TMOC-2005-007

Feb 3, 2005

TMOC

Telecom Management and Operations Committee
(Formerly T1M1 OAM&P Committee)

A Technical Committee of

ATIS

Alliance for Telecommunications Industry Solutions
www.atis.org

Accredited by the
American National Standards Institute

Michael J. Fargano
Chairman

Ronald C. Roman
Vice Chairman

Subject: Pre Letter Ballot Review:
Security Management System (TMOC Issue 56)

Fellow Industry Leaders:

The purpose of this correspondence is to inform you that the TMOC (Telecom Management and Operations Committee, Formerly T1M1 OAM&P Committee) has entered the pre Letter Ballot review phase for TMOC Issue 56, *Security Management System* Standard. This is a follow up notice to the TMOC correspondence entitled *Announcement of New Standards Work: Security Management System (TMOC Issue 56)*, document number T1M1/2003-207, transmitted on Aug 19, 2004.

The latest baseline document is attached for your review. Comments would be greatly appreciated before March 24, 2005. Please send your comments directly to me. The following people have been assigned as personal liaisons from TMOC to ITU-T (SG4) and to IETF (O&M Area) for this topic: Lakshmi Raman (lakshmi.raman@radisys.com) and Kam Lam (hklam@lucent.com) to ITU-T, and Chris Lonvick (clonvick@cisco.com) and Joe Salowey (jsalowey@cisco.com) to IETF. In ITU-T and IETF, please work with them as needed for clarifications and information sharing.

We look forward to your input on this important security topic. Please contact me if you have any comments, questions, or concerns.

Best regards,

Mike Fargano
TMOC Chairman

Michael J. Fargano
Qwest Communications International
26th Floor
1801 California St.
Denver, CO 80202-1984

303 896 3618 (T)
303-896-7040 (F)

email: Michael.Fargano@Qwest.com

To:
Pecha, Pascale; TISPAN WG 8 chair; ppecha@telcordia.com
Mak, Leen; TISPAN WG 8 vice chair; lmak@lucent.com
Schmidt, Jörg; 3GPP2 TSG-S WG5 chair; J.Schmidt@Motorola.com
Tse, Edwin; 3GPP2 TSG-S WG5; lmcedts@LMC.ERICSSON.SE
Wijnen, Bert; IETF O&M Area Co-Director; bwijnen@lucent.com
Ross Callon; IETF OPSEC working group Co-Chair; rcallon@juniper.net
Patrick Cain; IETF OPSEC working group Co-Chair; pcain@acmehacking.com
Lam, Kam; Q 14/15 Rapporteur; hklam@lucent.com
Richardson, Tony; TeleManagement Forum Liaison Director; sts@anglianet.co.uk
Creaner, Martin; TeleManagement Forum CTO; mcreaner@tmforum.org
Flemisch, Felix; TeleManagement Forum; felix.flemisch@siemens.com
Truss, Michael; 3GPP SA5 chair; Michael.Truss@motorola.com
Sidor, Dave; ITU-T SG 4 chair; djsidor@nortelnetworks.com
Caryer, Geoff ; ITU-T WP 2/4 chair; geoff@caryer.co.uk
Chisholm, Sharon; ITU-T Q 10/4 rapporteur; schishol@nortelnetworks.com

Young, Gavin; DLS Forum Technical Committee Chair;
gyoung@dslforum.org
Blum, Cheryl; TR45 Chair; cjblum@lucent.com
Jones, Jim; OIF Technical Committee Chair;
Jim.D.Jones@alcatel.com
Cherukuri, Rao; MPLS Forum Technical Committee Chair;
rcheruku@cisco.com
Klessig, Bob; Co-Chair of the MEF Technical Committee
bklessig@cisco.com

Cc:
Ron Roman, TMOC Vice Chair
Lakshmi Raman, TMOC-AIP Chair
Kam Lam, TMOC-AIP Vice Chair
Chris Lonvick TMOC Liaison
Joe Salowey TMOC Liaison
Nick Andre, NCS/USSGB
Nicole Butler, ATIS/Secretariat
Catrina Akers, ATIS/Secretariat
Steve Barclay, ATIS/Secretariat
Jean-Paul Emard, ATIS/Secretariat

Guidelines and Requirements for Network Security Management

DRAFT

Version .1

DRAFT

TMOC-AIP 2005-005r3 formerly T1M1.5/2003-112R4

January 2005

Authors/Contributors

Stuart Jacobs, CISSP CISM	Verizon Corporation
James Turner	ATIS
<FILL IN DETAILS>	

Contents

1 SCOPE

This document describes the security infrastructure architectural framework and the functional requirements of a security management system to meet the objective of the telecommunication service providers.

The Security Management System (SMS) is a risk management tool that offers a central view of a Telecommunications Service Provider's (TSP's) infrastructure security state. The TSP's infrastructure spans:

- Application servers (i.e., servers for mail, messaging, database, web, file, VoIP and other applications)
- Support servers (i.e., DNS, DHCP, NTP, backup and other infrastructure support services)

- internetworking components (i.e., multiplexers, switches, routers, transport gateways, application gateways, gateway controllers, packet-filters a.k.a. firewalls, content filters, access points, bridges, and monitoring probes for QoS and network activity to name a few)
- end user host systems (i.e. lap-top systems, desk-top systems, workstations, printers, etc.)
- management systems (i.e. element management, network management, service management and business management systems)

all of which are collectively referred to in this document as managed elements from a security management perspective.

2 References

ANSI Documents:

T1.276-2003	American National Standard T1-276-2003, "American National standard for Telecommunications - Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane", T1M1.5 Working Group, July 2003

Internet Engineering Task Force Documents:

RFC-0768	"User Datagram Protocol", STD 6, Postel, J., August 1980
RFC-0791	"Internet protocol", STD 5, Postel, J., September 1981
RFC-0792	"Internet Control Message Protocol", J. Postel, September 1981.
RFC-0793	"TRANSMISSION CONTROL PROTOCOL", STD 7, Postel, J., September 1981
RFC-0826	"Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", D. C. Plummer, November 1982.
RFC-0854	"Telnet Protocol Specification”, J. Postel, J. K. Reynolds, May 1983
RFC-0959	"File Transfer Protocol”, J. Postel, J. K. Reynolds, October 1985
RFC-1157	"Simple Network Management Protocol (SNMP)”, J. D. Case, M. Fedor, M. L. Schoffstall, C. Davin, May 1990
RFC-1288	"The Finger User Information Protocol", D. Zimmerman, December 1991
RFC-1321	"The MD5 Message -Digest Algorithm”, Rivest, R., April 1992
RFC-1350	"The TFTP Protocol (Revision 2), K. Sollins, July1992.
RFC-1905	"Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2), SNMPv2 Working Group”, J.Case, K. McCloghrie, M. Rose, S. Waldbusser, January 1996
RFC-2104	"HMAC: Keyed-Hashing for Message Authentication", Krawczyk, H., Bellare, M. and R. Canetti, February 1997
RFC-2246	“The TLS Protocol” , Dierks, T., and C. Allen, Internet Engineering Task Force, January 1999.
RFC-2271	“An Architecture for Describing SNMP Management Frameworks” , Harrington, D., R. Presuhn, and B., Wijnen, Internet Engineering Task Force, January 1998.
RFC-2272	“Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)” , Case, J., D. Harrington, R. Presuhn, and B. Wijnen, Internet Engineering Task Force, January 1998.
RFC-2273	“SNMPv3 Applications” , Levi, D., P. Meyer, and B. Stewart, Internet Engineering Task Force, January 1998.
RFC-2274	“User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)” , Wijnen, B., and U. Blumenthal, Internet Engineering Task Force, January 1998.
RFC-2275	“View-based Access Control Model (VACM) for the Simple Network

	Management Protocol (SNMP)” , Wijnen, B., R. Presuhn, and K. McCloghrie, Internet Engineering Task Force, January 1998.
RFC-2328	"Open Shortest Path First version 2 protocol"
RFC-2385	"Border Gateway Protocol version 4"
RFC-2401	"Security Architecture for the Internet Protocol", S. Kent, R. Atkinson, November 1998.
RFC-2402	"IP Authentication Header", S. Kent, R. Atkinson, November 1998.
RFC-2406	"IP Encapsulating Security Payload (ESP)", S. Kent, R. Atkinson, November 1998.
RFC-2408	“Internet Security Association and Key Management Protocol (ISAKMP)”, D. Maughan, M. Schertler, M. Schneider, J. Turner, November 1998
RFC-2409	"The Internet Key Exchange (IKE) ", D. Harkins, D. Carrel, November 1998.
RFC-2410	"The NULL Encryption Algorithm and Its Use With IPsec", Standards Track, Glenn, r., Kent, s., November 1998
RFC-2616	"Hypertext Transfer Protocol -- HTTP/1.1", R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, June 1999.
RFC-2817	“Upgrading to TLS within HTTP/1.1” , Khare, R., and S. Lawrence, Internet Engineering Task Force, May 2000.
RFC-2818	“HTTP over TLS” , Rescorla, E., Internet Engineering Task Force, May 2000.
RFC-2865	“Remote Authentication Dial In User Service (RADIUS)” , Rigney, C., S. Willens, A. Rubens, S. Willens, and W. Simpson, Internet Engineering Task Force, June 2000.
RFC-3036	"Constrained Lable Distribution Protocol" (CR-LDP)

Object Management Group Documents:

CORBAsecurity	“Security Service Specification”, Version 1.7, March 2001, Object Management Group, Inc. (OMG), http://www.omg.org
CESG-1-1.2	CESG Memorandum No.1, Issue 1.2, "Glossary of Security Terminology", October 1992 CORBAsecurity “Security Service Specification”, Version 1.7, March 2001, Object Management Group, Inc. (OMG), http://www.omg.org

US Government Documents:

DES	Data Encryption Standard, National Institute of Standards and Technology. Federal Information Processing Standard (FIPS) Publication 46-1. Supersedes FIPS Publication 46, (January, 1977; reaffirmed January, 1988).
POSIX.0/D15	POSIX.0/D15 Jun 1992
POSIX.6/D13	POSIX.6/D13 Nov 1992
SHA-1	Secure Hash Algorithm. NIST FIPS 180-1, (April, 1995) http://csrc.nist.gov/fips/fip180-1.txt (ASCII) http://csrc.nist.gov/fips/fip180-1.ps (Postscript)
TCSEC	DOD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, December 1985.

ITU/CCITT Documents:

M.3016	Telecommunications management network Security Overview
X.500-X.521	International Telegraph and Telephone Consultative Committee

	(CCITT), 1992, Recommendations X.500-X.521 Data Communications Networks, Directory.
X.805	Security Architecture for Systems Providing End to End Communications

ISO Document:

ISO/IEC 7498-1	International Organization for Standardization (ISO), 1994a, Information Technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model, ISO/IEC-7498-1.
ISO/IEC 7498-2	International Organization for Standardization (ISO), 1989a, Information Processing Systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture, ISO-7498-2.
ISO/IEC 7498-4	International Organization for Standardization (ISO), 1989b, Information Processing Systems -- Open Systems Interconnection -- Basic Reference Model -- Part 4: Management Framework, ISO-7498-4.
ISO/IEC 9798-1	ISO/IEC 9798-1; Information Technology-Security techniques-Entity authentication-Part 1: General model; 1996.
ISO/IEC-DIS 10181-1	International Organization for Standardization (ISO), 1995c, Information Technology -- Open Systems Interconnection - Security Frameworks for Open Systems - Part 1: Overview, ISO/IEC-DIS 10181-1.
ISO/IEC 10181-3	International Organization for Standardization (ISO), 1995d, Information Technology -- Open Systems Interconnection - Security Frameworks for Open Systems - Part 3: Access Control , ISO/IEC-10181-3.

ATM Forum Documents:

RTD-SECURITY-01.00	ATM Forum Technical Committee, ATM Forum RTD-SECURITY-01.00; “Requirements for phase I Security Specification”; December, 1996.
str-sec-01.00	ATM Forum Technical Committee, str-sec-01.00 ATM Security Specification 1.0; December, 1997.
ATMF/02-0179	Methods for Securely Managing ATM NE, Implementation Agreement Version 1.0, AF-SEC-0179.000 ATM Forum Technical Committee, April 2002
ATMF/97-0067	ATM Forum/97-0067; “Proposed work on management capabilities for ATM security”; February, 1997.

Miscellaneous Documents:

draft302	Freier, A.O., P. Carlton, and P.C. Kocher, “The SSL Protocol Version 3.0,” http://home.netscape.com/eng/ssl3/draft302.txt, November 1996.
ECMA TR/46	ECMA Technical Report TR/46, "Security in Open Systems - A Security Framework", July 1988
ECMA-219	ECMA-219, "Authentication and Privilege Attribute Security Application with related key distribution functions", 2nd edition, March 1996
H.248/Megaco	RFC-3015 The H.248/Megaco protocol

ITSEC-1.2	ITSEC Ver 1.2 1991
KERBEROS	“Kerberos Authentication and Authorization System”, S.P. Miller, B.C. Neuman, J.I. Schiller, J.H. Saltzer; MIT Project Athena Documentation Section E.2.1, December 1987
RFC2119	"Key words for use in RFCs to indicate requirement levels", Bradner, S., BCP 14, March 1997.
RFC-2459	Housley, R., W. Ford, W. Polk, and D. Solo, “Internet Public Key Infrastructure: Part I: X.509 Certificate and CRL Profile,” RFC 2459, Internet Engineering Task Force, January 1999.
RFC-2487	“SMTP Service Extension for Secure SMTP over TLS”, P. Hoffman, January 1999
RSA78	Rivest, R., Shamir, A., Adleman, L., ``A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 21(2):120-126, February 1978.
SS7	Signaling System 7 (SS7)
ssh1-draft	Ylönen, T., “The SSH (Secure Shell) Remote Login Protocol,” http://www.tigerlair.com/ssh/faq/ssh1-draft.txt, November 1995.
SSH96	Ylönen, T., “SSH—Secure Login Connections over the Internet,” Proceedings of the Sixth USENIX Security Symposium, July 1996, pp. 37–42
ssh-faq	Carasik, A., “Secure Shell FAQ,” Revision 1.4, http://www.tigerlair.com/ssh/faq, February 2001.

3 Glossary of Acronyms Table 1 - Glossary

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ADF	Access Control Decision Function
Advanced Encryption Algorithm (AES)	A new symmetric data encryption standard developed under the auspices of the United States Government as a replacement for DES. AES uses a variable length key to perform a series of nonlinear transformation on a 64 bit data block.
AEF	Access Control Enforcement Function
AH	IP Authentication Header, as defined by RFC-2402
AM	Accounting Management
AP	Application Provider
API	Application Protocol Interface
ARP	Address Resolution Protocol, as defined by RFC-0826
BGPv4	Border Gateway Protocol, as defined by RFC-2385
CALEA	Communications Assistance to Law Enforcement Agencies
CBC	Cipher Block Chaining
CCITT	International Telegraph and Telephone Consultative Committee
CLI	Command Line Interface
CM	Configuration Management
CO	Central Office
CORBA	Common Object Request Broker Architecture
CORBA security	CORBA Security Services as defined by OGM
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CR-LDP	Constrained Label Distribution Protocol as defined by RFC-3036
DES	Data Encryption Standard as defined in FIPS Publication 46-1
DH	Diffie-Hellman, as defined by
DHCP	Dynamic Host Configuration Protocol, as defined by
DNS	Domain Name Service, as defined by
DoS	Denial of Service
EMS	Element Management System
ESP	IP Encapsulating Security Payload as defined in RFC-2406

ESP-null	The NULL Encryption Algorithm and Its Use With IPsec, as defined by RFC-2410
finger	The Finger User Information Protocol as defined by RC-1288
FM	Fault Management
FTP or ftp	File Transfer Protocol and application, as defined by RFC-0959
GUI	Graphical User Interface
HTTP or http	Hyper Text Transfer Protocol, as defined by RFC-2616
ICMP	Internet Control Message Protocol, as defined by RFC-0792
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange, as defined by RFC-2409
IP	Internet Protocol, as defined by RFC-0791
IPSec	IP Security Architecture, as defined by RFC-2401
ISDN	Integrated Services Digital Network
ISAKMP	Internet Security Association and Key Management Protocol, as defined by RFC-2408
ISO	International Organization for Standardization
ISUP	ISDN Users Part (SS7)
KDC	Key Management and Distribution Center
KMS	Key Management System
LAN	Local Area Network
LATA	Local Access and Transport Area
MAC	Message Authentication Code
MAC	Media Access Control
MAN	Metropolitan Area Network
MAP	Management Application Process
MIB	Management Information Base
HMAC	Keyed-Hashing for Message Authentication, as defined by RFC-2104
SMIB	Security Management Information Base
MNE	Managed Network Element
MD5	MD5 Message-Digest Algorithm, as defined by RFC-1321
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair
NA	Not Applicable
NAT	Network Address Translation, as defined by

NE	Network Element
NFS	Network File System, as defined by
NGN	Next Generation Network
NMS	Network Management System
NOC	Network Operations Center
OA&M	Operation, Administration, & Maintenance
OAM&P	Operations, Administration, Maintenance and Provisioning
OEM	Original Equipment Manufacturer
OSI	Open Systems Interconnection
OSPFv2	Open Shortest Path First, as defined by RFC-2328
OSS	Operation Support System
PC	Personal Computer
PM	Performance Management
PNG	Pseudo-random Number Generation
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service, as defined by RFC-2865
RFC	Request for Comments
RFP	Request for Proposal
RIP	Route Information Protocol, as defined by
RMON2	Remote Monitoring, as defined by
RSA	RSA is the public key (asymmetric) encryption method used in PGP and most Public Key Infrastructure systems. R, S and A are the initials of the developers of the algorithm (Rivest, Shamir and Adleman). The basic security in RSA comes from the fact that, while it is relatively easy to multiply two huge prime numbers together to obtain their product, it is computationally difficult to go the reverse direction: to find the two prime factors of a given composite number. It is this one-way nature of RSA that allows an encryption key to be generated and disclosed to the world, and yet not allow a message to be decrypted. [RFC-1321]
SHA-1	Secure Hash Algorithm, as defined by FIPS 180-1
SM	Security Management (SM)
SMAP	Security Management Application Process
SNMP(v1)(v2)(v3)	Simple Network Management Protocol, as defined by RFCs 1157, 1905, 2271, 2272, 2273, 2274, 2275
SOC	Secvurity Operations Center
SQL	Structure Query Language

SS7	Signaling System 7
SSH	Secure Shell, as defined by
SSL	Secure Sockets Layer, as defined by
TCP	Transmission Control Protocol, as defined by RFC-0793
Telnet	Remote login session control protocol and application, as defined by RFCs 0854 and 0859
tftp	Trivial File Transfer Protocol, as defined by RFC-1350
TL1	Translation Language 1
TLS	Transport Layer Security, as defined by RFCs 2246, 2817 and 2818
TMN	Telecommunications Management Network
TSP	Telecommunications Services Provider
UDP	User Datagram Protocol, as defined by RFC-0768
user identifier (User ID)	Unique symbol or character string that is used by an IT product to uniquely identify a specific user.
uucp	Unix-unix communications protocol and application, as defined by
VPN	Virtual Private Network
WWW	World Wide Web
XML	Extensible Markup Language, as defined by

4 Security Management System Concepts

The Security Management System described in this document is primarily a manager of security concepts intended to mechanize the application of various security and security management tools. Because it in essence supports these tools, it is considered an Operations Support System for Security Management. Thus the title Security Management Operational Support System (SM-OSS).

The SM-OSS supports these tools by providing supporting services that contribute to the protection of information and resources in TSP networks and systems in accordance with applicable trust domain (virtual networks) and their information system (repository) security policies.

A Trust Domain is the set of components that maintain a particular set of information and associated resources. It consists of Users, Networks, Data Repositories, and Applications that manipulate the data in those Data Repositories. Different Trust Domains may share the same physical components. Also a single Trust Domain may promote various levels of trust depending on the users need to know and the sensitivity of the information and associated resources.

Security management is a particular instance of information system management. Managed objects are information system resources that may be managed. Management information is information associated with a managed object that is operated upon to manage that object.

An object is an instance of a Trust Domain. An object may contain information in transit (such as a network) or information at rest (such as a database)

A human administrator employs a Security Management Application Process (SMAP) to use and maintain management information contained in a logical repository called a Security Management

Information Base (SMIB). The contents of a single logical SMIB may exist in several end systems [referred to in this document as Managed Network Elements (MNEs)] as well as the networks that connect them and their users. . To ensure efficient and flexible system management, it is generally required that administrators have local or remote access to SMIBs.

MNEs that support multiple trust domains must provide the ability to manage each trust domain independently. In addition, the use of security services and security mechanisms shared among multiple trust domains requires security management coordination at the MNE level. Thus, an MNE security policy is necessary to specify how the shared use of security functions and resources among trust domains is accomplished. This MNE policy also must be managed.

A typical trust domain security policy might include some or all of the types of information listed below in the bullet items. Security management of MNEs is concerned with the installation, maintenance, and enforcement of the security policy rules and the information about users, security services, and security mechanisms needed to achieve the security policy. Not all security management activities are performed in MNEs. There are always supporting security management activities that are related to administrative and environmental security mechanisms or which are prerequisite to the use of MNE security management functions (e.g., issuance of credentials to users, scheduling human activities, auditing, or carrying out routine maintenance). These supporting activities must be understood to be an integral part of security management. Examples of trust domain security policy elements include:

- A description of the service area functions that the trust domain supports
- A description of the information objects and their attributes, including rules pertaining to creation and use of multi-domain information objects
- Membership criteria
- Rules for inter-domain transfers, if any
- Rules for intra-domain transfers, if any
- Security service requirements (including strength of service) appropriate to meet the risks determined by a threat analysis. Security services should be allocated to MNEs
- Criteria for acceptable security mechanisms to implement the required security services
- Security management-specific requirements
- Relationship of the security management trust domain to each trust domain
- Criteria for security administrators
- Roles, privileges, and duties of security administrators
- Identities of security administrators
- Configuration management requirements for the establishment or modification of trust domain security policy rules
- Identification of one or more members of the trust domain who are responsible for approving MNEs that will be deployed within the trust domain.

