

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

M.3410

(08/2008)

SERIES M: TELECOMMUNICATION MANAGEMENT,
INCLUDING TMN AND NETWORK MAINTENANCE

Telecommunications management network

**Guidelines and requirements for security
management systems to support
telecommunications management**

Recommendation ITU-T M.3410



International
Telecommunication
Union

Document Sharing Hub

ITU-T M-SERIES RECOMMENDATIONS

TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Introduction and general principles of maintenance and maintenance organization	M.10–M.299
International transmission systems	M.300–M.559
International telephone circuits	M.560–M.759
Common channel signalling systems	M.760–M.799
International telegraph systems and phototelegraph transmission	M.800–M.899
International leased group and supergroup links	M.900–M.999
International leased circuits	M.1000–M.1099
Mobile telecommunication systems and services	M.1100–M.1199
International public telephone network	M.1200–M.1299
International data transmission systems	M.1300–M.1399
Designations and information exchange	M.1400–M.1999
International transport network	M.2000–M.2999
Telecommunications management network	M.3000–M.3599
Integrated services digital networks	M.3600–M.3999
Common channel signalling systems	M.4000–M.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T M.3410

Guidelines and requirements for security management systems to support telecommunications management

Summary

Recommendation ITU-T M.3410 describes a set of functions considered necessary for the management of security mechanisms deployed in current and next generation packet-oriented networks. A logical collection of management functionality used to perform "operations, administration, maintenance and provisioning" (OAM&P) of security mechanisms, policies and services within a services and communications infrastructure.

Source

Recommendation ITU-T M.3410 was approved on 6 August 2008 by ITU-T Study Group 4 (2005-2008) under Recommendation ITU-T A.8 procedure.

Keywords

Authentication, authorization, confidentiality, FCAPS, management, security.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2009

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	2
3	Definitions	3
3.1	Terms defined elsewhere	3
3.2	Terms defined in this Recommendation.....	5
4	Abbreviations and acronyms	6
5	Conventions	9
6	Security management system (SMS) overview	9
6.1	Security management concepts relationship to next generation networks.....	11
6.2	Security management relationship to [ITU-T X.800] and [ITU-T X.805] security concepts	11
6.3	Security management concepts relationship to ITU-T Recommendations M.3016-series	12
6.4	Security management concepts relationship to ITU-T management Recommendations	12
7	Security management system functional requirements	12
7.1	Administrator interface FG.....	16
7.2	Administrator account management FG.....	16
7.3	Credentials management FG	19
7.4	Configuration management FG	20
7.5	Fault management FG	22
7.6	Security policy management FG	25
7.7	Verification and validation management FG	26
7.8	Corrective action management FG	27
7.9	Security management information FG	29
7.10	Communications interface FG.....	30
Annex A	Proforma – M.3410 – SMS requirements.....	32
A.1	Basis of profile proforma for security requirements	32
A.2	Guidelines and instructions for proforma specification	32
A.3	Proforma	32
Appendix I	Relationship of security management concepts to [ITU-T X.800].....	35
I.1	Trust domains	35
I.2	Security management information bases.....	35
I.3	Trust domain SMIB content	36
I.4	Communication of security management information.....	37
I.5	Distributed security management administration.....	38
I.6	Security mechanism management	42

	Page
Appendix II – SMS relationship with the role of security in other TSP management frameworks and systems.....	47
II.1 SMS relationship to ITU-T management Recommendations	47
II.2 Security of legacy/existing management systems	56
Appendix III – TSP infrastructure and security service managed elements.....	64
III.1 TSP NGN security service managed elements.....	64
III.2 Framework and topology of the NGN.....	64
III.3 NGN decomposition.....	67
III.4 Security mechanisms within an NGN	73
III.5 NGN computing platform security mechanisms	77
Bibliography.....	94

Copyright International Telecommunication Union/ITU Telecommunication Sector
 Provided by IHS Markit under license with ITU-T
 No reproduction or networking permitted without license from IHS
 Full document details: ITU-T M.3410 2008

Recommendation ITU-T M.3410

Guidelines and requirements for security management systems to support telecommunications management

1 Scope

This Recommendation describes the functional requirements of a security management system (SMS) that offers a centralized view for control and security oversight of a telecommunications service provider's (TSP) infrastructure. The SMS spans the management of the management security plane, the control security plane, and the end-user security plane. The TSP's infrastructure spans, at a minimum:

- Application servers (e.g., servers for mail, instant messaging, database, web, file, voice over IP (VoIP) and other applications);
- Support servers (e.g., DNS [b-IETF RFC 2181], DHCP [b-IETF RFC 2131], NTP [b-IETF RFC 1305], backup, and other infrastructure support services);
- Internetworking/transport components (e.g., multiplexers, switches, routers, transport gateways, application gateways, gateway controllers, packet-filters a.k.a. firewalls, content filters, access points, bridges, wired and wireless telephony devices and monitoring probes for QoS, and network activity, to name a few);
- End user host systems (e.g., laptop systems, desktop systems, workstations, printers, etc.); and
- Management systems (e.g., element management, network management, service management, and business management systems).

All of the above entities are referred to in this Recommendation as managed elements (MEs) from a security management perspective.

The requirements specified in this Recommendation should be applicable to a TSP's current infrastructure and also infrastructure evolution necessary for building their next generation networks (NGNs) (see [ITU-T Y.2001] and [ITU-T Y.2012]).

This Recommendation draws on an ATIS standard [b-ATIS 0300074] as a major source of information and text.

A key aspect of this Recommendation is that it defines a logical architecture and set of functionality independent of physical implementation. Functionality is defined in terms of functional entities, their logical relationships as well as aggregation of functional entities (FEs) into functional groups (FGs). Deployment and implementation of these FEs and FGs, within an infrastructure, can take many forms, such as centralized, hierarchical, distributed, or some combination of these. This Recommendation takes no stand as to the implementation of FEs and FGs in so far as implementation decisions do not have security-related ramifications. The detailed description of the interactions between FGs is not described in this Recommendation.

Annex A contains a normative proforma wherein specific SMS requirements are documented. Appendices I, II and III are informative and cover:

Appendix I: The relationship between the SMS and the security concepts covered in [ITU-T X.800].

Appendix II: The relationship between the SMS and other TSP management systems and frameworks.

Appendix III: The structure and organization of NGN networks and their growing complexity.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions*.
- [ITU-T M.3010] Recommendation ITU-T M.3010 (2000), *Principles for a telecommunications management network*.
- [ITU-T M.3016.0] Recommendation ITU-T M.3016.0 (2005), *Security for the management plane: Overview*.
- [ITU-T M.3016.1] Recommendation ITU-T M.3016.1 (2005), *Security for the management plane: Security requirements*.
- [ITU-T M.3016.2] Recommendation ITU-T M.3016.2 (2005), *Security for the management plane: Security services*.
- [ITU-T M.3016.3] Recommendation ITU-T M.3016.3 (2005), *Security for the management plane: Security mechanism*.
- [ITU-T M.3016.4] Recommendation ITU-T M.3016.4 (2005), *Security for the management plane: Profile proforma*.
- [ITU-T M.3050.2] Recommendation ITU-T M.3050.2 (2004), *Enhanced Telecom Operations Map (eTOM) – Process decompositions and descriptions*.
- [ITU-T M.3060] Recommendation ITU-T M.3060/Y.2401 (2006), *Principles for the management of Next Generation Networks*.
- [ITU-T X.500] Recommendation ITU-T X.500 (2005) | ISO/IEC 9594-1:2005, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*.
- [ITU-T X.509] Recommendation ITU-T X.509 (2000) | ISO/IEC 9594-8:2001, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- [ITU-T X.700] Recommendation ITU-T X.700 (1992), *Management framework for Open Systems Interconnection (OSI) for CCITT applications*.
- [ITU-T X.733] Recommendation ITU-T X.733 (1992) | ISO/IEC 10164-4:1992, *Information technology – Open Systems Interconnection – Systems Management: Alarm reporting function*.
- [ITU-T X.736] Recommendation ITU-T X.736 (1992) | ISO/IEC 10164-7:1992, *Information technology – Open Systems Interconnection – Systems Management; Security alarm reporting function*.
- [ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- [ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

