The Integrated Energy and Communication Systems Architecture

Volume IV:
Technical Analysis

Appendix D:
Technologies, Services, and Best Practices

(Extraction of Security-Related Items Only)

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.

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:

Table of Contents

List of Figures

List of Tables

This page left intentionally blank.

1. Security Technologies

1.1 Policy and Framework Related Technologies

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

1.1.1.1 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

Architectural Issues

Information integrity violation Ensuring that data is not changed or destroyed is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management	

Repudiation Ensuring that the source cannot deny sending the data or that the receiver cannot deny receiving the data is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management	

Replay Ensuring that data cannot be resent by an unauthorized source is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management	

Denial of Service Ensuring unimpeded access to data is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management	

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	
Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	Facilitates or Plays a role
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	Enables or Plays a defining role
Non-repudiation techniques	Enables or Plays a defining role
Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	

None, but needed	
None, and not needed	
Other _____	
Other _____	
ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Enables or Plays a defining role
Addition of security solutions is not feasible	
ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	Enables or Plays a defining role
Addition of security violation detection solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Enables or Plays a defining role
Addition of security solutions is not feasible	
ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	
Addition of security contractual proof solutions could be too costly	Enables or Plays a defining role
Addition of security contractual proof solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Enables or Plays a defining

	role
Addition of security solutions is not feasible	
ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management	

1.1.1.2 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

Architectural Issues

Repudiation Ensuring that the source cannot deny sending the data or that the receiver cannot deny receiving the data is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework	

Replay Ensuring that data cannot be resent by an unauthorized source is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework	

This data exchange has the following requirements with respect to proof of conformance and/or non-repudiation with contractual agreements	
Logging of all information exchanged during this interaction is required	Facilitates or Plays a role
Logging of only key information is required	Facilitates or Plays a role
Logging of the source, destination, requesting application, and requesting user of information exchanges is required, but not the data itself	Facilitates or Plays a role

Logging is not required	
ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	
Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	Enables or Plays a defining role
Non-repudiation techniques	Enables or Plays a defining role
Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Facilitates or Plays a role
Addition of security solutions is not feasible	
ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework	

Security Detection Issues, Concerns, and Problems

Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	Enables or Plays a defining role
Addition of security violation detection solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Facilitates or Plays a role
Addition of security solutions is not feasible	
ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	
Addition of security contractual proof solutions could be too costly	Enables or Plays a defining role
Addition of security contractual proof solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Facilitates or Plays a role
Addition of security solutions is not feasible	
ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework	

1.1.1.3 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

Architectural Issues

Information integrity violation Ensuring that data is not changed or destroyed is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems	

Repudiation Ensuring that the source cannot deny sending the data or that the receiver cannot deny receiving the data is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems	

Replay Ensuring that data cannot be resent by an unauthorized source is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems	

Denial of Service Ensuring unimpeded access to data is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role

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

This data exchange has the following requirements with respect to proof of conformance and/or non-repudiation with contractual agreements	
Logging of all information exchanged during this interaction is required	Enables or Plays a defining role
Logging of only key information is required	Enables or Plays a defining role
Logging of the source, destination, requesting application, and requesting user of information exchanges is required, but not the data itself	Enables or Plays a defining role
Logging is not required	
ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems	

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	
Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	Facilitates or Plays a role
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	Enables or Plays a defining role
Non-repudiation techniques	Enables or Plays a defining role
Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention	

solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Enables or Plays a defining role
Addition of security solutions is not feasible	
ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	Enables or Plays a defining role
Addition of security violation detection solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Enables or Plays a defining role
Addition of security solutions is not feasible	
ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	
Addition of security contractual proof solutions could be too costly	Enables or Plays a defining role
Addition of security contractual proof solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Enables or Plays a defining role
Addition of security solutions is not feasible	
ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems	

Ranking of issues of greatest concern

Indicate issue of greatest concern _____	Enables or Plays a defining role
Indicate 2nd issue of greatest concern _____	
Indicate 3rd issue of greatest concern _____	
Indicate 3rd issue of greatest concern _____	
Indicate 3rd issue of greatest concern _____	
ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems	

1.1.1.4   **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, (I) 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

Architectural Issues

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
FIPS PUB 112 Password Usage	

Security measures commonly used with this data exchange	
Access control through passwords	Enables or Plays a defining role
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	
Firewalls with Access Control Lists and/or	Facilitates or Plays a role

proxy servers	
Dial-back modems	Facilitates or Plays a role
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
FIPS PUB 112 Password Usage	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	
Addition of security violation prevention solutions could be too difficult or burdensome for users	Enables or Plays a defining role
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	Facilitates or Plays a role
Addition of security solutions is not feasible	
FIPS PUB 112 Password Usage	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	
Addition of security violation detection solutions could be too difficult or burdensome for users	Enables or Plays a defining role
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	Facilitates or Plays a role
Addition of security solutions is not feasible	
FIPS PUB 112 Password Usage	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions	

could impact the required performance	
Addition of security contractual proof solutions could be too costly	
Addition of security contractual proof solutions could be too difficult or burdensome for users	Enables or Plays a defining role
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	Facilitates or Plays a role
Addition of security solutions is not feasible	
FIPS PUB 112 Password Usage	

1.1.1.5   FIPS PUB 113 Computer Data Authentication

URL: http:// http://www.itl.nist.gov/fipspubs/fip113.htm
http://www.dice.ucl.ac.be/crypto/standards/ **fips**/**fips113**/fip**113**.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

Architectural Issues

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
FIPS PUB 113 Computer Data Authentication	

Repudiation Ensuring that the source cannot deny sending the data or that the receiver cannot deny receiving the data is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
FIPS PUB 113 Computer Data Authentication	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	

Detection that a security violation was attempted is crucial	Facilitates or Plays a role
FIPS PUB 113 Computer Data Authentication	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	Facilitates or Plays a role
No standard solutions are available	
Addition of security solutions is not feasible	
FIPS PUB 113 Computer Data Authentication	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	Facilitates or Plays a role
Addition of security violation detection solutions could be too costly	Enables or Plays a defining role
Addition of security violation detection solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	Facilitates or Plays a role
No standard solutions are available	
Addition of security solutions is not feasible	
FIPS PUB 113 Computer Data Authentication	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	Facilitates or Plays a role
Addition of security contractual proof solutions could be too costly	Enables or Plays a defining role
Addition of security contractual proof solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	Facilitates or Plays a role
No standard solutions are available	
Addition of security solutions is not feasible	
FIPS PUB 113 Computer Data Authentication	

1.1.1.6 RFC 2196 Site Security Handbook

URL: 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

Architectural Issues

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
RFC 2196 Site Security Handbook	

Denial of Service Ensuring unimpeded access to data is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
RFC 2196 Site Security Handbook	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	Facilitates or Plays a role
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	Enables or Plays a defining role
Backup	Enables or Plays a defining role
Security policies with procedures to follow	Enables or Plays a defining role
Trusted parties so no cyber security needed	

None, but needed	
None, and not needed	
Other _____	
Other _____	
RFC 2196 Site Security Handbook	

1.1.1.7   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

Architectural Issues

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
RFC 2401 Security Architecture for the Internet Protocol	

Denial of Service Ensuring unimpeded access to data is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
RFC 2401 Security Architecture for the Internet Protocol	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	

Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
RFC 2401 Security Architecture for the Internet Protocol	

1.1.1.8 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

1.2 General Security Technologies

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	
RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	

Repudiation Ensuring that the source cannot deny sending the data or that the receiver cannot deny receiving the data is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	Enables or Plays a defining role
Firewalls with Access Control Lists and/or proxy servers	Enables or Plays a defining role
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	

1.2.1.1 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

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

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	
PKI - Public Key Infrastructure (X.509)	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
PKI - Public Key Infrastructure (X.509)	

Repudiation Ensuring that the source cannot deny sending the data or that the receiver cannot deny receiving the data is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
PKI - Public Key Infrastructure (X.509)	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Enables or Plays a defining

	role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
PKI - Public Key Infrastructure (X.509)	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	Enables or Plays a defining role
Firewalls with Access Control Lists and/or proxy servers	Enables or Plays a defining role
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
PKI - Public Key Infrastructure (X.509)	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
PKI - Public Key Infrastructure (X.509)	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
PKI - Public Key Infrastructure (X.509)	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	Enables or Plays a defining role
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
PKI - Public Key Infrastructure (X.509)	

1.2.1.2 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.

