administration. SNMP version 2 (SNMPv2) [RFC 2576] and SNMPv3 [RFC 3411] are proposed updates of version 1 and 2 respectively that provides additional administrative structure, authentication, and privacy. The SNMPv3 Working Group produces a single set of specifications for the next generation of SNMP to provide a single recommended approach for SNMP evolution.

Keywords: Internet, Network Management, Security

1.4.1.2 Remote Network Monitor (RMON)

URL: <http://www.ietf.org/rfc/rfc2819.txt>

Remote Network Monitor (RMON) is a standard MIB that defines current and historical MAC-layer statistics and control objects, allowing capturing real-time information across the network. The RMON standard is an SNMP MIB definition described in [RFC 2819]. An RMON configuration consists of a central network management station and a remote monitoring device, RMON agent. From the management station, SNMP commands request information from the RMON agent. The RMON agent sends the requested information to the management station, which then processes and displays this information on its console. RMON also provides alarm and event mechanism for setting thresholds and notifying changes in network behavior.

Keywords: Internet, Network Management, Monitoring

1.4.1.3 OSI Network Management Model and CMIP

URL: <http://www.iso.org>
<http://www.iech.ch>

The OSI Network Management model is a conceptual model for managing all communication “entities” in a network, supported by the Common Management Information Service and Protocol (CMIS/CMIP). It is based around the concept of the abstract Management Information Base (MIB), consisting of all the data on a given device describing the operation of the OSI protocol suite on that device. CMIP accesses the MIB by extending the object-oriented paradigm over a communications protocol. It permits instantiation of objects having classes, attributes and inheritance, and allows them to generate events and alarms based on the state of the real entities the objects represent. CMIP has also proven to be effective for managing the behavior of any manner of devices and processes in an object-oriented fashion, and is frequently used for this function in addition to its original role in network management. The OSI network management model is ISO/IEC 7498-4, 10164 and 10165; CMIS/CMIP is ISO/IEC 9595 and 9596.

Advantages/Strengths of CMIP

One of CMIP's main advantages lies in the fact that not only can it query information from the network elements, but it can also carry out actions (tasks) on network elements that SNMP would find difficult or even impossible to carry out. For instance, if a terminal on a network cannot reach its file server within a predetermined number of times, then CMIP can notify the appropriate personnel of that failure event.

In addition, CMIP addresses many of the shortcomings of SNMP, including the security loopholes (although SNMP has addressed some of these concerns in SNMPv3). It has built in security that supports authorization, access control and security logs. CMIP is a powerful and easily extensible protocol with flexible naming conventions (based on X.500) and event driven. Couple that with an object-oriented model, connection-oriented communications and an unlimited data transfer length, and it is easy to see why the protocol looks so good on paper.

Briefly, the major advantages of CMIP over SNMP are:

- CMIP variables not only relay information, but also can be used to perform tasks. This is impossible under SNMP.
- CMIP is a safer system as it has built in security that supports authorization, access control, and security logs.
- CMIP provides powerful capabilities that allow management applications to accomplish more with a single request.
- CMIP provides better reporting of unusual network conditions.

Disadvantages/Weaknesses of CMIP

Unfortunately, CMIP has two major disadvantages. Firstly, the amount of processing power required to run CMIP 'powered' NMS is an order of magnitude more than that required to run an SNMP NMS. This doesn't just apply to the NMS, but also to each network element that can quickly mount up the cost of implementation. This major disadvantage has no "work-around", and therefore many people believe that the CMIP protocol is doomed to failure. Additionally, CMIP is very complex thus making it difficult to program; therefore skilled personnel with specialized training may be required to deploy, maintain and operate a CMIP based network management system.

These disadvantages have resulted in very few implementations of CMIP. However, despite the disadvantages of CMIP, it is supported by a number of network management systems including **Sun's Solstice® System**, **SpiderCMIP from Shiva** and **HP OpenView®** using the development toolkit.

Keywords: protocol, network management, information model

1.4.1.4 Telecommunications Management Network (TMN) - M series

URL: <http://www.itu.int/ITU-T/studygroups/com04/activities.html>

TMN, developed by ITU-T Study Group 4, provides a framework for interconnectivity and communication across heterogeneous operating systems and telecommunications networks. TMN functions include management of: performance, faults, configuration, accounting and security. TMN manages all types of networks and elements - such as analogue, digital, public and private networks, as well as switching, transmission, and telecommunication software systems. Communication transport protocols supported by TMN include OSI, Integrated Services Digital Network (ISDN), Signaling System No.7, and TCP/IP. Management-specific protocols include OSI's CMIP and FTAM, X.500, and CORBA's GIOP transported over IP (IIOP).

Keywords: Network Management, telephony

1.4.1.5 Transaction Language 1 (TL1)

URL: <http://www.telcordia.com/services/consulting/neps/tl1.html>

Transaction Language 1 (TL1) was defined by based on the ITU Z.300 series of standards. TL1 is the primary method for managing conventional telecom equipment such as access devices as well as optical networking gears such as SONET/SDH boxes. TL1 is a messaging protocol that represents data as human-readable strings of characters rather than as objects.

Keywords: Network Management, optical network, telecommunications equipment management

1.4.1.6 IEC 62351-7 Objects for Network Management

URL:

IEC 62351-7 is a developing standard in IEC TC57 WG15 on Security that is focused on developing standardized Network Management object definitions for monitoring and controlling the information infrastructure. These may include some or all of the following:

Possible types of networks and systems management functions.	
Possible types of network and system functions:	Possible responses or actions could include:
<ul style="list-style-type: none">▪ Numbers and times of all stops and starts of systems, controllers, and applications▪ Status of each application and/or software module: stopped, suspended, running, not responding, inadequate or inconsistent input, errors in outputs, error state, etc.▪ Status of all network connections to an IED, including numbers and times of temporary and permanent failures▪ Status of any "keep-alive" heartbeats, including any missed heartbeats▪ Status of backup or failover mechanisms, such as	<ul style="list-style-type: none">▪ Start or stop reporting▪ Restart IED▪ Kill and/or restart application▪ Re-establish connection to another IED▪ Shut down another IED▪ Provide event log of information events▪ Change password▪ Change backup or failover options

<p>numbers and times these mechanisms were unavailable</p> <ul style="list-style-type: none"> ▪ Status of data reporting: normal, not able to keep up with requests, missing data, etc. ▪ Status of access: numbers, times, and types of unauthorized attempts to access data or issue controls ▪ Anomalies in data access (e.g. individual request when normally reported periodically) 	
---	--

Keywords: Object model, MIB, security, network management, system management

1.4.2 Web-based Network Management

1.4.2.1 Web-based Enterprise Management (WBEM)

URL: <http://www.dmtf.org>

WBEM, under the control of the Distributed Management Task Force (DMTF), is based on a new object model, a new management protocol on top of HTTP as the network management platform. WBEM proposed the way for the encoding of the Common Information Model (DMTF CIM) schema in XML. The DMTF CIM is an object-oriented information model, providing a conceptual framework within which any management data may be modeled. Allowing DMTF CIM information to be represented in the form of XML brings the benefits of XML and its related technologies to management information, which uses the DMTF CIM meta-model. The XML encoding specification defines XML elements, written in Document Type Definition (DTD), is used to represent DMTF CIM classes and instances. The encoded XML message could be encapsulated within HTTP. Further, WBEM defines a mapping of DMTF CIM operations onto HTTP that allows implementations of DMTF CIM to operate in a standardized manner.

Keywords: Information model, web-based, CIM schema

1.4.2.2 Policy-based Management Technologies

URL: <http://www.ietf.org/rfc/rfc3483.txt>

In policy-based system/ network management, policies are defined as rules that govern the states and behaviors of the enterprise application, system and network entities. The management system needs to translate the management objectives to syntactical and verifiable rules governing the function and status of these entities, the translation of such rules to mechanical and device-dependent rules and configurations. Further, it needs to manage distribution and enforcement of these configurations by management entities.

Keywords: Policy, management, rules.

1.4.3 System Engineering Related Data Management Technologies

1.4.3.1 DoD Joint Technical Architecture

Keywords: <http://www-jta.itsi.disa.mil/>

The DoD Joint Technical Architecture (JTA) provides the minimum set of standards that, when implemented, facilitates the seamless flow of information among DoD's sensors, processing and command centers, shooters, and support activities to achieve dominant battlefield awareness and move inside the enemy's decision loop. The JTA:

- Provides the foundation for interoperability among all tactical, strategic, and combat support systems.
- Mandates IT standards and guidelines for DoD system development and acquisition that will facilitate interoperability in joint and coalition force operations.
- Communicates to industry DoD's preference for open system, standards-based products and implementations.
- Acknowledges the direction of industry's standards-based development.

The goals continues to be to "reach a consensus of a working set of standards" and "establish a single unifying DoD technical architecture that will become binding on all future DoD C4I acquisitions" so that "new systems can be born joint and interoperable, and existing systems will have a baseline to move toward interoperability."

Keywords: Technical architecture, Interoperability, Open system, Enterprise VP

1.4.3.2 MIL-STD-499

URL: <http://www.incose.org/stc/mil499.htm>

This standard was published on July 17, 1969. The purpose of this standard is to provide a set of criteria that will serve as a guide to (a) contractors preparing proposed Systems Engineering Management Plans (SEMPs) for the conduct and management of their systems engineering effort on a particular program; and (b) Government personnel when either tailoring a bid work statement calling for SEMPs or competitively evaluating and validating proposed SEMPs and negotiating them into contract statements of work. It also provides the basis for validating the contractor's SEM capability.

Keywords: Systems engineering management plan, Enterprise VP

2. Common Services

2.1 Security Services

2.1.1 Common Security Services

2.1.1.1 Audit Common Service

An audit service is responsible for producing records known as audit records which contain audit record fields, which track security relevant events. The resulting audit records may be reduced and examined in order to address several key aspects of security within a security domain:

- Audit records and audit trails can be used to determine if a pre-scripted security policy is being enforced.
- Auditing and subsequently reduction tooling are used by the security administrators within a Security Domain to determine the Security Domain's adherence to the stated access control and authentication policies.
- Audit records that support the recording of usage data, secure storage of that data, analysis of that data allows Security Domains to detect fraud and intrusion detection.

A robust auditing mechanism enables a Non-repudiation service through the creation of an audit trail.

There are several well-understood audit issues that must be taken into account when implementing the audit trail. The audit trails need to be analyzed to determine vulnerabilities, establish accountability, assess damage and recover the system. Manual analysis of audit trails though cumbersome is often resorted to because of the difficulty to construct queries to extract complex information from the audit logs. There are many tools that help in browsing the audits. The major obstacle in developing effective audit analysis tools is the copious amounts of data that logging mechanisms generate.

There are three significant issues in creating an audit trail from various electronic audit sources:

- A coherent and well-defined service to query an audit provider for audit records.

There needs to be mechanism through which queries for Audit records can be issued. Although multiple protocols could carry such a request, such a deployment strategy would require profile-mapping capabilities. While to date, there is no security specific standards for such a service a general purpose log query service could be used.

- A common and self-describing format for the audit records that can account for specializations.

The capability to query for audit records allows the start of the information transfer. However, in order to re-construct an Audit Trail from multiple audit record sources, there needs to be a common Audit Record format. The format should be self-describing with standardized contents, but allow for additional information to be conveyed. Some of the standardized fields might be:

<AuditRecord>, <RecordType>, <AuthBy>, <SubjectUid>, <TimeStamp>¹, etc... However, there is no internationally recognized specification for such. What is important here is that the record structure is self describing so that a general purpose log query service could present log data intelligently.

- A well-defined mechanism to detect tampering with the transferred audit records.

One of the major purposes for audits/audit trails/audit records is provide an authoritative mechanism to perform non-repudiation. One of the key issues with providing non-repudiation in an authoritative manner is to prove that the audit trail/record has not been tampered with.

Although there is no recognized standard for such purposes, there is a recognized approach to the problem. This is to digitally sign the audit record or to provide a non-repeating serial number for the record. The actual mechanics of the digital signature and how to convey the signature would be issues for the common audit record format specification.

- The ability to correlate audit records from multiple audit sources.

It is conceivable that different Security Domains would be in different time zones. In order to create an inter-domain audit trail, it is necessary to be able to correlate the times of the various audit records.

Thus all audit records should have a timestamp whose reference time is UTC. However, the timestamp itself may not have the accuracy to differentiate between several audit records that occur within the same timestamp period. Thus, it is also a requirement that an audit record serial number be provided within each audit record. The combination of the timestamp and serial number would need to be unique.

Problems with correlation can also occur if the timestamp accuracies of the audit records are not the same. Thus IECSA should specify an appropriate accuracy and time synchronization skew that is allowable.

- Determination of where to place auditing capability.

Many security infrastructures/policies have difficulty identifying the types of applications that need an audit trail. The use of the definition of the IECSA security services allows the following base recommendations to be made.

Audit records should be generated whenever/wherever the following security services are invoked: Authorization for Access Control; Credential Conversion; Credential Renewal; Delegation; Firewall Transversal; Identity Establishment; Identity Mapping; Profile; Security Protocol Mapping; Setting and Verifying User Authorization; Single Sign-On; Trust Establishment; User and Group Management.

- Determination of the minimum-maximum audit record time availability. There is a need to determine/specify through policy a minimum amount of time that an audit record must be maintained within the audit trail system. In the IECSA environment, this time would need to be specified so that non-repudiation for an appropriate period of time can be provided.

2.1.1.1.1 Audit Technologies/Specifications

Table 1 represents a set of specifications and/or standards that are relevant to the understanding of the issues regarding the audit service. Those specifications marked as Recommended or Recommended

¹extracted from

http://sybooks.sybase.com/onlinebooks/groupsec/secg0253e/epsec/@Generic__BookTextView/13539;pt=7509

Reading should be considered as materials that should be considered prior to actually implementing the audit service.

Table 1: Relevant Standards/Specifications relevant to the Audit Service

Identification Number	Name	Comment
ISO/IEC 10164-8:1993	Information technology -- Open Systems Interconnection -- Systems Management: Security audit trail function	Recommended
ISO/IEC 10181-7:1996	Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework	
ISO/IEC 18014-1:2002	Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework	Recommended Reading
ISO/IEC 18014-2:2002	Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens	
ISO/IEC 18014-3:2004	Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens	
21 CFR Part 11	Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application	Recommended Reading

2.1.1.1.1.1 Technological Assessment

An inspection of Table 1 shows that there are no technology specific specifications/standards that address the issues/problems previously discussed in this section.

2.1.1.2 Authorization for Access Control

The authorization for Access Control is concerned with resolving a policy based access control decision based upon appropriate Identity Establishment. The service consumes as input a credential/identity token which embodies the identity of a service requestor and/or for the resource that the service requestor requests. Based upon the credentials and trust factors and policy, the resource will determine if authenticating the peer is to be performed. Once authenticated, the peers may process each other's requests based upon appropriate policy enforcement (e.g. privilege or role based access).

It is expected that the hosting environment for OGSA compliant services will provide access control functions, and it is appropriate to further expose an abstract authorization service depending on the granularity of the access control policy that is being enforced. Allow for controlling access to OGSA services based on authorization policies (i.e., who can access a service, under what conditions) attached to each service. Also allow for service requestors to specify invocation policies (i.e. who does the client trust to provide the requested service). Authorization should accommodate various access control models and implementation.

Key definitions:

Authentication for Access Control relies upon several basic factors being achieved:

- That the identity of the entity/person is established.

The Identity Establishment Service performs this function.

- That there is an acceptable level of Trust established that the entity is who they claim to be.

The Trust Establishment and Quality of Identity services are involved in providing this functionality.

- That there is a policy and management process that has been used to determine which entity has the privileges to access certain assets, resources, or information.

The Policy and SMI related services provide this functionality.

- That there is a mechanism to enforce the mandates of the policy and management process.

The Authorization for Access Control service is responsible for providing this functionality.

There are generally three (3) categories of Access Control that need to be addressed within a SD: Physical Assets; Computational Resources; and Information.

2.1.1.2.1.1 Physical

The basic premise of physical access control is intended to allow authorized individuals to be able to enter the areas for which they have clearance to enter and to make it difficult for un-authorized individuals to enter. Based on the Security Domain definition, physical access control is not an inter-domain issue. However, there are some desirable aspects to any physical access control system:



- The system should be capable of providing an audit trail of who actually entered a specific area.
- The system should be capable of detecting intrusion attempts of an un-authorized individual to enter an area.
- There are issues in regards to the quickness/speed of enunciating intrusion or intrusion attempts. The speed at which this enunciation can occur is a key metric in regards to the ability of a SMI to respond to the intrusion.
- The system should be robust enough that intrusions can be proven in an authoritative manner so that legal prosecution has a probability of success.
- Properly implemented, a physical access control system can provide on-site personnel listings/locations in the event of an emergency event.
- The choice of access control mechanisms should allow for multi-factor authentication and ease of management in the event that revocation of access privileges is required (e.g. User and Group Management issues). In order to accomplish this service function, there must be a security token that is used to enable a final access mechanism (e.g. a lock).
- A policy/strategy needs to address assets that are not capable of being physically secured. For these types of resources, informational and resource security measures will need to be enhanced. Examples of such an assets are wireless networks and wireless technologies.
- A residual risk analysis and recovery plan needs to be developed, as part of the Policy service, to address resources for which no type of adequate security can be provided. Examples of such physical resources are transmission lines and telephone lines.

In order to provide physical access control, there needs to have a physical barrier that separates critical or controlled areas from un-controlled areas. These barriers would typically be fences, walls, or doors that have locks or security guards so that proper access privileges can be determined.

2.1.1.2.1.1.1 Physical Access Technologies/Specifications

There are no relevant specifications regarding Physical Authorization for Access Control. However, there are typical strategies that are worthy of some discussion (see Table 2).

Table 2: Typical Physical Access Control Strategies

Security Strategy	Authentication Factor			Biometric	Comments
	Single	Two	Three		
Security Guard Only					Needs to be augmented in order to provide audit capability, at a minimum.
Key/Lock	X				Adequate token that can be properly managed but can easily be duplicated that would facilitate un-authorized access.
Combination Lock	X				Typically adequate, but can be stolen through observation.
Sign-in sheet					Should not be used solely. At a minimum, verification of the person's identity signing-in must be facilitated.
Sign-in sheet with Photo-ID	X			X	Requires a security guard.
Sign-in sheet with confirmed clearance to enter.	X			X	Typically used for guest entry. In order to be biometric, the confirming party must visually recognize and clear the entity requesting entry.
Video Surveillance					Should be used as audit/security for major/sensitive entrances. Provides a good mechanism for legal prosecution for remote sites.
Photo-ID with no sign-in sheet				X	Should not be used since no audit trail is possible.
Smart Card	X				It is assumed that SMART Cards would be used in conjunction with computerized locks so that a computerized audit trail can be generated. However, it is typical that only ½ of the audit trail is generated since the cards are typically not required to exit the room.
Smart Card with Photo ID Card	X			X	Has the benefit of the Smart Card and can double as a Personal ID. This is the recommended strategy. 
Smart ID Card used to enable Combination Lock		X			This is the best mechanism for access to sensitive areas. 

Security Strategy	Authentication Factor			Biometric	Comments
	Single	Two	Three		
Biometric Combination Lock		X		X	This is the best mechanism for restricting access to sensitive areas.



Another method of analyzing the same strategies would be:

Table 3: Physical Security Strategies vs. Security Services Provided

Security Strategy	Security Service Provided			Comment
	Identity	Trust	Access Control	
Security Guard Only	?			It is questionable that a security guard only strategy could provide adequate identification establishment.
Key/Lock		x	x	Provides a mechanism to establish a relative level of Trust (due to the person having the key) and provides appropriate access control.
Combination Lock		x	x	Provides a mechanism to establish a relative level of Trust (due to the person having the combination) and provides appropriate access control.
Sign-in sheet				Without actual identity establishment, no security can be provided.
Sign-in sheet with Photo-ID	x			
Sign-in sheet with confirmed clearance to enter.	?	x		Only provides Identity Establishment if a photo-ID is used in conjunction with the sign-in sheet.
Video Surveillance				Provides audit and repudiation capability only.
Photo-ID with no sign-in sheet	x			
Smart Card		x	x	A Smart-Card only does not provide Identity Establishment. Identity Establishment is a required function/service for Access Control. Therefore, the use of Smart-Cards only should not be considered.
Smart Card with Photo ID Card	x	x	x	This is a recommended strategy for non-critical area access.
Smart ID Card used to enable	x	x	x	This is one of the recommended deployment

Combination Lock				strategies for critical areas.
Biometric Combination Lock	x	x	x	This is one of the recommended deployment strategies for critical areas.

2.1.1.2.1.1.1.1 Technological Assessment

The suggested technology to be used to provide Access Control to critical areas is the use of multi-factor access control. It is further suggested that SMART-CARD²s that double as personal identification cards be utilized to enable combination locks. Furthermore, it is also recommended that such technology deployment be used in conjunction with an electronic audit mechanism.

2.1.1.2.1.2 *Computational Resource*

The basic premise of computational access control is intended to allow authorized individuals to be able to access programs for which they have clearance to make use of. Based on the Security Domain definition, computational access control is both an inter-domain and intra-domain issue. However, the enforcement of computation access control is purely an intra-domain issue. For inter-domain access control the Identity Mapping service (and its required sub-functions) actually provides the mapping from an external identity to an identity recognized and managed intra-domain.

- The system should be capable of providing an audit trail of who accessed a given computational resource.
- The system should be capable of detecting intrusion attempts of an un-authorized individual to a computational resource.
- There are issues in regards to the quickness/speed of enunciating intrusion or intrusion attempts. The speed at which this enunciation can occur is a key metric in regards to the ability of a SMI to respond to the intrusion.
- The system should be robust enough that intrusions can be proven in an authoritative manner so that legal prosecution has a probability of success.
- The choice of access control mechanisms should allow for multi-factor authentication and ease of management in the event that revocation of access privileges is required (e.g. User and Group Management issues). In order to accomplish this service function, there must be a security token that is used to enable a final access mechanism (e.g. a lock).
- A policy/strategy needs to address assets that are not capable of being secured. For those types of resources, the level of trust should be considered low.

The aforementioned issues need to be addressed for a variety of computational resources: Operating Systems (OSs); programs within a OS that has access control; programs within an environment where there is no OS access control required to access the program (e.g. an RTU); and wireless networks.

2.1.1.2.1.2.1 *Operating System and Computer Programs*

Operating System (OS) access control requires Identity Establishment (see the identity establishment service). The access control service, for OSs, determines which programs/computational resources the Identified User/Program has privileges to execute/access.

The major issues regarding this access are:

² The actual technology recommendation for Smart-Cards can be found in the Identity Establish service section.

- To provide an appropriate policy and SMI so that such access is granular enough to provide enough audit capability.
- Managing the configuration in a distributed environment.
- The level of trust that can be associated with the OS to perform its tasks in a secure manner (see ACC-01). Several issues are mitigated if a “Trusted/Secure” OS is used. However, the use of such OSs in the IECSA environment is not viable in a majority of the cases, therefore this section will address non-Trusted OS issues.

For all OSs, the issue of access control relates to properly managed Access Control Lists that are typically OS specific. However, care needs to be taken to ensure that if Role Based Access is used, that an audit mechanism is provided in order to reference back to the actual individual/entity that has accessed the OS. Additionally, the information in ACC-02 should be considered when developing the OS access framework in a distributed environment.

Computer Programs

In the cases where an OS does not provide Access Control to the programmatic level, programs themselves need to provide this capability. This is particularly true for electronic protocol processes that bypass OS authentication on the destination of the communication path. In such a situation, it is incumbent upon the destination program/process to apply the appropriate security mechanisms.

In the IECSA there will be computational and communication technologies integrated of various capabilities. These various capabilities (e.g. process/memory/storage capacity or bandwidth limitations) require that different technological solutions be available. However the functional objectives remain consistent: provide a manageable environment and to provide enough granularity to provide a capability for non-repudiation.

2.1.1.2.1.2.2 Communication Networks

There are several types of communication networks that need to be addressed:

- Inter-Domain networks where the physical network are exposed.

The major issue with these types of physical networks is that both domains do not manage the network segments that provide the inter-domain interfaces. These segments are typically provided by a third party and therefore constitute a third Security Domain. Thus it is important that appropriate access control be provided at the security domain interface points.

- Intra-Domain networks where the physical network is within a Security Domain.

For intra-domain networks, some Security Domains may desire to control the computers/computer users that actually have access to the network. Once a resource is within a Security Domain, there is no reliable mechanism to prevent physical access to the network. Thus it becomes incumbent upon the SMI to detect that a non-authorized access to the network has been attempted or been successful. Additionally, it may be possible to make it more difficult for a non-authorized resource to make use of the network through proper management of the network addresses so that no address is assigned to the intruding resource.

- Wireless LAN/WAN Networks whose transmissions can be easily monitored and spoofed.

This type of network represents an intra-domain network that **REQUIRES** management in regards to who can actually make use of the network. The issue can be easily demonstrated by looking at the prevalence of WI-FI.

In the WI-FI case, hot-spots (e.g. Starbucks, airports) could not recoup their investment without a challenge response mechanism to ensure that only authorized (e.g. paid subscription entities) are actually assigned an address that facilitates real communications.

Such mechanisms may prevent off-segment communications, but will not prevent denial-of-service attacks (see ACC-03). Thus such systems need to be augmented beyond challenge-response.

- **Dial-up Networks:** There is a well-documented history in regards to the vulnerabilities associated with dial-up networks. These types of networks are inherently susceptible to denial-of-service attacks and have poor identity establishment/access control at a physical/network level. This is especially true for equipment that is deployed in the Transmission and Distribution environment.

Table 4: References regarding Computational Resource Access Control

ACC-01	Stephen Radford - Trusted Operating Systems and Their Evolving Non-Trusted Counterparts , January 23, 2003. SANS Institute
ACC-02	Fine-Grain Authorization for Resource Management in the Grid Environment. K. Keahey, V. Welch. <i>Proceedings of Grid2002 Workshop</i> , 2002.
ACC-03	AA-2004.02 -- Denial of Service Vulnerability in IEEE 802.11 Wireless Devices (AusCERT)

2.1.1.2.1.2.3 Technological Assessment Specifications/Standards

Table 5 represents a set of specifications and/or standards that are relevant to the understanding of the issues regarding access control for computational resources. Those specifications marked as Recommended or Recommended Reading should be considered as materials that should be considered prior to actually implementing the access control service.

Table 5: Relevant Computational Resource Access Control Standards/Specifications

Identification Number	Name	Comment
ANSI INCITS 359-2004	Role Based Access Control	Recommended
RFC 2244	ACAP -- Application Configuration Access Protocol	Recommended
RFC 1013	X Window System Protocol, version 11: Alpha update April 1987	
RFC 2086	IMAP4 ACL extension	
RFC 2820	Access Control Requirements for LDAP	Recommended for Directory Services
RFC 1305	Network Time Protocol (Version 3) Specification, Implementation	Recommended for NTP
RFC 2753	A Framework for Policy-based Admission Control	
RFC 2744	Generic Security Service API Version 2 : C-bindings	

RFC 2356	Sun's SKIP Firewall Traversal for Mobile IP	
RFC 1004	Distributed-protocol authentication scheme	
RFC 2865	Remote Authentication Dial In User Service (RADIUS)	Recommended for Dial-up Lines
RFC 2869	http://www.armware.dk/RFC/rfc/rfc2869.html RADIUS Extensions	
RFC 1221	Host Access Protocol (HAP) Specification - Version 2	
ISO/IEC 10164- 9:1995	Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control	
ISO/IEC 10181- 3:1996	Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework	Recommended
WebDAV	Access Control Extensions to WebDAV	

2.1.1.2.1.2.3.1 Technological Assessment and Recommendations

2.1.1.2.1.2.3.1.1 OS Recommendations

It is recommended that Trusted OSs be used whenever possible. Additionally, ANSI INCITS 359-2004 is suggested as an implementation strategy for Role Based Access.

2.1.1.2.1.2.3.1.2 Computer Programs

It is recommended that the appropriate access control list mechanisms be used in regards to the applications where such technologies have been noted in Table 5. Thus, make use of:

- RFC 1013 for X Windows applications.
- RFC 2086 for IMAP based applications.
- RFC 2820 for LDAP.
- RFC 1305 in regards to NTP.

Otherwise, it is suggested to follow the general policies/procedures set forth in ISO/IEC 10181-3:1996 and make use of any application specific access control strategies set forth.

2.1.1.2.1.2.3.1.3 Communication Networks and Protocols

In general it is recommended that all computational resources, when possible, be assigned dynamic addresses that allow off-segment communications. There is no single technology that can accomplish this, but a challenge response mechanism is suggested as part of the implementation strategy.

For those resources that require fixed addresses (e.g. servers of data), it is suggested that network based access control lists be implemented in order to prevent un-authorized off-segment communication.

There is a substantial amount of work occurring within IEC TC57 WG15 to secure several of the communication protocols that are intended to be used by IECSA. It is suggested that these be adopted and deployed as rapidly as is feasible.

Wireless networks are extremely susceptible to denial-of-service attacks. In order to mitigate this issue, AES encryption on wireless links is suggested.

Dial-up access control should be implemented through the use of RAIDUS (RFC 2865 and RFC 2869) when this is feasible. Such access should be deployed so that there is an additional access control list (e.g. a Firewall or router based ACL) that provides additional security. Thus, when possible, it is suggested that NO direct dial-up access be given to a computer or a computer process.

However, this is not feasible in the Transmission and Distribution systems deployed within the IECSA environment (e.g. RTUs and field devices). For this class of resource, or resources with similar constraints, it is suggested that the devices be implemented in such a manner that denial-of-service is mitigated:

- Dial-up connections should be constructed such there is an inactivity time-out to prevent a connect/hold the port open denial of service attack.
- Once the port is connected, there should be a time-out on the connection that requires valid communication protocol/application level information flow.

It is not suggested to implement a dial-back strategy since these become difficult to manage and maintain and does not allow the type of environment that IECSA is attempting to promote.

2.1.1.2.1.3 Informational Technology Assessment/Specification

Information access control is extremely similar to a combination of OS and program access. However, it is up to each individual program to provide the appropriate level of access control.

ACC-04 represents a very simple summary of the granularity required in access control for most PICOMs: Control over Reading; Control over Changing; and Control over Storing. Additionally, for Object Oriented access, there may need to be an ability to prevent an entity from discovering that an Object Exists (optional).

Table 6: References relating to Access Control for Informational Resources

ACC-04	Access Control on the Semantic Web (w3.org) Available from: http://www.w3.org/2002/03/semweb/access-control
--------	--

2.1.1.3 Confidentiality

Protect the confidentiality of the underlying communication (transport) mechanism, and the confidentiality of the messages or documents that flow over the transport mechanism in an OGSA compliant infrastructure. The confidentiality requirement includes point-to-point transport as well as store-and-forward mechanisms.

Key definitions:

confidentiality: 1. Of classified or sensitive data, the degree to which the data have not been compromised; *i.e.*, have not been made available or disclosed to unauthorized individuals, processes, or other entities. [After 2382-pt.8] **2.** Assurance that information is not disclosed to unauthorized persons, processes, or devices. [INFOSEC-99] **3.** A property by which information relating to an entity or party is not made available or disclosed to unauthorized individuals, entities, or processes. [T1.Rpt22-1993]

There are two main mechanisms to provide confidentiality for electronically transmitted information: encryption or transmission over a secure infrastructure.

2.1.1.3.1.1 Encryption

It is important to realize that there is no 100% effective mechanism to protect electronically transmitted information for an indefinite length of time. Initially, when the Data Encryption Standard (DES) was specified, it was thought that 56-bit encryption protection could protect information for 20-30 years. However, with the increase in computational capability, and the decrease in cost for that capability, in 1999 DES was cracked in under 22 hours (see CONF-02) . In 2004, DES could be cracked in under 5 minutes considering CPU performance increase only.

Estimated time to crack linear-symmetric encryption technologies			
Number of bits in encryption key	Estimated time to crack using current technology		
	DES	Triple DES (3DES)	AES
56	4 min	20 days	20 days
64	1024 min	70 days	70 days
128			100 days
256			200 days
512			400 days

To respond to the new reality, NIST and several standards organizations (in particular IEEE) developed a more advanced and secure encryption standard known as the Advanced Encryption Standard (AES).

“In comparison, DES keys are 56 bits long, which means that there are approximately 7.2×10^{16} possible DES keys. Thus, there are on the order of 10^{21} times more AES 128-bit keys than DES 56-bit keys. Assuming that one could build a machine that could recover a DES key in a second (i.e. try 255 keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key. To put this into perspective, the Universe is believed to be less than 20 billion years old. NIST believes that AES will remain secure beyond the next twenty years. AES implementations will also be exportable, and AES implementations in proprietary systems will just need a one-time review prior to export” [CONF-01]

The above claim is similar to the claims made by DES when it was first introduced. Whereas DES and Triple-DES (3DES) have had almost twenty years of deployment prior to replacement due to “crackability”, the advent of Quantum Computers (see CONF-03) may not allow the modern encryption

algorithms the same. If Quantum Computers were available today, using Grover's Algorithm (see CONF-04) it could be extrapolated that even 512 bit DES could be cracked in approximately 1 second. AES is more complex and is less prone to Grover's Algorithm, however the NIST statement (CONF-01) will definitely not be true in the near-term future.

The advent of Quantum Computers raises the issue of how to make encryption effective. Even without the advent of Quantum technology, the following recommendations are valid:

- Choose a modern encryption algorithm for the purposes of encryption.

There are many factors that enter into an appropriate algorithmic choice. The factors that need to be considered are the additional CPU processing that the use of encryption will require and the bandwidth/transmission performance characteristics desired.

At the NERC Data Exchange Working Group meeting in April 2004, the following results were presented for Secure IEC-60870-6 TASE.2 (ICCP).

The additional CPU performance requirements, for the use of TLS and AES 256, represented an increase from 1% to 1.35% for encryption and 1% to 1.41% for decryption (percentages based upon total CPU being 100%). It was also found that AES 256 was more CPU efficient than either DES or 3DES.

It was found that the bandwidth overhead increased by the size of certificates exchanged, but only increased 1% in regards to normal ICCP traffic once the initial connection and symmetric keys were established.

- When using encryption, make sure that the technology used to "negotiate" encryption can negotiate multiple encryption algorithms.
- If possible, make sure that the negotiation can be upgraded to newer encryption algorithms as new, more robust algorithms, become available.
- Make use of technologies where the encryption keys can dynamically be re-negotiated without interrupting the communication information flow.

Table 7: Reference Relevant to Encryption Technology

CONF-01	NIST Announces New Government Aes Encryption Standard - Technology Information Available from: http://articles.findarticles.com/p/articles/mi_m0BNO/is_2000_Nov/ai_66297312
CONF-02	Jason Meserve , DES code cracked in record time, Network World, 01/20/99 Available from: http://www.nwfusion.com/news/1999/0120cracked.html
CONF-03	Aaron Ricadela, Quantum's Next Leap, Information Week, May 10, 2004
CONF-04	Matias Castro ,What Use is My Quantum Computer Now I Have it? Available From: http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol2/mjc5/

2.1.1.3.1.1.1 Technological Assessment and Specifications

There are several different mechanisms through which to develop assessments regarding encryption. For the purposes of this section, applicability to specific communication media will be used.