The security policy for an MNE that supports multiple trust domains must specify the management rules for conducting the following activities:

- Providing strict isolation among trust domains
- Invoking and managing security mechanisms that implement the security services required by the security policies of the individual trust domains
- Developing rules for the management of multi-domain information objects, including criteria for user access, display labeling, and transfers within and among MNEs
- Controlling and maintaining security management mechanisms and information objects that enable a security manager of a particular trust domain to control that trust domain independently of others.

The security policy rules for both MNE security management and trust domain security management are part of their SMIBs. For a trust domain that is supported in more than one MNE, the security administrator may have physical access to only some of those MNEs. Thus, the SMAP that operates on the portion of a SMIB in a particular MNE must be accessible to the security administrator both locally and remotely. A SMAP is like any other application in that it operates in a security context which represents a security administrator (or process) operating in a particular security management trust domain. Thus, it is subject to the same strict separation mechanisms as other trust domains.

4.1 Security Management Concepts Relationship to *ISO 7498-2*

Clause 8 of ISO 7498-2 addresses many aspects of security management for open systems interconnection. The ISO 7498-2 security management structure is adopted as the basis for the infrastructure security architecture and is extended to apply to all aspects of open systems security management. Security domains and security policy are introduced in ISO 7498-2. Other topics covered at the concept level include security management information repository, communications security and security management functions. Using this as the basis the security management system architecture is defined in this document to address these topics. Even though the details such as the management information base definition are not part of this document, the architecture is defined with the need to support these elements required for interoperability and assure secure management of TSP network infrastructure.

4.2 Security Management Concepts Relationship to X.805

ITU-T Recommendation X.805 defines the security architecture to achieve an end-to-end security. In addition to the architectural concepts, eight security dimensions are defined to address the network security. Two architectural concepts are defined to explain the architecture. These are security layers and security planes. The former supports a hierarchical separation of capabilities required to meet end-to-end security. The security layers are infrastructure, services and application. The layering lends itself to reuse of countermeasures to overcome vulnerabilities at lower layers by the higher layers. For example many applications can use the same measures at the infrastructure layer. Examples of components belonging to infrastructure layer are routers, switches and servers. The services layers addresses network security such as basic connectivity to instant messaging. Applications such as email, distance learning etc, that are network based are considered in application layer. The planes are divided into management plane, control plane and user plane. The eight dimensions, namely access control, authentication, non-repudiation, data confidentiality, communications security, data integrity, availability, and privacy, are applicable to all the three layers. The architectural model and functional capabilities for security management system described in this document expands on the generic security framework emphasizing on the management plane. While X.805 concentrated on communications aspects in the infrastructure, as management system requirement, this document includes security requirements for operating environments, software configuration etc. Thus this document focuses on system level requirements to achieve management of the network management within the overall framework of X.805.

4.3 Security Management Concepts Relationship to T1-276-2003

T1.276 addresses the requirements, services and mechanisms in support of securing the management plane of the Telecommunications infrastructure. In this context T1.276 is focused on end to end security both in the case where management traffic is separate from user traffic and when they are mixed together. The reference model for deriving the requirements in T1.276 shows the interfaces where management traffic is to be secured. Given these end to end security requirements, this document focuses on requirements of a management system that offers the tools necessary to secure the service providers infrastructure. The management plane traffic addressed in T1.276 is a subset of the infrastructure to be secured by the requirements in this document. The reference model in T1.276 is further expanded to include other elements that are not specific to management plane such as the application servers etc. There are similarities in the functions to be supported in both documents. However, T1.276 relates to the interfaces between the network elements and OSSs and this document addresses functions to be supported by systems that oversee all the infrastructure components.

5 Telcom Network Architecture Overview

At the highest level of abstraction, a TSP's system infrastructure has four major functional areas:

- **Transport**; which includes:
  - transport bearer traffic related protocols (how information is transferred) over communications links of various types
  - the control, signaling and routing protocols necessary for correct operation of the transport bearer traffic related protocols
  - the network (intermediate) nodes responsible for information transfer.
- **Application**; which includes:
  - application bearer traffic related protocols (how application specific information is transferred) between application server (end) nodes and client (end) nodes
  - the control and signaling protocols necessary for correct operation of the application bearer traffic related protocols
  - the application server (end) nodes and client (end) nodes involved in the servicing and consumption of application services.
- **Management**; which includes:
  - management bearer traffic related protocols (how management information is transferred) between management server (end) nodes, client (end) nodes and managed element nodes.
  - the control, signaling and routing protocols necessary for correct operation of the management bearer traffic related protocols
  - the application server (end) nodes and client (end) nodes involved in the management of managed element nodes.
- **Execution Environment**; which includes:
  - Operating Systems of management server (end) nodes, client (end) nodes and managed element nodes.
  - File systems of management server (end) nodes, client (end) nodes and managed element nodes.
  - The hardware components of management server (end) nodes, client (end) nodes and managed element nodes.

There are many architecture models that group these functional areas and sub-areas differently. Some of these alternative models reflect implementation or deployment perspectives. Other models reflect specific technology perspectives. The above model, with 4 functional planes, focuses on providing a framework that is independent of any specific technology or implementation perspective. Using a different architectural model, one would likely combine the control, signaling and routing protocols of the Transport plane with the control and signaling protocols of the Application plane into a Control, Signaling and Routing Plane. However this approach makes discussing functions such as media gateway control and "SIP firewall pin-hole" management more difficult that the four plane model above.

5.1 Security Infrastructure Architectural Framework

A "top down" consideration of security starts with identifying objectives, then proceeds to examination of threats, which lead to establishing a set of high level security requirements that the security services within a network need to satisfy. These threats and high level security requirements are then mapped against the control and management planes within the infrastructure.

5.1.1 Architectural Considerations

Security assessment of the TSP infrastructure is done by analyzing managed element configurations and events from managed elements. These events can already be security alarms – especially in the case of security oriented managed elements like firewalls – or can be casual events that may be further analyzed to detect abnormal behaviors that can only be identified by correlating information from different sources. From the assessment of TSP infrastructure security state, the SMS should be able to propose mitigation actions and may apply them automatically.

The SMS has to fulfill the security requirements of a usual Network/System Monitoring System as described in T1.276-2003 and are out of the scope of this section. It is assumed that all the data, on which security analysis and mitigation decisions are made, are transmitted in a trusted way.

Security Management spans the functions and information necessary to manage security-related services and functions throughout a TSP's infrastructure. Security Management provides supporting services that contribute to the protection of information and resources in open systems in accordance with applicable trust domain and information system security policies. An SMS will provide these services to managed elements within a TSP’s current and evolving communications/services network.

The SMS approach provides an evolutionary path from the current diverse, and typically stove-piped or siloed, security management mechanisms to a common target methodology. All information assets should be operated in accordance with a security policy. However, a variety of mechanisms and tools are typically implemented in support of the policy. In general the voice, data, and management networks are secured using different techniques with different organizations having primary responsibility for each of the domains.

- Data Network and Data Management Network(s): Securing these networks involves using suppliers’ products or public domain software. For example, TACAS may be used for authentication and authorization and the RADIUS protocol may be used for authentication and accounting. Access lists (for network elements) and SNMP Access Control Lists (ACLs) may be used for authentication. User accounts may be secured by both password control and SecureID tokens. Other product mechanisms may also be used to scan for security vulnerabilities. The SSH protocol may be used for application layer authentication, confidentiality, and data integrity.
- Core Voice / Switched Network and Management System: Access to the network elements on the core switched network is primarily controlled through third-party management system(s). The purpose of these systems is to protect all the network elements, that make up the TSP's Telephone Network, from unauthorized OAM&P access.

5.1.2 TSP Infrastructure Security Objectives

Herein are described the objectives of security mechanisms within a TSP services infrastructure. The focus of this effort is to describe what security mechanisms must achieve, not how they are implemented. These security objectives form the basis of the threat analysis in the next section. Security objectives are derived from more general objectives that have an impact on security. The objectives of the following groups need to be considered:

- Customers (service subscribers and users)
- The TSP
- Peer operators.

5.1.2.1 *Customer Objectives*

Customer objectives are not uniform since each customer has its own set of objectives. For example, an enterprise does not always have the same objectives as a private person. The following list gives examples of objectives that may have security implications:

- Availability and correct functionality of service subscription, activation and deactivation
- Availability and correct functionality of TSP services
- Correct and verifiable billing
- Data integrity and data confidentiality and or privacy, and
- Capability to use a service anonymously.

5.1.2.2 *TSP Objectives*

The goal of the TSP is to generate revenue by operating a TSP network and providing services to customers. This goal implies maximum revenue for supplying connectivity and services while minimizing expenditures due to unauthorized use of TSP resources. The following list gives examples of objectives for achieving this goal. These objectives may have security implications:

- Availability and correct functionality of the TSP network and services
- Availability and correct functionality of the TSP network and service management
- Correct and verifiable billing, with no possibility of fraud
- Non-repudiation for all used TSP network services and for all management activities
- Preservation of reputation (preservation of customers' and investors' trust)
- Accountability for all activities
- Data integrity, data confidentiality and privacy.

5.1.2.3 *Peer Operator Objectives*

The goal of peer network operators and service providers is to generate revenue by operating a TSP network. This goal implies maximum revenue for supplying network services while minimizing expenditures due to unauthorized use of network services. The following list gives examples of objectives for achieving this goal. These objectives may have security implications:

- Availability and correct functionality of TSP inter-network service interfaces
- Availability and correct functionality of the TSP inter-network management interfaces
- Correct and verifiable billing, with no possibility of fraud
- Non-repudiation for all used TSP network services and for all management activities between inter-connected networks
- Preservation of reputation (preservation of customers' and investors' trust)
- Accountability for all activities
- Data integrity, data confidentiality and privacy.

5.1.2.4 *Common Security Objectives*

The objectives listed above can be expressed by one or by a combination of the following fundamental security objectives:

Table 2 Fundamental Security Objectives

Confidentiality:	Confidentiality of stored and transferred information,
Data Integrity:	Protection of stored and transferred information,
Accountability:	Accountability for all TSP network service invocations and for all TSP network

	management activities; any entity should be responsible for any actions initiated
Availability:	All legitimate entities should experience correct access to TSP facilities.

5.1.3 Generic Threats

A threat is a potential violation of a security objective. Three types of threats may be distinguished:

- An accidental threat where the origin of the threat does not involve any malicious intent.
- An administrative threat where the threat arises from a lack of administration of security.
- Intentional threats where the threat involves a malicious entity that may attack either the communication itself or network resources.

Accidental and administrative threats may be taken into account as long as their consequences are the same as intentional threats. The following intentional threats should be considered in a threat analysis of a TSP network:

Table 3 Intentional Threats

Masquerade ("spoofing")	The pretense by an entity to be a different entity.
Eavesdropping	A breach of confidentiality by monitoring communication.
Unauthorized access	An entity attempts to access data in violation to the security policy in force.
Loss or corruption of information	Unauthorized deletion, insertion, modification, reordering, replay or delay compromises the integrity of data transferred.
Repudiation	An entity involved in a communication exchange subsequently denies the fact.
Forgery	An entity fabricates information and claims that such information was received from another entity or sent to another entity.
Denial of Service	An entity fails to perform its function or prevents other entities from performing their functions. May include denial of access to TSP services and denial of communication by flooding the TSP network or components. In a shared network, this threat can be recognized as a fabrication of extra traffic that floods the network, preventing others from using the network or delaying the traffic of others.

The following table maps the threats to the security objectives. An "X" in a field of this table denotes that the threat (e.g. "masquerade") endangers the respective security objective (e.g. "confidentiality").

Table 4 Main Security Objectives vs. Generic Threats

	Generic Threats						
Main Security Objectives	Masquerade	Eavesdropping	Unauthorized access	Loss or corruption of information	Repudiation	Forgery	Denial of Service
Confidentiality	X	X	X				
Data Integrity	X		X	X		X	
Accountability	X		X		X	X	
Availability	X		X	X			X

5.1.4 Security Infrastructure Requirements and Security Services

A set of principal functional security requirements can be identified to deal with the aforementioned threats. The functional requirements stated here are not prioritized. Priorities are derived from the individual assessments of the security threats and depend on the respective network scenario. As a rule of thumb, it can be stated that open network environments require the application of more stringent technical security mechanisms than required in closed network environments. In closed environments, a sufficient level of security may be achieved by organizational means.

The following table gives an overview of the principal functional security requirements to counteract the security threats. An "X" in a field of this table denotes that a specific threat (e.g. "masquerade") leads to this functional security requirement (e.g. "verification of identities"). Note that a single threat may lead to more than one principal functional security requirement.

Table 5 Mapping of threats and functional security requirements

	Principal Functional Security Requirements								
Threats	Verification of Identities	Controlled Access and Authorization	Protection of confidentiality	Protection of Data Integrity	Strong Accountability	Activity Logging	Alarm Reporting	Audit	Security Recovery / Management of Security [1]
Masquerade	X	X				X	X	X	X
Eaves-dropping		X	X						X
Unauthorized Access	X	X	X	X		X	X	X	X
Corruption or Loss of (transferred) Information				X			X		X

	Principal Functional Security Requirements								
Threats	Verification of Identities	Controlled Access and Authorization	Protection of confidentiality	Protection of Data Integrity	Strong Accountability	Activity Logging	Alarm Reporting	Audit	Security Recovery / Management of Security[1]
Repudiation					X	X		X	X
Forgery					X	X		X	X
Denial of Service		X				X	X	X	X

The following table provides an overview of the mapping between security requirements and the security services, which guarantee fulfillment of these requirements. For each security requirement the relevant security services are named. These security services are defined in the following sub-sections 3.1 through 3.8.

Table 6 Mapping of functional security requirements and security services

Functional Security Requirement		Security Service
Verification of Identities		User Authentication Peer Entity Authentication Data Origin Authentication
Controlled Access and Authorization		Access Control
Protection of Confidentiality	Stored Data	Access Control
	Transferred Data	Confidentiality
Protection of Data Integrity	Stored data	Access Control
	Transferred Data	Data Integrity
Strong Accountability		Non-repudiation
Activity Logging		Security Alarm, Audit Trail & Recovery
Alarm Reporting		Security Alarm, Audit Trail & Recovery
Audit		Security Alarm, Audit Trail & Recovery
Security Recovery / Management		–

The following subsections describe the functional security requirements and the corresponding security services. However, for a specific TSP network, the risk assessment for that network determines which of these functional requirements must be fulfilled, and which corresponding security services must be provided. The proposed generic security services are derived from [ISO 7498/2].

The next eight requirements are based on ITU-T recommendation M3016 – Telecommunications Network Management Security Overview.

5.1.4.1 *Verification of Identities*

SEC-1: The TSP Infrastructure SHALL support capabilities to establish and verify the claimed identity of any subject interacting with, or within, the TSP Infrastructure.

Verification of identities is a fundamental security requirement for the TSP Infrastructure. Its main purpose is to support other security services and to provide accountability for actions taken. The following security services should be made available to fulfill this requirement:

User Authentication	Delivers corroboration of the identity of the (human) user.
Peer Entity Authentication	Establishes proof of the identity of the peer entity at one particular moment in time during a communication relationship.
Data Origin Authentication	Establishes proof of identity of the peer entity responsible for a specific data unit.

5.1.4.2 *Controlled Access and Authorization*

SEC-2: The TSP Infrastructure SHALL support capabilities to ensure that subjects are prevented from gaining access to information or resources they are not authorized to access.

The security servic e to meet this requirement is shown in the following table:

Access Control	Provides a means to ensure that objects are accessed by subjects only in an authorized manner. Objects include the physical system, the system software, applications and data. The limitations of access to these objects are laid out in access control information, which specifies: • the means to determine which subjects are authorized to have access to an object • the types of access is allowed (reading, writing, modifying, creating or deleting).

Granting access to objects requires identity verification of the subject attempting to gain access. Usage of access control is always linked to the usage of an authentication service.

5.1.4.3 *Protection of Confidentiality*

SEC-3: The TSP Infrastructure SHALL support the capability to keep stored and communicated data confidential.

Protection of confidentiality is needed to protect the following:

- User related TSP Infrastructure information
- Information used by other security services, e.g. cryptographic keys.

The security services that support this requirement are:

Access Control (stored data)	See SEC-2.
Confidentiality (communicated data)	The confidentiality service provides protection against unauthorized disclosure of exchanged data. The following kinds of confidentiality services can be distinguished: • data confidentiality • connection confidentiality.

5.1.4.4 *Protection of Data Integrity*

SEC-4: The TSP Infrastructure SHALL maintain the integrity of stored and communicated data.

Protection of data integrity is needed to protect the following:

- TSP Infrastructure user related information
- Information used by other security services.

Security services to support this requirement can be divided as follows:

- Services for the integrity of stored data
- Services for the integrity of communicated data.

Access Control (stored data)	See SEC-2.
Data Integrity (communicated data)	The integrity service provides means to ensure the correctness of exchanged data, protecting against data modification, deletion, creation (insertion) and replay of exchanged data. The following kinds of integrity services are distinguished: • selective field integrity • connection integrity without recovery • connection integrity with recovery.

5.1.4.5 *Strong Accountability*

SEC-5: The TSP Infrastructure SHALL support the capability that a subject cannot deny the responsibility for any of its performed actions as well as their effects.

Strong accountability requires that any individual subject in a TSP Infrastructure must hold full responsibility for any of his/her/its actions. In other words, the subject may not repudiate its actions in the TSP Infrastructure. The security service to support this requirement is:

Non-repudiation	Provides means to prove that exchange of data actually took place. It comes in two forms:- non-repudiation - proof of origin, and - non-repudiation - proof of delivery.

5.1.4.6 *Activity Logging*

SEC-6: The TSP Infrastructure SHALL support the capability to retrieve information about security activities stored in the Infrastructure and Management Elements with the possibility of tracing this information to subjects.

This requirement is supported by the following security service:

Security Logging	Logs information about security relevant events that have occurred or security

	relevant operations that have been performed or attempted. Log retrieval provides the security administrator the ability to determine if: • any records were lost • the characteristics of the records stored in the log were modified at any time.

5.1.4.7 *Alarm Reporting*

SEC-7: The TSP Infrastructure SHALL support the capability to generate alarm notifications about certain adjustable and selective security related events.

This requirement is supported by the following security service:

Security Alarms	Provides information regarding operational condition and quality of service, pertaining to security.

5.1.4.8 *Audit*

SEC-8: The TSP Infrastructure SHALL support the capability to analyze and exploit logged data on security relevant events in order to check for violations of system and network security.

This requirement is supported by the following security service:

Security Audit Trail	Provides an independent review and examination of system information and activities. The information is used as follows: • to test for adequacy of system controls • to ensure compliance with the established security policy and operational procedures • to detect breaches in security • to recommend changes in control, policy and procedures.

5.1.4.9 *Management of Security*

SEC-9: The TSP Infrastructure SHALL support recovery from successful and attempted breaches on security.

When an attempt to breach security occurs, a controlled response is required. The attempt should not result in a severe degradation of TSP Infrastructure availability.

SEC-10: The TSP Infrastructure SHALL support capabilities to manage the security services derived from the security requirements listed above.

Security management comprises all activities required to establish, maintain and terminate the security aspects of a system. For example, security management includes the following:

- Management of security services
- Installation of security mechanisms
- Key management (management part)
- Establishment of:
  - Identities

- Keys
- Access control information
- Security policies, etc.

The last two requirements (SEC-9 and SEC-10) do not lead to security services. They are requirements on the specification of the security services and the necessary infrastructure (e.g., they act on key management or on management of security mechanisms and algorithms). However, these requirements must be fulfilled to guarantee the maintenance of security services. TSP management within the Element, Network, System and Business Management layers of the TMN model must support SEC-9 and SEC-10.

5.1.5 Architecture Model Security Service Mapping

A key part of developing the 10 basic security requirements was the identification of the security services responsible for fulfilling these requirements. Here we discuss where and how the security services, as logical functions, fit into the architecture functional model. Figure 1 depicts the security functional elements within the Management, Application and Transport planes. Also shown in figure 1 are the security functional elements that need to exist within the Element Operating Environment or every element of the TSP Next Generation Network (NGN) infrastructure. This includes all network connected elements irrespective of their role as:

- Intermediate nodes(i.e., routers, switches, add drop multiplexers, wave division multiplexers, fire walls, intrusion detection systems, line/trunk media gateways, signaling gateways, etc.)
- End nodes (i.e., management servers and workstations, general purpose desktop systems, call/media gateway controllers, conference bridges, web servers, VoIP Proxy servers, messaging servers, announcement servers, DNS servers, LDAP directories, VoIP phones, etc.)

Section 6.1 provides a number of examples of elements by functional area.