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	

Kerberos

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
Kerberos	

Repudiation Ensuring that the source cannot deny sending the data or that the receiver cannot deny receiving the data is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
Kerberos	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
Kerberos	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	Enables or Plays a defining role
Public key encryption (e.g. SSL/TLS)	Enables or Plays a defining role
Firewalls with Access Control Lists and/or proxy servers	Enables or Plays a defining role
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	

Non-repudiation techniques	
Kerberos	Enables or Plays a defining role
Network management such as SNMP or CMIP	Facilitates or Plays a role
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Kerberos	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	
Addition of security violation prevention solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
Kerberos	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation detection solutions could be too costly	
Addition of security violation detection solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
Kerberos	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	Enables or Plays a defining role
Addition of security contractual proof solutions could be too costly	

Addition of security contractual proof solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
Kerberos	

1.2.1.3 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

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	
FIPS 140-2 Security Requirements for Cryptographic Modules	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
FIPS 140-2 Security Requirements for Cryptographic Modules	

Repudiation Ensuring that the source cannot deny sending the data or that the receiver cannot deny receiving the data is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was	Facilitates or Plays a role

attempted is crucial	
FIPS 140-2 Security Requirements for Cryptographic Modules	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
FIPS 140-2 Security Requirements for Cryptographic Modules	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
FIPS 140-2 Security Requirements for Cryptographic Modules	

1.2.1.4 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,

Architectural Issues

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
FIPS 197 for Advanced Encryption Standard (AES)	

Repudiation Ensuring that the source cannot deny sending the data or that the receiver cannot deny receiving the data is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
FIPS 197 for Advanced Encryption Standard (AES)	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
FIPS 197 for Advanced Encryption Standard (AES)	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	

None, but needed	
None, and not needed	
Other _____	
Other _____	
FIPS 197 for Advanced Encryption Standard (AES)	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
FIPS 197 for Advanced Encryption Standard (AES)	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
FIPS 197 for Advanced Encryption Standard (AES)	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
FIPS 197 for Advanced Encryption Standard (AES)	

1.2.1.5 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

Architectural Issues

Repudiation Ensuring that the source cannot deny sending the data or that the receiver cannot deny receiving the data is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
Role-Based Access Control	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
Role-Based Access Control	

Security measures commonly used with this data exchange	
Access control through passwords	Enables or Plays a defining role
Access control through database security mechanisms	Enables or Plays a defining role
Virtual Private Networks (VPNs)	
Private (secret) key encryption	

Public key encryption (e.g. SSL/TLS)	
Firewalls with Access Control Lists and/or proxy servers	Enables or Plays a defining role
Dial-back modems	
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Role-Based Access Control	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	Enables or Plays a defining role
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
Role-Based Access Control	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	Enables or Plays a defining role
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
Role-Based Access Control	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	Enables or Plays a defining role
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	Enables or Plays a defining role
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
Role-Based Access Control	

1.2.1.6 PKCS

URL:

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

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	
PKCS	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
PKCS	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	

Public key encryption (e.g. SSL/TLS)	
Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
PKCS	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	Facilitates or Plays a role
No standard solutions are available	
Addition of security solutions is not feasible	
PKCS	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	Facilitates or Plays a role
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	Facilitates or Plays a role
No standard solutions are available	
Addition of security solutions is not feasible	
PKCS	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	Facilitates or Plays a role
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	Facilitates or Plays a role
No standard solutions are available	
Addition of security solutions is not feasible	
PKCS	

1.2.1.7 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

Architectural Issues

Information integrity violation Ensuring that data is not changed or destroyed is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
FIPS 186 Digital Signatures Standard (DSS)	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
FIPS 186 Digital Signatures Standard (DSS)	

Replay Ensuring that data cannot be resent by an unauthorized source is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining

	role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
FIPS 186 Digital Signatures Standard (DSS)	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
FIPS 186 Digital Signatures Standard (DSS)	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	
Non-repudiation techniques	Enables or Plays a defining role
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
FIPS 186 Digital Signatures Standard (DSS)	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role

Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
FIPS 186 Digital Signatures Standard (DSS)	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	Facilitates or Plays a role
Addition of security violation detection solutions could be too costly	Enables or Plays a defining role
Addition of security violation detection solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
FIPS 186 Digital Signatures Standard (DSS)	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	Facilitates or Plays a role
Addition of security contractual proof solutions could be too costly	Enables or Plays a defining role
Addition of security contractual proof solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
FIPS 186 Digital Signatures Standard (DSS)	

1.2.1.8 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:

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	
Intrusion Detection Technologies	

Information integrity violation Ensuring that data is not changed or destroyed is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
Intrusion Detection Technologies	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
Intrusion Detection Technologies	

Replay Ensuring that data cannot be resent by an unauthorized source is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
Intrusion Detection Technologies	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
Intrusion Detection Technologies	

Denial of Service Ensuring unimpeded access to data is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
Intrusion Detection Technologies	

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Facilitates or Plays a role
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	Enables or Plays a defining role
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Intrusion Detection Technologies	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	

Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Enables or Plays a defining role
Addition of security solutions is not feasible	
Intrusion Detection Technologies	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	Facilitates or Plays a role
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Enables or Plays a defining role
Addition of security solutions is not feasible	
Intrusion Detection Technologies	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	Facilitates or Plays a role
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Enables or Plays a defining role
Addition of security solutions is not feasible	
Intrusion Detection Technologies	

Ranking of issues of greatest concern	
Indicate issue of greatest concern _____	
Indicate 2nd issue of greatest concern _____	Enables or Plays a defining role
Indicate 3rd issue of greatest concern _____	
Indicate 3rd issue of greatest concern _____	

Indicate 3rd issue of greatest concern _____	
Intrusion Detection Technologies	

1.2.1.9 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

Architectural Issues

Information integrity violation Ensuring that data is not changed or destroyed is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
Intrusion Prevention Systems (IPS)	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
Intrusion Prevention Systems (IPS)	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
Intrusion Prevention Systems (IPS)	

Denial of Service Ensuring unimpeded access to data is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role

Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
Intrusion Prevention Systems (IPS)	

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Facilitates or Plays a role
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	Enables or Plays a defining role
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	Enables or Plays a defining role
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Intrusion Prevention Systems (IPS)	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Enables or Plays a defining role
Addition of security solutions is not feasible	
Intrusion Prevention Systems (IPS)	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection	Facilitates or Plays a role

solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Enables or Plays a defining role
Addition of security solutions is not feasible	
Intrusion Prevention Systems (IPS)	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	Facilitates or Plays a role
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Enables or Plays a defining role
Addition of security solutions is not feasible	
Intrusion Prevention Systems (IPS)	

Ranking of issues of greatest concern	
Indicate issue of greatest concern _____	
Indicate 2nd issue of greatest concern _____	Enables or Plays a defining role
Indicate 3rd issue of greatest concern _____	
Indicate 3rd issue of greatest concern _____	
Indicate 3rd issue of greatest concern _____	
Intrusion Prevention Systems (IPS)	

1.2.1.10   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

Architectural Issues

Denial of Service Ensuring unimpeded access to data is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
Service Level Agreements (SLA)	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	
Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	Facilitates or Plays a role
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role

Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Service Level Agreements (SLA)	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Enables or Plays a defining role
Addition of security solutions is not feasible	
Service Level Agreements (SLA)	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	Facilitates or Plays a role
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	Enables or Plays a defining role
Addition of security solutions is not feasible	
Service Level Agreements (SLA)	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	Facilitates or Plays a role
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	

No standard solutions are available	Enables or Plays a defining role
Addition of security solutions is not feasible	
Service Level Agreements (SLA)	

Ranking of issues of greatest concern	
Indicate issue of greatest concern _____	
Indicate 2nd issue of greatest concern _____	Facilitates or Plays a role
Indicate 3rd issue of greatest concern _____	
Indicate 3rd issue of greatest concern _____	
Indicate 3rd issue of greatest concern _____	
Service Level Agreements (SLA)	

1.3   Transport Layer Security Technologies

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	
AGA-12 Cryptographic Protection of SCADA Communications General Recommendations	

Information integrity violation Ensuring that data is not changed or destroyed is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
AGA-12 Cryptographic Protection of SCADA Communications General Recommendations	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	

Detection that a security violation was attempted is crucial	Facilitates or Plays a role
AGA-12 Cryptographic Protection of SCADA Communications General Recommendations	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
AGA-12 Cryptographic Protection of SCADA Communications General Recommendations	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
AGA-12 Cryptographic Protection of SCADA Communications General Recommendations	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	Enables or Plays a defining role
Addition of security violation detection solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
AGA-12 Cryptographic Protection of SCADA Communications General Recommendations	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	

Addition of security contractual proof solutions could be too costly	Enables or Plays a defining role
Addition of security contractual proof solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
AGA-12 Cryptographic Protection of SCADA Communications General Recommendations	

1.3.1.1 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

1.4   Application Layer Security Technologies
Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	
Transport Layer Security (TLS)/Secure Sockets Layer (SSL)	