- [ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.
- [ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.
- [ITU-T X.812] Recommendation ITU-T X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*.
- [ITU-T X.816] Recommendation ITU-T X.816 (1995) | ISO/IEC 10181-7:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework*.
- [ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.
- [ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.
- [ISO/IEC 15408-1] ISO/IEC 15408-1:2005, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*.
<http://www.iso.org/iso/catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40612>
- [ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.
<http://www.iso.org/iso/catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 access control:** [ITU-T X.800]
- 3.1.2 access control list:** [ITU-T X.800]
- 3.1.3 alarm:** [ITU-T X.733]
- 3.1.4 active threat:** [ITU-T X.800]
- 3.1.5 asymmetric authentication method:** [ITU-T X.811]
- 3.1.6 audit trail, see security audit trail:** [ITU-T X.800]
- 3.1.7 authenticated identity:** [ITU-T X.811]
- 3.1.8 authentication:** [ITU-T X.800]
- 3.1.9 authentication information:** [ITU-T X.800]
- 3.1.10 authorization:** [ITU-T X.800]
- 3.1.11 business management layer:** [ITU-T M.3010]
- 3.1.12 ciphertext:** [ITU-T X.800]
- 3.1.13 cleartext:** [ITU-T X.800]
- 3.1.14 confidentiality:** [ITU-T X.800]
- 3.1.15 control security plane:** Clause 8.2 of [ITU-T X.805]
- 3.1.16 credentials:** [ITU-T X.800]

- 3.1.17 **cryptanalysis:** [ITU-T X.800]
- 3.1.18 **cryptography:** [ITU-T X.800]
- 3.1.19 **data integrity:** [ITU-T X.800]
- 3.1.20 **decipherment:** [ITU-T X.800]
- 3.1.21 **decryption:** [ITU-T X.800]
- 3.1.22 **denial of service:** [ITU-T X.800]
- 3.1.23 **digital signature:** [ITU-T X.800]
- 3.1.24 **element management layer:** [ITU-T M.3010]
- 3.1.25 **encipherment:** [ITU-T X.800]
- 3.1.26 **encryption:** [ITU-T X.800]
- 3.1.27 **end-to-end encipherment:** [ITU-T X.800]
- 3.1.28 **end-user security plane:** Clause 8.3 of [ITU-T X.805]
- 3.1.29 **hash function:** [ITU-T X.810]
- 3.1.30 **initiator:** [ITU-T X.812]
- 3.1.31 **integrity:** [ITU-T X.800]
- 3.1.32 **key:** [ITU-T X.800]
- 3.1.33 **key management:** [ITU-T X.800]
- 3.1.34 **network element:** [ITU-T M.3010]
- 3.1.35 **network management layer:** [ITU-T M.3010]
- 3.1.36 **managed element (ME):** [ITU-T M.60]
- 3.1.37 **managed resources:** [ITU-T M.60]
- 3.1.38 **management security plane:** Clause 8.1 of [ITU-T X.805]
- 3.1.39 **management system:** [ITU-T M.60]
- 3.1.40 **masquerade:** [ITU-T X.800]
- 3.1.41 **non-repudiation:** [ITU-T X.800]
- 3.1.42 **object:** [ITU-T M.60]
- 3.1.43 **one-way hash function:** [ITU-T X.810]
- 3.1.44 **operations system:** [ITU-T M.3010]
- 3.1.45 **passive threat:** [ITU-T X.800]
- 3.1.46 **password:** [ITU-T X.800]
- 3.1.47 **peer-entity authentication:** [ITU-T X.800]
- 3.1.48 **physical security:** [ITU-T X.800]
- 3.1.49 **privacy:** [ITU-T X.800]
- 3.1.50 **private key:** [ITU-T X.810]
- 3.1.51 **public key:** [ITU-T X.810]
- 3.1.52 **public-key certificate:** [ITU-T X.509]
- 3.1.53 **repudiation:** [ITU-T X.800]

- 3.1.54 **risk:** [ISO/IEC 27002]
- 3.1.55 **role:** [ISO/IEC 15408-1]
- 3.1.56 **secret key:** [ITU-T X.810]
- 3.1.57 **security alarm:** [ITU-T X.736]
- 3.1.58 **security audit:** [ITU-T X.800]
- 3.1.59 **security audit record:** [ITU-T X.816]
- 3.1.60 **security audit trail:** [ITU-T X.800]
- 3.1.61 **security certificate:** [ITU-T X.810]
- 3.1.62 **security management information base (SMIB):** [ITU-T X.700]
- 3.1.63 **security policy:** [ITU-T X.800]
- 3.1.64 **security-related event:** [ITU-T X.736]
- 3.1.65 **service management layer (SML):** [ITU-T M.3010]
- 3.1.66 **service management layer operations system function block (S-OSF):** [ITU-T M.3010]
- 3.1.67 **signature:** [ITU-T X.800]
- 3.1.68 **stratum/strata:** [ITU-T Y.2012]
- 3.1.69 **subject:** [ISO/IEC 15408-1]
- 3.1.70 **symmetric authentication method:** [ITU-T X.811]
- 3.1.71 **target:** [ITU-T X.812]
- 3.1.72 **threat:** [ITU-T X.800]
- 3.1.73 **trust:** [ITU-T X.810]
- 3.1.74 **trusted third party:** [ITU-T X.810]

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 application security administrator: An application security administrator is an individual who has responsibility for the administration of those attributes and capabilities of an application (sub-) system related to security of the application (e.g., application administrative and user accounts and authorizations).

3.2.2 application system administrator: An application system administrator is an individual who has responsibility for the administration of all non-security-related attributes and capabilities of an application (sub-) system (e.g., application features, capabilities, configuration parameters and monitoring of the application).

3.2.3 business management system (BMS): A business management system is a business management layer [ITU-T M.3010] operations system.

3.2.4 element management system (EMS): An element management system is an element management layer [ITU-T M.3010] operations system.

3.2.5 functional entity (FE): A functional entity is a cluster of functionality (sub-functions) that are viewed as a single entity from the point of view of the end-to-end functional architecture.

3.2.6 functional group (FG): A functional group is a cluster of functional entities grouped (and named) solely for convenience and architectural clarity.

3.2.7 managed element operator(s): A managed element operator is an individual who has responsibility to perform specified tasks/activities on a managed element that are administrative in nature (e.g., backup, patching, surveillance, etc.).

3.2.8 managed element security administrator: A managed element security administrator is an individual who has responsibility for the administration of those attributes and capabilities of a managed element related to security of the managed element, regardless of what applications execute on the managed element (e.g., managed element administrative and user accounts and authorizations).

3.2.9 managed element system administrator: A managed element system administrator is an individual who has responsibility for the administration of all non-security-related attributes and capabilities of a managed element (e.g., managed element features, capabilities, configuration parameters and monitoring of the managed element).

3.2.10 network management system (NMS): A network management system is a network management layer [ITU-T M.3010] operations system.

3.2.11 role: The description of an individual's sphere of responsibility.

NOTE – It may be used for enforcing access control in accordance with the principle of least privilege (see: managed element operator(s), managed element system administrator, managed element security administrator, application system administrator, application security administrator above).

3.2.12 security administrator: An authority (a person or group of people) responsible for implementing the security policy for a security domain.

3.2.13 security event: A security-related event [ITU-T X.736].

3.2.14 security management system (SMS): A logical collection of management functionality used to perform "operations, administration, maintenance and provisioning" (OAM&P) of security mechanisms, policies and services within a services and communications infrastructure.

3.2.15 service management system: A service management system is a service management layer [ITU-T M.3010] operations system.

