International Telecommunication Union

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

ITU-T

International Telecommunication Union

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/.

CONTENTS

Page

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/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/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 stratums. 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.

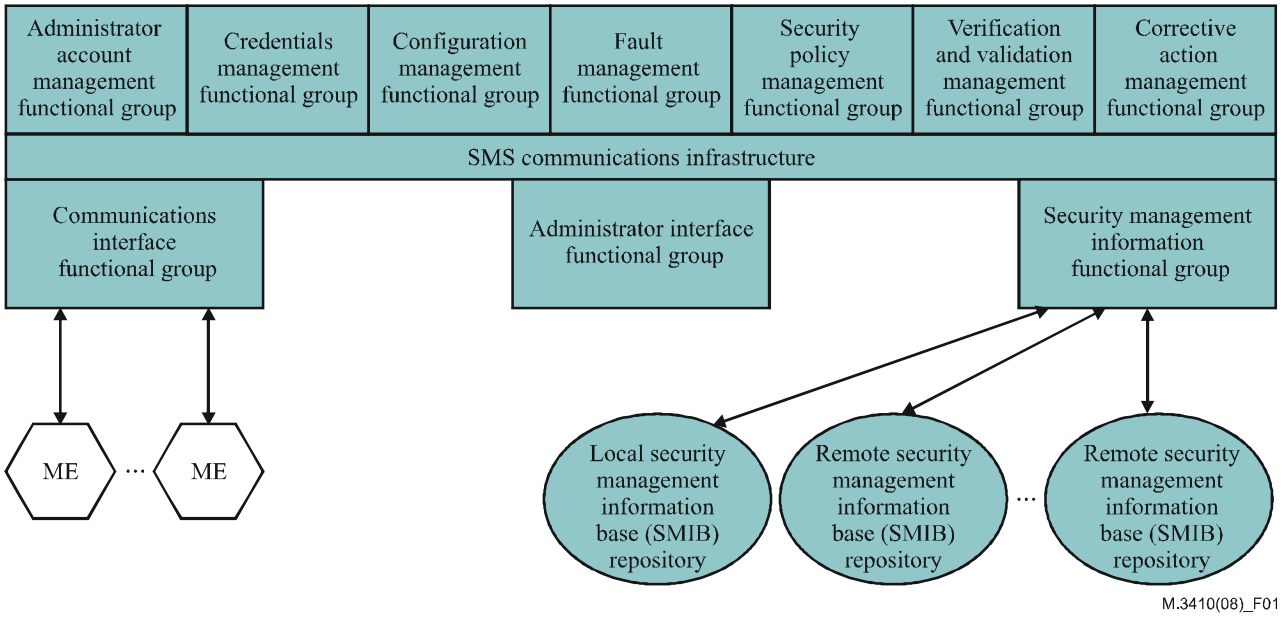

Figure 1 – SMS logical block structure

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

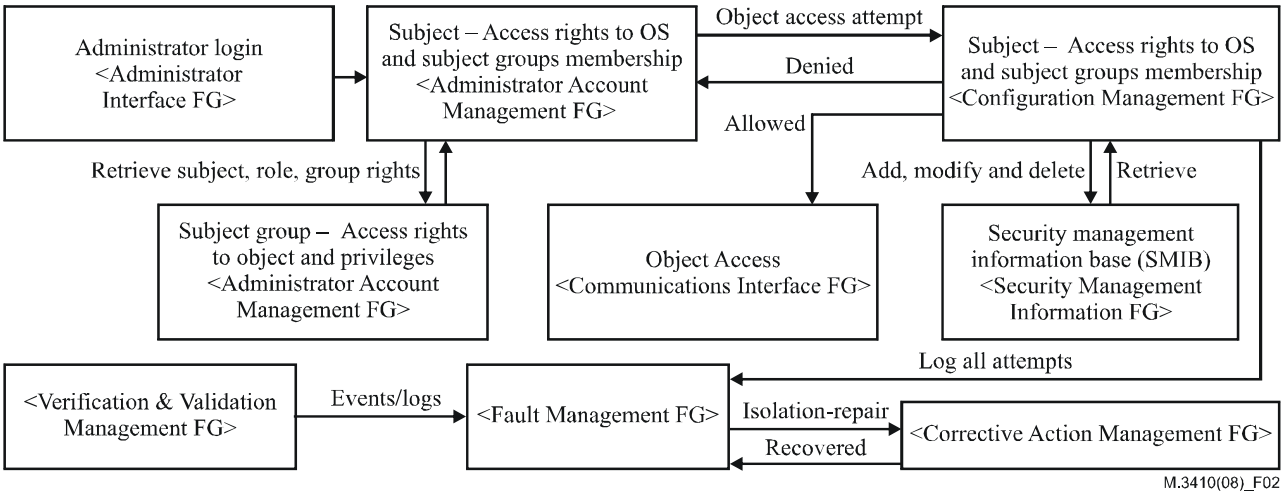

Figure 2 – Example SMS flow logic

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

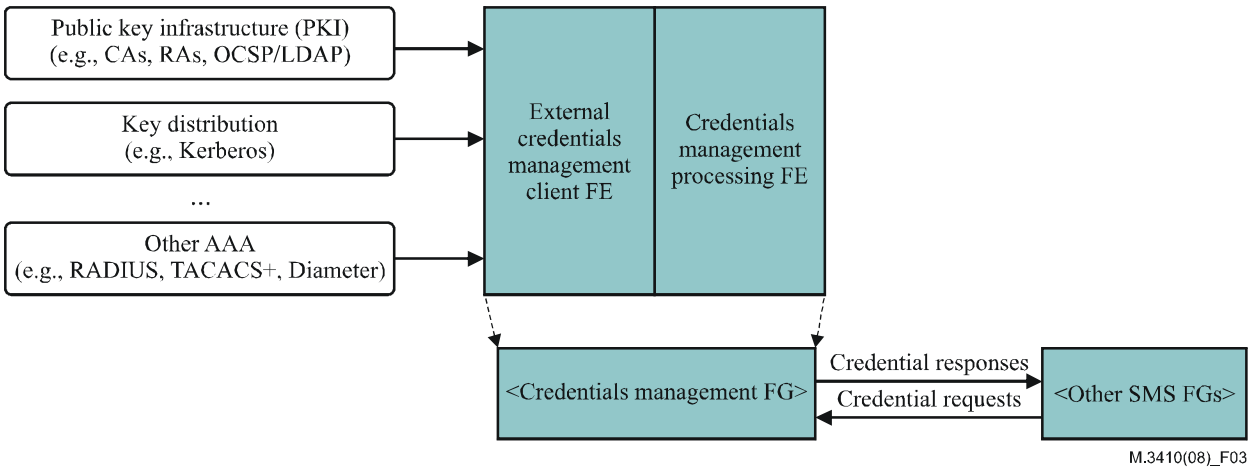

Figure 3 – Credentials management FG logical block diagram

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

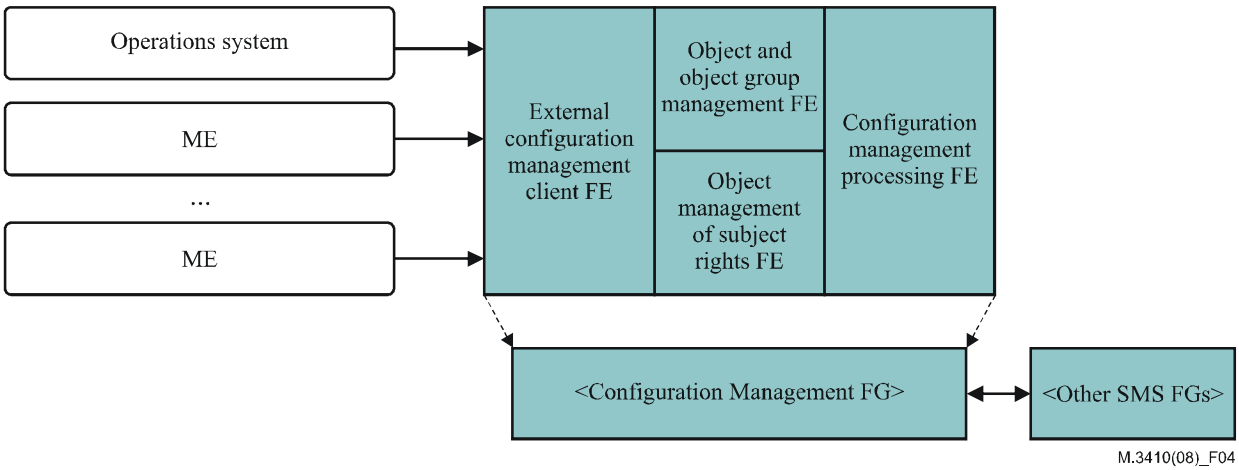

Figure 4 – Configuration management FG logical block diagram

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 dejure 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.

7.5 Fault management FG

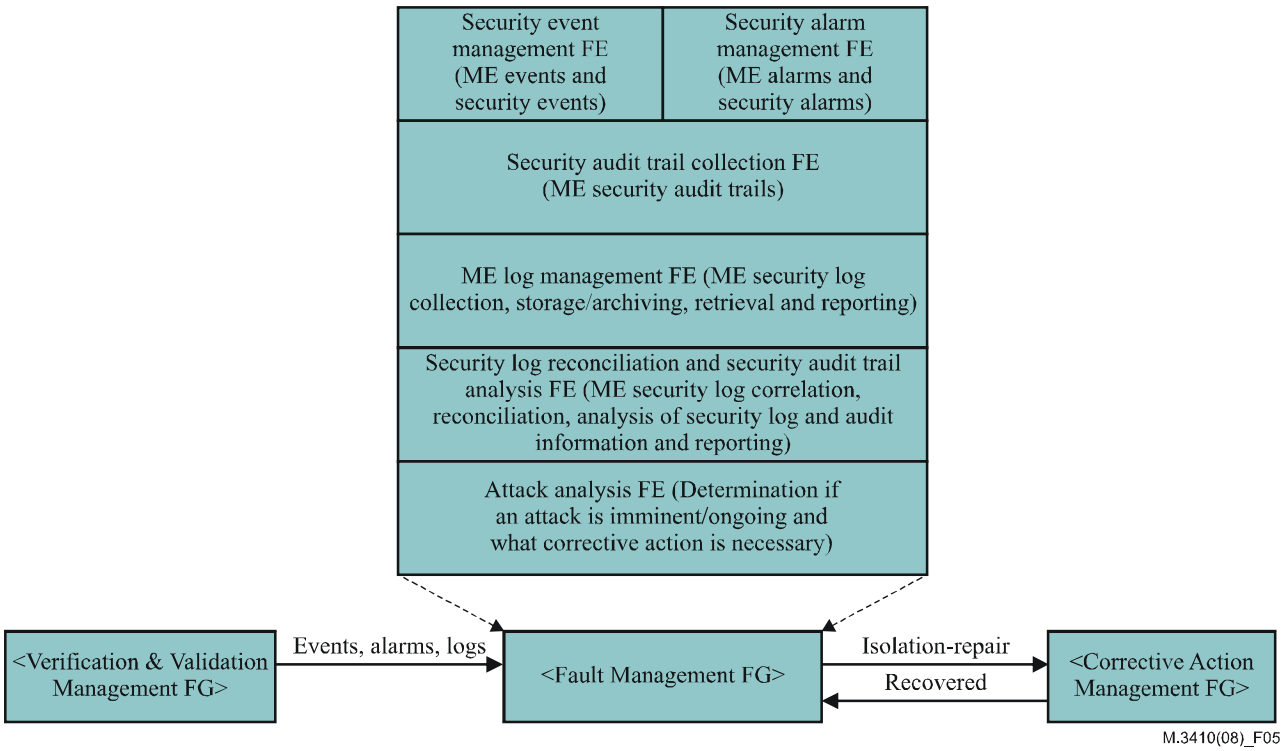

Figure 5 – Fault management FG logical block diagram

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

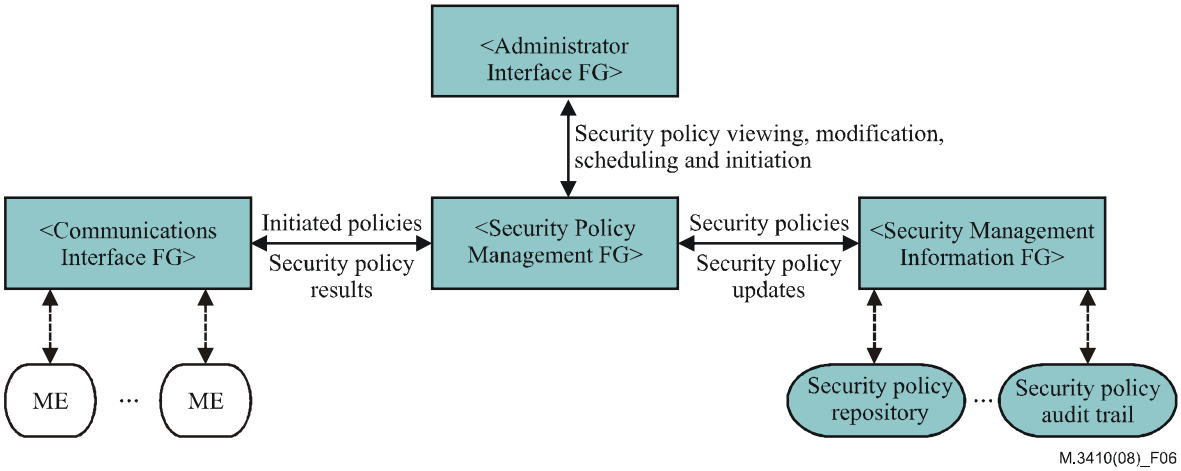

Figure 6 – Security policy management FG logical block diagram

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

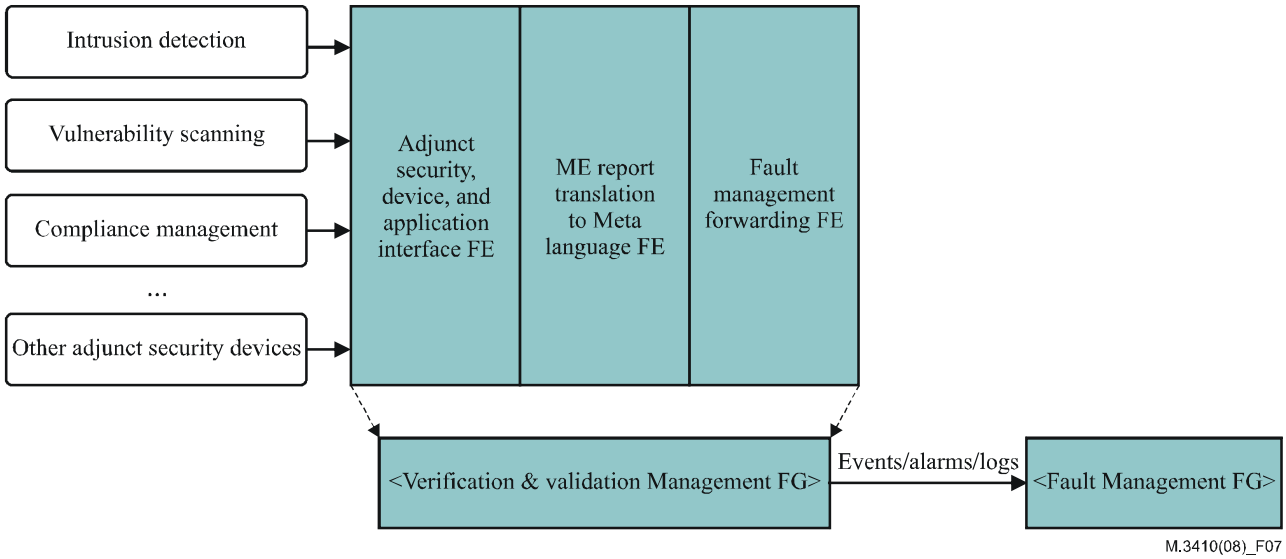

Figure 7 – Verification and validation management FG logical block diagram

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

management FG is translated into the SMS Meta language. These converted reports will be sent to other SMS FEs where they are indexed and stored for further analysis and reporting purposes.

7.7.1 Adjunct security, device and application interface FE

There may actually be multiple adjunct security, device and application interface FEs, one, or more, for each type of external security system deployed. Each interface FE will likely have used XML, or proprietarily, defined messages for interacting with these external systems, such as: intrusion detection systems, intrusion prevention systems, firewalls, vulnerability scanners, and compliance managers.

7.7.2 ME report translation to meta language FE

The ME report translation to meta language FE is responsible for translating the information received from external security products and software into a common meta language representation used by all SMS FGs and FEs. This FE can also be responsible for consolidation or otherwise reducing the volume of information.

7.7.3 Fault management forwarding FE

The fault management forwarding FE is responsible for interfacing with FEs within the SMS fault management FG and any other TSP specified OSs.

SEC-56: The verification and validation management FG should communicate with the other SMS FGs through the use of protocols specified in [ITU-T M.3016.1].

SEC-57: The vendor of SMS FEs should provide an application programming interface (API) so that vendors of adjunct security subsystems, devices and applications can produce an interface module for their product.