In general, it is suggested to make use of X.509 certificates to provide public/private key encryption exchanges when possible. Such a choice will ease integration with other certificate technologies (e.g. management) that are being recommended as part of other security services.

When X.509 certificate use is not appropriate, it is suggested that RFC 2898 (PKCS#5) be utilized. This allows encryption to be established based upon username/passwords.

2.1.1.3.1.1.1.1 Protocol Basis

In general, it is recommended to use the appropriately specified encryption standard associated with the protocol (e.g. HTTPS for HTTP). There are further recommendations for TCP/IP:

TCP/IP Transmissions

It is recommended that TLS with AES (RFC 3268) or PPP Encryption Control Protocol (RFC 1968) be used to provide encryption. These represent the most modern and secure mechanism.

2.1.1.3.1.1.1.2 Media

Serial

If the path of the serial link does not provide enough confidentiality or the protocol in use over the link, and confidentiality is still desired then the following is recommended:

- If the peers can be upgraded to support encryption, then this should be the preferred approach.
- For legacy systems, that are not upgradeable, it is suggested that external hardware be applied. Further it is recommended that AGA-12 be evaluated for this purpose.

Ethernet, SONET, FDDI, etc.

It is recommended to make use of VPN technology when possible.

WI-FI and Wireless Technologies

The Web Encryption Protocol (WEP) specified in IEEE 802.11b has been proven to be vulnerable and to not provide adequate protection. New versions of WI-FI and wireless technologies are coming equipped with AES encryption. It is the AES encryption that is recommended. Further it is recommended that WPA2/80211.i be adopted in order to achieve the implementation of this recommendation.

It is further recommended that any legacy (e.g. WEP based) WI-FI equipment be replaced or upgraded, as the vulnerabilities are well known and not manageable.

Table 8: Encryption Related Specifications/Standards

Identification Number	Name	Comment
RFC 3370	Cryptographic Message Syntax (CMS) Algorithms	
RFC 3447	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1	
RFC 2898	PKCS #5: Password-Based Cryptography Specification Version 2.0	Recommended when certificate exchange is not

Identification Number	Name	Comment
		appropriate.
RFC 1968	The PPP Encryption Control Protocol (ECP)	
RFC 2246	The TLS Protocol Version 1.0	
RFC 2409	The Internet Key Exchange (IKE)	Used for VPNs
RFC 1040	Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication	
RFC 2946	Telnet Data Encryption Option	
RFC 2440	OpenPGP Message Format	
RFC 1423	Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers	
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)	Used for VPNs
RFC 2510	Internet X.509 Public Key Infrastructure Certificate Management Protocols	
RFC 3268	Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)	
RFC 2093	Group Key Management Protocol (GKMP) Specification	
RFC 2459	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	
RFC 2040	The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms	
FIPS 197	Federal Information Processing Standards Publication 197, November 26, 2001, Specification for the Advanced Encryption Standard (AES) Available from: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf	Recommended
RSA PKCS #12	Personal Information Exchange Syntax Standard, version 1.0.	
RSA PKCS #8	Private-Key Information Syntax Standard	
IEEE 802.11b	Web Encryption Protocol	
AGA-12	Cryptographic Protection of SCADA Communications General Recommendations.	
WPA	WI-FI Protected Access	
IEEE 802.11i	Security for Wireless Networks	
WPA2	WI-FI Protected Access Version 2	

Table 9: Digital Certificate Related Specifications/Standards

Identification Number	Name	Comment
-----------------------	------	---------

Identification Number	Name	Comment
RFC 2510	Internet X.509 Public Key Infrastructure Certificate Management Protocols. C. Adams, S. Farrell. March 1999.	
RFC 2511	Internet X.509 Certificate Request Message Format. M. Myers, C. Adams, D. Solo, D. Kemp. March 1999.	
RFC 2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. S. Chokhani, W. Ford. March 1999.	
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams. June 1999.	

2.1.1.3.1.2 *Communication Path Selection*

There is a mechanism of mitigating the need to encryption. This is to evaluate or provide a communication path that inherently provides enough protection (see the Path Routing and QOS service for further information).

2.1.1.4 Credential Conversion

The credential conversion service provides credential conversion between one type of credential to another type or form of credential. This may include such tasks as reconciling group membership, privileges, attributes and assertions associated with entities (service requestors and service providers). For example, the credential conversion service may convert a Kerberos credential to a form which is which is required by the authorization service. The policy driven credential conversion service facilitates the interoperability of differing credential types, which may be consumed by services. It is expected that the credential conversion service would use the identity mapping service.

Key definitions:

credential: 1. In cryptography, a subset of access permissions (developed with the use of media-independent data) attesting to, or establishing, the identity of an entity, such as a birth certificate, driver's license, mother's maiden name, social security number, fingerprint, voice print, or other biometric parameter(s). [After X9.69] **2.** [In security], information, passed from one entity to another, used to establish the sending entity's access rights. [INFOSEC-99]

Credential conversion is also a required service for Single-Sign on and the Identity Mapping security services. Besides performing the actual mappings, there is an inherent requirement that such a service provide an audit mechanism so that it is possible to determine the original identity/credential that was converted. This is a necessary requirement in order to provide a robust audit mechanism in a multi-domain environment.

2.1.1.4.1.1 *Technological Assessment*

The prevalent work is being sponsored by OASIS. This is work in progress but is the first industry/standards based consortium that is attempting to solve the problem. However, the current work involves certificate usage and does not directly address the issue of username/password conversion or the audit trail issues.

Except for the general recommendations found in the Identity Establishment service, only certificates require further recommendations in regards to credential conversion.

2.1.1.4.1.1.1 *Certificate*

Furthermore, there has been little thought in enhancing the SAML specification to standardize a chain or properties that would allow the Quality of Identity service to be facilitated.

It is suggested that SAML and the OASIS work be adopted as the foundation for the Credential Delegation service. However, further work and IECSA enhancements may be required.

Table 10: References and Specifications regarding Credential Conversion

Identification Number	Name	Comment
OASIS Security Technical Committee	Security for Grid Services Available from: http://www.globus.org/Security/GSI3/GT3-Security-HPDC.pdf	
OASIS Security Technical Committee	Attribute Profiles for SAML 2.0 Available from: http://www.oasis-open.org/committees/download.php/6344/sstc-hughes-mishra-baseline-attributes-03.pdf	Incomplete, but is on the correct track.
OASIS Security Technical Committee	SAML 2.0: Security Assertion Markup Language Version 2.0	Recommended
OASIS Security Technical Committee	Bindings for OASIS Security Assertion Markup Language (SAML) V2.0 Available from: http://www.oasis-open.org/committees/download.php/6773/sstc-saml-bindings-2.0-draft-11-diff.pdf	Draft that specifies how to bind SAML over various protocols. Highly recommended.
OASIS Security Technical Committee	Authentication Context Available from: http://www.oasis-open.org/committees/download.php/6539/sstc-saml-authn-context-2.0-draft-04a-diff.pdf	Draft that is needed to establish identity within a SAML environment.

2.1.1.5 Credential Renewal Service

In many scenarios, a job initiated by a user may take longer than the life span of the user's initially delegated credential. In those cases, the user needs the ability to be notified prior to expiration of the credentials, or the ability to refresh those credentials such that the job can be completed.

It is worthy to note that the Credential Renewal service provides some of the capability of User and Group Management service. However, it does not include how to revoke or initially allocate the credentials. However, in general it is a Security Domain and IECSA issue in regards to the period of time required for credential renewal.

Performing a more in-depth analysis of the credential renewal process, the general issues are:

- Determining when the credentials need to be renewed. This is typically a Security Domain's policy issue.
- Determining a mechanism to detect a credential that needs to be renewed.
- Provide a mechanism for credential renewal.

OASIS specifies several different types of credentials that need to be considered for renewal. Each has different aspects to renewal. The IECSA relevant types are:

- Internet Protocol based credentials are related solely to address resolution as the credential. Address spoofing is a prevalent threat in the IECSA environment and therefore the use of this credential mechanism is not suggested.

In order to renew an addressed based credential, address-to-name resolution is required as well as appropriate security on such resolution requests.

- InternetProtocolPassword makes use of username/password as well as address resolution to establish credentials.

This credential methodology has the same issues with address credential renewal as well as verifying that the password is viable or in need of renewal.

- Password makes use of a username/password combination in the clear.

Username/Password management is a major issue that needs to be resolved.

- PasswordProtectedTransport makes use of an encrypted transport to transmit a username/password combination (e.g. HTTPS conveying a username/password).
- SmartCard renewal is strictly a policy and SMI issue. The policy must address when a SmartCard must be renewed and the mechanism for performing a renewal.
- SmartCardPKI renewal adds the issue of digital certificate renewal to the need to renew a particular Smart Card. Since most digital certificates have an expiration date, it is the certificate date that should take precedence in the renewal process (e.g. policy may be able to ignore the renewal of the card itself). However, this is not the case if the SmartCardPKI solution is being used as a Personal Identification card that requires visual inspection for physical access.
- SoftwarePKI uses digital certificates and therefore certificate renewal is the major issue.
- TimesyncToken is a hardware token that is used to generate a unique token as a credential.
- Visual Person Identification Card used with visual inspection to provide physical access control.

Any credential type that can be used to obtain physical access based upon visual inspection need to be replaced or modified in a timely manner. The periodicity of the change is dependent upon the Security Domain's policies.

2.1.1.5.1.1 Technological Assessment and Relevant Specifications

There are certain general recommendations that can be made:

- When using address resolution and TCP/IP, make use of the Domain Name Service and an authenticated Directory server. Dynamic address assignment should be the preferred mechanism with the resulting address being placed in the authenticated directory server.
- Visual Credentials should be replaced/modified on a time period based upon the Security Domain's policy. It may be less expensive to adopt a modification, as opposed to a replace strategy (e.g. the same model as automobile license tabs versus license plates).
- Smart Cards should include a renewal date as part of the information that is contained on the card. This field should encrypt and digitally signed so that tampering can be detected. As the Smart Card is used, advanced notification of the need for renewal needs to be given to the holder.
- Certificate based technologies: X.509 certificates are the recommended certificate type. Certificates should be accessible via PKCS#10 interfaces. The date of certificate lifetime expiration should be used as the renewal date. As the certificate is used, advanced notification of the need for renewal needs to be given to the holder.
- Biometric based technologies need to have renewal dates based upon the Security Domain's policy.

2.1.1.5.1.1.1 Specific Recommendations

2.1.1.5.1.1.1.1 Certificates

It is recommended that RFC 2797 or RFC 2560 (OCSP) to determine if the certificate needs to be renewed. If neither of these is possible, then it becomes a local Security Domain/implementation issue. Certificate renewal should be performed via RFC 2797 when possible.

Table 11: Relevant Specification regarding Credential Renewal

Identification Number	Name	Comment
ISO 9735-9:2002	Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 9: Security key and certificate management message (message type- KEYMAN)	
NERC	Certificate Policy for the Energy Market Access and Reliability Certificate (e-MARC) Program Version 2.4 Available from: ftp://www.nerc.com/pub/sys/all_updl/cip/pkitf/e-MARC-	

Identification Number	Name	Comment
	PKI_draft_version_V2-4b_March_2003-rev1.doc	
OASIS Security Technical Committee	Authentication Context Available from: http://www.oasis-open.org/committees/download.php/6539/sstc-saml-authn-context-2.0-draft-04a-diff.pdf	
RFC 2459	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	
RFC 2511	Internet X.509 Certificate Request Message Format	
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	
RFC 2797	Certificate Management Messages over CMS	
RFC 2875	Diffie-Hellman Proof-of-Possession Algorithms	
RFC 2986	http://www.armware.dk/RFC/rfc/rfc2986.html PKCS #10: Certification Request Syntax Specification Version 1.7	
RFC 3280	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	
RFC 3369	Cryptographic Message Syntax (CMS)	
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	
RFC 1591	http://www.armware.dk/RFC/rfc/rfc1591.html Domain Name System Structure and Delegation	
RFC 1608	Representing IP Information in the X.500 Directory	Recommended
RFC 1612	DNS Resolver MIB Extensions	Recommended
RFC 2230	Key Exchange Delegation Record for the DNS	
RFC 2276	Architectural Principles of Uniform Resource Name Resolution	
RFC 2535	Domain Name System Security Extensions	Recommended
RFC 2592	http://www.armware.dk/RFC/rfc/rfc2592.html Definitions of Managed Objects for the Delegation of Management Script	
RFC 2874	http://www.armware.dk/RFC/rfc/rfc2874.html DNS Extensions to Support IPv6 Address Aggregation and Renumbering	
ISO 10202-1:1991	Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle	Recommended Reading
ISO 10202-7:1998	Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management	

2.1.1.6 Delegation Service

Provide facilities to allow for delegation of access rights from requestors to services, as well as to allow for delegation policies to be specified. When dealing with delegation of authority from an entity to another, care should be taken so that the authority transferred through delegation is scoped only to the task(s) intended to be performed and within a limited lifetime to minimize the misuse of delegated authority.

Based upon the aforementioned definition, delegation involves Credential Conversion and Authorization for Access Control services. There are two primary types of delegation that need to be addressed:

- Delegation of Addresses: This type of delegation could occur due to proxies, firewalls or gateways. The main requirements of such delegation are to be able to provide an audit mechanism that allows repudiation to the original address.

A good example of why this is needed is the email SPAM problem that we face today. It is difficult with address and email account spoofing to determine the actual sender of the original SPAM message.

- Access Privilege Delegation would typically result in the transformation of one entity's privileges to some type of Role Based set of privileges. Once the ability to audit the delegation is of primary importance.

2.1.1.6.1.1 *Technological Assessment and Relevant Specifications*

It is recommended that either RBAC or SAML be considered as appropriate.

Table 12: Relevant Specifications for the Delegation Service

Identification Number	Name	Comment
BCP 65	Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures	
RFC 1034	http://www.armware.dk/RFC/rfc/rfc1034.html Domain names - concepts and facilities	
RFC 1507	DASS - Distributed Authentication Security Service	
RFC 1591	http://www.armware.dk/RFC/rfc/rfc1591.html Domain Name System Structure and Delegation	
RFC 1608	Representing IP Information in the X.500 Directory	
RFC 1612	DNS Resolver MIB Extensions	
RFC 2230	Key Exchange Delegation Record for the DNS	
RFC 2276	Architectural Principles of Uniform Resource Name Resolution	
RFC 2535	Domain Name System Security Extensions	
RFC 2592	http://www.armware.dk/RFC/rfc/rfc2592.html Definitions of Managed Objects for the Delegation of Management	

Identification Number	Name	Comment
	Script	
RFC 2874	http://www.armware.dk/RFC/rfc/rfc2874.html DNS Extensions to Support IPv6 Address Aggregation and Renumbering	
RFC 3401	Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS	
RFC 3402	Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm	
RFC 3403	Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database	
RFC 3404	Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI)	
RFC 3405	Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures	
RFC 3761	The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)	
STD 13	Domain Name System	Recommended
ANSI INCITS 359-2004	Role Based Access Control (RBAC)	Recommended
OASIS Security Technical Committee	SAML 2.0: Security Assertion Markup Language Version 2.0	Recommended

2.1.1.7 Firewall Traversal

A major barrier to dynamic, cross-domain Grid computing today is the existence of firewalls. As noted above, firewalls provide limited value within a dynamic Grid environment. However, it is also the case that firewalls are unlikely to disappear anytime soon. Thus, the OGSA security model must take them into account and provide mechanisms for cleanly traversing them—without compromising local control of firewall policy.

There are several major issues with the use of firewalls:

- Firewalls are typically invasive and perform address translation without providing a useable audit record.
- Firewalls that have the ability to perform state-based inspection are not capable of analyzing the complex protocols that IECSA is considering.
- Firewalls are difficult to manage and must be monitored as part of the SMI process.

However, firewalls are deployed in order to protect critical infrastructure computational resources and should be deployed at inter-domain connectivity points. With this deployment strategy, how can one facilitate firewall transversal?

2.1.1.7.1.1 *Technological Assessment and Relevant Specifications*

There are three major types of firewalls:

- Transparent (see FIRE-01 and FIRE-02): These firewalls perform OSI layer 2 or 3 bridging and do not typically provide state inspection. However, they do not obscure addressing information and tend to be the fastest type of firewall when performance is measured in terms of packet throughput. Since these are transparent, these types are the easiest to transverse when properly configured.

This is the only firewall type that could possible meet the 4msec performance requirement.

- Non-Transparent: These firewalls typically perform the following functions: packet filtering and proxy service (e.g. address translation).
- Non-Transparent with Stateful Inspection: Same capability as non-transparent but has the additional ability to examine the contents of each packet. This is typically the lowest performance type of firewall when performance is measured in regards to packet throughput.

Firewall Transversal is automatically provided when Transparent Firewalls are utilized, however the issue still remains for both versions of non-transparent firewalls. The typical mechanism for allowing transversal (e.g. from outside a Security Domain to inside) is via a proxy service or a set of firewall supplied cookies. However, there are several issues about sending/receiving such information in the clear. Therefore, encryption is desired.

Current firewall transversal thoughts are to create a SSL/TLS tunnel (thereby verifying the remote node has certain access rights) and then using an internal proxy to enforce further privilege restrictions.

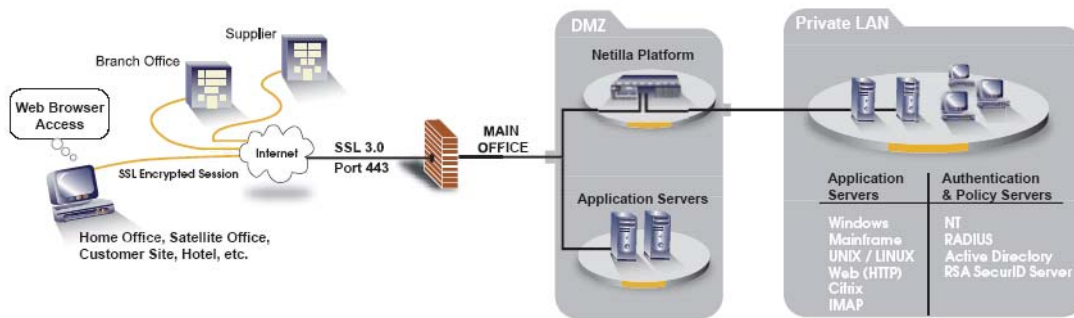


Figure 1: Example of SSL/TLS Tunnel for Firewall Transversal³

Figure 1 shows the SSL tunnel being used to a DMZ where the backend application data is proxied on servers located within the DMZ. It would also be possible to allow stateful and privilege proxy access directly to the back-end data providers if needed. Either architecture is viable and will be up to the Security Domain to decide which best meets its needs.

Whatever the choice, the functional characteristics found in RFC 2979 should be provided.

Table 13: References regarding Firewall Transversal

³ Image courtesy of Allegiant Data Systems

- FIRE-01 Matthew Tanase, **Transparent, Bridging and In-line Firewall Devices**, October 15, 2003
Available from: <http://www.securityfocus.com/infocus/1737>
- FIRE-02 Transparent Cisco IOS® Firewall
Available from:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gt_trans.htm

Table 14: Relevant Specifications regarding Firewall Transversal

Identification Number	Name	Comment
RFC 1579	Firewall-Friendly FTP	
RFC 1919	Classical versus Transparent IP Proxies	Recommended Reading
RFC 2008	Implications of Various Address Allocation Policies for Internet Routing	Recommended Reading
RFC 2401	Security Architecture for the Internet Protocol	
RFC 2505	http://www.armware.dk/RFC/rfc/rfc2505.html Anti-Spam Recommendations for SMTP MTAs	
RFC 2543	http://www.armware.dk/RFC/rfc/rfc2543.html SIP: Session Initiation Protocol	
RFC 2547	http://www.armware.dk/RFC/rfc/rfc2547.html BGP/MPLS VPNs	
RFC 2764	A Framework for IP Based Virtual Private Networks	
RFC 2775	Internet Transparency	Recommended Reading
RFC 2888	Secure Remote Access with L2TP	
RFC 2977	Mobile IP Authentication, Authorization, and Accounting Requirements	
RFC 2979	Behavior of and Requirements for Internet Firewalls	Recommended
RFC 2993	Architectural Implications of NAT	Recommended Reading

2.1.1.8 Identity Establishment Service

An identity establishment (e.g. identity authentication) service is concerned with verifying proof of an asserted identity. The implementation of the service must allow for multiple identity authentication mechanisms (e.g. identity tokens) to be utilized. Additionally, the service needs to provide a mechanism to allow the information from various identity tokens/identity authentication mechanisms to be electronically conveyed.

The requirement that the Identity Establishment service be agnostic in regards to technology can be easily demonstrated. One Security Domain may make use of a User ID/password combination as an identity

token. Another Security Domain may require the use of Kerberos based identity tokens. It is the Security Management Infrastructure (SMI) and the Security Domain's security policies that will determine the actual identity token(s) used and the mechanism(s) through which they are conveyed.

Key definitions:

identity authentication: The performance of tests to enable a data processing system to recognize entities. *Note:* An example of identity authentication is the checking of a password or identity token. [2382-pt.8]

identity token: 1. A device, such as a metal key or smart card, used for identity authentication. [After 2382-pt.8] **2.** [A] Smart card, metal key, or other physical object used to authenticate identity. [INFOSEC-99]

identity validation: Tests enabling an information system to authenticate users or resources. [INFOSEC-99]

2.1.1.8.1.1 Identity Establishment for Physical Assets

Physical access control should be based upon multi-factor Identity Establishment. The use of multi-factor authentication, using the appropriate technologies can provide a significant security advantage above and beyond simple identity cards. Additionally, the selection and creation of physical access control policies and procedures would need to include the capability to manage and revoke access privileges easily. This would typically indicate the need for some type of token/id that can be managed/changed. However, if only the picture matching the holder of the identity card determines access, there is a high probability that such access control mechanisms can be falsified. Thus, to improve access security there should be another security factor used in order to authorize access.

This "other-factor" should be "something the individual knows" (e.g. username/password) or combination code. However, typically username/passwords or combination codes can be compromised through observation or garbage diving. Therefore, it would be recommended that some type of electronic mechanism, with verification/challenge be implemented. The most widely deployed example of this would be the use of a Smart-ID card (e.g. a card that electronically authorizes the holder to enter a combination and that explicitly bound to the identity of the holder) and a combination lock. Only the proper Smart-ID badge authorization allows the combination to be entered into the lock, which then enables access. The side benefit of the use of such technology is that an audit trail of access can be created electronically. Additionally, management issues (especially revocation of access privileges) are eased since the Smart-ID card can be revoked thereby disallowing access.

Should a Security Domain decide to perform electronic auditing of physical access (recommended), then appropriate audit trail time-stamping techniques need to be utilized (see the audit service section).

2.1.1.8.1.2 Computational Resources

Identity establishment, for computational resources, is directly related to the types of credentials that are in use within a Security Domain. The definition of the credentials that IECSA may be using may be found in the Credential Renewal section (see page 2-18). The credential types used to establish identity are: addresses and address resolution, username/passwords, smart cards, digital certificates, and biometric identifications.

The issue with computational resource identification establishment is that of architecting a solution that creates a framework for authentication. Table 15 and Table 16 list relevant references and specifications that may aid in the construction of such a framework within a security domain.

Table 15: General References Regarding Identity Establishment and Identity Infrastructure

A National-Scale Authentication Infrastructure. R. Butler, D. Engert, I. Foster, C. Kesselman, S. Tuecke, J. Volmer, V. Welch. *IEEE Computer*, 33(12):60-66, 2000.

An Online Credential Repository for the Grid: MyProxy. J. Novotny, S. Tuecke, V. Welch. *Proceedings of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10)*, IEEE Press, August 2001.

A Community Authorization Service for Group Collaboration. L. Pearlman, V. Welch, I. Foster, C. Kesselman, S. Tuecke. *Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks*, 2002.

X.509 Proxy Certificates for Dynamic Delegation. V. Welch, I. Foster, C. Kesselman, O. Mulmo, L. Pearlman, S. Tuecke, J. Gawor, S. Meder, F. Siebenlist. *3rd Annual PKI R&D Workshop*, 2004.

Table 16: Relevant Specifications regarding Identification Frameworks

Identification Number	Name	Comment
ISO/IEC 10181-2:1996	Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework	Recommended
ISO/IEC 10181-4:1997	Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework	Recommended
ISO/IEC 10181-1:1996	Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview	Recommended
ISO 10202-8:1998	Financial transaction cards -- Security architecture of financial transaction systems	Recommended Reading

2.1.1.8.1.2.1 *Technological Assessment and Relevant Specifications*

The following section discusses issues and potential general resolution to the issues regarding the use of any particular identification mechanism. In general, two-factor authentication is desired.

2.1.1.8.1.2.1.1 Address Resolution

The most prevalent issue in using address resolution as an identification mechanism is address spoofing. This attack is easy to generate and is well documented. Therefore, such an identification mechanism should not be used on its own. It must be augmented with another factor to actually establish the identity. Address resolution is a worthwhile qualifier for actions/information exchanges that are only supposed to occur between certain peers. However, this is not a reasonable mechanism for inter-domain exchanges since neither domain controls the other domain's address allocation/changes.

2.1.1.8.1.2.1.2 Username/Password

This is a typical mechanism employed by Web based interfaces (especially for customers interfacing for retrieval of billing information). However, the use of cookies or password caches (e.g. the prompt to remember the username password) represents an issue that should be addressed by the addition of a challenge/response mechanism.

The challenge response should be user selectable/definable so that they can remember the response when prompted.

2.1.1.8.1.2.1.3 Smart Cards

The references given previously in this section give a large amount of guidance in the selection of SMART-CARDS that can be used in the implementation of physical or cyber access control. The smart card industry embraces ISO 7816 as one of the prevalent smart card specification and this is the recommended base specification for smart cards.

However, ISO 7816 does not specify a programmatic interface to such cards that is portable. Therefore, it is recommended that the Java Card™ Platform Specification be used in conjunction with ISO 7816 technology.

The remaining issue is how much storage to deploy on the smart cards. The Gartner Group published the information found in Figure 2. At this juncture there is no recommendation in regards to the amount of storage to deploy.

Table 17: Relevant Standards Concerning Smart Cards

Identification Number	Name	Comment
ISO/IEC 7816-1:1998	Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics	
ISO/IEC 7816-10:1999	Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards	
ISO/IEC 7816-11:2004	Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods	
ISO/IEC 7816-15:2004	Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application	
ISO/IEC 7816-3:1997	Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols	
ISO/IEC 7816-3:1997/Amd 1:2002	Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V	
ISO/IEC 7816-4:1995	Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Interindustry commands for interchange	
ISO/IEC 7816-4:1995/Amd 1:1997	secure messaging on the structures of APDU messages	
ISO/IEC 7816-5:1994	Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers	Highly recommended reading as part of the management (e.g. User/Group Management service)
ISO/IEC 7816-7:1999	Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured	

Identification Number	Name	Comment
	Card Query Language (SCQL) (available in English only)	
ISO/IEC 7816-8:1999	Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands	
ISO/IEC 7816-9:2000	Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes	
Java Card	Java Code Smart Card API	Can make use of ISO 7816 Based smart cards. Referenced by Global Platform and ETSI.
Java Card	Java Card Platform Specification v 2.2.1 Available from: http://java.sun.com/products/javacard/specs.html	
NIST GSC-IS	The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1 Available from: http://csrc.nist.gov/publications/nistir/nistir-6887.pdf	Recommended Reading. Specifies the use of ISO 7816 GSM based implementations.
Smart Card Alliance	Smart Card Primer Available from: http://www.smartcardalliance.org	Recommended Reading
Smart Card Alliance	Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology Available from: http://www.smartcardalliance.org	Recommended Reading
Smart Card Alliance	Government Smart Card Handbook Available from: http://www.smartcardalliance.org	Recommended Reading. Specifies the use of ISO 7816 based implementations.



Chip Comparisons

	Maximum Data Capacity	Processing Power	Cost of Card	Cost of Reader and Connection
Magnetic Stripe Cards	140 bytes	None	\$0.20 - \$0.75	\$750
Integrated Circuit Memory Cards	1 Kbyte	None	\$1 - \$2.50	\$500
Integrated Circuit Processor Cards	8 Kbytes	8-bit cpu, moving to 16- and 32-bit	\$7-\$15	\$500
Optical Memory Cards	4.9 Mbytes	None	\$7 - \$12	\$3,500 - \$4,000

Source: Gartner Group

Figure 2: Estimated Smart Card Storage Costs

2.1.1.8.1.2.1.4 Digital Certificates

The industry accepted digital certificate is an X.509 certificate. This is the certificate format that should be used by IECSA when applicable. There are some issues in identifying a certificate:

- There is an issue in regards to how to uniquely identify a certificate. There are many fields that could be used, however only the certificate Thumbprint is truly unique. All other fields could be non-unique. Therefore, it is the thumbprint that should be used to identify and match certificates.
- Enunciation of lifetime expiration (see Credential Renewal service).
- Policy issues in regards to use will need to be addressed. The NERC e-Marc certificate policy discusses many of these issues. It is recommended that the e-Marc policy be used as a basis for certificate usage.

It is worthwhile to note that the NERC policy does not allow the same certificate to be duplicated. Should a security domain adopt this as a policy, the number of certificates required (e.g. in the case of redundancy) will be higher.

- A policy in regards to how applications should react in the case that an in use certificate is revoked.

Revocation is basically caused when the integrity of a certificate has been compromised (e.g. the private certificate may have been stolen). Since none of the revocation protocols give an indication that could be used to determine if the certificate was compromised prior to use, the safe option is to terminate use of the certificate upon revocation. This may cause information exchange to be terminated if fail-over procedures are not made part of the policy.

Table 18: Public Key Infrastructure (PKI) Related Specification/Standards

Identification Number	Name	Comment
RFC 2898	PKCS #5: Password-Based Cryptography Specification Version 2.0. B. Kaliski. September 2000.	
RFC 2985	PKCS #9: Selected Object Classes and Attribute Types Version 2.0. M. Nystrom, B. Kaliski. November 2000.	
RFC 2986	PKCS #10: Certification Request Syntax Specification Version 1.7. M. Nystrom, B. Kaliski. November 2000.	
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	
ISO/IEC 9594-8:1998	Information technology -- Open Systems Interconnection -- The Directory: Authentication framework	Definition of X.509 Certificate is found here.
ISO/IEC 9594-8:2001	Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks	
X.521	TMN PKI - Digital certificates and certificate revocation lists profiles	
NERC	Certificate Policy for the Energy Market Access and Reliability Certificate (e-MARC) Program Version 2.4	
	Available from: ftp://www.nerc.com/pub/sys/all_updl/cip/pkitf/e-MARC-PKI_draft_version_V2-4b_March_2003-rev1.doc	

2.1.1.8.1.2.1.5 Digital Signatures

Typically considered a subset of Digital Certificates, as certificates are required in order to digitally sign, these have their own benefit for identification purposes. In instances where bandwidth or packet size is a limiting factor, a digital signature can be used in place of a certificate.

In IEC 61850, for GOOSE, this signature, in conjunction with address resolution would provide two-factor authentication if properly implemented. However, this raises the issue that:

- Digital signatures should not repeat often in order to prevent spoofing.

There are several different interpretations in regards to what a digital signature is.

It is recommended that RFC 2313 be used as the definitive definition for a digital signature algorithm:

“For digital signatures, the content to be signed is first reduced to a message digest with a message-digest algorithm (such as MD5), and then an octet string containing the message digest is encrypted with the RSA private key of the signer of the content. The content and the encrypted message digest are represented together according to the syntax in PKCS #7 to yield a digital signature.”

However, it is recommended that RFC 2437 be the actual Cryptography specification used⁴

Table 19: Relevant Specifications for Digital Signatures

Identification Number	Name	Comment
RFC 2313	http://www.armware.dk/RFC/rfc/rfc2313.html PKCS #1: RSA Encryption Version 1.5	
RFC 2315	PKCS #7: Cryptographic Message Syntax Version 1.5	
RFC 2437	PKCS #1: RSA Cryptography Specifications Version 2.0	

2.1.1.8.1.2.1.6 Biometrics

There is a large body of biometric work occurring. The standards development is largely being performed in ISO JTC1 SC37. The total scope of work can be obtained from www.jtc1.org. However, some of the major work items have been included in Table 20. The major focus of ISO JTC1 SC37 is focused on the biometric aspects of fingerprints and facial images. However, from a practical perspective fingerprint biometrics represents a much lower cost alternative than facial and therefore would be recommended for IECSA deployment.

It is also suggested that the biometric data be encoded on a smart-card so that two-factor authentication is achievable.

Table 20: Relevant References regarding Biometrics

Global Analytic Information Technology Services	Fingerprint Recognition Available from: http://www.gaits.com/biometrics_fingerprint.asp
	Ralph Gross, Quo Vadis Face Recognition? The current state of the art in Face Recognition Available from: http://dagwood.vsam.ri.cmu.edu/FaceRecognition/ Philip E. Agre, Your Face is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places.
ISO JTC1 SC37	SD 2 - Harmonized Biometric Vocabulary
ISO JTC1 SC37	1.37.19784.1 BioAPI - Biometric Application Programming Interface
ISO JTC1 SC37	1.37.19794 - Biometric Data Interchange Format
ISO JTC1	1.37.1974.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data

⁴ The definition was removed from RFC 2437.

SC37

ISO JTC1 1.37.1974.4 Biometric Data Interchange Format - Part 4: Finger Image Data
SC37

ISO JTC1 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data
SC37

Table 21: Relevant Specification regarding Biometrics and Smart Cards

Identification Number	Name	Comment
ISO/IEC 7816-11:2004	Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods	Recommended Reading

2.1.1.9 Identity Mapping Service

The identity mapping service provides the capability of transforming an identity that exists in one identity domain into an identity within another identity domain. It is worthwhile to note that there may be multiple identity domains within a single Security Domain. There is an additional attribute to identity mapping, the mapping may result in either a mapping of an individual into another set of credentials that represent the individual (but for a different resource) or in a mapping to a role/group based identity for the resource.

As an example, consider an identity in the form of an X.500 Distinguished Name (DN), which is carried within an X.509v3 digital certificate. The combination of the subject DN, issuer DN and certificate serial number may be considered to carry the subject's or service requestor's identity. The scope of the identity domain in this example is considered to be the set of certificates that are issued by the certificate authority. Assuming that the certificate is used to convey the service requestor's identity the identity mapping service via policy may map the service requestor's identity to an identity that has meaning (for instance) to the hosting environment's local platform registry. The identity mapping service is not concerned with the authentication of the service requestor; rather it is strictly a policy driven name mapping service.

The Identity Mapping can occur due to Credential Conversion or local/programmatic reasons. The major issues with Identity Mapping are very similar to the issues in Credential Conversion:

- There needs to be an audit mechanism inserted into the mapping process so that the originator of the transaction can be identified if needed.