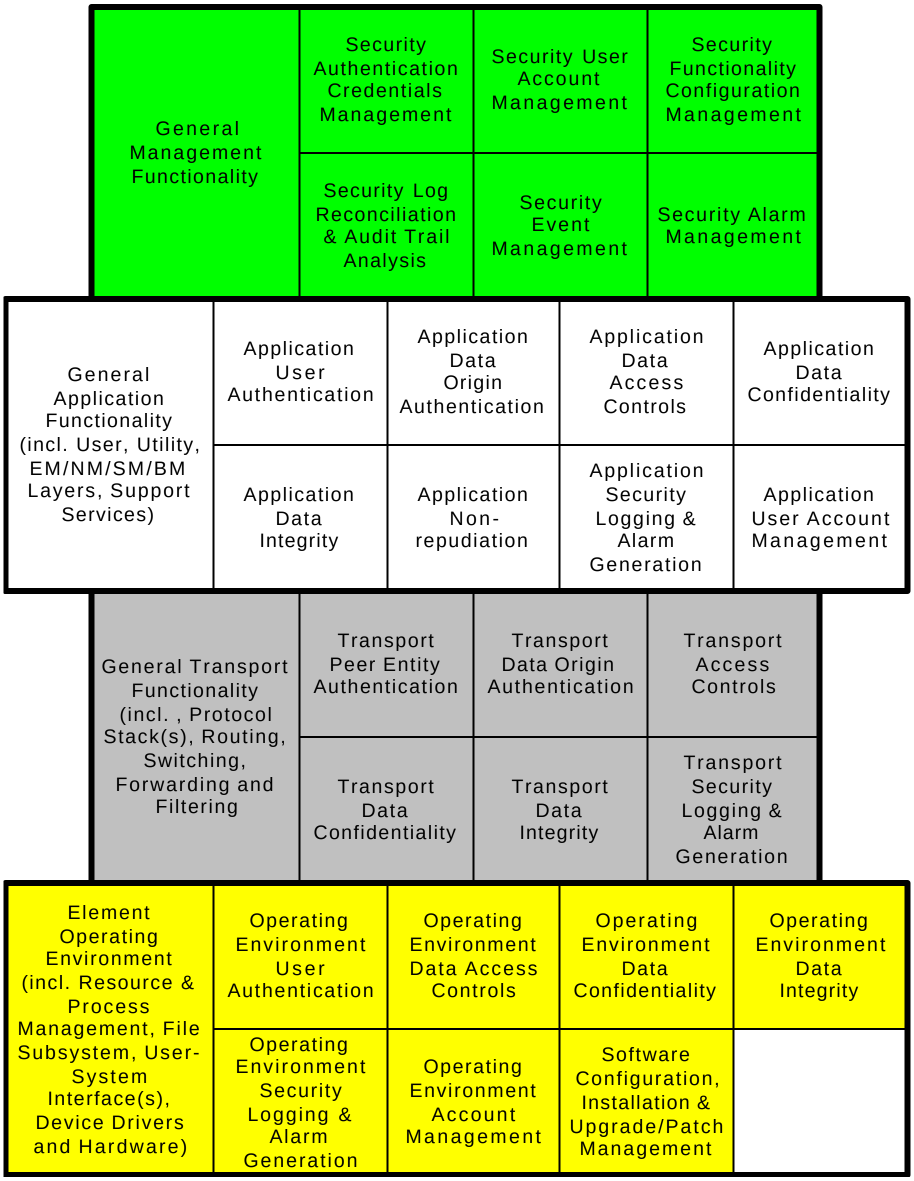

General Management Functionality
Security Authentication Credentials Management
Security User Account Management
Security Functionality Configuration Management
Security Log Reconciliation & Audit Trail Analysis
Security Event Management
Security Alarm Management
General Application Functionality (incl. User, Utility, EM/NM/SM/BM Layers, Support Services)
Application User Authentication
Application Data Origin Authentication
Application Data Access Controls
Application Data Confidentiality
Application Data Integrity
Application Non-repudiation
Application Security Logging & Alarm Generation
Application User Account Management
General Transport Functionality (incl. , Protocol Stack(s), Routing, Switching, Forwarding and Filtering
Transport Peer Entity Authentication
Transport Data Origin Authentication
Transport Access Controls
Transport Data Confidentiality
Transport Data Integrity
Transport Security Logging & Alarm Generation
Element Operating Environment (incl. Resource & Process Management, File Subsystem, User-System Interface(s), Device Drivers and Hardware)
Operating Environment User Authentication
Operating Environment Data Access Controls
Operating Environment Data Confidentiality
Operating Environment Data Integrity
Operating Environment Security Logging & Alarm Generation
Operating Environment Account Management
Software Configuration, Installation & Upgrade/Patch Management

Figure 1 Model Architecture Security Services (functions)

Some network elements use real-time embedded operating systems (OSs), non-modular application software and have no rotating storage capabilities. Other elements rely on general purpose OSs, easily loadable applications and gigabytes of rotating storage. Hence not all Element Operating Environments will include all the security functional elements identified in figure 1.

The remainder of this section examines the security services within each functional plane in greater detail, including both the interaction of security services of the functional plane with an element and between elements. The color-coding of figure 1 is continued in the following sections to remind the reader of where each security service resides in the three plane model.

5.1.6 Transport Plane Security Services

The Transport Plane Security Services are concerned with fulfilling the requirements of:

- Verification of Identities
- Data Origin Authentication
- Controlled Access and Authorization
- Protection of Confidentiality
- Protection of Data Integrity
- Activity Logging & Alarm Reporting

as these requirements apply to the general transport functionality of the element when communicating with other elements.

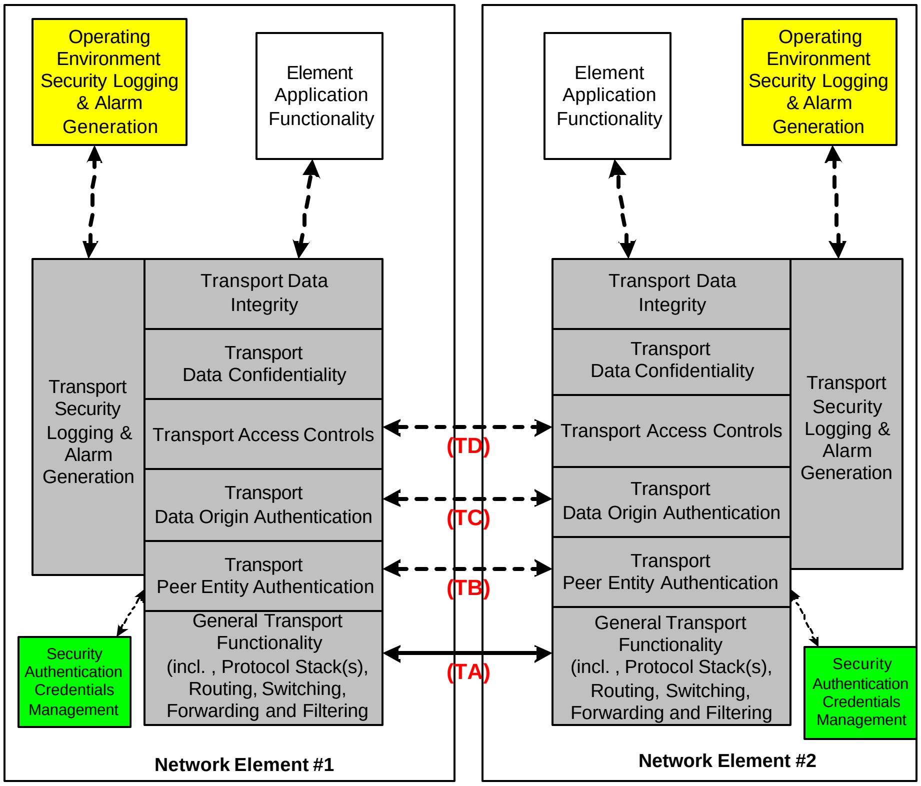

Operating Environment Security Logging & Alarm Generation
Element Application Functionality
Transport Security Logging & Alarm Generation
Transport Data Integrity
Transport Data Confidentiality
Transport Access Controls
Transport Data Origin Authentication
Transport Peer Entity Authentication
General Transport Functionality (incl. , Protocol Stack(s), Routing, Switching, Forwarding and Filtering
Security Authentication Credentials Management
Network Element #1
Element Application Functionality
Operating Environment Security Logging & Alarm Generation
Transport Data Integrity
Transport Data Confidentiality
Transport Access Controls
Transport Data Origin Authentication
Transport Peer Entity Authentication
General Transport Functionality (incl. , Protocol Stack(s), Routing, Switching, Forwarding and Filtering
Transport Security Logging & Alarm Generation
Security Authentication Credentials Management
Network Element #2
(TD)
(TC)
(TB)
(TA)

Figure 2 Transport Plane Security Services

Figure 2 depicts the Transport Plane Security Services within an element and their interaction with their peer services in other elements. The interface identified by Transport (TA) represents the general communication between two elements without regard for the specific communications media or protocol technology actually used. Solid lines denote transport medium and dashed lines represent security messaging.

5.1.6.1 *Transport Peer Entity Authentication*

Transport Peer Entity Authentication is responsible for ensuring that when an element claims to own a specific identity the identity can be verified as truly belonging to that element. This service performs:

- The initial identity authentication
- Verification of authentication credentials validity
- Negotiation of security attributes necessary for Transport Data Origin Authentication.

One example of Transport Peer Entity Authentication is the IPSec Internet Key Exchange (IKE) protocol and Internet Security Association Key Management Protocol (ISAKMP) combination. The authentication is based on the use of cryptographic material, either:

- A digital signature created (signed) by using an asymmetric private key to encrypt a message digest, or
- A digital authenticator created by producing a message digest from a message and a shared symmetric secret key.

5.1.6.2 *Transport Data Origin Authentication*

Transport Data Origin Authentication is responsible for ensuring that when a destination element receives information that is alleged to have come from a source node claims to own a specific identity the identity can be verified as truly belonging to that element. This service ensures that all information exchanged between the communicating entities can be authenticated as to source and relies on the security attributes (keys, message digest algorithms, etc.) negotiated during Transport Peer Entity Authentication. The authentication is based on the use of cryptographic material, either:

- A digital signature created (signed) by using an asymmetric private key to encrypt a message digest of the information being exchanged, or
- A digital authenticator created by producing a message digest from the information being exchanged and a symmetric secret key.

The keys used, along with the algorithm and other parameters are either predefined or negotiated as part of the initial Transport Peer Entity Authentication process (as in ISAKMP).

5.1.6.3 *Transport Access Controls*

Transport Access Controls are responsible for ensuring that only allowed traffic can pass between communicating nodes or across network boundaries (domains). The common forms of Transport Access Control services are:

- Classic network layer 3/4 packet filters (a.k.a. "Firewalls") which make packet forwarding or blocking decisions based on packet destination layer 3 IP address and layer 4 port number relative to a set of packet filtering/access rules
- Application protocol filters (a.k.a. "Application Proxies") which may either forward, block or perform translation actions on application protocol messages. Some examples of application protocol filters are FTP – Web Proxies, SIP aware Firewalls and SS7 Security GateKeepers.
- Network unauthorized activity detection (a.k.a. "Network Intrusion Detection and or Attack Prevention-Mitigation" which use either rules based on activity signatures or levels/types of activity to identify, and possibly block, unauthorized network traffic and activities.

The packet filtering services can be implemented in stand-alone platforms (i.e., classic Firewalls), combined with other network related functional capabilities such as packet forwarding (i.e., Router/Firewalls), or even implemented in end nodes to protect a host from unauthorized network traffic sent to that host.

5.1.6.4 *Transport Data Confidentiality*

Transport Data Confidentiality is responsible for ensuring that information exchanged between communicating nodes is rendered unintelligible to all but authorized subjects (elements). This service relies on the use of cryptographic symmetric algorithms and shared secret keys to render the information being exchanged as meaningless to all but the authorized possessors of the cryptographic keys. The keys used, along with the algorithm and other parameters are either predefined or negotiated as part of the initial Transport Peer Entity Authentication process (as in ISAKMP).

A fairly recent use of Transport Data Confidentiality in the commercial world is for secure "logical private networking"; where a group of elements communicate amongst themselves over media shared with other elements that are not part of the group. This establishment of "trusted communities of interest" was originally called Virtual Private Networking (VPN). However, the term VPN has taken on additional meaning and now is used for any form of logical private networking whether Transport Data Confidentiality, or some other mechanism (such as ATM or MPLS), is used. Consequently, this document uses the term "Secure VPN" when referring to logical private networking that is based on Transport Data Confidentiality.

5.1.6.5 *Transport Data Integrity*

Transport Data Integrity is responsible for ensuring that any intentional or inadvertent changes or modification to information exchanged between communicating nodes is recognized. One way to provide Transport Data Integrity is by the use of the The Transport Data Origin Authentication service. Historically cyclic redundancy checks (CRCs) and frame check sequences (FCSs) have been used to provide this function. In some situations actual error correction codes (ECCs) have been used to not only detect changes but actually correct for bit errors. However CRC, FCS and ECC methods are NOT able to protect against intentional modification during transfer.

5.1.6.6 *Transport Security Logging & Alarm Generation*

Transport Security Logging & Alarm Generation are responsible for recording the information necessary to track security related events within the Transport plane. This service can also be configured to generate asynchronous alarm messages to notify other system functions and the Management Plane Security Event Management service of a situation that needs immediate attention.

5.1.7 Application Plane Security Services

The Application Plane Security Services are concerned with fulfilling the requirements of:

- Verification of Identities
- Data Origin Authentication
- Controlled Access and Authorization
- Protection of Confidentiality
- Protection of Data Integrity
- Strong Accountability
- User Account Management
- Activity Logging & Alarm Reporting

as these requirements apply to the general application functionality within an element and when the element is communicating with other elements.

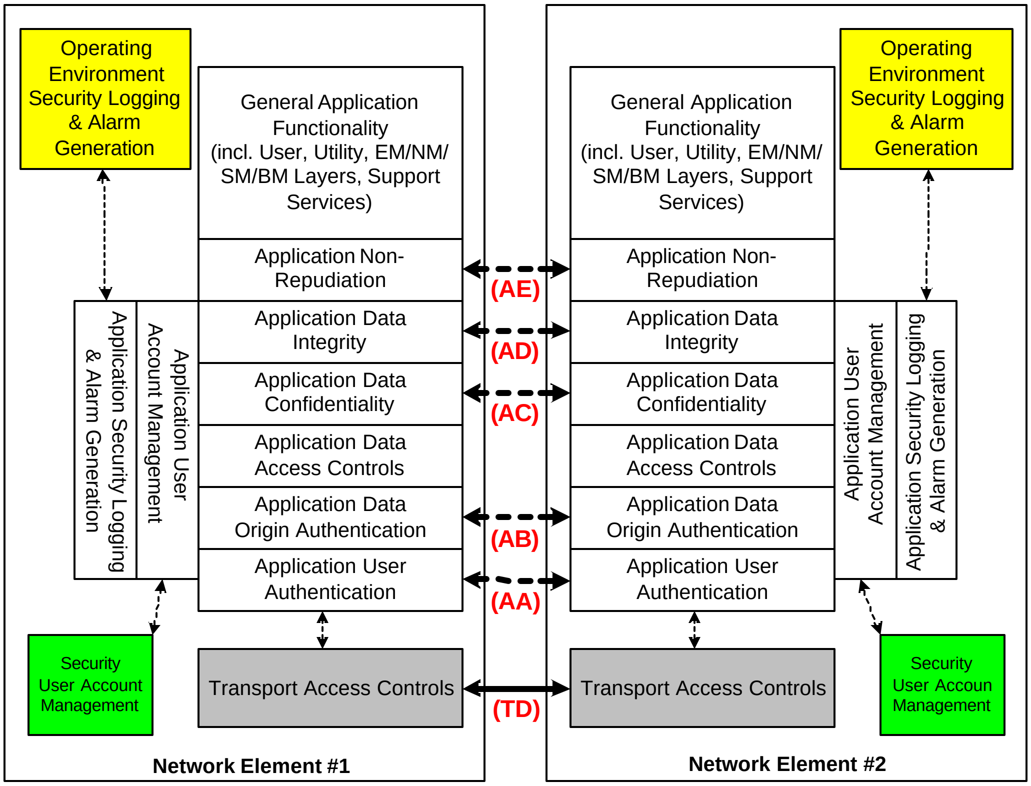

Operating Environment Security Logging & Alarm Generation
General Application Functionality (incl. User, Utility, EM/NM/ SM/BM Layers, Support Services)
Application Non-Repudiation
Application Data Integrity
Application Data Confidentiality
Application Data Access Controls
Application Data Origin Authentication
Application User Authentication
Application User Account Management
Application Security Logging & Alarm Generation
Security User Account Management
Transport Access Controls
Network Element #1
(AE)
(AD)
(AC)
(AB)
(AA)
(TD)
Operating Environment Security Logging & Alarm Generation
General Application Functionality (incl. User, Utility, EM/NM/ SM/BM Layers, Support Services)
Application Non-Repudiation
Application Data Integrity
Application Data Confidentiality
Application Data Access Controls
Application Data Origin Authentication
Application User Authentication
Application User Account Management
Application Security Logging & Alarm Generation
Security User Accoun Management
Transport Access Controls
Network Element #2

Figure 3 Application Plane Security Services

Figure 3 depicts the Application Plane Security Services within an element and their interaction with their peer services in other elements. The interface identified by Transport (TD) represents the general communication between two elements without regard for the specific communications media or protocol technology actually used. Solid lines denote transport medium and dashed lines represent security messaging.

5.1.7.1 *Application User Authentication*

Application User Authentication is responsible for ensuring that when a subject claims to own a specific identity the identity can be verified as truly belonging to that subject. The subject can be:

- a human logging into an application executing within an element, or
- an application executing within one element initially communicating with a peer application executing within a different element.

This service performs:

- the initial identity authentication
- verification of authentication credentials validity, as necessary
- negotiation of any security attributes necessary for Application Data Origin Authentication, if applicable.

One example of Application Peer Entity Authentication is the "classic" log-in identifier (IDs) and log-in password for human subjects. A variation on this theme is the Radius protocol typically used for remote access. Radius can work in a simple log-in IDs and password mode or in a "Chalenge/Response" mode. Another recent technique is the physical token, such as a "SecureID' or other device, which contains authentication information that may be used to authenticate the claimed identity of a human subject. The most recent technology in this space are "smart-cards"; credit card like intelligent devices that include processing capabilities and non-volatile storage for asymmetric cryptographic private keys and digital certificates of a Public Key Infrastructure (PKI).

For application process to application process some of the mechanisms based on the use of cryptographic material are:

- a digital authenticator created by producing a message digest from an application message and a shared symmetric secret key (used by many routing protocols, network service protocols such as NTPv3 and management protocols such as SNMPv3)
- Digital signatures (frequently combined with digital certificates of a PKI) as used by the Transport Layer Security (TLS) protocol, the Secure Sockets Layer (SSL) protocol, the Secure Shell (SSH) protocol replacement for FTP and Telnet. However TLS, SSL and SSH only support applications that rely on TCP
- The Kerberos security framework used either as part of the Distributed Computing Environment (DCE) or by itself with "kerberized" applications
- IPSec (including IKE, ISAKMP, AH and or ESP) by the Common Object Request Broker (CORBA) distributed application architecture.

5.1.7.2 *Application Data Origin Authentication*

Application Data Origin Authentication is responsible for ensuring that when an application, executing on a destination element, receives information that is alleged to have come from an application, executing on a source node, which claims to own a specific identity the identity can be verified as truly belonging to the source application. This service ensures that all information exchanged between the communicating applications can be authenticated as to source and relies on the security attributes (keys, message digest algorithms, etc.) negotiated during Application Peer Entity Authentication. The authentication is based on the use of cryptographic material, either:

- a digital signature created (signed) by using an asymmetric private key to encrypt a message digest of the information being exchanged, or
- a digital authenticator created by producing a message digest from the information being exchanged and a symmetric secret key.

The keys used, along with the algorithm and other parameters are either predefined or negotiated as part of the initial Application Peer Entity Authentication process (as in ISAKMP, TLS, SSL, SSH SNMPv3, NTPv3).

5.1.7.3 *Application Data Access Controls*

Application Data Access Controls are responsible for ensuring that subjects are only permitted to access (view, modify, delete) application specific information (objects) that the subject is allowed access to. The controls are effected by comparing a set of per-subject access privileges against a set of per-object access restriction rules (a.k.a. access control lists [ACLs]). This service is critical to the concept of "least privilege" where ONLY those access privileges necessary to perform a defined task are granted to a subject. Subjects here may be either human or non-human as in cooperating application programs. A fairly recent for of Access Control I unauthorized activity detection (a.k.a. "Host Intrusion Detection" which use either rules based on activity signatures or levels/types of activity to identify, and possibly block, unauthorized activities within the application or element.

5.1.7.4 *Application Data Confidentiality*

Application Data Confidentiality is responsible for ensuring that information exchanged between applications is rendered unintelligible to all but authorized subjects (applications). This service relies on the use of cryptographic symmetric algorithms and shared secret keys to render the information being exchanged as meaningless to all but the authorized possessors of the cryptographic keys. The keys used, along with the algorithm and other parameters are either predefined or negotiated as part of the initial Application Peer Entity Authentication process (as in ISAKMP, TLS, SSL, SSH, SNMPv3).

5.1.7.5 *Application Data Integrity*

Application Data Integrity is responsible for ensuring that any intentional or inadvertent changes or modification to information, exchanged between communicating applications or stored within an application, is recognized. Historically cyclic redundancy checks (CRCs) and frame check sequences (FCSs) have been used to provide this function. In some situations actual error correction codes (ECCs) have been used to not only detect changes but actually correct for bit errors. However CRC, FCS and ECC methods are NOT able to protect against intentional modification during transfer.

5.1.7.6 *Application Non-Repudiation*

Application Non-Repudiation is responsible for ensuring that the act of either sending or receiving information exchanged between communicating nodes can be traced back to subjects. This service cryptographically provides the proof that a subject performed an action and is unable to deny the act at a later time. Currently Non-Repudiation can only be provided for communication between applications when digital signatures, combined with digital certificates, are used for data origin authentication.

5.1.7.7 *Application User Account Management*

Application User Account Management is responsible for the creation, modification and deletion of application user accounts that define the rights and privileges of human, and non-human, subjects. This service also is responsible for maintaining any authentication credentials associated with the subject (such as log-in IDs, passwords, etc.).

5.1.7.8 *Application Security Logging & Alarm Generation*

Application Security Logging & Alarm Generation are responsible for recording the information necessary to track security related events within the Application plane. This service can also be configured to generate asynchronous alarm messages to notify other system functions and the Management Plane Security Event Management service of a situation that needs immediate attention.