7.8 Corrective action management FG

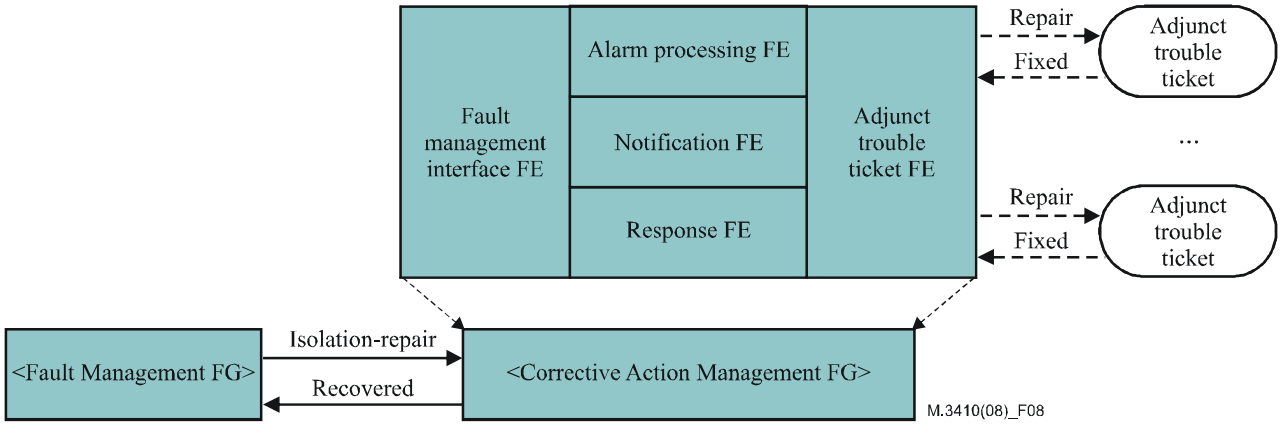

Figure 8 – Corrective action management FG logical block diagram

The corrective action management FG 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 or work order system.

SEC-58: The corrective action management FG should have a configurable table of security events, alarms and security alarms that can be received from the fault management FG.

SEC-59: The corrective action management FG's configurable table of security events, alarms and security alarms should be populated from the fault management FG.

SEC-60: The corrective action management FG's configurable table of security events, alarms and security alarms should be able to receive corresponding attributes from the fault management FG as to which trouble system 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 SMS must be able to receive a security-related event that indicates that the object has been repaired or notification that the correction cannot be made due to a negative impact on the production environment.

SEC-61: Reports from the corrective action management FG should be stored as part of the fault management FG for further analysis and reporting purposes.

7.8.1 Fault management interface FE

The fault management interface FE provides the interface from the fault management FG FEs. It potentially collects security events, alarms, security alarms, security logs, security audit trails, attack analysis, etc. It is also responsible for any translation and volume reduction required by the corrective action management FG and notification of any in-progress attacks that the fault management FG is able to identify.

7.8.2 Alarm processing FE

The alarm processing FE is responsible, through the processing of fault management information, for determining what type of responses and/or actions are appropriate for isolating those MEs under attack or mitigating the impact of an attack. Isolation may involve identifying those MEs, and the associated network segments, likely to be compromised by the attack and shutting down still unaffected links that interconnect the compromised MEs from still operational MEs. Mitigation actions should include identifying whether traffic throttling (changing session admission controls or QoS-related parameters), increased levels of packet filtering (as in deep packet inspection via intrusion prevention systems) or even the blocking of usually acceptable application protocols (as altering the rules of boarder or internally deployed state full firewall functionality).

7.8.3 Notification FE

The notification FE is responsible for interacting with ME security administrative personnel, via the administrative interface FG, to present notifications of recommended corrective actions and allow the said personnel to edit, create, modify and make action decisions regarding recommended corrective actions. Administrative decisions are forwarded to the Response FE as appropriate.

7.8.4 Response FE

The Response FE is responsible for constructing directives to be sent to peer management systems and MEs as a result of the alarm processing FE activities. This FE not only constructs appropriate messages and scripts, it also handles the storage (relying on security management information FG capabilities), retrieval and overseeing the execution of these scripts or corrective action scenarios. The Response FE is subordinate to the Notification FE for what response actions are to occur.

7.8.5 Adjunct trouble ticket FE

An important OAM&P activity is the management of field and facility located repair and emergency response personnel.

There may actually be multiple adjunct trouble ticket FEs, one, or more, for each type of external adjunct trouble ticket or workforce management system deployed. The adjunct trouble ticket FE receives the results of the alarm processing and response FEs, translates the results to the appropriate adjunct trouble ticket system format and synchronizes with the adjunct trouble ticket system when trouble ticket updates are made. The adjunct trouble ticket systems provide the ability to generate, store, track and close out work orders associated with the construction, repair and

administration of security issues. The adjunct trouble ticket FE may also provide an SMS-based trouble ticket/workforce management system when an adjunct system is not available.

7.9 Security management information FG

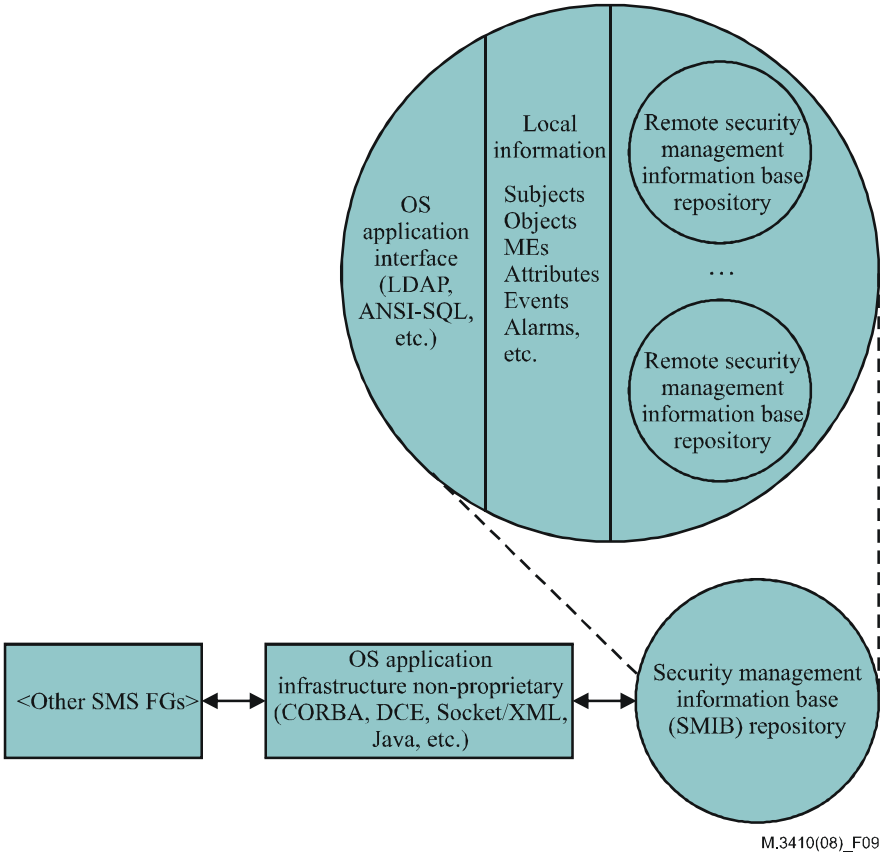

Figure 9 – Security management information FG logical block diagram

The security management information FG provides the functionality to manage the storage security-related information, and meta-data, both local to the SMS and remotely on other non-SMS systems. The purpose of this FG is to make the location, management of storage, and even format, of security information transparent to requesting SMS FGs.

SEC-62: The security management information base repository should be a de jure standards-based approach, such as ANSI structured query language (ANSI-SQL) or LDAP accessible database.

SEC-63: The security management information base repository should contain each managed element's security attributes.

SEC-64: The security management information base repository's attributes should 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; and
- The event type for each change of the attribute value.

SMS FEs communicate with the repository through the use of appropriate non-proprietary protocols, such as LDAP or ANSI-SQL.

SEC-65: The security management information base repository should have the ability to know where information is stored (local vs remote).

SEC-66: The security management information base repository should be able to add information at the storing location.

SEC-67: The security management information base repository should be able to modify information at the storing location.

SEC-68: The security management information base repository should be able to delete information at the storing location.

SEC-69: The security management information base repository should be able to retrieve information from the storing location.

SEC-70: The security management information base repository may be front-ended by an intermediary that can perform some of the responsibilities normally provided by FEs within this FG.

7.10 Communications interface FG

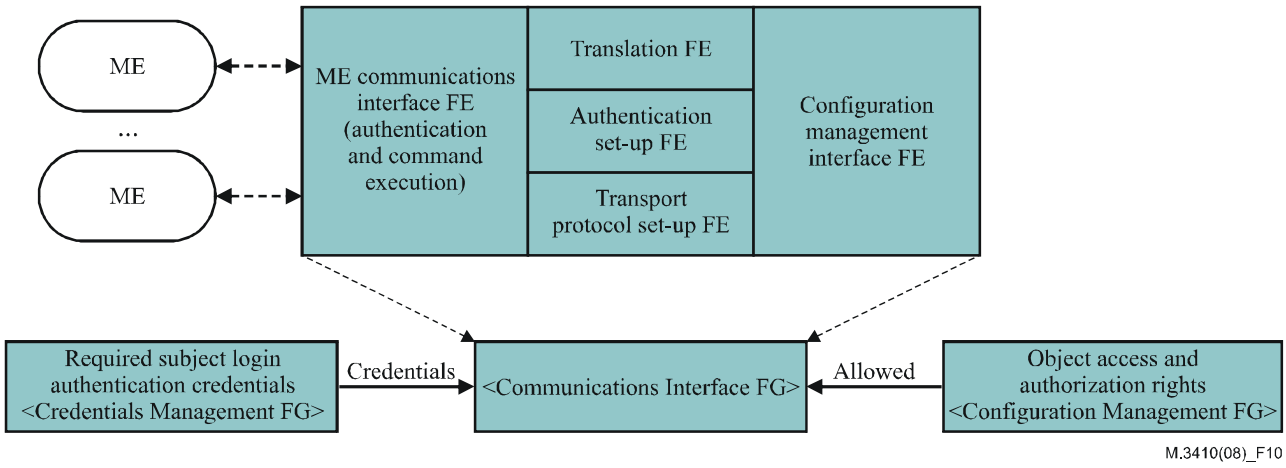

Figure 10 – Communications Interface FG logical block diagram

The communications interface FG provides the interfaces between SMS FGs, between SMS FEs and between SMS FGs and the MEs. As an example, the communications interface FG converts the generic configuration statements defined in the configuration management FG into the specific commands for each type of ME. The commands are passed to each ME in the appropriate supported protocol, such as IP, X.25, XML, SNMPv3, HTTP, HTTPS, telnet, FTP, TFTP, scp, sftp, etc. The communications interface FG also provides the SMS communications infrastructure between the SMS FGs.

SEC-71: The SMS FGs will communicate with the SMS FGs and other interface modules through the use of protocols in compliance with [ITU-T M.3016.1].

SEC-72: The communications interface FEs should set up the authentication request to the managed element and authenticate itself prior to the execution of the commands.

SEC-73: The vendor of SMS FEs should provide an API in their application so that managed element vendors may supply their own interface modules.

SEC-74: The communications interface FEs should obtain any necessary authentication credentials from a credentials management FE (or delegated authentication application), when required, for authenticating interaction with other MEs.

SEC-75: Confidentiality should be supported for all ME – SMS interaction.

7.10.1 ME communications interface FE

The ME communications interface FE is responsible for the management protocol level interaction between the SMS FGs and the MEs. This FE may include multiple modules necessary to support the wide diversity of deployed MEs, many using different *de facto* or de jure management protocols.

7.10.2 Translation FE

The translation FE is responsible for translating commands and responses from the SMS meta language format to the format(s) required for particular types of MEs. Similarly, it is responsible for translating commands and responses from the ME-specific format to the format required by the SMS. This translation may require converting messages between a number of syntactical, and possibly semantically, different formats. There may be multiple translation FEs based on the different types of ME communication required, different areas of ME communication (such as alarm-specific translation) and different ME protocols (such as translation based on a specific SNMP MIB). This FE is necessary as there is no common standardized communication protocol deployed in modern infrastructures.

7.10.3 Authentication set-up FE

The authentication set-up FE is responsible for interacting with the ME communications interface FE to handle authentication and dynamic credentials negotiation not directly handled by the ME communications interface FE or the transport protocol set-up FE.

7.10.4 Transport protocol set-up FE

The transport protocol set-up FE is responsible for controlling dynamic credentials negotiation not directly handled by the ME communications interface FE or the authentication set-up FE. This FE determines, based on policy, whether layer 3 (e.g., IPSec) mechanisms or layer 4 (e.g., TLS, SSL, DTLS, SSH) mechanisms are required and ensures that the appropriate security mechanism is engaged.

7.10.5 Configuration management interface FE

The configuration management interface FE provides the interface to and from the configuration management FG FEs.

Annex A

Proforma – M.3410 – SMS requirements

(This annex forms an integral part of this Recommendation)

A.1 Basis of profile proforma for security requirements

A.1.1 Overview

This Recommendation specifies 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 infrastructure. Because different administrations and organizations require varying levels of security support, this Recommendation does not specify whether a requirement is mandatory or optional.

The proforma defined in this Recommendation is to assist administrations and other national/international organizations to specify the mandatory and optional support of the requirements.

The proforma is specified using the numbered requirements from this Recommendation.

A.2 Guidelines and instructions for proforma specification

The proforma is specified using tabular representation. The proforma table has the following columns:

a) The requirement number from the Recommendation;

b) Status;

c) Comments or notes.

The tables in this Recommendation have the first column completed. Organizations using the profiles should complete the tables as follows.

For each requirement in the status column indicate:

m Mandatory;

o Optional;

c Conditional;

x Prohibited ("x" stands for "excluded");

– Not applicable or out of scope.

If status is "c", the comment column should define the condition that must be true for supporting the requirement.

The comment column is used to include information relevant for implementing the requirement according to that profile.

A.3 Proforma

A.3.1 M.3410 security requirements

Table A.1 contains the requirements from this Recommendation and the user should complete the other columns according to the guidelines provided above.

Table A.1 – Proforma for requirements in Recommendation ITU-T M.3410

Security requirements	Status	Comments
SEC-1		
SEC-2		
SEC-3		
SEC-4		
SEC-5		
SEC-6		
SEC-7		
SEC-8		
SEC-9		
SEC-10		
SEC-11		
SEC-12		
SEC-13		
SEC-14		
SEC-15		
SEC-16		
SEC-17		
SEC-18		
SEC-19		
SEC-20		
SEC-21		
SEC-22		
SEC-23		
SEC-24		
SEC-25		
SEC-26		
SEC-27		
SEC-28		
SEC-29		
SEC-30		
SEC-31		
SEC-32		
SEC-33		
SEC-34		
SEC-35		
SEC-36		
SEC-37		
SEC-38		
SEC-39		

Table A.1 – Proforma for requirements in Recommendation ITU-T M.3410

Security requirements	Status	Comments
SEC-40		
SEC-41		
SEC-42		
SEC-43		
SEC-44		
SEC-45		
SEC-46		
SEC-47		
SEC-48		
SEC-49		
SEC-50		
SEC-51		
SEC-52		
SEC-53		
SEC-54		
SEC-55		
SEC-56		
SEC-57		
SEC-58		
SEC-59		
SEC-60		
SEC-61		
SEC-62		
SEC-63		
SEC-64		
SEC-65		
SEC-66		
SEC-67		
SEC-68		
SEC-69		
SEC-70		
SEC-71		
SEC-72		
SEC-73		
SEC-74		
SEC-75		

Appendix I

Relationship of security management concepts to [ITU-T X.800]

(This appendix does not form an integral part of this Recommendation)

Clause 8 of [ITU-T X.800] addresses many aspects of security management for open systems interconnection. The X.800 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.

I.1 Trust domains

Clause 8.1.2 of [ITU-T X.800] begins its security management discussion by considering security policy and security domains. 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 [ITU-T X.810], the OSI security frameworks overview. 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 the need for the subset and superset notions.

I.2 Security management information bases

Clause 8.1.4 of [ITU-T X.800] 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 end system 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 end systems. In practice, parts of the SMIB may or may not be integrated with the MIB."

The TSP security architecture uses SMIBs to conduct trust domain and ME management, rather than for only ME management, as implied above by the appropriate security policy for each ME. 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 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.)

I.3 Trust domain SMIB content

The following examples of 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); and
- Security service and security mechanism requirements for specific applications, including intra-domain communications and inter-domain information transfer.

I.3.1 ME SMIB content

The ME 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., credential management). More detail is given in later clauses on several of the supporting security applications and related functions. The following example classes of objects might be included in the SMIB:

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

I.3.2 SMIB examples

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

- X.509v3 certificates [ITU-T X.509] 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, security event, security-related alarm, security alarm and audit data.
- ME security-related configuration data for those security services supported within each ME within the TSP infrastructure. This information will include, for each ME, object access control lists, network layer packet filtering rules, application layer message filtering rules, credential management, encryption, integrity, signature algorithm identifiers, and security protocol objects for both managed element security associations (ME-SAs) and application process security associations (APP-SAs), ME-SA default parameters, ME-SA options, APP-SA default parameters, APP-SA options, security event reporting parameters, security log management parameters, etc.

ME SMIB security information items include:

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

Some SMIB items may be held in the Directory services for ease of access by many users. Such items might include credential management information (e.g., certificates and user keying material). SMIB information stored in X.500 directories [ITU-T X.500] must be integrity-protected.

I.4 Communication of security management information

Clause 8.1.5 of [ITU-T X.800] 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 shall 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 MEs are described in clause 6.

Interactive distributed security exists when two different MEs 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-ME security associations
2) Inter-application process security associations.

I.4.1 Inter-ME security associations (ME-SAs)

ME-SAs ensure secure communication between the two MEs engaged in communication. These ME-SAs provide continuous ME data origin authentication, data integrity, and optional message level confidentiality. The TSP security architecture relies on the capabilities within the IPSec protocol suite for the establishment of ME-SAs. However, alternative forms of security associations provided by TLS v1, SSL v3, datagram transport layer security (DTLS) v1 [b-IETF RFC 4347] and SSH are reasonable substitutes for IPSec, provided the default encryption does not have a performance or functionality impact.