2.1.1.9.1.1 *Technological Assessment and Relevant Specifications*

Relevant specifications and references may be drawn from the Identity Establishment, Credential Conversion, and Firewall Transversal services. In order to be concise, they will not be repeated in this section. This section will only contain additional recommendation above and beyond the other service recommendations.

2.1.1.9.1.1.1 *Address Mapping*

It is recommended that Network Address Translation be used as part of the non-Transparent Firewall deployment. However, in the use of NAT or most non-Transparent firewalls, there is an issue of providing a proxy for multiple “protected addresses” into the public address space. It is recommended that firewalls be evaluated for their capability to proxy and map multiple addresses as it may save deployment and management cost.

2.1.1.9.1.1.2 UserName/Password

Although there are no relevant standards/specifications pertaining to this issue, the most natural mapping service is through the use of single sign-on (SSO). However, this does not truly represent the true Identity Mapping (although it is credential mapping).

2.1.1.9.1.1.3 Digital Certificates

See the discussion in the Credential Conversion service discussion.

2.1.1.10 Information Integrity Service

Ensure that unauthorized changes made to messages or documents may be detected by the recipient. The use of message or document level integrity checking is determined by policy, which is tied to the offered quality of the service (QoS).

Key definitions:

integrity: [In INFOSEC, the] quality of an information system (IS) reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. [INFOSEC-99]

The first thought, when it comes to Integrity, is that it is the same issue as Confidentiality. However, the Confidentiality Service provides protection from information disclosure not the detection of information modification. It is the protection from information modification that the Integrity Service represents.

In order to provide message integrity, an algorithm that generates a result similar to a CRC needs to be executed and imbedded in the message. However, this alone will not guarantee integrity as a man-in-the-middle attack could change the message, recalculate the CRC, and then forward the message.

In order to prevent man-in-the-middle attacks, a digital signature is typically used on the CRC like result and both are embedded in the message. It is this digital signature “seal” that actually prevents the attack. Such signatures are typically referred to as Message Authentication Codes (MACs) and it is recommended that the Integrity Service be implemented through the use of such techniques.

2.1.1.11 Inter-Domain Security

This service represents the capability to provide additional security services, as needed, in order to facilitate inter-domain information exchanges. These additional security services may not typically be required for intra-domain exchanges

The additional security services that must be provided for Inter-Domain security are:

- Confidentiality
- Credential Conversion
- Delegation
- Firewall Transversal
- Identity Mapping
- Security against Denial of Service

Additionally, a much more robust audit mechanism should be instituted at the inter-domain boundaries.

2.1.1.12 Non-repudiation

This service represents the ability of a security domain to provide proof that a given exchange action has occurred. This ability is used to resolve disputes with other entities that claim that the action did not occur, thus non-repudiation. In order to provide this service, a strong audit service must be present within the security domain.

Key definition:

repudiation: In cryptosystems, the denial by one of the entities involved in a communication of having participated in all or part of the communication.

In order to provide this service, strong audit capabilities need to be in place for Identity Establishment, Access Control, Credential Conversion, and Identity Mapping. Without an appropriate level of audit capability on these other services, non-repudiation will not be able to be performed.

Non-repudiation is typically a manual process of retrieving the relevant audit records, analyzing those records, creating a report that summarizes those records and the conclusion. Thus, strong policies and procedures must be put in place to accomplish non-repudiation as well.

2.1.1.12.1.1 *Technological Assessment and Relevant Specifications*

Table 22 shows the relevant specifications regarding non-repudiation. In order to provide the non-repudiation service, it is suggested that a non-repudiation framework similar to what is specified in ISO/IEC 10181-4 be created. It is further recommended that SAML be used and the non-repudiation capabilities of SAML be integrated into the created framework.

Table 22: Relevant Specification regarding non-repudiation

Identification Number	Name	Comment
ISO 9735-5:2002	Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)	

ISO/IEC 10181-4:1997	Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework	Recommended
ISO/IEC 13888-1:1997	Information technology -- Security techniques -- Non-repudiation -- Part 1: General	Recommended Reading
ISO/IEC 13888-2:1998	Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques	
ISO/IEC 13888-3:1997	Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques	
ISO/IEC TR 13335-5	Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security	
WC3	XML Key Management Specification (XKMS 2.0) Bindings	
OASIS Security Technical Committee	Bindings for OASIS Security Assertion Markup Language (SAML) V2.0 Available from: http://www.oasis-open.org/committees/download.php/6773/sstc-saml-bindings-2.0-draft-11-diff.pdf	Draft that specifies how to bind SAML over various protocols. Highly recommended.

2.1.1.13 Path Routing and QOS Service

This service represents the ability of a security domain to applications with the ability to request that a set of transactions be conveyed over a specific communication path with specific Quality of Security (QS) being provided. Such a service may be used in conjunction with many of the other security services.

There are two major issues that need to be resolved:

- The ability to specify the actual communication path that a given transaction will use.

This type of ability is a direct contradiction to the normal dynamic routing inherent in most networks, thus normal network infrastructures may not be able to be used.

- The ability to request a Quality of Security to be guaranteed over that path.

2.1.1.13.1.1 *Technological Assessment and Relevant Specifications*

2.1.1.13.1.1.1 *Communication Path Definition*

Although there are several IETF RFCs regarding the ability to perform this function (e.g. RFC 1940), few if any of the operating system APIs allow the full path specification to occur. In reality, the source routing

bit can be set TRUE and the packet will be delivered to the peer with the path hop information embedded within it. Such a mechanism could allow the receiver to determine if a packet was delivered over an acceptable path, and this is a useful check.

However, the ability to actually pre-determine the path that a packet will transverse falls upon manual configuration of static routing. It is this static routing that can actually allow policy to dictate what route a given communication packet will take. Typically, this is a configuration option in Firewalls or Operating Systems. Thus it is incumbent upon the SMI function to provide the appropriate configuration.

2.1.1.13.1.1.2 *Quality of Security*

There are no known Quality of Security standards/specifications available to allow packet routing based upon a requested level of security. Development of a similar specification to RFC 2386 (Quality of Service based Routing) is recommended.

Table 23: Relevant Specifications for the Path Routing Service

Identification Number	Name	Comment
RFC 1102	Policy routing in Internet protocols	Highly Recommended
RFC 1322	A Unified Approach to Inter-Domain Routing	
RFC 1940	Source Demand Routing: Packet Format and Forwarding Specification (Version 1)	Highly Recommended
RFC 2386	A Framework for QoS-based Routing in the Internet	Highly Recommended
RFC 2725	Routing Policy System Security	Highly Recommended

2.1.1.14 **Security Policies**

The Security Domain's policy service is concerned with the management of policies. The aggregation of the policies contained within and managed by the policy service comprises a Security Domain's policy set. This service is also responsible for the enforcement of the domain's policy for intra-domain and inter-domain exchanges. The policy service may be thought of as another primitive service, which is used by the authorization, audit, identity mapping and other services as needed.

General Process

The policy service is a process through which a Security Domain determines its risks vs. costs in order to protect critical assets. The policy development must encompass:

- A **Requirements** analysis process which is used to determine the critical assets that need protection, security needs of the Security Domain, technological choices for implementation, security management and monitoring requirements, audit capability, and non-repudiation capability.

- The **Implementation** process that monitors and tests the policies as they are implemented. If there are problems detected during implementation, the policy should be revised and requirements should be revisited.
- The **Monitoring** process is responsible for the detection of security attacks, detection of security breaches, and the performance of the installed security infrastructure. This process is critical to the overall effectiveness of security.
- The **Analysis** process is responsible for determining when the deployed security measures need to be re-evaluated. This re-evaluation may be required due to environment, legal, or internally developed metrics.

There is a relevant body of work that can be found in EPRI Report 1008988, Scoping Study on Security Processes and Impacts. The following is a summarization of that work.

Security Policy Requirements

A policy must determine what assets need to be protected, determine what attacks need to be mitigated, how to mitigate the attacks including technology and procedural, and how to detect attempted attacks.

- **Asset Protection:** In order to determine which assets need to be protected, all aspects of the “value” of an asset needs to be determined. This means that legal, community good will, asset value, and cascade effects (if an attack did compromise a particular asset) need to be taken into account. Since it is not possible to secure every asset in the infrastructure, it is recommended that the high risk or high-value assets be protected first.
- **Determining what Attacks to Mitigate:** The requirements process must determine what is the cost/benefit/probability of a successful attack and what form such an attack might take. The higher the probability of success indicates the higher need for mitigation.
- **Mitigation Strategies:** The security services, discussed in this report, provide suggestions in regards to how to mitigate many of the threats. It is up to each security domain (SMI) to determine the best method to mitigate the attack and then write the appropriate policies to reflect that intent.
- **Attack Detection:** Since there is no absolute security, detection of an attempted attack is an important objective of any security policy. For each asset being secured, a mechanism for detecting attempted/successful attacks needs to be part of the policy and it **MUST** be implemented and monitored on a constant basis.

As part of the requirement process, ISO/IEC 15408 (e.g. the standardized version of the NIST Common Criteria) should be used as a basis for the technological requirements assessment and determining threats and mitigation strategies.

The requirements phase of policy development must also take into account risk assessment.

Risk Assessment/Analysis

“The classical definition of Risk Analysis is one that describes it as a process to ensure that the security controls for a system are fully commensurate with its risks.”⁵

Translated, this means that the amount of security deployed should be related to the overall asset value (including collateral assets that could be effected⁶). Thus, risk analysis provides a

⁵ From: <http://www.eon-commerce.com/riskanalysis/whatis.htm>

⁶ For electric utility infrastructures, a successful security attack could impact other infrastructures. Therefore, infrastructure impact on other infrastructures and the public must be taken into account during the risk assessment. EPRI Report 1008988 provides a more detailed discussion.

mechanism to determine which assets should be protected immediately (based upon relative worth) and not require that all Security Domain assets be secured.

Some of the other documented benefits of performing risk assessment are:

- Provides a means to cost justify security investments.
- Breaks down business boundaries and build business relationships.

Business management would be responsible to determine the security risk level that would be tolerable for a particular asset. IT/Security staff would need to work with the management team to determine the cost/solution. Based upon both factors, a cost/security ratio could be developed and used as a metric.

- Risk Analysis allows security to be analyzed from a business needs perspective and not just from a technological solution basis.
- The team risk analysis activity raises the security awareness to a greater number of personnel.
- Provides a mechanism to evaluate security in a “consistent” manner.
- Facilitates communication between different business entities.

Fault Tolerance

Security issues can impact the fault tolerant aspect of systems. There are two(2) prevalent issues that need to be considered in determining a fault tolerance policy:

- System Availability.
- Denial of Service created by successful security attacks.

Policies and system designs must accommodate these issues.

Implementation

As the selected assets are secured, tests should be executed to make sure that the created policies and deployed technologies actually perform as desired. If not, new policies reflecting new requirements need to be generated. Therefore, test procedures need to be considered as part of the policy development cycle.

As an example, the policies and procedures for physical access should be tested on an un-announced basis. This should be written into the policy as well as the maximum re-test interval allowed. Additionally, the expected results of such tests should be documented. If the expected results are not obtained, an analysis of the causes for not achieving the expected results needs to occur. If the analysis indicates that the policy is in error, then the policy needs to be revised.

Analysis

Policies and procedures need to be written to state how often re-analysis of the existing policies and security infrastructure needs to occur (given no successful attack or repeated attempted attacks being detected). The policy for re-analysis needs to recognize that shifts in the world political environment (just think of before 9/11 versus now) and technology advances all need to be taken into account.

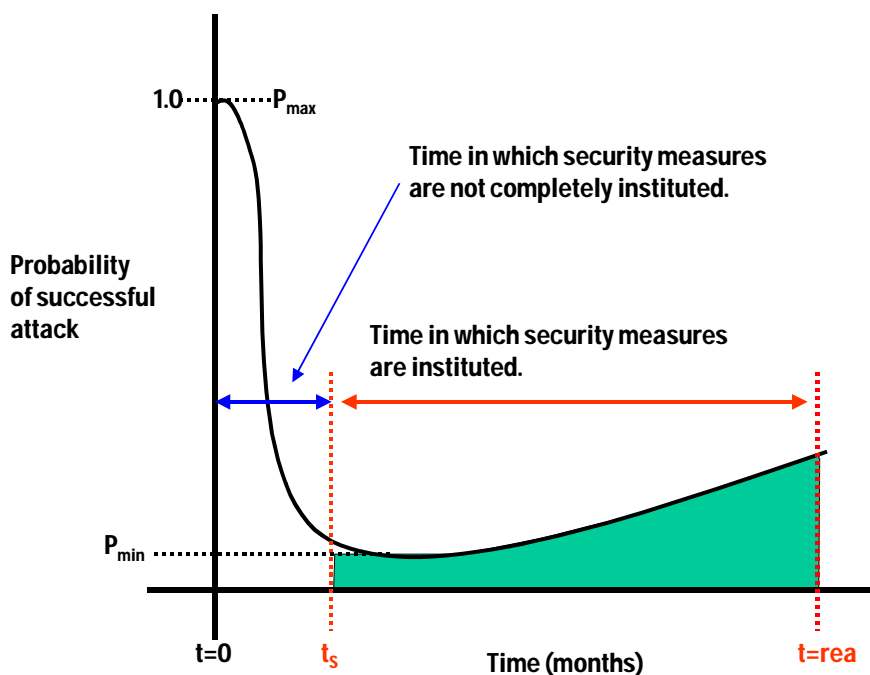


Figure 3: General trend is security vulnerabilities (extracted from EPRI Report 1008988)

Figure 5 shows the probability of a successful attack. It depicts a high probability prior to security measures being implemented. At the time the security measures are implemented, this represents the “lowest” probability of successful attack if the security process has worked properly. However, the figure accurately reflects that over time the probability of successful attack increases. Thus it is important to understand and specify the periodicity of security re-evaluation in order to keep the probability of successful attack at an acceptable level.

Thus the aforementioned represent the general types of problems that must be faced when developing an overall Security Domain security policy. However, there are technology specific policies that also need to be addressed.

Note: ISA-99, Integrating Electronic Security into the Manufacturing and Control Systems Environment is a document worth reading. It discusses, in more detail, the aspects of policy development.

PKI Infrastructure Policy and Issues

Note: This section is intended as a simple discussion of the issues regarding PKI. There are more authoritative documents available from NIST or NERC.

The purpose of the Public Key Infrastructure is to allow the establishment of Trust through the binding of encryption keys (typically “public” keys) and identities. In order to understand how PKI works, it is first important to that PKI to understand the three prevalent types of encryption: symmetric, asymmetric, and public/private.

- Symmetric encryption refers to the fact that both peers have the knowledge and use the same encryption key. Since both peers have and use the same key, symmetric encryption does not lend itself to unambiguous bindings (e.g. one key to a particular application/entity), thus symmetric encryption should not be used as the Trust establishment binding (e.g. should not be used within a PKI environment).
- Asymmetric encryption refers to the fact that each entity has its own key. Unlike symmetric encryption, asymmetric keys can allow for unambiguous identity establishment. However, since cooperating peers would need to have knowledge of the

other peer's key, it is often difficult to protect the identifying key. Although asymmetric keys could facilitate a PKI environment, the use of such keys for identity binding is not recommended since the keys must be disseminated/configured on multiple peers and therefore a prone to being compromised.

- Public/Private key encryption works on the basis that the use of the public key allows the decryption of information encrypted with the private key. Conversely, information encrypted with the public key can only be decrypted with the private key. It represents a specialization of asymmetric encryption.

The use of public/private key encryption can be used for two purposes: encryption and digital signatures.

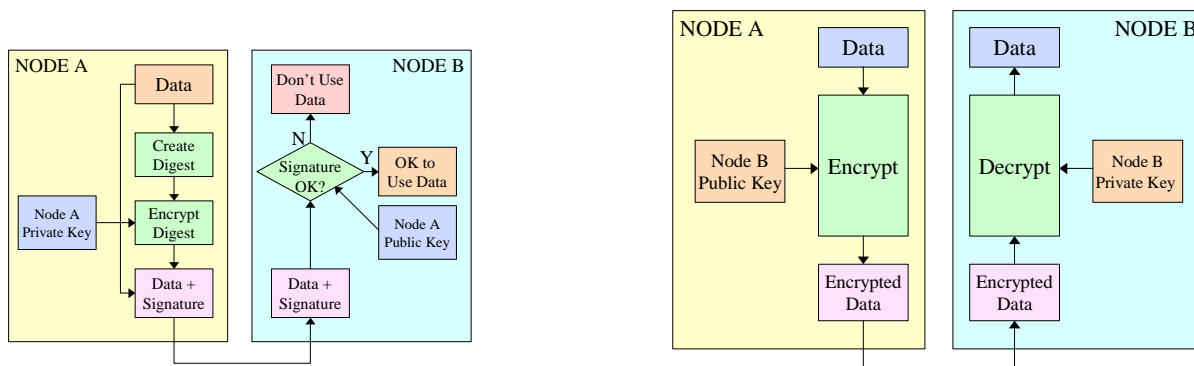


Figure 4: Simplified diagram of Public/Private Key encryption and Digital Signature

Figure 6 shows in order to Node A to encrypt data to be sent to Node B, the use of Node B's public key is required. It also shows that only the holder of Node B's private key can decrypt the information (neglecting encryption attacks). Likewise, the Digital Signature exchange shows that Node A's signature is decoded by Node B through the use of Node A's public key. Thus for both encryption and digital signatures, only public keys need to be exchanged and therefore it becomes easier to control and protect the private keys. Thus public/private key based PKI systems should be the preferred approach.

Obviously, it is critical to have a robust PKI infrastructure:

- Create the appropriate bindings between public/private keys and identification.

The typical mechanism for the bindings is through a digital X.509 certificate. A public certificate that includes the public key is created, and an equivalent is created as the "private certificate" that contains both the private and public keys. It is the creation of these two "certificates" that are typically the responsibility of a Certificate Authority (CA).

The protection of the public certificate/key is not that important, but the protection of the private key/certificate is. It is the responsibility of the CA to provide adequate protection during the generation process and to protect this information even if the certificate has been sent to the actual user.

Since the CA is the "root" source of the certificate, it is important that the CA also provide Certificate Revocation List (CRL) ability so that compromised or stolen certificates can be revoked.

- The user of a "private certificate" must provide security mechanism to protect the private information.

The actual mechanism for Security Domain/user archiving is a local issue, but great care needs to be taken during the policy establishment to be able to quickly and properly detect if there has been un-authorized access to the Security Domain private certificates. The policy must include the appropriate mechanism/procedures for reporting the compromised certificate and revoking its use locally.

- Even though the public certificates do not have the same criticality, the Security Domain policy should address the procedures for releasing the public certificate for use.
- A mechanism for tracking the lifetime expiration date in advance to actual expiration needs to be addressed.

Policies/procedures for replacement and renewal of older certificates (prior to expiration) or revoked certificates needs to be developed.

Of particular concern in IECSA, and the utility industry, is how to provide an appropriate revocation capability for a Security Domain. There are several design criteria for such an infrastructure:

- The infrastructure must be able to accommodate revocations of certificates that have been issued from more than one CA.

There is no central CA for the utility industry, or the world, and it does not appear that there is movement towards such an entity. Even NERC, in its e-Marc program, intends to allow certificates from multiple (although “certified”) CAs to be used. If a insecure CA is selected, problems can occur as is demonstrated in the following example

Example: (from <http://www.iona.com/support/docs/e2a/asp/5.0/corba/ssl/html/OpenSSL2.html>)

WARNING:

Most of the demonstration certificates supplied with CORBA SSL/TLS are signed by the CA `abigbank_ca.pem`. This CA is completely insecure because anyone can access its private key. To secure your system, you must create new certificates signed by a trusted CA. This chapter describes the certificates required by an CORBA SSL/TLS application and shows you how to create those certificates.

- Many of the certificate using computational resources will not be allowed direct access to the Internet that would be required in order to query the CRL of a particular CA.

Additionally, CRLs can be large and can consume bandwidth and be computationally intensive.

- An ability to determine if a particular Certificate has been revoked.

The X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC 2560) allows such a capability. It is worthwhile to note that OCSP is a request/response-oriented protocol (e.g. the certificate user must request to check if a certificate has been revoked).

However, the fact that OCSP is request/response means that there is an issue of timeliness in revocation information. However such a protocol/procedure does not exist today. In a future time, it could be envisioned that a central Security Domain revocation server (not a CRL server) could be created with the following attributes:

- Allows certificate users to register that certificates are in the user certificate cache.
- The Revocation Server would query the CAs CRL servers and process the revocation list(s).
- Based upon the CRL processing, the Revocation Server would notify the certificate user that the particular certificate has been revoked.

- Optionally, such a Revocation Server could alert Security Domain management that a certificate of a particular user is about to expire so that corrective action could be taken.
- Optionally, such a Revocation Server could respond to OCSP requests so that newly configured certificates could be validated as still being valid.

It is believed that work on such an entity is needed to allow more timely delivery of revocation information and to allow automation of such tasks.

2.1.1.15 Policy Exchange

Allow service requestors and providers to exchange dynamically security (among other) policy information to establish a negotiated security context between them. Such policy information can contain authentication requirements, supported functionality, constraints, privacy rules etc.

Typically, there has been no defined framework or policy exchange mechanism available that is technology neutral and therefore such exchanges have not occurred or have been performed manually. There are several issues that have prevented the development of such a framework:

- Agreement in regards to what constitutes security policy varies. Therefore, such an exchange mechanism would need to provide basic attribute definitions and also allow for a large amount of customization.
- There has not been a single secure and ubiquitous technology available over which to perform such an exchange.

2.1.1.15.1.1 *Technology Assessment and Relevant Specifications*

When analyzing how to exchange policies in the IECSA environment, the problem of having a ubiquitous technology has not been solved. There still does not appear to be a solution that can solve policy exchange issues in the Transmission & Distribution environment (especially serially connected devices), spanning to databases, to web technology. However, there are emerging specifications in how to perform such exchanges when web services/SOAP infrastructures are available.

For policy exchanges via SOAP, it is recommended that the WS-Policy, WS-PolicyAssertions, and WS-PolicyAttachment specifications form the basis of such exchanges. It is also recommended that customizations be kept to a minimum in order to maximize interoperability and interworkability.

Table 24: Relevant Specification regarding Policy Exchange

Identification Number	Name	Comment
OASIS	Web Services Policy Framework (WS-Policy) Available from: http://xml.coverpages.org/ws-policyV11.pdf	Recommended
OASIS	Web Services Policy Assertions Language (WS-PolicyAssertions) Available from: http://xml.coverpages.org/ws-policyassertionsV11.pdf	Recommended
OASIS	Web Services Policy Attachment (WS-PolicyAttachment) Available from:	Recommended

Identification Number	Name	Comment
	http://xml.coverpages.org/ws-policyattachmentV11.pdf	

2.1.1.16 Privacy Service

The privacy service is primarily concerned with the policy driven classification of personally identifiable information (PII). Service providers and service requestors may store personally identifiable information using the Privacy Service. Such a service can be used to articulate and enforce a Security Domain's privacy policy. Allow both a service requester and a service provider to define and enforce privacy policies, for instance taking into account things like personally identifiable information (PII), purpose of invocation, etc. (Privacy policies may be treated as an aspect of authorization policy addressing privacy semantics such as information usage rather than plain information access.)

Many may consider privacy equivalent to confidentiality/encryption, however this is not true. In reality, privacy is an issue regarding the PII after a secure transfer of that information occurs. The issue relevant, mostly to web technology, is how to determine in advanced if the privacy offered by a web site is sufficient.

2.1.1.16.1.1 *Technological Assessment and Relevant Documents*

A review of relevant information reveals that there are many well know legal/legislative aspects to privacy and disclosure of that information. However, there is little relevant work in regards to being able to determine and enforce the level of privacy electronically. The sole exception, that has maturity, is the P3P specification from W3C. References PRIV-01 and PRIV-02 are recommended reading to allow the SMI/policy services to determine if P3P can be used/monitored within the Security Domain.

Other work in this are is highly recommended.

Table 25: References Regarding Privacy

PRIV-01	Web consortium backs P3P privacy standard Available from: http://www.cnn.com/2002/TECH/internet/04/18/p3p.privacy.idg/
PRIV-02	Web Privacy Standard: It's a Start Available from: http://www.pcworld.com/news/article/0,aid,94544,00.asp

Table 26: Relevant Specification regarding Privacy

Identification Number	Name	Comment
W3C	The Platform for Privacy Preferences 1.1 (P3P1.1) Specification W3C Working Draft 27 April 2004	Highly Recommended

2.1.1.17 Profile Service (User Profile Service)

The profile service is concerned with managing service requestor's preferences and data which may not be directly consumed by the authorization service. This may be service requestor specific personalization

data, which for example can be used to tailor or customize the service requestor's experience (if incorporated into an application which interfaces with end-users.) It is expected that primarily this data will be used by applications that interface with a person.

2.1.1.17.1.1 *Technological Assessment and Relevant Specifications*

Research and experience indicates the web user profiles are the trend. To experience this, use any of the commercial web portals (e.g. Yahoo®, MSN®, etc...). These all offer the ability to personalize the information displayed and the actual display format. However, it is doubtful that any of the current portal technologies make use of the Semantic Web specification.

It is recommended, when possible, that the Semantic Web specification be utilized when possible. If such an implementation is not feasible or costly, it is recommended to implement based upon some local means.

Table 27: Relevant Specifications regarding the Profile Service

Identification Number	Name	Comment
Semantic Web	Pervasive Computing Standard Ontology (PERVASIVE-SO) Guide -- Describing User Profile and Preferences Available from: http://pervasive.semanticweb.org/doc/2004-01-ont-guide/part1/	Highly Recommended
IEEE	IEEE Personal and Private Information (PAPI) draft standard	

2.1.1.18 Quality of Identity Service

This service allows an entity to determine the trust level associate with the identity being conveyed. This is of particular interest where the source Identity, of the original transaction, has been mapped several times.

This service represents a specific capability that could be viewed as a subset of the Identity Service. However, technical evaluations of existing solutions indicate that no solutions provide this ability and therefore are worthy of being defined independently so that the service requirement is not lost.

This is a service that is not widely recognized, although QID-01 makes a strong case for its need. The basic issue raised by QID-01 is that of the ability to trust an identity being established if the identity has been mapped or its credentials converted several times. At a minimum, without a mechanism for originator determination, there is a relevant issue. However, originator determination could be provided by and adequate audit mechanism, but this does not assist the receptor of a transaction. Thus there is a need to provide a mechanism to allow the receptor to determine a level of trust based upon the number of mappings that have occurred along the transaction path.

Table 28: References Relating to Quality of Identity

QID-01 Audun Josang, An Algebra for Assessing Trust in Certification Chains, Telnor R&D
email: audun.josang@fou.telenor.no

2.1.1.18.1.1 *Technological Assessment and Relevant Specifications*

There are two aspects in regards to Quality of Identity, the ability to determine the number of times that an identity has been transformed, which is a superset of the number of times that credentials have been converted.

There are no relevant specifications/solutions that can be applied to the generalized identity mapping issue, as many of these mappings are local issues.

However, in the particular case of digital certificate conversion, the SAML specification yields a possible solution. However, the solution would require that attribute definitions and attribute chaining be added to SAML's use within the IECSA environment.

There are no such solutions for username/password and it may be worthwhile to develop such a specification based upon the SAML principles.

For address based credentials, source routing offers a potential solution (see Path Routing and QS service).

Table 29: Relevant Specification for the Quality of Identity Service

Identification Number	Name	Comment
OASIS Security Technical Committee	Attribute Profiles for SAML 2.0 Available from: http://www.oasis-open.org/committees/download.php/6344/sstc-hughes-mishra-baseline-attributes-03.pdf	Incomplete, but is on the correct track.
OASIS Security Technical Committee	SAML 2.0: Security Assertion Markup Language Version 2.0	Recommended
OASIS Security Technical Committee	Bindings for OASIS Security Assertion Markup Language (SAML) V2.0 Available from: http://www.oasis-open.org/committees/download.php/6773/sstc-saml-bindings-2.0-draft-11-diff.pdf	Draft that specifies how to bind SAML over various protocols. Highly recommended.
OASIS Security Technical Committee	Authentication Context Available from: http://www.oasis-open.org/committees/download.php/6539/sstc-saml-authn-context-2.0-draft-04a-diff.pdf	Draft that is needed to establish identity within a SAML environment.

2.1.1.19 Security against Denial-of-Service

This service is for assisting in preventing a denial of service. This is not a service that can be invoked programmatically; rather it is a service that must be designed into the capabilities of a Security Domain or the implementations deployed within the domain.

Key definitions:

denial of service: 1. The prevention of authorized access to resources or the delaying of time-critical operations. [2382-pt.8] **2.** The result of any action or series of actions that prevents any part of an information system (IS) from functioning. [INFOSEC-99]

The overall issue is to understand what can allow denial-of-service and then to take steps to mitigate the causes. There are several general categories of denial-of-service attacks that need to be well understood:

- **Resource exhaustion:** Resource exhaustion is a denial-of-service attack that causes required resources to be un-available for the intended use when a valid transaction needs to be processed. The recent SYN FLOOD attacks represents a well known denial-of-service attack.

Resources that can be exhausted are virtual connections, memory, serial ports, TCP ports, etc. However these could be generalized into two categories: connectivity resources and computational resources.

- **Buffer overflow:** This type of attack causes a memory overrun to occur within a computational resource. The end result is typically the computational process terminates or becomes unstable. In reality, this attack exploits poorly implemented programs that actually allow for the overrun to occur without being properly trapped. Recent examples of this type of attack are the PING OF DEATH and some attacks on SNMP.
- **Protocol oversights:** In some protocols, not all state transitions may be defined. Exploitation of such oversights could allow a denial of service attack to cause a protocol deadlock situation.

As an example, from STD 62 (SNMP):

“Denial of Service

A Security Model need not attempt to address the broad range of attacks by which service on behalf of authorized users is denied. Indeed, such denial-of-service attacks are in many cases indistinguishable from the type of network failures with which any viable management protocol must cope as a matter of course.”

Basically is a statement that no DOS countermeasures need to be taken within the specification. This is typical of most standards.

- **Improper Coding Practice:** Both the Buffer Overflow and Protocol Oversight threats are sub-categories of the improper coding practice category. However, this category includes improper use of semaphores, threads, etc. that could be utilized to decrease performance/resource available to the point that a valid transaction could not be processed in a timely manner.

2.1.1.19.1.1 *Technological Assessment and Relevant Specifications*

In order to provide a denial-of-service attack protection, inter-domain connection points need to be well designed and monitored.

For connectivity resources, it is recommended that timeouts be implemented that are based upon valid traffic being transmitted/received through the connection point. Additionally, it is recommended that

through policy or coding practice that a peer remote is limited to the number of connectivity resources that it is allowed to consume.

For protocol oversights, it is recommended that prior to implementation the protocol(s) are analyzed for vulnerabilities and that these be addressed during the implementation phase. It is recommended that appropriate coding methodology be employed to prevent CPU resource exhaustion as well as protocol oversight vulnerabilities.

It is also recommended that as part of the policy/SMI of a security domain that implementations are tested for vulnerabilities with tools that are publicly available.

Table 30: Relevant Specifications regarding Denial-of-Service

Identification Number	Name	Comment
ISO/IEC 17799:2000	Information technology -- Code of practice for information security management	
ISO/IEC TR 13335-1:1996	Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security	
ISO/IEC TR 13335-2:1997	Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security	

2.1.1.20 Security Assurance Management

Explicitly recognize the need for manageability of security functionality within the IECISA security model. For example, identity management, policy management, key management, and so forth. The need for security management also includes higher-level requirements such as anti-virus protection, intrusion detection and protection, which are requirements in their own rights but are typically provided as part of security management.

2.1.1.20.1.1 *Technological Assessment and Relevant Specifications*

Security assurance is part of a Security Domain's policy and SMI. It is recommended that ISO/IEC 15408-3:1999 be the guideline for determining and assessing such a policy.

Table 31: Relevant Specifications regarding Security Assurance

Identification Number	Name	Comment
RFC 2401	Security Architecture for the Internet Protocol	
RFC 2196	Site Security Handbook	
RFC 2350	Expectations for Computer Security Incident Response	
ISO/IEC 15408-1:1999	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode	

Identification Number	Name	Comment
ISO/IEC 15408-2:1999	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements	
ISO/IEC 15408-3:1999	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements	Highly Recommended

2.1.1.21 Security Protocol Mapping

Security protocol mapping services, enabling distributed security protocols to be transparently mapped onto native platform security services for participation by platform resource managers not implemented to support the distributed security authentication and access control mechanism.

2.1.1.21.1.1 *Technological Assessment*

To date there has been no definition of abstract security services and their parameters.

The security work found in this appendix actually defines a set of services, but further modeling is required in fully specify the parameters that are conveyed within those services.

The issue involving the ability to map to different communication technologies will be mitigated if a full abstract model of the IECSA security services can be developed.

2.1.1.22 Security Service Availability Discovery Service

A Security Domain must provide a mechanism for an entity to discover what other security services are available for its use.

Within the IECSA architecture, such a service would be required for Inter-Domain usage where a-priori knowledge is not available. It would also be a mandatory service if Quality of Security routing became a reality.

2.1.1.22.1.1 *Technological Assessment and Relevant Specifications*

Although there is no immediately usable technology to accomplish this service, it is recommended that the WS-Policy series be extended to provide this capability. It should be fairly straightforward to model security service availability as policy (e.g. the Policy Attachment may need to be extended). At a minimum, the information required to be conveyed needs to be determined in advance of attempting to adopt WS-Policy.

Since the discovery service is needed inter-domain, it is reasonable to attempt to make use of Web Services at the domain interconnect points to provide this capability.

Table 32: Potentially Relevant Specifications in regards to Security Capability Discovery

Identification Number	Name	Comment
OASIS	Web Services Policy Framework (WS-Policy) Available from:	

Identification Number	Name	Comment
	http://xml.coverpages.org/ws-policyV11.pdf	
OASIS	Web Services Policy Assertions Language (WS-PolicyAssertions) Available from: http://xml.coverpages.org/ws-policyassertionsV11.pdf	
OASIS	Web Services Policy Attachment (WS-PolicyAttachment) Available from: http://xml.coverpages.org/ws-policyattachmentV11.pdf	

2.1.1.23 Setting and Verifying User Authorization

This service is for assigning and validating authority given to a user or a group of users in accessing/utilizing specific enterprise resources.

2.1.1.24 Single Sign On Service

Relieve an entity having successfully completed the act of authentication once from the need to participate in re-authentications upon subsequent accesses to an Open Grid Services Architecture (OGSA) -managed resources for some reasonable period of time. This must take into account that a request may span security domains and hence should factor in federation between identity domains and mapping of identities. This requirement is important from two perspectives: a) It places a secondary requirement on an OGSA-compliant implementation to be able to delegate an entity's rights, subject to policy (e.g., lifespan of credentials, restrictions placed by the entity) b) If the credential material is delegated to intermediaries, it may be augmented to indicate the identity of the intermediaries, subject to policy.