5.1.8 Management Plane Security Services

The Management Plane Security Services are concerned with fulfilling the requirements pertaining to:

- Managing security related events
- Managing security related alarms
- Managing security log entry reconciliation and analysis of audit trails
- Managing subject authentication credentials
- Managing the configuration of security services within elements
- Managing application and execution environment subject accounts within elements
- Managing
- Activity Logging & Alarm Reporting.

The Management Plane Security Services are discussed on detail in section 4.2.

5.2 Security Management Architectural Framework

The Security Management Architectural Framework defines the relationship between the Management Plane Security Services and the security services of the Transport and Application Planes. Figures 4 and 5 depict the:

- ♦ Transport Plane Security Services within elements and their interaction amongst themselves and the Management Plane Security Services (Figure 4)
- ♦ Application Plane Security Services within elements and their interaction amongst themselves and the Management Plane Security Services (Figure 5).

The interfaces identified by (MTA-G) text represent communication between the Management Plane security services and the Transport Plane, Application Plane and Operating Environment security services without regard for the specific communications media or protocol technology actually used. The dashed lines represent communication between services within an element.

For security management framework to be interoperable, managed elements must utilize common syntax (structure) and semantic (content) definitions. These definitions are will be defined in other specifications

5.2.1 Security Event Management

An event is a report of something happening in the network (e.g., a netflow record).

- A security event is an event relating to violation of authentication, authorization, integrity, or availability (e.g., a user logging – see Appendix D – in a system, a change in a firewall configuration).
- A security alarm indicated a change in state from a normal statistical pattern of behavior. It generally is a result of the occurrence of security events (e.g., too many login failures on one piece of equipment).
- Security event and security alarms management is the process of collecting events and analyzing them in order to determine the security state of the network.
- Attack identification is the process of detecting malicious behaviors through the analysis of events collected from the network. The process leads to generation of security alarms. The identification can be local when a system is able to make a full diagnosis of the problem (e.g., too many login failure on one host, an illegal flow screened by a firewall). For some attacks scenarios, it may be necessary to combine information from different elements to detect the attack.
- Mitigation is the process of reaction to a security alarm by changing the network configuration in order to reduce the risk cause by this threat.

Security Event Management is responsible for receiving security alarms from the Transport and Application Plane Activity Logging & Alarm Reporting services. Upon receipt these alarms are indexed and stored for further analysis and reporting purposed. This service is also responsible for archiving and retrieval of prior alarms to/from off-site long term storage.

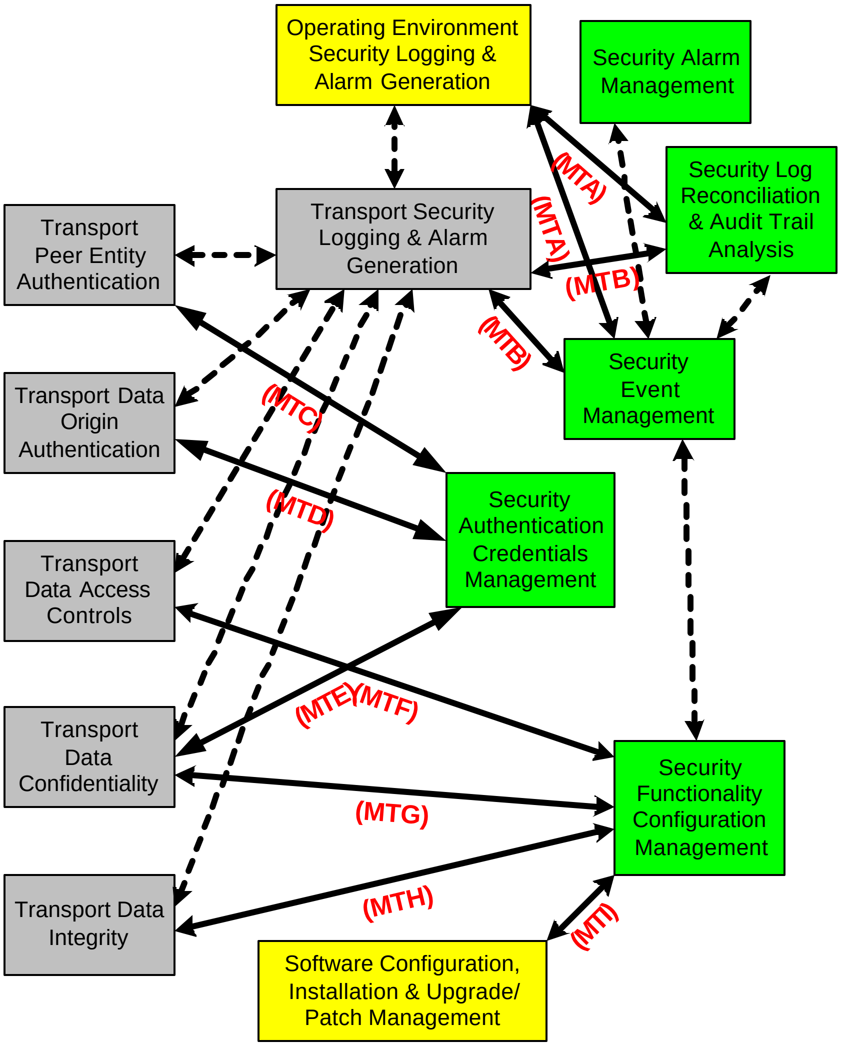

Operating Environment Security Logging & Alarm Generation
Security Alarm Management
Security Log Reconciliation & Audit Trail Analysis
Transport Peer Entity Authentication
Transport Security Logging & Alarm Generation
Security Event Management
Transport Data Origin Authentication
Security Authentication Credentials Management
Transport Data Access Controls
Transport Data Confidentiality
Security Functionality Configuration Management
Transport Data Integrity
Software Configuration, Installation & Upgrade/ Patch Management
(MTA)
(MTA)
(MTB)
(MTB)
(MTC)
(MTD)
(MTE)
(MTF)
(MTG)
(MTH)
(MTI)

Figure 4 Management Plane interaction with Transport Plane Security Services

Solid lines denote transport medium and dashed lines represent security messaging.

5.2.2 Security Alarm Management

Security Alarm Management is responsible for reviewing the security alarms received from the Transport and Application Plane Activity Logging & Alarm Reporting services and ascertaining criticality of each alarm as to the seriousness of the security breach each alarm signifies. This service also should provide recommendations to operations personnel for:

- Ascertaining the extent of a security breach
- limiting the extent of any security breach
- acquisition of forensic information to support possible criminal or civil court proceedings
- reestablishing normal services as quickly as possible without increasing the risk of continued or further security breaches.

Also provided by this service should be report generation capabilities and real-time notification mechanisms to alert Operations personnel in a timely fashion.

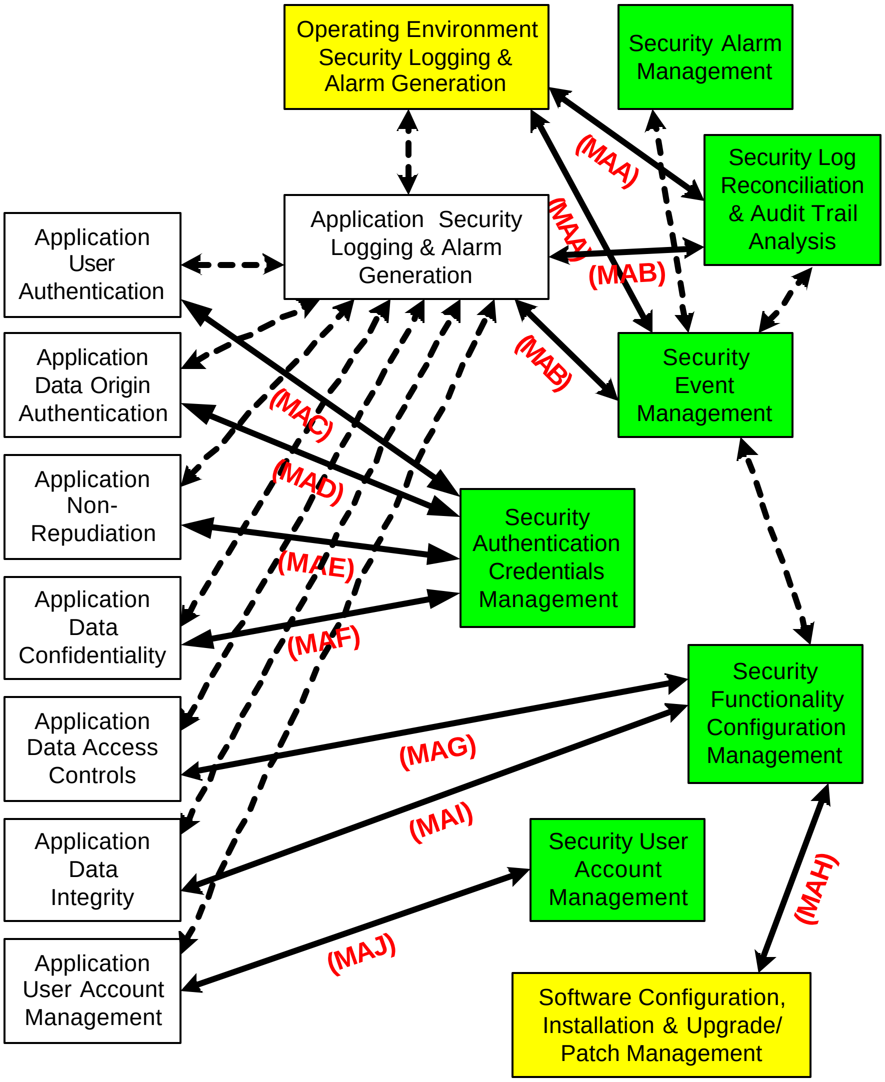

Operating Environment Security Logging & Alarm Generation
Security Alarm Management
Security Log Reconciliation & Audit Trail Analysis
Application Security Logging & Alarm Generation
Security Event Management
Application User Authentication
Application Data Origin Authentication
Application Non-Repudiation
Application Data Confidentiality
Application Data Access Controls
Application Data Integrity
Application User Account Management
Security Authentication Credentials Management
Security Functionality Configuration Management
Security User Account Management
Software Configuration, Installation & Upgrade/ Patch Management
(MAA)
(MAA)
(MAB)
(MAB)
(MAC)
(MAD)
(MAE)
(MAF)
(MAG)
(MAI)
(MAJ)
(MAH)

Figure 5 Management Plane interaction with Application Security Services

Solid lines denote transport medium and dashed lines represent security messaging.

5.2.3 Security Log Reconciliation & Audit Trail Analysis

Security Validation, for a heterogeneous mix of managed elements, includes:

- Auditing of managed element security related configuration attributes.
- Penetration testing of managed element.
- Network based intrusion detection.
- Host based intrusion detection.
- Verification of managed element compliance to organizational security policies.
- Certification, accreditation, threat/risk analysis, compliance auditing, and forensic auditing.

Security Log Reconciliation & Audit Trail Analysis are responsible for:

- retrieving transport, application and operating environment security log files
- indexing and storing security log files for analysis
- archiving and retrieval of security log files to/from off-site long term storage.

This service also provides:

- the ability to reconcile log entries across the transport and application functional planes, as well as the operating environment logs, by time stamps and other criteria
- trend analysis capabilities
- alarm generation based on the results of statistical, and other, criteria
- definable reporting capabilities.
- Can be implemented as a centralized, decentralized or a combination of both.

5.2.4 Security Authentication Credentials Management

Security protocols (such as SSL, SSH, SNMPv3) and security extensions to other protocols (such as CORBA, MPLS, BGPv4, OSPFv2) typically provide authentication and confidentiality functionality. Strong authentication among, and confidential transfer of information between, network elements are necessary for system security. Strong authentication and data confidentiality are based on a cryptographic foundation. Cryptography uses special algorithms and tightly control information referred to as keys. The algorithms are, and shall be, publicly available, thereby allowing for widespread scrutiny and ease of implementation. The "strength" of this concept is in the keys – strength refers to the amount of time required to reverse engineer (i.e., find or guess) the key value(s) being used with a specific algorithm. Consequently, the methods used to generate, store, distribute, destroy, and revoke these keys are of paramount importance. Additionally, the length of a cryptographic key has a direct bearing on the amount of security a crypto-system provides.

Authentication Credentials Management spans the creation, archiving, distribution, and revocation of digital credentials supporting authentication and authorization for a heterogeneous mix of managed elements, across the following areas:

- Subject authentication X.509v3 certificate request processing, public/private key generation, certificate creation, repository loading, archiving, and revocation (organization public key infrastructure).
- Shared authentication symmetric key generation, secure distribution, archiving/escrow, and revocation (organization electronic key management services).
- Subject authorization X.509v3 certificate request processing, certificate creation, repository loading, archiving, and revocation.

This function provides the ability to manage all authentication credentials related to identifying both human and non-human entities that wish to access managed elements. Credentials management includes the creation, assignment, storage, revocation, resetting, and escrowing of credentials. These credentials include login passwords, asymmetric cryptographic public-private key pairs, predefined symmetric cryptographic secret key pairs, X.509v3 digital certificates, and Kerberos tickets. . Also part of this service are the servers used to host RADIUS Authentication services, Kerberos Authentication services, PKI Certificate and Registration Authority services, as well as LDAP certificate repositories.

Security Authentication Credentials Management is responsible for managing all authentication credentials related to subject identities for both human and non-human subjects. Credentials management includes the creation, assignment, storage, revocation, resetting and escrowing of credentials. These credentials include log-in passwords, asymmetric cryptographic public-private key pairs, predefined symmetric cryptographic secret key pairs, X.509v3 digital certificates and Kerberos tickets. Also part of this service are the servers used to host Radius Authentication services, Kerberos Authentication services, PKI Certificate and Registration Authority services and LDAP certificate repositories.

5.2.5 Security Functionality Configuration Management

Security Service Configuration Management spans the creation, archiving, downloading, validation, and modification of security related configuration attributes, within a heterogeneous mix of managed elements for the following types of attributes within managed elements:

- Organizational policy definition;
- Specification as machine parsable rules; and
- Tracking of said rules against other organization security-related configuration attributes.
- Network located (inter network segment; AKA firewall) source/destination address and port packet filtering rules.
- Network located (inter network segment; a.k.a application proxy) application protocol packet filtering rules.
- Host located application protocol packet filtering rules.
- Managed element internal object access control rules.
- Managed element authentication, authorization, integrity, confidentiality, and logging/reporting (see Appendix D) default configuration parameters.
- Organizational default symmetric and asymmetric encryption parameters, attributes, and algorithms.

This function provides the ability to set, modify, and reset security related configurable parameters within managed elements and applications, especially access control lists and the security policy criteria to deliver services. This function also supports the management and verification of integrity and authenticity of all software downloaded to and or installed into a managed element. Security Configuration Management will have the ability to group network elements into common domains so that these domains can be managed as if they were a single network element.

Security Functionality Configuration Management is responsible for providing the ability to set, change and reset security related configurable parameters within elements and applications, especially object access control lists and the security policy criteria that Transport and Application Plane security services require. This service also supports the management and verification of integrity and authenticity of all software down-loaded to and or installed into elements.

5.2.6 Security User Account Management

Administrative User Account Management spans the following areas:

- Individual user account creation.
- Specification of user identifiers.
- Resetting of user passwords.
- Specification and maintenance of user access rights and privileges.

This function also provides the ability to add, change, or delete information about entities that may access managed elements. It includes the ability to manage group and sub-group memberships, access rules, and privileges to the entities. It also includes verifying the identity of an entity. In situations where management of an network element through the OSS is not available, related information about subjects and subject groups must be combined and propagated to the network element. It is through this service that:

- Account "lock-outs."
- Subject access privileges.
- User groups are defined, controlled and managed in a centralized manner.

Security User Account Management is responsible for providing the ability to define, change and reset security related attributes of human subject user accounts on a global basis for elements and applications. It is through this service that:

- Account "lock-outs"
- Subject access privileges
- User groups

are defined, controlled and managed in a centralized manner.

5.3 Relationship with other TSP Management Systems

Operational Support Systems (OSS) are the computerized and automated systems that help enable TSPs manage their services, share information, process orders and billing, handle maintenance and report requests of new customers. It is a generic name provided to any software system that is used to manage these very services, but was originally coined for voice line entities. Since then it has mushroomed into support for voic e, data, and application/presentation level interfaces.

As the OSS is nothing more then a software based system, each with its own security complexities, it can all be thought of as an application/presentation level entity exhibiting those same levels of need. Each has its own way of providing policy and privilege management. Each has its own golden source of data with its own integrity confidentiality issues. Finally each has at least one northbound and one southbound interface with its own key systems, notarization, and privilege/policy management. More importantly each has its own model of securing the specific features it exhibits.

- User Level access and authentication
- Golden Source integrity and access controls
- Security and User action audit logs
- North and Southbound interfaces
- Wholesale access bus

To add to the level of control required, the OSS systems also have been developed and created in a number of different ways using many different hardware and software services and methodologies. The first would be mainframe systems where presentation and application level services all extend from the same physical system. Newer OSS deployments are now making use of open systems as well as client server models where the presentation layer is completely separate from the application layer and each requires its own level of security management based upon the services it offers. For example the application layer maintains the golden source, provides for user actions, and provides for all the north and southbound external system interfaces. The presentation layer can be another piece of software running on a completely different machine that allows the user to interact with the application layer though a communications channel across, very typically, unsecured and open networks. As well by using a myriad of different architecture types and systems the management of this becomes ever more complex purely due to the total number of different platforms and how services can and are be exhibited on each.

Very similar to the needs of the OSS is the requirements placed upon security by the Element Management Systems (EMS) as well the Network Management Systems (NMS). Therefore weaved into this section will be a description of the additional requirements above and beyond that needed by the OSS.

In the following section is a brief description of the various services that the OSS and EMS's support in today's environment and what specifically those systems export that require security management. In some cases the OSS and EMS's are specified to support features that do not exist today, but are planned in the future. As such some assumptions are made to provide a holistic view of the needs for the SMS OSS. This section is then concluded with a description of the services that are or will exist within the OSS and EMS's that require management by the SMS.

5.3.1 OSS Security

5.3.1.1 *Order Entry and Business Workflow*

The starting point for any customer driven work performed at a TSP is to take an order via a service representative within the call centers and enter the order into the system that initiates work to provide services for the customer. The order can appear through a few different input portals. One method is for a user to enter the order information by hand via a GUI or a text based terminal interface. In all cases access to these systems is restricted by a request for credentials for each user that is then associated to a roles based security system to lock access to different features of the system and the underlying supportive data. The second method is via the wholesale gateway that is simply a message broker that bridges the traffic from CLEC/DLEC companies. The message brokers utilize asymmetric key pairs to provide for end point authentication. There are a number of transports including the likes of CORBA, XML Web Services, and batch files to fulfill the movement of that data once authenticated.

The public key is typically physically shared between the endpoints by hand and the private key is stored locally in a keying to support the message broker to ensure the identify of the requester and the provider of each request. In some cases the use of a certificate authority is provided for. Where possible the use of managed certificate authorities should and is utilized for single point of access for public key requests and to ensure its authenticity, as well the proper local key ring management for security access to the private keys. Of course any one single trust model does not always fit when dealing with external companies so various trust models need to be supported such as cross certification, hierarchical, user centric, and inter domain. This is driven by the authorities that signed the certificates provided by the remote partner and the level of security required in dealing with CLEC/DLEC's. This differs from interface to interface and the sensitivity of the data that is carried over it. It should be also noted that for the wholesale gateways, the requests may not always be transported over private networks and therefore, as there is confidential customer information contained in the requests, the underlying transport is authenticated, verified, and confidentially protected.

Once the order has been entered into the system the business workflow takes over the responsibility to flow that order to all the necessary underlying systems via south bound interfaces. There are many different manners of communicating these orders from order entry system to all of these supporting systems. Each system provides for its own method of secured communications, or lack thereof. Obviously the origination, integrity, confidentiality, and authentication of that request must be managed as much as possible from system to system thereby placing these very needs on the south bound interface of the ordering system.

Finally the ordering system and its supporting workflow maintain all of the customer details, network information, and any billing details taken on the original order in a local database or golden source of information. This information is considered highly sensitive and therefore undergoes a level of backup and securities commiserate with the level of sensitivity.

Both local and external orders are stored in a long-term storage system as well all security audits and any generalized security logging. All of these must be stored in such a way to ensure non-repudiation and data integrity of the logs.

5.3.1.2 *Provisioning and Activation Services*

Once an order has been taken, the next major step to perform is to ensure the necessary network resources exist to provide the requested level of service to the customer. If those resources do in fact exist then the necessary changes are made to the network to support that new service. It is the provisioning and activation systems that provide for this level of functionality. This request for service would appear via the southbound interface to the provisioning and activation system. If the provisioning system determines there are sufficient resources, then those resources are locked and a request is sent to the activation modules for real time modification of the underlying Managed Network Elements to support the requested services. As the provisioning system maintains the holistic view of the network from end to end, it is also responsible for providing these details via north bound interfaces to test and fault management OSS systems to initiate the careful monitoring of the new service and to enter the proper tickets where applicable.

It should be noted at this point that this level of provisioning is considered service level provisioning. There is yet another layer called infrastructure that is preformed prior to services turn up. This is when the engineers build new equipment and place them in the proper central offices and then build the necessary physical interconnects as well as the one time logical resources within the device to support auto-flow provisioning.

Once the provisioning system has fully allocated and locked down the resources the activation systems take over and communicates either to the EMS/NMS or to the network element directly though a number of different protocol types and stacks. Each protocol and stack has its own security requirements and needs. The activation systems communicate with the physical elements to make the necessary changes to support the new service for the customer. As well it has the capability to pull back all the data within the Managed Network Element(s) for the purposes of reconciliation of the golden source for the provisioning system to the physical network.