Information integrity violation Ensuring that data is not changed or destroyed is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
Transport Layer Security (TLS)/Secure Sockets Layer (SSL)	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
Transport Layer Security (TLS)/Secure Sockets Layer (SSL)	

Replay Ensuring that data cannot be resent by an unauthorized source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
Transport Layer Security (TLS)/Secure Sockets Layer (SSL)	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
Transport Layer Security (TLS)/Secure Sockets Layer (SSL)	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	Enables or Plays a defining role
Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	

Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	Enables or Plays a defining role
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Transport Layer Security (TLS)/Secure Sockets Layer (SSL)	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
Transport Layer Security (TLS)/Secure Sockets Layer (SSL)	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
Transport Layer Security (TLS)/Secure Sockets Layer (SSL)	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	
Addition of security contractual proof solutions	Facilitates or Plays a role

could be too costly	
Addition of security contractual proof solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
Transport Layer Security (TLS)/Secure Sockets Layer (SSL)	

1.4.1.1 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

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	
RFC 2228 FTP Security Extensions	

Information integrity violation Ensuring that data is not changed or destroyed is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
RFC 2228 FTP Security Extensions	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
RFC 2228 FTP Security Extensions	

Replay Ensuring that data cannot be resent by an unauthorized source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
RFC 2228 FTP Security Extensions	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
RFC 2228 FTP Security Extensions	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
RFC 2228 FTP Security Extensions	

1.4.1.2 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 ASCI textual messages, non-textual messages, multi-part message

bodies, and non-US ASCI 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

1.4.1.3 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

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	
RFC 2086 IMAP4 ACL extension	

Information integrity violation Ensuring that data is not changed or destroyed is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
RFC 2086 IMAP4 ACL extension	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
RFC 2086 IMAP4 ACL extension	

Replay Ensuring that data cannot be resent by an unauthorized source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role

Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
RFC 2086 IMAP4 ACL extension	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
RFC 2086 IMAP4 ACL extension	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
RFC 2086 IMAP4 ACL extension	

1.4.1.4 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

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	
SNMP Security	

Information integrity violation Ensuring that data is not changed or destroyed is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
SNMP Security	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
SNMP Security	

Replay Ensuring that data cannot be resent by an unauthorized source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
SNMP Security	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
SNMP Security	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	Enables or Plays a defining role
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
SNMP Security	

1.4.1.5 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

Architectural Issues

Accuracy of data requirements	
Requires quality flag indicating at least normal and not normal	
Age of data needs to be knowable	Enables or Plays a defining role

Time skew of data must be known	Enables or Plays a defining role
Adequate accuracy can be assumed	
Accuracy of data not an issue	
RFC 1305 Network Time Protocol (Version 3) Specification, Implementation	

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	
RFC 1305 Network Time Protocol (Version 3) Specification, Implementation	

Information integrity violation Ensuring that data is not changed or destroyed is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
RFC 1305 Network Time Protocol (Version 3) Specification, Implementation	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
RFC 1305 Network Time Protocol (Version 3) Specification, Implementation	

Replay Ensuring that data cannot be resent by an unauthorized source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
RFC 1305 Network Time Protocol (Version 3) Specification, Implementation	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role

Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
RFC 1305 Network Time Protocol (Version 3) Specification, Implementation	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	Enables or Plays a defining role
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
RFC 1305 Network Time Protocol (Version 3) Specification, Implementation	

1.4.1.6 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:

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	
IEC 62351-3 Security for Profiles including TCP/IP	

Information integrity violation Ensuring that data is not changed or destroyed is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
IEC 62351-3 Security for Profiles including TCP/IP	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
IEC 62351-3 Security for Profiles including TCP/IP	

Replay Ensuring that data cannot be resent by an unauthorized source is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
IEC 62351-3 Security for Profiles including TCP/IP	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
IEC 62351-3 Security for Profiles including TCP/IP	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	Enables or Plays a defining role

Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	Enables or Plays a defining role
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
IEC 62351-3 Security for Profiles including TCP/IP	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
IEC 62351-3 Security for Profiles including TCP/IP	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
IEC 62351-3 Security for Profiles including TCP/IP	

Security Contractual Proof Issues, Concerns, and Problems

Addition of security contractual proof solutions could impact the required performance	
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
IEC 62351-3 Security for Profiles including TCP/IP	

1.4.1.7 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:

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	
IEC 62351-4 Security for Profiles including MMS (ISO-9506)	

Information integrity violation Ensuring that data is not changed or destroyed is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
IEC 62351-4 Security for Profiles including MMS (ISO-9506)	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	

Detection that a security violation was attempted is crucial	Enables or Plays a defining role
IEC 62351-4 Security for Profiles including MMS (ISO-9506)	

Replay Ensuring that data cannot be resent by an unauthorized source is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
IEC 62351-4 Security for Profiles including MMS (ISO-9506)	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
IEC 62351-4 Security for Profiles including MMS (ISO-9506)	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
IEC 62351-4 Security for Profiles including MMS (ISO-9506)	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
IEC 62351-4 Security for Profiles including MMS (ISO-9506)	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
IEC 62351-4 Security for Profiles including MMS (ISO-9506)	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
IEC 62351-4 Security for Profiles including MMS (ISO-9506)	

1.4.1.8 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:

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	
IEC 62351-5 Security for IEC 60870-5 and Derivatives	

Information integrity violation Ensuring that data is not changed or destroyed is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
IEC 62351-5 Security for IEC 60870-5 and Derivatives	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
IEC 62351-5 Security for IEC 60870-5 and Derivatives	

Replay Ensuring that data cannot be resent by an unauthorized source is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
IEC 62351-5 Security for IEC 60870-5 and Derivatives	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	

Detection that a security violation was attempted is crucial	Facilitates or Plays a role
IEC 62351-5 Security for IEC 60870-5 and Derivatives	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
IEC 62351-5 Security for IEC 60870-5 and Derivatives	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
IEC 62351-5 Security for IEC 60870-5 and Derivatives	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection	Facilitates or Plays a role

solutions could be too costly	
Addition of security violation detection solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
IEC 62351-5 Security for IEC 60870-5 and Derivatives	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
IEC 62351-5 Security for IEC 60870-5 and Derivatives	

1.4.1.9 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:

1.5 XML Related Technologies

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	
IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles	

Information integrity violation Ensuring that data is not changed or destroyed is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining

	role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles	

Replay Ensuring that data cannot be resent by an unauthorized source is	
Crucial	Enables or Plays a defining role
Quite important	Enables or Plays a defining role
Not particularly important	
Detection that a security violation was attempted is crucial	Enables or Plays a defining role
IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	

Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	Facilitates or Plays a role
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	Facilitates or Plays a role

Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles	

1.5.1.1 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

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Enables or Plays a defining role
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	
Private (secret) key encryption	
Public key encryption (e.g. SSL/TLS)	
Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	

None, and not needed	
Other _____	
Other _____	
OASIS Security Assertion Markup Language (SAML)	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
OASIS Security Assertion Markup Language (SAML)	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
OASIS Security Assertion Markup Language (SAML)	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
OASIS Security Assertion Markup Language (SAML)	

1.5.1.2 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:

Architectural Issues

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
OASIS Extensible Access Control Markup Language (XACML	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
OASIS Extensible Access Control Markup Language (XACML	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
OASIS Extensible Access Control Markup Language (XACML	

1.5.1.3 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:

Architectural Issues

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
XML Key Management Specification (XKMS	

Security measures commonly used with this data exchange	
Access control through passwords	
Access control through database security mechanisms	
Virtual Private Networks (VPNs)	Facilitates or Plays a role
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	
Firewalls with Access Control Lists and/or proxy servers	
Dial-back modems	
Bilateral data access control tables	
Timestamping, logging, and data records	
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
XML Key Management Specification (XKMS	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention	

solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	Facilitates or Plays a role
No standard solutions are available	
Addition of security solutions is not feasible	
XML Key Management Specification (XKMS	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	Facilitates or Plays a role
No standard solutions are available	
Addition of security solutions is not feasible	
XML Key Management Specification (XKMS	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	Facilitates or Plays a role
No standard solutions are available	
Addition of security solutions is not feasible	
XML Key Management Specification (XKMS	

Ranking of issues of greatest concern	
Indicate issue of greatest concern _____	
Indicate 2nd issue of greatest concern _____	
Indicate 3rd issue of greatest concern _____	Enables or Plays a defining role
Indicate 3rd issue of greatest concern _____	
Indicate 3rd issue of greatest concern _____	
XML Key Management Specification (XKMS	

1.5.1.4 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:

Architectural Issues

Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is	
Crucial	Enables or Plays a defining role
Quite important	
Not particularly important	
Detection that a security violation was attempted is crucial	
Secure XML	

Masquerade and/or spoofing Ensuring that data comes from the stated source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
Secure XML	

Replay Ensuring that data cannot be resent by an unauthorized source is	
Crucial	Facilitates or Plays a role
Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
Secure XML	

Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is	
Crucial	Facilitates or Plays a role

Quite important	Facilitates or Plays a role
Not particularly important	
Detection that a security violation was attempted is crucial	Facilitates or Plays a role
Secure XML	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	Facilitates or Plays a role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
Secure XML	

Security Detection Issues, Concerns, and Problems	
Addition of security violation detection solutions could impact the required performance	
Addition of security violation detection solutions could be too costly	Facilitates or Plays a role
Addition of security violation detection solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
Secure XML	

Security Contractual Proof Issues, Concerns, and Problems	
Addition of security contractual proof solutions could impact the required performance	
Addition of security contractual proof solutions could be too costly	Facilitates or Plays a role
Addition of security contractual proof solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
Secure XML	

2. Security Services

2.1 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

---

[1]extracted from
http://sybooks.sybase.com/onlinebooks/groupsec/secg0253e/epsec/@Generic__BookTextView/13539;pt=7509

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.