I.4.2 Inter-application process security associations (APP-SAs)

APP-SAs ensure secure communication between a pair of application processes executing within different MEs. These APP-SAs provide peer-entity authentication and selective field data confidentiality. The TSP security architecture relies on the capabilities within the existing application layer protocols for the establishment of ME-SAs. APP-SAs between two MEs may share the same cryptographic algorithm and keys used by an ME-SA, or use different ME-SAs between the two communication MEs. The choice of which APP-SA to ME-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 ME (e.g., authenticated identity, access privileges). These attributes might be contained in a security certificate such as that defined in [ITU-T X.509]. The information contained in an X.509v3 certificate [ITU-T X.509] 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.

I.5 Distributed security management administration

Clause 8.1.6 of [ITU-T X.800] 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 methods not standardized by OSI [direct interaction with the MNE]. In other cases, it may be desirable to exchange such information over an OSI communication path in which case the information will be passed between two security management applications running in the real open systems. 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 credential 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 administering MEs within the transport plane and, at the same time, relies upon the transport planes MEs 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 MEs in which management applications are implemented only communicate as peers.

Management systems are composed of management applications implemented in MEs. Some management applications must coexist with other applications in MEs within the network element layer (NEL) of the telecommunications management network (TMN) model. For logistical reasons, it is necessary to dedicate some MEs 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; and
- Business management.

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

I.5.1 Security management application protocols

Clause 8.1.7 of [ITU-T X.800] requires security management application protocols for the exchange of security-relevant information. The general management application protocols used within the TSP security architecture are specified in [ITU-T M.3016.1].

I.5.2 ME security management functions

Clause 8.2.1 of [ITU-T X.800] observes the following about system security management:

> "System security management is concerned with the management of security aspects of the overall OSI environment. The following list is typical of the activities, which fall into this category of security management:
>
> a) overall security policy management, including updates and maintenance of consistency;
> b) interaction with other OSI management functions;
> c) interaction with security service management and security mechanism management;
> d) event handling management;
> e) security audit management; and
> f) security recovery management."

As noted previously, the TSP security architecture broadens the view of ME 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.

Clause 8.3.1 of [ITU-T X.800] 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."

Clause 8.3.2 of [ITU-T X.800] describes security audit management as follows:

> "Security audit management may include:
>
> a) the selection of events to be logged and/or remotely collected;
>
> b) the enabling and disabling of audit trail logging of selected events;
>
> c) the remote collection of selected audit records; and
>
> d) the preparation of security audit reports."

Clause 8.3.3 of [ITU-T X.800] describes security recovery management as follows:

> "Security recovery management may include:
>
> a) maintenance of the rules used to react to real or suspected security violations;
>
> b) the remote reporting of apparent violations of system security;
>
> c) security administrator interactions."

These security functions are related since the event handling function deals with all the apparent security violations recognized by an ME, 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 ME 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 objects may be recorded in a particular management trust domain SMIB, an ME 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.

I.5.3 Security service management

Clause 8.2.2 of [ITU-T X.800] describes security service management as follows:

> "Security service management is concerned with the management of particular security services. The following list is typical of the activities which may be performed in managing a particular security service:
>
> a) determination and assignment of the target security protection for the service;
>
> b) assignment and maintenance of rules for the selection (where alternatives exist) of the specific security mechanism to be employed to provide the requested security service;
>
> c) negotiation (locally and remotely) of available security mechanisms which require prior management agreement;
>
> d) invocation of specific security mechanisms via the appropriate security mechanism management function e.g., for the provision of administratively-imposed security services; and
>
> e) interaction with other security service management functions and security mechanism management functions."

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 security management application process 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.

I.5.4 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 ME. 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 thus may be required (by written policy) to employ a non-repudiation service. In cases like these, a selective means of invoking the security service must be available, but the strength of the service is likely to be predetermined.

I.5.5 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 the service. 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 MEs. In particular, the ME 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 ME than when protecting information between MEs within the same trust domain or between MEs 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 ME supports security services with different mechanisms and a security management application process is aware (or can be made aware) of the distinctions among activities within a trust domain, between MEs in the same trust domain, and between MEs 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 MEs in the same trust domain often exchange large files, but only infrequently with MEs 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.

I.5.6 Negotiating available security mechanisms

One or more MEs 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 ME. In such cases, the specific security mechanisms to be employed must be negotiated between the security services in the MEs at the time the security association is established between them.

I.5.7 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 security management application process 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 security management application process invokes the default security mechanism.

Although each application could make requests for security services and security mechanisms directly to the security management application process, there are significant advantages to adopting an application programming 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 define 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. The GSS API and other related APIs could be used to invoke all security functions by making them the standard interfaces to the security management application process (they could be incorporated into the security management application process).

The use of a combination of the GSS API, security management application processes, 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 ME life cycle, and for MEs to accommodate trust domains with different security service requirements.

I.6 Security mechanism management

Clause 8.2.3 of [ITU-T X.800] 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:
>
> a) key management;
>
> b) encipherment management;
>
> c) digital signature management;
>
> d) access control management;
>
> e) data integrity management;
>
> f) authentication management;
>
> g) traffic padding management;
>
> h) routing control management; and
>
> i) notarization management."

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

I.6.1 Key management

Clause 8.4.1 of [ITU-T X.800] describes key management as follows:

> "Key management may involve:
>
> a) generating suitable keys at intervals commensurate with the level of security required;
>
> b) determination, in accordance with access control requirements, of which entities should receive a copy of each key; and
>
> c) 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 centre 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.

I.6.2 Encryption management

Clause 8.4.2 of [ITU-T X.800] describes encryption (encipherment) management as follows:

"Encipherment management may involve:

a) interaction with key management;

b) establishment of cryptographic parameters;

c) 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 MEs. 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 ME.

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 centre 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.

I.6.3 Digital signature and authenticator management

Clause 8.4.3 of [ITU-T X.800] describes digital signature management as follows:

"Digital signature management may involve:

a) interaction with key management;

b) establishment of cryptographic parameters and algorithms; and

c) 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.

I.6.4 Access control management

Clause 8.4.4 of [ITU-T X.800] describes access control management as follows:

> "Access control management may involve distribution of security attributes (including passwords) 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 ME that supports a trust domain, it may be necessary to convey access control attributes between MEs. 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.

I.6.5 Data integrity management

Clause 8.4.5 of [ITU-T X.800] describes data integrity management as follows:

> "Data integrity management may involve:
>
> a) interaction with key management;
>
> b) establishment of cryptographic parameters and algorithms; and
>
> c) 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 ME, 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.

I.6.6 Authentication management

Clause 8.4.6 of [ITU-T X.800] 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 ME identities. With MEs, the certificates and ME private keys are stored within the ME or can be stored in a smart card that is inserted into a smart card reader built into the ME. When using smart cards with MEs, the smart card reader needs to include a lockable access door to reduce the probability of unauthorized smart card removal.

I.6.7 Traffic padding management

Clause 8.4.7 of [ITU-T X.800] 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:
>
> a) pre-specified data rates;
> b) specifying random data rates;
> c) specifying message characteristics such as length; and
> d) 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.

I.6.8 Routing control management

Clause 8.4.8 of [ITU-T X.800] 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 ME is connected to multiple networks.

I.6.9 Notarization management

Clause 8.4.9 of [ITU-T X.800] defines notarization management as follows:

> "Notarization management may include:
>
> a) the distribution of information about notaries;
>
> b) the use of a protocol between a notary and the communicating entities; and
>
> c) interaction with notaries."

The role of notarization management within the TSP security architecture is to be determined.

I.6.10 Availability management

Availability management is not described in [ITU-T X.800]. Availability mechanisms in communications networks and MEs 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.

Appendix II

SMS relationship with the role of security in other TSP management frameworks and systems

(This appendix does not form an integral part of this Recommendation)

II.1 SMS relationship to ITU-T management Recommendations

Both [b-ITU-T M.3400] and [ITU-T M.3050.2] consider system/network management capabilities. [b-ITU-T M.3400] looks at management from a functionality perspective; whereas [ITU-T M.3050.2] takes a services perspective.

II.1.1 SMS relationship to [ITU-T M.3010]

[ITU-T M.3010] addresses the functional principles and organization of a telecommunications management network (TMN) for managing networks. This Recommendation only touches on security in clause 7 as part of the following FCAPS management functional areas:

- Fault management;
- Configuration management;
- Accounting management;
- Performance management;
- Security management.

II.1.2 SMS relationship to [ITU-T M.3050.2]

[ITU-T M.3050.2] addresses the requirements, services, and structure of the enhanced telecom operations map (eTOM) concepts for managing networks. Table II.1 provides an example of mapping the SMS FGs to eTOM processes in [ITU-T M.3050.2].

Table II.1 – Mapping [ITU-T M.3050.2] services to SMS framework

Administrator interface FG	Administrator account management FG	Credentials management FG	Configuration management FG	Fault management FG	Security policy management FG	Verification &validation management FG	Corrective action management FG	SMI FG	Communications interface FG	No corresponding SMS clause	[b-ITU-T M.3400] function name	eTOM process ID [ITU-T M.3050.2]	eTOM process name
											Security management		
												1.A.3.4	Resource Performance Management
												1.E.2	Enterprise Risk Management
												1.E.6	Stakeholder & External Relations Management
												1.OFAB.1	Customer Relationship Management
												1.OFAB.2	Service Management & Operations
										X	Prevention		
												1.E.2.2	Security Management
												1.E.6.5	Legal Management
												1.F.1.5	Order Handling
										X	Legal review function set		

Table II.1 – Mapping [ITU-T M.3050.2] services to SMS framework

Administrator interface FG	Administrator account management FG	Credentials management FG	Configuration management FG	Fault management FG	Security policy management FG	Verification &validation management FG	Corrective action management FG	SMI FG	Communications interface FG	No corresponding SMS clause	[b-ITU-T M.3400] function name	eTOM process ID [ITU-T M.3050.2]	eTOM process name
												1.E.6.5	Legal management
										X	Physical access security function set		
												1.E.2.2	Security Management
										X	Guarding function set		
												1.E.2.2	Security Management
										X	Personnel risk analysis function set		
												1.E.2.2	Security Management
										X	Security screening function set		
												1.F.1.5.2	Authorize Credit
											Detection		
												1.E.2.2	Security Management
												1.E.2.3	Fraud Management
												1.FAB.4.6	S/P Interface Management
												1.O.3.1	Resource Data Collection & Processing
												1.SIP.3	Resource Development & Management
X			X			X		X	X		Investigation of changes in revenue patterns function set		
												1.E.2.3	Fraud Management
X			X	X				X	X		Support element protection function set		
												1.AB.3.5.1	Collect Resource Data
												1.AB.3.5.2	Process Resource Data
												1.AB.3.5.3	Report Resource Data
												1.AB.3.5.4	Audit Resource Usage Data
X			X	X			X	X	X		Customer security alarm function set		
												1.E.2.2	Security Management
X			X			X		X	X		Customer (external user) profiling function set		
												1.E.2.3	Fraud Management
X			X			X		X	X		Customer usage pattern analysis function set		
												1.AB.3.5.2	Process Resource Data
												1.AB.3.5.4	Audit Resource Usage Data
												1.E.2.3	Fraud Management
X			X			X		X	X		Investigation of theft of service function set		
												1.E.2.3	Fraud Management
												1.FAB.1.9.3	Analyse and Manage Customer Risk
X			X			X		X	X		Internal traffic and activity pattern analysis function set		
												1.O.3.1.2	Enable Resource Performance Management

Table II.1 – Mapping [ITU-T M.3050.2] services to SMS framework

Administrator interface FG	Administrator account management FG	Credentials management FG	Configuration management FG	Fault management FG	Security policy management FG	Verification &validation management FG	Corrective action management FG	SMI FG	Communications interface FG	No corresponding SMS clause	[b-ITU-T M.3400] function name	eTOM process ID [ITU-T M.3050.2]	eTOM process name
												1.O.3.1.4	Enable Resource Data Collection & Processing
X			X	X			X	X	X		Network security alarm function set		
												1.E.2.2	Security Management
												1.O.3.1.4	Enable Resource Data Collection & Processing
X			X			X		X	X		Software intrusion audit function set		
												1.AB.3.5.4	Audit Resource Usage Data
												1.E.2.2	Security Management
X			X	X			X	X	X		Support element security alarm reporting function set		
												1.E.2.2	Security Management
												1.O.3.1.4	Enable Resource Data Collection & Processing
											Containment and Recovery		
												1.E.2.1	Business Continuity Management
												1.E.2.2	Security Management
												1.E.6.5	Legal management
												1.S.3.1	Resource Strategy & Planning
X		X	X					X	X		Protected storage of business data function set		
												1.E.2.1	Business Continuity Management
X		X		X			X	X	X		Network intrusion recovery function set		
												1.F.3.2.2	Configure & Activate Resource
X		X	X					X	X		Administration of network revocation list function set		
												1.E.2.2	Security Management
X		X	X					X	X		Protected storage of network configuration data function set		
												1.E.2.1	Business Continuity Management
X		X	X				X	X	X		Severing internal connections function set		
												1.F.3.2.2	Configure & Activate Resource
X		X		X			X	X	X		NE(s) intrusion recovery function set		
												1.F.3.2.2	Configure & Activate Resource
X		X	X					X	X		Administration of NE(s) revocation list function set		
												1.E.2.2	Security Management
X		X	X					X	X		Protected storage of NE(s) configuration data function set		
												1.E.2.1	Business Continuity Management

Table II.1 – Mapping [ITU-T M.3050.2] services to SMS framework

Administrator interface FG	Administrator account management FG	Credentials management FG	Configuration management FG	Fault management FG	Security policy management FG	Verification &validation management FG	Corrective action management FG	SMI FG	Communications interface FG	No corresponding SMS clause	[b-ITU-T M.3400] function name	eTOM process ID [ITU-T M.3050.2]	eTOM process name
X		X		X			X	X	X		Exception report action function set		
												1.F.3.2.2	Configure & Activate Resource
												1.F.3.2.4	Collect, Update & Report Resource Configuration Data
X		X		X			X	X	X		Theft of service action function set		
												1.E.2.2	Security Management
												1.E.6.5	Legal Management
												1.F.3.2.4	Collect, Update & Report Resource Configuration Data
										X	Legal action function set		
												1.E.6.5	Legal Management
										X	Apprehending function set		
												1.E.2.2	Security Management
X		X		X			X	X	X		Service intrusion recovery function set		
												1.F.2.2.4	Implement & Configure Service
X		X	X					X	X		Administration of customer revocation list function set		
												1.E.2.2	Security Management
X		X	X					X	X		Protected storage of customer data function set		
												1.E.2.1	Business Continuity Management
X		X					X	X	X		Severing external connections function set		
												1.F.3.2.2	Configure & Activate Resource
											Security Administration		
												1.B.2.5	Service & Specific Instance Rating
												1.E.2.1	Business Continuity Management
												1.E.2.2	Security Management
												1.E.2.4	Audit Management
												1.FAB.4.6	S/P Interface Management
												1.S.3.1	Resource Strategy & Planning
					X					X	Security policy function set		
												1.E.2.2	Security Management
										X	Disaster recovery planning function set		
												1.E.2.1	Business Continuity Management
										X	Manage guards function set		
												1.E.2.2	Security Management

Table II.1 – Mapping [ITU-T M.3050.2] services to SMS framework

Administrator interface FG	Administrator account management FG	Credentials management FG	Configuration management FG	Fault management FG	Security policy management FG	Verification &validation management FG	Corrective action management FG	SMI FG	Communications interface FG	No corresponding SMS clause	[b-ITU-T M.3400] function name	eTOM process ID [ITU-T M.3050.2]	eTOM process name
X			X	X				X	X		Audit trail analysis function set		
												1.E.2.2	Security Management
												1.E.2.4	Audit Management
X			X	X			X	X	X		Security alarm analysis function set		
												1.E.2.2	Security Management
												1.O.3.1.4	Enable Resource Data Collection & Processing
										X	Assessment of corporate data integrity function set		
												1.E.2.2	Security Management
X	X	X	X					X	X		Administration of external authentication function set		
												1.E.2.2	Security Management
X	X		X					X	X		Administration of external access control function set		
												1.E.2.2	Security Management
X	X	X	X					X	X		Administration of external certification function set		
												1.E.2.2	Security Management
X	X	X	X					X	X		Administration of external encryption and keys function set		
												1.E.2.2	Security Management
X			X					X	X		Administration of external security protocols function set		
												1.E.2.2	Security Management
X			X	X				X	X		Customer audit trail function set		
												1.B.2.5.3	Analyse Usage Records
												1.E.2.2	Security Management
												1.E.2.4	Audit Management
X			X	X			X	X	X		Customer security alarm management function set		
												1.E.2.2	Security Management
												1.O.3.1.4	Enable Resource Data Collection & Processing
X			X	X				X	X		Testing of audit trail mechanism function set		
												1.E.2.4	Audit Management
X	X	X	X					X	X		Administration of internal authentication function set		
												1.E.2.2	Security Management
X	X		X					X	X		Administration of internal access control function set		
												1.E.2.2	Security Management
X	X	X	X					X	X		Administration of internal certification function set		
												1.E.2.2	Security Management
X	X	X	X					X	X		Administration of internal encryption and keys function set		
												1.E.2.2	Security Management
X			X	X				X	X		Network audit trail management function set		

Table II.1 – Mapping [ITU-T M.3050.2] services to SMS framework

Administrator interface FG	Administrator account management FG	Credentials management FG	Configuration management FG	Fault management FG	Security policy management FG	Verification &validation management FG	Corrective action management FG	SMI FG	Communications interface FG	No corresponding SMS clause	[b-ITU-T M.3400] function name	eTOM process ID [ITU-T M.3050.2]	eTOM process name
												1.E.2.2	Security Management
												1.E.2.4	Audit Management
												1.F.3.2.4	Collect, Update & Report Resource Configuration Data
X			X	X			X	X	X		Network security alarm management function set		
												1.E.2.2	Security Management
												1.O.3.1.4	Enable Resource Data Collection & Processing
X			X	X				X	X		NE(s) audit trail management function set		
												1.E.2.2	Security Management
												1.E.2.4	Audit Management
												1.F.3.2.4	Collect, Update & Report Resource Configuration Data
X			X	X			X	X	X		NE(s) security alarm management function set		
												1.E.2.2	Security Management
												1.O.3.1.4	Enable Resource Data Collection & Processing
X	X	X	X					X	X		Administration of keys for NEs function set		
												1.E.2.2	Security Management
X	X	X	X					X	X		Administration of keys by an NE function set		
												1.E.2.2	Security Management

Decomposition of SMS functionality sufficient for detailed mapping to all eTOM Processes, and sub-processes, requires further study.