Another area of security control is the golden source of data that represents the global view of the network. Obviously this data is a corporate asset that must be secured, as well who is able to alter that view must also be controlled whether that request appears from a machine to machine interface or a user to machine interface.

Of course with any changes to the network all actions and requests are greatly audited and stored for long term retrieval. This raises concerns for repudiation and data integrity for those audits and as well generalized security logging.

5.3.1.3 *Testing Services*

Once a new service has been turned up by the activation and provisioning system, all of the necessary customer service path information is sent to the test system and a request to verify the integrity of the new service is specified. The test systems will then issue various tests that can be either disruptive or non-disruptive to ensure that the service is in fact working, as it should be. The request for this will appear via a northbound interface from the provisioning system.

Another mode of request is when the operations organization is provided a ticket specifying that a customer indicated service is in a non-working state. This very system will be used to determine where the fault if any may lie. The requests to the test OSS are submitted from a presentation layer interface on a secured communications channel (a.k.a. northbound interface).

It should be noted that the requests to test could only appear from personal within the TSP. Any DLEC or CLEC issues will appear via the operations groups as described above. Therefore the need for confidentiality of the requests is not as important.

To perform these services, the test system is provided a complete services view of the new customer which is stored in a local golden source database. The specification for new service arrives via one of the two northbound interfaces that should be across an authenticated and notarized channel. As these tests can, in some cases, be service effecting it is important that the policy and privilege management also be very well managed to ensure that the request is legitimate before service disruption occurs.

5.3.1.4 *Fault Management Services*

After a service has been turned up and has under gone test to ensure it is working, it is then turned over to the fault management systems to monitor that service to ensure it is always working. If at any time a disruption occurs for that service, it is the responsibility of the fault management system to alert the necessary operations personnel that can investigate the problem and fix it if necessary.

Once the service has been turned up and tested, the entire service order and the entire layout of the underlying infrastructure required to support that service are transmitted to the fault management system. This information is provided via a message bus (a.k.a. northbound interface). This information is then stored in a golden source or database. The incoming information is authenticated, authorized, and then it is stored for monitoring. Of course this data is considered sensitive so the necessary controls and retention are undertaken to ensure this data and it's origin is not corrupted by accident or maliciously.

Now that the service is properly committed to the golden source the fault management system monitors the resources supporting all the services in the database. In most cases the fault management communicates to either an EMS/NMS or directly to the network elements. All of these interfaces must undergo authentication and authorization and to be placed in the proper role to ensure the sufficient levels of access to the network elements for monitoring.

There is no one single system that supports fault management for all services. These services are broken up into a number of different systems. Unfortunately in today's world each system is not an island. There are a number of places where the services are layered one on top of the other. When a problem occurs the monitoring systems must coordinate to ensure a single ticket is issued to the proper NOC based upon where in the layering of resources the problem has occurred. Because of this, it means the fault management systems must all intercommunicate and share data. As such all those communications channels as well data sharing are authenticated, authorized, confidentially secured if transmitted outside of local networks, and finally each sub-request is notarized.

5.3.1.5 *Billing*

Once the order has been completed, it is sent to the billing system so that the necessary charges can be sent to the customer. The data is transmitted on a message bus that, as with all the other systems, requires the proper levels of authentication and authorization. As the result of accepting the incoming service, a customer will be billed. It is important to ensure who sent the request and that it is a proper request. The data contained in the request for billing also will contain customer information that is highly confidential as if subverted could cost the customer money that is not valid. Beyond the normal services typically the data is treated properly for confidentially. This is seen in the communication channel when securing the transmission of the data, as well ensuring the proper levels of policy and privilege management upon the golden source of data. This of course is true not just of the hot data but also all backups be they standby or long term.

5.3.1.6 *Engineering*

To support any customer service a number of Managed Network Elements must be installed and managed. The systems that perform this role are used by the engineering groups which store the new equipment, the exact instance of each equipment type (i.e. number of cards, type, etc), and where it is located. The information is in most cases transmitted either by batch transactions or on a real time message bus to the provisioning systems. This is done so that the equipment can be used immediately for customer services. It is also done to ensure proper synchronization with the provisioning systems and the actual network which reduces lost dollars in lack of automated flow through as well the loss of money due to miss-tracked assets. The provisioning systems need to ensure that the incoming infrastructure assets are in fact from an authenticated source identity and that the requesting engineer has the authorization to inject that product for service. As such coordinated policy and privilege systems must exist between the two systems.

5.3.1.7 *Ticketing Systems*

When a customer calls the TSP to report trouble a ticket is entered which is then tracked though the various support organizations that will fix and monitor the problem until resolution. This ticket is opened for the lifetime of that trouble. The number of troubles reported and the duration of each is tracked daily for reports to management and more importantly the FCC/PUC's on fineable outages. As with any system the normal privilege and policy management is very important to prevent spoofed tickets, which could result in lost dollars due to wasted truck roles or miss-placed workforce. More importantly the tickets must also be verified to be correct in its data validity. The long term storage as well the reporting must ensure proper authenticity of the ticket, that it was time stamped with a secured source of time to ensure proper duration, and most importantly to ensure repudiation.

5.3.1.8 *Outside Plant Management*

Outside plant management includes not only systems to manage the work force outside of the central offices but also any supporting system that assists them in the roles they perform. As such work requests will arrive into OSP management systems via batch or on a real time message bus. These requests are authenticated and then processed. They can either appear from the ticketing systems or the provisioning systems.

There are a number of supporting services that assist the OSP workforce. For example GPS tracking systems to ensure the location and duration of each unit of work. Mobile devices that have the authority to take customers in and out of service or the ability to perform tests that can be service disrupting. Each of these systems communicates in batch or on a wireless channel and therefore requires identity, policy and privilege management as well high levels of confidentiality.

5.3.2 EMS Security Needs

The Element Management System (EMS) is responsible for the management of Managed Network Elements (MNE) in the network. It typically provides for the entire FCAPS umbrella. FCAPS (fault-management, configuration, accounting, performance, and security) is an acronym for a categorical model of the working objectives of network management. There are five levels, called the fault-management level (F), the configuration level (C), the accounting level (A), the performance level (P), and the security level (S).

To support the FCAPS model, the EMS provides for interfaces to all the MNE's under its control. At the same time it must support interfaces to all of the OSS systems that make use of these FCAPS features in addition to presentation level services that make use of the EMS which also require policy and privilege management.

The ability to inject security through the northbound interfaces of the EMS is not a major effort as most have been or can be standardized on a few different technologies such as CORBA and Secured XML. Of course there are a few technologies such as TL1 and PDS that do present needs for security above and beyond the transport. In most cases the EMS runs on Operating Systems that allow for the ability to plug IPSec under the covers such that the EMS requires no code change to support authenticated communication channels which is the primary need. The only caveat is that the EMS be capable of existing on specific version of the O/S that support this feature.

The major issue is securing the southbound interfaces of the EMS. There are a myriad of protocols and each has it's own issues to solve. Driving security to the MNE adds cost to the device as well as complexity. Most MNE's provide for a simple CPU or ASIC that has very little capability and barely provides for the basic MNE management. As such additional processing capability needs to either be built into the CPU/ASIC or an offload security card is added to the chassis thereby reducing open slots for the device. There is really no good answer here but the industry is slowing starting to respond. As such in the up coming years the need to manage security down to the MNE itself which will then provide for a host of PKI capabilities will be required. The MNE will support asymmetric key authentication, data confidentiality, intrusion detection, virus detection, notarization, and many other needs. In addition this need grows as features like firewalls are pushed directly into the network elements.

The SME OSS will be required to support the policy and privilege management for all of the interfaces including the presentation layer. It must support and manage all of the PKI usage by the south and northbound interfaces of the EMS. It must support security infrastructure on the MNE's such as firewalls. And it must support the ability to manage all of the audits and security logging that is generated from this layer of the network, which is a very large volume of information.

5.3.3 NMS Security Additions

The Network Management System (NMS) provides for all the features of the EMS but with one additional benefit. The EMS will treat the network element as an island. Services are looked at from a single element perspective. The NMS takes a holistic view of the network and then provides for true end point provisioning and management. This means all of the support MNEs in the network between ingress and egress points to the network are hidden from the user as it applies to provisioning. Instead only the ingress points and egress points are specified. Of course to do this, it means that all of the MNEs that provide for that part and layer of the network must all be managed out of the single NMS.

From a security perspective this is not always desired. The issue is that operations group's are not always a single point of control in one geographic area. In some cases they can be spread out regionally such that each group has a responsibility to a single part of the network. Global access to the entire network is not always desired. In most cases the EMS is regionalized by itself which provides for this, but with the NMS this cannot be done. A finer level of policy and privilege management is required to provide for domains in the network where access and visibility can be controlled at a regional level. In some cases this is required at even at a finer level of detail based upon access to only certain features of network elements in each domain. The ability to delegate responsibility based upon workload, follow the sun support, and other business drivers is also a requirement.

5.3.4 Key System Requirements

With the provided understanding of the OSS and EMS environments, below is a list of requirements needed for the interfaces and systems described above. With these interfaces and security needs, arises the need for the SMS OSS to ensure the proper overall management of these resources.

5.3.4.1 *Key Management*

Key management is a critical service required for the OSS and EMS systems. Use of asymmetrical keys for all of the methodologies described above is of great importance. The proper management and centralization of keys will greatly reduce the complexity of rolling out new services as well reduce the duplication of identities, or even worse miss-identification within the company. Unfortunately there is no one single method of centralized key authority today. Therefore SMS must be capable of supporting the various types of key authorities. The methods used are prescribed not just by TSP but by the various wholesale partners as well. A number of trust models must be supported and managed by the SMS OSS.

Beyond centralized key repositories proper key management such as key rings, backup and restore, automatic key updates, and key signature management will all be critical services offered and managed by the SMS OSS.

5.3.4.2 *Non-Repudation*

As data is moved back and forth between systems and more importantly wholesale partners the capability to repudiate the request is of high importance. Use of technologies described else where in this document are being utilized today in OSS and EMS systems. But to provide a cohesive system, the ability to manage the archival of secured data and it's signatures as well the proper archival of the keys used to sign the data will be required in support of SMS. This of course provides for single point of management and thereby contact for all repudiation issues.

5.3.4.3 *Time-Stamping*

The use of security level time stamping is required and used throughout security services. It is used by security audit and logging systems, key management, notarization services, data integrity, and many other areas. Therefore the support and management of proper timing will be required for SMS as it relates to OSS systems.

5.3.4.4 *Privilege and Policy Management*

The single greatest need for OSS and EMS's today is the need for privilege and policy management. Each system today implements its own identify and authorization services. The ability to standardize on a single method, such as single sign on, a single method to create a corporate identify, the use of standardized roles and responsibilities, and single point of management for all of this is required for SMS OSS support.

This not only reduces points of management but also assists in potential areas for mistakes or miss mapping of identities to capabilities. It will also reduce the amount of time required to map a new identity to the network, and more importantly provides for the ability to immediately revoke capabilities. Finally the ability to delegate responsibility by security administration allows for the seamless flow of work regardless of the need to delegate tasks for whatever the reason. With a single point of control, this task now becomes manageable in the face of the ever growing number of OSS and EMS systems and sub-systems.

5.3.4.5 *Notarization*

As specified previously all OSS and EMS systems support a north and sound bound interfaces, it is not always sufficient to just authenticate the identity of the communication channel. In many cases a single channel can be used for numerous identities. The ability to notarize each element of data based upon the sender becomes very important. The task of doing this grows more complex with each system deployed into the network. As such the standardized methodology and the proper management of such a task will fall to the SMS OSS.

5.3.4.6 *Confidentiality and Integrity*

For most OSS and EMS systems the need to provide for confidentiality with the data is not as important unless that data must travel across networks that are not within the private corporate network. For example any elements sent back and forth between the TSP and CLEC/DLECs. The ability to monitor and manage this service with sufficient performance levels becomes very important.

Beyond just communication channels the confidentiality and integrity of data maintained in global OSS and data repositories both online and offline is required. The centralized management of such systems would fall under the tasking of the SMS OSS.

5.3.4.7 *Audit and Logging*

Most if not all OSS and EMS systems generate copious amounts of security logging and audit trails. The ability to collect and maintain these data trails will need to be centralized for single point of control and thereby contact. The SMS OSS will be required to interface with the various OSS systems to collect this material real time. As well SMS is required to collect that information in such a way to ensure proper repudiation and proper long-term storage.

5.3.4.8 *Intrusion detection*

Every OSS and EMS runs on a piece of hardware. That hardware is provided access to the managed networks. As such it is open to intrusion by an outside party that was not provided identified access to that box. The ability to detect and counteract the intrusions is highly important due to the sensitivity of the data contained in the OSS and EMS. As such the proper management of intrusion detection systems to ensure for a cohesive policy for this feature will be paramount.

5.3.4.9 *Virus Detection*

The ability to either detect viruses detection or manage virus systems will be key. The injection of a virus or worm into both the OSS and EMS or to the devices it manages is highly important. These viruses and worms can provide for huge breaches in the security provided for in the network. As such systems watching the Operating Systems of the OSS and EMS will be required.

5.3.4.10 *Secured Software Distribution*

Most if not all EMS, NMS and OSSs provide for a means to automatically distribute software either to the OSS itself for self-upgrade or to the MNE provided by the vendor. In all cases the management of notarization of that software load is very important. When a vendor ships a piece of software, it should also provide for the notarization of that software via a secured hash to ensure the validity of the load as provided by the author. The same is true of the OSS and EMS where software upgrades are done be either IT or external vendors. In all cases the software should be ensured by installation/distribution systems to be from the proper author by the same means. The SMS OSS should manage all of the features listed above.

6 Security Management System Functional Requirements

Security administrators must have available a set of functions to assist them in performing their functions efficiently and conveniently. Not all of the functions discussed here are available currently, and steps will need to be taken to ensure their timely creation.

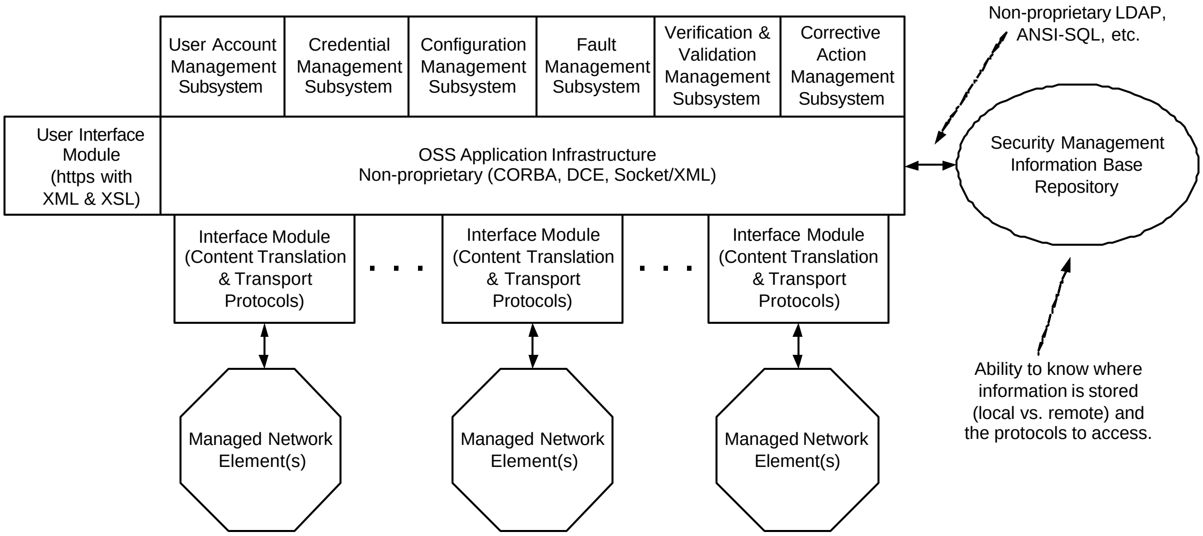
Each of the security management activities discussed in the following paragraphs will require automated support for security administrators. The applications that provide this support are concerned with various aspects of SMIB maintenance, key management, and examination, processing, and correlation of information such as audit records. These management applications should work together smoothly, but they must also be separable if it is desired to assign certain activities to specific security administrators. In some instances, it will be necessary to integrate security management applications with other applications. For example, X.500 Directory Service Agents might be used to store portions of a SMIB so that user certificates are easily available to a user community.

6.1 TSP Security Management Functional Requirements

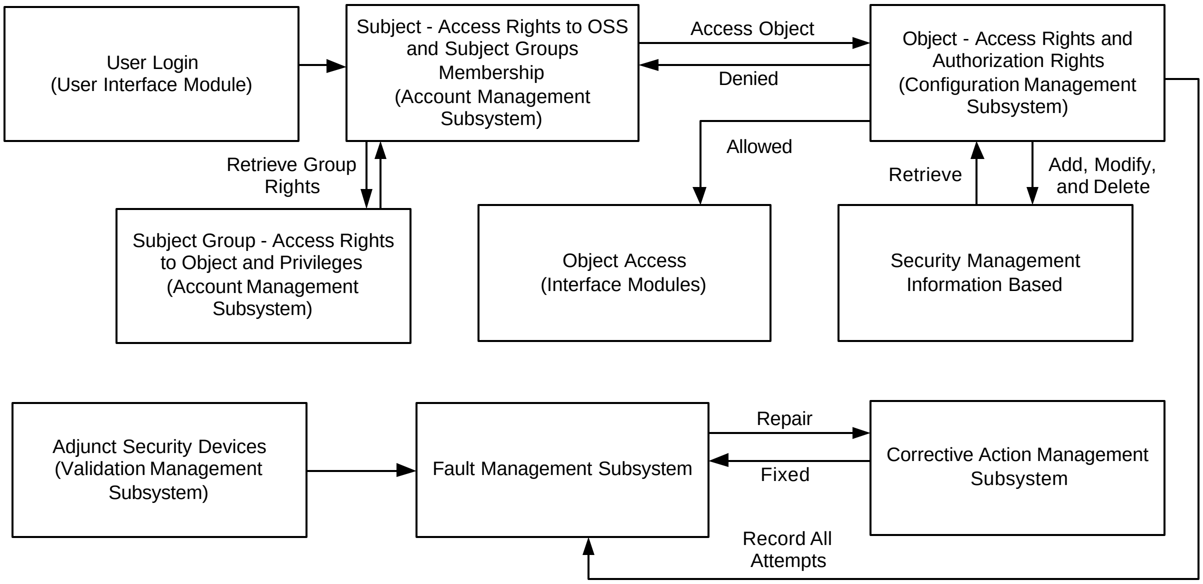
The Management Plane Security Services are concerned with fulfilling the requirements pertaining to the security services within an element, which includes:

- User Interface Module
- User Account Management Subsystem
  - Managing a subject's authentication credentials, subject group memberships, and access rules
  - Managing the subjects groups' identifiers and privileges
  - Managing subject propagation
  - Managing authentication
- Credential Management Subsystem
- Configuration Management Subsystem
  - Managing of objects and object groups
  - Managing an object's subject and subject group access and authorization rights
  - Managing the security functionality configuration
- Fault Management Subsystem
  - Managing security related events, including adjunct security devices reporting
  - Managing security related alarms
  - Managing security log entry reconciliation and analysis of audit trails
  - Reporting corrective action and receiving corrective action completion.
- Validation Management Subsystem
- Corrective Action Management Subsystem
- Security Management Information Base Repository
- Interface Modules

The basic design is pictured below.


User Account Management Subsystem
Credential Management Subsystem
Configuration Management Subsystem
Fault Management Subsystem
Verification & Validation Management Subsystem
Corrective Action Management Subsystem
Non-proprietary LDAP, ANSI-SQL, etc.
User Interface Module (https with XML & XSL)
OSS Application Infrastructure
Non-proprietary (CORBA, DCE, Socket/XML)
Security Management Information Base Repository
Interface Module (Content Translation & Transport Protocols)
. . .
Interface Module (Content Translation & Transport Protocols)
. . .
Interface Module (Content Translation & Transport Protocols)
Managed Network Element(s)
Managed Network Element(s)
Managed Network Element(s)
Ability to know where information is stored (local vs. remote) and the protocols to access.

The basic flow between subsystems and interface modules is pictured below.


User Login (User Interface Module)
Subject - Access Rights to OSS and Subject Groups Membership (Account Management Subsystem)
Access Object
Denied
Object - Access Rights and Authorization Rights (Configuration Management Subsystem)
Allowed
Retrieve Group Rights
Retrieve
Add, Modify, and Delete
Subject Group - Access Rights to Object and Privileges (Account Management Subsystem)
Object Access (Interface Modules)
Security Management Information Based
Adjunct Security Devices (Validation Management Subsystem)
Fault Management Subsystem
Repair
Fixed
Corrective Action Management Subsystem
Record All Attempts

6.1.1 User Interface Module

The user interface module is the interface presented to the security personnel managing the Security Network Operations Center.

SEC-11: The interface SHALL use https (a secure web based interface) with XML and XSL.

SEC-12: The user interface SHALL work with all of the popular web browsers.

SEC-13: The user interface SHALL be able to execute all functions within the OSS application.

SEC-14: There are no functions that must be performed via another method, such as a command line interface.

SEC-15: This interface module SHALL communicate with the subsystems and other interface modules through the use of a non-proprie tary method, such as CORBA, DCE, Sockets/XML, etc.

6.1.2 User Account Management Subsystem

User account management encompasses the addition, modification, and deletion of entities that will manage the managed network elements and the objects contained within each. User account management includes subject, subject group, subject propagation, and authorization management. There are two levels of user account management: 1) user accounts for the OSS application and, 2) user accounts for the managed network elements.

SEC-16: The account management subsystem will communicate with the other subsystems and interface modules through the use of a non-proprietary method, such as CORBA, DCE, Sockets/XML, etc.