3.2.16 telecommunications service provider (TSP) infrastructure: A TSP infrastructure includes all managed elements deployed by a TSP that provide management, application/services, service control or transport strata functionality.

3.2.17 trust domain: A set of information and associated resources consisting 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 employ various levels of trust, depending on what the users need to know and the sensitivity of the information and associated resources.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2G	Second Generation
3G	Third Generation
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ADF	Access control Decision Function
AEF	Access control Enforcement Function
AH	Authentication Header

API	Application Programming Interface
APP-SA	Application Process Security Associations
ASIC	Application-Specific Integrated Circuit
BMS	Business Management System
CA	Certificate Authority
CLEC	Competitive Local Exchange Carrier
CORBA	Common Object Request Broker Architecture
CPU	Central Processing Unit
CRL	Certificate Revocation List
DCE	Distributed Computing Environment
DDoS	Distributed Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DLEC	Data Local Exchange Carrier
DLL	Data Link Layer
DNS	Domain Name System
DoS	Denial-of-Service
DSL	Digital Subscriber Line
DTLS	Datagram Transport Layer Security
EMS	Element Management System
ENNI	External Network-Network Interface
ESP	Encapsulating Security Payload
eTOM	enhanced Telecom Operations Map
FCAPS	Fault, Configuration, Accounting, Performance, and Security management
FE	Functional Entity
FG	Functional Group
FTP	File Transfer Protocol
GPS	Global Positioning System
GSS	General Security Service
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IDS	Intrusion Detection System
IKE	Internet Key Exchange
INNI	Internal Network-Network Interface
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol



ISDN	Integrated Services Digital Network
KDC	Key Distribution Centre
LDAP	Lightweight Directory Access Protocol
ME	Managed Element
ME-SA	Managed Element Security Association
MIB	Management Information Base
MNE	Managed Network Element
NE	Network Element
NEL	Network Element Layer
NGN	Next Generation Network
NMS	Network Management System
NNI	Network-Network Interface
NOC	Network Operations Centre
NTP	Network Time Protocol
OAM&P	Operations, Administration, Maintenance and Provisioning
OCSP	Online Certificate Status Protocol
OS	Operations System
OSI	Open Systems Interconnection
OSP	Outside Plant
OSS	Operations Support System, same as OS
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PON	Passive Optical Network
PSTN	Public Switched Telephone Network
PUC	Public Utilities Commission
QoS	Quality of Service
RA	Registration Authority
RADIUS	Remote Authentication Dial In User Service
RBAC	Role-Based Access Control
RVM	Reference Validation Mechanism
S&C	Signalling and Control
SA	Security Association
SC	Service Control
SDU	Service Data Unit
SMAP	Security Management Application Process
SMI	Security Management Information

SMIB	Security Management Information Base
SML	Service Management Layer
SMS	Security Management System
SNMP	Simple Network Management Protocol
S-OSF	Service Management Layer Operations System Function
SPDF	Security Policy Decision Function
SPEF	Security Policy Enforcement Function
SQL	ANSI Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TDM	Time-Division Multiplexing
TFTP	Trivial File Transfer Protocol
TL1	Transaction Language 1
TLS	Transport Layer Security
TMN	Telecommunications Management Network
TSP	Telecommunications Service Provider
UNI	User-to-Network Interface
VoIP	Voice over IP
WLAN	Wireless Local Area Network
XML	eXtensible Markup Language
XSL	eXtensible Stylesheet Language

5 Conventions

The term "should" is used within this Recommendation to denote those functional capabilities that are appropriate in performing the activities of managing security mechanisms in an integrated manner. A proforma for SMS realization is in Annex A that contains specific requirements.

6 Security management system (SMS) overview

The *security management system* (SMS) described in this Recommendation is primarily an operations system intended to mechanize the application of various security services and security management tools. The SMS supports the management of security of the TSP infrastructure by providing supporting services to protect the information and resources in TSP networks and systems. It manages the security in accordance with the applicable trust domains and their security policies.

A *trust domain* is a 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 employ various levels of trust, depending on what the users need to know and the sensitivity of the information and associated resources.

Security management is concerned with the management of security services and mechanisms. Such management requires distribution of management information to those services and mechanisms, as well as the collection of information concerning the operation of the services and mechanisms. Objects are resources that may be managed. *Management information* is information associated with an object that is operated upon to manage that object.

A human administrator employs a *security management application process* 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 Recommendation as *Managed Elements* (MEs) – 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.

MEs 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 ME level. Thus, an ME security policy is necessary to specify how the shared use of security functions and resources among trust domains is accomplished. This ME policy also must be managed.

Security management of MEs 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 MEs. There are always supporting security management activities that are related to administrative and environmental security mechanisms or which are prerequisite to the use of ME 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 security services and mechanisms that the trust domain supports
- A description of the objects and their attributes, including rules pertaining to creation and use of multi-domain 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 MEs
- Criteria for acceptable security mechanisms to implement the required security services
- Security management-specific requirements
- Interaction of the security management of each trust domain to other trust domains
- 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 MEs that will be deployed within the trust domain

The security policy for an ME 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 objects, including criteria for user access, display labelling, and transfers within and among MEs
- Controlling and maintaining security management mechanisms and 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 ME security management and trust domain security management are part of their SMIBs. For a trust domain that is supported in more than one ME, the security administrator may have physical access to only some of those MEs. Thus, the security management application process that operates on the portion of a SMIB in a particular ME must be accessible to the security administrator both locally and remotely. A security management application process is like any other application in that it operates in a security context that 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 applications in the same trust domains.

6.1 Security management concepts relationship to next generation networks

As defined in [ITU-T Y.2001], a next generation network (NGN) is a packet-based network that is able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies, and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for subscribers to networks and to competing service providers and/or services of their choice. It supports generalized mobility that will allow consistent and ubiquitous provision of services to users. A goal of NGN is to provide the capabilities to make the creation, deployment, and management of all kinds of services possible. In order to achieve this goal, it decouples the service creation/deployment infrastructure from and independent of the transport infrastructure. Such decoupling is reflected in the NGN architecture as the separation of the transport and service strata and shown as two independent strata. Figure 1 of [ITU-T M.3060] shows the scope of the management architecture in the context of NGN.

From a TSP's perspective, the information and resources of the NGN transport and service strata are part of the TSP's infrastructure and are within the scope of the security management system architecture and requirements defined in this Recommendation.

6.2 Security management relationship to [ITU-T X.800] and [ITU-T X.805] security concepts

[ITU-T X.800] and [ITU-T X.805] define the general security-related architectural elements that are necessary for providing end-to-end security, and which can be applied appropriately in the circumstances for which protection of communication between open systems is required.

This Recommendation uses information from these ITU-T Recommendations to develop system level, operating environment and software requirements to assure secure management of TSP network infrastructures.

The security management structure of these ITU-T Recommendations 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 these ITU-T Recommendations. 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 Recommendation to address these topics. Even though the details – such as the management information base definition – are not part of this Recommendation, the architecture is defined with the need to

support these elements required for interoperability and assure secure management of TSP network infrastructure.

6.3 Security management concepts relationship to ITU-T Recommendations M.3016-series

ITU-T Recommendations M.3016-series: [ITU-T M.3016.0] [ITU-T M.3016.1] [ITU-T M.3016.2] [ITU-T M.3016.3] [ITU-T M.3016.4] address the requirements, services, and mechanisms in support of securing the management plane of the telecommunications infrastructure. In this context, they are focused on management plane 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 shows the interfaces where management traffic is to be secured. Given these end-to-end security requirements, this Recommendation focuses on requirements of a management system that offers the tools necessary to manage the security of the TSP's infrastructure. The management plane traffic addressed in the ITU-T Recommendations M.3016-series is a subset of the TSP's infrastructure to be secured by the requirements in this Recommendation. The reference model in the ITU-T Recommendations M.3016-series is further expanded in this Recommendation to include other MEs that are not specific to management plane such as the application servers, etc. While there are similarities in the functions to be supported in all these Recommendations, the ITU-T Recommendations M.3016-series relate to the interfaces between the MEs and operations systems (OSs) and between OSs, and this Recommendation addresses functions to be supported by systems that oversee all the infrastructure components.

