International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2701

(04/2007)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Security

Security requirements for NGN release 1

ITU-T Recommendation Y.2701

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	**Y.2700–Y.2799**
Generalized mobility	Y.2800–Y.2899

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

ITU-T Recommendation Y.2701

Security requirements for NGN release 1

Summary

ITU-T Recommendation Y.2701 provides security requirements for next generation networks (NGNs) and its interfaces (e.g., UNIs, NNIs and ANIs) by applying ITU-T Rec. X.805, *Security architecture for systems providing end-to-end communications* to ITU-T Recs Y.2201, *NGN release 1 requirements* and Y.2012, *Functional requirements and architecture of the NGN release 1*.

The requirements are to provide network-based security of end user communications across multiple-network administrative domains. Security of customer assets and information in the customer domain (e.g., user network), and the use of peer-to-peer application capabilities on customer equipment are not within the scope of this Recommendation.

This Recommendation uses trust model based on network elements (physical boxes). NGN providers will be deploying network elements that support the functional entities defined in ITU-T Rec. Y.2012. The bundling of these functional entities to a given network element will vary, depending on the vendor. Therefore, this Recommendation will not attempt to show a strict and fixed bundling between logical functional entities and physical network elements.

The requirements in this Recommendation should be treated as a minimum set of security requirements, and NGN providers are encouraged to take additional measures beyond those specified in Recommendations for NGN security.

Source

ITU-T Recommendation Y.2701 was approved on 27 April 2007 by ITU-T Study Group 13 (2005-2008) under the WTSA Resolution 1 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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

ITU-T Recommendation Y.2701

Security requirements for NGN release 1

1 Scope

This Recommendation provides security requirements for next generation networks (NGNs) against security threats. It is achieved by applying the principles of [ITU-T X.805], *Security architecture for systems providing end-to-end communications* to [ITU-T Y.2201], *NGN release 1 requirements* and [ITU-T Y.2012], *Functional requirements and architecture of the NGN release 1*.

The requirements are to protect the following in a multi-network environment:

- network and service provider infrastructure and its assets (e.g., NGN assets and resources such as network elements, systems, components, interfaces, and data and information), its resources, its communications (i.e., signalling, management and data/bearer traffic) and its services;
- NGN services and capabilities (e.g., voice, video and data services);
- end user communication and information (e.g., private information).

The requirements are to provide network-based security of end user communications across multiple-network administrative domains. Security of customer assets and information in the customer domain (e.g., user network), and the use of peer-to-peer application capabilities on customer equipment are not within the scope of this Recommendation.

The requirements specified in this Recommendation are applicable to an NGN, including user-to-network interfaces (UNIs), network-to-network interfaces (NNIs) and application-to-network interfaces (ANIs) in a multi-network environment.

NGN service providers will be deploying "network elements" that support the functional entities defined in [ITU-T Y.2012]. The bundling of these functional entities to a given network element will vary, depending on the vendor. Therefore, this Recommendation will not attempt to show a strict and fixed bundling between logical functional entities and physical network elements.

The requirements in this Recommendation should be treated as a minimum set of requirements for NGN security and should not be considered to be exhaustive. Therefore, an NGN provider may need to take additional measures beyond those specified in Recommendations for NGN security.

In addition, the requirements in this Recommendation cover some of the technical aspects of what is generally known as IdM ("identity management"). A working definition of IdM is "management by NGN providers of trusted attributes of an entity such as: a subscriber, a device or a provider". This is not intended to indicate positive validation of a person.

Administrations may require NGN providers to take into account national regulatory and national policy requirements in implementing this Recommendation.

1.1 X.805 principles

[ITU-T X.805] defines the following security dimensions:

access control;

authentication;

non-repudiation;

data confidentiality;

communication security;

data integrity;

availability;

privacy.

It also identifies the following security threats.

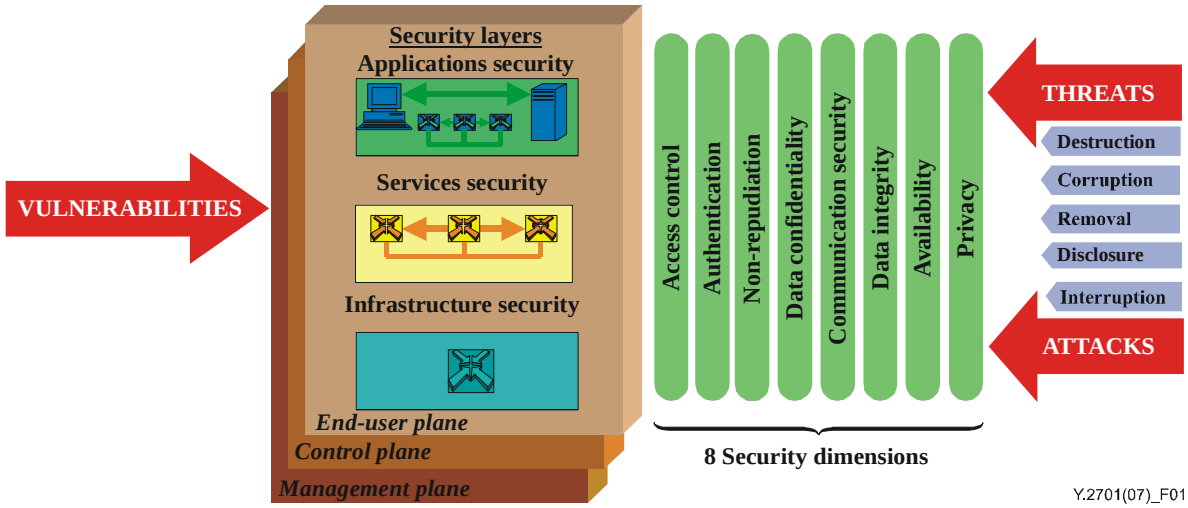

Figure 1 – Security architecture of X.805 (Figure 3/X.805)

These security dimensions and security threats stated above are considered as the base of this Recommendation.

This Recommendation does not further define or distinguish the use of the X.805 security layers (applications, services, or infrastructure) and compliance with this standard does not require such a distinction. This Recommendation does make reference to a distinction between management, control, and user plane traffic, but cautions the reader that the utilization of that classification varies depending on the layer in a protocol stack that is under consideration. Therefore, additional standards will need to be referenced to determine compliance with such distinctions. This standard provides recommendations concerning application of the security dimensions, but does not infer completeness for use as a security assessment for NGN networks.

1.2 Assumptions

This Recommendation is based on the following assumptions:

1) The bundling of functional entities, as defined in [ITU-T Y.2012], to a given network element will vary, depending on the vendor.

2) Each NGN provider has specific responsibilities within its domain for security. For example, implementing applicable security services and practices to:

   a) protect itself;

   b) assure end-to-end security is not compromised within its network; and

   c) assure high availability of NGN communications.

3) Each network domain will establish and enforce policies for service level agreements (SLAs) to assure the security of its domain and the security of the network interconnections. It is assumed that the SLAs would specify security services, mechanisms and practices to be implemented to protect the interconnected networks and the communications (signalling/control traffic, bearer traffic and management traffic) across UNIs, ANIs and NNIs.

4) This Recommendation addresses network-based security, which is a layered architecture, consisting of perimeter security to trusted domains, physical security of provider equipment, and potentially the use of encryption.

1.3 Overview

This Recommendation is organized as follows:

- Clause 2 (References) – This clause provides normative references.
- Clause 3 (Definitions and abbreviations) – This clause provides definitions and abbreviations used in this Recommendation.
- Clause 4 (Security threats and risks) – This clause highlights security threats and risks assumed for the NGN environment. Assumed security threats and risks are used as guidance to develop requirements for security and to identify security capabilities and procedures to be supported.
- Clause 5 (Security trust model) – This clause describes a trust model for NGN security. The trust model can be used to develop trust relations for UNI, ANI and NNI connectivity and design of security architecture.
- Clause 6 (Security architecture) – This clause describes the relationship between the functional NGN architecture defined in [ITU-T Y.2012] and composite security architectures.
- Clause 7 (Objectives and requirements) – This clause describes security objectives and general requirements for NGNs to be used as the basis to define security requirements for NGNs.
- Clause 8 (Specific security requirements) – This clause provides specific security requirements as defined in clause 7.
- Appendix I – Security objectives and requirements for emergency telecommunications services (ETS).
- Bibliography.

This Recommendation is defined to provide a base for NGN security. Various companion Recommendations for specific security areas, e.g., authenticaition and authorization, certificate management, identity management, among others, are to be provided in the future.

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.3016.0] ITU-T Recommendation M.3016.0 (2005), *Security for the management plane: Overview*.