II.1.3 SMS relationship to [ITU-T M.3060]

[ITU-T M.3060] addresses the requirements, services, and structure of the NGN management architecture. Although clause 9.5 of [ITU-T M.3060], security considerations, notes "Security is an extensive domain with a mission to protect important business assets against different types of threats." and sites both ITU-T Recommendations M.3016-series and [ITU-T X.805]. [ITU-T M.3060] simply states that "To deal with the complexity of securing all of the NGN, including its management plane, there is a need to mechanize the application of various security services, mechanisms, and tools by employing operation systems to automate the process. Requirements and architecture for such operations systems, also known as Security Management Systems (SMS), is for further study."

II.1.4 SMS relationship to [b-ITU-T M.3400] management service function sets

[b-ITU-T M.3400] notes that a "TMN management function is a cooperative interaction between application processes in managing and managed systems for the management of telecommunications resources, and is the smallest functional part of a TMN management service as perceived by the TMN users."

[b-ITU-T M.3400] goes on to say:

> "Within the scope of TMN management context, TMN management services are defined by the descriptions of roles, related resources and TMN functions. The TMN management functions that belong together according to context are grouped into TMN management function sets (and the sets into groups) for the purpose of management information modelling. TMN management function sets may be reusable for TMN management services applied to different telecommunications managed areas.
>
> TMN management function sets are described from the TMN users' perspective and they are independent from the individual protocols as well as management information modelling so that the applicability to the diversified protocols in TMN interfaces will be maintained.
>
> The managers and agents identified in this Recommendation are capabilities of function blocks in TMN building blocks: Operations Systems (OSs), Mediation Devices, Network Elements (NEs), Work Stations, or Q Adaptors. Function blocks in NEs and Q Adaptors act as agents when interacting with function blocks in OSs and Mediation Devices. Further information is provided in specific Recommendations on TMN Management Services.
>
> Each TMN Management Function Set contains a list of the TMN Management Functions that are supported by a function block.
>
> The Management Requirements subclause for each TMN Management Function Set describes the purpose, internal functionality and overall input and output information flow to the function block that supports the TMN Function Set.
>
> A recommended assignment to a logical layer is provided for each function block (where possible). For example, a function block that deals with requests for a service sent by a service customer to a service provider would be assigned to the Service Management Layer (the block would be called an S-OSF, an Operations System Function block of the Service Management Layer). Such an assignment would imply that the TMN Management Functions, in the context of that TMN Management Function Set, could be used within the Service Management layer, or between that layer and any other layer (as specified in the General Functional Model)."

Table II.2 provides an example of mapping the SMS FGs to function sets in [b-ITU-T M.3400].

Table II.2 – Mapping [b-ITU-T M.3400] services to SMS framework

[b-ITU-T M.3400] clause	[b-ITU-T M.3400] function set	Administrator interface FG	Administrator account management FG	Credential management FG	Configuration management FG	Fault management FG	Security policy management FG	Verification & validation management FG	Corrective action management FG	SMI FG	Communications interface FG	No corresponding SMS clause
9	Security Management	–	–	–	–	–	–	–	–	–	–	–
9.1	Prevention	–	–	–	–	–	–	–	–	–	–	–
9.1.1	Legal review											X
9.1.2	Physical access security											X
9.1.3	Guarding											X
9.1.4	Personnel risk analysis											X
9.1.5	Security screening											X
9.2	Detection	–	–	–	–	–	–	–	–	–	–	–
9.2.1	Investigation of changes in revenue patterns	X			X			X(1)		X	X	
9.2.2	Support element protection	X			X	X(2)				X	X	

Table II.2 – Mapping [b-ITU-T M.3400] services to SMS framework

[b-ITU-T M.3400] clause	[b-ITU-T M.3400] function set	Administrator interface FG	Administrator account management FG	Credential management FG	Configuration management FG	Fault management FG	Security policy management FG	Verification & validation management FG	Corrective action management FG	SMI FG	Communications interface FG	No corresponding SMS clause
9.2.3	Customer security alarm	X			X	X(3)			X(4)	X	X	
9.2.4	Customer (external user) profiling	X			X			X(5)		X	X	
9.2.5	Customer usage pattern analysis	X			X			X(6)		X	X	
9.2.6	Investigation of theft of service	X			X			X(7)		X	X	
9.2.7	Internal traffic and activity pattern analysis	X			X			X(8)		X	X	
9.2.8	Network security alarm	X			X	X(3)			X(4)	X	X	
9.2.9	Software intrusion audit	X			X			X(9)		X	X	
9.2.10	Support element security alarm reporting	X			X	X(3)			X(4)	X	X	
9.3	Containment and Recovery	–	–	–	–	–	–	–	–	–	–	–
9.3.1	Protected storage of business data	X		X	X					X	X	
9.3.2	Exception report action	X		X		X(10)			X(4)	X	X	
9.3.3	Theft of service action	X		X		X(10)			X(4)	X	X	
9.3.4	Legal action											X
9.3.5	Apprehending											X
9.3.6	Service intrusion recovery	X		X		X(10)			X(4)	X	X	
9.3.7	Administration of customer revocation list	X		X	X					X	X	
9.3.8	Protected storage of customer data	X		X	X					X	X	
9.3.9	Severing external connections	X		X					X(4)	X	X	
9.3.10	Network intrusion recovery	X		X		X(10)			X(4)	X	X	
9.3.11	Administration of network revocation list	X		X	X					X	X	
9.3.12	Protected storage of network configuration data	X		X	X					X	X	
9.3.13	Severing internal connections	X		X	X				X(4)	X	X	
9.3.14	NE(s) intrusion recovery	X		X		X(10)			X(4)	X	X	
9.3.15	Administration of NE(s) revocation list	X		X	X					X	X	
9.3.16	Protected storage of NE(s) configuration data	X		X	X					X	X	
9.4	Security Administration	–	–	–	–	–	–	–	–	–	–	–
9.4.1	Security policy						X					X
9.4.2	Disaster recovery planning											X
9.4.3	Manage guards											X
9.4.4	Audit trail analysis	X			X	X(11)				X	X	
9.4.5	Security alarm analysis	X			X	X(3)			X(4)	X	X	

Table II.2 – Mapping [b-ITU-T M.3400] services to SMS framework

[b-ITU-T M.3400] clause	[b-ITU-T M.3400] function set	Administrator interface FG	Administrator account management FG	Credential management FG	Configuration management FG	Fault management FG	Security policy management FG	Verification & validation management FG	Corrective action management FG	SMI FG	Communications interface FG	No corresponding SMS clause
9.4.6	Assessment of corporate data integrity											X
9.4.7	Administration of external authentication	X	X(12)	X	X					X	X	
9.4.8	Administration of external access control	X	X(13)		X					X	X	
9.4.9	Administration of external certification	X	X	X	X					X	X	
9.4.10	Administration of external encryption and keys	X(14)	X(14)	X(14)	X(14)					X(14)	X(14)	
9.4.11	Administration of external security protocols	X			X					X	X	
9.4.12	Customer audit trail	X			X	X(11)				X	X	
9.4.13	Customer security alarm management	X			X	X(3)			X(4)	X	X	
9.4.14	Testing of audit trail mechanism	X			X	X(11)				X	X	
9.4.15	Administration of internal authentication	X	X(12)	X	X					X	X	
9.4.16	Administration of internal access control	X	X(13)		X					X	X	
9.4.17	Administration of internal certification	X	X	X	X					X	X	
9.4.18	Administration of internal encryption and keys	X(14)	X(14)	X(14)	X(14)					X(14)	X(14)	
9.4.19	Network audit trail management	X			X	X(11)				X	X	
9.4.20	Network security alarm management	X			X	X(3)			X(4)	X	X	
9.4.21	NE(s) audit trail management	X			X	X(11)				X	X	
9.4.22	NE(s) security alarm management	X			X	X(3)			X(4)	X	X	
9.4.23	Administration of keys for NEs	X(14)	X(14)	X(14)	X(14)					X(14)	X(14)	
9.4.24	Administration of keys by an NE	X(14)	X(14)	X(14)	X(14)					X(14)	X(14)	

Table II.3 – Notes for Table II.2

X(n) where n =	SMS Functional Entities (FEs) within SMS Functional Groups (FGs)
1	External (Adjunct) Revenue Analysis FE that interacts with the Verification & Validation FG
2	Security Event Mgt. FE within the Fault Mgt. FG
3	Security Alarm Mgt. FE and attack analysis FE within the Fault Mgt. FG
4	Response FE within the Corrective Action Mgt. FG
5	Adjunct Security, Device and Application Interface FE within the Verification & Validation FG that interacts with an external system
6	External system that interacts with the Adjunct Security, Device and Application Interface FE within the Verification & Validation FG
7	Adjunct Security, Device and Application Interface FE within the Verification & Validation FG that interacts with an external system
8	Adjunct Security, Device and Application Interface FE within the Verification & Validation FG that interacts with an external system
9	Adjunct Security, Device and Application Interface FE within the Verification & Validation FG that interacts with an external system
10	Attack Analysis FE within the Fault Mgt. FG
11	ME Log Mgt. FE within the Fault Mgt. FG
12	Authentication Mgt. FE within the Administrator Account Mgt. FG
13	Subject Mgt, Subject Group Mgt., Subject Propagation Mgt., Authentication Mgt. FEs within the Administrator Account Mgt. FG
14	SMS FEs involved to the extent necessary to support key distribution and session symmetric keys not dynamically managed by MEs via IPSec, TLS/SSL, SSH, XML type mechanisms

Decomposition of SMS functionality sufficient for detailed mapping to all [b-ITU-T M.3400] function sets requires further study.

II.2 Security of legacy/existing management systems

Operations systems (OSs), also referred to as OSSs, 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 voice, data, and application/presentation level interfaces.

As the OS is nothing more than 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 authoritative 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.
- Authoritative 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 OS 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 OS 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. By using a myriad of different architecture types and systems as well, 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 OS are the requirements placed upon security by the element management systems (EMSs) as well as the network management systems (NMSs). Therefore, woven into this clause will be a description of the additional requirements above and beyond those needed by the OS.

In the following subclause is a brief description of the various services that the OS and EMSs support in today's environment, and what specifically those systems export that require security management. In some cases, the OS and EMSs 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 OS. This clause is then concluded with a description of the services that are or will exist within the OS and EMSs that require management by the SMS.

II.2.1 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 centres, 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, which is simply a message broker that bridges the traffic from competitive local exchange carrier (CLEC)/data local exchange carrier (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 fulfil 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 Key ring to support the message broker in order to ensure the identity 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 be – and is – utilized for single point of access for public key requests and to ensure its authenticity, as well as 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/DLECs. 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 southbound 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 security commensurate with the level of sensitivity.

Both local and external orders are stored in a long-term storage system, as well as 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.

II.2.2 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 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 northbound interfaces to test and fault management OS 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 it 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 communicate either to the EMS/NMS or to the managed element directly through 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 MEs to make the necessary changes to support the new service for the customer. It has the capability to pull back all the data within the MEs for the purposes of reconciliation of the golden source for the provisioning system to the physical network as well.

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: who is able to alter that view must also be controlled as well, and 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 as well as generalized security logging.

II.2.3 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 OS 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 personnel 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-affecting, 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.

II.2.4 Fault management services

After a service has been turned up and has undergone 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 its origin are 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 managed elements. All of these interfaces must undergo authentication and authorization and be placed in the proper role to ensure the sufficient levels of access to the managed 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 network operations centre (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 as data sharing are authenticated, authorized, confidentially secured (if transmitted outside of local networks), and finally each sub-request is notarized.

II.2.5 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, and 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 as 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.

II.2.6 Engineering

To support any customer service, a number of MEs 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 as the loss of money due to mistracked 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.

II.2.7 Ticketing systems

When a customer calls the TSP to report trouble, a ticket is entered which is then tracked through 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, to the Federal Communications Commission (FCC)/Public Utilities Commissions (PUCs) 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 misplaced workforce. More importantly, the tickets must also be verified to be correct in their data validity. The long term storage as well as 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 non-repudiation.

II.2.8 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 outside plant (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, global positioning system (GPS) tracking systems can 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 as high levels of confidentiality.

II.2.9 EMS security needs

The element management system (EMS) is responsible for the management of MEs in the network. It typically provides for the entire FCAPS umbrella. FCAPS (fault-management, configuration, accounting, performance, and security – see [b-ITU-T M.3400] for details) 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 MEs under its control. At the same time, it must support interfaces to all of the OS systems that make use of these FCAPS features, in addition to presentation level services that make use of the EMS that 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 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 a specific version of the operating system that supports this feature.

The major issue is securing the southbound interfaces of the EMS. There are a myriad of protocols and each has its own issues to solve. Driving security to the ME adds cost to the device as well as complexity. Most MEs provide for a simple central processing unit (CPU) or application-specific integrated circuit (ASIC) that has very little capability and barely provides for the basic ME management. As such, an 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 slowly starting to respond. As such, in the upcoming years, the need to manage security down to the ME itself will then provide for a host of PKI capabilities that will be required. The ME 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 managed elements.

The EMS OS 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 MEs, such as firewalls. It must also support the ability to manage all of the audits and security logging that are generated from this layer of the network, which is a very large volume of information.

II.2.10 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 managed element as an island. Services are looked at from a single managed 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 MEs 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 MEs 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 groups 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 managed elements in each domain. The ability to delegate responsibility based upon workload, "follow the sun" support, and other business drivers is also a requirement.

II.2.11 Key system requirements

With the provided understanding of the OS 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 OS to ensure the proper overall management of these resources.

II.2.12 Key management

Key management is a critical service required for the OS 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 as reduce the duplication of identities, or even worse misidentification within the company. Unfortunately, there is no one single method of centralized key authority today. Therefore, the 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 OS.

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 OS.

II.2.13 Non-repudiation

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

II.2.14 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 OS systems. A common time source should be available to all managed elements to facilitate time-stamp synchronization. Note that this need is broader than just security.

II.2.15 Privilege and policy management

The single greatest need for OS and EMSs today is the need for privilege and policy management. Each system today implements its own identity and authorization services. The ability to standardize on a single method, such as single sign on, a single method to create a corporate identity, the use of standardized roles and responsibilities, and a single point of management for all of this is required for SMS OS 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 reason. With a single

point of control, this task now becomes manageable in the face of the ever-growing number of OS and EMS systems and sub-systems.

II.2.16 Notarization

As specified previously, while all OS and EMS systems support north- and southbound 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 managed 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 OS.

II.2.17 Confidentiality and integrity

For most OS 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 managed 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 OS and data repositories, both online and offline, is required. The centralized management of such systems would fall under the tasking of the SMS OS.

II.2.18 Audit and logging

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

II.2.19 Intrusion detection

Every OS and EMS runs on a piece of hardware, which 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 OS and EMS. As such, the proper management of intrusion detection systems to ensure for a cohesive policy for this feature will be paramount.

II.2.20 Virus detection

The ability to either detect viruses or manage virus systems will be the key. The injection of a virus or worm into the OS and EMS or to the devices it manages is highly important. These viruses and worms can create huge breaches in the security of the network. As such, systems watching the operating systems of the OS and EMS will be required.

II.2.21 Secured software distribution

Most, if not all EMS, NMS, and OSs, provide for a means to automatically distribute software either to the OS itself for self-upgrade or to the ME 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 or digital signature to ensure the validity of the load as provided by the author. The same is true of the OS and EMS where software upgrades are done by 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 OS should manage all of the features listed above.

Appendix III

TSP infrastructure and security service managed elements

(This appendix does not form an integral part of this Recommendation)

III.1 TSP NGN security service managed elements

Service providers are rapidly evolving from the classic TDM based public switched telephone network (PSTN) to packet-based next generation networks (NGNs) that rely on numerous access technologies and provide a wide array of customer/subscriber/user services. The objective of this appendix is to provide a brief overview of the functional requirements and architecture of standards-based NGNs (as described in [ITU-T Y.2012] scope and [b-ITU-T Y.2201] NGN release 1 requirements) and relate the security services that an SMS needs to be able to manage to the NGN framework. The [ITU-T Y.2012] functional architecture Recommendation provides a clear distinction between the definition and specification aspects of services provided by the NGN and the actual specification of the network technologies used to support those services.

III.2 Framework and topology of the NGN

The NGN increases the level of complexity over existing fixed networks as a result of its architecture and services. The addition of support for multiple access technologies and for mobility results in the need to support a wide variety of network configurations. Figure III.1 shows an NGN core network with a set of example access networks.