6.4 Security management concepts relationship to ITU-T management Recommendations

Appendix II provides a discussion of the relationship between the SMS and existing ITU-T management Recommendations other than the ITU-T Recommendations M.3016-series.

7 Security management system functional requirements

The functions of an SMS can be logically organized into the following FGs which include FEs providing logically-related functionality:

- *Administrator interface FG*

This FG provides the ability of administrative personnel to interact with other SMS FGs/FEs and, at a minimum, typically would include one or more of the following FEs:

 - Local command line administrator interface FE
 - Remote command line administrator interface FE
 - Local graphical administrator interface FE
 - Remote graphical administrator interface FE
- *Administrator account management FG*

This FG provides the ability to centrally administer and manage administrative user accounts to include managing administrator subjects, groups and roles and includes one or more of the following:

 - Authentication credentials, subject group memberships, and access rules
 - Group identifiers and privileges
 - Account propagation
 - Authentication, identification and other administrative account related demographic information.

- *Credentials management FG*

This FG provides the ability to centrally administer/manage authentication, and possibly authorization credentials.

FEs within this FG interact with:

- Existing authentication and authorization functionality (such as RADIUS [b-IETF RFC 2865], Diameter [b-IETF RFC 3588], TACACS+ and Lightweight directory access protocol (LDAP) [b-IETF RFC 4510] [b-IETF RFC 4511] [b-IETF RFC 4512] [b-IETF RFC 4513] servers)
- X.509 certificate and registration authorities (including online certificate status protocol (OCSP) servers and DNS/LDAP certificate and certificate revocation list (CRL) repositories)
- Security token and 'one-time pad' systems
- Key distribution centres (KDCs) (such as Kerberos [b-IETF RFC 4120])
- Public key infrastructures (PKIs)
- Certificate authorities (CAs)

- *Configuration management FG*

This FG provides the ability to centrally administer/manage security-related attributes and configurable parameters within MEs, such as:

- Objects and object groups
- Object's subject and subject group access and authorization rights
- Security functionality configuration

FEs within this FG interact with:

- Existing configuration management and provisioning applications.

- *Fault management FG*

This FG provides the ability to centrally manage security-related events, security-related alarms, security alarms and logs within MEs, as well as identification of attack-related activities, such as:

- Security-related events [ITU-T X.736], including adjunct security devices reporting
- Security-related alarms [ITU-T X.733] and security alarms [ITU-T X.736]
- Security log entry reconciliation and analysis of security audit trails

FEs within this FG interact with:

- Existing fault management and surveillance applications

- *Security Policy Management FG*

This FG provides the ability to centrally manage security policy and procedures information and can include:

- Policy development and version tracking
- Operational procedures development and version tracking
- Document repository
- Policy and procedure periodic reviews

- *Verification and Validation Management FG*

This FG provides the ability to centrally administer and manage the verification and validation that deployed network and ME security mechanisms are configured and operating according to policy.

FEs within this FG interact with:

- Network deployed intrusion detection and prevention systems (IDS/IPS)
- ME deployed intrusion detection and prevention systems (IDS/IPS)
- ME vulnerability and intrusion scanning applications

- *Corrective action management FG, including reporting corrective action and receiving corrective action completion report*

This FG provides the ability to centrally administer/manage activities required to contain, isolate, investigate and restore services following security-related, or other, event occurrences.

FEs within this FG interact with:

- Existing trouble-ticket and workforce management applications
- System surveillance and performance management applications

- *Security management information FG*

This FG provides the ability to centrally administer/manage security-related information in a security management information base (SMIB) repository. FEs within this FG should be able to transpose information, stored using various formats and organizational structures both locally and by remote MEs, into and from a common Meta-language usable by all SMS FEs. Meta-data should be relied on for locating (i.e., local vs remote storage location) and controlling both translations (i.e., or syntax, structure) and access attributes (i.e., access control lists (ACLs), rights, views).

FEs within this FG interact with:

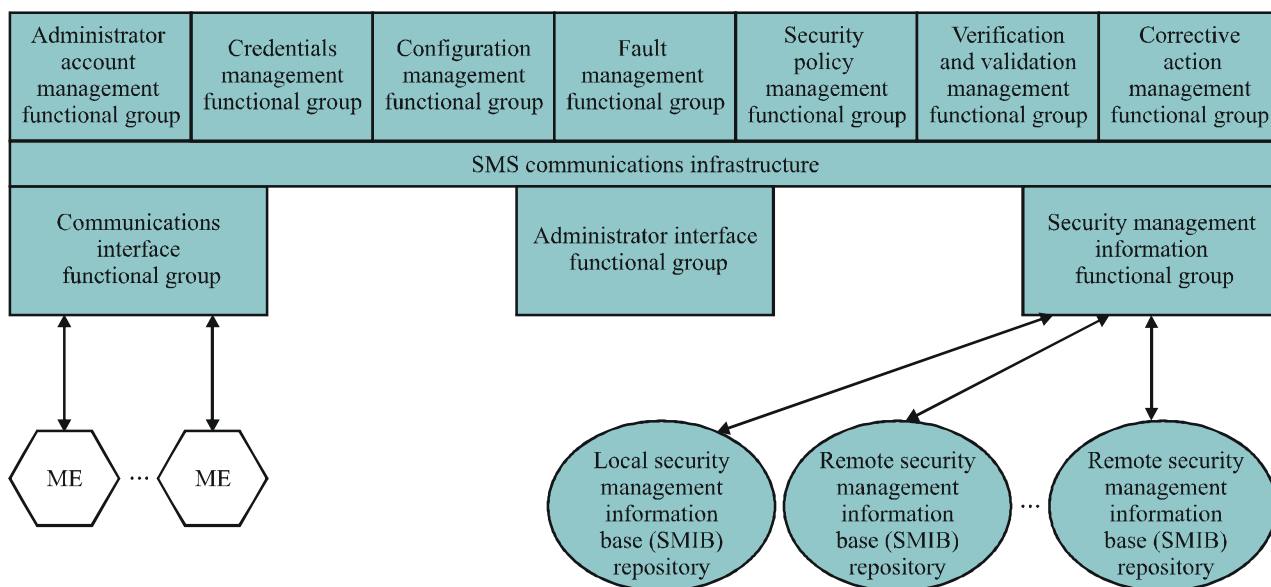
- Currently deployed Management MEs (element management systems (EMSs), network management systems (NMSs), business management systems (BMSs), service management systems, operations systems (OSs)) and other MEs that retain security management information.

- *Communications interface FG*

This FG provides the ability to communicate with other MEs via standards based and proprietary networking and application protocols. All other SMS FEs rely on the FEs within this FG to serve as a communications and translation proxy whenever any SMS FE exchanges information with other MEs. These FEs include those necessary to support those management protocols in use by deployed MEs.

It is anticipated that the majority of SMS FEs will be co-located, but co-location is not required. A foundation concept behind the SMS is to leverage existing security management capabilities into a flexible interoperable framework for achieving unified and consistent adherence to organizational security policies and requirements. As such, SMS FEs not just interact with other management systems but should allow delegation of SMS FE functionality to existing management applications. From a communications perspective, SMS FEs will interact with peer OSs, existing EMS/NMS applications and MEs within the application/services, service control and transport strata.