[ITU-T M.3016.1] ITU-T Recommendation M.3016.1 (2005), *Security for the management plane: Security requirements*.

[ITU-T X.800] ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[ITU-T X.805] ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[ITU-T Y.2012] ITU-T Recommendation Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

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

3 Definitions and abbreviations

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 emergency telecommunications service (ETS): National service, providing authorized priority communications to facilitate the work of emergency personnel in times of disaster. (See ITU-T Rec. E.107.)

3.1.2 user: A user includes end user (ITU-T Rec. Y.2091), person, subscriber, system, equipment, terminal (e.g., FAX, PC), (functional) entity, process, application, provider, or corporate network.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 asset: Anything that has value to the organization, its business, its operations and its continuity.

3.2.2 border element: Network element providing functions connecting different security and administrative domains.

3.2.3 corporate network: A private network that supports multiple users and may be in multiple locations (e.g., an enterprise, a campus).

3.2.4 domain border element: Border element under sole control of the provider, providing security functions with other network domains.

3.2.5 network border element: Border element under sole control of the provider, providing security functions with terminal equipment.

3.2.6 security domain: A set of elements, a security policy, a security authority and a set of security-relevant activities in which the elements are managed in accordance with the security policy. The policy will be administered by the security authority. A given security domain may span multiple security zones.

3.2.7 security zone: This Recommendation defines 3 security zones:

1) trusted;

2) trusted but vulnerable; and

3) un-trusted.

A security zone is defined by operational control, location, and connectivity to other device/network elements.

3.2.8 terminal equipment border element: Border element providing security functions between customer premises equipment and service provider network.

3.2.9 trust: Entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.

3.2.10 trusted but vulnerable zone: From the viewpoint of a NGN provider, a security zone where the network elements/devices are operated (provisioned and maintained) by the NGN provider. The equipment may be under the control by either the customer/subscriber or the NGN provider. In addition, the equipment may be located within or outside the NGN provider's domain. They communicate with elements both in the trusted zone and with elements in the un-trusted zone, which is why they are "vulnerable". Their major security function is to protect the NEs in the trusted zone from the security attacks originated in the un-trusted zone in a fail-safe manner.

3.2.11 trusted zone: From the viewpoint of a NGN provider, a security domain where a NGN provider's network elements and systems reside and never communicate directly with customer equipment. The common characteristics of NGN network elements in this domain are that they are under the full control of the related NGN provider, are located in the NGN provider premises (which provides physical security), and they communicate only with elements in the "trusted" domain and with elements in the "trusted-but-vulnerable" domain.

3.2.12 un-trusted zone: From the viewpoint of a NGN provider, a zone that includes all network elements of customer networks or possibly peer networks or other NGN provider zones outside of the original domain, which are connected to the NGN provider's border elements.

3.2.13 user network: A private network consisting of terminal equipment that may have multiple users.

3.3 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms.

3G	3rd Generation
AGW	Access Gateway
ANI	Application-to-Network Interface
B2BUA	Back-to-Back User Agent
BE	Border Element
CSC-FE	Call Session Control Functional Entity
DBE	Domain Border Element
DNS	Domain Name System
ETS	Emergency Telecommunications Service
FE	Functional Entity
GW	Gateway
I-CSC-FE	Interrogating Call Session Control Functional Entity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LAN	Local Area Network
MPLS	Multi Protocol Label Switching
MRP-FE	Media Resource Processing Functional Entity
NAC-FE	Network Access Control Functional Entity
NAPT	Network Address and Port Translation
NAT	Network Address Translation

NBE	Network Border Element
NE	Network Element
NGN	Next Generation Network
NNI	Network-to-Network Interface
OAMP	Operations, Administration, Maintenance and Provisioning
P-CSC-FE	Proxy Call Session Control Functional Entity
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAC-FE	Resource and Admission Control Functional Entity
RAN	Radio Access Network
RTSP	Real Time Streaming Protocol
SAA-FE	Service Authentication and Authorization Functional Entity
S-CSC-FE	Serving Call Session Control Functional Entity
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SL-FE	Subscription Locator Functional Entity
TAA-FE	Transport Authentication and Authorization Functional Entity
TE	Terminal Equipment
TE-BE	Terminal Equipment Border Element
TMN	Telecommunication Management Network
UA	User Agent
UICC	Universal Integrated Circuit Card
UNI	User-to-Network Interface
VLAN	Virtual LAN
W-CDMA	Wideband Code Division Multiple Access
WLAN	Wireless LAN
xDSL	x Digital Subscriber Line

4 Security threats and risks

This Recommendation assumes that the systems, components, interfaces, information, resources, communications (i.e., signalling, management and data/bearer traffic) and services that make up an NGN will be exposed to a variety of security threats and risks. Those threats and risks will depend on a variety of factors. In addition, end users will also be exposed to certain threats (e.g., unauthorized access to private information).

Threats to the NGN:

- unauthorized reconnaissance, such as the remote analysis of the system to determine points of weakness (these may include scans, sweeps, port interrogation, route tables, etc.);
- break-in/device takeover resulting in loss of control of the device, anomalies and errors in the configuration audits;
- destruction of information and/or other resources;
- corruption or modification of information;
- theft, removal or loss of information and/or other resources;
- disclosure of information; and
- interruption of services and denial of services.

Further, it is clear that NGNs will be operating in an environment different from the PSTN environment and may therefore be exposed to different types of threats and attacks from within or externally. NGNs will have direct or indirect connectivity to un-trusted and trusted networks and terminal equipment, and therefore will be exposed to security risks and threats associated with connectivity to un-secure networks and customer premises equipment. For example, a provider's NGN may have direct or indirect (i.e., through another network) connectivity to the following as shown in Figure 2:

- other service providers, and their applications;
- other NGNs;
- other IP-based networks;
- public switched telephone network (PSTN);
- corporate networks;
- user networks;
- terminal equipment;
- other NGN transport domains.

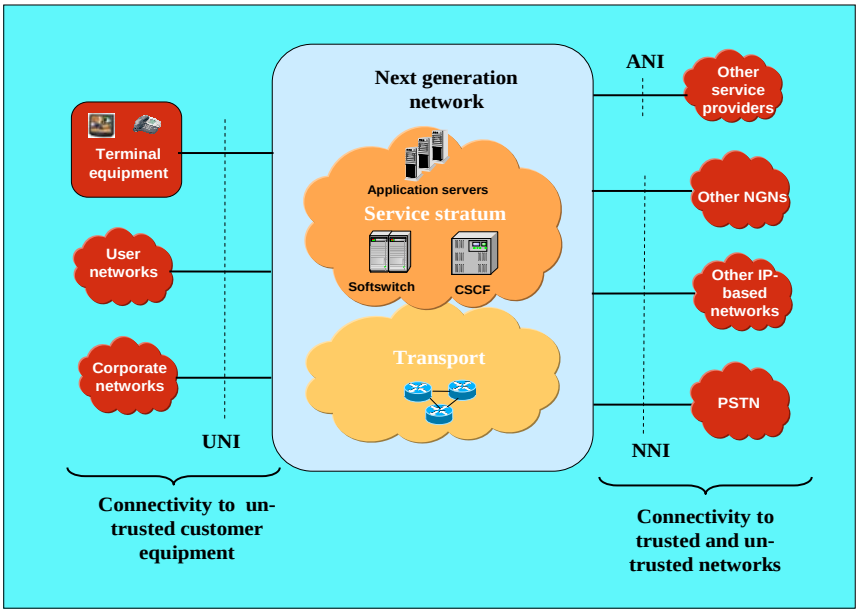

Figure 2 – Connectivity to networks and users

In the evolving environment, security across multiple network provider domains relies on the aggregation of what all providers elect to do for securing their networks. Unauthorized network access into one provider's network can easily lead to exploitation of an interconnected network and its associated services. This is an example of the exploitation of the weakest link that can threaten a provider network's integrity and service continuity along with a host of various types of attacks.

Each NGN provider is responsible for security within its domain. Each NGN provider is responsible for designing and implementing security solutions using network specific policy for trust relations (clause 5), to meet its own network-specific needs and to support global end-to-end security objectives across multiple network provider domains.

5 Security trust model

This clause defines the NGN security trust model.

The NGN functional reference architecture defines functional entities (FEs). However, since network security aspects depend heavily on the way that FEs are bundled together, the NGN security architecture is based on physical network elements (NEs), i.e., tangible boxes that contain one or more FEs. The way these FEs are bundled into NEs will vary, depending on the vendor.

5.1 Single network trust model

This subclause defines three security zones:

1) trusted;

2) trusted but vulnerable;

3) un-trusted,

that are dependent on operational control, location, and connectivity to other device/network elements. These three zones are illustrated in the security trust model shown in Figure 3.