6.1.2.1 *Subject Management*

A subject is an entity that causes information to flow among objects or changes the system state. A subject can be a person, process, or device.

SEC-17: The management of subjects SHALL include the ability to add the entity's authentication credentials.

SEC-18: The management of subjects SHALL include the ability to modify the entity's authentication credentials.

SEC-19: The management of subjects SHALL include the ability to delete the entity's authentication credentials.

(examples; user name, passwords, biological identifiers, certificates, etc.), which subject groups that subject belongs (examples; system admin, system operator, etc.), and access rules into the OSS system (examples; what functions can be performed, web, time of day, day of week, account lock-out, etc.).

6.1.2.2 *Subject Group Management*

Subject grouping is a method to define role-based access control. A subject group is an identifier for the subject. A subject may have multiple roles (belonging to multiple subject groups) within his, her, or its work definition. By assigning identifiers, if the role is no longer valid the subject's appropriate rights can be easily be removed to objects managed by that identifier. This is a must when controlling access to tens of millions of objects.

SEC-20: The management system SHALL include the ability to add subject identifiers and the privileges each identifier holds.

SEC-21: The management system SHALL include the ability to modify subject identifiers and the privileges each identifier holds.

SEC-22: The management system SHALL include the ability to delete subject identifiers and the privileges each identifier holds.

6.1.2.3 *Subject Propagation Management*

Because there will be situations where management of an object through the OSS may not be available, subjects and subject groups related information must be combined and propagated to the object. This requires the management of the distribution, modification, and removal of authentication credentials, access rules, and privileges to the object.

SEC-23: The User Management attributes SHALL be passed to the managed network element in the appropriate supported protocol, such as XML, SNMP, web interface, telnet, ftp, tftp, etc.

6.1.2.4 *Authentication Management*

Authentication includes validation of systems or users, and permissions assigned to those systems/users.

SEC-24: All authentication information that traverses a data communications network, regardless of being private or public, SHALL not travel in "clear" text or otherwise be able to be read by an eavesdropping third party.

SEC-25: IPSec SHALL be the preferred mechanism for all MNE – SMS interaction.

Application User Authentication is responsible for ensuring that when a subject claims to own a specific identity the identity can be verified as truly belonging to that subject. The subject can be:

- a human logging into an application executing within an element, or
- an application executing within one element initially communicating with a peer application executing within a different element.

This service performs:

- the initial identity authentication
- verification of authentication credentials validity, as necessary
- negotiation of any security attributes necessary for Application Data Origin Authentication, if applicable.

One example of Application Peer Entity Authentication is the "classic" log-in identifier (IDs) and log-in password for human subjects. A variation on this theme is the Radius protocol typically used for remote access. Radius can work in a simple log-in IDs and password mode or in a "Challenge/Response" mode. Another recent technique is the physical token, such as a "SecureID' or other device, which contains authentication information that may be used to authenticate the claimed identity of a human subject. The most recent technology in this space are "smart-cards"; credit card like intelligent devices that include processing capabilities and non-volatile storage for asymmetric cryptographic private keys and digital certificates of a Public Key Infrastructure (PKI).

For application process to application process some of the mechanisms based on the use of cryptographic material are:

- a digital authenticator created by producing a message digest from an application message and a shared symmetric secret key (used by many routing protocols, network service protocols such as NTPv3 and management protocols such as SNMPv3)
- Digital signatures (frequently combined with digital certificates of a PKI) as used by the Transport Layer Security (TLS) protocol, the Secure Sockets Layer (SSL) protocol, the Secure Shell (SSH) protocol replacement for FTP and Telnet. However TLS, SSL and SSH only support applications that rely on TCP

- The Kerberos security framework used either as part of the Distributed Computing Environment (DCE) or by itself with "kerberized" applications
- IPSec (including IKE, ISAKMP, AH and or ESP) by the Common Object Request Broker (CORBA) distributed application architecture.

6.1.3 Security Authentication Credentials Management Subsystem

Security Authentication Credentials Management is responsible for managing all authentication credentials related to subject identities for both human and non-human subjects. Credentials management includes the creation, assignment, storage, revocation, resetting and escrowing of credentials. These credentials include log-in passwords, asymmetric cryptographic public-private key pairs, predefined symmetric cryptographic secret key pairs, X.509v3 digital certificates and Kerberos tickets. Also part of this service are the servers used to host Radius Authentication services, Kerberos Authentication servic es, PKI Certificate and Registration Authority services and LDAP certificate repositories.

SEC-26: The security authentication credentials management subsystem SHALL communicate with the other subsystems and interface modules through the use of a non-proprietary method, such as CORBA, DCE, Sockets/XML, etc.

6.1.4 Configuration Management Subsystem

SEC-27: The configuration management subsystem SHALL communicate with the other subsystems and interface modules through the use of a non-proprietary method, such as CORBA, DCE, Sockets/XML, etc.

6.1.4.1 *Object and Object Group Management*

An object is an entity that contains or passes information. Examples of objects includes: records, blocks, pages, segments, files, directories, directory trees, programs, video displays, keyboards, clocks, printers, laptops, access points, network elements, etc. Object groups are similar objects that share common access and authorization rights; an example of an object group could be all routers within a building. Management includes the ability to places objects into trust domains.

SEC-28: The application must be able to scale to manage tens of millions of managed network elements.

6.1.4.2 *Object's Subject Rights Management*

The management of objects and object groups must include the ability to manipulate the access rights (time of day, entry method, etc.) and authorization rights (examples; read, write, delete, backup, etc.), based upon subject and subject groups. These access and authorization rights establish the rules for security functionality configuration.

SEC-29: The management of objects and object groups SHALL include the ability to add the access rights.

SEC-30: The management of objects and object groups SHALL include the ability to modify the access rights.

SEC-31: The management of objects and object groups SHALL include the ability to delete the access rights.

6.1.4.3 *Security Configuration Management*

Security functionality configuration management is responsible for providing the ability to set, modify, and reset security related configurable parameters within objects, especially object access control lists and the security policy criteria that Transport and Application Plane security services require. This service also supports the management and verification of integrity and authenticity of all software downloaded to and or installed into an object.

SEC-32: The user SHALL have the ability to enter commands in a pseudo type (Meta) language as the different type of managed network elements may not be consistent across like devices, i.e., routers from vendor A and vendor B.

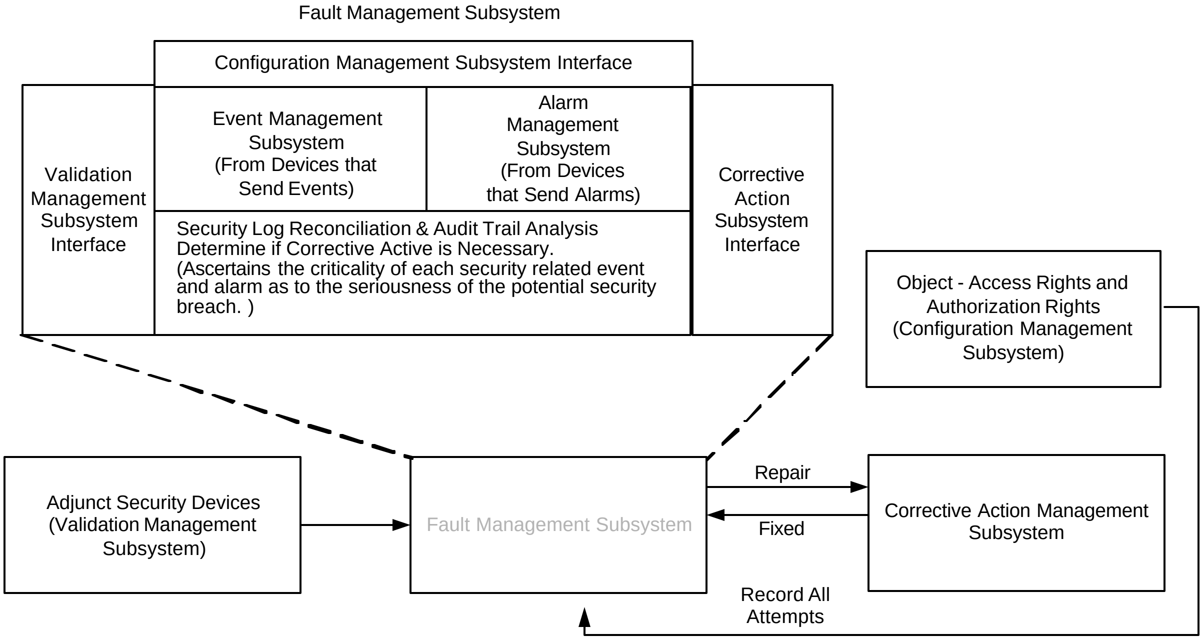
While configuration may be similar the user shouldn't need to know the exact syntax for each.

SEC-33: The OSS application SHALL pass this generic configuration commands, in XML format, from the security configuration subsystem to the interface modules for translation.

The user will enter the generic command and which objects or object groups will be targeted for that command.

In the 3 to 5 year timeframe, this function should migrate to provide security policy management where management of objects is directed by policy statements. For example, if the policy statement is "no tftp access is allowed", the policy statement is converted into the appropriate commands to modify each object that the policy would apply. To continue the example, the routers and firewalls would block access to the tftp port, the Linux based host would stop the local tftp service, the intrusion detection system would detection of the use of tftp, etc. This capability will allow for consistent security configuration and monitoring across the entire network.

6.1.5 Fault Management Subsystem


Fault Management Subsystem
Configuration Management Subsystem Interface
Event Management Subsystem (From Devices that Send Events)
Alarm Management Subsystem (From Devices that Send Alarms)
Validation Management Subsystem Interface
Security Log Reconciliation & Audit Trail Analysis
Determine if Corrective Active is Necessary.
(Ascertains the criticality of each security related event and alarm as to the seriousness of the potential security breach.)
Corrective Action Subsystem Interface
Object - Access Rights and Authorization Rights (Configuration Management Subsystem)
Adjunct Security Devices (Validation Management Subsystem)
Fault Management Subsystem
Repair
Fixed
Corrective Action Management Subsystem
Record All Attempts

SEC-34: The fault management subsystem SHALL communicate with the other subsystems and interface modules through the use of a non-proprietary method, such as CORBA, DCE, Sockets/XML, etc.

6.1.5.1 *Security Event Management*

Security Event Management subsystem is responsible for receiving security events from the Transport and Application Plane Activity Logging & Alarm Reporting services. Upon receipt these events are indexed and stored for further analysis and reporting purposes. This service is also responsible for archiving and retrieval of prior events to/from off-site long term storage. Each event will be received from the managed network element and contains certain attributes that define the event. These attributes include: the managed network element that sent the event (element name), the managed network element's IP address, and the time of the event as generated by the managed network element. This information will be used to compare to the Alarm Management subsystem's attribute table to determine the proper notification and correct action.

SEC-35: The Security Event Management subsystem SHALL be able to receive information from the following types of sources:

- **Passive logging, such as syslog and NT EventLog**
- **Active Polling, such as SNMP GET/query**
- **Active alerting, such as SNMP trap/alert**

A table of security related events is stored within the OSS application.

SEC-36: The table SHALL contain a list of each managed network element's security related events.

SEC-37: Each event SHALL contain user defined attributes.

SEC-38: These definable attributes SHALL include: the severity of the event.

6.1.5.2 *Security Related Alarm Management*

Security related alarm management is responsible for reviewing the security alarms received from the Transport and Application Plane Activity Logging & Alarm Reporting services.

SEC-39: The security related alarm management service SHALL upon receipt of alarms, index and store these alarms for further analysis.

SEC-40: The security related alarm management service SHALL upon receipt of alarms, index and store these alarms for reporting purposes.

SEC-41: The security related alarm management service SHALL be responsible for archiving and retrieval of prior alarms to/from off-site long-term storage.

6.1.5.3 *Security Log Reconciliation & Audit Trail Analysis*

Security log reconciliation & audit trail analysis are responsible for ascertaining criticality of each security related event and alarm as to the seriousness of the potential security breach each signifies. This service also provides:

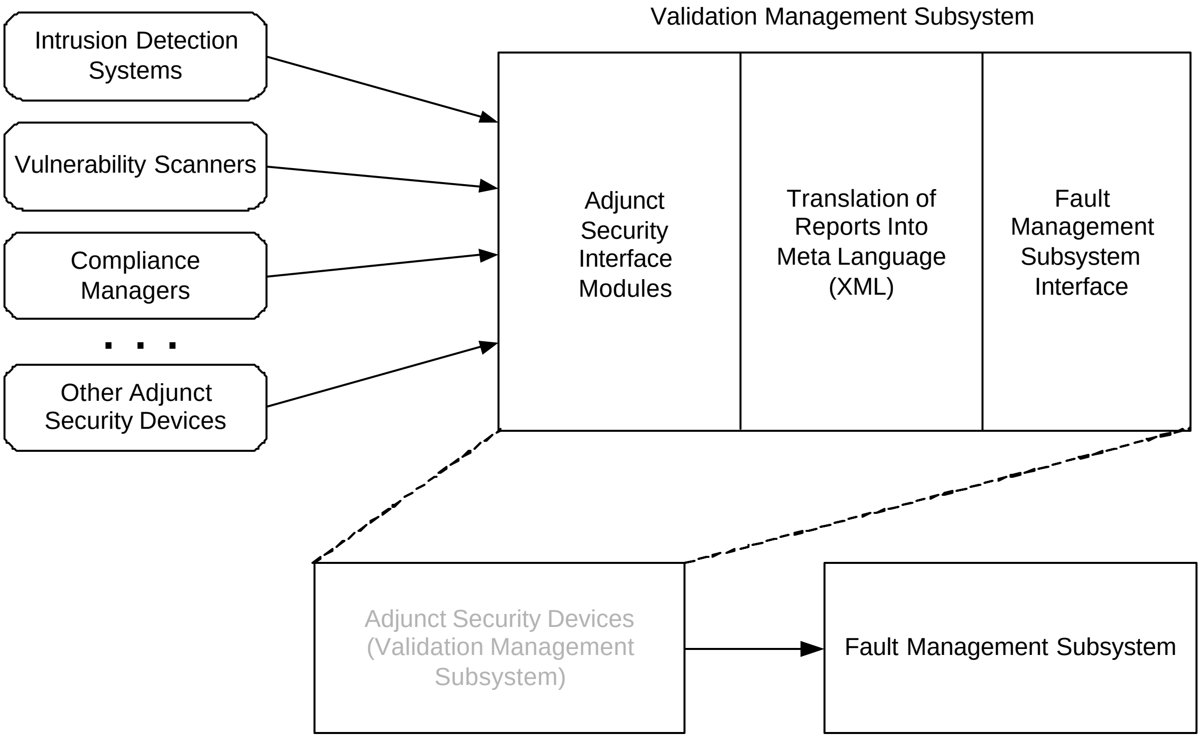
- the ability to reconcile log entries across the transport and application functional planes, as well as the operating environment logs, by time stamps and other criteria
- trend analysis capabilities
- alarm generation based on the results of statistical, and other, criteria
- definable reporting capabilities
- sending corrective action requests and receiving notification of completion of the corrective action.

SEC-42: The Security log reconciliation & audit trail analysis SHALL provide recommendations to operations personnel for ascertaining the extent of a security breach
SEC-43: The Security log reconciliation & audit trail analysis SHALL provide recommendations to operations personnel for limiting the extent of any security breach
SEC-44: The Security log reconciliation & audit trail analysis SHALL provide recommendations to operations personnel for acquisition of forensic information to support possible criminal or civil court proceedings
SEC-45: The Security log reconciliation & audit trail analysis SHALL provide recommendations to operations personnel for reestablishing normal services as quickly as possible without increasing the risk of continued or further security breaches.

6.1.6 Security Policy Management Subsystem

A function is needed to assist in or perform the reduction of security policies to security policy rules that can be interpreted by MNEs.

6.1.7 Validation Management Subsystem

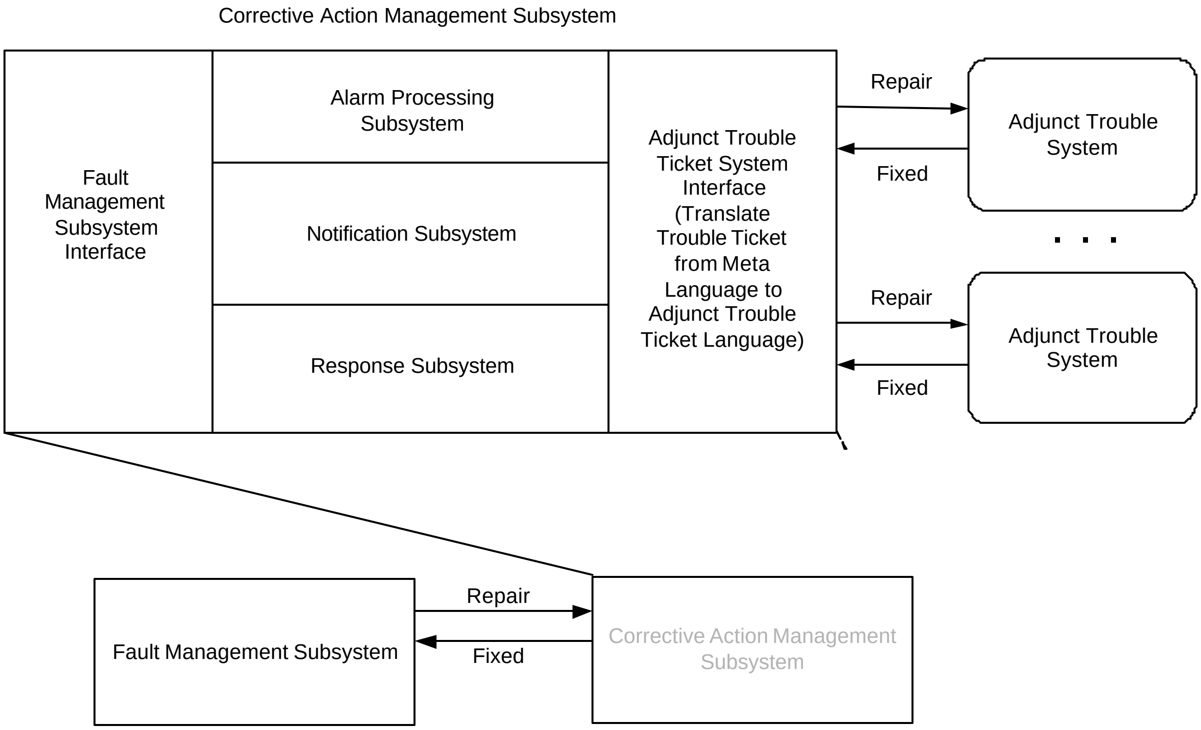

Validation Management Subsystem
Intrusion Detection Systems
Vulnerability Scanners
Compliance Managers
. . .
Other Adjunct Security Devices
Adjunct Security Interface Modules
Translation of Reports Into Meta Language (XML)
Fault Management Subsystem Interface
Adjunct Security Devices (Validation Management Subsystem)
Fault Management Subsystem

This function must receive reports through interface modules from security devices, which are adjunct to the objects; these include intrusion detection systems, intrusion prevention systems, vulnerability scanners, integrity checkers, compliance managers, etc. The information received by the Validation Subsystem is translated into the OSS application's Meta language based upon XML. These converted reports will be sent to the OSS application and indexed and stored for further analysis and reporting purposes.

SEC-46: The validation Management subsystem SHALL communicate with the other subsystems and interface modules through the use of a non-proprietary method, such as CORBA, DCE, Sockets/XML, etc.

SEC-47: The vendor of the OSS application SHALL provide an API so that adjunct security device vendors can produce an interface module for their product.

6.1.8 Corrective Action Management Subsystem


Corrective Action Management Subsystem
Fault Management Subsystem Interface
Alarm Processing Subsystem
Notification Subsystem
Response Subsystem
Adjunct Trouble Ticket System Interface (Translate Trouble Ticket from Meta Language to Adjunct Trouble Ticket Language)
Repair
Fixed
Adjunct Trouble System
. . .
Repair
Fixed
Adjunct Trouble System
Fault Management Subsystem
Repair
Fixed
Corrective Action Management Subsystem

Management of corrective action includes the ability to generate a message to a third-party produced corrective action system, i.e., Trouble Ticket System, and self-maintain its own trouble ticket system.