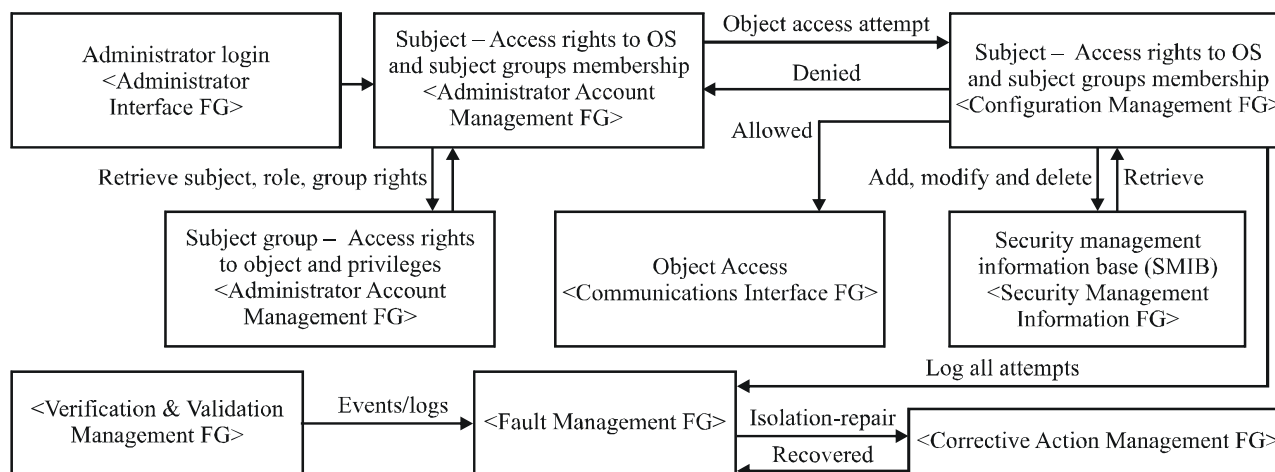
The platforms that host SMS FGs/FEs have their own security hardening requirements given the sensitivity of the very information processed and the control capabilities of these FEs. A basic SMS logical block structure by FG is pictured in Figure 1 below.



M.3410(08)_F01

Figure 1 – SMS logical block structure

An example relationship between FGs is pictured in Figure 2 below.



M.3410(08)_F02

Figure 2 – Example SMS flow logic

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

Each of the security management functions discussed in the following subclauses will require automated support for security administrators. The applications that provide this support are concerned with the various aspects of the security management information base (SMIB) maintenance, credential management, examination, processing, and correlation of information – such as security 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 public-key certificates are easily available to a user community.

7.1 Administrator interface FG

The administrator interface FG is the aggregation of all available administrative interfaces (FEs) presented to the security personnel managing the security network operations centre (NOC). These user interface FEs include local and remote command line and graphical user interface technologies that are operated on by SMS managed element security administrator(s) and/or SMS managed element system administrator(s).

SEC-1: The administrator interface FG should support standards-based web browsers using de jure standards (e.g., XML and XSL).

SEC-2: The administrator interface FG should use HTTPS to communicate over the network with the management system server.

SEC-3: The administrator interface FG should be able to invoke all authorized functions within SMS FEs.

SEC-4: There should not be FG functions that must be performed via another method, such as a command line interface, unless a mechanism is used that provides strong authentication and confidentiality, such as secure shell (SSH).

SEC-5: Administrator interface FEs should communicate with other SMS FEs through the use of a de jure standards-based method, such as CORBA, HTTPS/XML, etc. in compliance with [ITU-T M.3016.1].

All SNMP and CORBA references are referring to the communications mechanisms and NOT the middleware or are presented simply as examples of common protocols used in management. This Recommendation at no time requires the use of any of these protocols.

7.1.1 Local command line administrator interface FE

The local command line administrator interface FE provides a command line interface for SMS FG commands.

7.1.2 Remote command line administrator interface FE

The remote command line administrator interface FE provides a command line interface for commands sent to and executed on MEs.

7.1.3 Local graphical administrator interface FE

The local graphical administrator interface FE provides a graphical user interface (e.g., web-based user interface) for SMS FG commands.

7.1.4 Remote graphical administrator interface FE

The remote graphical administrator interface FE provides a graphical user interface (e.g., web-based user interface) for commands sent to and executed on MEs.

7.2 Administrator account management FG

Administrator account management encompasses the addition, modification, and deletion of entity accounts that are authorized to manage MEs and the objects contained within each ME. Administrator account management includes subject, subject group, subject propagation, and authorization management. There are two levels of administrator account management: 1) administrator accounts for SMS FEs; and 2) administrator accounts for MEs.

FEs within administrator account management FG interact with deployed transport, signalling and control, application service delivery and management MEs, as defined in [ITU-T Y.2012], as well as non-NGN MEs.

SEC-6: The administrator account management FG should communicate with other SMS FGs through the use of a de jure standards-based method, such as CORBA, HTTPS/XML, etc. in compliance with [ITU-T M.3016.1].

7.2.1 Subject management FE

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

SEC-7: The management of subjects should include the ability to add the entity's authentication credentials.

SEC-8: The management of subjects should include the ability to modify the entity's authentication credentials.

SEC-9: The management of subjects should include the ability to delete the entity's authentication credentials.

SEC-10: The management of subjects should include the ability to invalidate and revoke the entity's authentication credentials.

Examples of credentials are user name, passwords, biological identifiers, and public-key certificates.

7.2.2 Subject group management FE

Subject grouping is a method to define role-based access control. A subject group is an identifier for a uniquely identifiable group of subjects. A subject or subject group may have multiple roles within their work definition. By assigning identifiers to these groups of subjects, if the role is no longer valid, the subject's appropriate rights can be easily removed from objects managed by that subject group identifier. This is a necessary means when controlling access to tens of millions of objects. Examples of subject groups are ME system administrator and ME system operator.

SEC-11: The security management system should include the ability to add subject group identifiers and the privileges each identifier holds.

SEC-12: The management system should include the ability to modify subject group identifiers and the privileges each identifier holds.

SEC-13: The management system should include the ability to delete subject group identifiers and the privileges each identifier holds.

SEC-14: The management system should include the ability to map subjects to subject groups.

7.2.3 Subject propagation management FE

Because there will be situations where management of an object through the OS 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-15: The subject and subject group attributes should be passed to the managed elements in the appropriate supported protocol, such as XML, SNMPv3, HTTP, HTTPS, telnet, ssh, FTP, TFTP, sctp, sftp, etc., in compliance with [ITU-T M.3016.1].

These protocols are defined in the identified IETF RFCs: XML, SNMPv3 [b-IETF RFC 3414], HTTP [b-IETF RFC 2616], HTTPS [b-IETF RFC 2818], telnet [b-IETF RFC 854], ssh

[b-IETF RFC 4251], FTP [b-IETF RFC 959], TFTP [b-IETF RFC 1350], sctp [b-IETF RFC 4960], and sftp [b-IETF RFC 913].

7.2.4 Authentication management FE

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

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 a ME; or
- An application executing within one ME initially communicating with a peer application executing within a different ME.

This service performs:

- The initial identity authentication;
- Verification of authentication credentials validity, as necessary; and
- Negotiation of any security attributes necessary for data-origin authentication within applications, if applicable.

One example of peer-entity authentication within applications is the "classic" log-in identifier (ID) 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 ID and password mode or in a "Challenge/Response" mode. Other recent techniques are the physical token, which contains authentication information that may be used to authenticate the claimed identity of a human subject, and keyboards, which contain built-in biometric fingerprint readers. 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 public-key certificates of a PKI.

For communication between application processes, 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 protocols such as NTPv3 [b-IETF RFC 1305] and management protocols such as SNMPv3).
- Digital signatures (frequently combined with digital public-key certificates of a PKI) as used by the transport layer security (TLS) protocol [b-IETF RFC 4346], 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 [b-IETF RFC 793]. TLS and SSL are also used with the common object request broker architecture (CORBA).
- The Kerberos [b-IETF RFC 4120] security framework used either as part of the distributed computing environment (DCE) or by itself with "kerberized" applications.
- IPSec, including the Internet key exchange (IKE) [b-IETF RFC 4306] [b-IETF RFC 4307] protocol, Internet security association key and management protocol (ISAKMP), the authentication header (AH) [b-IETF RFC 4302], and or the encapsulating security payload (ESP) [b-IETF RFC 4303], usable by numerous application and management protocols.