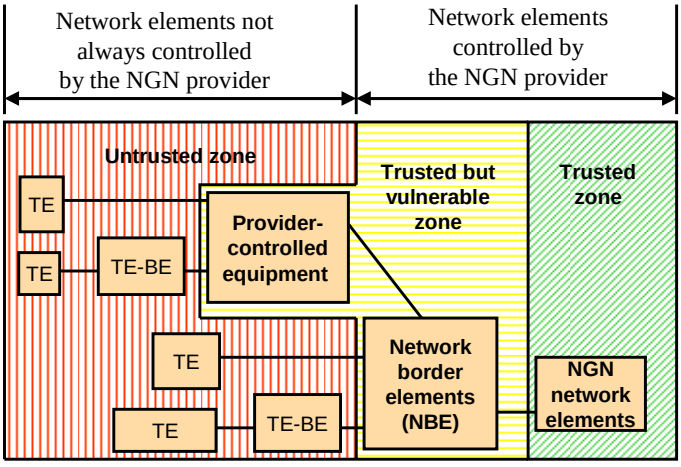

Figure 3 – Security trust model

A "trusted network security zone" or "trusted zone" in short is a zone where a NGN provider's network elements and systems reside and never communicate directly with customer equipment or other domains. The common characteristics of NGN network elements in this zone are that they are under the full control of the NGN provider, are located in the NGN provider domain, and they communicate only with elements in the "trusted" zone and with elements in the

"trusted-but-vulnerable" zone. It should not be assumed that because it is in a trusted zone it is secure *per se*.

The "trusted zone" will be protected by a combination of various methods. Some examples are physical security of the NGN network elements, general hardening of the systems, use of secure signalling, security for OAMP messages separate VPN within the (MPLS/)IP network for communication within the "trusted" zone and with NGN network elements in the "trusted-but-vulnerable" zone. See clause 8 for more details.

A "trusted but vulnerable network security zone", or "trusted but vulnerable zone" in short, is a zone where the network elements/devices are operated (provisioned and maintained) by the NGN provider. The equipment may be under the control by either the customer/subscriber or the NGN provider. In addition, the equipment may be located within or outside the NGN provider's premises. They communicate with elements both in the trusted zone and with elements in the un-trusted zone, which is why they are "vulnerable". Their major security function is to protect the NEs in the trusted zone from the security attacks originated in the un-trusted zone.

Elements that are located on the NGN provider's domain with connectivity to elements outside the trusted zone are referred to as network border elements (NBEs). Examples of these are the:

- Network border elements (NBE) at the UNI that interface with the service control or transport elements of the NGN provider in the trusted zone in order to provide the user/subscriber access to the NGN provider's network for services and/or transport.
- Domain border element (DBE) that is the same kind of equipment with network border element except that it resides at the border of domains.
- Device configuration & bootstrap NBE (DCB-NBE) that interface with the NGN provider's device configuration system in the trusted zone in order to configure the user's/subscriber's device and NGN provider's equipment in the outside plant.
- OAMP-NBE interfaces with the NGN provider's OAMP systems in the trusted zone in order to provide and maintain the user's/subscriber's device and NGN provider's equipment in the outside plant.
- Application server/web server NBE (AS/WS-NBE) that interfaces with the NGN provider's AS/WS-NBE in the trusted zone in order to provide the user/subscriber access to web-based services.

Examples of devices/elements that are operated by an NGN provider but are not located on the NGN provider's premises, and that may or may not be under the control of the NGN provider, are:

- outside plant equipment in the access network/technology;
- base station router (BSR), a network element that integrates the base station, radio network controller and router functionalities;
- optical units (ONUs) within a user/subscriber's residence.

The "trusted-but-vulnerable" zone, comprised of NBEs, will be protected by a combination of various methods. Some examples are physical security of the NGN network elements, general hardening of the systems, use of secure signalling for all signalling messages sent to NGN network elements in the "trusted" zone, security for OAMP messages and packet filters and firewalls as appropriate. See clause 8 for more details.

An "un-trusted zone" includes all network elements of customer networks or possibly peer networks or other NGN provider domains outside of the original domain, which are connected to the NGN provider's network border elements. In the "un-trusted zone", comprised of terminal equipment, equipment may not be under the control of NGN providers and it may be impossible to enforce provider's security policy on user. It is still desirable to try to apply some security measures and, to that end, it is recommended that signalling, media, and OAM&P be secured and the TE-BE located

in the "un-trusted zone" be hardened. However, due to the lack of physical security, these measures cannot be considered absolutely safe. See clause 8 for more details.

5.2 Peering network trust model

When an NGN is connected to another network, the trust depends on:

- physical interconnection, where the interconnection can range from a direct connection in a secure building to via shared facilities;
- peering model, where the traffic can be exchanged directly between the two NGN service providers, or via one or more NGN transport providers;
- business relationships, where there may be penalty clauses in the SLA agreements, and/or a trust in the other NGN provider's security policy;
- in general, NGN providers should view other providers as un-trusted.

Figure 4 shows an example when a connected network is judged un-trusted.

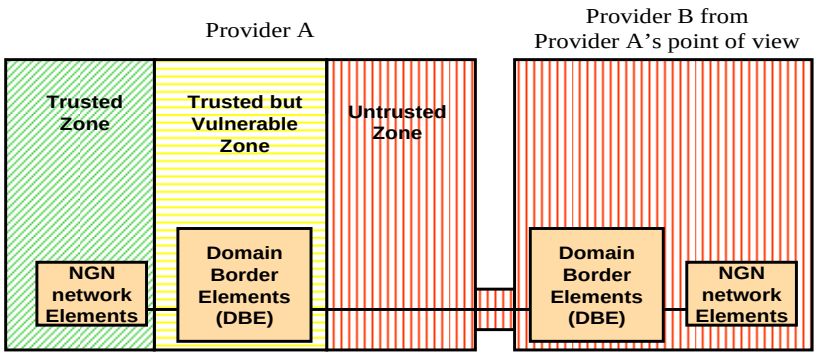

Figure 4 – Peering trust model

6 Security architecture

6.1 Functional NGN architecture reference

The NGN architecture that realizes [ITU-T Y.2201], *NGN release 1 requirements* is defined in [ITU-T Y.2012], *Functional requirements and architecture of the NGN release 1.*

Figure 5 shows a functional view of the NGN architecture.