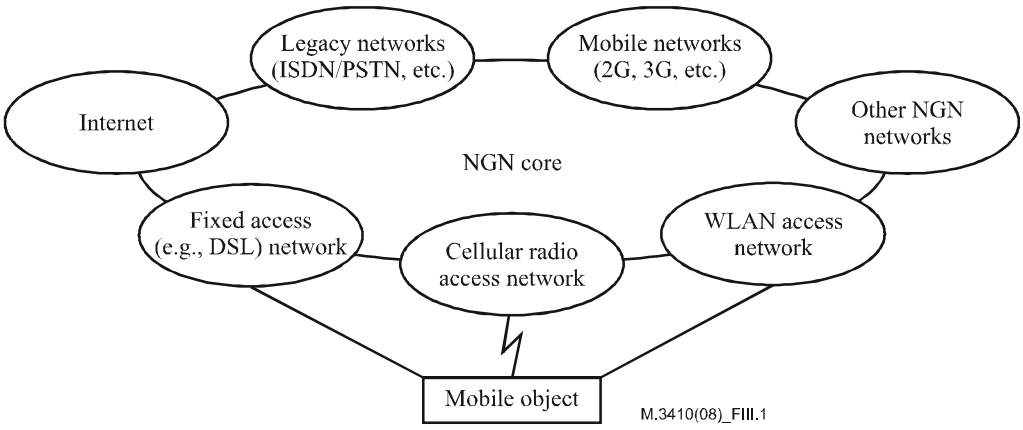

Figure III.1 – NGN core and access networks

In this figure, the core network is that part of the NGN that provides NGN services contracted by the user. It is different from access network(s) in that it provides common functions shared across one or more access networks. Access networks are different from the core in that they do not provide end-user services directly (other than transport). Access and core networks may be distinguished from each other based on aspects such as technology, ownership, or administrative needs.

Figure III.2 depicts the high-level framework or structure that serves as the basis for the NGN functional reference model. As described in [ITU-T Y.2012], this framework is organized into four layers of functionality in the vertical direction plus three domains in the horizontal direction. These are discussed in the subclauses below.

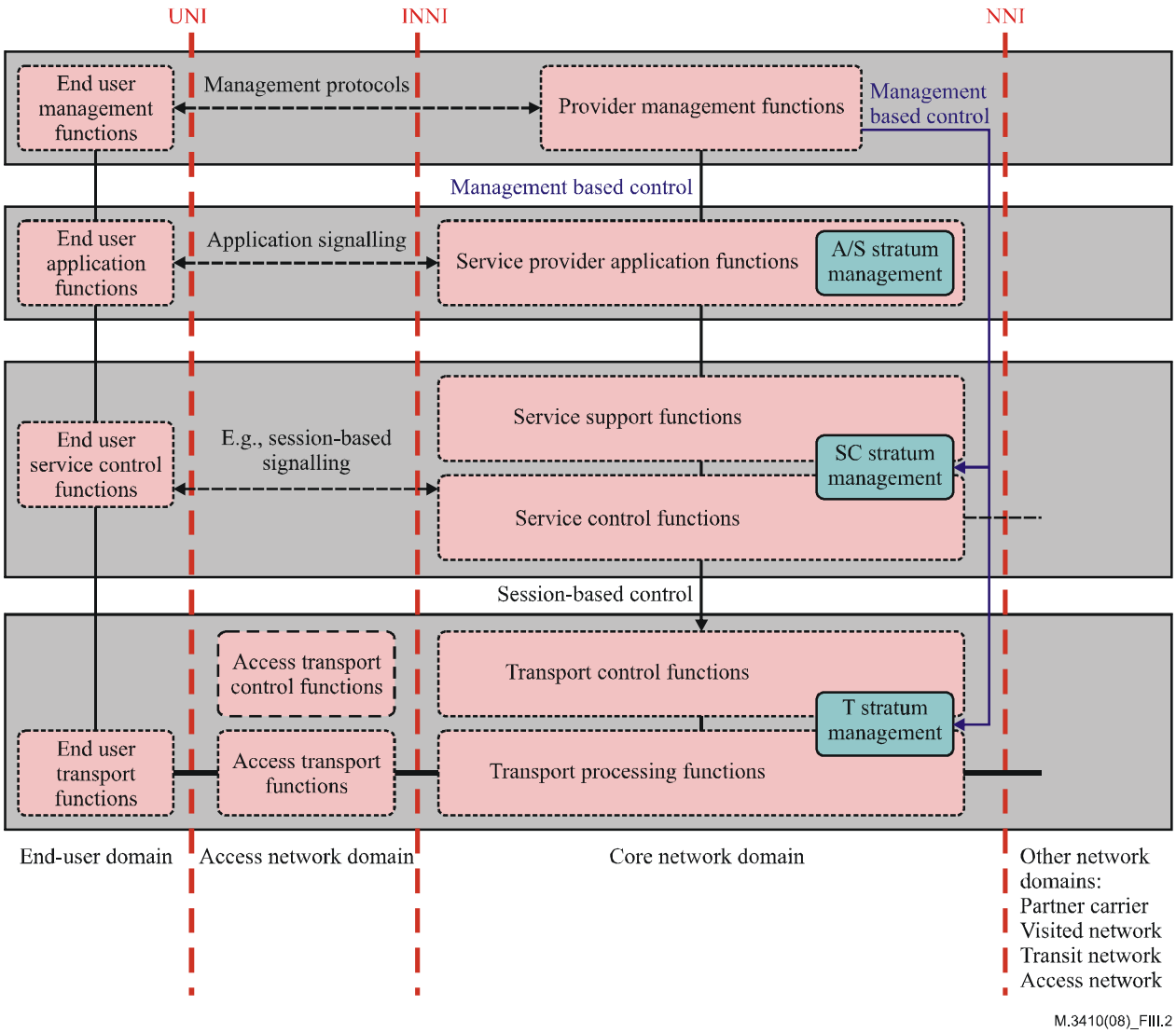

Figure III.2 – Framework of the NGN functional reference model

The NGN architecture is divided into multiple interrelated, logical layers, shown in gray above. These logical layers define logical subsets of the NGN's functions without regard to the technology used to implement those functions. Each functional layer provides capabilities to adjacent layers. This grouping is useful in understanding the functionality involved but does not imply any physical implementation.

III.2.1 Management functions

The management functions contain the management functionality relating to QoS, security, and system and network management. This functionality is responsible for providing the FCAPS (fault, configuration, accounting, performance, and security) management functions to all functional entities within all layers, e.g., operational support functions such as provisioning, configuration management, accounting and performance.

III.2.2 Application functions

The application/services functionality is responsible for:

i) defining and managing subscribers, including their subscriptions, their preferences, and their key data items,

ii) defining and managing services, including the infrastructure to support services and the common data and media functions upon which they are built,

iii) authenticating and authorizing service users,

iv) providing the environment for the distinct service applications (application servers, proxies, etc.).

III.2.3 Service functions

The service functions are responsible for handling the call processing and real-time routing of application-layer traffic within the network. It manages assignable transport resources.

III.2.4 Transport functions

Transport functions provide:

i) basic cross-connect and flow management functions (including network-layer routing) between logical ports. It manages queuing functions, communicating state and availability information about its resources to the service control stratum,

ii) the physical termination, logical connectivity, adaptation, connection provisioning, and port functions for the management, signalling, and bearer traffic connections.

III.2.5 Functional entities and groups

A key component of the NGN architecture is the concept of functional entities (FEs) and functional groups (FGs). A functional entity (FE) is a cluster of functionality (sub-functions) that is viewed as a single entity from the point of view of the end-to-end functional architecture. An FE may be localized at a single geographical location (e.g., a central office, a data centre) or it may be implemented across several cooperating physical managed elements. An FE is typically a software process, or a portion of a software process, running on some managed element. The correct granularity for an FE is based on the desired or required decomposition. If the functionality can be broken down into two or more processes that could advantageously be located at different geographical or physical locations, then it is better to define two or more separate, cooperating functional entities with a relationship or association between them rather than considering the given functionality as a single functional entity.

It should be noted that it is the possibility (and potential desirability) of functional separation that matters here. Defining a set of sub-functions as a single, distinct FE (i.e., separately from some other set of sub-functions) does not constrain the mappings to a physical implementation. It simply allows for multiple physical scenarios for the same overall set of functionality. Of course, it is always possible to combine two or more distinct FEs in a single physical implementation. This might be dictated by a particular vendor implementation or driven by performance requirements.

- A functional entity reference model is an abstract description of a system architecture that provides a framework or structure for examining significant FEs and their key associations or relationships. The granularity of the reference model will vary with the use objectives for the model.

Each functional layer within the framework contains a functional entity reference model:

- A functional group (FG) is a cluster of FEs grouped (and named) solely for convenience and architectural clarity. This concept is particularly useful in descriptions of functional reference models and functional architectures as it provides a means of organizing or clustering closely-related FEs. FGs are less useful once FEs have been assigned or allocated to physical entities, as often there may not be a one-to-one mapping of FGs to physical entities.

However, FGs are not intended to constrain FE physical groupings.

III.3 NGN decomposition

The NGN network can be logically decomposed into different sub-networks, as shown in Figure III.3. The emphasis on logical decomposition instead of physical decomposition is based on the fact that, in the future, physical equipment may have features of both the access network and the core network. A pure physical decomposition will encounter difficulties when such features are combined into a single managed element.

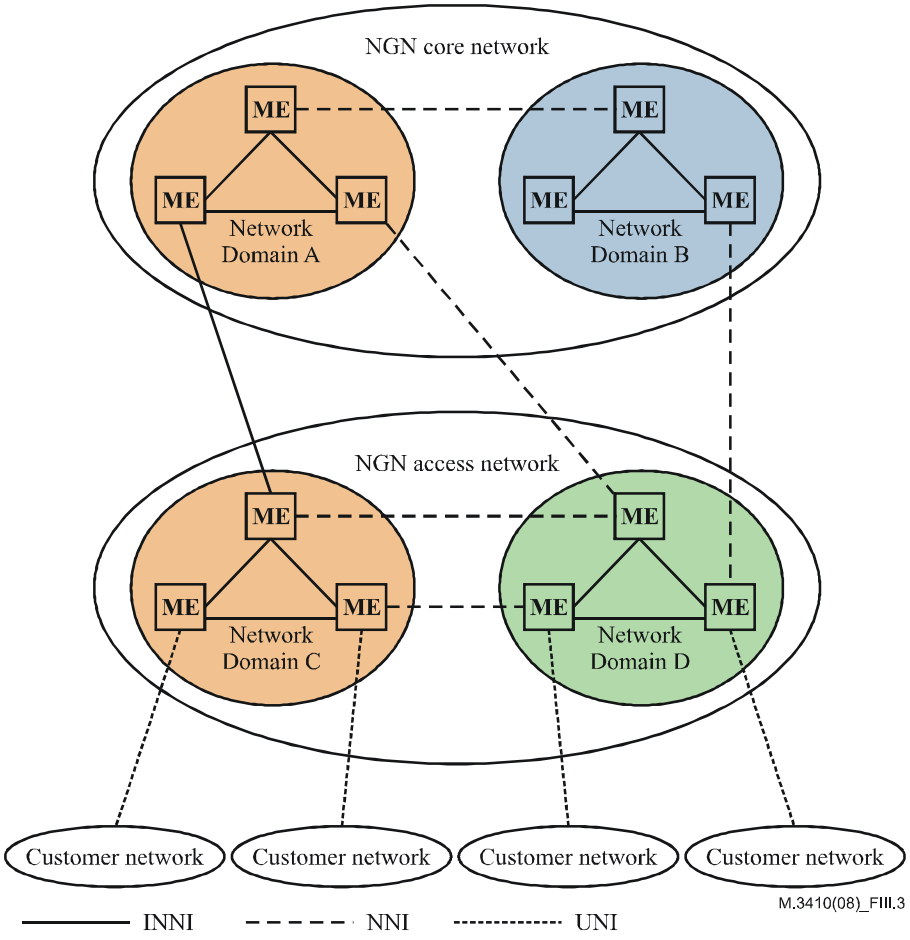

Figure III.3 – Major components of the NGN at the network level

The major components of an NGN network are as follows:

- End-user network: An end-user network can be a network within a home or an enterprise network. It is connected to the service provider's network via a UNI (user-to-network interface). The UNI is also the demarcation point between the service provider and the user. An end-user network may obtain its content service from:
  - the core network;
  - another instance of the end-user network providing public services; or
  - another instance of the end-user network providing private services, possibly with a private addressing scheme.
- Access network: An access network collects end-user traffic from the end-user network to the core network. The access network service provider is responsible for the access network. The access network can be further partitioned into different domains, with the intra-domain interface being termed an INNI (internal network-network interface) and the

inter-domain interface being termed an NNI (network-network interface). The access network belongs to the transport layer of functionality.

- Core network: The core network belongs to both the transport and the service layers of functionality. The core network service provider is responsible for the core network. The interface between the core network and the access network or between core networks can be an INNI (in the case of partitioning as a single domain) or an NNI.

The concept of an NGN domain is introduced to outline the administrative boundaries. Detailed topology information may or may not be shared across the NNI, but may be shared if available for INNI links. As depicted in Figure III.3 above, the access network and the core network may or may not belong to the same NGN domain.

III.3.1 Domains

The domain perspective provides a view of organizational ownership, control and trust. Any, or all, of these domain attributes may be tightly held by the domain owner or shared/entrusted to another party.

III.3.1.1 Basic domains

There are four major domains to be considered:

- End-user domain
- Access domain
- Core domain
- Transit domain

III.3.1.2 End-user domain

This domain aggregates the various access methods for services, ranging from plain old telephones to IP phones and appliances, as well as applications that provide web access, messaging and other non-verbal communication.

III.3.1.3 Access domain

The access domain has a number of technologies that implement layer 1 and layer 2 forwarding plane protocols in the access function. The access domain may also include distributed L3 functions. Typically, the equipment deployed in the access domain has a relatively simple ring-based topology to distribute traffic between the end-user and the edge-aggregation domain. The access domain may also implement a passive optical network (PON) as discussed in [b-ITU-T G.983.1] and [b-ITU-T G.984.1].

III.3.1.4 Core domain

This domain includes functions central to the delivery of suites of services to customers. FEs in this domain interact with FEs in all the other domains.

III.3.1.5 Transit domain

This domain represents peer FEs from various Partner networks with which a network operator FE will interact according to agreed upon and established rules and business relationships.

Relationship between the NGN and service domains

The NGN provides access to a wide variety of services. The specific services offered by any service provider are determined by business needs and customer needs. Figure III.4 shows an example that illustrates multiple domains within which services may be accessed.

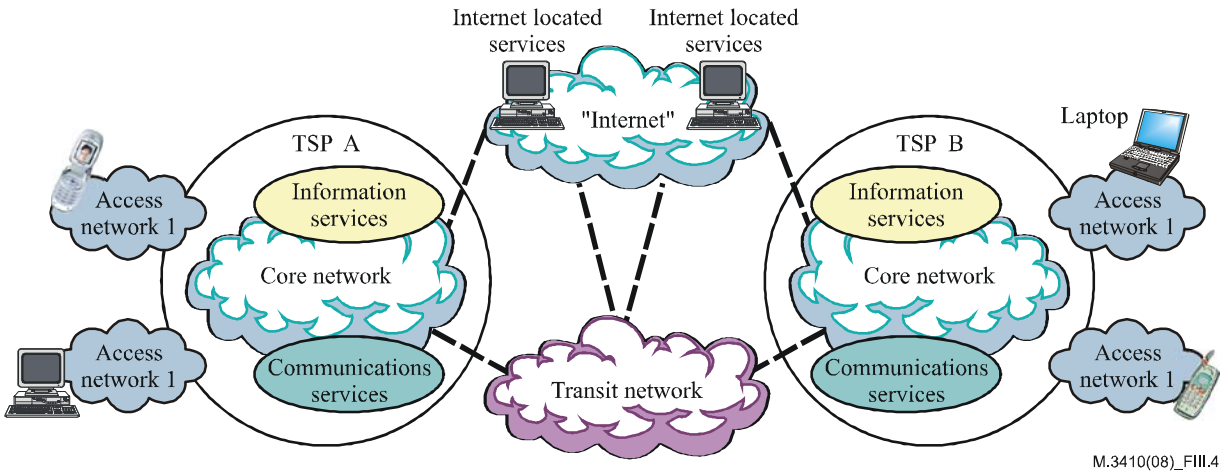

Figure III.4 – NGN example of service domains

In this example, TSP A supports a single access network technology that provides access to three service domains via its core network.

1) One service domain is the Communications services bubble. These services may be completely within TSP A's domain or may support end-to-end services to other TSPs. In this example, TSP A supports end-to-end communication services inter-operating with TSP B's communications services. They are interconnected through a transit network. Other transit network configurations are of course allowed, and the transit network may be null in the case where TSP A is directly connected to the other endpoint network. Network access control FEs are used to protect service domain FEs within a domain from FEs in other domains and the transit network. It should also be noted that the network on the other side of the transit network might be another type of external network, such as the PSTN.

2) A second service domain in this example is the Information services bubble of TSP A. This could provide services such as web hosting. These service FEs may be attached directly to TSP A's core network or may be provided by third parties through agreed upon security arrangements.

3) A third service domain shown here is access to Internet-based services. These services are not part of TSP A's domain, nor are they provided by business arrangements with TSP A. These services are accessed via TSP A transport connections to the Internet.

As mentioned earlier, this example shows only a small set of the possible configurations that might be supported by TSP NGNs.

III.3.2 Interfaces

The interfaces between the various FEs, as well as the boundary points between the domains, provide meeting points for integration and interoperability. Figure III.5 depicts the notion that multiple NGN core networks may interoperate to provide an end-to-end service to the user. Although not depicted, a single TSP may deploy multiple core networks within and between metropolitan regions. In a simple case, an end-to-end session will have originating and terminating core networks. Depending on the TSP's particular configuration, one or more separate access networks might be involved.

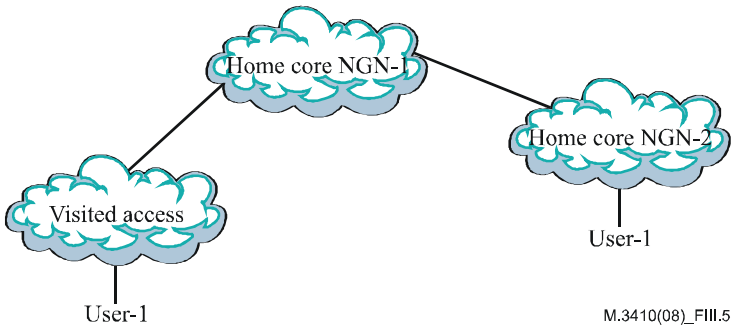

Figure III.5 – NGN example of home and visited networks

Since, in many cases, the specific division of functionality between core and access networks, and between the originating and terminating networks is based on the, or multiple, TSP's business decisions, it is difficult to precisely define the attributes that make up each of these configuration managed elements. Rather than hard points of separation in the architecture, these aspects should be thought of as configurable topology managed elements that may be mixed and matched in many different ways.