SEC-16: All authentication information that traverses a data communications network, regardless of being private or public, should not travel in "clear" text or otherwise be able to be read by an eavesdropping third party.

7.3 Credentials management FG

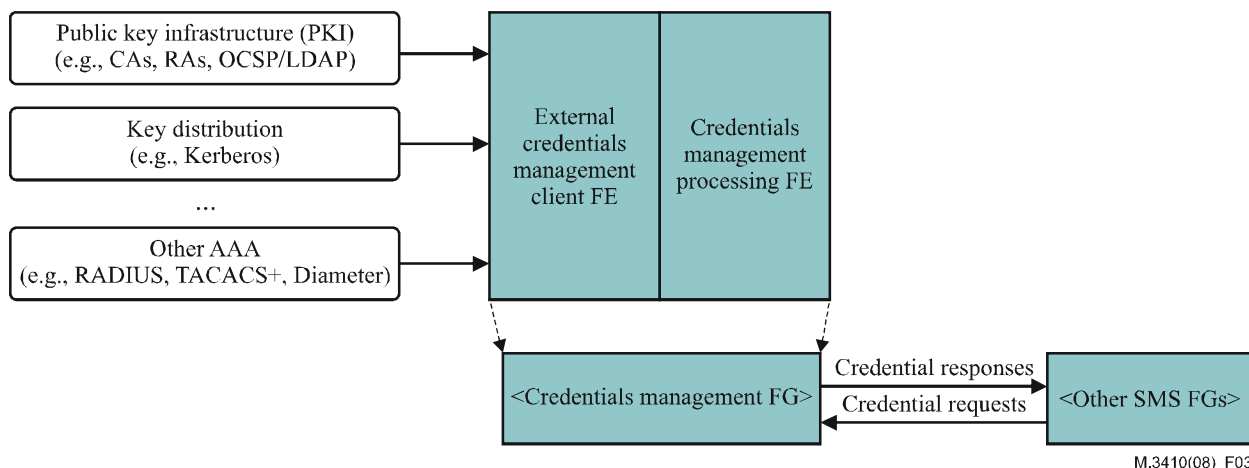


Figure 3 – Credentials management FG logical block diagram

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 public-key certificates [ITU-T X.509], and Kerberos tickets. Also part of this FG are the servers used to host RADIUS authentication services, Kerberos authentication services, PKI public-key certificate authority and registration authority services, and LDAP public-key certificate repositories. One need remember that the management of credentials is a different set of functions vs the use of credentials for authentication of authorization enforcement.

SEC-17: The credentials management FG should communicate with other SMS FGs through the use of a de jure standards-based method, such as CORBA, HTTPS/XML, etc. in compliance with [ITU-T M.3016.1].

7.3.1 External credentials management client FE

There may actually be multiple external credentials management client FEs, one, or more, for each type of external credentials management. As an example, the client interacting with registration authorities (RAs) within a PKI will likely use public-key cryptography standards (PKCS) (such as [b-RSA]) defined messages for requesting, retrieving and revoking digital certificates. A different client FE may be used to manage credentials information in LDAP and OCSP servers/directories. There will be other client FEs determined by the various external AAA and key distribution centres (KDC) systems deployed.

7.3.2 Credentials management processing FE

The credentials management processing FE is responsible for controlling the administration of credentials. This FE provides storage and retrieval of passwords, pass phrases, and static secret keys. ME private keys are also escrowed by this FE. The information handled by this FE is of such significance that it should be stored in an encrypted form directly within this FE.

7.4 Configuration management FG

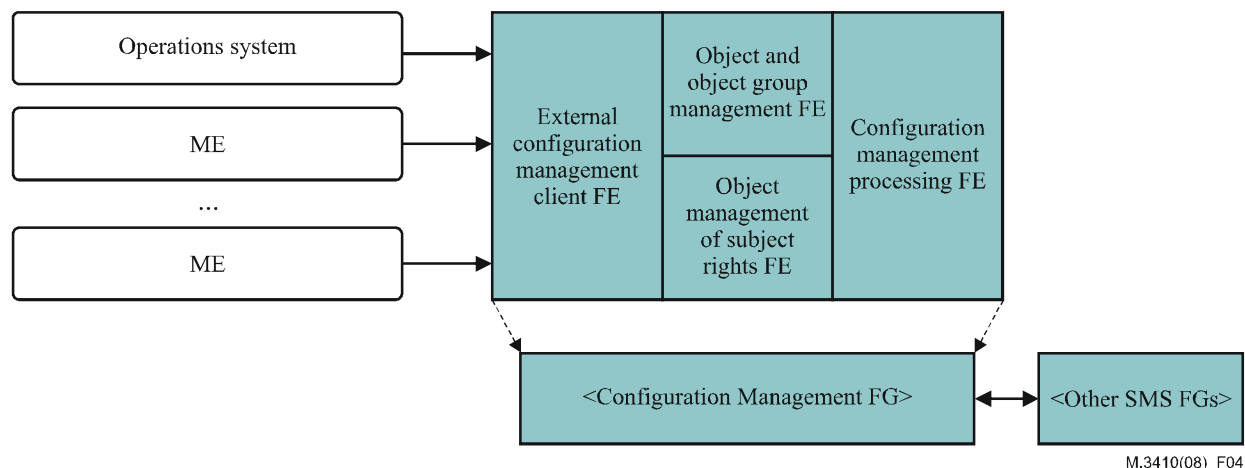


Figure 4 – Configuration management FG logical block diagram

The configuration management FG is responsible for what is sometimes referred to as "the management of security". As an example, it is responsible for the provisioning of credentials and other parameters (such as encryption parameters) for security associations between MEs. 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 mechanisms require. The configuration management FG is also responsible for ensuring that any issued commands meet the currently established security policy.

SEC-18: The configuration management FG should communicate with other SMS FGs through the use of a de jure standards-based method, such as CORBA, HTTPS/XML, etc. in compliance with [ITU-T M.3016.1].

The administrator should have the ability to enter commands in a pseudo type (Meta) language, e.g., XML, as the different type of MEs may not be consistent across like devices, i.e., routers from vendor A and vendor B. In this context, a Meta language would use syntax and semantics that are not specific and unique to any specific vendor products. While configuration may be similar, the administrator should not need to know the exact syntax for each.

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

In the future, 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 to which the policy would apply. To continue the example, the routers and firewalls would block access to the TFTP port, the host would stop the local TFTP service, the intrusion detection system would detect of the use of TFTP, etc. This capability will allow for consistent security configuration and monitoring across the entire network.

7.4.1 Object and object group management FE

An object is an entity that contains or passes information. Examples of objects include records, blocks, pages, segments, files, directories, directory trees, programs, video displays, keyboards, clocks, printers, laptops, access points, and MEs. 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." Object management includes the ability to place objects into trust domains.

SEC-19: SMS FEs should be able to scale to accommodate the number of subjects to be managed within the enterprise; this could result in very large numbers of subjects.

SEC-20: SMS FEs should be able to scale to accommodate the number of objects to be managed within the enterprise; this could result in very large numbers of objects.

Most TSPs will deploy a growing number of MEs and distributed services that the number of subjects will grow tremendously over time.

7.4.2 Object management of subject rights FE

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 (read, write, delete, backup, etc.), based upon subject and subject groups. These access and authorization rights establish the rules for security functionality configuration.

SEC-21: The management of objects and object groups should include the ability to add the access and authorization rights.

SEC-22: The management of objects and object groups should include the ability to modify the access and authorization rights.

SEC-23: The management of objects and object groups should include the ability to delete the access and authorization rights.

7.4.3 External configuration management client FE

There may actually be multiple external configuration management client FEs, one, or more, for each type of external configuration management systems deployed. Each client will likely use XML, or proprietarily defined messages for interacting with these external systems.