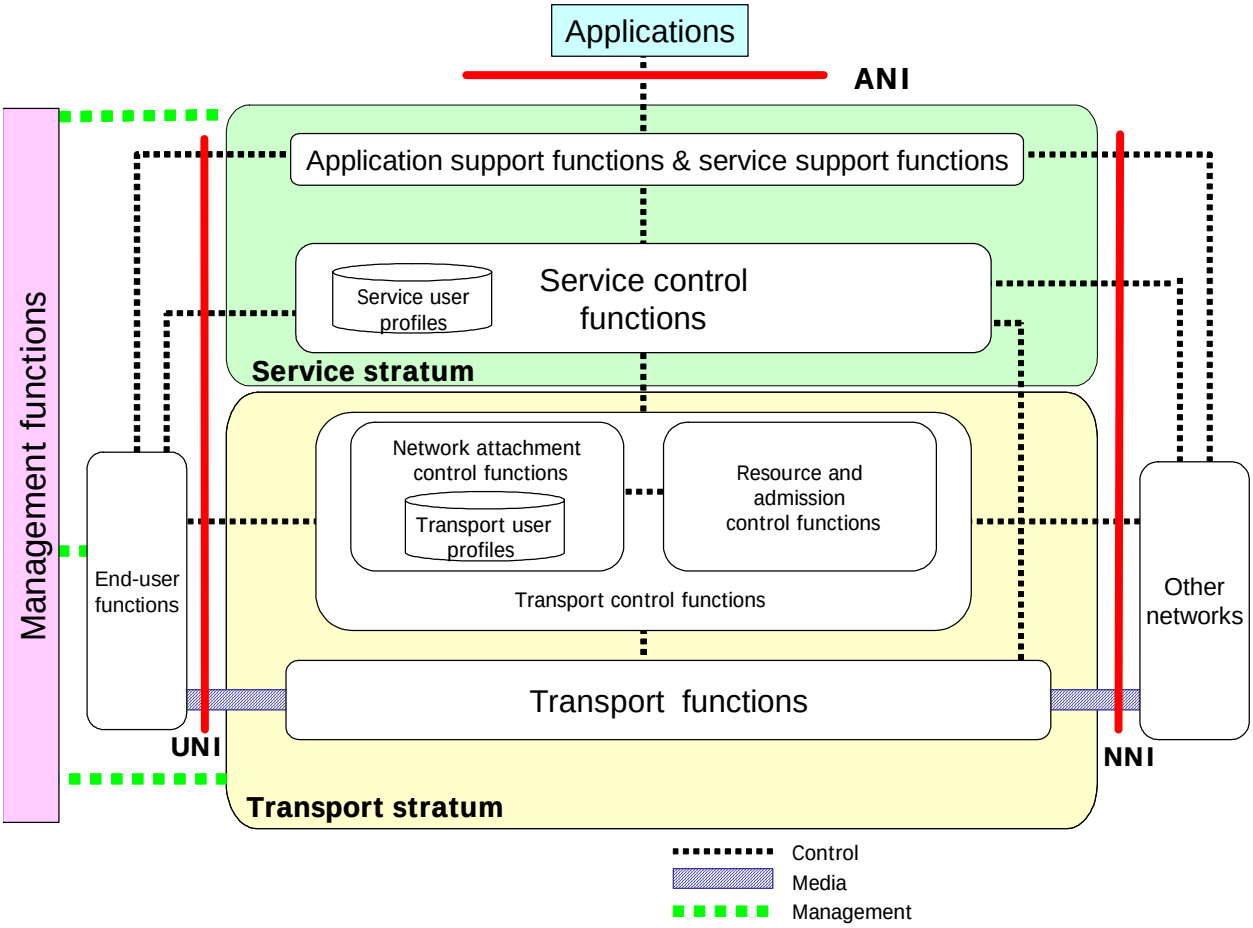

Figure 5 – NGN architecture overview (Figure 1/Y.2012)

The NGN supports a reference point to the end-user functions called user-to-network interface (UNI), and to other networks called network-to-network interface (NNI). It also supports a reference point to the applications functional group called application-to-network interface (ANI), enabling application of NGN capabilities to create and provision applications for NGN users.

The NGN Release 1 transport stratum provides IP connectivity services to NGN users under the control of transport control functions, including the network attachment control functions (NACF) and resource and admission control functions (RACF).

The service stratum delivers services and applications to the end-user by utilizing the application support functions and service support functions and related control functions.

The end-user functions are functions connected to the NGN access networks and no assumptions are made about the diverse end-user interfaces and end-user networks.

The management functions provide the ability to manage the NGN in order to provide NGN services with the expected quality, security and reliability.

For further details, see [ITU-T Y.2012].

6.2 Mapping to NGN functional architecture

This Recommendation describes the method to achieve security by using the trust model shown in clause 5, that is, an NGN composed of trusted domain (green zone), un-trusted domain (red zone), and trusted but vulnerable domain (yellow zone) in-between.

One of the key issues to achieve security with this model is the method to transmit signalling, media, OAMP traffic from the un-trusted domain to the trusted domain. There are various methods to achieve this, and NGN provider decides the method considering its policy. Below are examples of these methods.

a) Install NEs to terminate traffic (e.g., B2BUA for SIP signalling) between the green zone and the red zone. It receives a packet from the red zone, examines it, discards it if inappropriate, and if appropriate copies the necessary part to reconstruct a packet appropriate for the green zone. In this case, NEs to terminate traffic become the yellow zone NEs.

b) Controls the traffic in media layer (e.g., by opening and closing a particular port (pinhole) at the firewall, and guarantees that only authorized NEs (and users) can send traffic to the equipment in the green zone). In this case, NEs that control traffic become the yellow zone NEs.

c) End to end encryption between the sender and the receiver.

In the functional architecture shown in [ITU-T Y.2012] (Figure 6 of this Recommendation), SIP signalling generated by the end-user function (it is usually un-trusted because the NGN provider cannot confirm that the function is not forged) is transmitted to S-2, P-CSC-FE. NEs that contain P-CSC-FE therefore are considered as yellow zone NEs, or as green zone NEs due to the firewall functions. If NEs that contain S-1 (S-CSC-FE) are separated from NEs that contain P-CSC-FE, they are considered as green zone NEs.

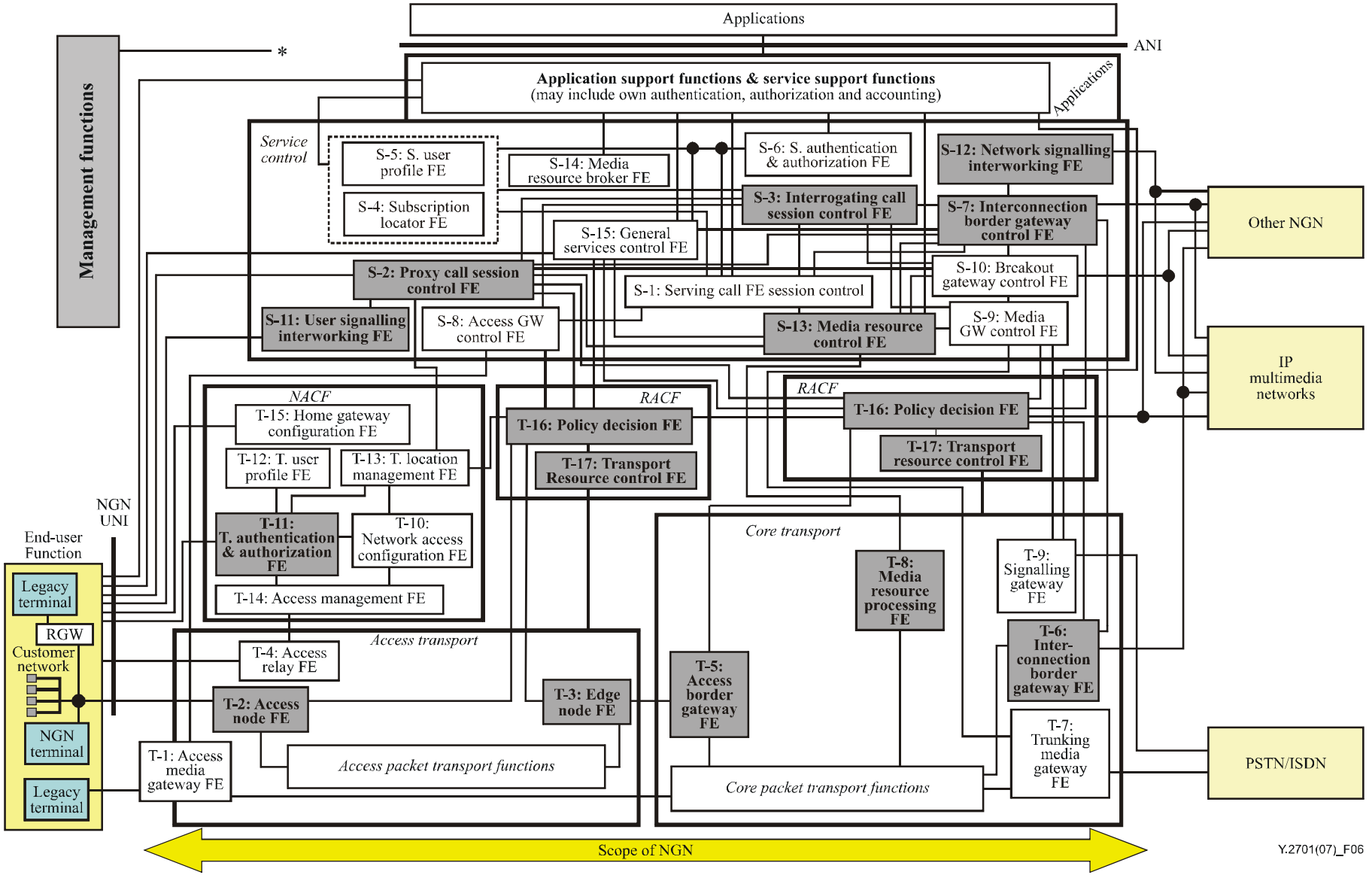

Figure 6 – Generalized functional architecture (Figure 3/Y.2012)

6.3 Identification of NGN resources for security protection

Each network provider is required to identify assets, resources, information and interfaces within its network to be protected, and the threats that need to be mitigated. For example, network elements, interfaces (UNI, ANI and NNI), management systems, and signalling, management and media/bearer communications. In identifying NGN resources for security protection against threats, the theoretical layered architecture defined in [ITU-T Y.2012] is to be considered together with practical realization of the functional entities.

The following tables provide example NGN assets, resources and interfaces for security protection against threats, organized as follows:

- Table 1 – Example UNI related assets, resources and information.
- Table 2 – Example transport stratum related assets, resources, information and interfaces.
- Table 3 – Example service stratum related assets, resources, information and interfaces.
- Table 4 – Example management related assets, resources, information and interfaces.

The examples in Tables 1 to 4 are not exhaustive.