1.1.1.1.1 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 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.

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Facilitates or Plays a role
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	Facilitates or Plays a role
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	Facilitates or Plays a role
Non-repudiation techniques	Enables or Plays a defining role
Kerberos	
Network management such as SNMP or CMIP	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Audit Common Service	

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.

1.1.1.1.2 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   *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.

Security Strategy	Authentication Factor			Biometric	Comments
	Single	Two	Three		
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 C double as a Personal ID. This recommended strategy.
Smart ID Card used to enable Combination Lock		X			This is the best mechanism f access to sensitive areas.
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	x			

Photo-ID				
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 Combination Lock	x	x	x	This is one of the recommended deployment 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   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-CARD[2]s 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.

1.1.1.1.3 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.

---

[2] The actual technology recommendation for Smart-Cards can be found in the Identity Establish service section.

- 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   *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:

- 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.

2.1.1.2.1.3   *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. *Proceedings of Grid2002 Workshop*, 2002.

ACC-03   AA-2004.02 -- Denial of Service Vulnerability in IEEE 802.11 Wireless Devices (AusCERT)

2.1.1.2.1.4   *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.htmlRADIUS 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	

2.1.1.2.1.4.1 Technological Assessment and Recommendations

2.1.1.2.1.4.1.1 OS Recommendations

It is recommended that Trusted OSs be used whenever possible. Additionally, ANSI INCITS 359-2004 us suggested as an implementation strategy for Role Based Access.

2.1.1.2.1.4.1.2 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.

2.1.1.2.1.4.1.3 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 implement 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.

1.1.1.1.4 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 (wc3.org)
               Available from: http://www.w3.org/2002/03/semweb/access-control

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Enables or Plays a defining role
Access control through database security mechanisms	Enables or Plays a defining role
Virtual Private Networks (VPNs)	Enables or Plays a defining role
Firewalls with Access Control Lists and/or proxy servers	Enables or Plays a defining role
Dial-back modems	Enables or Plays a defining role
Bilateral data access control tables	Enables or Plays a defining role
Non-repudiation techniques	Enables or Plays a defining role
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role
Backup	
Security policies with procedures to follow	Enables or Plays a defining role
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Authorization for 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.

1.1.1.1.5 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 x 1016 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   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   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.

2.1.1.3.1.1.2   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 appropriate.
RFC 1968	The PPP Encryption Control Protocol (ECP)	
RFC 2246	The TLS Protocol Version 1.0	

Identification Number	Name	Comment
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
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.	

Identification Number	Name	Comment
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.	

1.1.1.1.6 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).

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Facilitates or Plays a role
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	Significantly hinders
Non-repudiation techniques	Significantly hinders
Kerberos	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Confidentiality	

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.

1.1.1.1.7 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   *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.

Identification Number	Name	Comment
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.

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Enables or Plays a defining role
Firewalls with Access Control Lists and/or proxy servers	Enables or Plays a defining role
Dial-back modems	Facilitates or Plays a role
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	Facilitates or Plays a role
Non-repudiation techniques	Enables or Plays a defining role
Kerberos	
Network management such as SNMP or CMIP	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Credential Conversion	

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.

1.1.1.1.8 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 *Specific Recommendations*

2.1.1.5.1.1.1 *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-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	

Identification Number	Name	Comment
RFC 2875	Diffie-Hellman Proof-of-Possession Algorithms	
RFC 2986	http://www.armware.dk/RFC/rfc/rfc2986.htmlPKCS #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.htmlDomain 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.htmlDefinitions of Managed Objects for the Delegation of Management Script	
RFC 2874	http://www.armware.dk/RFC/rfc/rfc2874.htmlDNS 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	

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Enables or Plays a defining role
Private (secret) key encryption	Facilitates or Plays a role
Dial-back modems	Enables or Plays a defining role
Timestamping, logging, and data records	Facilitates or Plays a role
Non-repudiation techniques	Enables or Plays a defining role
Kerberos	

Network management such as SNMP or CMIP	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Credential Renewal Service	

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.

1.1.1.1.9 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.htmlDomain names - concepts and facilities	
RFC 1507	DASS - Distributed Authentication Security Service	
RFC 1591	http://www.armware.dk/RFC/rfc/rfc1591.htmlDomain Name System Structure and Delegation	
RFC 1608	Representing IP Information in the X.500 Directory	

Identification Number	Name	Comment
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.htmlDefinitions of Managed Objects for the Delegation of Management Script	
RFC 2874	http://www.armware.dk/RFC/rfc/rfc2874.htmlDNS 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

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Enables or Plays a defining role
Private (secret) key encryption	Facilitates or Plays a role
Dial-back modems	Enables or Plays a defining role
Timestamping, logging, and data records	Facilitates or Plays a role

Non-repudiation techniques	Enables or Plays a defining role
Kerberos	
Network management such as SNMP or CMIP	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Delegation Service	

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?

1.1.1.1.10   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.
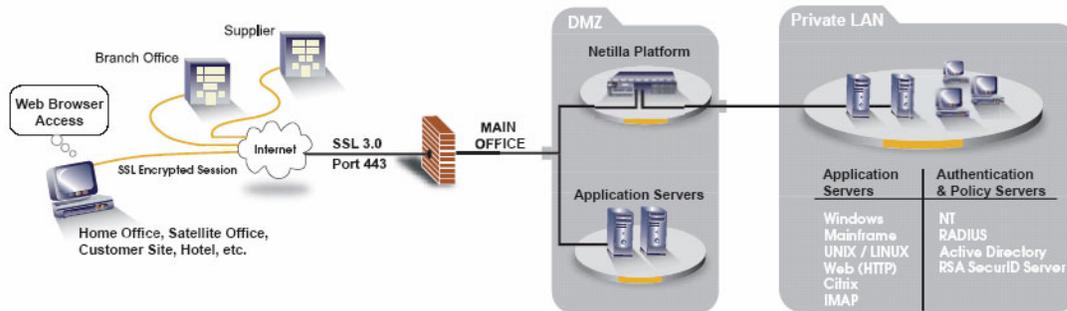
Figure 1: Example of SSL/TLS Tunnel for Firewall Transversal[3]

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

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.htmlAnti-Spam Recommendations for SMTP MTAs	

---

[3] Image courtesy of Allegiant Data Systems

Identification Number	Name	Comment
RFC 2543	http://www.armware.dk/RFC/rfc/rfc2543.htmlSIP: Session Initiation Protocol	
RFC 2547	http://www.armware.dk/RFC/rfc/rfc2547.htmlBGP/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

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Enables or Plays a defining role
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	Enables or Plays a defining role
Dial-back modems	Facilitates or Plays a role
Timestamping, logging, and data records	Facilitates or Plays a role
Non-repudiation techniques	Facilitates or Plays a role
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role
Physical isolation	Enables or Plays a defining role
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Firewall Traversal	

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]

1.1.1.1.11   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 needs 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).

1.1.1.1.12   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 2-92). 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

2.1.1.8.1.1   *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.

2.1.1.8.1.1.1   *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.

2.1.1.8.1.1.2   *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.

2.1.1.8.1.1.3 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 CardTM 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

Identification Number	Name	Comment
		Management service)
ISO/IEC 7816-7:1999	Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured 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

2.1.1.8.1.1.4   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	

2.1.1.8.1.1.5   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 used[4]

Table 19: Relevant Specifications for Digital Signatures

Identification Number	Name	Comment
RFC 2313	http://www.armware.dk/RFC/rfc/rfc2313.htmlPKCS #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	

2.1.1.8.1.1.6   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

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Enables or Plays a defining role
Access control through database security mechanisms	Enables or Plays a defining role
Virtual Private Networks (VPNs)	Enables or Plays a defining role
Private (secret) key encryption	Enables or Plays a defining role
Public key encryption (e.g. SSL/TLS)	Enables or Plays a defining role
Firewalls with Access Control Lists and/or proxy servers	Enables or Plays a defining role
Dial-back modems	Enables or Plays a defining role
Bilateral data access control tables	Enables or Plays a defining role
Non-repudiation techniques	Enables or Plays a defining role
Kerberos	
Network management such as SNMP or CMIP	Enables or Plays a defining role
Backup	
Security policies with procedures to follow	Enables or Plays a defining role
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Identity Establishment Service	

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.