7.4.4 Configuration management processing FE

The configuration management processing FE is responsible for controlling, at a logical level, interaction between SMS FG components and external systems with configuration management responsibility.

Document Sharing Hub

7.5 Fault management FG

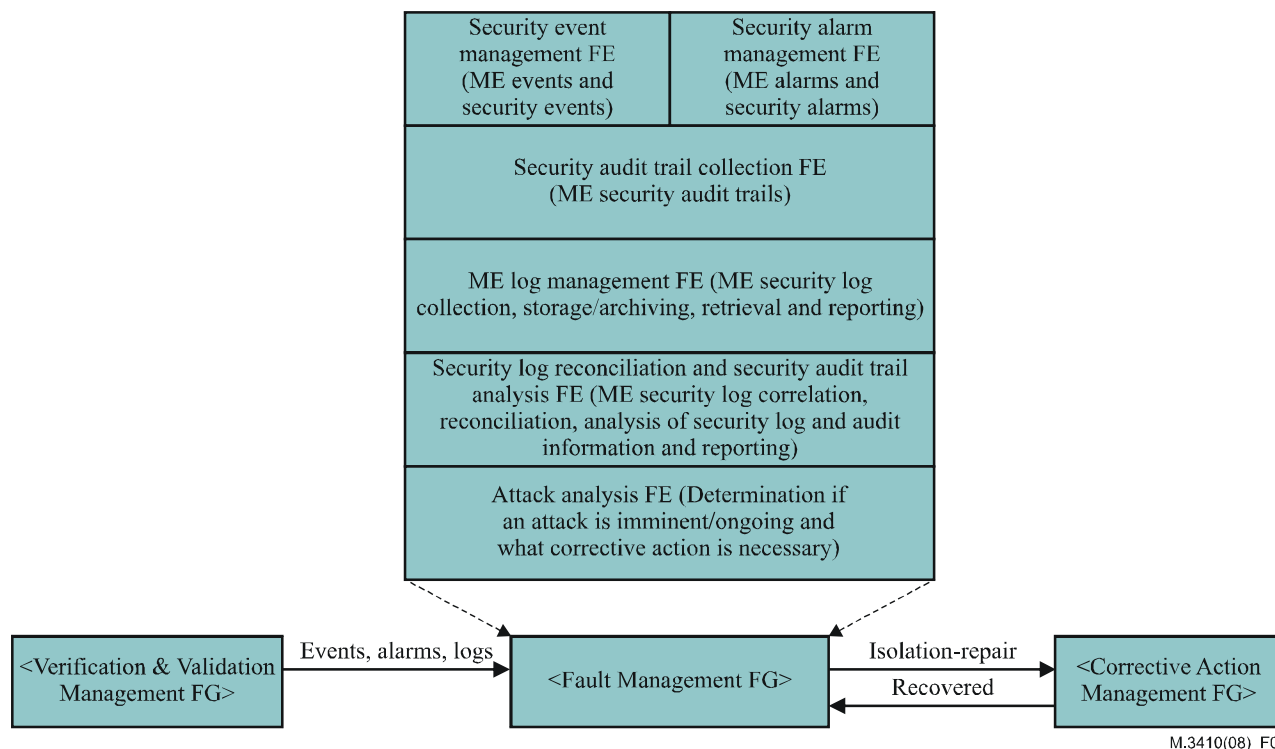


Figure 5 – Fault management FG logical block diagram

The fault management FG is composed of FEs which focus on events and alarms that either are security relevant or specifically security-related. Security logs and security audit trail information are also processed by FEs in this FG. The fault management FG may also communicate to peer OSs for the transmission of SMS generated alarms and security alarms and for any alarms generated from the correlation and analysis of security events, alarms and security alarms.

SEC-24: The fault management FG should communicate with the other FGs and interface modules through the use of protocols specified in [ITU-T M.3016.1].

7.5.1 Security event management FE

The security event management FE is responsible for receiving security events from the activity logging and alarm reporting mechanisms within transport and service stratum, along with application and management MEs. Upon receipt, these events are indexed and stored for further analysis and reporting purposes. This FE 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 element and contains certain attributes that define the event. These attributes can include (among others): the managed element that sent the event (ME name), the ME's IP address [b-IETF RFC 791], and the time of the event as generated by the ME. This information will be used to compare to the security alarm management FE's attribute table to determine the proper notification and correct action.

SEC-25: The security event management FE should be able to receive information from the following types of sources:

- Passive logging, such as syslog and security audit trail logs;
- Active polling, such as SNMP GET/GET-Next; and
- Active alerting, such as SNMP notifications.

A table of security-related events is stored within the SMS SMIB.

SEC-26: The table for security-related events should contain a list of each managed element's security-related events.

SEC-27: Each event should contain administrator defined attributes.

SEC-28: The security event management FE should be responsible for archiving and retrieval of current and prior event information to/from off-site long-term storage.

7.5.2 Security alarm management FE

Security alarm management is responsible for collecting and reviewing managed element security-related alarms and security alarms.

SEC-29: The security alarm management FE should, upon receipt of security-related alarms/security alarms, index and store these alarms for further analysis.

SEC-30: The security alarm management FE should, upon receipt of security-related alarms/security alarms, index and store these alarms for reporting purposes.

SEC-31: The security alarm management FE should be responsible for archiving and retrieval of current and prior security-related alarms/security alarms to/from off-site long-term storage.

7.5.3 ME log management FE

ME log management is responsible for receiving, archiving and retrieval of log records and files from MEs. This FE provides:

- The ability to retrieve/receive log entries/files from MEs, as well as the operating environment logs, by time stamps and other criteria.
- Retrieval capabilities based on time, polling and ME initiated.
- Alarm generation based on failure to receive log information according to policy and other criteria.
- Definable reporting capabilities.
- Sending log information to designated repositories (both local and remote).

SEC-32: The ME log management FE should provide retrieval capabilities based on time, polling and ME initiated transfers.

SEC-33: The ME log management FE should provide alarm generation capabilities based on the failure to receive log information according to policy and other criteria.

SEC-34: The ME log management FE should provide definable reporting capabilities.

SEC-35: The ME log management FE should provide the ability to send log information to designated local repositories.

SEC-36: The ME log management FE should provide the ability to send log information to designated remote repositories (both electronically and physically).

SEC-37: The ME log management FE should be responsible for archiving and retrieval of current and prior security logs to/from off-site long-term storage.

In the absence of a common message format, a translation FE will be needed to meet the above requirements. This translation FE would include the ability to convert the syntax, and perhaps the semantics, of messages between different syntax formats.

7.5.4 Security audit trail collection FE

Security audit trail collection is responsible for collecting and processing managed element security audit trails. Security audit trails include logs of network element executed command, and other data collected to be potentially used to facilitate a security audit.

SEC-38: The SMS FGs should maintain a security audit trail of all commands issued by SMS FGs.

SEC-39: The Security Audit Trail Collection FE should upon receipt of managed element security audit trails, index and store these security audit trails for further analysis.

SEC-40: The Security Audit Trail Collection FE should upon receipt of managed element security audit trails, index and store these security audit trails for reporting purposes.

SEC-41: The Security Audit Trail Collection FE should be responsible for archiving and retrieval of current and prior security audit trails to/from off-site long-term storage.

7.5.5 Security log reconciliation and security audit trail analysis FE

The security log reconciliation and security audit trail analysis FE is responsible for ascertaining criticality of each security-related event, alarm and security alarm as to the seriousness of the potential security breach each signifies. This FE provides:

- The ability to reconcile log entries from MEs, 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.

In the context of the following five requirements, "security breach" refers to any actual or suspected compromise of confidentiality, integrity, authenticity, availability or authorized functionality.

SEC-42: The security log reconciliation and security audit trail analysis FE should provide recommendations to operations personnel for ascertaining the extent of a security breach.