Table 1 – Example UNI related assets, resources and information

Examples	Objectives and goals
End user resources: • User devices • User network gateways • Corporate network gateways	a) Protect end user equipment attached to the network (e.g., terminals, user network and corporate network gateways) against network originated attacks (e.g., attacks to destroy, corrupt, modify user equipment). b) Protect against interruption of services (e.g., denial of service attacks) and assurance of service availability. c) Protect the network from unauthorized access (e.g., unauthorized users and user devices).
End-user information: • Subscription information • Identity information • Location information	a) Protect against corruption or modification of information. b) Protect against theft, removal or loss (e.g., identity theft). c) Protect against disclosure (e.g., unauthorized access to location information).
NGN provider information • Identity information	a) Protect against corruption or modification of information. b) Protect against theft, removal or loss (e.g., identity theft). c) Protect against disclosure (e.g., unauthorized access to location information).
UNI interfaces	a) Transport stratum – Provide security protection of media/bearer traffic across UNI interfaces. b) Service stratum (service control) – Provide security protection of signalling and management across UNI interfaces (e.g., SIP, HTTPs, ISDN, and H.248). c) Service stratum (application and service support) – Provide security protection of application and service control functions across UNI interfaces (e.g., in-band signalling).

Table 2 – Example transport stratum related assets, resources, information and interfaces

Examples	Goals and objectives
Transport stratum resources: • Transport network elements (e.g., IP routers, MPLS nodes) • Transmission links • Routing information (e.g., DNS servers) • Transport user profile information (e.g., transport databases and data repository)	a) Protect all transport network elements, components and functions against unauthorized access. b) Protect the integrity of transport network elements, components and functions. c) Protect availability of transport network elements, components and functions. Protection against interruption of services (i.e., against denial of service attacks). d) Protect against disclosure of any user or network private information.
Transport stratum inter-system communications (communications within a network provider network)	a) Provide security protection of media/bearer traffic between systems within a provider network. b) Provide security protection of transport control (e.g., OSPF) signalling and management within a provider network. c) Provide security of signalling between systems in the service stratum (e.g., application servers) and systems in the transport stratum (e.g., IP routers).
Transport interfaces and communications	a) Provide security protection of media/bearer traffic across transport UNI, NNI and ANI interfaces. b) Provide security protection of transport control signalling (e.g., OSPF) and management across transport UNI, NNI and ANI interfaces.

Table 3 – Example service stratum related assets, resources, information and interfaces

	Examples	Goals and objectives
Service stratum – Service control	Service stratum – Service control resources • Service control network elements (e.g., CSC-FEs, SL-FE, MRP-FE, Gateways, S/BCs)	a) Protect all service control network elements, components and functions against unauthorized access. b) Protect the integrity of service control network elements, components and functions, including protection against corruption or modification of information. c) Protect availability of service control network elements, components and functions. Protect against interruption of services (i.e., against denial of service attacks).
	Service stratum – Service control information • Subscriber information (e.g., databases and data repository containing user profiles and service profiles) • NGN provider information (e.g., databases and data repository containing routing, numbering and addressing information)	a) Protect against corruption or modification of data and information. b) Protect against theft, removal or loss (e.g., identity theft). c) Protect against disclosure (e.g., unauthorized access to user and network private information).
	Service stratum – Service control inter-system communication	Provide security protection of inter-system signalling (e.g., SIP, RADIUS, Diameter) within a network provider network (e.g., CSCF to HSS signalling).
	Interfaces and communications	Provide security protection of signalling and management across UNI, NNI and ANI interfaces.

Table 3 – Example service stratum related assets, resources, information and interfaces

	Examples	Goals and objectives
Service stratum – Application and service support	Service stratum – Application and service support resources: • Application and service support network elements and platforms (e.g., application servers, databases, web portals)	a) Protect all service support network elements, components and functions against unauthorized access. b) Protect the integrity of service support network elements, components and functions, including protection against corruption or modification of information. c) Protect availability of service support network elements, components and functions. d) Protect against interruption of services (i.e., against denial of service attacks).
	Service stratum – Application and service support information: • Application and service information • Subscription information	a) Protect against corruption or modification of data and information. b) Protect against theft, removal or loss (e.g., identity theft). c) Protect against disclosure (e.g., unauthorized access to user and network private information).
	Interfaces	a) Provide security protection of network elements and resources for other application provider access (e.g., Parlay and Open Mobile Alliance gateways). b) Provide security protection of UNI, NNI and ANI interfaces. c) Provide security protection of signalling and management traffic across ANI interfaces.

Table 4 – Example management related assets, resources, information and interfaces

Example	Goals and objectives
Management resources • Transport stratum management systems (e.g., network element management, network management and service management systems) • Service stratum management systems (e.g., network element management, network management and service management systems)	a) Protect all management network elements, components, functions and interfaces against unauthorized access. b) Protect the integrity of management network elements, components, functions and interfaces. This includes protection against corruption or modification of information. c) Protect availability of management network elements, components, functions and interfaces. Protection against interruption of services (i.e., against denial of service attacks).
Inter-system communications within a network provider network	a) Provide security protection of management traffic between management systems within a network (e.g., service stratum). b) Provide security protection of management traffic between user network, and network provider transport stratum and service stratum
Interfaces and inter-system communications	a) Provide security of internal network management interfaces and any UNI, NNI and ANI management interfaces. b) Provide security protection of management traffic across UNI, ANI, NNI interfaces.

7 Objectives and requirements

7.1 General security objectives

The following is a list of general security objectives used to guide the requirements in this Recommendation.

- NGN security features should be extensible, and flexible enough to satisfy various needs.
- Security requirements should take the performance, usability, scalability and cost constraints of NGN into account.
- Security methods should be based on existing and well-understood security standards as appropriate.
- The NGN security architecture should be globally scalable (within network provider domains, across multiple network provider domains, in security provisioning).
- The NGN security architecture should respect the logical or physical separation of signalling and control traffic, user traffic, and management traffic.
- NGN security should be securely provisioned and securely managed.
- An NGN should provide security from all perspectives: service, network provider and subscriber.
- Security methods should not generally affect the quality of provided services.
- Security should provide simple, secure provisioning and configuration for subscribers and providers (plug & play).
- Appropriate security levels should be maintained even when multicast functionality is used.

- The service discovery capabilities should support a variety of scoping criteria (e.g., location, cost, etc.) to provide appropriate scaling, with appropriate mechanisms to ensure security and privacy.
- The address resolution system should be a special system used only by this network, and certain security measures are required to be in place. This system may use databases that are internal or external of a domain.
- The principles and general security objectives for secure TMN management as outlined in clause 7 of [ITU-T M.3016.0] should be followed.

7.2 Objectives for security across multiple network provider domains

The general objective is to provide network-based security for end-to-end communications across multiple provider domains. This is achieved by providing security of the end-to-end communication on a hop-by-hop basis across the different provider's domains. Figure 7 shows the general concept of network provided security for end-to-end communications between end users. Each network segment has specific security responsibilities within its security zone to facilitate security and availability of NGN communications across multiple networks.

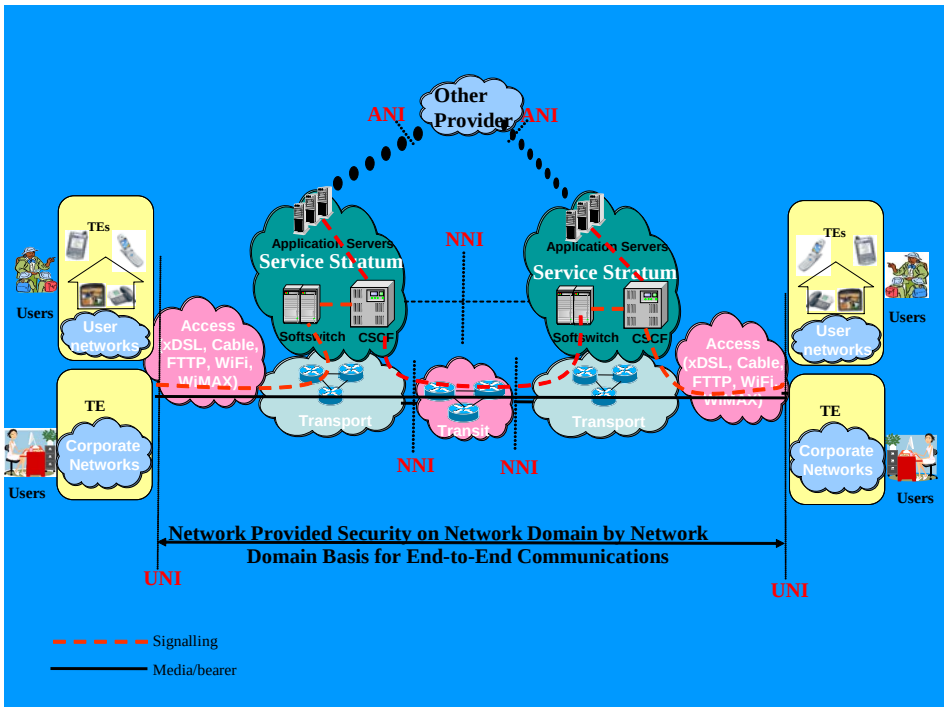

Figure 7 – Security of communications across multiple networks

As described in clause 5.2, the trust model between interconnected NGNs depends on several aspects such as the physical interconnections, peering models and business relationships.