This service is a local combination of the Credential Conversion and Identity Mapping services.

2.1.1.25 Trust Establishment Service

This service represents the ability of one resource to determine if its peer can be trusted. In order to establish trust, well known identities and security policies must be used, additionally, if inter-domain trust establishment requires an analysis of the security policies and procedures of the peer security domain.

Key definitions:

trust: In cryptology and cryptosystems, that characteristic allowing one entity to assume that a second entity will behave exactly as the first entity expects. Note: Trust may apply only for some specific function. The critical role of trust in the authentication framework is to describe the relationship between an authenticating entity and a certification authority; an authenticating entity must be certain that it can trust the certification authority to create only valid and reliable certificates. [After X.509]

Trust establishment is implemented through the Identity Establishment and Quality of Identity Services.

2.1.1.26 User and Group Management

This is to define, assign, organize, control and maintain mapping for user and group identifiers within the enterprises.

2.2 Network and System Management Services

2.2.1 Enterprise Management Services

2.2.1.1 Inventory Management

This service tracks, maintains and provides the inventory information on network and system assets. Network and system inventory include: (i) hardware such as routers, switches, servers, facilities, customer premises equipment, desktop equipment; storage systems, and service provider or customer access points; (ii) software such as operations systems, data bases, applications, network and system software; and (iii) other scarce resources, such as IP address ranges, capacities, sites, etc. Inventory management should provide an accurate account of these resources and parameters such as ownership, versioning, installation status, configuration status, availability, etc. This service should provide visibility, traceability and control of the resources.

2.2.1.2 Communication System/Network Discovery

This service collects, analyzes, discovers and reports on the state of networks and systems, including the configuration status, capabilities, resource availability of system/network entities, addresses, services, and the interconnection pattern/ topology of the devices. Auto discovery services provide such information dynamically, although security considerations and virtual connectivity may cause problems with accuracy of returned information of auto discovery services. Discovery and Inventory management services are essential for proper execution of provisioning and maintenance as well as performance, fault and configuration management.

2.2.1.3 Routing Management

Routing management configures, selects and prioritizes routes for traffic and messages exchanged amongst various enterprise entities; implements specified routing policies and preferences; also provides support for route-reconfiguration, as well as necessary route diversity/fault-tolerance to fulfill QoS and route-service availability requirements. Routing is a network control mechanism by which a path is obtained for establishing communication between

a source and a destination. Routing management becomes more challenging in heterogeneous, multi-domain, multi-technology networks, with extensive business policies and stringent QoS and reliability requirements of various applications.

2.2.1.4 Traffic Management

Traffic management provides services on scheduling, prioritization and congestion control at various layers such as packet, flow, call, user, and application in order to manage and share resources such as the network bandwidth, system buffer and processor time in order to meet the quality of service requirements of applications. As networking and system features become more complex and application become more QoS sensitive, traffic management becomes more important and involved. For example, for real-time applications, with strict delay requirements, careful use of traffic management services which provide more detailed monitoring, scheduling, and intelligence is needed.

2.2.1.5 Traffic Engineering

Traffic engineering monitors traffic usage and growth trend and helps determine adjustments in network/system resource allocation accordingly. For example, logical data pipes connecting various end-points can be re-sized dynamically or quasi-dynamically based on SLA, application requirements, actual usage, or time-of-the-day/day-of-the-week traffic trends and patterns. Traffic engineering also supports the provisioning of redundancies to assure reliability requirements.

2.2.1.6 System/Network Health-Check Analysis

This service determines the set of system/network indicators needed to check the health of the network and system components. A component is considered not healthy if it is not working, is congested, or is under a security attack. Different indicators and thresholds may need to be considered for different conditions, The service determines threshold values, which if exceeded indicate health issues, and also determines health check intervals to efficiently monitor the resources without utilizing excessive network and system resources. For example, the availability of a system may be checked with sending periodic messages, the return status of the message will indicate its availability. To reduce resource consumption, some management mechanisms use traps, messages from management agents to managers, in order to report a fault as opposed to periodic health checks (polling).

2.2.1.7 System/Network Fault Diagnosis

Fault Diagnosis service provides mechanisms to determine the location of faults by running diagnostic tests on application/system/network entities. In order to diagnose root cause alarm filtering/correlation algorithms and fault data summarization and analysis may also be used. Sometimes, identification of the root cause may be difficult and require extensive analysis. In such cases, a partial diagnosis is done to locate and isolate the fault in order to restore service quickly, and a follow-up full investigation identifies the root cause. Many artificial intelligence and statistical approaches for fault diagnosis are suggested and embedded in intelligent agents of new enterprise management products.

2.2.1.8 System/Network Fault Correcting

Fault correcting provides mechanisms to correct faults after fault diagnosis. Fault correction service role is to provide an action plan and coordinate this with the other functions within the enterprise. Resulting fault correction action may include: fault isolation, device reset, SW re-initialization, issuing SW fault reports, reconfiguration, rerouting, removal of system/network entities, issuing trouble tickets, dispatching repair technicians and assisting technician in locating faults. Fault correcting actions need to be followed with testing in order to verify that the correcting action was effective.

2.2.1.9 Service Level Agreement (SLA) Determination and Maintenance

This service defines, provisions, enables, monitors, and maintains SLAs. It also may translate policies, rules, SLAs and user requirements to system/network performance objectives, device configuration, and management objectives. SLAs may specify required performance, such as packet loss less than 1%; reliability, such as system availability of 99.999%; security, such as need for authentication; and routing constraints, such as bypassing specific sites. With the introduction of more QoS sensitive applications, automation of this service and introduction of more intelligent components become more desirable. The service is needed for proper operations of various management functions such as performance management, and fault management.

2.2.1.10 System/Network Performance Analysis

This service determines the set of system/network performance indicators, threshold levels and monitoring intervals. It supports performance management functions. For example, processing time measurements on a system indicate whether the system is in overloaded or not, or measurements of traffic on a specific route determine its level of congestion. This service determines the frequency of measurements, and the processing and network traffic thresholds that will indicate excessive load.

2.2.1.11 System/Network Performance Diagnosis

Performance diagnosis determines and isolates the cause of performance problems based on the analysis of system/network statistics and measurements. Similar to fault diagnosis, identification of performance root-cause may be involved and require network/system-wide quality analysis and assessment. For example, it may be easier to help identify an alternative route in case of congestion, rather than identify the source for congestion. This service could also be deployed in a pro-active manner to identify potential performance issues in the future and perform corrective action such as capacity planning and capacity enhancements.

2.2.1.12 Performance Tuning/Correction

Following identification of performance problems, this service helps to fix performance problems, or support meeting performance SLAs, by means of system/network reconfiguration, traffic/message rerouting, parameter tuning, resource allocation, and resource re-adjustment. For example, an application which is not completing in time required, may be ran on a different platform or given higher priority on an existing platform. Similar to fault correction, performance correction action need to be followed by testing to verify that the corrective action was effective.

2.2.1.13 Accounting and/or Billing

This function helps define accounting metrics and specifies accounting information to be collected, such as resource usage by user/organization, or frequency of access to specific sites. It also supports the setting and modifications of accounting limits. It provides the “toll booth” measurements on traffic to make them available to a billing entity. It controls the storage of and the access to accounting information. Lastly, it generates accounting/billing reports regarding application/system/network resource usage.

2.3 Data Management Common Services

2.3.1 Data Management Common Services

2.3.1.1 Distributed Data Management Service

Management of distributed data archives that are stored at multiple sides can be very complex. In these cases the data can consist of a combination of flat files, relational databases, as well as data stored internally by applications. Much of the data changes over time, i.e. there are frequent updates. Users and applications need access to all authorized data. Performance is critical, but the data must “stay at home”. Coherence is critical, so caching must be done with great care. Audit trails must exist for all data updates. Data management and sharing is one of the most common and important uses of utility distributed systems. How do we manage data stores so that they may be accessed across a utility infrastructure? How do we cache data and manage its consistency? How do we index and discover data and metadata? These are all questions that are central to most current IECSA deployments. They are likely to become more important in the future.

2.3.1.2 Object Management Service

This service supports the creation and deletion of objects associated with resources being managed. The service supports the specification of attributes and their corresponding ranges associated with a resource. This service also includes the setting, modifying and examining of attribute values of a managed object. This service also manages the relationships between managed objects.

2.3.1.3 Address and Naming Management

This service assigns, maintains addressing and naming schemes for entities to be managed within the enterprise(s). It also includes the support of lookup services between address and names as well as translation/mapping across multiple address/naming schemes. Proper implementation of address and naming services is critical for systems with high point counts (tens of thousands to millions). Experience has shown that typical implementations of address and naming management services originally designed for small to moderate point counts do not scale well.

2.3.1.4 Generic Eventing And Subscription

A collection of dynamic, distributed services that must be able to notify each other asynchronously of interesting changes to their state. This service is generally thought of in terms of a publish/subscribe model. This event-driven, or notification-based, interaction service is a commonly used service for inter-object communications. In the notification service an entity disseminates information to a set of other services or devices without having to have prior knowledge of these other Services or devices. Characteristics of this service include:

- The entities that wish to consume information (which we call Notification Consumers) are registered dynamically with the service/entity that is capable of distributing information. As part of this registration process the Notification Consumers may provide some indication of the nature of the information that they wish to receive.
- The distributing entity disseminates information by sending one-way messages to the Notification Consumers that are registered to receive the information. It is possible that more than one Notification Consumer is registered to consume the same information. In such cases, each Notification Consumer that is registered receives a separate copy of the information.
- The distributing entity may send any number of messages to each registered Notification Consumer; it is not limited to sending just a single message. Note also that a given Notification Consumer may receive zero or more Notification Messages throughout the time during which it is registered.

2.3.1.5 Alarm Detection/Reporting

These functions support mechanisms such as polling, watch-dog timers, process traps, etc, to detect and report application/system/network faults. They also provide the logging of events and errors as well as the specification and enabling of logging filters. This service may utilize some of the mechanisms provided by the generic eventing and subscription service.

2.3.1.6 Instrumentation and Monitoring Service

Instrumentation and monitoring services, supporting the discovery of sensors in a distributed environment, the collection and analysis of information from these sensors, the generation of alerts when unusual conditions are detected, and so forth. This service is provided via a request/reply and/or a publish/subscribe oriented interface to support hierarchical browsing and querying of schema (class) and instance information about data.

2.3.1.7 Measurement Data Logging Service

This service supports the recording and distribution of time series measurements. That is sequences of repetitive measurements that can be correlated by time. The service may have different implementations based upon the time frame for which the information is obtained or must be logged/reported. For example, high speed, high point count measurements may require special considerations regarding the underlying protocol mapping required to implement the service and meet bandwidth, latency, and other performance requirements.

2.3.1.8 Remote Control

This service provides supervisory control over remote applications including program invocation services and the ability to load/upgrade remotely installed software. These services include concepts such as select before operate, verify before commit, and verify before execute. The remote control service typically is more sensitive to implementations of security services than other services and often makes heavy use of logging and reporting services to maintain audit trails.

2.3.1.9 Network Time

This service provides distributed time synchronization over a network. The implementation of a time synchronization service is very dependent upon the underlying resolution, accuracy, and integrity requirements of a specific application. Time synchronization services have been shown to be particularly susceptible to spoofing and must be taken into consideration when considering the security aspects of the service.

2.3.1.10 File Transfer

This is to distribute and upgrade software for system/network elements within the enterprise(s). The file transfer service is also used to exchange arbitrary data values that are in a proprietary format or other standardized format and represented as an arbitrary length collection of bytes. File transfer services typically include the ability to create, open, close, read, write, and delete files.

2.4 Common Platform Services

2.4.1 Common Platform Services

2.4.1.1 Component Registry Service

Registry Services provide the mechanisms for services to advertise their existence. This service is closely related to Component Discovery Service.

2.4.1.2 Component Lookup Service

Allows search for a service and download the code needed to access it;

2.4.1.3 Component Discovery Service

Clients require mechanisms for discovering available services and for determining the characteristics of those services so that they can configure themselves and their requests to those services appropriately. spontaneously find a community and join;

2.4.1.4 Component Initialization and Termination

This is to provide means and mechanisms to initialize, shutdown, re-initialization and reset various networks and systems operations.

2.4.1.5 Storage

This service is used to store data.

2.4.1.6 Resource Management

This service is used to arbitrate access to computer resources such as CPU time or memory access.

2.4.1.7 Transactions

This service is used to ensure that a system's distributed state stays consistent.

2.4.1.8 Checkpoint and Recovery

This service is used to help ensure that a system's distributed state stays consistent.

2.4.1.9 Workflow Service

Support the coordinated execution of multiple application tasks on multiple distributed resources;

3. Best Practices

3.1 Data Management Best Practices

3.1.1 Data Management Best Practices

3.1.1.1 Unified Modeling Language (UML)

URL: <http://www.omg.org>

Abstract Modeling in UML

Abstraction, the focus on relevant details while ignoring others, is a key to learning and communicating. Modeling is the process of abstracting from the morass of stuff to develop a coherent, multi-faceted vision. Because of this:

- Every complex system is best approached through a small set of nearly independent views of a model. No single view is sufficient.
- Every model may be expressed at different levels, ranging from highly abstract to the concrete.
- The best models are connected to reality.

The generally accepted methodology for software modeling is the Unified Modeling Language (UML), which has been endorsed by the Object Management Group (OMG), the leading industry standard for distributed object programming. UML is the standard language for visualizing, specifying, constructing, and documenting the artifacts of a software-intensive system. It can be used with all processes, throughout the development life cycle, and across different implementation technologies. UML combines the best of the best from Data Modeling concepts (Entity Relationship Diagrams), Business Modeling (work flow), Object Modeling, and Component Modeling

Vendors of computer-aided software engineering products are now supporting UML and it has been endorsed by almost every maker of software development products, including IBM and Microsoft (for its Visual Basic environment). UML is a standard notation for the modeling of real-world objects as a first step in developing an object-oriented design methodology, and is used as the language for specifying, visualizing, constructing, and documenting the artifacts of software systems, as well as for business modeling and other non-software systems. UML represents a collection of the best engineering practices that have proven successful in the modeling of large and complex systems.

The UML modeling methodology is very powerful in that it can be used from the highest overview levels to actual implementation code, and from the largest global project to a tiny enhancement project. The key benefit of using UML is that provides methodologies for visualizing the complex interactions that must be implemented in an invisible cyber world. It consists primarily of structured diagrams that are designed to illustrate different aspects of cyber behavior. A number of CASE tools exist for developing these UML models as well-structured diagrams. The different UML modeling concepts and types of diagrams are described below.

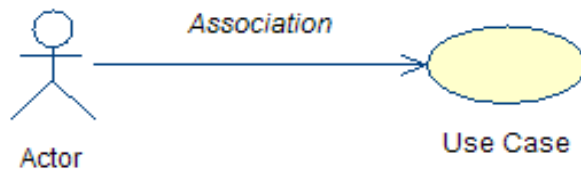
Use Cases

Use Cases are modeling constructs which focus on the interactions between functions and actors from a users point of view. The basic idea for a Use Case is to capture the requirements of these actors in relationship to the function. "Actors" are defined as the ultimate sources or users of information for a particular Use Case scenario, and do not need to be humans. For instance, the

power system can be seen as an Actor when it provides the source data for a SCADA system, while a billing system can be the user of metering data from an Automatic Meter Reading system.

Use Cases are layered or iterative in concept. For instance, in a Use Case diagram, a function is defined as a Use Case itself (which sometimes leads to confusion, but does emphasize the layered nature of Use Cases). As an example, in one Use Case diagram, the function "Distribution Automation Functions" could be defined as a single entity within distribution operations, while this same function could be expanded into its own Use Case, showing the individual functions as separate entities.

Therefore, the scope of a particular Use Case is entirely a function of what needs to be defined. In a broad picture Use Case, distribution system operations can be one function within utility operations. In a detailed picture Use Case, the Distribution Automation Volt/Var Optimization application can be the primary function. Therefore, often Use Cases are used first to define the overall Business Processes, and then are utilized to take each function within a Business Process and drill down to more detailed levels.



Modeling implies diagrams. Use Case Diagrams consist of Actors (often represented as little stick people) and Use Cases (ovals) linked by lines that indicate relationships, such as "is associated with", "is an aggregation of", or "is a generalization of". An association, which is

represented as a line with one or two arrows, provides a pathway for communication. The communication can be between use cases, actors, classes or interfaces. Associations are the most general of all relationships and consequentially the most semantically weak. If two objects are usually considered independently, the relationship is an association. Other relationships include "generalization" and "dependency".

The benefits of Use Cases include:

- Visualizing processes and interactions which otherwise might be obscure or lost in the complexity of a system
- Capturing requirements from user's perspective
- Users are not only involved in providing requirements, but can actually understand and validate what is being designed
- A good way to start identifying information which will be exchanged among the functions and actors
- One way of estimating the percentage of requirements captured
- Categorizing functions and determining which impact the others particularly if a "phased delivery" implementation is planned
- A better way of estimating the percentage of requirements completed during development.
- Test plan can be immediately generated based on use cases
- Helps technical writers in structuring the overall work on the users manuals at an early stage
- Better traceability throughout the system development process
- Quality of the software is improved by identifying the exception scenarios earlier in the development process

Behavior Diagrams

Behavior Diagrams are used to model the behavior of entities. Two primary types of diagrams can be used: the Activity Diagram and the State Chart Diagram.

Activity Diagrams provide a way to model the workflow of a business process. Activity diagrams are very similar to a flowchart because the workflow can be modeled from activity to activity. An activity diagram is basically a special case of a state machine in which most of the states are activities and most of the transitions are implicitly triggered by completion of the actions in the source activities.

These diagrams should not replace the original Use Cases, although there is sometimes a tendency to bypass the Use Case process as unnecessary and jump right to the Activity Diagrams. However, the Use Case is vital to capturing the views of the user, which is often overlooked or assumed if the business process analysis starts with the Activity Diagram.

State Chart Diagrams define the States and the dynamic behavior for going between States for a particular function (Use Case) or object (Class). These diagrams show the sequences of states that an entity goes through, the events that cause a transition from one state to another, and the actions that result from a state change. State Chart diagrams are closely related to Activity diagrams. The main difference between the two diagrams is that State Chart diagrams are state centric, while activity diagrams are activity centric. A State Chart diagram is typically used to model the discrete stages of an entity's lifetime, whereas an activity diagram is better suited to model the sequence of activities in a process.

Each state represents a named condition during the life of an entity during which it satisfies some condition or waits for some event. A State Chart diagram typically contains one start state and multiple end states. Transitions connect the various states on the diagram. As with activity diagrams, decisions, synchronizations, and activities may also appear on State Chart diagrams.

An example from the OASIS submittal of transmission requests is shown in the Figure OASIS State Diagram (click to enlarge).

Interaction Diagrams, consisting of Sequence Diagrams and Collaboration Diagrams, focus on the interactions between entities. These diagrams are particularly important in the development of Information Exchange Models (IEMs).

Sequence Diagrams specify the precise sequence of information flows between functions, including acknowledgments, error handling, and other details. A sequence diagram is a graphical view of a scenario that shows object interaction in a time-based sequence, i.e., what happens first, what happens next. This type of diagram is best used during early analysis phases in design because they are simple and easy to comprehend. A sequence diagram has two dimensions: typically, vertical placement represents time and horizontal placement represents different objects. Sequence diagrams are normally associated with Use Cases, since they can be used to focus on the interactions between Actors and the functions they interact with.

Sequence diagrams are closely related to collaboration diagrams and both are alternate representations of an interaction. There are two main differences between sequence and collaboration diagrams: sequence diagrams show time-based object interaction while collaboration diagrams show how objects associate with each other.

Collaboration Diagrams illustrate how entities interact with each other. Collaboration diagrams and sequence diagrams really are alternative representations of the same interaction, in which a collaboration diagram shows the order of messages that implement an operation or a transaction, while a sequence diagram shows object interaction in a time-based sequence. In some CASE tools, the capability is provided to create a Collaboration diagram from a Sequence diagram and vice versa. Collaboration diagrams show objects, their links, and their messages. They can also contain simple class instances and class utility instances.

Class Diagrams visually describe the structures and relationships of data entities, explicitly showing their contents (attributes) and their actions (operations). The word "entity" is used rather than "object" because Class Diagrams can be used to describe both objects models of individual data items and metadata models of definitions of data items and their relationships. The Figure shows a Class Diagram of a metamodel of an Energy Schedule.

Visually, Class Diagrams contain icons representing classes, interfaces, and their relationships, and can be multi-level and nested through the use of Packages. Packages are used to group similar Class Diagrams.

For utilities, the best known set of Class Diagrams is the Common Information Model (CIM) which is a metadata model of the power system (primarily) with additional Packages describing other aspects of power system operations. This CIM model is being expanded to encompass distribution operations, asset management, and other areas.

For Information Exchange Modeling purposes, Class Models can be used both to define the metamodels of the data to be exchanged, as well as the structure of the information messages themselves.

Implementation Diagrams take the abstract information of the other types of diagrams and convert it into more physical views, using one of many software languages, such as C++, Java, JavaScript™, CORBA, Microsoft's COM, and others. Alternatively, the conversion can be into a data language, such as Document Type Definition (DTD) or XML.

Component Diagrams provide a physical view of the current model. A component diagram shows the organizations and dependencies among software components, including source code components, binary code components, and executable components. These diagrams also show the externally-visible behavior of the components by displaying the interfaces of the components. Calling dependencies among components are shown as dependency relationships between components and interfaces on other components. Note that the interfaces actually belong to the logical view, but they can occur both in class diagrams and in component diagrams.

Component diagrams contain Component packages, Components, Interfaces, and Dependency relationships. A Component Package Specification enables you to display and modify the properties of a component package. Similarly, a Component Specification and a Class Specification enables you to display and modify the properties of a component and an interface, respectively. The information in these specifications is presented textually. Some of this information can also be displayed inside the icons representing component packages and components in component diagrams, and interfaces in class diagrams.

In some CASE tools, the properties of, or relationships among, component packages, components, and interfaces can be changed by editing the specification or modifying the icon on the diagram. The affected diagrams or specifications are automatically updated. An additional capability of some CASE tools is to reverse engineer a set of objects that are already in another language (such as C++ or XML) and convert them back into abstract Classes with all attributes and relationships where possible.

A portion of the energy schedule class information, specifically the first couple of objects in the E-tagging specification, is shown in XML in the Figure.

Deployment Diagrams show processors, devices, and connections, in other words, the physical location where each of the component models will be implemented. Therefore, each model contains a single deployment diagram that shows the connections between its processors and devices, and the allocation of its processes to processors.

UML Methodology

The methodology for using UML can be summarized as follows:

1. Develop Business Processes, using Use Cases

Pick a business process, e.g. Day-ahead Submittal of Energy Schedules by Scheduling Coordinators

Determine all the Actors, e.g. Scheduling Coordinator and Time Line Manager

Determine the Use Case functions or systems involved, e.g. Market Interface Web Server, Format Validation Procedures, Database of Energy Schedules, and Congestion Management function. Since business processes are usually at a higher and broader level than individual

functions, these Use Cases are do not focus on a single function to show basically its inputs and outputs, but show the "forest" rather than the "trees".

Describe all performance requirements, pre- and post-conditions, and other assumptions, e.g. responses to submittals will be within 5 seconds or at pre-specified times, Scheduling Coordinators are all registered, post-condition is that schedule is accepted or rejected

Draw and describe the interactions between the Actors and Use Cases, including sequences of steps and decisions affecting information flows, e.g. Sequences for error checking, ability of Scheduling Coordinator to withdraw schedule, etc. These can be documented in Activity Diagrams, Sequence Diagrams, Collaboration Diagrams, and State Diagrams, along with text to clarify the interactions.

2. Develop Data and/or Messages Contents, using Class Diagrams

a. Identify the Data or Message Type for each interaction in the business process: Message Type consists of a noun (the data) and a verb (how/when/under what conditions is the message sent)

- There are many, many Nouns, e.g. New energy schedule or update to an existing energy schedule

- There are very few Verbs, e.g. Send, Request, Acknowledge Response, Error Response

b. Organize and list all elements required by each Data or Message Type

- "Organize" means identify specific parts of a message that are probably re-usable for other messages, e.g. Message Header, Scheduling Coordinator information, RTO information, E-tagging information (so that format can be used), Time and Date information, Other

- Indicate if there is a one-to-one or a many-to-one correspondence between a part and the message, e.g. only one Scheduling Coordinator, but one or more schedules

- List all elements for each part, e.g. Scheduling Coordinator Corporate name, Scheduling Coordinator ID, individual sending schedule, etc.

3. Translate Classes into Component Models

a. Convert the classes into Document Type Definitions (DTD), using IDL or, as is becoming more common, using XML-DTD.

b. These components can be translated into actual software code if so desired.

4. **Register these DTDs** so that all users of the information can access them. XML Registries can be public (e.g. ebXML uses OASIS XML Registry) or can be private. This step is not actually part of UML, but is becoming a powerful means to publish, maintain, and update information exchange templates among large groups of users.

3.1.1.2 Alternate Communication Channels

One of the best ways to handle availability of data from remote sites is to have alternate communications channels. In particular, these should have no common points of failure. This includes:

- Physically separated channels, so that channels in the same microwave link or fiber optic cable are not considered physically separate. Also entry points into buildings or sites need to be different.
- Different media, so that if one type of media suffers a failure, the other type is not affected (e.g. weather conditions affect radio-based communications)
- Automated switchover from one communications channel to the other within the performance requirements of the functions using the channels

Keywords: Backup, communications

3.1.1.3 Backup Data Sources

When high availability of data is required, one of the better ways to ensure that availability is to have backup data sources. These data sources could be:

- Older versions of the data. This is the most common for large sets of data or files that do not intrinsically have another source than a copy of the original data.
- Second sources that can generate the same or very similar data. This is often used in real-time monitoring by having alternate sensors to collect the same data from (electrically) near-by sites
- Calculated data. This is possible if other data can be used to calculate the original value.

When high accuracy of data is required, multiple sources can be used to check against each other. Sometimes voting is included, for instance 2 out of 3 data values must agree before the data is accepted as valid.

Keywords: Backup, high availability, high accuracy

3.1.1.4 Backup Databases

Backup is the activity of copying files or databases so that they will be preserved in case of equipment failure or other catastrophe. Simple as this practice is, it is often not followed unless rigorously demanded or automatically performed. However, a backup of data can be vital to maintain high availability even during failures or security attacks.

Keywords: Backup, Database, high availability,

3.1.1.5 Backup Sites

Backup sites for computer systems, control centers, and equipment can support the high availability requirements for power system operations. These backup site scenarios can range from minimal to complete:

- Critical system files and databases can be stored off-line and off-site so that they can be used in case of the destruction of the on-site files through fire, earthquake, theft, or other catastrophe
- Critical system files and databases can be stored off-site, but remain on-line and interconnected with the main system so that they can be used as normal backup during routine maintenance or short-term failures. This scenario implies that communications systems have been installed which permit the users to remain at their normal site, but just run the systems at the backup site.
- “Bunker sites” can be created which contain primarily user interfaces connected to the main systems over communications systems. These bunker sites can be used by the users if the normal site is not available (e.g. evacuation has been ordered). These sites can be close by or far away, with the time for users to travel between the sites a major consideration in deciding this distance.
- Exchanging backup sites with a neighbor, so that duplicates of their systems are at your site, and duplicates of your systems are at their sites. This can be less costly than renting space from a commercial backup site.

- Including each other's system software on each other's systems, so that if one system fails or the users cannot access it, the other system is available to run the first systems software. This is usually only practical for organizations that are tightly coupled.
- Mostly complete system at the backup site.
- Complete backup site that is a total mirror of the original site.

The required availability and the financial capabilities are the main drivers of which alternative to choose. In addition, the type of "failover" from one site to the other can vary, depending upon the degree of automation and communications support. Failover can range from manual to completely automated, with failover times ranging from weeks to milliseconds.

Keywords: Backup, sites, failover

3.1.1.6 Metadata Files and Databases

Metadata is the "data describing the data", and is particularly appropriate for object modeling. Metadata files and databases contain the names and structures of object models in electronic format. A metabase (sometimes called a *metadatabase* or *metadata repository*) is a database for storing metadata (data that describes data) for a specific purpose. For example, a metabase might include metadata about all configuration information in a system gathered from a number of sources. A physical metabase is one in which the metadata is actually collected into a single place before it is accessed. A virtual metabase is one in which metadata is gathered on the fly when it is needed, possibly when a program is executing. Metadata is usually expressed in XML.

Metadata is becoming increasingly important for managing data because it acts as a roster of what data exists and possibly where it exists.

Keywords: Metadata, metabase,

3.1.1.7 Object Modeling Techniques for IEC61850-based Devices

When an IEC61850-based device object model is created, the following steps are used:

- The information exchange requirements are developed from the functional requirements or Use Cases for different types of information exchanges.
- Lists of data are created, which are derived from the Use Cases and from vendor product specifications. This provides the raw data for the objects
- A block diagram is created of the device, showing its different logical parts and functions, focusing on the information exchange requirements.
- These logical parts or functions are further separated into one or more Logical Nodes (LNs). A Logical Node is a logical grouping of objects required by a particular function, which could be reused by many different devices. Many Logical Nodes already exist in the IEC61850-7-4; these should be used if they meet the device requirements. However, new Logical Nodes must be created to meet new needs, such as those for the Distributed Resources environment.
- Each logical piece of data that may be exchanged between the Server and a Client is defined as a **data object**. Many data objects have already been defined in the IEC61850-7-4, and should be used as defined. New data objects must be defined when no existing IEC61850-7-4 objects can serve. Data objects may be simple (e.g. open/close status of a switch), complex (e.g. all ratings and static characteristics of a device), or an array (e.g.

an array of bits defining alarm reasons). Discussion among experts is sometimes required to determine exactly what constitutes a particular data object.

- Existing IEC61850 Logical Nodes have their data objects already assigned to them. A new IEC61850 Logical Node must have new and existing data objects assigned to it, based on their logical role within the device model. Sometimes a data object could be assigned to more than one Logical Node: therefore, a decision must be made as to where it most logically lies.
- Each type of data object is also assigned to one of the **Functional Component** categories (e.g. the open-close status of a water valve is assigned to the ST functional component category).
- Each data object is given a unique **object name**, which must follow certain guidelines, but should be relatively self-explanatory (e.g. the open-close status of a switch is called SwDS, where DS stands for Device State). This name is critical: it is the way that Clients and Servers can recognize what data is being transmitted.
- Each data object is assigned a **Common Data Class**, which defines what format the data is in (e.g. SwDS is assigned to the CDC SPS, which is defined as a two-bit binary, plus quality code, plus timestamp, plus description). A CDC can be defined to be a single item, or, more usually, as a structure of items (such as the SPS CDC, which consists of 4 items). If no existing CDC can meet the requirements of the data element, then a new CDC must be developed, following the procedures established for IEC61850.
- Each data object is defined as **mandatory** or **optional** or **conditional** (m/o/c column).
- The meaning of the **values** for each data object are defined; some are implicitly defined by the type of Class, but certain Classes have flexibility in what values might mean, so these must be clarified for each data element (e.g. for SwDS, the two-bit status has the following meanings: 00 = between (in transit), 01 = closed, 10 = open, 11 = invalid).
- The **reporting objects** are defined, based on the conditions under which each client needs to receive data (e.g. SwDS should be reported to Client 1 anytime the two-bit value or the quality code changes), and what groups (**Data Sets**) of data objects should be reported. The actual rules for the reporting procedures are defined in the IEC61850-7-2 standard. Once Data Sets are established on either side of a link, then only the data (not the long names) can be sent over the communications network.

Keywords: IEC61850, object models, objects, logical nodes

3.1.1.8 Quality Flagging

Quality flags are critical for determining the state, age, and availability of data. Some quality flag parameters include:

- Valid
- Invalid
- Older than normal
- Questionable
- Overflow of an analog value
- Out of range
- Bad reference
- Oscillating too rapidly
- Failure
- Inconsistent

- Inaccurate
- Substituted for another value
- Provided by a source that does not provide quality flags
- Calculated value
- Manually entered value
- Under test or in maintenance
- Blocked so that the value is not updated
- Tagged to prevent different types of control actions

Keywords: Quality, flag, tag, block, validation

3.1.1.9 Time Stamping

Time stamps are crucial for determining the time of an event. Different resolutions are required by different situations, but typically time resolutions for power system events should be within 1 to 10 milliseconds.

Time accuracy and time synchronization requirements across many systems and devices can also vary, but again for power system operations, typical **relative** accuracy/synchronization requirements are:

- Events within a substation should be timestamped with a relative accuracy within the substation of 1 millisecond
- Events across multiple substations should be timestamped with a relative accuracy of 10 milliseconds

With the availability of GPS time, the requirements for **absolute** time accuracy are becoming more stringent, and 1 millisecond absolute accuracy across large territories can now be met if GPS devices are connected to the time-critical devices.

Time stamps are particularly important for:

- Data values, to indicate exactly what time they were monitored
- Control actions, to indicate exactly when a control action took place
- Alarms, to indicate when the event took place that caused the alarm, as well as additional time stamps to indicated when an alarm was acknowledged and when the situation that caused the alarm was resolved
- Events, to indicate when events took place

Keywords: Time, relative time, absolute time, GPS

3.1.1.10 Validation of Source Data and Data Exchanges

Validation of data should be performed at each step in a process, and “flags” should be included with the data to indicate the “quality” of the data. This quality flag will normally have to be carried forward with the data to each additional step, with additional validation included whenever feasible and pertinent. For instance, power flow data from field equipment may only be validated for reasonability within a substation, but compared with other data for bias or inconsistency in a state estimation process at a control center.

Validation of data is not a technology per se, but is a theme that should run through all system designs.

Keywords: keywords

3.1.1.11 Data Update Management

Many functions are sensitive to the time when data last updated. For these functions, a number of mechanisms are available for handling this sensitivity. These mechanisms include:

- Time stamping data as to when it was last updated
- Flagging data as “out-of-date” if it exceeds a specified time limit.
- Extrapolating or interpolating data values from other more timely data

Keywords: keywords

3.1.1.12 Management of Time-Sensitive Data Flows and Timely Access to Data by Multiple Different Users

Management of time-sensitive data flows entails ensuring that systems can handle the streams of data in a timely manner. Although the primary solution to this issue is to ensure that the systems and communications are appropriately sized, this sizing can entail addressing the following questions:

- Is the flow of data relatively constant or are there bursts of data? (Queuing theory can be used to establish sizing for this issue).
- Is maximum time of data flows critical? If so, then the system should be designed for deterministic delivery times (as opposed to statistical delivery times) and sized to handle the maximum throughput. An example is the requirement for maximum response time of 10 ms for protective relaying. In this case, non-absolute protocols like Ethernet are not feasible unless they are used in a switched network (so that essentially there never is a conflict).
- Is it acceptable to base the timeliness of data flows on statistical characteristics? For example, access by Market Participants to market information often has statistical requirements, e.g. 95% of Market Participants must be able to access information within one second 99% of the time. The primary solution is the provision of adequate bandwidth, processor power, and well-deigned applications to ensure these contractual requirements are met. Additional solutions include alternative or backup sources of the time-sensitive information, as well as measures to prevent denial-of-service security attacks. In addition, performance logging should be implemented so that proof of meeting the statistical characteristics is available.
- Must multiple users be accommodated with contractual commitments for access within specific time windows (e.g. access within 10 seconds after each hour, or response to a request within 30 seconds)? The primary solution is the provision of adequate bandwidth, processor power, and well-deigned applications to ensure these contractual requirements are met.