SEC-48: The corrective action management subsystem SHALL have a configurable table of alarms that can be received from the Fault Management Subsystem

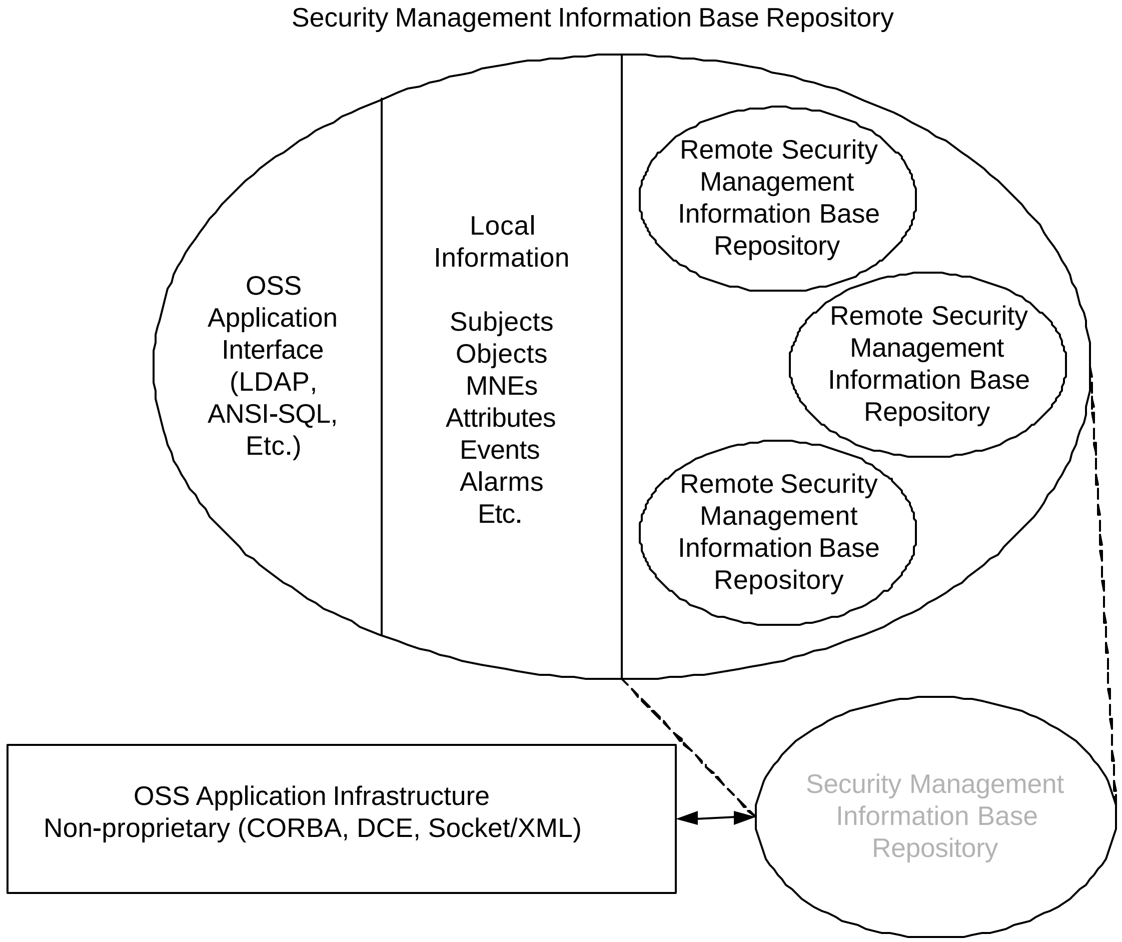
SEC-49: The corrective action management subsystem's configurable table of alarms SHALL be populated from the Fault Management Subsystem

SEC-50: The corrective action management subsystem's configurable table of alarms SHALL be able to receive corresponding attributes from the Fault Management Subsystem as to where the information is to be forwarded

The information sent to the corrective action system identifies which objects need correction, the reason for the correction, and suggested repairs for the object. Once the object has been repaired, the OSS must be able to receive a security related event that indicates that the object has been repaired or notification that the correction can not be made due to a negative impact on the production environment.

SEC-51: Reports from the corrective action system SHALL be stored as part of the Fault Management subsystem for further analysis and reporting purposes.

6.1.9 Security Management Information Base Repository


Security Management Information Base Repository
OSS Application Interface (LDAP, ANSI-SQL, Etc.)
Local Information
Subjects
Objects
MNEs
Attributes
Events
Alarms
Etc.
Remote Security Management Information Base Repository
Remote Security Management Information Base Repository
Remote Security Management Information Base Repository
OSS Application Infrastructure
Non-proprietary (CORBA, DCE, Socket/XML)
Security Management Information Base Repository

SEC-52: The Security Management Information Base Repository SHALL be an ANSI-SQL or LDAP accessible database.

SEC-53: The security management information base Repository SHALL contain each managed network element's security attributes.

SEC-54:The security management information base Repository's attributes SHALL contain

- **the name of the attribute**
- **the current value of the attribute**
- **the allowable values or ranges for the attribute**
- **the subject groups that can access the attribute**
- **the rights of each subject group to the attribute**
- **the event type for each change of the attribute value**

. The OSS application communicates with the repository through the use of appropriate non-proprietary protocols , such as LDAP or ANSI-SQL.

SEC-55: The repository SHALL have the ability to know where information is stored (local vs. remote)

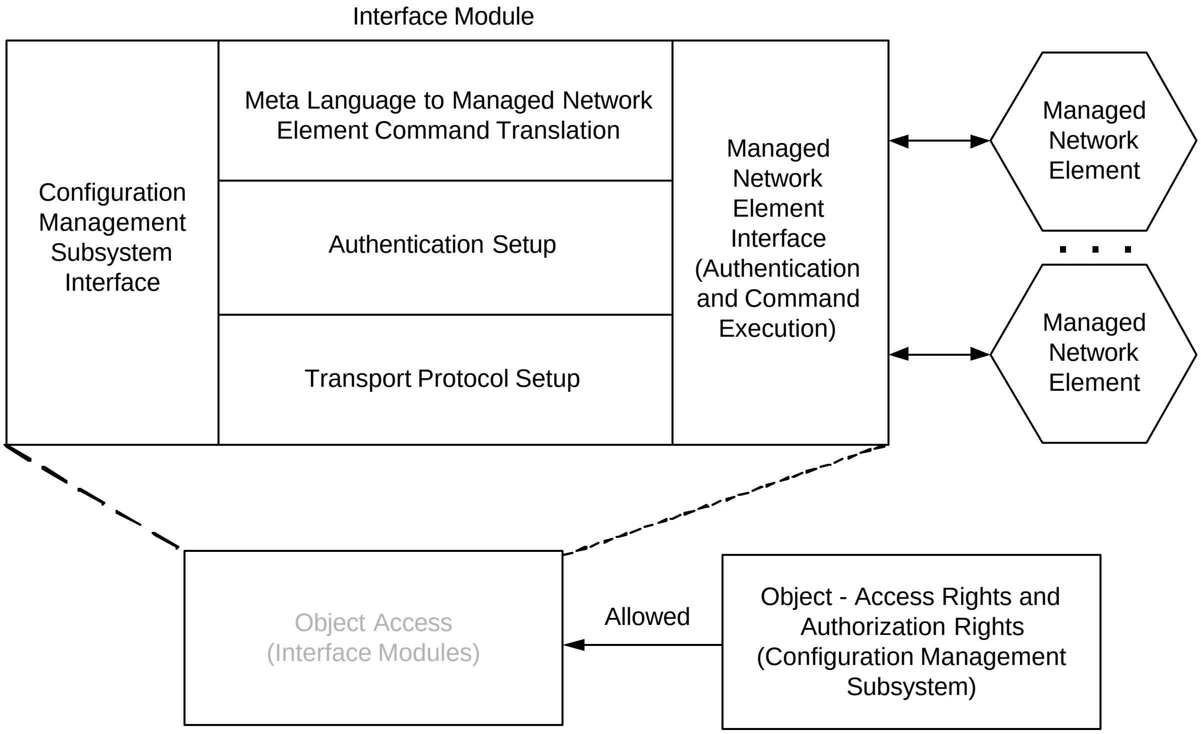
SEC-56: The repository SHALL be able to add information at the storing location.

SEC-57: The repository SHALL be able to modify information at the storing location.

SEC-58 The repository SHALL be able to delete information at the storing location, modified,

SEC-59 The repository may be front-ended by an intermediary that can perform some of the mandatory responsibilities.

6.1.10 Interface Modules


Interface Module
Configuration Management Subsystem Interface
Meta Language to Managed Network Element Command Translation
Authentication Setup
Transport Protocol Setup
Managed Network Element Interface (Authentication and Command Execution)
Managed Network Element
. . .
Managed Network Element
Object Access (Interface Modules)
Allowed
Object - Access Rights and Authorization Rights (Configuration Management Subsystem)

Interface Modules convert the generic configuration statements defined in the Configuration Management subsystem into the specific commands for each vendor's managed network element. The commands are passed to the managed network element in the appropriate supported protocol, such as IP, X.25, XML, SNMP, web interface, telnet, ftp, tftp, etc.

SEC-60: The interface module will communicate with the subsystems and other interface modules through the use of a non-proprietary method, such as CORBA, DCE, Sockets/XML, etc.

SEC-61: The Interface Module SHALL setup the authentication request to the managed network element and authenticate itself prior to the execution of the commands.

SEC-62: The OSS application SHALL have a supported API so that vendors of managed network elements may supply their own interface modules.

SEC-63: The vendor of the OSS application SHALL provide an API so that managed network element vendors can produce an interface module for their product.

Appendix I Semantics of Terms Used in this Document

Table 7 - **Definitions** used within this document

Access	A specific type of interaction between a subject and an object that results in the flow of information from one to the other. Possible information flows include the transfer of attributes pertaining to that object, the transfer of data pertaining to that object, or the fact of existence of that object. [POSIX.6]
access control	The prevention of unauthorized use of a resource including the prevention of use of a resource in an unauthorized manner. [ISO 7498-2]
access control list (ACL)	A list of entities, together with their access rights, which are authorized to have access to a resource. [ISO 7498-2]
Accountability	The property that ensures that the actions of an entity may be traced to that entity. [ISO 7498-2]
active threat	The threat of a deliberate unauthorized change to the state of the system. Note: Examples of security-relevant active threats may be: modification of messages, replay of messages, insertion of spurious messages, masquerading as an authorized entity and denial of service. [ISO 7498-2]
Advanced Encryption Algorithm (AES)	A new symmetric data encryption standard developed under the auspices of the United States Government as a replacement for DES. AES uses a variable length key to perform a series of nonlinear transformation on a 64 bit data block.
asymmetric authentication method	Method for demonstrating knowledge of a secret, in which not all authentication information is shared by both entities. [ISO 10181-2]
audit record	The discrete unit of data reportable in an audit trail on the occurrence of an audit event. [POSIX.6]
audit trail	See Security Audit Trail [ISO 7498-2]
Authenticate	To establish the validity of a claimed identity. [POSIX.6]
authenticated identity	An identity of a principal that has been assured through authentication. [ISO 10181-2]
Authentication	See data origin authentication, and peer entity authentication. The property of knowing that the data received is the same as the data that was sent, and that the claimed sender is in fact the actual sender. [ISO 7498-2]
authentication information	Information used to establish the validity of a claimed identity. [ISO 7498-2]
Authorization	The granting of rights, which includes the granting of access based on access rights. [ISO 7498-2]
Certificate	A security certificate, as defined in [ISO 10181-1]. [ECMA-219]
Ciphertext	Data produced through the use of encipherment. The semantic content of the resulting data is not available. Note: Ciphertext may itself be input to encipherment, such that super-enciphered output is produced. [ISO 7498-2]
clear-text	Intelligible data, the semantic content of which is available.

Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO 7498-2]
Credentials	Data that is transferred to establish the claimed identity of an entity. [ISO 7498-2]
Cryptanalysis	The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including clear-text. [ISO 7498-2]
Cryptography	The discipline which embodies principles, means, and the methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. [ISO 7498-2]
data integrity	The property that data has not been altered or destroyed in an unauthorized manner. [ISO 7498-2]
Decipherment	The reversal of a corresponding reversible encipherment. [ISO 7498-2]
Decryption	See Decipherment. [ISO 7498-2]
denial of service	The prevention of authorized access to resources or the delaying of time-critical operations. [ISO 7498-2]
DES (Data Encryption Standard)	A data encryption standard developed by IBM under the auspices of the United States Government. DES uses a 56 bit key to perform a series of nonlinear transformation on a 64 bit data block. Even when it was first introduced a number of years ago, it was criticized for not having a long enough key. 56 bits just didn't put it far enough out of reach of a brute force attack. Today, with the increasing speed of hardware and its falling cost, it is feasible to build a machine that can crack a 56 bit key in under an hour.
digital signature	Data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery. [ISO 7498-2]
Encipherment	The cryptographic transformation of data (see cryptography) to produce ciphertext. Note Encipherment may be irreversible, in which case the corresponding decipherment process cannot feasibly be performed. [ISO 7498-2]
Encryption	See encipherment. [ISO 7498-2]
end-to-end encipherment	Encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system. (See also link-by-link encipherment.) [ISO 7498-2]
hash function	A function that maps values from a (possibly very) large set of values to a smaller range of values. [ISO 10181-1], see MD-5 and SHA-1.
Host	A computer system attached to a network.
human/computer interface	The boundary across which physical interaction between a human being and the application platform takes place. [POSIX.0/D15]
Initiator	An entity (e.g., human user or computer based entity) that attempts to access other entities. [ISO 10181-3]
Integrity	The prevention of the unauthorized modification of information. [ITSEC-1.2]
Key	A sequence of symbols that controls the operations of encipherment and decipherment. [ISO 7498-2]

key management	The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy. [ISO 7498-2]
Known Plain Text Attack	A method of attack on a crypto system where the cryptanalyst has matching copies of plain text, and its encrypted version. With weaker encryption systems, this can improve the chances of cracking the code and getting at the plain text of other messages where the plain text is not known.
least privilege	The principle of granting only such access rights as are required for subjects to perform their authorized tasks. [CESG-1-1.2]
Masquerade	The pretence by an entity to be a different entity. [ISO 7498-2]
MD5 (Message Digest Algorithm #5)	The message digest algorithm used in PGP is the MD5 Message Digest Algorithm, placed in the public domain by RSA Data Security, Inc.
non-repudiation	The property of a receiver being able to prove that the sender of some data did in fact send the data even though the sender might later deny ever having sent it.
Object	A passive entity within a system that contains or receives information. Examples: records, blocks, pages, segments, files, etc. [CESG-1-1.2], See also: Subject
one-way encryption	A method of encryption used where a requirement exists to prevent the decryption of the cipher text, given full information about the algorithm. Note: Often used for encryption of passwords and integrity checksums. [CESG-1-1.2]
one-way function	A function which is easy to compute but whose inverse is computationally intractable. [ISO 10181-1]
owner	User granted privileges with respect to security attributes and privileges affecting specific subjects and objects.
passive threat	The threat of unauthorized disclosure of information without changing the state of the system. [ISO 7498-2]
Password	Confidential authentication information, usually composed of a string of characters. [ISO 7498-2]
PC	Personal Computer
peer-entity authentication	The corroboration that a peer entity in an association is the one claimed. [ISO 7498-2]
physical security	The measures used to provide physical protection of resources against deliberate and accidental threats. [ISO 7498-2]
Policy	See: Security Policy. [ISO 7498-2]
principle of least privilege	A security design principle that states that a person, process, or program be granted only those privileges necessary to accomplish a legitimate function, and only for the time that such privileges are actually required. The proper application of this principle limits the damage that can result from accident, error, or unauthorized use of available privileges by a process. [POSIX.6]
Privacy	The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. Note: because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring

	security. [ISO 7498-2]
private key	A key used in an asymmetric algorithm. Possession of this key is restricted, usually to only one entity. [ISO 10181-1]
Privilege	See: Access Right. [CESG-1-1.2]
public key	The key, used in an asymmetric algorithm, that is publicly available. [ISO 10181-1]
Repudiation	Denial by one of the entities involved in a communication of having participated in all or part of the communication. [ISO 7498-2]
resource	Anything used or consumed while performing a function. The categories of resources are: time, information, objects (information containers), or processors (the ability to use information). Specific examples are: CPU time; terminal connect time; amount of directly-addressable memory; disk space; number of I/O requests per minute, etc. [TCSEC]
Risk	The likelihood that a successful attack will be mounted against a computer system. Risk is a function of both vulnerability and threat. [CESG-1-1.2]
Role	The description of a user's sphere of responsibility. Note: May be used for enforcing access control in accordance with the principle of least privilege. Example: System Administrator. [CESG-1-1.2]
RSA	RSA is the public key (asymmetric) encryption method used in PGP and most Public Key Infrastructure systems. R, S and A are the initials of the developers of the algorithm (Rivest, Shamir and Adleman). The basic security in RSA comes from the fact that, while it is relatively easy to multiply two huge prime numbers together to obtain their product, it is computationally difficult to go the reverse direction: to find the two prime factors of a given composite number. It is this one-way nature of RSA that allows an encryption key to be generated and disclosed to the world, and yet not allow a message to be decrypted. [RFC1321]
secret key	The key shared between two entities in a symmetric cryptographic algorithm. [ISO 10181-1]
Security	The protection of computer hardware, software, and data from accidental or malicious access, use, modification, destruction, or disclosure. Tools for the maintenance of security are focused on availability, confidentiality, and integrity. [POSIX.0/D15]
security audit	An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures. [ISO 7498-2]
security audit record	A single record in a security audit trail corresponding to a single security-related event. [ISO 10181-7]
security audit trail	Data collected and potentially used to facilitate a security audit. [ISO 7498-2]
security certificate	A set of security relevant data which is protected by integrity and data origin authentication via an issuing security authority, and includes an indication of a time period of validity. Note: All certificates are deemed to be security certificates

	(see the relevant definitions in ISO 7498-2). [ISO 10181-1]
security object	An entity in a passive role to which a security policy applies. [ECMA TR/46]
security policy	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. [POSIX.6]
security subject	An entity in an active role to which a security policy applies. [ECMA TR/46]
SHA	Secure Hash Algorithm
Signature	See Digital Signature. [ISO 7498-2]
Subject	An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Examples: process, executing program. See also: Object. [TCSEC]
subject authority	An authority recognized in a Security Domain as a trusted source of security information concerning security subjects (human beings and Applications). [ECMA-219]
symmetric authentication method	Method for demonstrating knowledge of a secret, in which both entities share a common authentication information. [ISO 10181-2]
Target	An entity to which access may be attempted. [ISO 10181-3]
Threat	The likelihood of an attack being mounted against a computer system. [CESG-1-1.2]
Trust	A relationship between two elements, a set of activities and a security policy in which element X trusts element Y if and only if X has confidence that Y will behave in a well defined way (with respect to the activities) that does not violate the given security policy. [ISO 10181-1]
trusted third party	A security authority or its agent, trusted by other entities with respect to security-related activities. In the context of this standard a trusted third party is trusted by a claimant and/or verifier for the purposes of authentication. [ISO 10181-2]
unprivileged subject	A subject without appropriate privileges to perform an operation. [POSIX.6]
User	Any person who interacts with a computer system. [POSIX.6] See subject.
user identifier (User ID)	Unique symbol or character string that is used by an IT product to uniquely identify a specific user.

APPENDIX II Detail Relationship of Security Management Concepts to ISO 7498-2

Clause 8 of ISO 7498-2 addresses many aspects of security management for open systems interconnection. The ISO 7498-2 security management structure is adopted as the basis for the infrastructure security architecture and is extended to apply to all aspects of open systems security management.

II.1.1 Trust Domains

ISO 7498-2 begins its security management discussion by considering security policy and security domains (clause 8.1.2): There can be many security policies imposed by the administration(s) of distributed open systems and Open Systems Interconnection (OSI) security management standards should support such policies. Entities that are subject to a single security policy, administered by a single authority, are sometimes collected into what has been called a "security domain".

In the TSP environment, trust domain is substituted for security domain. Some of the future extensions noted above have been included in the OSI Security Frameworks Overview, ISO 10181-1 (ISO, 1995c). The Frameworks Overview allows, but does not require, security domains to have subset and superset relationships. The TSP security architecture does allow trust domains to be hierarchically related, and so has need for the subset and superset notions.

II.1.2 Security Management Information Bases

ISO 7498-2 (clause 8.1.4) describes security management information bases as follows:

"The Security Management Information Base (SMIB) is the conceptual repository for all security-relevant information needed by open systems. This concept does not suggest any form for the storage of the information or its implementation. However, each MNE must contain the necessary local information to enable it to enforce an appropriate security policy. The SMIB is a distributed information base to the extent that it is necessary to enforce a consistent security policy in a (logical or physical) grouping of MNEs. In practice, parts of the MIB may or may not be integrated with the SMIB."

The TSP security architecture uses SMIBs to conduct trust domain and MNE management, rather than for only MNE management as implied above by the appropriate security policy for each MNE. A distinct security management trust domain may be responsible for the management of a single trust domain (1:1) or several trust domains (1:many), or the trust domain may contain its security management trust domain (embedded). The SMIB in these cases, respectively, contains security information for the single trust domain, contains security information for all of the several trust domains, or is contained in the trust domain with its information objects. In the 1:many case, the trust domains may or may not be related to the same service or function. This flexibility allows a security administrator (or group of security administrators) to manage more than one trust domain from the same SMIB. Also, it implies that each security administrator has the same attributes (privileges) with respect to the security management information of all of the trust domains that share a management trust domain. (However, not every security administrator necessarily has the same attributes as the other security administrators in other areas.)

II.1.2.1 Trust Domain SMIB Content

The following examples of information objects might be placed in a SMIB to manage a trust domain:

- Trust domain security policy rules
- Member registration information
- Member authentication criteria (e.g., strength of mechanism required)

- Member authentication information
- Member attributes (privileges) (e.g., access privileges, release authority for inter-domain transfers)
- Visible security label information (i.e., what label, if any, is attached to information that is printed or displayed)
- Security service and security mechanism requirements for specific applications, including intra-domain communications and inter-domain information transfer.

II.1.2.2 Managed Network Element SMIB Content

The MNE SMIB contains information for management of security functions and resources shared by several trust domains, including hardware resources, security-critical functions (particularly security services and mechanisms), and supporting applications (e.g., key management). More detail is given in later sections on several of the supporting security applications and related functions. The following example classes of information objects might be included in the SMIB:

- Trust Domain security policy rules
- Security services management information (see Section 5.2.7)
- Security mechanisms management information (see Section 5.2.8)
- Supporting services and mechanisms management information (e.g., alarm reporting, information system auditing, cryptographic key distribution, security contexts, security-critical functions, security-related applications).

II.1.2.3 SMIB Examples

Information is required in the MNE SMIBs and the trust domain SMIBs to support secure infrastructure operations. Trust domain SMIB information items include:

- X.509 certificates to carry appropriate security information, such as subject identity authentication certificates and subject access privilege certificates
- User access control information for distributed operations not already contained in certificates
- Manually distributed Traffic and message shared secret keys
- User account information not already contained in certificates (such as group memberships, demographic information)
- Accumulated security log, event and audit data.
- MNE security related configuration data for those security services supported within each MNE within the TSP infrastructure. This information will include, for each MNE, object access control lists, network layer packet filtering rules, application layer message filtering rules, Key management, encryption, integrity, and signature algorithm identifiers, and security protocol objects for both MNE-SAs and APP-SAs, MNE-SA default parameters, MNE-SA options, APP-SA default parameters, APP-SA options, security event reporting parameters, security log management parameters, etc.