7.3 Requirements specific for security dimensions

The objectives described here are specific to particular security dimensions, such as authentication. They are common to all interfaces.

7.3.1 Access control

NGN providers are required to restrict access to authorized subscribers. Authorization may be given by the provider providing the access or by other providers after validation by an authentication and access control processes.

The NGN is required to prevent unauthorized access, such as by intruders masquerading as authorized users.

7.3.2 Authentication

NGN providers are required to support capabilities for authenticating subscribers, equipment, network elements and other providers. This includes support of, but is not limited to, the following:

1) Capabilities to authenticate users for transport network access (e.g., authentication and authorization of an end user device, a user-network gateway, or a corporate network gateway to obtain access or attachment to the transport network access).
2) Capabilities to authenticate users for access to services at the start of, and during, service delivery (e.g., authentication of a user, a device or a combined user/device where the authentication applies to NGN service/application access).
3) Capabilities for a NGN user to authenticate the NGN provider on each stratum (e.g., user authenticating the identity of the connected NGN provider or of the service provider) if required by security policy.
4) Capabilities to allow user peer-to-peer authentication (e.g., authentication of the called user, the originating entity, or data origin) as network services or features.
5) Capabilities to allow bilateral authentication between two NGN providers on each stratum for exchange of signalling, management and media/bearer traffic (e.g., authentication of directly interconnected and remote networks across NNI interfaces).
6) Capabilities to allow authentication of other service providers across ANI interfaces. SIM-based and/or non-SIM-based approaches are to be supported.

NOTE – Authentication of an entity is not intended to indicate positive validation of a person.

7.3.3 Non-repudiation

This Recommendation does not specify any non-repudiation security requirements.

7.3.4 Data confidentiality

NGN providers are required to protect the confidentiality of subscriber traffic by cryptographic or other means.

NGN providers are required to protect confidentiality of control messages by cryptographic or other means if security policy requests it.

NGN providers are required to protect the confidentiality of management traffic by cryptographic or other means.

7.3.5 Communication security

NGN providers are required to provide mechanisms for ensuring that information is not unlawfully diverted or intercepted.

7.3.6 Data integrity

NGN providers are required to protect the integrity of subscriber traffic by cryptographic or other means.

NGN providers are required to protect integrity of control messages by cryptographic or other means if security policy requests it.

NGN providers are required to protect the integrity of management traffic by cryptographic or other means.

7.3.7 Availability

NGN is required to provide security capabilities to enable NGN providers to prevent or terminate communications with the non-compliant end-user equipment: e.g., to mitigate DoS attacks, spreading of viruses or worms and other attacks. These capabilities may be suspended to allow emergency communications. NGN internal network elements may also be susceptible to viruses, worms and other attacks. Similar measures to quarantine network components are also required.

An NGN should provide provision of security capabilities to enable a NGN provider to filter out packets and traffic that is considered harmful by the respective security policy.

NGN is required to provide capabilities for the support of disaster recovery functions and procedures. The specific requirements are outside the scope of this Recommendation.

7.3.8 Privacy

NGN is required to provide capabilities to protect the subscriber's private information such as location of data, identities, phone numbers, network addresses or call-accounting data according to national regulations and laws. Specific requirements for privacy are a national matter and are outside the scope of this Recommendation.

8 Specific security requirements

This clause deals with the specific requirements for security for each of the network elements within the NGN infrastructure. However, since many of the security needs will be the same for the various types of network elements, the overall security requirements are specified first, in clause 8.1.

Border elements can be integrated or separated according to implementation.

8.1 Common security requirements for NGN elements

These requirements apply to the NGN network elements in trusted zone and in trusted but vulnerable zone. It is desirable that devices in the un-trusted zone follow these requirements.

The following is a list of general security requirements:

Interoperability is required to be supported by the different NGN network elements, in particular among the various NGN security mechanisms. Minimum standardized security features are required to be available worldwide.

Authentication and authorization is required to be performed at both service and transport strata (user-to-network, network-to-user, network-to-network). This should be possible also in presence of NAPT transversal.

A NGN element is required to provide security measures against unauthorized access to network resources, devices, services and subscriber data (profile), for example, to block unauthorized traffic.

The NGN infrastructure is required to allow providers to limit the visibility of the network topology and resources to authorized entities.

The NGN infrastructure is required to support multiple security zones. Isolation in security terms may be required between different security zones.

The NGN infrastructure is required to ensure the confidentiality and integrity of the signalling/control flows and management flows transported on it.

The NGN infrastructure should ensure the confidentiality, the integrity of the media flows transported on it.

NGN is required to carefully ensure the security of network elements linking to management resources (OSS, database, etc.) and service resources.

The security requirements for secure TMN management are to follow those stated in clause 10.1 of [ITU-T M.3016.0] and as further detailed in clause 6 of [ITU-T M.3016.1].

Security functionality is required to be enforced on the network border elements (NBE or TE-BE, i.e., the NEs in trusted but vulnerable zone). This includes functions such as access control on data packets and signalling information according to the policies specified, e.g., refusal of traffic from particular applications or users.

The sensitive NGN elements, especially for network border elements, may perform the logical and/or physical separation of transport paths according to the security policies in place, e.g., the separation of the control and/or managements flows from the media flows using logically different interfaces or different address plans, and using physically different real or virtual transport network (virtual such as VPNs and VLANs).

NGN is required to provide safe storage for security-related data (e.g., identity and credentials data). Such storage is required to be separate from the general data repository that contains subscribers' services-related information. The NGN is required to provide security policy, which includes a set of rules that determine which traffic has to be protected based on, e.g., contracts, what kind of protection is used, how often session keys are changed, and the rules that determine security compliance of a device.

The NGN is required to support the capability to monitor network traffic and establish a baseline of what should be considered normal network events.

The NGN is required to be capable of detecting, reporting, and mitigating occurrences of the abnormal network events.

8.1.1 Security policy

Security policy is a set of rules laid down by the security authority governing the use and provision of security services and facilities. NGN providers shall prepare appropriate security policy and shall be responsible for applying it to all NEs and devices under its control.

8.1.2 Hardening and service disablement

All NGN elements are required to be capable of being configured to support the minimum services needed to support the NGN provider NGN infrastructure. Any service or transport layer port that is not required for the correct operation of the NGN element is required to be disabled on all systems and network elements. In addition, applications are required to run under minimum privileges (e.g., on "UNIX/Linux" platforms applications should not run as root if root privileges are not indispensable). The base operating system (OS) supporting any NGN element is required to be capable of being specifically configured for security and appropriately hardened. No "backdoors" are permitted (software access which would circumvent usual access control mechanisms) into any NGN element.

In addition to hardening, physical and logical access controls are required to be put in place to meet industry best-practices.

8.1.3 Audit trail, trapping and logging

All NGN elements are required to be capable of creating an audit trail that maintains a record of security related events in accordance with NGN provider's security policy. Mechanisms to prevent unauthorized or undetected modification are required.

The audit trail is required to be capable of being managed and is required to allow old data in the audit trail to be placed on other media, e.g., removable media, for long-term storage. This interface is required to allow authorized administrators to move old data out of the audit trail onto removable media. This ability is required to be protected by a specific authorization to manage the audit trail.

Clause 10.1.2.6.3 of [ITU-T M.3016.0] and clauses 6.6, 6.7 of [ITU-T M.3016.1] further detail the security requirements for security logging and audit.

8.1.4 Time stamping and time source

The NGN element is required to support the use of a trusted time source for both system clock and audit trail item stamping. A trusted time source in this case means a time source that can be verified to be resistant to unauthorized modification. Transitive trust is acceptable, i.e., a time source that relies on a trusted time source is itself an acceptable trusted time source.

8.1.5 Resource allocation and exception handling

Each NGN element is required to provide the capability to limit the amount of its own important resources (e.g., memory allocation) it allocates to servicing requests. Such limits can minimize negative effects of denial of service attacks. Resources used to service requests compete with other resource utilization requests on the system. In addition, each specific NGN application is required to have the ability to limit its own usage of important resources that it allocates for satisfying requests.