In either case, very precise specifications, statistical analysis of data flows, and rigorous factory and field testing are the most effective ways of ensuring this requirement is met.

Keywords: keywords

3.1.1.13 Management of Data Consistency and Synchronization across Systems

Management of data consistency is becoming more crucial as more functions are automated, and as more decisions are made in “real-time” in which there is no leisure to check the consistency of data.

No single solution exists for ensuring data consistency; normally it is a combination of technologies and best practices applied consistently across a system. These technologies and best practices include:

- Clear identification of primary sources of data
- Publish/subscribe, so that systems, applications, and databases can “subscribe” to data, which will be “published” to them whenever it changes
- Validation of data consistency through a variety of data checks
- Alarming on inconsistencies so that they can be corrected
- Automated procedures for establishing or re-establishing consistent data after systems are restarted or re-initialized

Keywords: keywords

3.1.1.14 Management of Data and Object Naming

The management of object naming has become more important as object models proliferate and the number of implementations of these objects increases. Some efforts have been proposed to make all object names universally valid, through the assignment of universal IDs. Most object modeling sets limits on the length and imposes rules on the construction of the names. For instance, IEC61850 allows a maximum of 64 characters for each object’s name.

Keywords: keywords

3.1.1.15 Management of Data Formats in Data Exchanges

Mismatches in data formats or structures are frequently a cause of incompatible data exchanges. For instance, one system will be updated so that a new attribute is added to a data item, or a new data element is deleted from a list of data. The other system usually cannot manage these mismatches in expectations, and either shuts down with an error, or blithely continues processing what it thinks it can do (sometimes correctly and sometimes incorrectly), but does not inform anyone of the inconsistency.

The use of object models to establish both the structure of each object and the contents of each data exchange can alleviate many of these problems. In addition, if metadata models of the objects are available in electronic format (e.g. as XML), then systems can automatically detect and correct mismatches.

Keywords: keywords

3.1.1.16 Management of Transaction Integrity (backup and rollback capability)

Many systems require one-step transactions, where if the transaction fails for some reason, the results must be either ignored or rolled back. Two-step transactions are even more complex, since sometimes the results of the second transaction must also roll back the results of the first transaction.

Utility operations systems have not often needed this capability except peripherally. For example in updating the SCADA database, roll back to a previous version is needed if some error was introduced into the updated version of the database. However, this type of capability is certainly required in the market operations, and increasingly in other control center functions.

Two-step transactions and roll-back have been implemented in a number of products.

Keywords: keywords

3.1.1.17 Management of Data Accuracy

Data, whether it is monitored from the field or retrieved from some other system, needs to have appropriate precision and accuracy. In particular, distribution automation functions require more accurate data than system operators who merely need to get an estimate of conditions. This data accuracy requirement implies that (to the appropriate degree for the functions using the data):

- The source of the data must be precise, with accurate CTs and PTs, appropriately scaled analog-to-digital conversions, appropriate resolution of the digital values (8-bits, 12 bits, or more bits to represent the analog value), and appropriately precise calculations of derived values (e.g. var, VA, kW).
- The data sources must be accurately calibrated.
- The data must be converted correctly to engineering units or other measurement units.
- Data should be validated for reasonableness, if not for more precise checks. For instance, within IEDs, certain checks for consistency could be used to detect inconsistent data, while at the control center State Estimation at both the transmission and the distribution levels could be used.

Keywords: keywords

3.1.1.18 Management of Data Acquisition

Data acquisition has many pitfalls as well for data management. Some of these pitfalls can be ameliorated by new information technologies, while others require old-fashioned carefulness. The main problem is the sheer volume of data now required. Some IED controllers contain hundreds (even thousands) of points. Although many are not needed by SCADA operations, they are useful for engineers and maintenance personnel. Given this magnitude of data items, data management must be viewed as a significant aspect in the design of new and upgraded systems. In particular:

- Object-oriented protocols (e.g. UCA (IEC61850) for field equipment, CIM for power system data, and XML for general data) should be required. These protocols require that the IEDs that control the field devices are organized with well-known point names which are self-describing and can be “browsed” for information much like Web pages. This self-description allows applications to link automatically to the correct data with minimal human intervention (thus avoiding one of the main causes of error).
- Data objects required by SNMP MIBs should be retrieved from field equipment, regardless whether object-oriented or point-oriented protocols are used.

Keywords: keywords

3.1.1.19 Management of Manual Data Entry

One of the most difficult areas for managing data is data entry, in which humans type information into a system or database. The primary issue is trying to maintain high levels of accuracy. Again, information technology has begun to address this issue:

- Data entry by humans should be avoided as much as possible. For instance, no data should be entered twice: a single source of each type of data should be established and used to populate other databases.
- Object-oriented data should be used, so that applications and database tools can be used as much as possible to automate the data entry process.
- Data should be validated as much as possible during the data entry process. This validation should include reasonability and consistency checking as well as format checking. Roll-back and two-step entry procedures should be used where critical functions must have accurate data.
- Applications using this data should validate it as well, to avoid “crashes” and security violations.
- Logs should be kept of all data entries.
- Data backup of all important data should be provided.

Keywords: keywords

3.1.1.20 Data Storage and Access Management

Data storage and access management is another critical area in the design of systems. Often systems have been developed for one purpose, then added-to for another purpose. Later, other applications need data, so an additional jury-rig is added. Some key recommendations for avoiding this problem (or migrating away from it) include:

- The real-time database in the SCADA system, which is focused on providing timely but limited amounts of data to operators, should not be used as a source of data for other systems. Rather the front-end data acquisition and control (DAC) system should be structured to supply the required real-time data to SCADA system, but also provide other kinds of data to other applications without impacting the SCADA system itself.
- The DAC should support access to field equipment by planners, protection engineers, and technicians
- Object-oriented protocols should be used for all data exchanges between systems. With data having well-defined names, managing the access to the data is easier and more likely to be correct. These object-oriented protocols include the UCA (IEC61850), the CIM, and XML information exchange models (see next section).
- Currently some of these object-oriented protocols are not completely interoperable or consistent in their structure. In particular, the data names and structures of IEC61850 and the CIM need to be harmonized. This activity is taking place in the IEC.
- Standard formats and methodologies for Application Program Interfaces (APIs) for data access also need to be formalized. Currently the CIM specifies the Generic Interface Definition (GID). The GID identifies explicitly which features of existing APIs (such as DAF and DAIS) will be implemented to exchange data implemented in CIM-based databases, to extend these capabilities to include features needed in utility operations, and to specify the exact formats to use when implemented over different types of middleware (e.g. CORBA or Microsoft COM).

- Electronic registers should be developed which contain the metadata models of the object-oriented data. This is discussed in more detail in the section on Information Exchange Management.
- As major assets are purchased, their characteristics should be entered into an electronic asset database (e.g. AM/FM system), possibly using bar codes (to avoid the fallible human data entry process). They should then be tracked throughout their life as they move from the warehouse to one or more field locations over time. This method could provide the accuracy so often missing but badly needed in the asset databases.

Keywords: keywords

3.1.1.21 Data Consistency across Multiple Systems

Data consistency across multiple systems is vital for reliable automation of functions. If data is inconsistent, then the applications will have inconsistent and probably incorrect results. Many factors impact data consistency, but some methodologies can be used to help insure consistency. These include:

- Use of publish/subscribe application services, in which every application that requires certain data “subscribes” to it. Then, whenever the source data is updated, it is “published” to all subscribers simultaneously.
- Data should carry “quality” indications as it is passed from its source to other systems. These quality indications could include “invalid”, “out-of-date”, “manually-entered”, and “calculated”. More complex indications could include multiple timestamps indicating when the data was first created, as well as when it arrived at each database, or indications of what parameters were used in calculating its value, etc.
- Applications should validate the input data, possibly by analysis (e.g. State Estimation), possibly by accessing multiple sources of similar data that can be cross-checked.
- Error handling mechanisms should be in place to notify the Network Manager of loss of data, inaccessibility of data, invalid data, and other data quality indications.

Keywords: keywords

3.1.1.22 Database Maintenance Management

Database maintenance is one of the most difficult jobs to perform accurately all the time. Again, the best method for managing this effort is to provide as many tools as possible for capturing the data automatically, and then verifying it before the database is released for use by the control center systems. Many of these tools and methodologies have been mentioned in previous sections:

- Object-oriented data using self-description techniques for correctness; eventually for automatic update capabilities
- Cross-database consistency checking
- Data quality indications and time-stamping
- Updating of metadata registers and notification to applications to access this register to determine if data exchange formats have been modified

Keywords: keywords

3.1.1.23 Data Backup and Logging Management

Data management will never achieve perfection. Therefore, critical data should always be backed up, all changes should be logged, and some means should be available to “roll back” to a previous version if necessary.

The logging requirement can also be critical for auditing as utility operations are being scrutinized in more and more detail due to the market environment.

Keywords: keywords

3.1.1.24 Application Management

The management of applications is also necessary in order to ensure that functions operate correctly and accurately. Most of this management must involve the individual applications themselves, but general management methodologies can be recommended. These include:

- The Unified Modeling Language (UML) methodology described in the previous section should be used/required for all new application development or upgrades of existing applications. Use of this methodology will help ensure that the application is properly integrated with other applications.
- All new and updated applications should be very thoroughly tested to ensure they execute correctly under both normal and error conditions. Applications that have not been properly tested will not be trusted by users, often leading to the applications being “turned off” or ignored (this has been the fate of many power system network analysis applications).
- The status of applications should be monitored by the SNMP Manager, with appropriate levels of notifications sent to users (e.g. alarm if a critical function is impacted, warnings if applications are “taking too long” to process data, “not responding” notifications, etc.).

Keywords: Keywords

3.1.2 Enterprise (Network and System) Management Best Practices

3.1.2.1 Analysis of the Integration of Enterprise Management and Power Systems

Specific to power systems operations, the team developed the list of abstract enterprise management services needed to support these operations. This list was originally derived from the generic enterprise management functions described under Enterprise Management Services and subsequently focused to meet the IECSA’s requirements addressed in the Use Cases Architectural Issues (see Vol. 2, Appendix E) for the various domain functions and abstract use cases. These requirements do not explicitly raise the need for enterprise management. However, the need can be derived. Examples of these requirements and the derived enterprise management services are listed below:

- For the Field Device Integration, the requirements of SCADA communicating with thousands of devices imply the need to perform configuration and fault management of numerous local and remote devices.

- In Field Device Integration, the requirements for *any* communications media: wireline, wireless; raises the need for the enterprise management system to be able to manage multi-protocol, multi-technology systems and networks.
- In Field Device Integration, the requirements of the fault to be communicated to sub-station computer within one second, raises the need for tight performance management and appropriate configuration management.
- In Field Device Integration, the requirements for the communications of IED and the sub-station master to be 99.999% reliable, implies tight performance and alarm monitoring, substantial effort in survivable network design and traffic engineering, and fast fault detection and recovery services.
- In Integrated Security Across Domains, the requirements that the communication media can have any forms of ownership: utility-owned, jointly owned, commercially provided, Internet; implies the need for policy management, establishing and enforcing SLAs, and fairly tight security management.
- In Integrated Security and Energy Markets, the requirements for the communications to take place between various organizations and different administrative domains imply the need for extensive policy management and enforcements of inter-domain management policies.
- The various functional aspects of the domain tasks implied similarities with generic enterprise management functions and the need for integration of these services for ease of operations and cost reductions.

From an abstract modeling perspective, it is worth considering the OSI architecture model of enterprise management that can be described from the four views of: (i) organizational model, (ii) Information model, (iii) communication model, and (iv) functional model. In RM-ODP terms: The OSI Organization Model can be seen as a RM-ODP Engineering Model; The OSI Information Model can be seen as a RM-ODP Information View The OSI communication Model can be seen as a RM-ODP Computational View; And the OSI Functional Model can be seen as a RM-ODP Enterprise Model

The *organization model* includes the various components of the enterprise management system, namely *managed object*, *agent*, *manager*, *user interface* and the *management database*. The managed objects include the network elements, devices, applications, processors, memories, storage devices, etc. The agent runs on the managed object and provides data on the managed object to the manager. The manager manages the managed objects. The database contains information on the managed objects. The organization model is fairly common within various enterprise management technologies.

Complementary to this organizational model, are a Functional Model consisting of Common Services, an Information model, and a Communication Model consisting of Generic Interfaces/Protocols. With regard to where components are deployed, both the OSI Enterprise Management Organization Model and the IECSA Deployment model are flexible enough to allow implementers to deploy managers, agents, and gateways as needed. The important point is that both the OSI Enterprise Management Model and IECSA architecture treat their models orthogonally.

Although there are differences between the various models for enterprise management and power system management, the similarities in the functional aspects of the management tasks and the need for coordination of these tasks implies the need for integration of the services for ease of operations and cost reductions.

3.2 Security Best Practices

3.2.1 Security Policy

3.2.1.1 General Security Policy Process

3.2.1.1.1 Security Policy Development Process

The Security Domain's policy service is concerned with the management of policies. The aggregation of the policies contained within and managed by the policy service comprises a Security Domain's policy set. This service is also responsible for the enforcement of the domain's policy for intra-domain and inter-domain exchanges. The policy service may be thought of as another primitive service, which is used by the authorization, audit, identity mapping, and other services as needed.

The policy service is a process through which a Security Domain determines its risks vs. costs in order to protect critical assets. The policy development must encompass:

- A Requirements analysis process which is used to determine the critical assets that need protection, security needs of the Security Domain, technological choices for implementation, security management and monitoring requirements, audit capability, and non-repudiation capability.
- The Implementation process that monitors and tests the policies as they are implemented. If there are problems detected during implementation, the policy should be revised and requirements should be revisited.
- The Monitoring process is responsible for the detection of security attacks, detection of security breaches, and the performance of the installed security infrastructure. This process is critical to the overall effectiveness of security.
- The Analysis process is responsible for determining when the deployed security measures need to be re-evaluated. This re-evaluation may be required due to environment, legal, or internally developed metrics.

There is a relevant body of work that can be found in EPRI Report 1008988, Scoping Study on Security Processes and Impacts. The following is a summarization of that work.

3.2.1.1.2 Security Policy Coverage Requirements

A policy must determine what assets need to be protected, determine what attacks need to be mitigated, how to mitigate the attacks including technology and procedural, and how to detect attempted attacks.

- **Asset Protection:** In order to determine which assets need to be protected, all aspects of the "value" of an asset needs to be determined. This means that legal, community good will, asset value, and cascade effects (if an attack did compromise a particular asset) need to be taken into account. Since it is not possible to secure every asset in the infrastructure, it is recommended that the high risk or high-value assets be protected first.
- **Determining what Attacks to Mitigate:** The requirements process must determine what is the cost/benefit/probability of a successful attack and what form such an attack might take. The higher the probability of success indicates the higher need for mitigation.
- **Mitigation Strategies:** The security services, discussed in this report, provide suggestions in regards to how to mitigate many of the threats. It is up to each security domain (SMI) to determine the best method to mitigate the attack and then write the appropriate policies to reflect that intent.
- **Attack Detection:** Since there is no absolute security, detection of an attempted attack is an important objective of any security policy. For each asset being secured, a mechanism for detecting attempted/successful attacks needs to be part of the policy and it **MUST** be implemented and monitored on a constant basis.

As part of the requirement process, ISO/IEC 15408 (e.g. the standardized version of the NIST Common Criteria) should be used as a basis for the technological requirements assessment and determining threats and mitigation strategies.

The requirements phase of policy development must also take into account risk assessment.

3.2.1.1.3 Security Risk Assessment/Analysis of Assets

“The classical definition of Risk Analysis is one that describes it as a process to ensure that the security controls for a system are fully commensurate with its risks.”⁷

Translated, this means that the amount of security deployed should be related to the overall asset value (including collateral assets that could be effected⁸). Thus, risk analysis provides a mechanism to determine which assets should be protected immediately (based upon relative worth) and not require that all Security Domain assets be secured.

Some of the other documented benefits of performing risk assessment are:

- Provides a means to cost justify security investments.
- Breaks down business boundaries and build business relationships.

Business management would be responsible to determine the security risk level that would be tolerable for a particular asset. IT/Security staff would need to work with the management team to determine the cost/solution. Based upon both factors, a cost/security ratio could be developed and used as a metric.

- Risk Analysis allows security to be analyzed from a business needs perspective and not just from a technological solution basis.
- The team risk analysis activity raises the security awareness to a greater number of personnel.
- Provides a mechanism to evaluate security in a “consistent” manner.
- Facilitates communication between different business entities.

3.2.1.1.4 Implementation of Security Policies

As the selected assets are secured, tests should be executed to make sure that the created policies and deployed technologies actually perform as desired. If not, new policies reflecting new requirements need to be generated. Therefore, test procedures need to be considered as part of the policy development cycle.

As an example, the policies and procedures for physical access should be tested on an un-announced basis. This should be written into the policy as well as the maximum re-test interval allowed. Additionally, the expected results of such tests should be documented. If the expected results are not obtained, an analysis of the causes for not achieving the expected results needs to occur. If the analysis indicates that the policy is in error, then the policy needs to be revised.

3.2.1.1.5 Analysis and Re-Analysis of Security Policies

Policies and procedures need to be written to state how often re-analysis of the existing policies and security infrastructure needs to occur (given no successful attack or repeated attempted

⁷ From: <http://www.eon-commerce.com/riskanalysis/whatis.htm>

⁸ For electric utility infrastructures, a successful security attack could impact other infrastructures. Therefore, infrastructure impact on other infrastructures and the public must be taken into account during the risk assessment. EPRI Report 1008988 provides a more detailed discussion.

attacks being detected). The policy for re-analysis needs to recognize that shifts in the world political environment (just think of before 9/11 versus now) and technology advances all need to be taken into account.

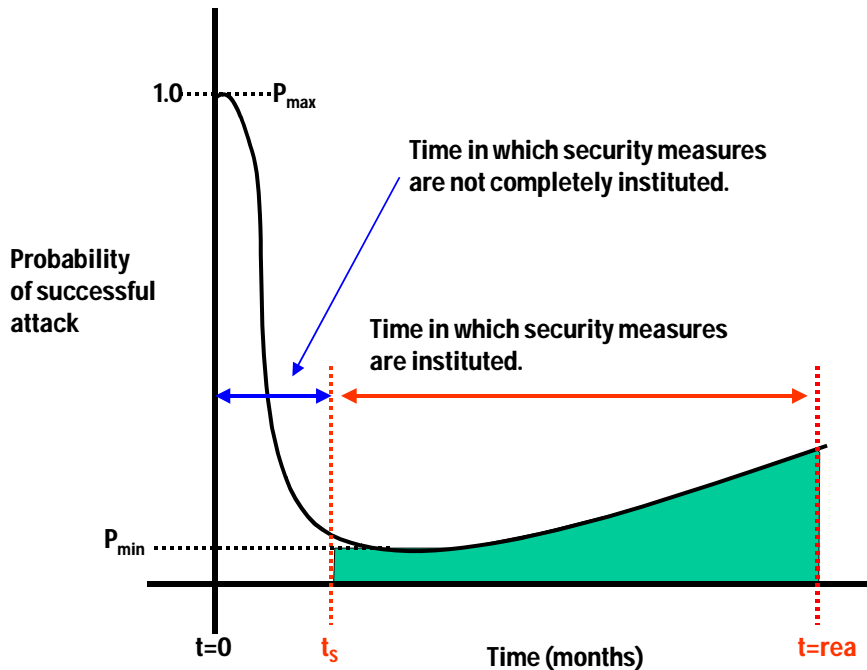


Figure 5: General trend is security vulnerabilities (extracted from EPRI Report 1008988)

Figure 5 shows the probability of a successful attack. It depicts a high probability prior to security measures being implemented. At the time the security measures are implemented, this represents the “lowest” probability of successful attack if the security process has worked properly. However, the figure accurately reflects that over time the probability of successful attack increases. Thus it is important to understand and specify the periodicity of security re-evaluation in order to keep the probability of successful attack at an acceptable level.

Thus the aforementioned represent the general types of problems that must be faced when developing an overall Security Domain security policy. However, there are technology specific policies that also need to be addressed.

Note: ISA-99, Integrating Electronic Security into the Manufacturing and Control Systems Environment is a document worth reading. It discusses, in more detail, the aspects of policy development.

3.2.1.2 PKI Infrastructure Policy and Issues

Note: This section is intended as a simple discussion of the issues regarding PKI. There are more authoritative documents available from NIST or NERC.

The purpose of the Public Key Infrastructure is to allow the establishment of Trust through the binding of encryption keys (typically “public” keys) and identities. In order to understand how PKI works, it is first important to that PKI to understand the three prevalent types of encryption: symmetric, asymmetric, and public/private.

- Symmetric encryption refers to the fact that both peers have the knowledge and use the same encryption key. Since both peers have and use the same key, symmetric

encryption does not lend itself to unambiguous bindings (e.g. one key to a particular application/entity), thus symmetric encryption should not be used as the Trust establishment binding (e.g. should not be used within a PKI environment).

- Asymmetric encryption refers to the fact that each entity has its own key. Unlike symmetric encryption, asymmetric keys can allow for unambiguous identity establishment. However, since cooperating peers would need to have knowledge of the other peer's key, it is often difficult to protect the identifying key. Although asymmetric keys could facilitate a PKI environment, the use of such keys for identity binding is not recommended since the keys must be disseminated/configured on multiple peers and therefore a prone to being compromised.
- Public/Private key encryption works on the basis that the use of the public key allows the decryption of information encrypted with the private key. Conversely, information encrypted with the public key can only be decrypted with the private key. It represents a specialization of asymmetric encryption.

The use of public/private key encryption can be used for two purposes: encryption and digital signatures.

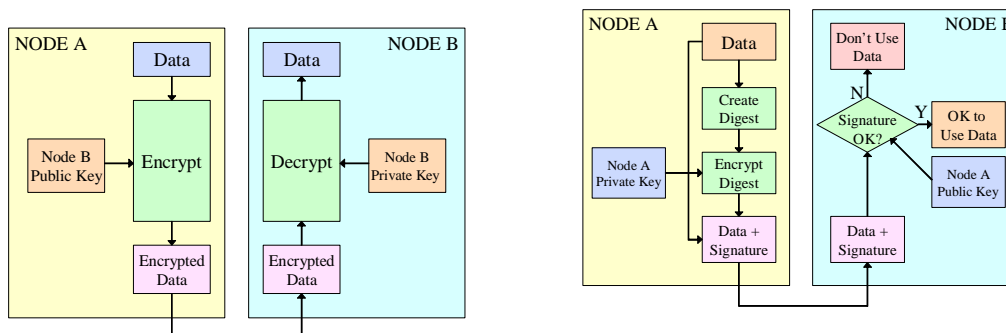


Figure 6: Simplified diagram of Public/Private Key encryption and Digital Signature

Figure 6 shows in order for Node A to encrypt data to be sent to Node B, the use of Node B's public key is required. It also shows that only the holder of Node B's private key can decrypt the information (neglecting encryption attacks). Likewise, the Digital Signature exchange shows that Node A's signature is decoded by Node B through the use of Node A's public key. Thus for both encryption and digital signatures, only public keys need to be exchanged and therefore it becomes easier to control and protect the private keys. Thus public/private key based PKI systems should be the preferred approach.

Obviously, it is critical to have a robust PKI infrastructure:

- Create the appropriate bindings between public/private keys and identification.

The typical mechanism for the bindings is through a digital X.509 certificate. A public certificate that includes the public key is created, and an equivalent is created as the "private certificate" that contains both the private and public keys. It is the creation of these two "certificates" that are typically the responsibility of a Certificate Authority (CA).

The protection of the public certificate/key is not that important, but the protection of the private key/certificate is. It is the responsibility of the CA to provide adequate protection during the generation process and to protect this information even if the certificate has been sent to the actual user.

Since the CA is the “root” source of the certificate, it is important that the CA also provide Certificate Revocation List (CRL) ability so that compromised or stolen certificates can be revoked.

- The user of a “private certificate” must provide security mechanism to protect the private information.

The actual mechanism for Security Domain/user archiving is a local issue, but great care needs to be taken during the policy establishment to be able to quickly and properly detect if there has been un-authorized access to the Security Domain private certificates. The policy must include the appropriate mechanism/procedures for reporting the compromised certificate and revoking its use locally.

- Even though the public certificates do not have the same criticality, the Security Domain policy should address the procedures for releasing the public certificate for use.
- A mechanism for tracking the lifetime expiration date in advance to actual expiration needs to be addressed.
- Policies/procedures for replacement and renewal of older certificates (prior to expiration) or revoked certificates needs to be developed.

Of particular concern in IECSA, and the utility industry, is how to provide an appropriate revocation capability for a Security Domain. There are several design criteria for such an infrastructure:

- The infrastructure must be able to accommodate revocations of certificates that have been issued from more than one CA.

There is no central CA for the utility industry, or the world, and it does not appear that there is movement towards such an entity. Even NERC, in its e-Marc program, intends to allow certificates from multiple (although “certified”) CAs to be used.

- Many of the certificate using computational resources will not be allowed direct access to the Internet that would be required in order to query the CRL of a particular CA.

Additionally, CRLs can be large and can consume bandwidth and be computationally intensive.

- An ability to determine if a particular Certificate has been revoked.

The X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC 2560) allows such a capability. It is worthwhile to note that OCSP is a request/response-oriented protocol (e.g. the certificate user must request to check if a certificate has been revoked).

However, the fact that OCSP is request/response means that there is an issue of timeliness in revocation information. However such a protocol/procedure does not exist today. In a future time, it could be envisioned that a central Security Domain revocation server (not a CRL server) could be created with the following attributes:

- Allows certificate users to register that certificates are in the user certificate cache.

- The Revocation Server would query the CAs CRL servers and process the revocation list(s).
- Based upon the CRL processing, the Revocation Server would notify the certificate user that the particular certificate has been revoked.
- Optionally, such a Revocation Server could alert Security Domain management that a certificate of a particular user is about to expire so that corrective action could be taken.
- Optionally, such a Revocation Server could respond to OCSP requests so that newly configured certificates could be validated as still being valid.

It is believed that work on such an entity is needed to allow more timely delivery of revocation information and to allow automation of such tasks.

3.2.1.3 Specific Policy Issues and Recommendations per Service

Some security services merit specific policy recommendations that were not expressed within the security service section explicitly.

3.2.1.3.1 Audit Service and Non-Repudiation

The major policy issue that affects non-repudiation is the time frame for which a valid audit trail can be generated. It is recommended that audit information be archived and available for no less than a three (3) month period of time.

3.2.1.3.2 Credentials and User Accounts

3.2.1.3.2.1 *Credentials*

There are some general issues for credentials that apply to many of the credential types that have been discussed.

- How many credentials of a given type will a user be allocated?

In general, it is recommended to allocate a single physical credential of each type (e.g. Smart Card, Personal ID card, Token Generator). This recommendation even applies to Digital certificates. Such a policy will minimize the effort required for management, renewal, and revocation (if needed).

- Upon revocation, a policy/mechanism needs to be developed to detect and enunciate if that credential, even a network address, has been used after revocation. The policy must address the expected detection timeframe allowed and the type of response expected from SMI.

Note: Typically, the smaller the detection window the higher the cost to implement.

- The period at which credentials need to be renewed/modified.
- The determination of an appropriate non-use time that causes an investigation and potential revocation of the credential if the credential has not been used within that non-use time period.
- Determine a policy for revoking the credentials.

3.2.1.3.2.1.1 *Personal Identification*

The design and management of Personal Identification cards will impact the ability to enforce physical access control.

It is recommended that such ID cards require a photograph of the person and also have an area where an easy modification can be made.

As a minimum, it is suggested that these modifications occur on a monthly basis and be a multi-colored/foil label with a valid through date printed on it.

3.2.1.3.2.1.2 *Addresses*

In order to provide an infrastructure for monitor and revocation of addresses, it is important to address the two (2) main address types: statically and dynamically assigned.

3.2.1.3.2.1.2.1 *Statically Assigned Addresses*

For statically address assigned computation resources:

- The policy should require that the physical (e.g. Media Access Control address or equivalent) be recorded. The policy must also allow for tracking changes in that address.
- That the communication segment has an Access Control List (ACL) that prevents off segment communication if the address is revoked.

It is recommended that this policy be enforced through the deployment of SNMP manageable switches. So that an address can be associated with a switch port, and upon revocation the port is disabled.

- The policy/implementation should allow for continuous monitoring/detection of addresses that should not be present and that have not been used for a policy specified period of time.

The policy/implementation infrastructure must provide the technology to detect usage and determine periods of inactivity.

- A policy/procedure is needed that allows renewal/reactivation of the address if the address has been revoked incorrectly.
- A policy/procedure is needed that allows re-assignment of a previously assigned addressed.

3.2.1.3.2.1.2.2 *Dynamically Assigned Addresses*

For dynamically addressed computation resources:

- The policy should prohibit dynamically assigned addresses from being used as single-factor identification credentials. The probability of incorrect identity establishment is high; therefore it should not be allowed.
- The policy should not allow off-segment communication unless a challenge-response is performed.
- The policy/procedures/SMI must be able to provide an audit record/trail regarding the address assigned to the challenge/response so that actual identification of the user can occur.
- The challenge-response should be on an individual basis (e.g. no group assigned passwords).

3.2.1.3.2.1.3 Username/Passwords

There are a couple of recommendations in regards to the use of usernames/passwords:

- In general, a particular user should be allowed one and only one password for a given computational resource.
- The size of the password, and its required characters/format needs to be specified and enforced.

The first question that needs to be answered is the character set. It is recommended that upper, lower, punctuation, and numeric characters be allowed. This increases the possible permutations of passwords dramatically:

Example assumes ANSI Character Set:

Number upper case characters:	24	
Number of lower case characters:		24
Number of numeric characters:	10	
Number of punctuation characters ⁹ :		30

Based upon a four(4) character password, then number of possible permutations is shown to be:

Permutations if upper case only:	331,776
Permutations if upper and lower case :	5,308,416
Permutations if upper, lower, numeric case :	11,316,496
Permutations if using all characters:	59,969,536

It should be noted that some computational resources may not be able to accept punctuation characters within passwords, but it is strongly recommended to include upper, lower, and numeric characters within the password character set.

The policy needs to determine the minimum size of a password in order to provide adequate protection.

Unfortunately, many existing policies assume that password size is the criteria, however protection comes from the number of possible permutations. It is suggested that the minimum number of password permutations be approximately 1 trillion for any computational resource.

This means, based upon allowed characters, the minimum password size is :

Table 33: Recommended Minimum Password size

Character Set Allowed	Recommended Password Size
Upper Case Characters Only	9
Upper/lower case characters only	8
Upper/lower/numeric characters	7
All characters	6

⁹ Assuming the following characters: !, @, #, \$, %, ^, &, *, (,), -, +, =, {, }, [,], |, \, :, ;, “, ’, <, >, ., comma, ?, and /.
For a total of

It is further recommended that seven(7) characters be the absolute minimum.

- The policy needs to require at least one numeric character, if numeric characters are allowed. Additionally, the policy should not allow numeric characters as the last character of the password. Such a policy will eliminate the natural tendency to append a number to a base password when revision of the password is required.
- The policy needs to address the period of time that requires password changing.

3.2.1.3.2.1.4 Smart Cards

Smart cards can be used to contain personal identification information (e.g. username/passwords), digital certificates, biometric information, and other types of information. Therefore, the credential types they contain typically address the credential aspects of a smart card.

The major policy issue, specifically related to smart cards, is the development of policies/procedures relating to the serialization of the smart cards.

3.2.1.3.2.1.5 Digital Certificates

There is a major issue regarding digital certificates, and that is the handling of revocation. Certificate Authorities (CAs) typically maintain Certificate Revocation Lists (CRLs) that are updated on a twenty-four (24) hour interval. A certificate that has been placed on a CRL is no longer trustworthy and therefore should not be useable.

Policies and procedures should be developed to:

- Specify a periodicity to check the CAs CRLs and how to disseminate this information within the security domain.

The NERC DEWG has expressed a major concern in this area and further policy study in order to develop a specific recommendation is warranted.

3.2.1.3.2.1.6 Virus Protection

The developed policy should address virus and worm protection. It is suggested that the following NIST guide be used as part of the policy development.

NIST, NIST SP 500-166, August 1989, Computer Viruses and Related Threats: A Management Guide, Springfield, Springfield, VA: NTIS.

3.2.1.3.3 User and Group Account Management

This service allows the ability to define, assign, organize, control and maintain mapping for user and group identifiers within the security domain. There is no authoritative technology that is applicable to providing this service and therefore must be rigorously addressed via policy.

However, there are several relevant articles that may prove of assistance.

Table 34: Relevant Articles concerning User and Group Account Management

Oblix	Best Practices in Extranet Portals and Identity Management
Oblix	Mastering Supply Chain Partnerships: Achieving Core Business Objectives through Effective Identity Management Available from: http://www.oblix.com/resources/whitepapers/index.html
Oblix	Lowering eBusiness Administrative Costs with Effective Group Management Available from: http://www.oblix.com/resources/whitepapers/index.html
Oblix	An Overview of Federated Identity Architecture Available from: http://www.oblix.com/resources/whitepapers/index.html
Oblix	Creating a Secure and Unified eBusiness Infrastructure Available from: http://www.oblix.com/resources/whitepapers/index.html
Oblix	An Overview of Federated Identity Architecture Available from: http://www.oblix.com/resources/whitepapers/index.html
Oblix	Creating a Secure and Unified eBusiness Infrastructure Available from: http://www.oblix.com/resources/whitepapers/index.html
Computerworld	Five rules for top-notch user management and provisioning Available from: http://www.computerworld.com/securitytopics/security/story/0,10801,90407,00.html?f=x10

If thoroughly reviewed, the articles clearly indicate that the basic premise of User and Group Management has its foundations in Identity management (e.g. Identity Establishment and Mapping services). Thus, the technological recommendations from those security services needs to be part of the User and Group Management service. Additionally, the following are key recommendations from the literature:

- Deprecation or changing of all default accounts is needed.

This would mean that for Operating Systems, that the default user accounts should be removed or a least have the credentials changed (e.g. passwords). This should include ALL user accounts, including remote diagnostic accounts.

- Accounts that are not frequently used should be de-activated.

One of the most prevalent issues is determining the usage of a particular user account. The Security Domain's policy should specify a period of inactivity that causes user accounts to become inactive (e.g. no longer valid but available to be renewed/re-activated).