III.3.3 Enterprise role model

The primary purpose of an enterprise model is to identify interfaces that are likely to be of general commercial importance. To do this, a number of roles are identified:

- which describe reasonably well-defined business activities that are unlikely to be subdivided between a number of players
- players may aggregate roles as they see fit
- thereby not limit players in anyway
- does identify the roles that the architecture should enable.

A basic role model for NGN is shown in Figure III.6. It identifies the following roles:

- Customer: The role denoting a person or other entity that has a contractual relationship with a service provider on behalf of one or more users.
- User: The role in which a person or other entity authorized by a customer uses services subscribed to by the customer.
- Retailing service provider: The role that has overall responsibility for the provision of a service or set of services to users associated with a subscription as a result of commercial agreements established with the users (i.e., subscription relationships). The user profile is maintained by the retailing service provider. Service provision is the result of combining wholesale network services and service provider service capabilities.
- Wholesale service provider: The role that combines a retailing service provider's service capabilities with its own network service capabilities to enable users to obtain services.
- Value-added service provider: The role that provides services other than basic telecommunications service (e.g., content provision or information services) for which additional charges may be incurred. These may be billed via the customer's service provider or directly to the customer.

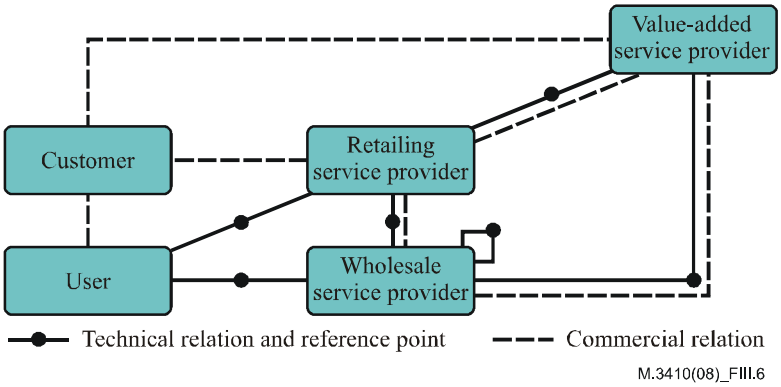

Figure III.6 – Basic NGN roles

This basic model provides a kind of super-class for roles and their relations. Wholesale service provider players may need to combine their services to provision an end-to-end service. This is illustrated by the looped line and reference point in Figure III.6 above. The first step in wholesale provider role specialization is shown is Figure III.7.

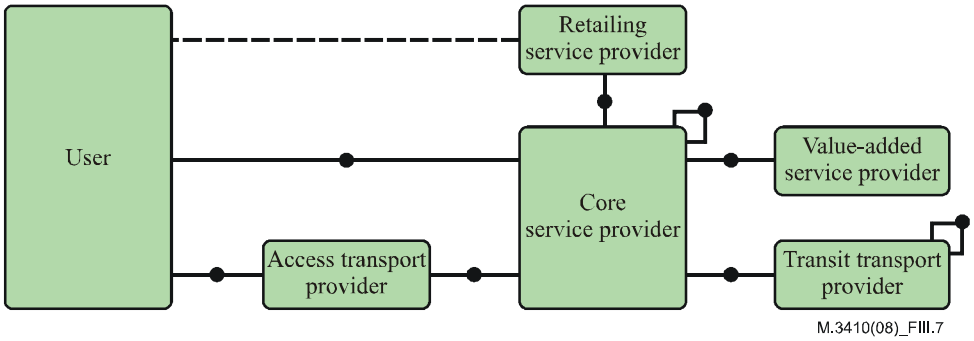

Figure III.7 – NGN roles: First level of specialization

A basic tenet of the NGN architecture is the separation of transport and service layer functions so that the transport functions will support different types of service control systems. This can be taken further by specializing the core service provider into a "core transport" and a "service control and integration" provider role. The implication is that the reference points between functions in the transport and the service functional layers become security-trust domain boundaries and will have to support inter-TSP security requirements.

The service control and integration provider role can be split into separate service control provider and integration service provider roles. Virtual network TSPs are players who perform this role, and these are so well established that it is deemed appropriate to reflect this in the second level of specialization. The resulting role model is depicted in Figure III.8.

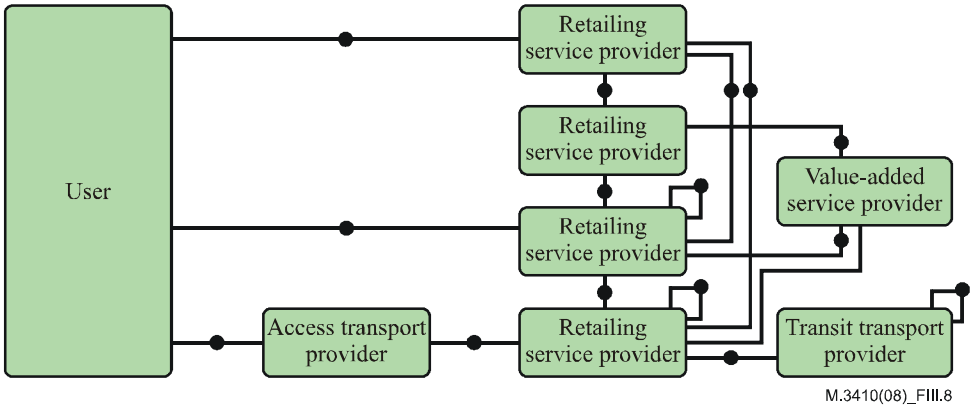

Figure III.8 – NGN roles: Second level of specialization

Each of the new roles has a relationship with the retailing service provider role that holds the user profile database. A retailing role player may hold the user information for all three roles, or a user may have a relationship with multiple retailing role players. In summary, the second level of specialization of the NGN enterprise model defines the following roles:

- User: The role in which a person or other entity authorized by a customer uses services subscribed to by the customer.
- Retailing service provider: The role that has overall responsibility for the provision of a service or set of services to users. The user profile is maintained by the retailing service provider. Service provision is the result of combining retailing service provider services with wholesale services from at least the access and core transport provider roles and at most from all other provider roles.
- Integrating service provider: The role that creates unique new service offerings from the wholesale services provided by other roles.
- Service control provider: The role that provides session and call control and related services, such as registration, presence, and location, wholesale to retailing and integrating service providers.
- Value-added service provider: The role that provides value-added services (e.g., content provision or information services) on top of the basic telecommunications service provided by the service control provider role. It does not provide a complete service on its own.
- Core transport provider: The role that provides connectivity either end-to-end or in part, and related services such as registration for connectivity service, by combining its own services with those of the access transport provider and transit provider roles as necessary.
- Access transport provider: The role that provides a wholesale connectivity service between the user and a core transport provider.
- Transit transport provider: The role that provides a wholesale connectivity service between core transport providers, in conjunction with other transit transport providers as necessary. It also provides related DNS services.

A fundamental point is that many of the aforementioned roles align with individual, and independent domains, both from an ownership perspective and an administrative and security perspective.

III.4 Security mechanisms within an NGN

Identification of security FEs and allocation of these FEs to security mechanisms proceeds from an initial allocation of security services and functions and then defines the types of components and security mechanisms that are available to implement the security services with particular strengths.

III.4.1 Security services

The security services described below are the basic security services within the NGN. In practice, they will be invoked at appropriate protocol layers and within computing elements, in appropriate combinations, to satisfy TSP security policy. Particular security mechanisms can be used to implement combinations of the basic security services. Practical realizations of systems may implement particular combinations of the basic security services for direct invocation.

Table III.1 – Necessary NGN security services

Security service functional groupings		Applies to communications assets	Applies to computing assets
1	Authentication		
1.1	Peer entity authentication	Yes	
1.2	Data origin authentication	Yes	
1.3	User authentication		Yes
2	Authorization		
2.1	Communications access controls	Yes	
2.1	Computing system access controls		Yes
3	Confidentiality		
3.1	Connection confidentiality	Yes	
3.2	Connectionless confidentiality	Yes	
3.3	Selective field confidentiality	Yes	Yes
3.4	Traffic flow confidentiality	Yes	
4	Integrity		
4.1	Information integrity		
4.1.1	Separation of duties		Yes
4.1.2	Well-formed transactions		Yes
4.1.3	Logging & auditing	Yes	Yes
4.2	Data integrity		
4.2.1	Connection integrity with recovery	Yes	
4.2.2	Connection integrity without recovery	Yes	
4.2.3	Selective field connection integrity	Yes	
4.2.4	Connectionless integrity	Yes	
4.2.5	Selective field connectionless integrity	Yes	

Table III.1 – Necessary NGN security services

Security service functional groupings		Applies to communications assets	Applies to computing assets
5	Non-repudiation		
5.1	Non-repudiation with proof of origin	Yes	Yes
5.2	Non-repudiation with proof of delivery	Yes	Yes
5.3	Non-repudiation of actions	Yes	Yes

III.4.2 Authentication

These services provide for the authentication of identities presented/asserted by entities (a.k.a. subjects) and the identity of sources of data as described below.

III.4.2.1 Peer entity authentication

This service is provided for use at the establishment of, or at times during, the data transfer phase of a connection to confirm the identities of one or more of the entities connected to one or more of the other entities. This service provides confidence, at the time of usage only, that an entity is not attempting a masquerade or an unauthorized replay of a previous connection. One-way and mutual peer entity authentication schemes, with or without a liveliness check, are possible and can provide varying degrees of protection as discussed in [ITU-T X.800].

III.4.2.2 Data origin authentication

The data origin authentication service provides the corroboration of the source of a data unit. The service does not provide protection against duplication or modification of data units as discussed in [ITU-T X.800].

III.4.2.3 User authentication

This service is provided for confirming the identity of a human subject when logging into a computer system (managed element). This service provides confidence, at the time of log-in, that a human entity is not attempting a masquerade of a different human subject.

III.4.3 Authorization

This service provides protection against unauthorized use of resources. These may be communications or computing resources. This protection service may be applied to various types of access to a resource (e.g., the use of a communications resource; the reading, the writing, or the deletion of an information resource; the execution of a processing resource) or to all accesses to a resource. The control of access will be in accordance with various security policies.

III.4.3.1 Communications access controls

This service provides protection against unauthorized use of communications resources. The control of access will be in accordance with various security policies as discussed in [ITU-T X.800].

III.4.3.2 Computing system access controls

This service provides protection against unauthorized use of computing resources. The control of access will be in accordance with various security policies.

III.4.4 Confidentiality

These services provide for the protection of data from unauthorized disclosure as described below.

III.4.4.1 Connection confidentiality

This service provides for the confidentiality of all (N)-user-data on an (N)-connection as discussed in [ITU-T X.800].

III.4.4.2 Connectionless confidentiality

This service provides for the confidentiality of all (N)-user-data in a single connectionless (N)-SDU (service data unit) as discussed in [ITU-T X.800].

III.4.4.3 Selective field confidentiality

This service provides for the confidentiality of selected fields within the (N)-user-data on an (N)-connection or in a single connectionless (N)-SDU as discussed in [ITU-T X.800].

Beyond what is in [ITU-T X.800], this service can also provide confidentiality of information within computing system storage devices (i.e., file systems) and dynamic memory.

III.4.4.4 Traffic flow confidentiality

This service provides for the protection of the information which might be derived from observation of traffic flows as discussed in [ITU-T X.800].

III.4.5 Integrity

There are actually two parts to the concept of integrity:

1) information integrity; and

2) data integrity.

III.4.5.1 Information integrity

Information integrity is not really a service but rather a way to implement services. Information integrity focuses on the correctness of information, namely, is a piece of information valid. The simplest way to express this is by example:

> An Accounts Payable clerk will not issue a payment on an invoice from a supplier unless the clerk can match the invoice against a purchase order and a set of shipping documents from the receiving department.

The above example highlights that the legitimacy of the invoice is established from documentary evidence that the product was ordered and received.

Separation of duty

The concept of separation of duties, as part of information integrity, can also be seen in the above example. If:

- employee A is only authorized to issue purchase orders,
- employee B is only authorized to receive shipments and shipping papers/receipts, and
- employee C is only authorized to issue checks to suppliers

then any attempt by the supplier to get paid for an invalid invoice (products/services not ordered) would require the supplier to conspire with at least employees A and B.

A successful conspiracy amongst suppliers and employees, or only amongst employees, becomes more difficult as the number of conspiracy members increases. By separating duties amongst multiple employees, a network operator reduces the probability that information is forged (not valid).

Well-formed transactions

The concept of well-formed transaction, as part of information integrity, can also be seen in the above example. If:

- employee A is required to process purchase orders using a specific process,
- employee B is required to process shipping papers/receipts using a different specific process, and
- employee C is only authorized to issue checks using a third specific process

then control over which employee is authorized to perform which operation may be controlled by which employee is allowed to invoke which of the three specific processes. Another aspect of well-formed transactions is that only production processes are allowed to be used for the aforementioned activities and that these production processes cannot be modified, circumvented, or replaced without authorization and detection.

Logging

The concept of logging, as part of information integrity, directly speaks to the last point made above regarding well-formed transactions. Specifically, all activities that alter information, or the processes that process information, need to generate log entries that allow for the auditing of the production processes. This auditing is critical, in conjunction with separation of duties and well-formed transaction, in providing a high level of assurance that information is correct and valid. This capability relies on the presence of non-circumvent able logging mechanisms.

III.4.5.2 Data integrity

These services counter active threats and may take one of the forms described below.

Connection integrity with recovery

This service provides for the integrity of all (N)-user-data on an (N)-connection and detects any modification, insertion, deletion or replay of any data within an entire SDU sequence (with recovery attempted) as discussed in [ITU-T X.800].

Connection integrity without recovery

Same as for connection integrity with recovery but with no recovery attempted as discussed in [ITU-T X.800].

Selective field connection integrity

This service provides for the integrity of selected fields within the (N)-user data of an (N)-SDU as discussed in [ITU-T X.800].

Connectionless integrity

This service, when provided by the (N)-layer, provides integrity assurance to the requesting (N+1)-entity as discussed in [ITU-T X.800].

Selective field connectionless integrity

This service provides for the integrity of selected fields within a single connectionless SDU and takes the form of determination of whether the selected fields have been modified, as discussed in [ITU-T X.800].

III.4.6 Non-repudiation

Non-repudiation is the ability to prevent an entity (a.k.a. subject, actor) from being able to deny that the entity performed some action as elaborated below.

III.4.6.1 Non-repudiation with proof of origin

The recipient of data is provided with proof of the origin of data. This will protect against any attempt by the sender to falsely deny sending the data or its contents, as discussed in [ITU-T X.800].

III.4.6.2 Non-repudiation with proof of delivery

The sender of data is provided with proof of delivery of data. This will protect against any subsequent attempt by the recipient to falsely deny receiving the data or its contents, as discussed in [ITU-T X.800].

III.4.6.3 Non-repudiation of actions

Non-repudiation of actions is provided by enforcing the sole use of well-formed transactions and logging to provide an accurate record of what occurred, when it occurred and by whom. This capability may be augmented by the use of authentication mechanisms such as digital signatures.

III.5 NGN computing platform security mechanisms

All NGN managed elements contain FEs typically implemented as software, sometime as firmware. The primary managed element software components is its operating system. The operating system controls the execution of other software (applications) within which are implemented FEs.

III.5.1 NGN operating system security

All NGN deployed managed elements contain some form of operating software. This software can take the form of:

Type 1 A general purpose operating system, typically some form of UNIX/Linux like multi-tasking operating system, along with a full complement of file-system, graphical interface, command interpreters, network protocol stack and application server capabilities (as in DNS, HTTP, FTP, VoIP, packet/message filtering, etc.),

Type 2 A general purpose operating system, typically some form of UNIX/Linux like multi-tasking operating system with real-time scheduling capabilities, with a minimized set of file-system, graphical interface, command interpreters, network protocol stack and application service capabilities configured to perform a limited set of functions,

Type 3 A real-time operating system, typically some form of embedded operating system, along with file-system, graphical interface, command interpreters, network protocol stack and application server capabilities (as in DNS, HTTP, FTP, VoIP, packet/message filtering, etc.), or

Type 4 A basic input-output set of functions for storage, memory, clock and interrupt management tightly bound with a single application service capability (as in DNS, HTTP, FTP, VoIP, packet/message filtering, etc.)

The mapping of NGN security to computing security focuses primarily on conventional computer systems (Types 1 and 2 above), which represent a large portion of all managed elements. Other managed element types may need to implement only portions of the computing security architecture (Type 3 above). In other cases, such as simple sensor or probe devices, the managed element functions may be so limited that only specialized implementations of a small portion of the computing security architecture are appropriate (Type 4 above).

Fundamental allocations of security services are made to managed elements (computing systems) within security domains. Managed element security makes additional security service allocations to managed element hardware and software. Not every security service allocation needs to be made identically in every managed element.

Some security service allocations are implemented as physical and administrative security mechanisms within the security domain, such as access control to facilities and some aspects of authentication of personnel.

III.5.1.1 Hardware protects software

There are a variety of security mechanism choices available between the hardware and software portions of each managed element, but certain general allocations and properties can be stated for the hardware. The hardware is relied upon to function correctly, to enforce isolation of software functions, and to contribute to the protection of the integrity of the system applications and the operating system. It provides protected paths between users and trusted parts of the software. The hardware indirectly supports the isolation of information processed and stored in the managed element by protecting the integrity of the software. In some environments, specific hardware technologies (e.g., hardened or alarmed chassis) may be necessary to protect against tampering with managed element components. Availability of a managed element may be enhanced through technologies such as fault-tolerant and fault-detecting hardware features. Hardware cryptographic mechanisms are employed as needed to support various security services. Other hardware mechanisms (e.g., memory management/mapping) support specific aspects of the software architecture.