The purpose of this requirement is to limit the effect of bursts of activity so that they do not affect other service requests. This will also allow/leave the application (and OS) capability to signal monitoring systems that the application and/or its platform may be under DoS attack. The NGN element is required to provide an interface to monitor resource utilization.

The NGN element is required to silently discard any packets that do not conform to the expected protocol or format and, based on security policy, be capable of generating a log entry for each of these events. "Silent discard" is to trap and log the received packet, and discard the received packet while not responding with an indication of the discard (e.g., error response).

The purpose is to limit potential attacks from malicious or incorrect packets. Clearly, if the resource utilization of the logging operation is so large that it is interfering with other operations of the element, the obvious heuristic to apply is that logging will stop until resource utilization returns to an acceptable level.

NOTE – This is part of managing internal resources as mentioned above.

8.1.6 Code and system integrity and monitoring

The network element is required to be capable of monitoring 1) its configuration and software and 2) any changes to detect unauthorized changes, both based on the security policy. Any unauthorized changes are required to create a log entry and cause an alarm to be generated. Based on the security policy, the network element is required to do the following. The element is required to be capable of periodically scanning its resources and software for malicious software, e.g., a virus. The element is required to generate an alarm if malicious software is discovered during a scan.

Monitoring is required to be controlled so that it does not impact the performance of delay-sensitive real-time communications or unnecessarily cause connections to be torn down.

Clause 10.1.2.6.4 of [ITU-T M.3016.0] further details the security requirement for system integrity.

8.1.7 Patches, hotfixes and supplementary code

To trust signals generated by NGN provider NGN elements within un-trusted networks, say terminal. It is a requirement that software on the system is not compromised. This ensures that "Trojans[1]" (that phone home), "worms" (that generate useless traffic or turn systems into

[1] Many Trojan horses act as a remote-control software device for the hacker who sends them out. When they are safely installed on the target system, they initiate a connection back to the hacker to inform him/her that they are ready for use.

"zombies") and other viruses are not downloaded onto NGN elements or underlying OS. Such viruses would compromise system integrity, confidentiality and/or availability of data.

NGN provider network elements and systems are required to provide a capability to verify and audit all their software. The audit results are to be accessible to an OSS. This would allow for an analysis of the security posture of the NGN provider NGN infrastructure and provide guidance to administrators and providers with respect to where mitigation is necessary.

Security patches are to be obtained from the equipment vendors and installed in a timely fashion, once the NGN provider has certified them.

Clause I.5.2 of [ITU-T M.3016.1] provides further considerations on a patching process; while clause I.5.3.9 of [ITU-T M.3016.1] gives considerations on security assumptions of the operating system.

8.1.8 Access to OAMP functions in devices

In order to safeguard the OAMP infrastructure, each internal NGN network element is required to be managed through a separate IP address allocated from a separate address block. Each internal NGN network element should have a physically or logically separate interface for the exclusive use of this OAMP traffic. When a separate interface is used, the NGN network element is required to silently discard all packets received on the OAMP interface with source addresses other than the OAMP address. The NGN network element is required to silently discard all packets received over the non-OAMP interface with source addresses assigned to OAMP traffic.

Access to OAMP functions is required to be capable of being controlled by authentication. Once a user has authenticated to a system, the internal NGN element is required to track all changes that they make, and provide the opportunity to roll them back.

All security relevant use of authorization is required to be logged in the audit trail for a specified time. In particular, all access attempts, successful or not, to the element are required to be logged in the audit trail.

OAMP traffic is required to be securely protected. If OAMP traffic (including SNMP and NTP) travels over an un-trusted network, then it is required to be securely protected (e.g., IPsec or an MPLS, etc.).

8.2 Requirements for NGN elements in the trusted zone

The NGN Release 1 element in the "trusted" zone is to be assigned an IP address in the block reserved for internal NGN elements. All signalling is required to use this address. The NGN Release 1 element is also required to be assigned an IP address in the block reserved for OAMP, and all OAMPs are required to use this address.

In order to preserve the confidentiality and integrity of customer communication, signalling and media traffic is to be protected, either with transport encryption or assurance that the traffic only travels over a protected domain.

8.3 Requirements for NGN border elements in the "trusted-but-vulnerable" domain

Network border elements are the main defence against external attacks, i.e., attacks from devices/network elements in the un-trusted zone. All traffic from devices/network elements in the "un-trusted" zone is sent first to a network border element, where it is validated before it is transmitted to its destination in the "trusted" domain. The capabilities of providing physical/logical separation of networks are utilized to prohibit traffic from a device/network element in the un-trusted zone from reaching any element in the "trusted" domain.

Network border elements (NBE) are the main defence against signalling attacks. All signalling traffic from TE or TE-BE in un-trusted zone is processed at its assigned NBE, which retransmits the

signalling to the network equipments in the trusted zone. The capabilities of providing physical/logical separation of networks at the NBE are utilized to prohibit a TE/TE-BE in un-trusted zone from reaching any network element in trusted zone except its assigned NBE(s).

As with signalling, the network border elements (NBE) are also the main defence against media attacks. All media traffic from TE/TE-BE is processed at a NBE, and the NBE relays the media. NBE routes media packets, towards the destination and through the trusted domain, only if media packet can be associated with an authorized session in progress. Media packets that are not associated with a session request are not valid, have no place to go and are discarded. Furthermore, the NBE verifies the source of the media stream, and verifies the packet rate is consistent with the session established. The media is transferred within the NGN provider facilities to either a PSTN gateway (for a PSTN connection) or to another NBE. At the second NBE, the media is processed and retransmitted to a TE destination.

NOTE – The term "session" is used to mean any type of media flow, independent of the convention used to establish the session.

The network border element is required to support multiple IP addresses, or multiple network interfaces. One IP address (the "internal" address) is to be assigned from the block reserved for internal NGN Release 1 elements. All signalling and media to and from other internal NGN Release 1 elements is required to use this address (or this interface). One IP address (the "external" address) is to be assigned; it is to be accessible from the TE equipment. All signalling and media to and from the TE is required to use this address (or this interface). One IP address (the "OAMP address") is required to be assigned from the block reserved for OAMP, which is accessible from the OAMP servers.

In order to preserve the confidentiality of customer communication against eavesdropping on the signalling traffic, the signalling transport of all signalling messages is required to be secured to NGN elements in the "trusted" or "trusted-but-vulnerable" zones. All connections initiated by a NBE used for transfer of signalling information to such NGN elements is to be established using secure channels with authentication. All signalling messages received by a NBE at its "internal" NGN address over un-secure channels are to be silently discarded.

Media streams are to be protected either with transport encryption or assurance that the traffic only travels over a protected network. In addition, source address assurance at the edge of the network will guarantee that packets from outside will not claim to be from the internal NGN address block.

Media packets received by the NBE at its external address are to be checked for an active session (based on the signalling exchange), and against the expected source address (based on the session description contained in the signalling exchange). The NBE is required to silently discard any media packets received that do not correspond to an active session. The NBE is also required to verify that the packet rate is consistent with the negotiated session parameters. The NBE may verify the packet size is consistent with the session established. Media packets received from a source IP address that is not a valid originator of media to this NBE are to be silently discarded.

The NBE is required to authenticate all requests if required by the service agreement with the customer. When a request is received over a non-encrypted connection, each individual request is to be authenticated. When a request is received over an encrypted connection that was created without a client authentication, the first request over that connection is to be authenticated. When a request is received over an encrypted connection that was created with authentication, no further authentication is required. Note that requests that are sent through a TE-BE will not be challenged for device authentication, since the TE-BE will be using an encrypted connection to the NBE. If the request comes from a source IP address that is not a valid originator of requests to this NBE, it is to be silently discarded. Requests for secure channel from a source IP address that is not a valid originator of requests to this NBE are also to be silently discarded.

8.4 Requirements for TE border elements in the "un-trusted" domain

Physical security is a challenge for equipment placed on customer site. Ultimately, it must be accepted that, to a large extent, the security of these devices is dependent on the customer. That said, each device is required to provide reasonable precautions against being attacked, compromised or otherwise tampered with. In order to preserve the confidentiality of customer communication against eavesdropping on the signalling traffic, signalling messages are required to use a secure signalling connection between the TE-BE and the NBE. The TE-BE may perform a media-relay function.

8.4.1 OAMP functions

All OAMP functions between TE-BE and the NGN provider are required to be protected against determined eavesdropping. Since OAMP can be provided both in-band and out-of-band, these are dealt with separately.

8.5 Security recommendations for terminal equipment in the "un-trusted" domain

The terminal equipment (TE) is often outside the control of the NGN provider. Therefore it is not required for the NGN provider to place requirements on its security features or policies, rather it is the function of the various network border elements to adapt to whatever policies are chosen by the customer and to provide the best service under those conditions.