- Group Accounts should be granular enough to provide appropriate access privilege restriction.

At a general level, the following privileges need to be addressed:

Remote Login: Does the User belong to a group that has the privilege to make use of the computational resource remotely.

Execute: Does the User belong to a group that has the privilege to execute a particular program/application.

Access: Does the User belong to a group that has the privilege to access the information contained in a computational resource (e.g. file, database, etc...). There is a need for further granularity based upon the particular instance of file/resource.

Modification: Does the User belong to a group that has the privilege to modify the information contained in a computational resource. Similar granularity to Access is typically needed.

View: Does the User belong to a group that is allowed to view the existence of a particular resource (e.g. the ability to have a directory with particular files appearing in the directory response).

Within the IECSA architecture, there are two additional privileges that need to be considered. These are privileges that typically relate to interactions with field devices and not business level computational resources, although they may be needed in some cases (e.g. User Management): Configuration and Control Privileges.

Configuration: Does the user belong to a group that has the privilege to change the configuration of a computational resource. There may be further granularity required based upon the types of configuration supported by the computational resource (e.g. users, protective schemes, control settings, initial values, setting groups, etc.).

Control: Does the user belong to a group that has the privilege to change /control real-time process aspects of a computational resource. Further granularity may need to be provided based upon the class of controllable resources available on a computational resource.

- Within a Security Domain, there needs to be centralized management and storage of the user/account information, typically in a directory like environment.
- Single Sign-On is a typical objective of intra-domain management.

This service can be subdivided into a policy part and an actual security service: Setting and Verifying User Accounts.

3.2.1.3.3.1 *Setting and Verifying User Accounts Service*

This service is for assigning and validating authority given to a user or a group of users in accessing/utilizing specific enterprise resources.

There is no authoritative technology to evaluate for this service. However, from an abstract security service level such a service needs to exist. The service needs to provide the functionality of:

- Lifecycle management of user and group account. This includes the ability to create, renew, deprecate, modify, and delete users and groups.
- Credential Management is required so that passwords, certificates, etc. can be replaced/renewed/deprecated as required.

3.2.1.4 *Security Training*

Security training implies continuous training on security threats, security technologies, corporate, and legal policies that impact security. Security measures analysis is a periodic, and best practice that is needed. It is this training in the security process that will allow the security infrastructure to evolve.

When attempting to evaluate the security process on an enterprise basis, as is required by IECSA, it is impossible to account for all of the business entities, politics, and technological choices that could be chosen by the various entities that aggregate into the enterprise. Thus to discuss security on an enterprise level is often a daunting task that may never come to closure. In order to simplify the discussion, allow for various entities to control their own resources, and to enable the discussion to focus on the important aspects, security will be discussed in regards to Security Domains

3.2.1.5 Impact of Security Policy for Credential Renewal on Availability

Policy: The developed policy for credential renewal and revocation will have an impact on availability. If an in-use credential is revoked/deprecated incorrectly, then information exchange will not be able to be achieved, thus impacting availability. Thus, policy development must be particularly careful in only revoking the credentials for appropriate reasons.

However, the actual revocation, based upon stolen or compromised credentials will have an impact on availability. Thus the time required to renew, create, or deploy new credentials needs to be factored into the availability calculation. For further discussion see credential renewal.

3.2.2 Security Frameworks and Policy Documents

3.2.2.1 ISO/IEC Security Best Practices

3.2.2.2 ISO/IEC 10164-8:1993 Information technology -- Open Systems Interconnection -- Systems Management: Security audit trail function

URL: <http://www.iso.ch>

Establishes user requirements for the service definition needed to support the security audit trail reporting function, defines the service provided by the security audit trail reporting function, specifies the protocol that is necessary in order to provide the service, defines the relationship between the service and management notifications, defines relationships with other systems management functions, specifies conformance requirements.

Keywords: Security, Audit, Non-Repudiation

3.2.2.3 ISO/IEC 18014-1:2002 Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework

URL: <http://www.iso.ch>

ISO/IEC 18014-1:2002:

1. identifies the objective of a time-stamping authority;
2. describes a general model on which time-stamping services are based;
3. defines time-stamping services;
4. defines the basic protocols of time-stamping;
5. specifies the protocols between the involved entities.

Keywords: Audit, Non-Repudiation, Security

3.2.2.4 ISO/IEC 18014-2:2002 Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens

URL: <http://www.iso.ch>

ISO/IEC 18014-2:2002 describes time-stamping services producing independent tokens. It describes a general model for time-stamping services of this type and the basic components used to construct a time-stamping service of this type, it defines the data structures and protocols used to interact with a time-stamping service of this type, and it describes specific instances of such time-stamping services.

The usage of independent tokens presumes a high trust on the time-stamping authority (TSA).

Three independent mechanisms are currently covered:

Time-stamps using digital signatures

In this mechanism the TSA has an asymmetric key pair, and uses the private key to digitally sign the time-stamp token. Signature verification will use the public key. This mechanism may require the use of a PKI (Public Key Infrastructure).

Time-stamps using message authentication codes

In this mechanism the TSA uses a secret key to digitally bind the time association. The time-stamp token is authenticated using a Message Authentication Code (MAC). When using this mechanism, the TSA is needed to carry out the verification.

Time-stamps using archiving

In this mechanism the TSA returns a time-stamp token that only has reference information to bind the time-stamp to the messageImprint in the time-stamp token. The TSA archives locally enough information to verify that the time-stamp is correct.

Keywords: TSA, Time Stamping Services, ISO/IEC 18014:2002

3.2.2.5 ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens

URL: <http://www.iso.ch>

The documents describe the timestamp request protocol and the timestamp verification protocol for timestamp based credentials/token generators.

Keywords:

3.2.2.6 ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework

URL: <http://www.iso.ch/>

Provides guidance to the creation of a robust audit and alarming framework that is critical for intrusion detection.

Keywords: Audit, Non-Repudiation, Security

3.2.2.7 ISO JTC1 SC37 SD 2 - Harmonized Biometric Vocabulary

URL:

Provides a dictionary of vocabulary that should be used as the standardized vocabulary when discussing biometrics.

Keywords:

3.2.2.8 Federal Security Best Practices

3.2.2.9 CICS 6731.01 Global Command and Control System Security Policy

URL: http://www.dtic.mil/cjcs_directives/cdata/unlimit/6722_02.pdf

Provides a framework and policy directives that allow security to assist in operational assurance.

Keywords:

3.2.2.10 FIPS PUB 112 Password Usage

URL: <http://www.itl.nist.gov/fipspubs/fip112.htm>
<http://csrc.nist.gov/publications/fips/fips112/fip112-2.pdf>

The document specifies basic security criteria for two different uses of passwords in an ADP system, (1) personal identity authentication and (2) data access authorization. It establishes the basic criteria for the design, implementation and use of a password system in those systems where passwords are used. It identifies fundamental ADP management functions pertaining to passwords and specifies some user actions required to satisfy these functions. In addition, it specifies several technical features that may be implemented in an ADP system in order to support a password system. An implementation schedule is established for compliance with the Standard. Numerous guidelines are provided in the Appendices for managers and users seeking to comply with the Standard.

Keywords: Identity Establishment, Policy, Authorization for Access Control, Credential Renewal, Security

3.2.2.11 FIPS PUB 113 Computer Data Authentication

URL: <http://www.itl.nist.gov/fipspubs/fip113.htm>
<http://www.dice.ucl.ac.be/crypto/standards/fips/fips113/fip113.pdf>

This publication specifies a standard to be used by Federal organizations that require that the integrity of computer data be cryptographically authenticated. In addition, it may be used by any organization whenever cryptographic authentication is desired. Cryptographic authentication of data during transmission between electronic components or while in storage is necessary to maintain the integrity of the information represented by the data. The standard specifies a cryptographic authentication algorithm for use in ADP systems and networks. The authentication algorithm makes use of the Data Encryption Standard (DES) cryptographic algorithm as defined in Federal Information Processing Standard 46 (FIPS PUB 46).

Keywords: Information Integrity, Confidentiality, Privacy, Authorization for Access Control, Setting and Verifying User Authorization, Encryption, Spoof, Security

3.2.2.12 IETF Security Best Practices Internet Requests for Comments (RFCs)

3.2.2.13 RFC 1102 Policy routing in Internet protocols

URL: <http://www.ietf.org/rfc/rfc1102.txt>

An integral component of the Internet protocols is the routing function, which determines the series of networks and gateways a packet will traverse in passing from the source to the destination. Although there have been a number of routing protocols used in the Internet, they share the idea that one route should be selected out of all available routes based on minimizing some measure of the route, such as delay. Recently, it has become important to select routes in order to restrict the use of network resources to certain classes of customers. These considerations, which are usually described as resource policies, are poorly enforced by the existing technology in the Internet. This document proposes an approach to integrating policy controls into the Internet.

Keywords: Policy, Security

3.2.2.14 RFC 1322 A Unified Approach to Inter-Domain Routing

URL: <http://www.ietf.org/rfc/rfc1322.txt>

The document's focus is on scalability to very large networks and functionality, as well as scalability, to support routing in an environment of heterogeneous services, requirements, and route selection criteria.

Keywords: Policy, Security

3.2.2.15 RFC 1351 SNMP Administrative Model

URL: <http://www.ietf.org/rfc/rfc1351.txt>

This memo presents an elaboration of the SNMP administrative model set forth in [1]. It describes how the elaborated administrative model is applied to realize effective network management in a variety of configurations and environments. The model described here entails the use of distinct identities for peers that exchange SNMP messages. Thus, it represents a departure from the community-based administrative model set forth in [1]. By unambiguously identifying the source and intended recipient of each SNMP message, this new strategy improves upon the historical community scheme both by supporting a more convenient access control model and allowing for effective use of asymmetric (public key) security protocols in the future.

Keywords: Policy, Security

3.2.2.16 RFC 2008 Implications of Various Address Allocation Policies for Internet Routing

URL: <http://www.ietf.org/rfc/rfc2008.txt>

Keywords: IP unicast address allocation and management are essential operational functions for the Public Internet. The exact policies for IP unicast address allocation and management continue to be the subject of many discussions. Such discussions cannot be pursued in a vacuum - the participants must understand the technical issues and implications associated with various address allocation and management policies.

Keywords: The purpose of this document is to articulate certain relevant fundamental technical issues that must be considered in formulating unicast address allocation and management policies for the Public Internet, and to provide recommendations with respect to these policies.

Keywords:

3.2.2.17 RFC 2196 Site Security Handbook

URL: [http:// www.ietf.org/rfc/rfc2196.txt](http://www.ietf.org/rfc/rfc2196.txt)

This handbook is a guide to developing computer security policies and procedures for sites that have systems on the Internet. The purpose of this handbook is to provide practical guidance to administrators trying to secure their information and services. The subjects covered include policy content and formation, a broad range of technical system and network security topics, and security incident response.

Keywords: Policy, Security

3.2.2.18 RFC 2276 Architectural Principles of Uniform Resource Name Resolution

URL: [http:// www.ietf.org/rfc/rfc2276.txt](http://www.ietf.org/rfc/rfc2276.txt)

This document addresses the issues of the discovery of URN (Uniform Resource Name) resolver services that in turn will directly translate URNs into URLs (Uniform Resource Locators) and URCs (Uniform Resource Characteristics). The document falls into three major parts, the assumptions underlying the work, the guidelines in order to be a viable Resolver Discovery Service or RDS, and a framework for designing RDSs. The guidelines fall into three principle areas: evolvability, usability, and security and privacy. An RDS that is compliant with the framework will not necessarily be compliant with the guidelines. Compliance with the guidelines will need to be validated separately.

3.2.2.19 RFC 2350 Expectations for Computer Security Incident Response

URL: [http:// www.ietf.org/rfc/rfc2350.txt](http://www.ietf.org/rfc/rfc2350.txt)

The purpose of this document is to express the general Internet community's expectations of Computer Security Incident Response Teams (CSIRTs). It is not possible to define a set of requirements that would be appropriate for all teams, but it is possible and helpful to list and describe the general set of topics and issues that are of concern and interest to constituent communities.

CSIRT constituents have a legitimate need and right to fully understand the policies and procedures of 'their' Computer Security Incident Response Team. One way to support this understanding is to supply detailed information which users may consider, in the form of a formal template completed by the CSIRT. An outline of such a template and a filled in example are provided.

3.2.2.20 RFC 2386 A Framework for QoS-based Routing in the Internet

URL: [http:// www.ietf.org/rfc/rfc2386.txt](http://www.ietf.org/rfc/rfc2386.txt)

Keywords: QoS-based routing has been recognized as a missing piece in the evolution of QoS-based service offerings in the Internet. This document describes some of the QoS-based routing issues and requirements, and proposes a framework for QoS-based routing in the Internet. This framework is based on extending the current Internet routing model of intra and interdomain routing to support QoS.

3.2.2.21 RFC 2401 Security Architecture for the Internet Protocol

URL: <http://www.ietf.org/rfc/rfc2401.txt>

This memo specifies the base architecture for IPsec compliant systems. The goal of the architecture is to provide various security services for traffic at the IP layer, in both the IPv4 and IPv6 environments. This document describes the goals of such systems, their components and how they fit together with each other and into the IP environment. It also describes the security services offered by the IPsec protocols, and how these services can be employed in the IP environment. This document does not address all aspects of IPsec architecture.

Keywords: Policy, Security, Encryption, Path Routing and QOS, Confidentiality, Encryption, Security

3.2.2.22 RFC 2505 Anti-Spam Recommendations for SMTP MTAs

URL: <http://www.ietf.org/rfc/rfc2505.txt>

This memo gives a number of implementation recommendations for SMTP, [1], MTAs (Mail Transfer Agents, e.g. sendmail, [8]) to make them more capable of reducing the impact of spam(*). The intent is that these recommendations will help clean up the spam situation, if applied on enough SMTP MTAs on the Internet, and that they should be used as guidelines for the various MTA vendors. We are fully aware that this is not the final solution, but if these recommendations were included, and used, on all Internet SMTP MTAs, things would improve considerably and give time to design a more long term solution. The Future Work section suggests some ideas that may be part of such a long term solution. It might, though, very well be the case that the ultimate solution is social, political, or legal, rather than technical in nature.

Keywords:

3.2.2.23 RFC 2518 HTTP Extensions for Distributed Authoring - WEBDAV

URL: <http://www.ietf.org/rfc/rfc2518.txt>

This document describes an extension to the HTTP/1.1 protocol that allows clients to perform remote web content authoring operations. This extension provides a coherent set of methods, headers, request entity body formats, and response entity body formats that provide operations for:

Properties: The ability to create, remove, and query information about Web pages, such as their authors, creation dates, etc. Also, the ability to link pages of any media type to related pages.

Collections: The ability to create sets of documents and to retrieve a hierarchical membership listing (like a directory listing in a file system).

Locking: The ability to keep more than one person from working on a document at the same time. This prevents the "lost update problem," in which modifications are lost as first one author then another writes changes without merging the other author's changes.

Namespace Operations: The ability to instruct the server to copy and move Web resources.

Requirements and rationale for these operations are described in a companion document, "Requirements for a Distributed Authoring and Versioning Protocol for the World Wide Web" [RFC2291].

Keywords:

3.2.2.24 RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

URL: <http://www.ietf.org/rfc/rfc2527.txt>

The purpose of this document is to establish a clear relationship between certificate policies and CPSs, and to present a framework to assist the writers of certificate policies or CPSs with their tasks. In particular, the framework identifies the elements that may need to be considered in formulating a certificate policy or a CPS. The purpose is not to define particular certificate policies or CPSs, per se.

Keywords: Policy, Identity Establishment, Identity Mapping, Credential Renewal, Spoof, Security

Keywords:

3.2.2.25 RFC 2725 Routing Policy System Security

URL: <http://www.ietf.org/rfc/rfc2725.txt>

The RIPE database specifications and RPSL language define languages used as the basis for representing information in a routing policy system. A repository for routing policy system information is known as a routing registry. A routing registry provides a means of exchanging information needed to address many issues of importance to the operation of the Internet. The implementation and deployment of a routing policy system must maintain some degree of integrity to be of any operational use. This document addresses the need to assure integrity of the data by providing an authentication and authorization model.

Keywords:

3.2.2.26 RFC 2775 Internet Transparency

URL: <http://www.ietf.org/rfc/rfc2775.txt>

This document describes the current state of the Internet from the architectural viewpoint, concentrating on issues of end-to-end connectivity and transparency. It concludes with a summary of some major architectural alternatives facing the Internet network layer.

Keywords:

3.2.2.27 RFC 2993 Architectural Implications of NAT

URL: <http://www.ietf.org/rfc/rfc2993.txt>

In light of the growing interest in, and deployment of network address translation (NAT) RFC-1631, this paper will discuss some of the architectural implications and guidelines for implementations. It is assumed the reader is familiar with the address translation concepts presented in RFC-1631.

Keywords:

Keywords:

3.2.2.28 RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

URL: <http://www.ietf.org/rfc/rfc3411.txt>

This document describes an architecture for describing Simple Network Management Protocol (SNMP) Management Frameworks. The architecture is designed to be modular to allow the evolution of the SNMP protocol standards over time. The major portions of the architecture are an SNMP engine containing a Message Processing Subsystem, a Security Subsystem and an Access Control Subsystem, and possibly multiple SNMP applications that provide specific functional processing of management data. This document obsoletes RFC 2571.

Keywords:

3.2.2.29 Other Security Best Practices

3.2.2.30 21 CFR Part 11 Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application

URL: <http://www.fda.org>

The rule provides criteria under which FDA will consider electronic records to be equivalent to paper records, and electronic signatures equivalent to traditional handwritten signatures. Part 11 (21 CFR part 11) applies to any paper records required by statute or agency regulations and supersedes any existing paper record requirements by providing that electronic records may be used in lieu of paper records. Electronic signatures which meet the requirements of the rule will be considered to be equivalent to full handwritten signatures, initials, and other general signings required by agency regulations.

Keywords:

3.2.2.31 ISA-99 Integrating Electronic Security into the Manufacturing and Control Systems Environment

URL: <http://www.isa.org>

Is a work, in progress, that is attempting to standardized/document issues that allow risk-assessment to be factored into the development of security policies.

Keywords:

3.2.2.32 EPRI 100898 Scoping Study on Security Processes and Impacts

URL: http://www.epri.com/OrderableItemDesc.asp?product_id=1008988

“The primary objective of this Scoping Study is the assessment of the financial and societal costs of implementing security measures. Financial costs include the costs for developing security policies and implementing security countermeasure technologies. Societal costs include the impact of security policies and technologies on the efficiency of personnel and systems.

A second objective of this Scoping Study is twofold: (a) to assess whether or not the Internet can provide adequate security for the different utility control center functions, including power operations and market operations; and (b) to identify viable alternatives to the Internet for this purpose. This assessment would include determining what alternative communication means are possible and what the impact would be to move functions using the Internet to using these alternative communications methods. As a part of this assessment, the communication security needs of different functions would be addressed, along with possible alternative communications methods, such as privately owned media, private access to media owned by telecommunications

providers, and secure access to more public media. The assessment methodology does not directly analyze the use of alternative media, but discusses the mechanisms for analysis. Specific recommendations may be developed as part of future work.”

Keywords:

3.2.2.33 EPRI 100174 Communication Security Assessment for the United States Electric Utility Infrastructure

URL: <http://www.epri.com>

Provides an overview of the state of the US power utility infrastructure.

Keywords:

3.2.2.34 NIST SP 500-166 Computer Viruses and Related Threats: A Management Guide

URL: <http://www.csrc.nist.gov/publications/nistpubs/>

Describes policies and procedures for management, detection, and elimination of viruses.

Keywords:

3.2.2.35 Radius Protocol Security and Best Practices

URL: <http://www.microsoft.com/windows2000/techinfo/administration/radius.asp>

Remote Authentication Dial-In User Service (RADIUS) is commonly used to provide centralized authentication, authorization, and accounting for dial-up, virtual private network, and, more recently, wireless network access. This article provides an overview of RADIUS and the Extensible Authentication Protocol (EAP) and describes how to minimize or resolve various security issues of the RADIUS protocol using implementation and deployment best practices.

Keywords: RADIUS, Remote Authentication Dial-In User Service, Extensible Authentication Protocol, EAP

4. Security Documents

4.1 Security Technology Documents

4.1.1 ISO/IEC Documents on Security Technologies

4.1.1.1 ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=29257&ICS1=35&ICS2=240&ICS3=15>

This Standard specifies the physical characteristics of integrated circuit(s) cards with contacts. It applies to identification cards of the ID-1 card type that may include embossing and/or a magnetic stripe

Keywords:

4.1.1.2 ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=14735&ICS1=35&ICS2=240&ICS3=15>

This part of ISO/IEC 7816 specifies the power and signal structures, and information exchange between an integrated circuit(s) card and an interface device such as a terminal. It also covers signal rates, voltage levels, current values, parity convention, operating procedure, transmission mechanisms and communication with the card. It does not cover information and instruction content, such as identification of issuers and users, services and limits, security features, journaling and instruction definitions.

Keywords:

4.1.1.3 ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=34974&ICS1=35&ICS2=240&ICS3=15>

Update to the original ISO/IEC 7816-3: 1997. Adds signal levels of 5, 3, and 1.8 V.

Keywords:

4.1.1.4 ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=14738&ICS1=35&ICS2=240&ICS3=15>

This part of ISO/IEC 7816 specifies

- the content of the messages, commands and responses, transmitted by the interface device to the card and conversely,
- the structure and content of the historical bytes sent by the card during the answer to reset,
- the structure of files and data, as seen at the interface when processing interindustry commands for interchange.
- access methods to files and data in the card,
- a security architecture defining access rights to files and data in the card,

- methods for secure messaging,
 - access methods to the algorithms processed by the card. It does not describe these algorithms.
- It does not cover the internal implementation within the card and/or the outside world.

It allows further standardization of additional interindustry commands and security architectures.

Keywords:

4.1.1.5 ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=28731&ICS1=35&ICS2=240&ICS3=15>

Adds security and management commands to the original 7816-4.

Keywords:

4.1.1.6 ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=19980&ICS1=35&ICS2=240&ICS3=15>

This standard specifies a numbering system for application identifiers and a registration procedure for application provider identifiers.

Keywords: Numbering system, registration procedure

4.1.1.7 ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=28869&ICS1=35&ICS2=240&ICS3=15>

This standard specifies: the concept of a SCQL database (SCQL = Structured Card Query Language based on SQL, see MS ISO 9075); and the related inter industry enhanced commands. These commands allow access to information store on smartcards.

Keywords: SCQL, SQL, ISO/IEC 7816

4.1.1.8 ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=30194&ICS1=35&ICS2=240&ICS3=15>

This part of ISO/IEC 7816 specifies:

- security protocols for use in cards;
- secure messaging extensions;
- the mapping of the security mechanisms on to the card(s) security functions/services, including a description of the in-card security mechanisms;
- data elements for security support;
- the use of algorithms implemented on the card though the algorithms themselves are not described in detail;
- the use of certificates;
- security related commands.

Keywords: Card Security Methods, certificates, security commands

4.1.1.9 ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=31035&ICS1=35&ICS2=240&ICS3=15>

This standard specifies: a description and coding of the life cycle of cards and related objects; a description and coding of security attributes of card related objects; functions and syntax of additional inter industry commands; data elements associated with these commands; and a mechanism for initiating card-originated messages. This part of ISO 7816 does not cover the internal implementation within the card and/or the outside world.

Keywords: Card life cycle, ISO 7816

4.1.1.10 ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=30558&ICS1=35&ICS2=240&ICS3=15>

This part of ISO/IEC 7816 specifies the power, signal structures, and the structure for the answer to reset between an integrated circuit(s) card with synchronous transmission and an interface device such as a terminal. The specifications in ISO/IEC 7816-3 apply where appropriate, unless otherwise stated here. It also covers signal rates, operating conditions, and communication with the integrated circuit(s) card.

This part of ISO/IEC 7816 specifies two types of synchronous cards: type 1 and type 2.

Keywords:

4.1.1.11 ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=31419&ICS1=35&ICS2=240&ICS3=15>

Defines basic fields used by biometric data (e.g. security, additional biometric information, and the biometric data).

Keywords:

4.1.1.12 ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=35168&ICS1=35&ICS2=240&ICS3=15>

From <http://www.csa-intl.org>:

ISO/IEC 7816-15:2004 specifies a card application. This application contains information on cryptographic functionality. Further, ISO/IEC 7816-15:2004 defines a common syntax (in ASN.1) and format for the cryptographic information and mechanisms to share this information whenever appropriate.

ISO/IEC 7816-15:2004 supports the following capabilities:

- * storage of multiple instances of cryptographic information in a card;
- * use of the cryptographic information;
- * retrieval of the cryptographic information;
- * cross-referencing of the cryptographic information with DOs defined in ISO/IEC 7816 when appropriate;
- * different authentication mechanisms; and
- * multiple cryptographic algorithms.

Keywords:

4.1.1.13 ISO 9735-9:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 9: Security key and certificate management message (message type- KEYMAN)

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=35040&ICS1=35&ICS2=240&ICS3=60>

This part of ISO 9735 for batch EDIFACT security defines the security key and certificate management message KEYMAN.

Keywords:

4.1.1.14 ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=32210&ICS1=35&ICS2=100&ICS3=70>

This standard defines a framework for public-key certificates. That framework includes specification of data objects used to represent the certificates themselves as well as revocation notices for issued certificates that should no longer be trusted.

Keywords:

4.1.1.15 ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=34551&ICS1=35&ICS2=100&ICS3=70>

Defines additional attributes for ISO/IEC 9594-8.

Keywords:

4.1.1.16 ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=35036&ICS1=35&ICS2=240&ICS3=60>

This part of ISO 9735 specifies syntax rules for EDIFACT security. It provides a method to address message/package level, group level and interchange level security for authenticity, integrity and non-repudiation of origin, in accordance with established security mechanisms.

Keywords:

Keywords:

4.1.1.17 ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=18166&ICS1=35&ICS2=100&ICS3=70>

Describes an Access Control Security Model and the management information necessary for creating and administering access control associated with OSI System Managements. Security policy adopted for any instance of use is not specified and is left as an implementation choice. This Specification is of generic application and is applicable to the security management of many types of application. It is expected to be adopted for TMN use. Identical text is published as ITU-T Recommendation X.741.

Keywords:

4.1.1.18 ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=24404&ICS1=35&ICS2=100&ICS3=1>

From <http://www.csa-intl.org>:

The security frameworks address the application of security services in an Open Systems environment, where the term Open Systems is taken to include areas such as Database, Distributed Applications, ODP and OSI. The security frameworks are concerned with defining the means of providing protection for systems and objects within systems, and with the interactions between systems. The security frameworks are not concerned with the methodology for constructing systems or mechanisms.

The security frameworks address both data elements and sequences of operations (but not protocol elements) that are used to obtain specific security services. These security services may apply to the communicating entities of systems as well as to data exchanged between systems, and to data managed by systems.

The security frameworks provide the basis for further standardization, providing consistent terminology and definitions of generic abstract service interfaces for specific security

requirements. They also categorize the mechanisms that can be used to achieve those requirements.

One security service frequently depends on other security services, making it difficult to isolate one part of security from the others. The security frameworks address particular security services, describe the range of mechanisms that can be used to provide the security services, and identify interdependencies between the services and the mechanisms. The description of these mechanisms may involve a reliance on a different security service, and it is in this way that the security frameworks describe the reliance of one security service on another.

This part of the security frameworks:

- describes the organization of the security frameworks;
- defines security concepts which are required in more than one part of the security frameworks;
- describes the inter-relationship of the services and mechanisms identified in other parts of the frameworks.

Keywords:

4.1.1.19 ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=18198&ICS1=35&ICS2=100&ICS3=1>

From <http://www.csa-intl.org>:

This series of Recommendations / International Standards on Security Frameworks for Open Systems addresses the application of security services in an Open Systems environment, where the term "Open Systems" is taken to include areas such as Database, Distributed Applications, Open Distributed Processing and OSI. The Security Frameworks are concerned with defining the means of providing protection for systems and objects within systems, and with the interactions between systems. The Security Frameworks are not concerned with the methodology for constructing systems or mechanisms.

The Security Frameworks address both data elements and sequences of operations (but not protocol elements) that are used to obtain specific security services. These security services may apply to the communicating entities of systems as well as to data exchanged between systems, and to data managed by systems.

This Recommendation / International Standard:

- defines the basic concepts for authentication;
- identifies the possible classes of authentication mechanisms;
- defines the services for these classes of authentication mechanism;
- identifies functional requirements for protocols to support these classes of authentication mechanism; and
- identifies general management requirements for authentication.

A number of different types of standards can use this framework including:

- (1) standards that incorporate the concept of authentication;
- (2) standards that provide an authentication service;
- (3) standards that use an authentication service;
- (4) standards that specify the means to provide authentication within an open system architecture; and
- (5) standards that specify authentication mechanisms.

Keywords:

4.1.1.20 ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework

URL: <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=18199&ICS1=35&CS2=100&ICS3=1>

From <http://www.csa-intl.org>:

The Security Frameworks are intended to address the application of security services in an Open Systems environment, where the term Open Systems is taken to include areas such as Database, Distributed Applications, ODP and OSI. The Security Frameworks are concerned with defining the means of providing protection for systems and objects within systems, and with the interactions between systems. The Security Frameworks are not concerned with the methodology for constructing systems or mechanisms.

The Security Frameworks address both data elements and sequences of operations (but not protocol elements) that are used to obtain specific security services. These security services may apply to the communicating entities of systems as well as to data exchanged between systems, and to data managed by systems.

In the case of Access Control, accesses may either be to a system (i.e. to an entity that is the communicating part of a system) or within a system. The information items that need to be presented to obtain the access, as well as the sequence of operations to request the access and for notification of the results of the access, are considered to be within the scope of the Security Frameworks. However, any information items and operations that are dependent solely on a particular application and that are strictly concerned with local access within a system are considered to be outside the scope of the Security Frameworks.

Many applications have requirements for security to protect against threats to resources, including information, resulting from the interconnection of Open Systems. Some commonly known threats, together with the security services and mechanisms that can be used to protect against them, in an OSI environment, are described in CCITT Rec. X.800 / ISO 7498-2.

The process of determining which uses of resources within an Open System environment are permitted and, where appropriate, preventing unauthorized access is called access control. This Recommendation / International Standard defines a general framework for the provision of access control services.

This Security Framework:

- (a) defines the basic concepts for access control;
- (b) demonstrates the manner in which the basic concepts of access control can be specialized to support some commonly recognized access control services and mechanisms;
- (c) defines these services and corresponding access control mechanisms;
- (d) identifies functional requirements for protocols to support these access control services and mechanisms;
- (e) identifies management requirements to support these access control services and mechanisms;
- (f) addresses the interaction of access control services and mechanisms with other security services and mechanisms.

As with other security services, access control can be provided only within the context of a defined security policy for a particular application. The definition of access control policies is outside the scope of this Recommendation / International Standard, however, some characteristics of access control policies are discussed.

It is not a matter for this Recommendation / International Standard to specify details of the protocol exchanges which may need to be performed in order to provide access control services.

This Recommendation / International Standard does not specify particular mechanisms to support these access control services or the details of security management services and protocols.

A number of different types of standard can use this framework including:

- (a) standards that incorporate the concept of access control;
- (b) standards that specify abstract services that include access control;
- (c) standards that specify uses of an access control service;
- (d) standards that specify the means of providing access control within an Open System environment; and
- (e) standards that specify access control mechanisms.

Keywords:

4.1.1.21 ISO/IEC 10181-4:1997 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework

URL: <http://www.iso.ch>

From <http://www.csa-intl.org>:

This Recommendation / International Standard addresses the application of security services in an Open Systems environment, where the term "Open Systems" is taken to include areas such as Database, Distributed Applications, Open Distributed Processing and OSI. The Security Frameworks are concerned with defining the means of providing protection for systems and objects within systems, and with the interactions between systems. The Security Frameworks are not concerned with the methodology for constructing systems or mechanisms.

The Security Frameworks address both data elements and sequences of operations (but not protocol elements) that are used to obtain specific security services. These security services may apply to the communicating entities of systems as well as to data exchanged between systems, and to data managed by systems.

This Recommendation / International Standard:

- defines the basic concepts of Non-repudiation;
- defines general Non-repudiation services;
- identifies possible mechanisms to provide the Non-repudiation services;
- identifies general management requirements for Non-repudiation services and mechanisms.

As with other security services, Non-repudiation can only be provided within the context of a defined security policy for a particular application. The definitions of security policies are outside the scope of this Recommendation / International Standard.

The scope of this Recommendation / International Standard does not include specification of details of the protocol exchanges which need to be performed in order to achieve Non-repudiation.

This Recommendation / International Standard does not describe in detail the particular mechanisms that can be used to support the Non-repudiation services nor does it give details of the supporting security management services and protocols.

4.1.1.22 ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle

URL: <http://www.iso.ch>

Keywords: Specifies the principles for the protection of the Integrated Circuits from their manufacture and issue, through use to their termination. Annex A forms an integral part of this standard. Annexes B and C are for information only.

Keywords:

4.1.1.23 ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management

URL: <http://www.iso.ch>

Specifies policies, procedures, and algorithms for performing key management for financial transaction cards.

Keywords:

4.1.1.24 ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems

URL: <http://www.iso.ch>

Specifies an architecture for security financial transaction systems when using transaction cards.

Keywords:

4.1.1.25 ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security

URL: <http://www.iso.ch>

Presents the basic management concepts and models that are essential for an introduction into the management of IT security. These concepts and models are further discussed and developed in the remaining parts to provide more detailed guidance.

Keywords:

4.1.1.26 ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security

URL: <http://www.iso.ch>

URL: <http://www.csa-intl.org/onlinestore/GetCatalogItemDetails.asp?mat=2414358&Parent=2586>

From <http://www.csa-intl.org>:

The guidelines in this part of ISO/IEC TR 13335 address subjects essential to the management of IT security, and the relationship between those subjects. These guidelines are useful for the identification and the management of all aspects of IT security.

Familiarity with the concepts and models introduced in Part 1 is essential for a complete understanding of this part.

Keywords:

4.1.1.27 ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security

URL: <http://www.iso.ch>

URL: <http://www.csa-intl.org/onlinestore/GetCatalogItemDetails.asp?mat=2416204&Parent=3548>

From <http://www.csa-intl.org>:

ISO/IEC TR 13335-5 provides guidance with respect to networks and communications to those responsible for the management of IT security. This guidance supports the identification and analysis of the communications related factors that should be taken into account to establish network security requirements.

This part of ISO/IEC TR 13335 builds upon Part 4 of this Technical Report by providing an introduction on how to identify appropriate safeguard areas with respect to security associated with connections to communications networks. It is not within the scope of this TR to provide advice on the detailed design and implementation aspects of the technical safeguard areas. That advice will be dealt with in future ISO documents.