1.1.1.1.13   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   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.

2.1.1.9.1.2   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).

2.1.1.9.1.3   Digital Certificates

See the discussion in the Credential Conversion service discussion.

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role

Virtual Private Networks (VPNs)	Enables or Plays a defining role
Private (secret) key encryption	Facilitates or Plays a role
Dial-back modems	Enables or Plays a defining role
Non-repudiation techniques	Facilitates or Plays a role
Kerberos	
Network management such as SNMP or CMIP	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Identity Mapping Service	

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 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.

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Timestamping, logging, and data records	Facilitates or Plays a role
Non-repudiation techniques	Facilitates or Plays a role
Kerberos	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	

None, but needed	
None, and not needed	
Other _____	
Other _____	
Information Integrity Service	

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.

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Facilitates or Plays a role
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	Facilitates or Plays a role
Bilateral data access control tables	Facilitates or Plays a role
Non-repudiation techniques	Facilitates or Plays a role
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role
Physical isolation	Facilitates or Plays a role
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Inter-Domain Security	

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.

1.1.1.1.14 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-	Information technology - Guidelines for the management	

5	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.

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Facilitates or Plays a role
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	Facilitates or Plays a role
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	Enables or Plays a defining role
Non-repudiation techniques	Enables or Plays a defining role
Kerberos	
Network management such as SNMP or CMIP	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Non-repudiation	

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.

1.1.1.1.15 Technological Assessment and Relevant Specifications

2.1.1.13.1.1 *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.

2.1.1.13.1.2 *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

Architectural Issues

Security measures commonly used with this data exchange	
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role
Physical isolation	Facilitates or Plays a role
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	

None, but needed	
None, and not needed	
Other _____	
Other _____	
Path Routing and QOS Service	

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. he 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 breeches, 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 effected[6]). 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.

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.

---

[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.

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.
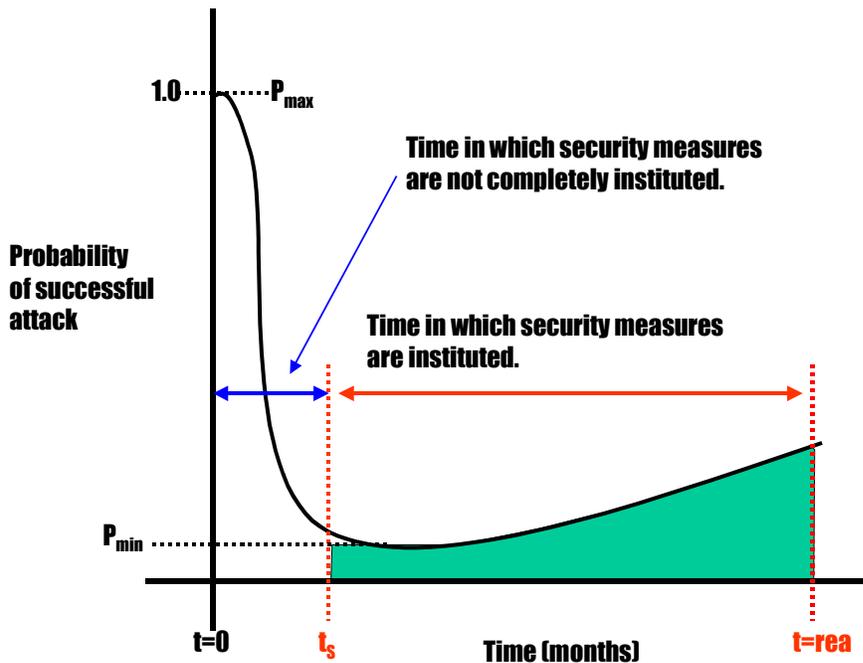
Figure 3: General trend is security vulnerabilities (extracted from EPRI Report 1008988)

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.

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Enables or Plays a defining role
Access control through database security mechanisms	Enables or Plays a defining role
Virtual Private Networks (VPNs)	Enables or Plays a defining role
Private (secret) key encryption	Enables or Plays a defining role
Public key encryption (e.g. SSL/TLS)	Enables or Plays a defining role
Firewalls with Access Control Lists and/or proxy servers	Enables or Plays a defining role
Dial-back modems	Enables or Plays a defining role
Bilateral data access control tables	Enables or Plays a defining role
Timestamping, logging, and data records	Enables or Plays a defining role
Non-repudiation techniques	Enables or Plays a defining role
Kerberos	
Network management such as SNMP or CMIP	Enables or Plays a defining role
Physical isolation	Enables or Plays a defining role
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	

Other _____	
Security Policies	

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.

1.1.1.1.16   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: http://xml.coverpages.org/ws-policyattachmentV11.pdf	Recommended

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.

1.1.1.1.17   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

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Facilitates or Plays a role
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	Facilitates or Plays a role
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	Facilitates or Plays a role
Non-repudiation techniques	Facilitates or Plays a role

Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Privacy Service	

2.1.1.17 Profile Service (User Profile Service)

The profile service is concerned with managing service requestor's preferences and data which my 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.

1.1.1.1.18   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	

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role

Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Facilitates or Plays a role
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	Facilitates or Plays a role
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	Facilitates or Plays a role
Non-repudiation techniques	Enables or Plays a defining role
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Profile Service (User Profile Service)	

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

1.1.1.1.19   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.

1.1.1.1.20   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	

Identification Number	Name	Comment
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	

Architectural Issues

Security measures commonly used with this data exchange	
Virtual Private Networks (VPNs)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	Facilitates or Plays a role
Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	Facilitates or Plays a role
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Security against Denial-of-Service	

2.1.1.20 Security Assurance Management

Explicitly recognize the need for manageability of security functionality within the IECSA 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.

1.1.1.1.21 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	

Identification Number	Name	Comment
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	
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

Architectural Issues

Location of information producer (source of data)	
Operations center	
Corporate building	
Building	
Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	
Security Assurance Management	

Location of information receiver (user of data)	
Operations center	
Corporate building	
Building	
Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	
Security Assurance Management	

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Facilitates or Plays a role
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role

Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	Facilitates or Plays a role
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	Facilitates or Plays a role
Non-repudiation techniques	Facilitates or Plays a role
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role
Physical isolation	Facilitates or Plays a role
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Security Assurance Management	

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.

1.1.1.1.22   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.

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Facilitates or Plays a role
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	Facilitates or Plays a role
Timestamping, logging, and data records	Facilitates or Plays a role
Non-repudiation techniques	
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	

Other _____	
Other _____	
Security Protocol Mapping	

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.

1.1.1.1.23   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: 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	

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Facilitates or Plays a role
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role

Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	Facilitates or Plays a role
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	Facilitates or Plays a role
Non-repudiation techniques	Facilitates or Plays a role
Kerberos	
Network management such as SNMP or CMIP	
Physical isolation	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Security Service Availability Discovery Service	

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.

Architectural Issues

Location of information producer (source of data)	
Operations center	
Corporate building	
Building	
Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	

Single Sign On Service

Location of information receiver (user of data)	
Operations center	
Corporate building	
Building	
Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	
Single Sign On Service	

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Facilitates or Plays a role
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	Facilitates or Plays a role
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	Facilitates or Plays a role
Non-repudiation techniques	Facilitates or Plays a role
Kerberos	
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Single Sign On Service	

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.

Architectural Issues

Security measures commonly used with this data exchange	
Access control through passwords	Facilitates or Plays a role
Access control through database security mechanisms	Facilitates or Plays a role
Virtual Private Networks (VPNs)	Facilitates or Plays a role
Private (secret) key encryption	Facilitates or Plays a role
Public key encryption (e.g. SSL/TLS)	Facilitates or Plays a role
Firewalls with Access Control Lists and/or proxy servers	Facilitates or Plays a role
Dial-back modems	Facilitates or Plays a role
Bilateral data access control tables	Facilitates or Plays a role
Timestamping, logging, and data records	Facilitates or Plays a role
Non-repudiation techniques	Enables or Plays a defining role
Kerberos	
Network management such as SNMP or CMIP	Facilitates or Plays a role
Backup	
Security policies with procedures to follow	
Trusted parties so no cyber security needed	
None, but needed	
None, and not needed	
Other _____	
Other _____	
Trust Establishment Service	

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.