MNE SMIB security information items include:

- Key management, encryption, integrity, and signature algorithm identifiers, and security protocol objects
- MNE access control information
- Encryption algorithm initialization information
- Security association configuration information
- Compromise action information (e.g., revoked certificates lists)
- Contingency plan parameters (e.g., auto-purge and security policy replacement actions under emergency conditions).

Some SMIB items may be held in Directory Servicers for ease of access by many users. Such items might include key management information (e.g., certificates and user keying material). SMIB information stored in X.500 Directories must be integrity protected.

II.1.3 Communication of Security Management Information

ISO 7498-2 (clause 8.1.5) observes the following about the communication of security management information:

"Management protocols, especially security management protocols, and the communication channels carrying the management information, are potentially vulnerable. Particular care must therefore be taken to ensure that the management protocols and information are protected such that the security protection provided for usual instances of communication is not weakened."

Security management information will be protected in accordance with the security policy of each management trust domain. Management applications used to communicate security management information will rely upon the same protocol infrastructure as other applications. Management applications operate in security contexts. Security associations that ensure secure communications between security contexts in different MNEs are described in Section 6.

Interactive distributed security exists when two different MNEs are joined securely using a set of mechanisms that is referred to as Security Associations (SAs). The TSP security architecture utilizes two different types of SAs:

1. Inter-MNE security associations
2. Inter-application process security associations

II.1.3.1 Inter-MNE security associations (MNE-SAs)

MNE-Sas ensure secure communication between the two MNEs engaged in communication. These MNE-SAs provide continuous MNE data origin authentication, data integrity and optional message level confidentiality. The TSP security architecture relies on the capabilities within the IETF IPSec protocol suite for the establishment of MNE-SAs.

II.1.3.2 Inter-application process security associations (APP-SAs)

APP-SAs ensure secure communication between a pair of application processes executing within different MNEs. These APP-SAs provide peer-entity authentication and selective field data confidentiality. The TSP security architecture relies on the capabilities within existing application layer protocols for establishment of MNE-SAs. APP-SAs between two MNEs may share the same cryptographic algorithm and keys used by an MNE-SA or use different MNE-SAs between the two communication MNEs. The choice of which APP-SA to MNE-SA arrangement must be specifiable for interactive communication within the same trust domain or between different trust domains.

The security management information for a security association is contained in a SMIB and includes all the security-relevant attributes required to establish and maintain a security association, such as the trust domain label and secure communications attributes (e.g., cryptographic algorithm identifiers and keys).

Making a decision about whether to allow establishment of a security association may require several related functions to be performed such as the exchange and processing of security attributes of the user or MNE (e.g., authenticated identity, access privileges). These attributes might be contained in a security certificate such as that defined in the X.509 Directory Services Authentication Framework (CCITT, 1992). The information contained in an X.509 certificate may be signed by any number of hierarchically related certificate-issuing authorities, down to a trust domain-specific certificate-issuing authority if that level of granularity is required. This signature verification adds greater assurance to the credibility of the information contained in the certificate.

II.1.4 Distributed Security Management Administration

ISO 7498-2 (clause 8.1.6) describes distributed security management administration:

"Security management may require the exchange of security-relevant information between various system administrations, in order that the SMIB can be established or extended. In some cases, the security-relevant information will be passed through non OSI ["out-of-band"] paths, and the local systems administrators will update the SMIB through not standardized by OSI [direct interaction with the MNE]. In other cases, it may be desirable to exchange such information over a n OSI communication path in which case the information will be passed between two security management applications running in the MNEs. The security management application will use the communicated information to update the SMIB. Such updating of the SMIB may require the prior authorization of the appropriate security administrator."

The TSP security architecture is consistent with this view and uses it as the basis for TSP distributed security management. Each management trust domain uses and maintains the SMIB for the trust domain it manages. Cooperation with local administrators may be necessary for functions that cannot be managed remotely (e.g., aspects of key management that require physical access and personal accountability dictated by administrative and environmental considerations).

When a distributed approach for management of information systems is used, the distributed management functionality is responsible for managing MNEs within the transport plane and, at the same time, relies upon the Transport Plans MNEs for correct transport operation. Management systems will rely upon the same Transport Plane security structures (security services, security associations, and security protocols) as any other application.

When distributed information systems become very large, their management becomes very complex. To make the complexity manageable, hierarchical management approaches are often adopted. It then becomes necessary to coordinate the levels of delegated management authority. The coordination is achieved by the way management information is organized and through the control of that information as required by security policies. Hierarchical management relationships are not reflected in the way management applications communicate with one another. That is, management protocols are peer oriented, not hierarchically related. When the term hierarchical management system is used, it must be understood that a set of information relationships is being described, not a communications structure. This means that the hierarchical aspect of management is a human, organizational function. The organizations, administrators and management systems may be organized hierarchically, but the MNEs in which management applications are implemented only communicate as peers.

Management systems are composed of management applications implemented in MNEs. Some management applications must coexist with other applications in MNEs within the Managed Element Layer of the TMN model. For logistical reasons it is necessary to dedicate some MNEs to management system activities. This is especially true at the Element, Network, System and Business Management Layers of the TMN model. Management systems can be grouped into categories based on the particular type of management function being performed. While these categories are logically separate, they often support one another. The categories are:

- Element Management
- Network Management
- Service Management (which includes Security Management)
- Business Management.

Traditional element and network management systems are located within network control centers that monitor and configure network components, perform fault isolation functions, manage MNE configuration attributes, and collect accounting and performance information. Security management systems typically provide information to support security services and mechanisms in all MNEs.

II.1.4.1 Security Management Application Protocols

ISO 7498-2 (clause 8.1.7) requires security management application protocols for exchange of security-relevant information. The general management application protocols used within the TSP security architecture are CORBA and SNMP.

II.1.4.2 MNE Security Management Functions

ISO 7498-2 (clause 8.2.1) observes the following about system security management:

System security management is concerned with the management of security aspects of the overall environment. The following list is typical of the activities, which fall into this category of security management:

- overall security policy management, including updates and maintenance of consistency;
- interaction with other management functions;
- interaction with security service management and security mechanism management;
- event handling management;
- security audit management; and
- security recovery management.

As noted previously, the TSP security architecture broadens the view of MNE security management to the entire systems environment, especially with respect to the support of multiple trust domains. The topics of event handling, security audit, and security recovery management are interrelated and will be treated together.

ISO 7498-2 (clause 8.3.1) describes event-handling management as follows:

The management aspects of event handling visible in OSI are the remote reporting of apparent attempts to violate system security and the modification of thresholds used to trigger event reporting.

ISO 7498-2 (clause 8.3.2) describes security audit management as follows:

Security audit management may include:

- the selection of events to be logged and/or remotely collected;
- the enabling and disabling of audit trail logging of selected events;
- the remote collection of selected audit records; and,
- the preparation of security audit reports.

ISO 7498-2 (clause 8.3.3) describes security recovery management as follows:

Security recovery management may include:

- maintenance of the rules used to react to real or suspected security violations;
- the remote reporting of apparent violations of system security; and
- security administrator interactions.

These security functions are related since the event handling function deals with all the apparent security violations recognized by an MNE, the audit function selects those events that will be recorded, and the recovery function acts upon some of the selected events. The selection of audited events and those requiring a recovery action is determined by trust domain security policies or by the MNE security policy.

Event handling includes local as well as remote reporting of security-related events. Depending on whether a management entity (a security manager or a security recovery application) or a user is expected to examine or act on various alarms or audit records, alarm or audit information objects may be recorded in a particular management trust domain SMIB, an MNE SMIB, or a user-accessible file in a trust domain.

Security recovery actions might include terminating a particular security context, temporarily prohibiting certain activities within a trust domain, or disabling a particular communications interface. Some security recovery actions may depend on specialized data structures, such as a compromised cryptographic key material list, which controls continued use of key materials.

II.1.4.3 Security Service Management

ISO 7498-2 (clause 8.2.2) describes security service management as follows:

Security service management is concerned with the management of security services. The following list is typical of the activities performed in managing a security service:

- Determination and assignment of the target security protection for the service
- Assignment and maintenance of rules for the security mechanism to be employed to provide the requested security service
- Negotiation (locally and remotely) of available security mechanisms which require prior management agreement
- Invocation of specific security mechanisms via the appropriate security mechanism function, e.g., for the provision of administratively-imposed security services
- Interaction with other security service management functions and security mechanism management functions
- Generation, collection, filtering, consolidation and evaluation of security related events and alarms and
- Retrieval, correlation and analysis of MNE security logs.

A trust domain security policy may be very specific about how security service requirements are to be met (by mandating particular security mechanisms). Alternatively, it may give only a general requirement for a security service of a particular strength and allow the SMAP to select an appropriate mechanism from those available. Each of the activities in the list above is concerned with an aspect of determining how security service requirements are satisfied by security mechanisms, as discussed below.

II.1.4.3.1 Determining and Assigning Strength of Service

Determining security services to be used and their strength is one aspect of developing a security policy for a trust domain or an MNE. The choices made are dependent on threats, vulnerabilities, and acceptable risk. That is, for large classes of information processing activities, a single determination of required security services can be made in advance because the value of the information being protected does not change often or quickly, nor do the vulnerabilities and risk. There are other classes of information activities for which it may be appropriate to choose whether or not to employ a particular security service. For example, within the same trust domain, some electronic mail messages may be of an informal or personal nature and not require a non-repudiation service, but other messages may be official business and may be required (by written policy) to employ a non-repudiation service. In cases like this, a selective means of invoking the security service must be available, but the strength of the service is likely to be predetermined.

II.1.4.3.2 Assigning and Maintaining Rules for Mechanism Selection

For a given security service, one or more security mechanisms, alone or in combination with others, may be able to implement it. Some security mechanisms may be able to support more than one security service.

One of the aspects of the principle of protection is that the security services chosen within a trust domain security policy each have a minimum strength associated with them. Not all the security mechanisms that support a given security service need to be provided within MNEs. In particular, the MNE may employ various administrative and environmental security mechanisms that contribute to the provision of one or more security services. As a result, the security mechanisms that support a given security service may be different when protecting information within an MNE than when protecting information between MNEs within the same trust domain or between MNEs in different trust domains. The resulting security service implementations must provide at least the minimum protection demanded by the security policy in all situations. Thus, to the extent that an MNE supports security services with different mechanisms and a SMAP is aware (or can be made aware) of the distinctions among activities within a trust domain, between MNEs in the same trust domain, and between MNEs in different trust domains, alternate choices of security mechanisms could be made.

The added complexity involved in making such choices might lead information system security architects to use only one set of mechanisms that satisfies a trust domain security policy in all cases. However, in some situations this strategy would not be appropriate. For example, if some MNEs in the same trust domain often exchange large files, but only infrequently with MNEs in different trust domains, a confidentiality mechanism necessary in the latter case might introduce an unacceptable performance penalty in the local situation, but administrative and environmental mechanisms could be relied upon to achieve the required level of protection.

II.1.4.3.3 Negotiating Available Security Mechanisms

One or more MNEs that support the same trust domain may be able to support a particular security service with more than one security mechanism, but it may not be known in advance of attempted communications which of these security mechanisms may be implemented in a specific MNE. In such cases, the specific security mechanisms to be employed must be negotiated between the security services in the MNEs at the time the security association is established between them.

II.1.4.3.4 Invoking Security Mechanisms

The invocation of security services and security mechanisms within the TSP security architecture involves several functions. Most applications will rely upon the resident operating system for use of a security service. If a request for a security service does not specify a security mechanism, the SMAP makes a choice among the available security mechanisms based on the trust domain policy and invokes it through an appropriate operating system call. Otherwise, the SMAP invokes the default security mechanism.

Although each application could make requests for security services and security mechanisms directly to the SMAP, there are significant advantages to adopting an Application Program Interface (API) approach. APIs provide a common set of subroutine calls to a related set of programming functions or services. An API not only relieves application designers of creating a specific set of interfaces, but also allows underlying services to be replaced (by equivalent mechanisms) without affecting the application implementation. Various efforts are defining APIs for the invocation of security mechanisms. One such effort is the General Security Service (GSS) API intended for use with the

Internet suite of communications protocols (Linn, 1993). The GSS API and other related APIs could be used to invoke all security functions by making them the standard interfaces to the SMAP (they could be incorporated into the SMAP).

The use of a combination of the GSS API, SMAPs, and the standard kernel interface can contribute to the independence of security services and security mechanisms and to their transparency to users and applications. This independence allows different security mechanisms to be accommodated at various stages in an MNE life cycle, and for MNEs to accommodate trust domains with different security service requirements.

II.1.4.4 Security Mechanism Management

ISO 7498-2 (clause 8.2.3) describes security mechanism management as follows:

Security mechanism management is concerned with the management of particular security mechanisms. The following list of security mechanism management functions is typical but not exhaustive:

- Key management
- Encryption management
- Digital signature and authenticator management
- Access control management
- Data integrity management
- Authentication management
- Traffic padding management
- Routing control management
- Notarization management and
- Availability management

The TSP security architecture adopts this list and adds availability management.

II.1.4.4.1 Key Management

ISO 7498-2 (clause 8.4.1) describes key management as follows:

Key management may involve:

- Generating suitable keys at intervals commensurate with the level of security required
- Determining, in accordance with access control requirements, of which entities should receive a copy of each key and
- Making available or distributing the keys in a secure manner to entity instances in real open systems.

It is understood that some key management functions will be performed outside the OSI environment. These include the physical distribution of keys by trusted means.

Exchange of working keys for use during an association is a normal layer protocol function. Selection of working keys may also be accomplished by access to a key distribution center or by pre-distribution via management protocols or manual means.

The TSP security architecture relies upon standard key management techniques, specifically the Internet Key Exchange (IKE) Protocol and the Internet Security Association Key Management Protocol (ISAKMP) within the IETF IP security (IPSec) suite of protocols.

II.1.4.4.2 Encryption Management

ISO 7498-2 (clause 8.4.2) describes encryption (encipherment) management as follows:

Encryption management may involve:

- Interaction with key management
- Establishment of cryptographic parameters and
- Cryptographic synchronization.

The existence of an encryption mechanism implies the use of key management and of common ways to reference the cryptographic algorithms.

The degree of discrimination of protection afforded by encryption is determined by which entities within the environment are independently keyed. This is in turn determined, in general, by the security architecture and specifically by the key management mechanism.

A common reference for cryptographic algorithms can be obtained by using a register for cryptographic algorithms or by prior agreements between entities.

It is expected that new cryptographic products will support multiple algorithms that can be selected by each application. In such an environment, the registration of cryptographic algorithms will be necessary so that algorithm selection can be negotiated between MNEs. The ability to select a cryptographic algorithm has implications for the security management of the devices involved, such as determining under what conditions an algorithm can be employed and for auditing algorithm use.

The creation of distributed security services, which provide communications and information security, is usually dependent on cryptographic mechanisms. Thus, the availability of low-cost cryptographic capabilities is a critical element of the TSP security architecture. These cryptographic capabilities must be sufficiently flexible to support requirements of different trust domains in the same MNE.

This flexibility will be achieved if the mechanisms accommodate multiple cryptographic algorithms and multiple key management schemes, including public key encryption schemes and various key distribution center schemes. Otherwise, a multiplicity of cryptographic devices will be needed, resulting in increased costs. To manage these devices, there must be a registry of cryptographic algorithms and key management schemes so that the specific choices can be negotiated for a particular security association.

II.1.4.4.3 Digital Signature and Authenticator Management

ISO 7498-2 (clause 8.4.3) describes digital signature management as follows:

Digital signature management may involve:

- Interaction with key management
- Establishment of cryptographic parameters and algorithms and
- Use of protocols between communicating entities and possibly a third party.

There exist strong similarities between digital signature management, digital authenticator management and encryption management.

When digital signatures support a non-repudiation service that relies upon a trusted third party, additional security management responsibilities may be added with respect to long-term archiving of keys and algorithm identifiers so that transactions can be verified well after they occur.

II.1.4.4.4 Access Control Management

ISO 7498-2 (clause 8.4.4) describes access control management as follows:

Access control management may involve distribution of security attributes or updates to access control lists or capabilities lists. It may also involve the use of a protocol between communication entities and other entities providing access control services.

The distribution of security attributes includes their initial installation in a SMIB. Since not all the information in a trust domain SMIB is necessarily locally present in every MNE that supports a trust domain, it may be necessary to convey access control attributes between MNEs. Note that user-specific access control attributes may not always be required since a trust domain security policy may confer certain access rights on all its members.

II.1.4.4.5 Data Integrity Management

ISO 7498-2 (clause 8.4.5) describes data integrity management as follows:

Data integrity management may involve:

- Interaction with key management
- Establishment of cryptographic parameters and algorithms, and
- Use of protocol between communicating entities.

When using cryptographic techniques to support the data integrity service, similarities exist between data integrity management and encryption management. In some instances, within a single MNE, data integrity can be attained as a by-product of strong access control mechanisms. When a strong communications data integrity service is required, cryptographic mechanisms are likely candidates.

II.1.4.4.6 Authentication Management

ISO 7498-2 (clause 8.4.6) describes authentication management as follows:

Authentication management may involve distribution of descriptive information, passwords or keys (using key management) to entities required to perform authentication. It may also involve use of a protocol between communicating entities and other entities providing authentication services.

Authentication mechanisms rely upon particular authentication information to validate a given identity. The authentication information against which user-supplied authentication information is verified is stored in the SMIB and is subject to similar considerations as access control attributes.

Authentication of the claimed identities of individuals, as individuals or as members of a group, is a typical security policy requirement. Authentication mechanisms provide varying degrees of credibility that such claims are correct. Authentication responsibilities are often shared between administrative, environmental, and technical (i.e., hardware and software) mechanisms. Probably the most common mechanism is the picture badge and the guard. The picture on the badge matching the appearance of the holder affirms the association of the individual with what the badge represents. The identity of the individual is thereby authenticated and, in some cases, the possession of the badge establishes further claims. The reading of the magnetic code on a badge matched with the entry of a personal identification number is similar in capability to picture confirmation. Similarly, the matching of fingerprints or retina images authenticates the identity of an individual.

The use of keys with locks, passwords, or cipher lock codes authenticates identity only to the extent of the probability that the presenter is a valid holder of the object or information. That probability is based on the administrative handling and physical protection of such mechanisms or information. The same considerations apply to the use of smart cards, cryptographic ignition keys, and other credentials that make no positive connection with the holder. In general, non-forgeable information bound to the holder is the strongest type of authentication mechanism. Security mechanisms for authentication depend upon system security administrators who perform the initial assignment of the badge or other credential to an individual.

The TSP security architecture relies on the use of smart cards that contain cryptographic processing and storage capabilities. These smart cards serve as picture badges for visual identification and authentication and also provide electronic authentication via the use of asymmetric (public key) cryptographic mechanisms used in conjunction with X.509v3 digital certificates. The positive connection between the possessor of a smart card picture badge and the badge is accomplished by one, or more, of the following alternatives:

1. The badge holder knowing a numeric Personal Identification Number (PIN) that matches the PIN stored within the card

2. The digitized fingerprint image from one of the fingers of the badge holder matching the digitized fingerprint image stored within the card

3. The combination of alternatives 1 and 2 above; namely the digitized fingerprint image and PIN supplied by the badge holder must match the corresponding objects within the smart card badge.

The same type of asymmetric (public key) cryptographic mechanisms used in conjunction with X.509v3 digital certificates will provide electronic authentication of MNE identities. With MNEs, the certificates and MNE private keys are stored within the MNE or can be stored in a smart card that is inserted into a smart card reader built into the MNE. When using smart cards with MNEs, the smart card reader needs to include a lockable access door to reduce the probability of unauthorized smart card removal.

II.1.4.4.7 Traffic Padding Management

ISO 7498-2 (clause 8.4.7) describes traffic padding management as follows:

Traffic padding management may include maintenance of the rules to be used for traffic padding. For example, this may include:

- Pre-specified data rates
- Specifying random data rates
- Specifying message characteristics such as length, and
- Variation of the specification, possibly in accordance with time of day and/or calendar.

Traffic padding in physical layer communications devices is often managed as a configuration parameter. In an open systems environment, traffic padding in the physical layer will occur infrequently. Traffic padding in application layer protocols could be invoked as the result of a user request or as the result of a trust domain security policy requirement applied to all or some class of communications. The critical management aspect of satisfying such a request is to assure that the padding is applied at the correct stage of processing with respect to other security services, such as data integrity or data confidentiality.

II.1.4.4.8 Routing Control Management

ISO 7498-2 (clause 8.4.8) defines routing control management as follows.

Routing control management may involve the definition of the links or sub-networks which are considered to be either secured or trusted with respect to particular criteria.

Routing control in open systems meeting TSP security architecture requirements will normally be restricted to choosing a particular network interface when an MNE is connected to multiple CNs or LCSs.

II.1.4.4.9 Notarization Management

ISO 7498-2 (clause 8.4.2) defines notarization management as follows.

Notarization management may include:

- The distribution of information about notaries
- The use of a protocol between a notary and the communicating entities, and
- Interaction with notaries.

The role of Notarization Management within the TSP security architecture is to be determined.

II.1.4.4.10 Availability Management

Availability management is not described in ISO 7498-2. Availability mechanisms in communications networks and MNEs satisfy security policy requirements for availability of communications and processing resources. The ability of communications networks to provide timely and regular service depends upon the total security architecture, implementation, and management of those systems. The techniques of redundancy, diversity, contingency reserves, and contingency planning play a large part in communications network availability. Within MNEs, the LCS must be similarly designed and protected to avoid failure outages. Generally, the physical protection and integrity checking of the MNEs, relay systems, and LCSs will provide for their availability.

End of Document