Keywords:

4.1.1.28 ISO/IEC 13888-1:1997 Information technology -- Security techniques - - Non-repudiation -- Part 1: General

URL: <http://www.iso.ch>

URL: <http://www.csa-intl.org/onlinestore/GetCatalogDrillDown.asp?Parent=2628>

From <http://www.csa-intl.org>:

Non-repudiation mechanisms provide protocols for the exchange of non-repudiation tokens specific to each non-repudiation service. Non-repudiation tokens consist of Secure Envelopes and/or digital signatures and, optionally, of additional data. Non-repudiation tokens may be stored as non-repudiation information that may be used subsequently by disputing parties or by an adjudicator to arbitrate in disputes.

Depending on the non-repudiation policy in effect for a specific application, and the legal environment within which the application operates, additional information may be required to complete the non-repudiation information, e.g.,

- evidence including a trusted time stamp provided by a Time Stamping Authority,
- evidence provided by a notary which provides assurance about data created or the action or event performed by one or more entities.

Non-repudiation can only be provided within the context of a clearly defined security policy for a particular application and its legal environment. Non-repudiation policies are described in ISO/IEC 10181-4.

This part of ISO/IEC 13888 serves as a general model for subsequent parts specifying non-repudiation mechanisms using cryptographic techniques. ISO/IEC 13888 provides non-repudiation mechanisms for the following phases of non-repudiation:

- evidence generation,
- evidence transfer, storage and retrieval, and
- evidence verification.

Dispute arbitration is outside the scope of ISO/IEC 13888.

Keywords:

**4.1.1.29 ISO/IEC 13888-2:1998 Information technology -- Security techniques -
- Non-repudiation -- Part 2: Mechanisms using symmetric techniques**

URL: <http://www.iso.ch>

This standard provides the same service as ISO/IEC 13888-3, but through the use of symmetric encryption techniques.

Keywords:

**4.1.1.30 ISO/IEC 13888-3:1997 Information technology -- Security techniques -
- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques**

URL: <http://www.iso.ch>

URL: <http://www.csa-intl.org/onlinestore/GetCatalogDrillDown.asp?Parent=2627>

From <http://www.csa-intl.org>:

The goal of the Non-repudiation Service is to generate, collect, maintain, make available and validate evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action. This part of ISO/IEC 13888 specifies mechanisms for the provision of some specific, communication related non-repudiation Services using asymmetric techniques.

Non-repudiation mechanisms are specified to establish the following non-repudiation services:

- non-repudiation of origin,
- non-repudiation of delivery,
- non-repudiation of submission,
- non-repudiation of transport.

Non-repudiation mechanisms involve the exchange of non-repudiation tokens specific for each non-repudiation Service. Non-repudiation tokens consist of digital signatures and additional data. Non-repudiation tokens shall be stored as non-repudiation information that may be used subsequently in case of disputes.

Depending on the non-repudiation policy in effect for a specific application, and the legal environment within which the application operates, additional information may be required to complete the non-repudiation information, e.g.,

- evidence including a trusted time stamp provided by a Time Stamping Authority,
- evidence provided by a notary which provides assurance about the action or event performed by one or more entities.

Non-repudiation can only be provided within the context of a clearly defined security policy for a particular application and its legal environment. Non-repudiation policies are described in the multipart Standard of Security Frameworks for open systems - Part 4: Non-repudiation Framework, ISO/IEC 10181-4.

Keywords:

Keywords:

4.1.1.31 ISO/IEC 15408-1:1999 Information technology -- Security techniques - - Evaluation criteria for IT security -- Part 1: Introduction and general mode

URL: <http://www.iso.ch>

URL: <http://www.csa-intl.org/onlinestore/GetCatalogItemDetails.asp?mat=2414891&Parent=3052>

From <http://www.csa-intl.org>:

This multipart standard ISO/IEC 15408 defines criteria, which for historical and continuity purposes are referred to herein as the Common Criteria (CC), to be used as the basis for evaluation of security properties of IT products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience.

The CC will permit comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them meet these requirements. The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable.

The CC is useful as a guide for the development of products or systems with IT security functions and for the procurement of commercial products and systems with such functions. During evaluation, such an IT product or system is known as a Target of Evaluation (TOE). Such TOEs include, for example, operating systems, computer networks, distributed systems, and applications.

The CC addresses protection of information from unauthorized disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. The CC may also be applicable to aspects of IT security outside of these three. The CC concentrates on threats to that information arising from human activities, whether malicious or otherwise, but may be applicable to some nonhuman threats as well. In addition, the CC may be applied in other areas of IT, but makes no claim of competence outside the strict domain of IT security.

The CC is applicable to IT security measures implemented in hardware, firmware or software. Where particular aspects of evaluation are intended only to apply to certain methods of implementation, this will be indicated within the relevant criteria statements.

Certain topics, because they involve specialized techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of the CC. Some of these are identified below.

a) The CC does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security measures. However, it is recognized that a significant part of the security of a TOE can often be achieved through administrative measures such as organizational, personnel, physical, and procedural controls. Administrative security measures in the operating environment of ISO/IEC 15408-1:1999(E) © ISO/IEC the TOE are treated as secure usage assumptions where these have an impact on the ability of the IT security measures to counter the identified threats.

b) The evaluation of technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered, although many of the concepts addressed will be applicable to that area. In particular, the CC addresses some aspects of physical protection of the TOE.

c) The CC addresses neither the evaluation methodology nor the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is

expected that the CC will be used for evaluation purposes in the context of such a framework and such a methodology.

d) The procedures for use of evaluation results in product or system accreditation are outside the scope of the CC. Product or system accreditation is the administrative process whereby authority is granted for the operation of an IT product or system in its full operational environment. Evaluation focuses on the IT security parts of the product or system and those parts of the operational environment that may directly affect the secure use of IT elements. The results of the evaluation process are consequently a valuable input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related product or system security properties and their relationship to the IT security parts, accreditors should make separate provision for those aspects.

e) The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the CC. Should independent assessment of mathematical properties of cryptography embedded in a TOE be required, the evaluation scheme under which the CC is applied must make provision for such assessments.

Keywords:

**4.1.1.32 ISO/IEC 15408-2:1999 Information technology -- Security techniques -
- Evaluation criteria for IT security -- Part 2: Security functional
requirements**

URL: <http://www.iso.ch>

URL: <http://www.csa-intl.org/onlinestore/GetCatalogItemDetails.asp?mat=2414892&Parent=3053>

From <http://www.csa-intl.org>:

Security functional components, as defined in this part of ISO/IEC 15408, are the basis for the TOE IT security functional requirements expressed in a Protection Profile (PP) or a Security Target (ST). These requirements describe the desired security behavior expected of a Target of Evaluation (TOE) and are intended to meet the security objectives as stated in a PP or an ST. These requirements describe security properties that users can detect by direct interaction with the TOE (i.e. inputs, outputs) or by the TOEs response to stimulus.

Security functional components express security requirements intended to counter threats in the assumed operating environment of the TOE and/or cover any identified organizational security policies and assumptions.

The audience for this part of ISO/IEC 15408 includes consumers, developers, and evaluators of secure IT systems and products. ISO/IEC 15408-1 clause 3 provides additional information on the target audience of ISO/IEC 15408, and on the use of the standard by the groups that comprise the target audience. These groups may use this part of ISO/IEC 15408 as follows:

- Consumers who use ISO/IEC 15408-2 when selecting components to express functional requirements to satisfy the security objectives expressed in a PP or ST. ISO/IEC 15408-1 sub clause 4.3 provides more detailed information on the relationship between security objectives and security requirements.

- Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, may find a standardized method to understand those requirements in this part of ISO/IEC 15408. They can also use the contents of this part of ISO/IEC 15408 as a basis for further defining the TOE security functions and mechanisms that comply with those requirements.

- Evaluators, who use the functional requirements defined in this part of ISO/IEC 15408 in verifying that the TOE functional requirements expressed in the PP or ST satisfy the IT security

objectives and that all dependencies are accounted for and shown to be satisfied. Evaluators also should use this part of ISO/IEC 15408 to assist in determining whether a given TOE satisfies stated requirements.

Keywords:

4.1.1.33 ISO/IEC 15408-3:1999 Information technology -- Security techniques - - Evaluation criteria for IT security -- Part 3: Security assurance requirements

URL: <http://www.iso.ch>

<http://www.csa-intl.org/onlinestore/GetCatalogItemDetails.asp?mat=2414893&Parent=3054>

From <http://www.csa-intl.org>:

This part of ISO/IEC 15408 defines the assurance requirements of the standard. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance, the individual assurance components from which the assurance levels are composed, and the criteria for evaluation of PPs and STs.

Keywords:

4.1.1.34 ISO/IEC 17799:2000 Information technology -- Code of practice for information security management

URL: <http://www.iso.ch>

URL: </iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3=>

From NIST <http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf>:

ISO/IEC 17799 is a code of practice. As such it offers guidelines and voluntary directions for information security management. It is meant to provide a high level, general description of areas currently considered important when initiating, implementing or maintaining information security in an organization.

Keywords:

Keywords:

4.1.1.35 ISO JTC1 SC37 1.37.19784.1 BioAPI - Biometric Application Programming Interface

URL: <http://www.jtc1.org>

This emerging standard on a programming interface that provides the general capability to query and exchange biometric information. It is based upon the work of the BioAPI consortia and the source document can be obtained from their website.

URL: <http://www.bioapi.org/BIOAPI1.1.pdf>

Keywords:

4.1.1.36 ISO JTC1 SC37 1.37.19794 - Biometric Data Interchange Format

URL: <http://www.jtc1.org>

The standardization of the content, meaning and representation of biometric data formats which are specific to a particular biometric technology. To ensure a common look and feel for Biometric Data Structure standards, with notation and transfer formats that provide platform independence and separation of transfer syntax from content definition.

Keywords:

4.1.1.37 ISO JTC1 SC37 1.37.19794.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data

URL: <http://www.jtc1.org>

A specification that further refines ISO JTC1 SC37 1.37.19794 and standardizes formats for finger spectral data (e.g. blood/heat patterns) for biometric identification use.

Keywords:

4.1.1.38 ISO JTC1 SC37 1.37.19794.4 Biometric Data Interchange Format - Part 4: Finger Image Data

URL: <http://www.jtc1.org>

A specification that further refines ISO JTC1 SC37 1.37.19794 and standardizes formats for finger print image (also known as Fingerscanning) for biometric identification use.

The definition of Fingerscanning (supplied by SearchSecurity.com) is:

Fingerscanning is a biometric process, because it involves the automated capture, analysis, and comparison of a specific characteristic of the human body. There are several different ways in which an instrument can bring out the details in the pattern of raised areas (called ridges) and branches (called bifurcations) in a human finger image. The most common methods are optical, thermal, and tactile. They work using visible light analysis, heat-emission analysis, and pressure analysis, respectively.

Keywords:

4.1.1.39 ISO JTC1 SC37 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data

URL: <http://www.jtc1.org>

A specification that further refines ISO JTC1 SC37 1.37.19794 and standardizes formats for facial images for biometric identification use.

Keywords:

Keywords:

4.1.2 Federal Documents on Security Technologies

4.1.2.1 FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)

URL: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

The standard is based on the Rijndael encryption formula and has been in the works since 1997 when the National Institute of Standards and Technology (NIST) began a contest to determine the best encryption algorithm. The new standard is compulsory and binding on Federal agencies for the protection of sensitive, unclassified information. This new robust encryption standard replaces the aging DES standard, which was developed in the 1970s.

Keywords:

4.1.3 IETF Internet Requests for Comments (RFCs) on Security Technologies

4.1.3.1 STD 13 Domain Name System

URL: <http://www.ietf.org/RFC/std/std13.html>

This RFC is an introduction to the Domain Name System (DNS), and omits many details that can be found in a companion RFC, "Domain Names - Implementation and Specification" [RFC-1035]. That RFC assumes that the reader is familiar with the concepts discussed in this memo.

A subset of DNS functions and data types constitutes an official protocol. The official protocol includes standard queries and their responses and most of the Internet class data formats (e.g., host addresses).

However, the domain system is intentionally extensible. Researchers are continuously proposing, implementing and experimenting with new data types, query types, classes, functions, etc. Thus while the components of the official protocol are expected to stay essentially unchanged and operate as a production service, experimental behavior should always be expected in extensions beyond the official protocol.

Keywords: Policy, Identity Establishment, Profile

4.1.3.2 RFC 1004 Distributed-protocol authentication scheme

URL: <http://www.ietf.org/rfc/rfc1004.txt>

The purpose of this RFC is to focus discussion on authentication problems in the Internet and possible methods of solution. The proposed solutions in this document are not intended as standards for the Internet at this time. Rather, it is hoped that a general consensus will emerge as to the appropriate solution to authentication problems, leading eventually to the adoption of standards.

4.1.3.3 RFC 1013 X Window System Protocol, version 11: Alpha update April 1987

URL: <http://www.ietf.org/rfc/rfc1013.txt>

This RFC is distributed to the Internet community for information only. It does not establish an Internet standard. The X window system has been widely reviewed and tested. The Internet community is encouraged to experiment with it.

Keywords:

4.1.3.4 RFC 1034 Domain names - concepts and facilities

URL: <http://www.ietf.org/rfc/rfc1034.txt>

This RFC introduces domain style names, their use for Internet mail and host address support, and the protocols and servers used to implement domain name facilities.

Keywords:

4.1.3.5 RFC 1040 Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication

URL: <http://www.ietf.org/rfc/rfc1040.txt>

This RFC defines message encipherment and authentication procedures, as the initial phase of an effort to provide privacy enhancement services for electronic mail transfer in the Internet. Detailed key management mechanisms to support these procedures will be defined in a subsequent RFC. As a goal of this initial phase, it is intended that the procedures defined here be compatible with a wide range of key management approaches, including both conventional (symmetric) and public-key (asymmetric) approaches for encryption of data encrypting keys. Use of conventional cryptography for message text encryption and/or integrity check computation is anticipated.

Privacy enhancement services (confidentiality, authentication, and message integrity assurance) are offered through the use of end-to-end cryptography between originator and recipient User Agent processes, with no special processing requirements imposed on the Message Transfer System at endpoints or at intermediate relay sites. This approach allows privacy enhancement facilities to be incorporated on a site-by-site or user-by-user basis without impact on other Internet entities. Interoperability among heterogeneous components and mail transport facilities is supported.

Keywords:

4.1.3.6 RFC 1423 Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers

URL: <http://www.ietf.org/rfc/rfc1423.txt>

This document provides definitions, formats, references, and citations for cryptographic algorithms, usage modes, and associated identifiers and parameters used in support of Privacy Enhanced Mail (PEM) in the Internet community. It is intended to become one member of the set of related PEM RFCs. This document is organized into four primary sections, dealing with message encryption algorithms, message integrity check algorithms, symmetric key management algorithms, and asymmetric key management algorithms (including both asymmetric encryption and asymmetric signature algorithms).

Some parts of this material are cited by other documents and it is anticipated that some of the material herein may be changed, added, or replaced without affecting the citing documents. Therefore, algorithm-specific material has been placed into this separate document.

Use of other algorithms and/or modes will require case-by-case study to determine applicability and constraints. The use of additional algorithms may be documented first in Prototype or Experimental RFCs. As experience is gained, these protocols may be considered for incorporation into the standard. Additional algorithms and modes approved for use in PEM in this context will be specified in successors to this document.

Keywords:

4.1.3.7 RFC 1221 Host Access Protocol (HAP) Specification - Version 2

URL: <http://www.ietf.org/rfc/rfc1221.txt>

The Host Access Protocol (HAP) is a network layer protocol (as is X.25). ("Network layer" here means ISO layer 3 lower, the protocol layer below the DoD Internet Protocol (IP) layer [3] and above any link layer protocol.) HAP defines the different types of host-to-network control

messages and host-to-host data messages that may be exchanged over the access link connecting a host and the network packet switch node. The protocol establishes formats for these messages, and describes procedures for determining when each type of message should be transmitted and what it means when one is received.

Keywords:

4.1.3.8 RFC 1305 Network Time Protocol (Version 3) Specification, Implementation

URL: <http://www.ietf.org/rfc/rfc1305.txt>

This document describes Version 3 of the Network Time Protocol (NTP). It supersedes Version 2 of the protocol described in RFC-1119 dated September 1989. However, it neither changes the protocol in any significant way nor obsoletes previous versions or existing implementations. The main motivation for the new version is to refine the analysis and implementation models for new applications at much higher network speeds to the gigabit-per-second regime and to provide for the enhanced stability, accuracy and precision required at such speeds. In particular, the sources of time and frequency errors have been rigorously examined and error bounds established in order to improve performance, provide a model for correctness assertions and indicate timekeeping quality to the user. The revision also incorporates two new optional features, (1) an algorithm to combine the offsets of a number of peer time servers in order to enhance accuracy and (2) improved local-clock algorithms that allow the poll intervals on all synchronization paths to be substantially increased in order to reduce network overhead. It also adds recommendations in regards to security.

Keywords: Authorization for Access Control, Policy, Spoof, Security

4.1.3.9 RFC 1352 SNMP Security Protocols

URL: <http://www.ietf.org/rfc/rfc1352.txt>

The Simple Network Management Protocol (SNMP) specification [1] allows for the protection of network management operations by a variety of security protocols. The SNMP administrative model described in [2] provides a framework for securing SNMP network management. In the context of that framework, this memo defines protocols to support the following three security services:

- o data integrity,
- o data origin authentication, and
- o data confidentiality.

Keywords: Confidentiality, Integrity, Identity Establishment, Policy, Spoof, Security

4.1.3.10 RFC 1507 DASS - Distributed Authentication Security Service

URL: <http://www.ietf.org/rfc/rfc1507.txt>

DASS supports the concept of global identity and network login. A user is assigned a name from a global namespace and that name will be recognized by any node in the network. (In some cases, a resource may be configured as accessible only by a particular user acting through a particular node. That is an access control decision, and it is supported by DASS, but the user is still known by his global identity). From a practical point of view, this means that a user can have a single password (or smart card) which can be used on all systems which allow him access and access control mechanisms can conveniently give access to a user through any computer the

user happens to be logged into. Because a single user secret is good on all systems, it should never be necessary for a user to enter a password other than at initial login. Because cryptographic mechanisms are used, the password should never appear on the network beyond the initial login node.

Keywords: Confidentiality, Identity Establishment, Security

4.1.3.11 RFC 1579 Firewall-Friendly FTP

URL: <http://www.ietf.org/rfc/rfc1579.txt>

This document describes a suggested change to the behavior of FTP client programs. No protocol modifications are required, though we outline some that might be useful.

The FTP protocol uses a secondary TCP connection for actual transmission of files. By default, this connection is set up by an active open from the FTP server to the FTP client. However, this scheme does not work well with packet filter-based firewalls, which in general cannot permit incoming calls to random port numbers. If, on the other hand, clients use the PASV command, the data channel will be an outgoing call through the firewall. Such calls are more easily handled, and present fewer problems.

Keywords: Policy, Firewall Transversall

4.1.3.12 RFC 1591 Domain Name System Structure and Delegation

URL: <http://www.ietf.org/rfc/rfc1591.txt>

This memo provides some information on the structure of the names in the Domain Name System (DNS), specifically the top-level domain names; and on the administration of domains. The Internet Assigned Numbers Authority (IANA) is the overall authority for the IP Addresses, the Domain Names, and many other parameters, used in the Internet. The day-to-day responsibility for the assignment of IP Addresses, Autonomous System Numbers, and most top and second level Domain Names are handled by the Internet Registry (IR) and regional registries.

Keywords: Policy

4.1.3.13 RFC 1608 Representing IP Information in the X.500 Directory

URL: <http://www.ietf.org/rfc/rfc1608.txt>

This document describes the objects necessary to include information about IP networks and IP numbers in the X.500 Directory. It extends the work "Charting networks in the X.500 Directory" [1] where a general framework is presented for representing networks in the Directory by applying it to IP networks. This application of the Directory is intended to support the work of IP network assigning authorities, NICs, as well as other applications looking for a mapping of IP numbers to data of related networks. Furthermore, Autonomous Systems and related routing policy information can be represented in the Directory along with their relationship to networks and organizations.

Keywords:

4.1.3.14 RFC 1612 DNS Resolver MIB Extensions

URL: <http://www.ietf.org/rfc/rfc1612.txt>

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes a set of extensions that instrument DNS resolver functions. This memo was produced by the DNS working group.

With the adoption of the Internet-standard Network Management Framework [4,5,6,7], and with a large number of vendor implementations of these standards in commercially available products, it became possible to provide a higher level of effective network management in TCP/IP-based

internets than was previously available. With the growth in the use of these standards, it has become possible to consider the management of other elements of the infrastructure beyond the basic TCP/IP protocols. A key element of the TCP/IP infrastructure is the DNS.

Up to this point there has been no mechanism to integrate the management of the DNS with SNMP-based managers. This memo provides the mechanisms by which IP-based management stations can effectively manage DNS resolver software in an integrated fashion.

We have defined DNS MIB objects to be used in conjunction with the Internet MIB to allow access to and control of DNS resolver software via SNMP by the Internet community.

Keywords:

4.1.3.15 RFC 1826 IP Authentication Header

URL: <http://www.ietf.org/rfc/rfc1826.txt>

This document describes a mechanism for providing cryptographic authentication for IPv4 and IPv6 datagrams. An Authentication Header (AH) is normally inserted after an IP header and before the other information being authenticated.

The Authentication Header is a mechanism for providing strong integrity and authentication for IP datagrams. It might also provide non-repudiation, depending on which cryptographic algorithm is used and how keying is performed. For example, use of an asymmetric digital signature algorithm, such as RSA, could provide non-repudiation.

Confidentiality, and protection from traffic analysis are not provided by the Authentication Header. Users desiring confidentiality should consider using the IP Encapsulating Security Protocol (ESP) either in lieu of or in conjunction with the Authentication Header [Atk95b]. This document assumes the reader has previously read the related IP Security Architecture document that defines the overall security architecture for IP and provides important background information for this specification [Atk95a].

Keywords:

4.1.3.16 RFC 1827 IP Encapsulating Security Payload (ESP)

URL: <http://www.ietf.org/rfc/rfc1827.txt>

This document describes the IP Encapsulating Security Payload (ESP). ESP is a mechanism for providing integrity and confidentiality to IP datagrams. In some circumstances it can also provide authentication to IP datagrams. The mechanism works with both IPv4 and IPv6.

ESP is a mechanism for providing integrity and confidentiality to IP datagrams. It may also provide authentication, depending on which algorithm and algorithm mode are used. Non-repudiation and protection from traffic analysis are not provided by ESP. The IP Authentication Header (AH) might provide non-repudiation if used with certain authentication algorithms [Atk95b]. The IP Authentication Header may be used in conjunction with ESP to provide authentication. Users desiring integrity and authentication without confidentiality should use the IP Authentication Header (AH) instead of ESP. This document assumes that the reader is familiar with the related document "IP Security Architecture", which defines the overall Internet-layer security architecture for IPv4 and IPv6 and provides important background for this specification [Atk95a].

Keywords:

4.1.3.17 RFC 1919 Classical versus Transparent IP Proxies

URL: <http://www.ietf.org/rfc/rfc1919.txt>

Many modern IP security systems (also called "firewalls" in the trade) make use of proxy technology to achieve access control. This document explains "classical" and "transparent" proxy techniques and attempts to provide rules to help determine when each proxy system may be used without causing problems.

Keywords:

4.1.3.18 RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)

URL: <http://www.ietf.org/rfc/rfc1940.txt>

The purpose of SDRP is to support source-initiated selection of routes to complement the route selection provided by existing routing protocols for both inter-domain and intra-domain routes. This document refers to such source-initiated routes as "SDRP routes". This document describes the packet format and forwarding procedure for SDRP. It also describes procedures for ascertaining feasibility of SDRP routes. Other components not described here are routing information distribution and route computation. This portion of the protocol may initially be used with manually configured routes. The same packet format and processing will be usable with dynamic route information distribution and computation methods under development.

The packet forwarding protocol specified here makes minimal assumptions about the distribution and acquisition of routing information needed to construct the SDRP routes. These minimal assumptions are believed to be sufficient for the existing Internet. Future components of the SDRP protocol will extend capabilities in this area and others in a largely backward-compatible manner.

This version of the packet forwarding protocol sends all packets with the complete SDRP route in the SDRP header. Future versions will address route setup and other enhancements and optimizations.

Keywords:

4.1.3.19 RFC 1968 The PPP Encryption Control Protocol (ECP)

URL: <http://www.ietf.org/rfc/rfc1968.txt>

The Point-to-Point Protocol (PPP) [1] provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP also defines an extensible Link Control Protocol.

This document defines a method for negotiating data encryption over PPP links.

Keywords:

4.1.3.20 RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms

URL: <http://www.ietf.org/rfc/rfc2040.txt>

This document defines four ciphers with enough detail to ensure interoperability between different implementations. The first cipher is the raw RC5 block cipher. The RC5 cipher takes a fixed size input block and produces a fixed sized output block using a transformation that depends on a key. The second cipher, RC5-CBC, is the Cipher Block Chaining (CBC) mode for RC5. It can process messages whose length is a multiple of the RC5 block size. The third cipher, RC5-CBC-Pad, handles plaintext of any length, though the ciphertext will be longer than the plaintext by at most

the size of a single RC5 block. The RC5-CTS cipher is the Cipher Text Stealing mode of RC5, which handles plaintext of any length and the ciphertext length matches the plaintext length.

The RC5 cipher was invented by Professor Ronald L. Rivest of the Massachusetts Institute of Technology in 1994. It is a very fast and simple algorithm that is parameterized by the block size, the number of rounds, and key length. These parameters can be adjusted to meet different goals for security, performance, and exportability.

RSA Data Security Incorporated has filed a patent application on the RC5 cipher and for trademark protection for RC5, RC5-CBC, RC5-CBC-Pad, RC5-CTS and assorted variations.

Keywords:

4.1.3.21 RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME

URL: <http://www.ietf.org/rfc/rfc2045.txt>

Multipurpose Internet Mail Extensions (MIME) [RFC2045-RFC2049] extends the format of Internet mail to allow non-US ASCII textual messages, non-textual messages, multi-part message bodies, and non-US ASCII information in the headers. The Secure/MIME (S/MIME) working group is developing specifications, e.g., [RFC 2311], to send and receive secure MIME data, providing the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption).

Keywords: Security, Mail, Internet, protocol, application layer

4.1.3.22 RFC 2086 IMAP4 ACL extension

URL: <http://www.ietf.org/rfc/rfc2086.txt>

Provides Access Control List (ACL) ability to IMAP applications.

Keywords: Authorization for Access Control, Setting and Verifying User Accounts, Policy, Unauthorized access, Security

4.1.3.23 RFC 2093 Group Key Management Protocol (GKMP) Specification

URL: <http://www.ietf.org/rfc/rfc2093.txt>

This specification proposes a protocol to create grouped symmetric keys and distribute them amongst communicating peers. This protocol has the following advantages: 1) virtually invisible to operator, 2) no central key distribution site is needed, 3) only group members have the key, 4) sender or receiver oriented operation, 5) can make use of multicast communications protocols.

Keywords:

4.1.3.24 RFC 2228 FTP Security Extensions

URL: <http://www.ietf.org/rfc/rfc2228.txt>

This document defines extensions to the FTP specification STD 9, RFC 959, "FILE TRANSFER PROTOCOL (FTP)" (October 1985). These extensions provide strong authentication, integrity, and confidentiality on both the control and data channels with the introduction of new optional commands, replies, and file transfer encodings.

Keywords: Encryption, Authorization for Access Control, Confidentiality, Security

Keywords:

4.1.3.25 RFC 2230 Key Exchange Delegation Record for the DNS

URL: <http://www.ietf.org/rfc/rfc2230.txt>

This note describes a mechanism whereby authorization for one node to act as key exchanger for a second node is delegated and made available via the Secure DNS. This mechanism is intended to be used only with the Secure DNS. It can be used with several security services. For example, a system seeking to use IP Security [RFC-1825, RFC-1826, RFC-1827] to protect IP packets for a given destination can use this mechanism to determine the set of authorized remote key exchanger systems for that destination.

The Domain Name System (DNS) is the standard way that Internet nodes locate information about addresses, mail exchangers, and other data relating to remote Internet nodes. [RFC-1035, RFC-1034] More recently, Eastlake and Kaufman have defined standards-track security extensions to the DNS. [RFC-2065] These security extensions can be used to authenticate signed DNS data records and can also be used to store signed public keys in the DNS.

The KX record is useful in providing an authenticatable method of delegating authorization for one node to provide key exchange services on behalf of one or more, possibly different, nodes. This note specifies the syntax and semantics of the KX record, which is currently in limited deployment in certain IP-based networks.

Keywords:

4.1.3.26 RFC 2244 ACAP -- Application Configuration Access Protocol

URL: <http://www.ietf.org/rfc/rfc2244.txt>

The Application Configuration Access Protocol (ACAP) is designed to support remote storage and access of program option, configuration and preference information. The data store model is designed to allow a client relatively simple access to interesting data, to allow new information to be easily added without server re-configuration, and to promote the use of both standardized data and custom or proprietary data. Key features include "inheritance" which can be used to manage default values for configuration settings and access control lists which allow interesting personal information to be shared and group information to be restricted.

Keywords:

4.1.3.27 RFC 2246 The TLS Protocol Version 1.0

URL: <http://www.ietf.org/rfc/rfc2246.txt>

This document specifies Version 1.0 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

Keywords:

4.1.3.28 RFC 2313 PKCS #1: RSA Encryption Version 1.5

URL: <http://www.ietf.org/rfc/rfc2313.txt>

This document describes a method for encrypting data using the RSA public-key cryptosystem. Its intended use is in the construction of digital signatures and digital envelopes, as described in PKCS #7:

- For digital signatures, the content to be signed is first reduced to a message digest with a message-digest algorithm (such as MD5), and then an octet string containing the message digest is encrypted with the RSA private key of the signer of the content. The content and the encrypted message digest are represented together according to the syntax in PKCS #7 to yield a digital signature. This application is compatible with Privacy-Enhanced Mail (PEM) methods.
- For digital envelopes, the content to be enveloped is first encrypted under a content-encryption key with a content-encryption algorithm (such as DES), and then the content-encryption key is encrypted with the RSA public keys of the recipients of the content. The encrypted content and the encrypted content-encryption key are represented together according to the syntax in PKCS #7 to yield a digital envelope. This application is also compatible with PEM methods.

The document also describes a syntax for RSA public keys and private keys. The public-key syntax would be used in certificates; the private-key syntax would be used typically in PKCS #8 private-key information. The public-key syntax is identical to that in both X.509 and Privacy-Enhanced Mail. Thus X.509/PEM RSA keys can be used in this document.

The document also defines three signature algorithms for use in signing X.509/PEM certificates and certificate-revocation lists, PKCS #6 extended certificates, and other objects employing digital signatures such as X.401 message tokens.

Details on message-digest and content-encryption algorithms are outside the scope of this document, as are details on sources of the pseudorandom bits required by certain methods in this document.

Keywords:

4.1.3.29 RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5

URL: <http://www.ietf.org/rfc/rfc2315.txt>

This document describes a general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes. The syntax admits recursion, so that, for example, one envelope can be nested inside another, or one party can sign some previously enveloped digital data. It also allows arbitrary attributes, such as signing time, to be authenticated along with the content of a message, and provides for other attributes such as countersignatures to be associated with a signature. A degenerate case of the syntax provides a means for disseminating certificates and certificate-revocation lists.

Keywords:

4.1.3.30 RFC 2356 Sun's SKIP Firewall Traversal for Mobile IP

URL: <http://www.ietf.org/rfc/rfc2356.txt>

The Mobile IP specification establishes the mechanisms that enable a mobile host to maintain and use the same IP address as it changes its point of attachment to the network. Mobility implies higher security risks than static operation, because the traffic may at times take unforeseen network paths with unknown or unpredictable security characteristics. The Mobile IP specification makes no provisions for securing data traffic. The mechanisms described in this document allow a mobile node out on a public sector of the internet to negotiate access past a SKIP firewall, and construct a secure channel into its home network.

In addition to securing traffic, our mechanisms allow a mobile node to roam into regions that (1) impose ingress filtering, and (2) use a different address space.

4.1.3.31 RFC 2406 IP Encapsulating Security Payload (ESP)

URL: <http://www.ietf.org/rfc/rfc2406.txt>

The Encapsulating Security Payload (ESP) header is designed to provide a mix of security services in IPv4 and IPv6. ESP may be applied alone, in combination with the IP Authentication Header (AH) [KA97b], or in a nested fashion, e.g., through the use of tunnel mode (see "Security Architecture for the Internet Protocol" [KA97a], hereafter referred to as the Security Architecture document). Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host. For more details on how to use ESP and AH in various network environments, see the Security Architecture document [KA97a].

4.1.3.32 RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0

URL: <http://www.ietf.org/rfc/rfc2437.txt>

This document provides recommendations for the implementation of public-key cryptography based on the RSA algorithm [18], covering the following aspects:

- cryptographic primitives
- encryption schemes
- signature schemes with appendix
- ASN.1 syntax for representing keys and for identifying the schemes

The recommendations are intended for general application within computer and communications systems, and as such include a fair amount of flexibility. It is expected that application standards based on these specifications may include additional constraints. The recommendations are intended to be compatible with draft standards currently being developed by the ANSI X9F1 [1] and IEEE P1363 working groups [14]. This document supersedes PKCS #1 version 1.5 [20]. Editor's note. It is expected that subsequent versions of PKCS #1 may cover other aspects of the RSA algorithm such as key size, key generation, key validation, and signature schemes with message recovery.

Keywords:

4.1.3.33 RFC 2440 OpenPGP Message Format

URL: <http://www.ietf.org/rfc/rfc2440.txt>

This document is maintained in order to publish all necessary information needed to develop interoperable applications based on the OpenPGP format. It is not a step-by-step cookbook for writing an application. It describes only the format and methods needed to read, check, generate, and write conforming packets crossing any network. It does not deal with storage and implementation questions. It does, however, discuss implementation issues necessary to avoid security flaws. Open-PGP software uses a combination of strong public-key and symmetric cryptography to provide security services for electronic communications and data storage. These services include confidentiality, key management, authentication, and digital signatures. This document specifies the message formats used in OpenPGP.

Keywords:

4.1.3.34 RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)

URL: <http://www.ietf.org/rfc/rfc2408.txt>

This memo describes a protocol utilizing security concepts necessary for establishing Security Associations (SA) and cryptographic keys in an Internet environment. A Security Association

protocol that negotiates, establishes, modifies and deletes Security Associations and their attributes is required for an evolving Internet, where there will be numerous security mechanisms and several options for each security mechanism. The key management protocol must be robust in order to handle public key generation for the Internet community at large and private key requirements for those private networks with that requirement. The Internet Security Association and Key Management Protocol (ISAKMP) defines the procedures for authenticating a communicating peer, creation and management of Security Associations, key generation techniques, and threat mitigation (e.g. denial of service and replay attacks). All of these are necessary to establish and maintain secure communications (via IP Security Service or any other security protocol) in an Internet environment.