III.5.1.2 Software protects information

The security service allocations made to software are wide ranging. The networking subsystem supported by the managed element software is responsible for the confidentiality and integrity of information transferred amongst managed elements, for the authentication of managed elements to one another, and for user authentication and access control in distributed systems. Security services and the mechanisms that implement them must be managed.

The managed element software is responsible for user authentication and access control, and for the integrity of information being processed and in storage. Correct operation of certain software is required to ensure managed element availability. Additionally, the software is expected to provide functions that support the security policies and requirements that are not directly expressed as security services, such as support for multiple security policies. The remainder of this clause refines the computing security architecture, which primarily is concerned with software structure.

III.5.1.3 Managed element security contexts

A computing security architecture must respond to the security allocations discussed earlier, and a security context is a combination of all the security domain, hardware, system software, user application software, and information supporting the activities of a user (or system function) operating in a security (sub-) domain. A security context builds on the common operating system notion of a user process space (sometimes called a context) as supported by hardware features and OS functions. The primary distinctions between an ordinary user process space and a security context are aspects of protection provided by the security domain are explicitly included, and that user applications operate in a controlled process space subject to a security domain security policy.

A kernel manipulates the protection features of the managed element hardware (e.g., processor state registers, memory mapping registers) to maintain strict separation among security contexts by creating separate address spaces for each of them. A kernel also controls communications among security contexts to allow sharing or transfer of information and to allow services to be performed by one security context for another. All user security contexts and many system function security contexts are constrained to make requests for basic managed element services on the kernel through a standard kernel interface. The functions that make and enforce security policy decisions are intimately related to the kernel.

The hardware (including any microcode or firmware) is considered very highly trusted in the sense that its operation is assumed to be correct. Less than highly trusted software is able to perform

operations on basic system resources only through invocations of security-critical functions that are mediated by the kernel; inter-security context operations (e.g., inter-security domain communications) are performed by security-critical functions within the kernel.

Trusted security-related functions (such as security management applications, portions of networking subsystem components, intrusion detection, configuration monitoring, host packet filtering and anti-virus) are expected to operate correctly to satisfy user operational needs, but need not be subjected to the rigorous scrutiny applied to the security-critical functions. Security-related software is not assumed to be free of security defects, although it is certainly prudent to obtain such software from reliable sources, test it before use, apply integrity safeguards to ensure it remains unchanged, and apply configuration management to it. Service functions (such as:

- CORBA, DCE, Java Virtual Machines and .NET Application Framework software and
- FTP, ntp, DNS, Email, VoIP type application servers)

should be assumed safe and obtained from reliable sources, apply integrity safeguards to ensure they remain unchanged, and apply configuration management to them. Application software (obtained from less than reliable sources) should be considered untrusted and may need to be inspected more carefully, test it before use, apply integrity safeguards to ensure it remains unchanged, and apply configuration management to it. Under these conditions, if faulty application software is introduced into a system it will, at worst, prevent certain operations, but information compromise will not result because of the combination of strict isolation of security domains enforced by the managed element, testing, and configuration management.

The following subclauses provide additional detail on the managed element security software components, primarily for the kernel, security contexts, security-critical functions, and operating system implementations.

III.5.1.4 The kernel

The kernel presents abstractions of the fundamental resource management mechanisms to other, less primitive, service providers (information system functions and applications). In operating system implementations that attempt to provide a basis for secure information processing, the kernel software is carefully constructed and evaluated. To aid the evaluation process, the kernel functions are implemented as relatively small programs that are independent of one another to the maximum extent possible. A kernel is charged with the critical task of providing separation among process spaces by manipulating the protection features of the managed element hardware.

The traditional operating system kernel functions are divided among the kernel, security policy enforcement and decision functions, and the remainder of the trusted operating system functions, called the security-critical functions. The kernel serves as the ultimate security policy enforcement function by mediating all use of the basic information system resources. The kernel notion is the foundation of the computing security architecture.

The computing security architecture generalizes an approach that is becoming widely accepted concerning access control, namely the independence between the decision of whether or not an access to a resource is allowed and the enforcement of that decision. The separation of access control decision-making and access control enforcement functions allows the support of multiple access control policies. [ITU-T X.812] designates these functions the access control decision function (ADF) and the access control enforcement function (AEF), respectively. In fact, most existing secure operating system designs have concerned themselves only with access control policy. This managed element architecture extends the AEF concept to include the enforcement of all aspects of a security domain security policy. The resulting function is called the security policy enforcement function (SPEF). Similarly, the ADF concept is extended to a security policy decision function (SPDF). The kernel is the implementation of the SPEF.

The kernel also is an extension (beyond access control) of the reference validation mechanism (RVM) described in the Trusted Computer System Evaluation Criteria [b-DoD 5200.28]. The basic properties of the RVM must be applied to any kernel implementation: it must be invoked for every security-critical operation, it must be small enough to be verified, and its integrity must be maintained. The kernel is reflected in Table III.2 as residing within ring 0. The concept of rings directly reflects the Biba Integrity model where integrity levels are associated with subjects and objects, such that:

- A subject can have write access to objects on its own level or below but not above,
- A subject can have read access to objects on its own level or above but not below,

and information flows downwards in this model. Integrity levels are not security levels as the issue is trustworthiness, not disclosure (access/confidentiality) so the higher the level, the more confidence that data is accurate/reliable or that a program will execute correctly. From a managed element software perspective, this is depicted in Table III.2:

Table III.2 – Mapping of ring to software objects

Software processing ring	Integrity level	Object
0	Highly trusted	Kernel
1	Trusted	Non-kernel operating system functions
2	Assumed Safe	Service functions
3	Untrusted	Application functions

The standard interface to the kernel is a single strongly controlled mechanism for functions residing within rings 1, 2 and 3 to make requests on kernel functionality.

III.5.1.5 Security contexts

From the perspective of the kernel, a security context is defined by a set of data and programs operating in accordance with a security domain security policy. As noted earlier, a security context also includes the physical and administrative security mechanisms of the security domain, and the hardware-based resources (e.g., registers, memory, disks) that are in use when the managed element is serving a particular user (or system function). That is, a security context encompasses all managed element resources and security mechanisms that support the activity of a user operating in a security domain. The kernel must maintain all the information needed to isolate one security context from another. When the managed element ceases performing operations in one security context and begins performing operations in another security context, no information can be allowed to pass from one security context to the other unless a specific request is made, and it is allowable under the security policies of the security domains involved.

Examples of information that managed element security-critical functions (including the kernel) must maintain to support the operation and isolation of security contexts include:

- A unique identification for each security context
- The identification of the security domain being supported
- Hardware register values related to control of managed element resources, including virtual memory and all devices in or attached to the managed element
- The authenticated identity of the user being served
- The users security attributes (permissions)
- Data structures needed to operate security-related functions and other untrusted system applications.

Each security context supports a user (or a system function) operating in a particular security domain. Over a period of time, a managed element may maintain several security contexts to support one or more users operating in one or more security domains. A particular user might use (simultaneously or serially) security contexts operating in the same or different security domains. Different users may employ security contexts operating in the same or different security domains.

Since security contexts are isolated from one another by the kernel, communications among security contexts (requests for service or information transfer) in a managed element can only take place in accordance with the security policies of the security domains supported by the security contexts. If the security policies of the supported security domains do not explicitly permit inter-security domain transfer, the SPDF will necessarily deny the request and the kernel will enforce that decision. Since a security domain contains the information of a particular user community, it would be unusual for a security domain security policy to prohibit information sharing between two security contexts supporting the same security domain.

III.5.1.6 Security critical functions

The security critical functions described in this clause implement the various security services allocated to the managed element and several additional supporting services.

Security policy decision function (SPDF)

The separation of security mechanisms from security policy enforcement and decisions is crucial to the flexibility of the computing security architecture. The SPDF is responsible for making all security policy decisions. The primary role of the SPDF is to isolate the rest of the managed element software from knowledge of security policies. The importance of this approach is threefold:

1) First, the support of multiple security domains with different policies is accomplished easily because the security policies are represented in only one place and are interpreted by only one function. In many current secure system designs, it is difficult to point to the actual software code that implements the single security policy of those systems because it is embedded and scattered throughout the code that performs multiple functions.

2) Second, by keeping security policy representations in one place, it is relatively easy to install, modify, or even replace the security policy for a security domain. It is not necessary to rewrite trusted software that implements the security policy. Rather, the rules that the SPDF interprets for a security domain are updated or replaced.

3) Third, changing the implementation of the SPDF would be transparent to the operation of the remainder of the managed element software. Any correct implementation of the SPDF is acceptable, but it may be useful to standardize the representation of security attributes and security policy rules.

The SPDF approach allows security critical functions to be implemented independently of particular security policies.

Authentication function

The authentication function invokes one or more mechanisms used by a managed element to identify and authenticate users (and to authenticate a managed element to users), and for managed elements to authenticate one another in a distributed environment. A common interface to the authentication function is used that is independent of any of the security domain security policy or the authentication mechanisms employed. That is, the authentication function is the service interface to the mechanisms used to identify and authenticate users and managed elements. The exact mechanisms selected will depend on the security domain policies in effect. A managed element supporting multiple security domain policies may need to implement more than one authentication mechanism.

Audit function

The audit function accepts audit messages from functions in the managed element in accord with the security domain and management security domain security policies. Audit records may become part of the security management information that is part of an information management domain (for one or more security domains or managed element domains). Audit records may be directed to multiple repositories. In some cases, the audit information may best be used by an individual user (for example, time and method of most recent managed element or security domain use). The audit function guarantees that audit messages cannot be lost and that the ordering of messages is preserved. As part of a distributed audit system, audit functions can forward the audit data they collect to a base-level, regional, or central audit centre to alleviate local audit data storage requirements and to coordinate audit information from different managed elements or security domains. Audit data must be protected from unauthorized access or modification.

Process scheduling function

In operating systems that share the managed element processor among multiple processes, the process scheduling function determines which of the processes next uses the processor (or processors in a multiprocessor managed element) and for how long. The process scheduling function must be included among the security critical functions so that no process can deny the processor to other processes either purposefully or inadvertently.

Device management functions and device controllers

The remainder of the security critical functions are each responsible for a particular class of managed element resources. These resources include memory, storage devices, display systems, inter-process communications, cryptographic services, and any other input/output devices controlled by the managed element.

Security-related functions

Some software functions within the managed element are required to manage information or to provide an interface to the security critical functions, but are not critical to system security. Of particular interest here are residual operating system functions, security management functions, and networking subsystem functions.

Operating system structure

Most of the security critical functions are part of traditional operating system structures. Many other operating system components are not included in the security critical functions, such as the user interface, utility functions, and high-level abstractions of information. These functions are present in varying forms in all traditional operating systems. The user interface, the particular utility functions, and the information abstractions provided characterize a particular operating system. That is, they distinguish one operating system from another even though they provide essentially the same services to a user. Because the security critical functions provide commonly used, low-level services, many different operating systems can be implemented using them.

Security management function

The primary role of the security management function is to control information needed by security-critical and security-related functions within the computing security architecture. Security management is a particular instance of general management functions. Examples of the information manipulated by the security management function include security domain security policy rules used by the SPDF, configuration parameters for security mechanisms (e.g., cryptographic algorithms), configuration parameters for cryptographic mechanisms and managed element devices, and audit information. Some information is managed for specific security domains and some is managed for managed elements or security domains.

Networking subsystem function

The networking subsystem is defined in accordance with [b-ITU-T X.200] and [ITU-T X.800]. Communications applications and communications protocols used to communicate with other managed elements are implemented as trusted operating system functions within the computing security architecture. These applications make requests for security services (which process information and generate protocol information) that provide required protection. For information to be transferred between managed elements and within a security domain, a distributed security context is established through the use of security management and transfer system applications, and security critical functions.

III.5.1.7 Security management within NGN managed elements

Each NGN deployed managed element includes some set of security mechanisms and therefore must also include a local mechanism for managing these local security mechanisms. Local security management functionality is typically embodied within the general management/administrative functions within the managed element, referred to herein as a security management application process (SMAP).

One or more managed elements within the same security domain may 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 managed element. In such cases, the specific security mechanisms to be employed must be negotiated between the SMAPs in the managed elements at the time a security association is established between them.

The invocation of security services and security mechanisms within a managed element involves several functions. Since all security services are security-critical, they should be accessible only within the kernel, and applications should invoke them only through a standard kernel interface. Since most applications will rely upon the operating system for use of this standard kernel interface, the use of the interface should be transparent to those applications. If a request for a security service does not specify a security mechanism, the SMAPs should make a choice among the available security mechanisms based on the security domain policy and invokes it through an appropriate operating system call. Otherwise, the SMAPs invokes the specified security mechanism.

Consistent with [ITU-T X.800], managed element 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 (for use with encryption, digital signature, data integrity, authentication and notarization mechanisms);
- encryption management;
- digital signature management;
- access control management;
- data integrity management;
- authentication management;
- traffic padding management;
- routing control management;
- notarization management;
- availability management.

III.5.1.7.1 Key management

[ITU-T X.800] describes key management as follows:

"Key management may involve:

a) generating suitable keys at intervals commensurate with the level of security required;

b) determining, in accordance with access control requirements, of which entities should receive a copy of each key; and

c) making available or distributing the keys in a secure manner to entity instances in real open systems."

Exchange of session keys will typically be negotiated within the security association establishment and renegotiation mechanisms of security protocols such as within IPSec IKE, TLS, DTLS and SSH. Key management functions for distribution of key distribution keys (master keys) and keys used in peer-entity authentication may be performed as part of a key management service such as a PKI.

NGN managed element key management functionality should include the ability to securely store multiple sets of master keys (especially multiple asymmetric encryption private keys and associated X.509v3 certificate [ITU-T X.509] chains) as well as multiple shared secret keys used with symmetric encryption and 'keyed' hash based data origin authentication mechanisms. Managed element SMIBs are expected to support the ability to store security policy rules governing keys and their usage within the NGN security domain.

III.5.1.7.2 Encipherment (encryption) management

[ITU-T X.800] describes encryption management as follows:

"Encipherment management may involve:

a) interaction with key management;

b) establishment of cryptographic parameters; and

c) cryptographic synchronization."

Selection of cryptographic algorithms, parameters, synchronization and keys will typically be negotiated within the security association establishment and renegotiation mechanisms of security protocols such as within IPSec-ISAKMP, TLS, DTLS and SSH. These security protocols will require interaction with the managed element's key management functionality for access to master keys when a security protocol is performing peer entity authentication. The managed element SMIB will be expected to support the ability to store security policy rules governing encryption usage within the NGN security domain.

III.5.1.7.3 Digital signature management

[ITU-T X.800] describes digital signature management as follows:

"Digital signature management may involve:

a) interaction with key management;

b) establishment of cryptographic parameters and algorithms; and

c) use of protocol between communicating entities and possibly a third party."

NOTE – Generally, there exist strong similarities between digital signature management and encryption management.

When digital signatures support a non-repudiation service that relies upon a trusted third party (public key infrastructure), additional security management responsibilities may be required within the managed element with respect to long-term archiving of keys and algorithm identifiers so that transactions can be verified well after they occur. This additional capability will typically reside

within the application functionality of a managed element. The managed element SMIB will be expected to support the ability to store security policy rules governing long-term archiving of keys and algorithm identifiers within the NGN security domain along with the actual storage of keys and algorithm identifiers used in transactions.

III.5.1.7.4 Access control management

[ITU-T X.800] describes access control management as follows:

> "Access control management may involve distribution of security attributes (including passwords) 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 the NGN security domain SMIB is necessarily locally present in every managed element that is part of the security domain, it may be necessary to distribute access control attributes between managed elements. Given the complex nature of the application functionality now residing on a network operator's managed elements, it is recommended that the managed element implement role-based access control mechanisms (RBAC) for both general managed element and application specific access control. These managed elements should support secure reliable interaction with an SMS within the security domain. The managed element SMIB will be expected to support the ability to store security policy rules governing access controls within the security domain.

III.5.1.7.5 Data integrity management

[ITU-T X.800] describes data integrity management as follows:

> "Data integrity management may involve:
>
> a) interaction with key management;
>
> b) establishment of cryptographic parameters and algorithms; and
>
> c) 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. For information residing within a managed element, data integrity can be attained by use of strong access control mechanisms on memory and storage subsystems. When a strong communications data integrity service is required, reversible (symmetric) or non-reversible (hashing) cryptographic mechanisms are necessary. Selection of cryptographic data integrity mechanisms, parameters, and keys will typically be negotiated within the security association establishment and renegotiation mechanisms of security protocols such as within IPSec-ISAKMP, TLS, DTLS and SSH. The managed element SMIB will be expected to support the ability to store security policy rules governing both managed element internal and communications data integrity within the security domain.

III.5.1.7.6 Authentication management

[ITU-T X.800] 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 (credentials) to validate a given identity. The authentication information against which user-supplied authentication information is verified is stored in the SMIB (where managed element data structures such as password files and registry heaps constitute part of the SMIB) and is subject to similar considerations as access control attributes. The managed element should provide support for

peer-entity, data-origin and user login authentication. Selection of authentication mechanisms will typically be negotiated within the security association establishment and renegotiation mechanisms of security protocols such as within IPSec-IKE, TLS, DTLS and SSH. Managed element support for some form of security domain "single-sign on" is highly desirable to reduce managed element user login account authentication workload. These managed elements should support secure reliable interaction with an SMS within the security domain. The managed element SMIB will be expected to support the ability to store security policy rules and information governing both local and remote authentication to managed elements within the security domain.

III.5.1.7.7 Traffic padding management

Traffic padding in physical layer communications devices is often managed as a configuration parameter. In the NGN context, 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 security 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.