3.   Security Best Practices

3.1   Security Policy

3.1.1 General Security Policy Process

3.1.1.1.1   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 breeches, 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.

3.1.1.1.2   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.

3.1.1.1.3 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 effected[8]). 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.

3.1.1.1.4 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.

---

[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.

3.1.1.1.5   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 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.
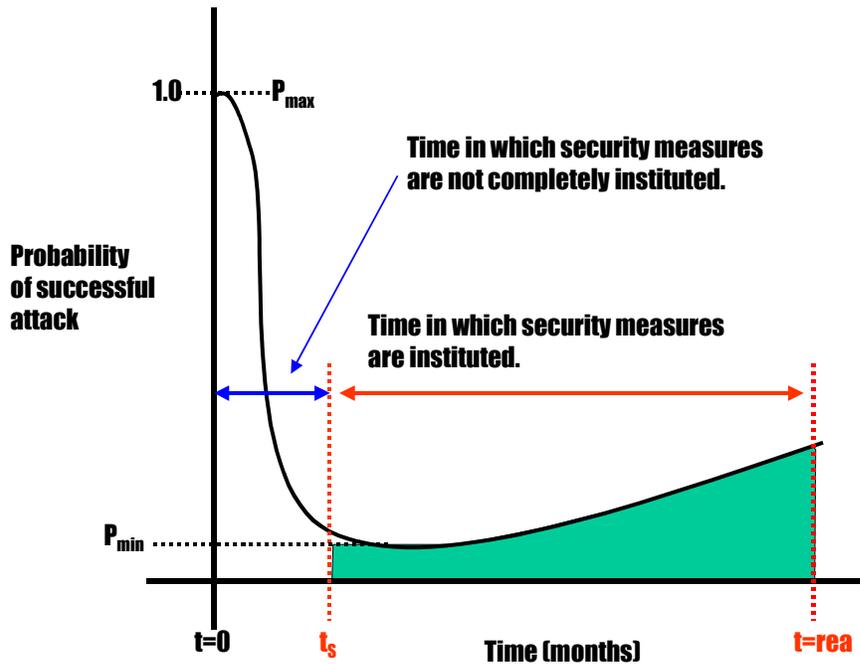
Figure 5: General trend is security vulnerabilities (extracted from EPRI Report 1008988)

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.

3.1.1.2   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 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.

- 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.

3.1.2 Specific Policy Issues and Recommendations per Service

Some security services merit specific policy recommendations that were not expressed within the security service section explicitly.

3.1.2.1.1 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.

3.1.2.1.2 Credentials and User Accounts

1.1.1.1.24 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.

3.1.2.1.2.1　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.

3.1.2.1.2.2　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.

3.1.2.1.2.2.1　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.

3.1.2.1.2.2.2　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).

3.1.2.1.2.3   *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 characters9:   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

---

[9] Assuming the following characters: !, @, #, $, %,^,&,*,(,), _, -, +, =, {, }, [,], |, \, :, ;, ",', <, >, . , comma, ?, and /. For a total of

All characters	6

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.

3.1.2.1.2.4   *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.

3.1.2.1.2.5   *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.

3.1.2.1.2.6   *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.

3.1.2.1.3   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.

1.1.1.1.25   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.

3.1.2.2 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

3.1.2.3 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 Security Frameworks and Policy Documents

3.2.1.1 ISO/IEC Security Best Practices

3.2.1.2 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

3.2.1.3 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

3.2.1.4 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

3.2.1.5 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:

3.2.1.6 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

3.2.1.7 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:

3.2.1.8 Federal Security Best Practices

3.2.1.9 CICSI 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:

3.2.1.10 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, (I) 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

3.2.1.11 FIPS PUB 113 Computer Data Authentication

URL: http:// http://www.itl.nist.gov/fipspubs/fip113.htm
http://www.dice.ucl.ac.be/crypto/standards/ **fips/fips113**/fip**113**.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

3.2.1.12 IETF Security Best Practices Internet Requests for Comments (RFCs)

3.2.1.13   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

3.2.1.14   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

3.2.1.15   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

3.2.1.16   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:

3.2.1.17   RFC 2196 Site Security Handbook

URL: 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

3.2.1.18   RFC 2276 Architectural Principles of Uniform Resource Name Resolution

URL: 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.

3.2.1.19   RFC 2350 Expectations for Computer Security Incident Response

URL: 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.

3.2.1.20   RFC 2386 A Framework for QoS-based Routing in the Internet

URL: 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.

3.2.1.21   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

3.2.1.22   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:

3.2.1.23   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:

3.2.1.24 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:

3.2.1.25 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:

3.2.1.26 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:

3.2.1.27 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:

3.2.1.28   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:

3.2.1.29 Other Security Best Practices

3.2.1.30   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:

3.2.1.31   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:

3.2.1.32   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:

3.2.1.33   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:

3.2.1.34   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:

3.2.1.35   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 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.

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.

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.

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).

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:

Architectural Issues

Location of information producer (source of data)	
Operations center	
Corporate building	
Building	
Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	
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	

Location of information receiver (user of data)	
Operations center	
Corporate building	

Building	
Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	
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	

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:

Architectural Issues

Location of information producer (source of data)	
Operations center	
Corporate building	
Building	
Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	
ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks	

Location of information receiver (user of data)	
Operations center	
Corporate building	
Building	

Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	
ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks	

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:

Architectural Issues

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview	

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&ICS2=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:

Architectural Issues

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security	

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:

Architectural Issues

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the	

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:

Architectural Issues

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security	

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:

Architectural Issues

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode	

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:

Architectural Issues

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
ISO/IEC 15408-2:1999 Information technology -- Security techniques --	

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:

Architectural Issues

Location of information producer (source of data)	
Operations center	
Corporate building	
Building	
Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	
ISO/IEC 15408-3:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements	

Location of information receiver (user of data)	
Operations center	
Corporate building	
Building	
Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	
ISO/IEC 15408-3:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements	

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:

Architectural Issues

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
ISO/IEC 17799:2000 Information technology -- Code of practice for information security management	

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:

4.2 Federal Documents on Security Technologies

4.2.1.1 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:

4.3 IETF Internet Requests for Comments (RFCs) on Security Technologies

4.3.1.1 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

4.3.1.2 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.

4.3.1.3 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:

4.3.1.4 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:

4.3.1.5 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:

4.3.1.6 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:

4.3.1.7 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:

4.3.1.8 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

4.3.1.9 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

Architectural Issues

Communication access services requirements	
Any or all	
Request-response	
Periodic reporting	
Report-by-exception	
Control command	
Select-before-operate	
Set parameter values	
Query for data by name	
Subscribe	
Broadcast	
Multi-cast	
Data discovery	
Use of data sets	
Query to find location of data	
Query to determine what data is available (discovery)	
Execute application	Enables or Plays a defining role
Establish and end association	Enables or Plays a defining role
Logging	
Journaling	
Remote restart	
Remote reconfiguration	Enables or Plays a defining role

Remote diagnosis	Enables or Plays a defining role
RFC 1352 SNMP Security Protocols	

Commonly used techniques for meeting quality of service requirements of this data exchange	
Failure detection	Enables or Plays a defining role
Automatic restart	Enables or Plays a defining role
Automatic failover to second source of data or function	Enables or Plays a defining role
Automatic failover of communication channels to secondary channel	Enables or Plays a defining role
Backup of data	
Transaction rollback	
QoS monitoring	Enables or Plays a defining role
Alarming on QoS failure	Enables or Plays a defining role
None	
Not needed or not relevant	
Other _____	
Other _____	
RFC 1352 SNMP Security Protocols	

Management of large volumes of data that are being exchanged	
Major part of step involves handling large volumes of data	Enables or Plays a defining role
Some part of step involves handling large volumes of data	Enables or Plays a defining role
No part of step involves handling large volumes of data	
RFC 1352 SNMP Security Protocols	

Data consistency and synchronization management across systems	
Second-by-second synchronization Data being exchanged must be kept consistent and synchronized with other systems within seconds	Enables or Plays a defining role
Minute-by-minute synchronization Data being exchanged must be kept consistent and synchronized with other systems within minutes	
Day-by-day synchronization Data being exchanged must be kept consistent and synchronized with other systems within hours or days	
No synchronization Data being exchanged does not need to be kept consistent or synchronized with other systems	

RFC 1352 SNMP Security Protocols

Management of timely access to data by multiple different users	
Contractual/required time windows for multiple access are less than one second	Enables or Plays a defining role
Contractual/required time windows for multiple access are within seconds	Enables or Plays a defining role
Contractual/required time windows for multiple access are within tens of seconds	
Contractual/required time windows for multiple access are within minutes	
Timely access by multiple users is not relevant	
RFC 1352 SNMP Security Protocols	

4.3.1.10   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

4.3.1.11   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

4.3.1.12   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

4.3.1.13   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:

4.3.1.14   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:

4.3.1.15 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:

4.3.1.16 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:

4.3.1.17   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:

4.3.1.18   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:

Architectural Issues

Communication access services requirements	
Any or all	
Request-response	
Periodic reporting	
Report-by-exception	
Control command	
Select-before-operate	
Set parameter values	
Query for data by name	
Subscribe	
Broadcast	
Multi-cast	
Data discovery	
Use of data sets	
Query to find location of data	
Query to determine what data is available (discovery)	
Execute application	Enables or Plays a defining role
Establish and end association	Enables or Plays a defining role
Logging	
Journaling	
Remote restart	
Remote reconfiguration	Enables or Plays a defining role
Remote diagnosis	Enables or Plays a defining role
RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)	

Commonly used techniques for meeting quality of service requirements of this data exchange	
Failure detection	Enables or Plays a defining role
Automatic restart	Enables or Plays a defining role
Automatic failover to second source of data or function	Enables or Plays a defining role
Automatic failover of communication channels to secondary channel	Enables or Plays a defining role
Backup of data	
Transaction rollback	
QoS monitoring	Enables or Plays a defining

	role
Alarming on QoS failure	Enables or Plays a defining role
None	
Not needed or not relevant	
Other _____	
Other _____	
RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)	

Management of large volumes of data that are being exchanged	
Major part of step involves handling large volumes of data	Enables or Plays a defining role
Some part of step involves handling large volumes of data	Enables or Plays a defining role
No part of step involves handling large volumes of data	
RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)	

Data consistency and synchronization management across systems	
Second-by-second synchronization Data being exchanged must be kept consistent and synchronized with other systems within seconds	Enables or Plays a defining role
Minute-by-minute synchronization Data being exchanged must be kept consistent and synchronized with other systems within minutes	
Day-by-day synchronization Data being exchanged must be kept consistent and synchronized with other systems within hours or days	
No synchronization Data being exchanged does not need to be kept consistent or synchronized with other systems	
RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)	

Management of timely access to data by multiple different users	
Contractual/required time windows for multiple access are less than one second	Enables or Plays a defining role
Contractual/required time windows for multiple access are within seconds	Enables or Plays a defining role
Contractual/required time windows for multiple access are within tens of seconds	
Contractual/required time windows for multiple access are within minutes	
Timely access by multiple users is not relevant	
RFC 1940 Source Demand Routing: Packet Format and Forwarding	

4.3.1.19 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:

4.3.1.20 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:

4.3.1.21 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 ASCI textual messages, non-textual messages, multi-part message bodies, and non-US ASCI 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

4.3.1.22 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, Un-authorized access, Security

4.3.1.23 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:

4.3.1.24 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:

4.3.1.25 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 authenticatible 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:

4.3.1.26 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:

4.3.1.27   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:

4.3.1.28   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:

4.3.1.29   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:

4.3.1.30 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.

4.3.1.31 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].

4.3.1.32 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:

4.3.1.33 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:

4.3.1.34 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:

4.3.1.35 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.

4.3.1.36 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:

4.3.1.37 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:

4.3.1.38 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:

4.3.1.39 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:

4.3.1.40 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:

4.3.1.41   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:

4.3.1.42   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:

Architectural Issues

Communication access services requirements	
Any or all	
Request-response	
Periodic reporting	
Report-by-exception	
Control command	
Select-before-operate	
Set parameter values	
Query for data by name	
Subscribe	
Broadcast	
Multi-cast	
Data discovery	

Use of data sets	
Query to find location of data	
Query to determine what data is available (discovery)	
Execute application	Enables or Plays a defining role
Establish and end association	Enables or Plays a defining role
Logging	
Journaling	
Remote restart	
Remote reconfiguration	Enables or Plays a defining role
Remote diagnosis	Enables or Plays a defining role
RFC 2547 BGP/MPLS VPNs	

Commonly used techniques for meeting quality of service requirements of this data exchange	
Failure detection	Enables or Plays a defining role
Automatic restart	Enables or Plays a defining role
Automatic failover to second source of data or function	Enables or Plays a defining role
Automatic failover of communication channels to secondary channel	Enables or Plays a defining role
Backup of data	
Transaction rollback	
QoS monitoring	Enables or Plays a defining role
Alarming on QoS failure	Enables or Plays a defining role
None	
Not needed or not relevant	
Other _____	
Other _____	
RFC 2547 BGP/MPLS VPNs	

Management of large volumes of data that are being exchanged	
Major part of step involves handling large volumes of data	Enables or Plays a defining role
Some part of step involves handling large volumes of data	Enables or Plays a defining role
No part of step involves handling large volumes of data	
RFC 2547 BGP/MPLS VPNs	

Data consistency and synchronization management across systems	
Second-by-second synchronization Data	Enables or Plays a defining

being exchanged must be kept consistent and synchronized with other systems within seconds	role
Minute-by-minute synchronization Data being exchanged must be kept consistent and synchronized with other systems within minutes	
Day-by-day synchronization Data being exchanged must be kept consistent and synchronized with other systems within hours or days	
No synchronization Data being exchanged does not need to be kept consistent or synchronized with other systems	
RFC 2547 BGP/MPLS VPNs	

Management of timely access to data by multiple different users	
Contractual/required time windows for multiple access are less than one second	Enables or Plays a defining role
Contractual/required time windows for multiple access are within seconds	Enables or Plays a defining role
Contractual/required time windows for multiple access are within tens of seconds	
Contractual/required time windows for multiple access are within minutes	
Timely access by multiple users is not relevant	
RFC 2547 BGP/MPLS VPNs	

4.3.1.43 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:

4.3.1.44 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:

4.3.1.45   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:

4.3.1.46   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:

Architectural Issues

Communication access services requirements	
Any or all	
Request-response	
Periodic reporting	
Report-by-exception	
Control command	
Select-before-operate	
Set parameter values	
Query for data by name	
Subscribe	
Broadcast	
Multi-cast	
Data discovery	
Use of data sets	
Query to find location of data	
Query to determine what data is available (discovery)	
Execute application	Enables or Plays a defining role
Establish and end association	Enables or Plays a defining role
Logging	
Journaling	

Remote restart	
Remote reconfiguration	Enables or Plays a defining role
Remote diagnosis	Enables or Plays a defining role
RFC 2764 A Framework for IP Based Virtual Private Networks	

Commonly used techniques for meeting quality of service requirements of this data exchange	
Failure detection	Enables or Plays a defining role
Automatic restart	Enables or Plays a defining role
Automatic failover to second source of data or function	Enables or Plays a defining role
Automatic failover of communication channels to secondary channel	Enables or Plays a defining role
Backup of data	
Transaction rollback	
QoS monitoring	Enables or Plays a defining role
Alarming on QoS failure	Enables or Plays a defining role
None	
Not needed or not relevant	
Other _____	
Other _____	
RFC 2764 A Framework for IP Based Virtual Private Networks	

Management of large volumes of data that are being exchanged	
Major part of step involves handling large volumes of data	Enables or Plays a defining role
Some part of step involves handling large volumes of data	Enables or Plays a defining role
No part of step involves handling large volumes of data	
RFC 2764 A Framework for IP Based Virtual Private Networks	

Data consistency and synchronization management across systems	
Second-by-second synchronization Data being exchanged must be kept consistent and synchronized with other systems within seconds	Enables or Plays a defining role
Minute-by-minute synchronization Data being exchanged must be kept consistent and synchronized with other systems within minutes	
Day-by-day synchronization Data being exchanged must be kept consistent and synchronized with other systems within hours or days	

No synchronization Data being exchanged does not need to be kept consistent or synchronized with other systems	
RFC 2764 A Framework for IP Based Virtual Private Networks	

Management of timely access to data by multiple different users	
Contractual/required time windows for multiple access are less than one second	Enables or Plays a defining role
Contractual/required time windows for multiple access are within seconds	Enables or Plays a defining role
Contractual/required time windows for multiple access are within tens of seconds	
Contractual/required time windows for multiple access are within minutes	
Timely access by multiple users is not relevant	
RFC 2764 A Framework for IP Based Virtual Private Networks	

4.3.1.47　　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:

Architectural Issues

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
RFC 2753 A Framework for Policy-based Admission Control	

4.3.1.48　　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:

Architectural Issues

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
RFC 2797 Certificate Management Messages over CMS	

4.3.1.49   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

4.3.1.50   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

4.3.1.51 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:

4.3.1.52 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:

4.3.1.53 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:

4.3.1.54 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:

4.3.1.55 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:

4.3.1.56 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:

4.3.1.57 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:

4.3.1.58 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:

4.3.1.59 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:

Architectural Issues

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements	

4.3.1.60 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:

4.3.1.61 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:

4.3.1.62 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:

Architectural Issues

Location of information producer (source of data)	
Operations center	
Corporate building	
Building	
Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	
RFC 2986 PKCS #10: Certification Request Syntax Specification Version 1.7	

Location of information receiver (user of data)	
Operations center	
Corporate building	
Building	
Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	
RFC 2986 PKCS #10: Certification Request Syntax Specification Version 1.7	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
RFC 2986 PKCS #10: Certification Request Syntax Specification Version 1.7	

4.3.1.63 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:

Architectural Issues

Communication access services requirements	
Any or all	
Request-response	
Periodic reporting	
Report-by-exception	
Control command	
Select-before-operate	
Set parameter values	
Query for data by name	
Subscribe	
Broadcast	
Multi-cast	
Data discovery	
Use of data sets	
Query to find location of data	
Query to determine what data is available (discovery)	
Execute application	Enables or Plays a defining role
Establish and end association	Enables or Plays a defining role
Logging	
Journaling	
Remote restart	
Remote reconfiguration	Enables or Plays a defining role
Remote diagnosis	Enables or Plays a defining role
RFC 3053 IPv6 Tunnel Broker	

Commonly used techniques for meeting quality of service requirements of this data exchange	
Failure detection	Enables or Plays a defining role
Automatic restart	Enables or Plays a defining role
Automatic failover to second source of data or function	Enables or Plays a defining role
Automatic failover of communication channels to secondary channel	Enables or Plays a defining role
Backup of data	
Transaction rollback	
QoS monitoring	Enables or Plays a defining role
Alarming on QoS failure	Enables or Plays a defining role

None	
Not needed or not relevant	
Other _____	
Other _____	
RFC 3053 IPv6 Tunnel Broker	

Management of large volumes of data that are being exchanged	
Major part of step involves handling large volumes of data	Enables or Plays a defining role
Some part of step involves handling large volumes of data	Enables or Plays a defining role
No part of step involves handling large volumes of data	
RFC 3053 IPv6 Tunnel Broker	

Data consistency and synchronization management across systems	
Second-by-second synchronization Data being exchanged must be kept consistent and synchronized with other systems within seconds	Enables or Plays a defining role
Minute-by-minute synchronization Data being exchanged must be kept consistent and synchronized with other systems within minutes	
Day-by-day synchronization Data being exchanged must be kept consistent and synchronized with other systems within hours or days	
No synchronization Data being exchanged does not need to be kept consistent or synchronized with other systems	
RFC 3053 IPv6 Tunnel Broker	

Management of timely access to data by multiple different users	
Contractual/required time windows for multiple access are less than one second	Enables or Plays a defining role
Contractual/required time windows for multiple access are within seconds	Enables or Plays a defining role
Contractual/required time windows for multiple access are within tens of seconds	
Contractual/required time windows for multiple access are within minutes	
Timely access by multiple users is not relevant	
RFC 3053 IPv6 Tunnel Broker	

4.3.1.64   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:

4.3.1.65 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.

Architectural Issues

Location of information producer (source of data)	
Operations center	
Corporate building	
Building	
Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	
RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	

Location of information receiver (user of data)	
Operations center	
Corporate building	
Building	
Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	
RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	

Security Prevention Issues, Concerns, and Problems

Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role
No standard solutions are available	
Addition of security solutions is not feasible	
RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	

4.3.1.66 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:

4.3.1.67 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:

4.3.1.68 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:

4.3.1.69 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:

4.3.1.70 RFC 3403 Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database

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:

4.3.1.71 RFC 3404 Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI)

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:

4.3.1.72 RFC 3405 Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures

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:

4.3.1.73 RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

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:

Architectural Issues

Communication access services requirements	
Any or all	

Request-response	
Periodic reporting	
Report-by-exception	
Control command	
Select-before-operate	
Set parameter values	
Query for data by name	
Subscribe	
Broadcast	
Multi-cast	
Data discovery	
Use of data sets	
Query to find location of data	
Query to determine what data is available (discovery)	
Execute application	Enables or Plays a defining role
Establish and end association	Enables or Plays a defining role
Logging	
Journaling	
Remote restart	
Remote reconfiguration	Enables or Plays a defining role
Remote diagnosis	Enables or Plays a defining role
RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)	

Commonly used techniques for meeting quality of service requirements of this data exchange	
Failure detection	Enables or Plays a defining role
Automatic restart	Enables or Plays a defining role
Automatic failover to second source of data or function	Enables or Plays a defining role
Automatic failover of communication channels to secondary channel	Enables or Plays a defining role
Backup of data	
Transaction rollback	
QoS monitoring	Enables or Plays a defining role
Alarming on QoS failure	Enables or Plays a defining role
None	
Not needed or not relevant	
Other _____	
Other _____	
RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)	

Management of large volumes of data that are being exchanged	
Major part of step involves handling large volumes of data	Enables or Plays a defining role
Some part of step involves handling large volumes of data	Enables or Plays a defining role
No part of step involves handling large volumes of data	
RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)	

Data consistency and synchronization management across systems	
Second-by-second synchronization Data being exchanged must be kept consistent and synchronized with other systems within seconds	Enables or Plays a defining role
Minute-by-minute synchronization Data being exchanged must be kept consistent and synchronized with other systems within minutes	
Day-by-day synchronization Data being exchanged must be kept consistent and synchronized with other systems within hours or days	
No synchronization Data being exchanged does not need to be kept consistent or synchronized with other systems	
RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)	

Management of timely access to data by multiple different users	
Contractual/required time windows for multiple access are less than one second	Enables or Plays a defining role
Contractual/required time windows for multiple access are within seconds	Enables or Plays a defining role
Contractual/required time windows for multiple access are within tens of seconds	
Contractual/required time windows for multiple access are within minutes	
Timely access by multiple users is not relevant	
RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)	

4.3.1.74 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:

4.3.1.75   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:

4.3.1.76   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:

4.4 Other Security Technologies

4.4.1.1 IEEE Documents on Security Technologies

4.4.1.1.1 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:

4.4.1.1.2 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

4.4.1.1.3 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.

4.4.1.2 RSA Documents on Security Technologies

4.4.1.2.1 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:

4.4.1.2.2 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:

4.4.1.3 OASIS Documents on Security Technologies

4.4.1.3.1   OASIS Security for Grid Services

URL: http://www.globus.org/Security/GSI3/GT3-Security-HPDC.pdf

Provides policy directives for distributed computing environments.

Keywords:

4.4.1.3.2   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:

4.4.1.3.3   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:

4.4.1.3.4 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:

4.4.1.3.5   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:

4.4.1.3.6 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:

4.4.1.3.7 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:

4.4.1.3.8 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:

4.4.1.3.9 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:

4.4.1.4 World Wide Web Consortium (W3C) Documents on Security Technologies

4.4.1.4.1 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:

Architectural Issues

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	Enables or Plays a defining role
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
WC3 XML Key Management Specification (XKMS 2.0) Bindings	

4.4.1.4.2 W3C The Platform for Privacy Preferences 1.1 (P3P1.1) SpecificationW3C 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:

4.4.1.5 Miscellaneous Security Technologies

4.4.1.5.1 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

4.4.1.5.2 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

4.4.1.5.3 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:

4.4.1.5.4 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:

4.4.1.5.5 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:

Architectural Issues

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention	Enables or Plays a defining

solutions could impact the required performance	role
Addition of security violation prevention solutions could be too costly	Enables or Plays a defining role
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	
No standard solutions are available	
Addition of security solutions is not feasible	
NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4	

4.4.1.5.6 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:

4.4.1.5.7 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:

4.4.1.5.8 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:

4.4.1.5.9 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:

4.4.1.5.10   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:

4.4.1.5.11   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:

4.4.1.5.12   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:

4.4.1.5.13   WPA WI-FI Protected Access

See IEEE 802.11b

4.4.1.5.14   WPA2 WI-FI Protected Access Version 2

See IEEE 802.11i

4.4.1.5.15   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:

Architectural Issues

Location of information producer (source of data)	
Operations center	
Corporate building	
Building	
Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	
TMN PKI - Digital certificates and certificate revocation lists profiles	

Location of information receiver (user of data)	
Operations center	
Corporate building	
Building	
Substation	
Field outside substation	
Customer site	
Another corporation	Enables or Plays a defining role
Mobile	
Changes frequently	
TMN PKI - Digital certificates and certificate revocation lists profiles	

Security Prevention Issues, Concerns, and Problems	
Addition of security violation prevention solutions could impact the required performance	
Addition of security violation prevention solutions could be too costly	
Addition of security violation prevention solutions could be too difficult or burdensome for users	
Data exchanges go across organizational boundaries, making security difficult	Enables or Plays a defining role

No standard solutions are available	
Addition of security solutions is not feasible	
TMN PKI - Digital certificates and certificate revocation lists profiles	