Keywords:

4.1.3.35 RFC 2409 The Internet Key Exchange (IKE)

URL: <http://www.ietf.org/rfc/rfc2409.txt>

ISAKMP ([MSST98]) provides a framework for authentication and key exchange but does not define them. ISAKMP is designed to be key exchange independent; that is, it is designed to support many different key exchanges. Oakley ([Orm96]) describes a series of key exchanges—called "modes"—and details the services provided by each (e.g. perfect forward secrecy for keys, identity protection, and authentication). SKEME ([SKEME]) describes a versatile key exchange technique that provides anonymity, repudiability, and quick key refreshment. This document describes a protocol using part of Oakley and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec DOI.

4.1.3.36 RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile

URL: <http://www.ietf.org/rfc/rfc2459.txt>

This memo profiles the X.509 v3 certificate and X.509 v2 CRL for use in the Internet. An overview of the approach and model are provided as an introduction. The X.509 v3 certificate format is described in detail, with additional information regarding the format and semantics of Internet name forms (e.g., IP addresses). Standard certificate extensions are described and one new Internet-specific extension is defined. A required set of certificate extensions is specified. The X.509 v2 CRL format is described and a required extension set is defined as well. An algorithm for X.509 certificate path validation is described. Supplemental information is provided describing the format of public keys and digital signatures in X.509 certificates for common Internet public key encryption algorithms (i.e., RSA, DSA, and Diffie-Hellman). ASN.1 modules and examples are provided in the appendices.

Keywords:

4.1.3.37 RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols

URL: <http://www.ietf.org/rfc/rfc2510.txt>

This document describes the Internet X.509 Public Key Infrastructure (PKI) Certificate Management Protocols. Protocol messages are defined for all relevant aspects of certificate creation and management. Note that "certificate" in this document refers to an X.509v3 Certificate as defined in [COR95, X509-AM].

Keywords:

4.1.3.38 RFC 2511 Internet X.509 Certificate Request Message Format

URL: <http://www.ietf.org/rfc/rfc2511.txt>

This document describes the Certificate Request Message Format (CRMF). This syntax is used to convey a request for a certificate to a Certification Authority (CA) (possibly via a Registration Authority (RA)) for the purposes of X.509 certificate production. The request will typically include a public key and associated registration information.

Keywords:

4.1.3.39 RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

URL: <http://www.ietf.org/rfc/rfc2527.txt>

This document presents a framework to assist the writers of certificate policies or certification practice statements for certification authorities and public key infrastructures. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a certificate policy definition or a certification practice statement.

Keywords:

4.1.3.40 RFC 2535 Domain Name System Security Extensions

URL: <http://www.ietf.org/rfc/rfc2535.txt>

Extensions to the Domain Name System (DNS) are described that provide data integrity and authentication to security aware resolvers and applications through the use of cryptographic digital signatures. These digital signatures are included in secured zones as resource records. Security can also be provided through non-security aware DNS servers in some cases. The extensions provide for the storage of authenticated public keys in the DNS. This storage of keys can support general public key distribution services as well as DNS security. The stored keys enable security aware resolvers to learn the authenticating key of zones in addition to those for which they are initially configured. Keys associated with DNS names can be retrieved to support other protocols. Provision is made for a variety of key types and algorithms. In addition, the security extensions provide for the optional authentication of DNS protocol transactions and requests.

Keywords:

4.1.3.41 RFC 2543 SIP: Session Initiation Protocol

URL: <http://www.ietf.org/rfc/rfc2543.txt>

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants. These sessions include Internet multimedia conferences, Internet telephone calls and multimedia distribution. Members in a session can communicate via multicast or via a mesh of unicast relations, or a combination of these. SIP invitations used to create sessions carry session descriptions that allow participants to agree on a set of compatible media types. SIP supports user mobility by proxying and redirecting requests to the user's current location. Users can register their current location. SIP is not tied to any particular conference control protocol. SIP is designed to be independent of the lower-layer transport protocol and can be extended with additional capabilities.

Keywords:

4.1.3.42 RFC 2547 BGP/MPLS VPNs

URL: <http://www.ietf.org/rfc/rfc2547.txt>

This document describes a method by which a Service Provider with an IP backbone may provide VPNs (Virtual Private Networks) for its customers. MPLS (Multiprotocol Label Switching) is used for forwarding packets over the backbone, and BGP (Border Gateway Protocol) is used for distributing routes over the backbone. The primary goal of this method is to support the outsourcing of IP backbone services for enterprise networks. It does so in a manner that is simple for the enterprise, while still scalable and flexible for the Service Provider, and while allowing the Service Provider to add value. These techniques can also be used to provide a VPN which itself provides IP service to customers.

Keywords:

Keywords:

4.1.3.43 RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

URL: <http://www.ietf.org/rfc/rfc2560.txt>

This document specifies a protocol useful in determining the current status of a digital certificate without requiring CRLs. Additional mechanisms addressing PKIX operational requirements are specified in separate documents. An overview of the protocol is provided in section 2. Functional requirements are specified in section 4. Details of the protocol are in section 5. We cover security issues with the protocol in section 6. Appendix A defines OCSP over HTTP, appendix B accumulates ASN.1 syntactic elements and appendix C specifies the mime types for the messages.

Keywords:

4.1.3.44 RFC 2592 Definitions of Managed Objects for the Delegation of Management Script

URL: <http://www.ietf.org/rfc/rfc2592.txt>

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes a set of managed objects that allow the delegation of management scripts to distributed managers.

Keywords:

4.1.3.45 RFC 2744 Generic Security Service API Version 2 : C-bindings

URL: <http://www.ietf.org/rfc/rfc2744.txt>

This document specifies C language bindings for Version 2, Update 1 of the Generic Security Service Application Program Interface (GSS-API), which is described at a language-independent conceptual level in RFC-2743 [GSSAPI]. It obsoletes RFC-1509, making specific incremental changes in response to implementation experience and liaison requests. It is intended, therefore, that this memo or a successor version thereof will become the basis for subsequent progression of the GSS-API specification on the standards track. The Generic Security Service Application Programming Interface provides security services to its callers, and is intended for implementation atop a variety of underlying cryptographic mechanisms. Typically, GSS-API callers will be application protocols into which security enhancements are integrated through invocation of services provided by the GSS-API. The GSS-API allows a caller application to authenticate a principal identity associated with a peer application, to delegate rights to a peer, and to apply security services such as confidentiality and integrity on a per-message basis.

Keywords:

4.1.3.46 RFC 2764 A Framework for IP Based Virtual Private Networks

URL: <http://www.ietf.org/rfc/rfc2764.txt>

This document describes a framework for Virtual Private Networks (VPNs) running across IP backbones. It discusses the various different types of VPNs, their respective requirements, and proposes specific mechanisms that could be used to implement each type of VPN using existing or proposed specifications. The objective of this document is to serve as a framework for related protocol development in order to develop the full set of specifications required for widespread deployment of interoperable VPN solutions.

Keywords:

4.1.3.47 RFC 2753 A Framework for Policy-based Admission Control

URL: <http://www.ietf.org/rfc/rfc2753.txt>

This document is concerned with specifying a framework for providing policy-based control over admission control decisions. In particular, it focuses on policy-based control over admission control using RSVP as an example of the QoS signaling mechanism. Even though the focus of the work is on RSVP-based admission control, the document outlines a framework that can provide policy-based admission control in other QoS contexts. We argue that policy-based control must be applicable to different kinds and qualities of services offered in the same network and our goal is to consider such extensions whenever possible.

Keywords:

4.1.3.48 RFC 2797 Certificate Management Messages over CMS

URL: <http://www.ietf.org/rfc/rfc2797.txt>

This document defines a Certificate Management protocol using CMS (CMC). This protocol addresses two immediate needs within the Internet PKI community:

1. The need for an interface to public key certification products and services based on [CMS] and [PKCS10], and
2. The need in [SMIMEV3] for a certificate enrollment protocol for DSA-signed certificates with Diffie-Hellman public keys.

A small number of additional services are defined to supplement the core certificate request service.

Throughout this specification the term CMS is used to refer to both [CMS] and [PKCS7]. For both signedData and envelopedData, CMS is a superset of the PKCS7. In general, the use of PKCS7 in this document is aligned to the Cryptographic Message Syntax [CMS] that provides a superset of the PKCS7 syntax. The term CMC refers to this specification.

Keywords:

4.1.3.49 RFC 2817 Upgrades to TLS within HTTP/1.1

URL: <http://www.ietf.org/rfc/rfc2817.txt>

This document extends the use of TLS (e.g. HTTPS) so that hostnames can be exchanged.

TLS, a.k.a., SSL (Secure Sockets Layer), establishes a private end-to-end connection, optionally including strong mutual authentication, using a variety of cryptosystems. Initially, a handshake phase uses three subprotocols to set up a record layer, authenticate endpoints, set parameters, as well as report errors. Then, there is an ongoing layered record protocol that handles encryption, compression, and reassembly for the remainder of the connection. The latter is intended to be completely transparent. For example, there is no dependency between TLSs record markers and or certificates and HTTP/1.1's chunked encoding or authentication.

Keywords: keywords

4.1.3.50 RFC 2818 HTTP over TLS (HTTPS)

URL: <http://www.ietf.org/rfc/rfc2818.txt>

This document describes how to use TLS to secure HTTP connections over the Internet. Current practice is to layer HTTP over SSL and allowing the distinguishing secured traffic from insecure traffic by the use of a different server port.

Keywords: keywords

4.1.3.51 RFC 2820 Access Control Requirements for LDAP

URL: <http://www.ietf.org/rfc/rfc2820.txt>

This document describes the fundamental requirements of an access control list (ACL) model for the Lightweight Directory Application Protocol (LDAP) directory service. It is intended to be a gathering place for access control requirements needed to provide authorized access to and interoperability between directories.

Keywords:

4.1.3.52 RFC 2865 Remote Authentication Dial In User Service (RADIUS)

URL: <http://www.ietf.org/rfc/rfc2865.txt>

This document describes a protocol for carrying authentication, authorization, and configuration information between a Network Access Server that desires to authenticate its links and a shared Authentication Server.

Keywords:

4.1.3.53 RFC 2869 RADIUS Extensions

URL: <http://www.ietf.org/rfc/rfc2869.txt>

This document describes additional attributes for carrying authentication, authorization and accounting information between a Network Access Server (NAS) and a shared Accounting Server using the Remote Authentication Dial In User Service (RADIUS) protocol described in RFC 2865 [1] and RFC 2866 [2].

Keywords:

4.1.3.54 RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering

URL: <http://www.ietf.org/rfc/rfc2874.txt>

This document defines changes to the Domain Name System to support renumberable and aggregatable IPv6 addressing. The changes include a new resource record type to store an IPv6 address in a manner that expedites network renumbering and updated definitions of existing query types that return Internet addresses as part of additional section processing.

For lookups keyed on IPv6 addresses (often called reverse lookups), this document defines a new zone structure that allows a zone to be used without modification for parallel copies of an address space (as for a multihomed provider or site) and across network renumbering events.

Keywords:

4.1.3.55 RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms

URL: <http://www.ietf.org/rfc/rfc2875.txt>

This document describes two methods for producing an integrity check value from a Diffie-Hellman key pair. This behavior is needed for such operations as creating the signature of a PKCS #10 certification request. These algorithms are designed to provide a proof-of- possession rather than general purpose signing.

Keywords:

4.1.3.56 RFC 2888 Secure Remote Access with L2TP

URL: <http://www.ietf.org/rfc/rfc2888.txt>

Keywords: L2TP protocol is a virtual extension of PPP across IP network infrastructure. L2TP makes possible for an access concentrator (LAC) to be near remote clients, while allowing PPP termination server (LNS) to be located in enterprise premises. L2TP allows an enterprise to retain control of RADIUS database, which is used to control Authentication, Authorization and Accountability (AAA) of dial-in users. The objective of this document is to extend security characteristics of IPsec to remote access users, as they dial-in through the Internet. This is accomplished without creating new protocols and using the existing practices of Remote Access and IPsec. Specifically, the document proposes three new RADIUS parameters for use by the LNS node, acting as Secure Remote Access Server (SRAS) to mandate network level security between remote clients and the enterprise. The document also discusses limitations of the approach.

Keywords:

4.1.3.57 RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0

URL: <http://www.ietf.org/rfc/rfc2898.txt>

This memo represents a republication of PKCS #5 v2.0 from RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, and change control is retained within the PKCS process. The body of this document, except for the security considerations section, is taken directly from that specification. This document provides recommendations for the implementation of password-based cryptography, covering key derivation functions, encryption schemes, message-authentication schemes, and ASN.1 syntax identifying the techniques.

The recommendations are intended for general application within computer and communications systems, and as such include a fair amount of flexibility. They are particularly intended for the protection of sensitive information such as private keys, as in PKCS #8 [25]. It is expected that application standards and implementation profiles based on these specifications may include additional constraints.

Other cryptographic techniques based on passwords, such as password-based key entity authentication and key establishment protocols [4][5][26] are outside the scope of this document. Guidelines for the selection of passwords are also outside the scope.

Keywords:

4.1.3.58 RFC 2946 Telnet Data Encryption Option

URL: <http://www.ietf.org/rfc/rfc2946.txt>

This document describes a telnet encryption option as a generic method of providing data confidentiality services for the telnet data stream. While this document summarizes currently utilized encryption types and codes, it does not define a specific encryption algorithm. Separate documents are to be published defining implementations of this option for each encryption algorithm.

Keywords:

4.1.3.59 RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements

URL: <http://www.ietf.org/rfc/rfc2977.txt>

The Mobile IP and Authentication, Authorization, Accounting (AAA) working groups are currently looking at defining the requirements for Authentication, Authorization, and Accounting. This document contains the requirements that would have to be supported by an AAA service to aid in providing Mobile IP services.

Keywords:

4.1.3.60 RFC 2979 Behavior of and Requirements for Internet Firewalls

URL: <http://www.ietf.org/rfc/rfc2979.txt>

This memo defines behavioral characteristics of and interoperability requirements for Internet firewalls. While most of these things may seem obvious, current firewall behavior is often either unspecified or underspecified and this lack of specificity often causes problems in practice. This requirement is intended to be a necessary first step in making the behavior of firewalls more consistent across implementations and in line with accepted IP protocol practices.

Keywords:

4.1.3.61 RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0

URL: <http://www.ietf.org/rfc/rfc2985.txt>

This memo represents a republication of PKCS #9 v2.0 from RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, and change control is retained within the PKCS process. The body of this document, except for the security considerations section, is taken directly from that specification.

This memo provides a selection of object classes and attribute types for use in conjunction with public-key cryptography and Lightweight Directory Access Protocol (LDAP) accessible directories. It also includes ASN.1 syntax for all constructs.

Keywords:

4.1.3.62 RFC 2986 PKCS #10: Certification Request Syntax Specification Version 1.7

URL: <http://www.ietf.org/rfc/rfc2986.txt>

This memo represents a republication of PKCS #10 v1.7 from RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, and change control is retained within the PKCS process. The body of this document, except for the security considerations section, is taken directly from the PKCS #9 v2.0 or the PKCS #10 v1.7 document.

Keywords:

4.1.3.63 RFC 3053 IPv6 Tunnel Broker

URL: <http://www.ietf.org/rfc/rfc3053.txt>

The IPv6 global Internet as of today uses a lot of tunnels over the existing IPv4 infrastructure. Those tunnels are difficult to configure and maintain in a large scale environment. The 6bone has proven that large sites and Internet Service Providers (ISPs) can do it, but this process is too complex for the isolated end user who already has an IPv4 connection and would like to enter the IPv6 world. The motivation for the development of the tunnel broker model is to help early IPv6 adopters to hook up to an existing IPv6 network (e.g., the 6bone) and to get stable, permanent IPv6 addresses and DNS names. The concept of the tunnel broker was first presented at Orlando's IETF in December 1998. Two implementations were demonstrated during the Grenoble IPng & NGtrans interim meeting in February 1999.

Keywords:

4.1.3.64 RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)

URL: <http://www.ietf.org/rfc/rfc3268.txt>

This document proposes several new ciphersuites. At present, the symmetric ciphers supported by Transport Layer Security (TLS) are RC2, RC4, International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES), and triple DES. The protocol would be enhanced by the addition of Advanced Encryption Standard (AES) ciphersuites.

Keywords:

4.1.3.65 RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

URL: <http://www.ietf.org/rfc/rfc3280.txt>

This memo profiles the X.509 v3 certificate and X.509 v2 Certificate Revocation List (CRL) for use in the Internet. An overview of this approach and model are provided as an introduction. The X.509 v3 certificate format is described in detail, with additional information regarding the format and semantics of Internet name forms. Standard certificate extensions are described and two Internet-specific extensions are defined. A set of required certificate extensions is specified. The X.509 v2 CRL format is described in detail, and required extensions are defined. An algorithm for X.509 certification path validation is described. An ASN.1 module and examples are provided in the appendices.

4.1.3.66 RFC 3369 Cryptographic Message Syntax (CMS)

URL: <http://www.ietf.org/rfc/rfc3369.txt>

This document describes the Cryptographic Message Syntax (CMS). This syntax is used to digitally sign, digest, authenticate, or encrypt arbitrary message content.

Keywords:

4.1.3.67 RFC 3370 Cryptographic Message Syntax (CMS) Algorithms

URL: <http://www.ietf.org/rfc/rfc3370.txt>

This document describes the conventions for using several cryptographic algorithms with the Cryptographic Message Syntax (CMS). The CMS is used to digitally sign, digest, authenticate, or encrypt arbitrary message contents.

Keywords:

4.1.3.68 RFC 3401 Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS

URL: <http://www.ietf.org/rfc/rfc3401.txt>

This document specifies the exact documents that make up the complete Dynamic Delegation Discovery System (DDDS). DDDS is an abstract algorithm for applying dynamically retrieved string transformation rules to an application-unique string. This document along with RFC 3402, RFC 3403 and RFC 3404 obsolete RFC 2168 and RFC 2915, as well as updates RFC 2276.

Keywords:

4.1.3.69 RFC 3402 Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm

URL: <http://www.ietf.org/rfc/rfc3402.txt>

This document describes the Dynamic Delegation Discovery System (DDDS) algorithm for applying dynamically retrieved string transformation rules to an application-unique string. Well-formed transformation rules will reflect the delegation of management of information associated with the string. This document is also part of a series that is completely specified in "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS" (RFC 3401). It is very important to note that it is impossible to read and understand any document in this series without reading the others.

Keywords:

4.1.3.70 RFC 3403 Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database

URL: <http://www.ietf.org/rfc/rfc3403.txt>

This document describes a Dynamic Delegation Discovery System (DDDS) Database using the Domain Name System (DNS) as a distributed database of Rules. The Keys are domain-names and the Rules are encoded using the Naming Authority Pointer (NAPTR) Resource Record (RR).

Since this document obsoletes RFC 2915, it is the official specification for the NAPTR DNS Resource Record. It is also part of a series that is completely specified in "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS" (RFC 3401). It is very important to note that it is impossible to read and understand any document in this series without reading the others.

Keywords:

4.1.3.71 RFC 3404 Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI)

URL: <http://www.ietf.org/rfc/rfc3404.txt>

This document describes a specification for taking Uniform Resource Identifiers (URI) and locating an authoritative server for information about that URI. The method used to locate that authoritative server is the Dynamic Delegation Discovery System. This document is part of a series that is specified in "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS" (RFC 3401). It is very important to note that it is impossible to read and understand any document in this series without reading the others.

Keywords:

4.1.3.72 RFC 3405 Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures

URL: <http://www.ietf.org/rfc/rfc3405.txt>

This document is fifth in a series that is completely specified in "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS" (RFC 3401). It is very important to note that it is impossible to read and understand any document in this series without reading the others.

Keywords:

4.1.3.73 RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

URL: <http://www.ietf.org/rfc/rfc3414.txt>

This document describes the User-based Security Model (USM) for Simple Network Management Protocol (SNMP) version 3 for use in the SNMP architecture. It defines the Elements of Procedure for providing SNMP message level security. This document also includes a Management Information Base (MIB) for remotely monitoring/managing the configuration parameters for this Security Model. This document obsoletes RFC 2574.

Keywords:

4.1.3.74 RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1

URL: <http://www.ietf.org/rfc/rfc3447.txt>

This memo represents a republication of PKCS #1 v2.1 from RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, and change control is retained within the PKCS process. The body of this document is taken directly from the PKCS #1 v2.1 document, with certain corrections made during the publication process.

Keywords:

4.1.3.75 RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

URL: <http://www.ietf.org/rfc/rfc3647.txt>

This document presents a framework to assist the writers of certificate policies or certification practice statements for participants within public key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on certificates. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a certificate policy or a certification practice statement. This document supersedes RFC 2527.

Keywords:

4.1.3.76 RFC 3761 The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)

URL: <http://www.ietf.org/rfc/rfc3761.txt>

This document discusses the use of the Domain Name System (DNS) for storage of E.164 numbers. More specifically, how DNS can be used for identifying available services connected to one E.164 number. It specifically obsoletes RFC 2916 to bring it in line with the Dynamic Delegation Discovery System (DDDS) Application specification found in the document series specified in RFC 3401. It is very important to note that it is impossible to read and understand this document without reading the documents discussed in RFC 3401.

Keywords:

4.1.4 Other Security Technologies

4.1.4.1 IEEE Documents on Security Technologies

4.1.4.1.1 IEEE 802.11b Web Encryption Protocol

URL: <http://www.ieee.org>

From <http://cms.syr.edu/connecting/wireless/glossary.html>:

Also referred to as 802.11 High Rate or Wi-Fi Applies to wireless LANs and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps depending on Range and Signal Strength) in the 2.4 GHz band. 802.11b uses only DSSS (Acronym for direct-sequence spread spectrum. DSSS is one of two types of spread spectrum radio.) 802.11b was a 1999 IEEE ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.

Keywords:

4.1.4.1.2 IEEE 802.11i Security for Wireless Networks (WPA2)

URL: <http://standards.ieee.org/reading/ieee/std/lanman/drafts/P802.11i.pdf>

The IEEE 802.11i protocol is the update to 802.11 security that includes all of the interim measures found in WPA (Wi-Fi Protected Access), and also adds a longer, strong encryption key using AES and fast handoff through quick re-authentication among access points.

Keywords: Confidentiality, Policy, Authorization for Access Control, Encryption, Security

4.1.4.1.3 IEEE Personal and Private Information (PAPI) draft standard

URL: <http://www.ieee.org>

PAPI is a system for providing access control to restricted information resources across the Internet. The authentication mechanisms are designed to be as flexible as possible, allowing each organization to use its own authentication schema, keeping user privacy, and offering information providers data enough for statistics. Access control mechanisms are transparent to the user and compatible with the most commonly employed Web browsers and any operating system. Since PAPI uses standard HTTP procedures, PAPI authentication and access control does not require any specific hardware or software, thus providing users with ubiquitous access to any resource they have right to.

4.1.4.2 RSA Documents on Security Technologies

4.1.4.2.1 RSA PKCS #8 Private-Key Information Syntax Standard

URL: <ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-8.doc>

This standard describes a syntax for private-key information. Private-key information includes a private key for some public-key algorithm and a set of attributes. The standard also describes a syntax for encrypted private keys. A password-based encryption algorithm (e.g. one of those described in PKCS #5) could be used to encrypt private-key information.

Keywords:

4.1.4.2.2 RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.

URL: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf>

From: <https://selfservice.exostar.com/certenroll/client/help/concepts/glossary.htm>

A standard that specifies a portable format for storing or transporting a user's private keys and Digital IDs.

PRIVATE KEY A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.

Keywords:

4.1.4.3 OASIS Documents on Security Technologies

4.1.4.3.1 OASIS Security for Grid Services

URL: <http://www.globus.org/Security/GSI3/GT3-Security-HPDC.pdf>

Provides policy directives for distributed computing environments.

Keywords:

4.1.4.3.2 OASIS Attribute Profiles for SAML 2.0

URL: <http://www.oasis-open.org/committees/download.php/6344/sstc-hughes-mishra-baseline-attributes-03.pdf>

Provides flexible means of specifying attribute names and values within SAML 2.0. Additionally, it provides a flexible means of specifying queries.

Keywords:

4.1.4.3.3 OASIS SAML 2.0: Security Assertion Markup Language Version 2.0

URL: <http://www.oasis-open.org/committees/download.php/2290/oasis-sstc-saml-1.0.zip>

This document provides extensions to SAML 2.0 that allows for exchanging of authentication and authorization information between security systems.

Keywords:

4.1.4.3.4 OASIS Security Assertion Markup Language (SAML) V2.0

URL: <http://www.oasis-open.org/committees/download.php/6773/sstc-saml-bindings-2.0-draft-11-diff.pdf>

This document specifies SAML protocol bindings for the use of SAML assertions and request-response messages in communications protocols and frameworks.

Protocol Binding Concepts: Mappings of SAML request-response exchanges onto standard messaging or communication protocols are call SAML protocol bindings.

Keywords:

4.1.4.3.5 OASIS Authentication Context

URL: <http://www.oasis-open.org/committees/download.php/6539/sstc-saml-authn-context-2.0-draft-04a-diff.pdf>

This specification defines an XML Schema for the creation of Authentication Context statements that allow the authentication authority to provide to the service provider this additional information. Additionally, this specification defines a number of Authentication Context classes: categories into which many Authentication Context will fall, thereby simplifying their interpretation.

Keywords:

4.1.4.3.6 Web Services Policy Framework (WS-Policy)

URL: <http://xml.coverpages.org/ws-policyV11.pdf>

The Web Services Policy Framework (WS-Policy) provides a general-purpose model and corresponding syntax to describe and communicate the policies of a Web Service. WS-Policy defines a base set of constructs that can be used and extended by other Web Services specifications.

Keywords:

4.1.4.3.7 Web Services Policy Assertions Language (WS-PolicyAssertions)

URL: <http://xml.coverpages.org/ws-policyassertionsV11.pdf>

This document specifies a set of common message policy assertions that can be specified within a policy.

By using the XML, SOAP, and WSDL extensibility models, the WS* specifications are designed to be composed with each other to provide a rich Web services environment. PolicyAssertions by itself does not provide a negotiation solution for Web services. It is a building block that is used in conjunction with other Web service and application-specific protocols to accommodate a wide variety of policy exchange models.

Keywords:

4.1.4.3.8 Web Services Policy Attachment (WS-PolicyAttachment)

URL: <http://xml.coverpages.org/ws-policyattachmentV11.pdf>

This document specifies three specific attachment mechanisms for using policy expressions with existing XML Web service technologies.

Keywords:

Keywords:

4.1.4.3.9 OASIS Extensible Access Control Markup Language (XACML)

URL: <http://xml.coverpages.org/xacml-schema-policy-v15.pdf>

The objective of XACML is to provide a mechanism policy exchange by defining a language capable of expressing policy statements for a wide variety of information systems and devices.

Keywords:

4.1.4.4 World Wide Web Consortium (W3C) Documents on Security Technologies

4.1.4.4.1 WC3 XML Key Management Specification (XKMS 2.0) Bindings

URL: <http://www.w3.org/TR/xkms2/>

This document specifies protocols for distributing and registering public keys, suitable for use in conjunction with the W3C Recommendations for XML Signature [XML-SIG] and XML Encryption [XML-Enc]. The XML Key Management Specification (XKMS) comprises two parts — the XML Key Information Service Specification (X-KISS) and the XML Key Registration Service Specification (X-KRSS).

Keywords:

4.1.4.4.2 W3C The Platform for Privacy Preferences 1.1 (P3P1.1) Specification W3C Working Draft 27 April 2004

URL: <http://www.w3.org/TR/2004/WD-P3P11-20040427/>

This is the specification of the Platform for Privacy Preferences 1.1 (P3P 1.1). This document, along with its normative references, includes all the specification necessary for the implementation of interoperable P3P 1.1 applications. P3P 1.1 is based on the P3P 1.0 Recommendation and adds some features using the P3P 1.0 Extension mechanism. It also contains a new binding mechanism that can be used to bind policies for XML Applications beyond HTTP transactions.

Keywords:

4.1.4.5 Miscellaneous Security Technologies

4.1.4.5.1 AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.

URL: <http://www.aga.org>

The American Gas Association (AGA) represents almost 200 local utilities that deliver natural gas to homes in the USA. These utilities are part of the critical infrastructure and rely on SCADA networks to control the operations. AGA, in conjunction with GTI and other industry groups, created AGA 12 to develop cyber security standards and protocols for the industry.

AGA 12 has taken a unique approach to focus on securing the communications link between field devices and the control servers or control center. While there certainly is a risk of data insertion and modification in the communication channel, it may not be the most likely or even easiest avenue of attack on a SCADA system.

The first Technical Report, TR-1, defines an add-on encryption module that also could be integrated into an RTU or PLC. Oddly enough, the most recent version includes significantly less technical detail and removed the SCADA Link Security (SLS) protocol defined in Appendix K. If you are interested in AGA 12, Digital Bond recommends you look at Appendix K of the March 2003 version. Note: hit cancel when the login request appears and the document will load.

The big hole in TR-1 is key management, which is to be addressed at a later date. This is a significant issue given the number of encryptors that would be deployed in a SCADA system. Until key management is addressed AGA 12-1 encryptors can be considered a proof of concept solution at best.

The best news on the AGA 12 front is sample implementation code exists. Andrew Wright of Cisco's Critical Infrastructure Assurance Group (CIAG) has written and documented the code. There are also good technical papers on the security of the protocol available through Andrew's ScadaSafe site.

Keywords: Confidentiality, Authorization for Access Control, Policy, Eavesdropping, Security

4.1.4.5.2 ANSI INCITS 359-2004 Role Based Access Control (RBAC)

URL: <http://www.incits.org/>

Security administration can be costly and prone to error because administrators usually specify access control lists for each user on the system individually. With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more

roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs, and assigning employees to the proper roles. Complexities introduced by mutually exclusive roles or role hierarchies are handled by the RBAC software, making security administration easier.

Keywords: Role Based Access Control, RBAC

4.1.4.5.3 BCP 65 Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures

URL: <http://www.armware.dk/RFC/bcp/bcp65.html>

See RFC 3405.

Keywords:

4.1.4.5.4 EPRI 1002596 ICCP TASE.2 Security Enhancements

URL: <http://www.epri.com>

Determines the security vulnerabilities for IEC 60870-6 TASE.2 (ICCP) and provides recommended solutions to those vulnerabilities. This document is the basis for several of the IEC TC57 WG15 IEC 62351 documents.

Keywords:

4.1.4.5.5 NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4

URL: ftp://www.nerc.com/pub/sys/all_updl/cip/pkitf/e-MARC-PKI_draft_version_V2-4b_March_2003_rev1.doc

Provides recommendations in regards to certificate authority selection, certificate distribution, and other certificate related issues.

Keywords:

4.1.4.5.6 NIST GSC-IS The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1

URL: <http://csrc.nist.gov/publications/nistir/nistir-6887.pdf>

The document defines an architectural model for interoperable smart card service provider modules compatible with both file system cards and virtual machine cards. It includes a Basic Services Interface that addresses interoperability of a core set of smart card services at the interface layer between client applications and smart card service provider modules. It also defines a mechanism at the card edge layer for interoperation with smart cards that use a wide variety of APDU sets, including both file system cards and virtual machine cards.

Keywords:

4.1.4.5.7 NISTIR 6529 Common Biometric File Format (CBEFF)

URL: <http://www.itl.nist.gov/div893/biometrics/documents/NISTIR-6529-A.pdf>

The Common Biometric Exchange Formats Framework (CBEFF) describes a set of data elements necessary to support biometric technologies in a common way. These data elements can be placed in a single file used to exchange biometric information between different systems developed by different vendors.

Keywords:

4.1.4.5.8 Semantic Web Pervasive Computing Standard Ontology (PERVASIVE-SO) Guide -- Describing User Profile and Preferences

URL: <http://pervasive.semanticweb.org/doc/2004-01-ont-guide/part1/>

In a pervasive computing environment, computer systems often need to access the profiles and the preferences of a user in order to provide services and information that are tailored to the user. The profile of a user includes typical contact information (telephone numbers, email addresses, name, etc.) and information that describe other computing entities that can act on the behalf of the user (e.g., the personal agent of a user). The preference of a user is a description of the environment state that the user desires the computer systems to honor or achieve whenever it is possible.

The purpose of this document is to show how to describe the profile and the preferences of a user using the PERVASIVE-SO ontologies, which are defined using the Web Ontology Language OWL. Readers are assumed to be familiar with the OWL language and its associated terminologies. For details on the OWL language, readers can consult the listed documents in the References section.

Keywords:

4.1.4.5.9 Smart Card Alliance Smart Card Primer

URL: http://www.smartcardalliance.org/industry_info/smart_cards_primer.cfm

Provides a high level overview of Smart Card technology and describes how the technology works.

Keywords:

4.1.4.5.10 Smart Card Alliance Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology

URL: <http://www.smartcardalliance.org>

Individuals are currently required to confirm their identity for many diverse purposes, such as verifying eligibility within a health care system, accessing a secure network or facility, or validating their authority to travel. In almost every discussion about implementing personal identification (ID) systems to improve identity verification processes, concerns about privacy and the protection of personal information quickly emerge as key issues. Government agencies and private businesses that are implementing ID systems to improve the security of physical or logical access must factor these issues into their system designs. While technologies are available that can provide a higher level of security and privacy than ever before, ID system complexity coupled with increasing public awareness of the risks of privacy intrusion require that organizations focus on privacy and personal information protection throughout the entire ID system design.

Keywords:

4.1.4.5.11 Smart Card Alliance Government Smart Card Handbook

URL: http://www.smartcardalliance.org/pdf/industry_info/smartcardhandbook.pdf

Provides the use practices of the US Government for Smart Cards.

Keywords:

4.1.4.5.12 WebDAV Access Control Extensions to WebDAV

URL: <http://www.webdav.org/acl/protocol/draft-ietf-webdav-acl-13.htm>

This document specifies a set of methods, headers, message bodies, properties, and reports that define Access Control extensions to the WebDAV Distributed Authoring Protocol. This protocol permits a client to read and modify access control lists that instruct a server whether to allow or deny operations upon a resource (such as HyperText Transfer Protocol (HTTP) method invocations) by a given principal. A lightweight representation of principals as Web resources supports integration of a wide range of user management repositories. Search operations allow discovery and manipulation of principals using human names.

Keywords:

4.1.4.5.13 WPA WI-FI Protected Access

See IEEE 802.11b

4.1.4.5.14 WPA2 WI-FI Protected Access Version 2

See IEEE 802.11i

4.1.4.5.15 TMN PKI - Digital certificates and certificate revocation lists profiles

URL: <http://webstore.ansi.org/ansidocstore/product.asp?sku=T1.268-2000>

This standard is intended to promote interoperability among TMN elements that use Public Key Infrastructure (PKI) to support security-related functions. It applies to all TMN interfaces and applications. It is independent of which communications protocol stack or which network management protocol is being used. PKI facilities can be used for a broad range of security functions, such as, authentication, integrity, non-repudiation, and key exchange. However, this standard does not specify how such functions should be implemented, with or without PKI.

Keywords:

This page intentionally left blank.