SEC-43: The security log reconciliation and security audit trail analysis FE should provide recommendations to operations personnel for limiting the extent of any security breach.

SEC-44: The security log reconciliation and security audit trail analysis FE should provide recommendations to operations personnel for acquisition of forensic information.

SEC-45: The security log reconciliation and security audit trail analysis FE should provide recommendations to operations personnel for re-establishing normal services as quickly as possible, without increasing the risk of continued or further security breaches.

SEC-46: The security log reconciliation and security audit trail analysis FE should be responsible for archiving and retrieval of current and prior log files and security audit trails to/from off-site long-term storage.

In the absence of a common message format, a translation FE will be needed to meet the above requirements. This translation FE would include the ability to convert the syntax, and perhaps the semantics, of messages between different syntax formats.

7.5.6 Attack analysis FE

The attack analysis FE is responsible for ascertaining criticality of each security-related event and alarm as to the seriousness of the potential security breach each signifies. The attack analysis FE differs from the security log reconciliation and security audit trail analysis FE as each FE relies on different inputs, and produces different output when performing analyses. As an example, the attack

analysis FE is driven by many different types of data including alarms and events, whereas the security log reconciliation and security audit trail analysis FE is driven by log and security audit trail inputs. This FE also provides:

- The ability to reconcile event and alarm notifications, possibly in conjunction with performance status, from MEs, 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.

In the context of the following five requirements, "security breach" refers to any actual or suspected violation of organizational security policies resulting in compromise of confidentiality, integrity, authenticity, availability or authorized functionality.

SEC-47: The attack analysis FE should provide recommendations to operations personnel for ascertaining the extent of a security breach.

SEC-48: The attack analysis FE should provide recommendations to operations personnel for limiting the extent of any security breach.

SEC-49: The attack analysis FEs should provide recommendations to operations personnel for acquisition of forensic information.

SEC-50: The attack analysis FE should provide recommendations to operations personnel for re-establishing normal services as quickly as possible, without increasing the risk of continued or further security breaches.

SEC-51: The attack analysis FE should be responsible for archiving and retrieval of current and prior forensic information to/from off-site long-term storage.

In the absence of a common message format, a translation function will be needed to meet the above requirements.

7.6 Security policy management FG

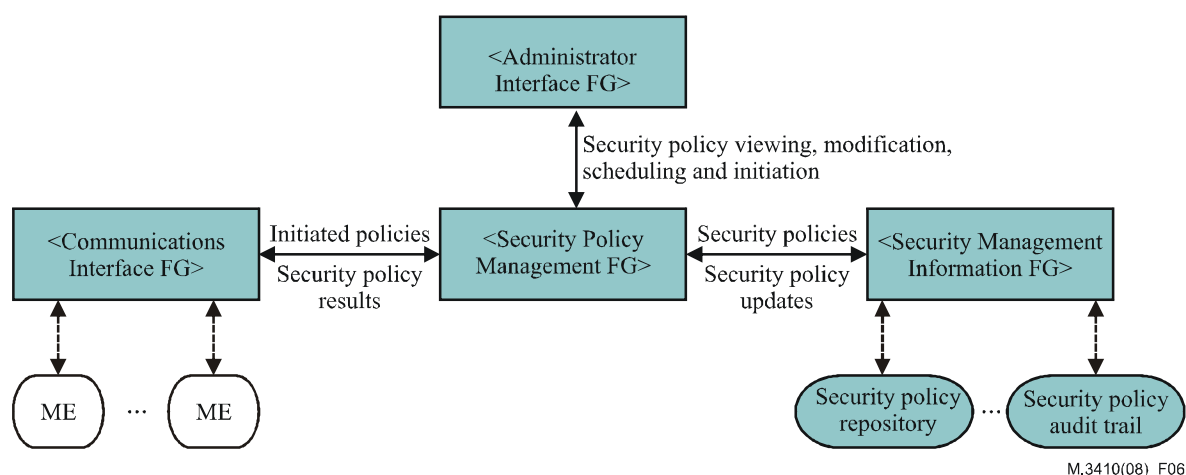


Figure 6 – Security policy management FG logical block diagram

The security policy management FG assists in or performs the translation of security policies to security policy rules that can be communicated, interpreted and implemented by MEs and audited by the security policy management FG. Security policy management FG includes the capabilities to develop, communicate and schedule security policy decisions throughout an organization. Security policies may include organization-wide password complexity and aging, organization-wide single sign-on use, organization-wide encryption algorithm settings, organization-wide revoking of credentials, etc. The security policy management FG can provide:

- Security policy viewing, modification, versioning, revocation and initiation
- Security policy dissemination to MEs
- Security policy auditing
- Security policy repository, including security policy audit trail
- Security policies scheduling
- Periodic security policy review and policy updates

SEC-52: The security policy management FG should maintain a repository of initiated security policies, pending security policies, potential security policies, draft/revoked security policies and a security audit trail of security policy modifications and initiations.

SEC-53: The security policy management FG should include the ability to add, modify, delete, schedule, revoke and initiate security policies.

SEC-54: The security policy management FG should communicate initiated security policies to MEs.

SEC-55: The security policy management FG should include the ability to audit MEs as to their application of the current security policies.

7.7 Verification and validation management FG

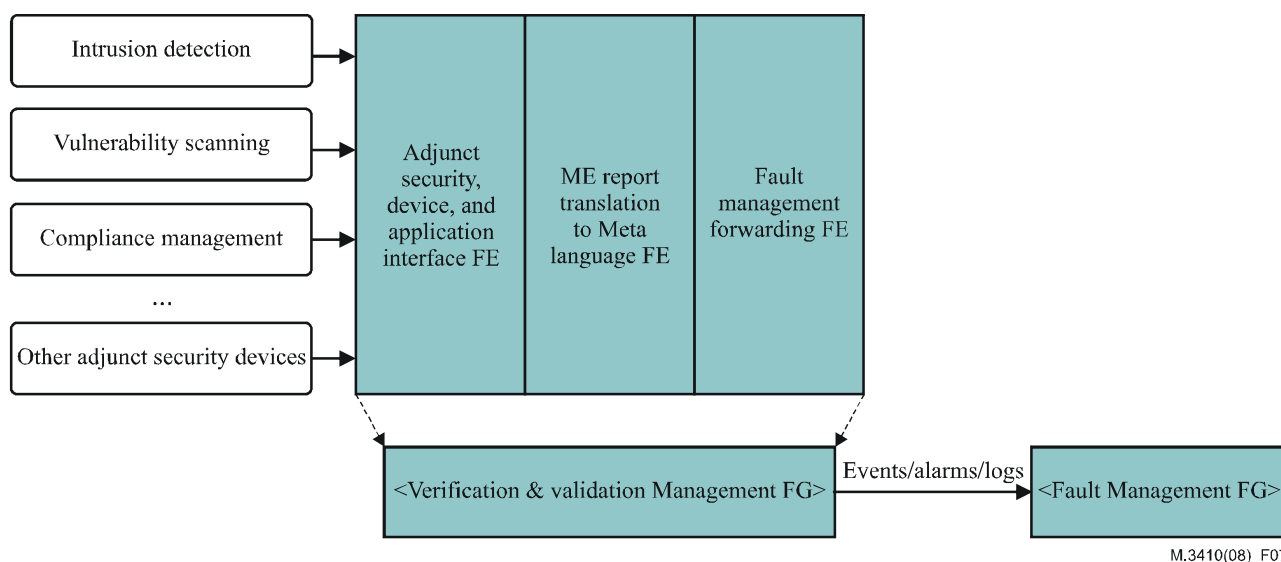


Figure 7 – Verification and validation management FG logical block diagram

The verification and validation management FG receives reports through interface modules from security subsystems, devices and applications, which are adjunct to other FEs; these include intrusion detection systems, intrusion prevention systems, vulnerability scanners, integrity checkers, firewalls, compliance managers, etc. The information received by the verification and validation