III.5.1.7.8 Routing control management

[ITU-T X.800] 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."

In an NGN, routing control should be effected through the use of strong peer-entity and data-origin authentication of data link and internetworking signalling and control protocols used to disseminate switching and routing information. This capability will require interaction between routing control, encryption and authentication management functions within the managed element.

III.5.1.7.9 Notarization management

In an NGN, notarization management is highly unlikely to be provided.

III.5.1.7.10 Availability management

Availability management is not described in [ITU-T X.800]. Availability management applies to:

- interactions within an NGN for notifications of outages and, if applicable, alternate service information, and
- for those NGN managed elements that interconnect with other security domains, the ability to contend with likely denial-of-service (DoS and distributed DoS) attack events.

The managed element SMIB will be expected to support the ability to store security policy rules and information governing the recognition of, logging information about, generation and distribution of alarms relative DoS/DDoS attacks targeting managed elements within the security domain.

III.5.1.8 Managed element security information storage management

Each NGN deployed managed element must contain the necessary local information to enable it to enforce an appropriate security policy. A managed element local security management information base (SMIB) is a necessary capability for the storage of security relevant configuration parameters, policy rules, cryptographic keys and other security associated information. The SMIB may be implemented using any number of approaches and not limited to concepts such as SNMP MIBs, nor be implemented as a monolithic or homogeneous structures within the managed element. Managed element SMIBs contain information for management and use of security functions and resources within the managed element the use of which is required by the security domain security policy, including hardware resources, security critical functions (particularly security services and

mechanisms), and supporting applications (e.g., key management). The following example classes of objects should be included in the managed element SMIB:

- End system security policy rules
- Security services management information
- Security mechanisms management information
- Supporting services and mechanisms management information (e.g., alarm reporting, information system auditing, cryptographic key distribution, security contexts, security critical functions, security related applications operating for the managed element).

III.5.2 NGN communications security mechanisms

[ITU-T X.800] defines the general security-related architectural elements that can be applied to communications systems. [ITU-T X.800] provides a general description of security services and the related mechanisms that may be used to provide the services based on the networking architecture concepts of [b-ITU-T X.200]. However, [ITU-T X.800] is concerned only with those visible aspects of a communications path that permit networked managed elements to achieve secure transfer of information between them. It does not attempt to provide any kind of implementation specification, and it does not provide the means to assess conformance of any implementation to this or any other security standard. Nor does it indicate, in any detail, the additional security mechanisms needed within the networked managed elements to ensure reliable secure computer operation.

III.5.2.1 Protocol layers and functional planes

[b-ITU-T X.200] states that there is a functional layering of protocols into what is commonly referred to as the ISO/OSI seven-layer protocol model comprising:

1 Physical layer,

2 Data link layer,

3 Internetworking layer,

4 Transport layer,

5 Session layer,

6 Presentation layer; and

7 Application layer.

It has been frequently argued that, for the most part, the Internet protocol model has displaced the ISO/OSI protocol model in virtually all modern networking infrastructures. This Internet model is essentially a five-layer protocol model comprising:

1 Physical layer,

2 Data link layer,

3 Internetworking layer,

4 Transport layer,

5 Application layer,

and for the purpose of a network operator security architecture, the 5-layer model is used. Since the publication of [b-ITU-T X.200], the concept that each protocol layer actually provides communications functionality to three forms of activities, namely:

- User plane (a.k.a. Media),
- Signalling and control plane, and
- Management plane

has become commonly accepted.

III.5.2.2 Management communications

Management activities certainly pertain to controlling the capabilities and behaviour of functions within each protocol layer. However, from a communications perspective, there is no management plane in protocol layers 1 through 4 as management activities are, in fact, simply a form of application activities where the application activity focuses specifically on (as defined in [ITU-T X.700]):

- **F**ault management,
- **C**onfiguration management,
- **A**ccounting management,
- **P**erformance management,
- **S**ecurity management,

also referred to as FCAPS. Consequently, it is only appropriate to refer to a management plane within the application protocol layer.

III.5.2.3 Physical layer

Clause 7.7 of [b-ITU-T X.200] states the physical layer:

> "provides the mechanical, electrical, functional and procedural means to activate, maintain, and de-activate physical-connections for bit transmission between data-link-entities. A physical-connection may involve intermediate open systems, each relaying bit transmission within the Physical Layer. Physical Layer entities are interconnected by means of a physical medium."

and, as such, does not meaningfully decompose into the aforementioned planes of functionality, thus it is reasonable to reference physical layer technologies relative to specific data link layer technologies, where relevant.

Another complication is the concept of user-network interfaces (UNIs), internal network-network interfaces (INNIs) and network-network interfaces (NNIs) sometimes referred to as external network-network interfaces (ENNIs). This Recommendation will use the more common ITU-T terminology of NNI rather than ENNI.

III.5.2.4 Mapping security services to the communications protocol layers

Tables III.4 to III.11 depict which security services apply within the hierarchy of network interfaces, protocol layers and protocol functional planes.

In the following tables:

- Data link layer is abbreviated as DLL
- Signalling and control is abbreviated as S&C
- Internetworking protocol layer (IP versions 4 & 6) are simply referred to as IP
- "Apply" represents that a service is expected to be present
- "Should" represents that a service should be present
- "May" represents that a service may be present

Table III.3 – DLL user plane

I/F	Security service	Provided
UNI	Peer-Entity Authentication	MAY
	Data-Origin Authentication	SHOULD
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	MAY
	Connectionless Confidentiality	MAY
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	MAY
INNI	Peer-Entity Authentication	MAY
	Data-Origin Authentication	MAY
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	MAY
	Connectionless Confidentiality	MAY
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	MAY
NNI	Peer-Entity Authentication	MAY
	Data-Origin Authentication	MAY
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	MAY
	Connectionless Confidentiality	MAY
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	MAY

Table III.4 – DLL S&C plane

I/F	Security service	Provided
UNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	MAY
	Connectionless Confidentiality	MAY
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	MAY
INNI	Peer-Entity Authentication	APPLY
	Data-Origin Authentication	APPLY
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	MAY
	Connectionless Confidentiality	MAY
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	MAY
NNI	Peer-Entity Authentication	APPLY
	Data-Origin Authentication	APPLY
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	MAY
	Connectionless Confidentiality	MAY
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	MAY

Table III.5 – IP user plane

I/F	Security service	Provided
UNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD
INNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD
NNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD

Table III.6 – IP S&C plane

I/F	Security service	Provided
UNI	Peer-Entity Authentication	APPLY
	Data-Origin Authentication	APPLY
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD
INNI	Peer-Entity Authentication	APPLY
	Data-Origin Authentication	APPLY
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD
NNI	Peer-Entity Authentication	APPLY
	Data-Origin Authentication	APPLY
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD

Table III.7 – Transport layer user plane

I/F	Security service	Provided
UNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	SHOULD
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD
INNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD
NNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD

Table III.8 – Transport layer S&C plane

I/F	Security service	Provided
UNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	SHOULD
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD
INNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD
NNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	MAY
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	MAY
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	MAY
	Connection Integrity without Recovery	MAY
	Selective Field Connection Integrity	MAY
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	MAY
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD

Table III.9 – Application layer user plane

I/F	Security service	Provided
UNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	SHOULD
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	SHOULD
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	SHOULD
	Connection Integrity without Recovery	SHOULD
	Selective Field Connection Integrity	SHOULD
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	SHOULD
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD
INNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	SHOULD
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	SHOULD
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	SHOULD
	Connection Integrity without Recovery	SHOULD
	Selective Field Connection Integrity	SHOULD
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	SHOULD
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD
NNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	SHOULD
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	SHOULD
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	SHOULD
	Connection Integrity without Recovery	SHOULD
	Selective Field Connection Integrity	SHOULD
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	SHOULD
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD

Table III.10 – Application layer S&C plane

I/F	Security service	Provided
UNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	SHOULD
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	SHOULD
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	SHOULD
	Connection Integrity without Recovery	SHOULD
	Selective Field Connection Integrity	SHOULD
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	SHOULD
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD
INNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	SHOULD
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	SHOULD
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	SHOULD
	Connection Integrity without Recovery	SHOULD
	Selective Field Connection Integrity	SHOULD
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	SHOULD
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD
NNI	Peer-Entity Authentication	SHOULD
	Data-Origin Authentication	SHOULD
	User Authentication	SHOULD
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	SHOULD
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	SHOULD
	Connection Integrity without Recovery	SHOULD
	Selective Field Connection Integrity	SHOULD
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	SHOULD
	Non-repudiation with Proof of Origin	SHOULD
	Non-repudiation with Proof of Delivery	SHOULD

Table III.11 – Application layer management plane

I/F	Security service	Provided
UNI	Peer-Entity Authentication	APPLY
	Data-Origin Authentication	APPLY
	User Authentication	APPLY
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	SHOULD
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	SHOULD
	Connection Integrity without Recovery	APPLY
	Selective Field Connection Integrity	SHOULD
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	SHOULD
	Non-repudiation with Proof of Origin	APPLY
	Non-repudiation with Proof of Delivery	APPLY
INNI	Peer-Entity Authentication	APPLY
	Data-Origin Authentication	APPLY
	User Authentication	APPLY
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	SHOULD
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	SHOULD
	Connection Integrity without Recovery	APPLY
	Selective Field Connection Integrity	SHOULD
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	SHOULD
	Non-repudiation with Proof of Origin	APPLY
	Non-repudiation with Proof of Delivery	APPLY
NNI	Peer-Entity Authentication	APPLY
	Data-Origin Authentication	APPLY
	User Authentication	APPLY
	Access Controls	APPLY
	Connection Confidentiality	SHOULD
	Connectionless Confidentiality	SHOULD
	Selective Field Confidentiality	SHOULD
	Traffic Flow Confidentiality	MAY
	Logging	APPLY
	Connection Integrity with Recovery	SHOULD
	Connection Integrity without Recovery	APPLY
	Selective Field Connection Integrity	SHOULD
	Connectionless Integrity	APPLY
	Selective Field Connectionless Integrity	SHOULD
	Non-repudiation with Proof of Origin	APPLY
	Non-repudiation with Proof of Delivery	APPLY

Bibliography

[b-ITU-T G.983.1] Recommendation ITU-T G.983.1 (2005), *Broadband optical access systems based on Passive Optical Networks (PON)*.

[b-ITU-T G.984.1] Recommendation ITU-T G.984.1 (2008), *Gigabit-capable passive optical networks (G-PON): General characteristics*.

[b-ITU-T M.3050.0] Recommendation ITU-T M.3050.0 (2004), *Enhanced Telecom Operations Map (eTOM) – Introduction*.

[b-ITU-T M.3400] Recommendation ITU-T M.3400 (2000), *TMN management functions*.

[b-ITU-T X.200] Recommendation ITU-T X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

[b-ITU-T X.1051] Recommendation ITU-T X.1051 (2008) | ISO/IEC 27011:2008, *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*.

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2007), *NGN release 1 requirements*.

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[b-ATIS 0100014] ATIS 0100014 (2007), *Information and Communications Security for NGN Converged Services IP Networks and Infrastructure*. <http://store.ihs.com/specsstore/controller;jsessionid=UFdMsksPEtYRCIgq5a6LpA**.app12?event=DOCUMENT_DETAILS&docId=BDHYKCAAAAAAAAAA>

[b-ATIS 0300074] ATIS 0300074 (2006), *Guidelines and Requirements for Security Management Systems*. <http://global.ihs.com/family_search_res.cfm?currency_code=USD&customer_id=2125482C4E0A&shopping_cart_id=2624482B2F4B30204D0A&country_code=US&lang_code=ENGL&item_s_key=00481633&document_name=ATIS%200300074&stage=H>

[b-3GPP TS 32.371] 3GPP TS 32.371 (2008), *Telecommunication management: Security Management concept and requirements*. <http://webapp.etsi.org/action/PU/20080729/ts_132371v070301p.pdf>

[b-ANSI T1.276] ANSI T1.276-2003[1], *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane*. <http://engineers.ihs.com/document/abstract/EBPFJBAAAAAAAAAA>

[b-DoD 5200.28] DoD Standard 5200.28 (1985), *Department of Defense Trusted Computer System Evaluation Criteria*. <http://www.iwar.org.uk/comsec/resources/standards/rainbow/5200.28-STD.html>

[1] T1 standards are maintained since November 2003 by ATIS.

[b-ETSI TS 188 003] ETSI TS 188 003 v1.1.2 (2006), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); OSS requirements; OSS definition of requirements and priorities for further network management specifications for NGN*. <http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=24397>

[b-IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol DARPA Internet Program Protocol Specification*. <http://www.ietf.org/rfc/rfc0791.txt?number=791>

[b-IETF RFC 793] IETF RFC 793 (1981), *Transmission Control Protocol DARPA Internet Program Protocol Specification*. <http://www.ietf.org/rfc/rfc0793.txt?number=793>

[b-IETF RFC 854] IETF RFC 854 (1983), *TELNET Protocol Specification*. <http://www.ietf.org/rfc/rfc0854.txt?number=854>

[b-IETF RFC 913] IETF RFC 913 (1984), *Simple File Transfer Protocol*. <http://www.ietf.org/rfc/rfc0913.txt?number=913>

[b-IETF RFC 959] IETF RFC 959 (1985), *File Transfer Protocol (FTP)*. <http://www.ietf.org/rfc/rfc0959.txt?number=959>

[b-IETF RFC 1305] IETF RFC 1305 (1992), *Network Time Protocol (Version 3), Specification, Implementation and Analysis*. <http://www.ietf.org/rfc/rfc1305.txt?number=1305>

[b-IETF RFC 1350] IETF RFC 1350 (1992), *The TFTP Protocol (Revision 2)*. <http://www.ietf.org/rfc/rfc1350.txt?number=1350>

[b-IETF RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*. <http://www.ietf.org/rfc/rfc2104.txt?number=2104>

[b-IETF RFC 2131] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*. <http://www.ietf.org/rfc/rfc2131.txt?number=2131>

[b-IETF RFC 2181] IETF RFC 2181 (1997), *Clarifications to the DNS Specification*. <http://www.ietf.org/rfc/rfc2181.txt?number=2181>

[b-IETF RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*. <http://www.ietf.org/rfc/rfc2403.txt?number=2403>

[b-IETF RFC 2404] IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and AH*. <http://www.ietf.org/rfc/rfc2404.txt?number=2404>

[b-IETF RFC 2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm with Explicit IV*. <http://www.ietf.org/rfc/rfc2405.txt?number=2405>

[b-IETF RFC 2410] IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use With IPsec*. <http://www.ietf.org/rfc/rfc2410.txt?number=2410>

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol – HTTP/1.1*. <http://www.ietf.org/rfc/rfc2616.txt?number=2616>

[b-IETF RFC 2818] IETF RFC 2818 (2000), *HTTP over TLS*. <http://www.ietf.org/rfc/rfc2818.txt?number=2818>

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)*. <http://www.ietf.org/rfc/rfc2865.txt?number=2865>

[b-IETF RFC 3268] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*. <http://www.ietf.org/rfc/rfc3268.txt?number=3268>

[b-IETF RFC 3414] IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*. <http://www.ietf.org/rfc/rfc3414.txt?number=3414>

[b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*. <http://www.ietf.org/rfc/rfc3588.txt?number=3588>

[b-IETF RFC 4120] IETF RFC 4120 (2005), *The Kerberos Network Authentication Service (V5)*. <http://www.ietf.org/rfc/rfc4120.txt?number=4120>

[b-IETF RFC 4251] IETF RFC 4251 (2006), *The Secure Shell (SSH) Protocol Architecture*. <http://www.ietf.org/rfc/rfc4251.txt?number=4251>

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*. <http://www.ietf.org/rfc/rfc4301.txt?number=4301>

[b-IETF RFC 4302] IETF RFC 4302 (2005), *IP Authentication Header*. <http://www.ietf.org/rfc/rfc4302.txt?number=4302>

[b-IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP)*. <http://www.ietf.org/rfc/rfc4303.txt?number=4303>

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol*. <http://www.ietf.org/rfc/rfc4306.txt?number=4306>

[b-IETF RFC 4307] IETF RFC 4307 (2005), *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*. <http://www.ietf.org/rfc/rfc4307.txt?number=4307>

[b-IETF RFC 4346] IETF RFC 4346 (2006), *The Transport Layer Security (TLS) Protocol Version 1.1*. <http://www.ietf.org/rfc/rfc4346.txt?number=4346>

[b-IETF RFC 4347] IETF RFC 4347 (2006), *Datagram Transport Layer Security*. <http://www.ietf.org/rfc/rfc4347.txt?number=4347>

[b-IETF RFC 4510] IETF RFC 4510 (2006), *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*. <http://www.ietf.org/rfc/rfc4510.txt?number=4510>

[b-IETF RFC 4511] IETF RFC 4511 (2006), *Lightweight Directory Access Protocol (LDAP): The Protocol*. <http://www.ietf.org/rfc/rfc4511.txt?number=4511>

[b-IETF RFC 4512] IETF RFC 4512 (2006), *Lightweight Directory Access Protocol (LDAP): Directory Information Models*. <http://www.ietf.org/rfc/rfc4512.txt?number=4512>

[b-IETF RFC 4513] IETF RFC 4513 (2006), *Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms*. <http://www.ietf.org/rfc/rfc4513.txt?number=4513>

[b-IETF RFC 4835] IETF RFC 4835 (2007), *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*. <http://www.ietf.org/rfc/rfc4835.txt?number=4835>

[b-IETF RFC 4960] IETF RFC 4960 (2007), *Stream Control Transmission Protocol*. <http://www.ietf.org/rfc/rfc4960.txt?number=4960>

[b-RSA] RSA Laboratories PKCS 12 v1.0 (1999), *Personal Information Exchange Syntax*. <http://www.rsa.com/rsalabs/node.asp?id=2138>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	**Telecommunication management, including TMN and network maintenance**
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009