The actual security functionalities of the NGN provider border elements are for further study.

Media traffic should be protected from eavesdropping or modification.

Appendix I

Security objectives and guidelines for interconnection of emergency telecommunications services

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

I.1 Background

Emergency telecommunications service (ETS) is a national service, providing priority telecommunications services to ETS authorized users in times of disaster and emergencies. ETS implementation is a national matter. However, disasters/emergencies can transcend geographic boundaries, and thus there is a potential that countries/administrations may enter into bilateral and/or multilateral agreements to link their respective ETS systems. This would allow priority telecommunications services (e.g., voice, messaging, video and data) under the umbrella of ETS to be supported between different national networks with bilateral and/or multilateral agreements in times of disaster and emergencies.

ETS telecommunications services between different national networks (i.e., countries/administrations) need to be protected against security threats. To allow network provided security of end-to-end ETS telecommunications services between different national networks (i.e., countries/administrations) implementation of ETS, guidance and common security objectives and requirements are needed. Security and availability of ETS telecommunications services will depend on the security of each network involved in an end-to-end communication.

I.2 Scope/purpose

This appendix provides common security objectives and requirements, and provides guidance to allow support of network provided security for ETS telecommunications services across different national networks (i.e., countries/administrations) implementations of ETS.

End-user peer-to-peer security function using special end-user equipment security functions is not included in the scope of this appendix. The scope of this appendix is limited to network provided security for ETS telecommunications services across multiple networks on a hop-by-hop basis. However, the NGN should be capable of transparently supporting such peer-to-peer functions.

This appendix is not intended to impose conditions on national implementations of ETS. Its primary purpose is to allow network provided security for ETS telecommunications services (i.e., secure priority voice, video, data and messaging communications).

I.3 General objectives

The general objective is for networks to be capable of providing security of ETS telecommunications services (e.g., secure priority voice, video, data, and messaging communications) across different national networks (i.e., countries/administrations) and protecting availability of ETS. This would involve security of the end-to-end communication that may traverse different network provider domains of national and international networks (i.e., countries/administrations) where each network is responsible for security within its domain.

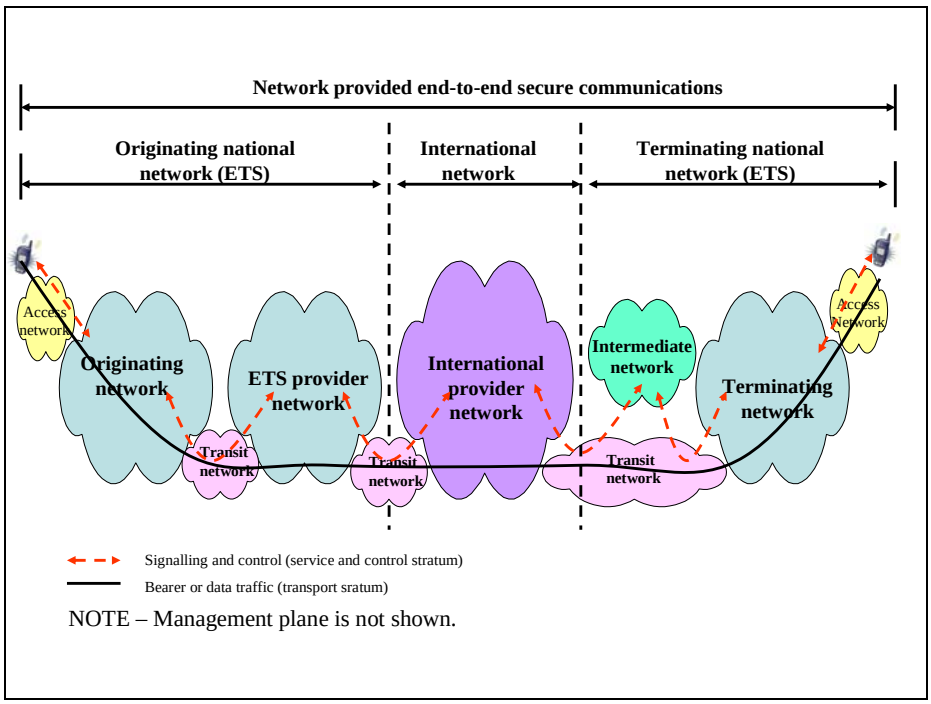

Figure I.1 – Example of end-to-end communication across different national ETS implementations

Figure I.1 illustrates end-to-end ETS telecommunications services (e.g., priority voice, video, data or messaging communication) between two different national networks. The example illustrates that the end-to-end priority communication for ETS may involve multiple network segments and administrative domains (e.g., access network, originating network, ETS provider network, international provider network, intermediate network and terminating network).

Each network segment will have specific security responsibilities within its domain to facilitate end-to-end security and availability of ETS telecommunications services.

The following is a minimal set of general guidelines and security planning to protect signalling, bearer and data, and management-related data and information (e.g., user profile information) for ETS:

- Each network domain should establish and enforce security policies and implement mitigation capabilities for ETS within its domain. Specifically, it is recommended that mitigation capabilities and security practices beyond those needed for general application services should be identified and enforced for ETS priority communications. For example, these capabilities and practices should be designed to prevent use of ETS resources by unauthorized users, and to prevent denial of service and other types of attacks.
- Each network domain should establish trust relations, methods and procedures for identifying ETS telecommunications services, and for identity management and authentication of end-users and networks across multiple network administration domains. For example, service level agreements (SLAs) should establish security policy for authenticating each domain when handing off and receiving ETS telecommunications services.
- Each network administrative domain should establish and enforce security policies to protect ETS management-related data and information (e.g., user profile information).

I.4 General security capabilities

It is recommended that the following be supported for ETS:

- Security capabilities to protect end-to-end ETS telecommunications services across multiple network domains.
- Security capabilities to protect availability of ETS telecommunications services across multiple network domains.
- Security capabilities to provide identity management and authentication of end-users and networks across multiple network administration domains. It is highly desirable that the end-user interact with the ETS service only once and that the security mechanisms pass the end-user's credentials from administrative domain to domain.

I.5 Authentication, authorization and access control

It is recommended that the following minimum set of authentication, authorization and access control capabilities be supported for ETS:

- Security capabilities to protect mechanisms used to authenticate and authorize ETS end-users and devices.
- Security capabilities to protect mechanisms used to bind ETS end-user with associated devices.
- Security capabilities to protect mechanisms used to share authentication information (e.g., confirm that an end-user has been authenticated) across multiple network domains.
- Security capabilities to protect mechanisms used for bilateral authentication of end-user and entities. This includes mechanisms for an ETS end-user to authenticate the called party or communicating entities (e.g., website, content server, etc.).
- Security capabilities to protect mechanisms used by one network to authenticate another network. This includes mechanisms used to authenticate the network handing off an ETS telecommunications services (e.g., originating network) and to authenticate the network receiving the ETS telecommunications services (e.g., intermediate or terminating networks).
- Security capabilities to protect against unauthorized access to ETS information and resources (e.g., user information in authentication servers and management systems).

I.6 Confidentiality and privacy

It is recommended that the following minimum set of confidential capabilities be supported:

- Security capabilities to provide confidentiality protection of ETS signalling and control.
- Security capabilities to provide confidentiality protection of ETS bearer and data traffic (e.g., voice, video or data).
- Security capabilities to provide confidentiality protection of ETS end-user and communicating entities identities and subscription information.
- Security capabilities to provide confidentiality protection of ETS end-user location.

It is recommended that the following minimum set of privacy capabilities be supported:

- Security capabilities to provide privacy protection of ETS information (e.g., information derived from the observation of network activities such as web-sites that an end-user has visited, a end-user's geographic location, and the IP addresses and DNS names of devices in a service provider network).

- Security capabilities to provide privacy protection against unauthorized observation of ETS usage information (e.g., usage patters such as ETS traffic volume, locations, time, frequency, etc.).

I.7 Data integrity

It is recommended that the following minimum set of data integrity capabilities be supported:

- Security mechanisms to provide integrity protection of ETS telecommunications services (e.g., protection against unauthorized modification, deletion, creation, or replay). This includes mechanisms to provide notification of information tampering or modification.
- Security mechanisms to provide integrity protection of ETS information (e.g., priority marking, voice, data and video).
- Security mechanisms to provide integrity protection of ETS specific configuration data (e.g., priority information stored in policy decision functions, user priority level, etc.).

I.8 Communication

It is recommended that the following minimum capability be supported:

- Security mechanisms to protect ETS telecommunications services from an authorized ETS end-user against intrusions (e.g., mechanisms to prevent unlawful interception, hijacking or replay of ETS signalling or bearer/data traffic).

I.9 Availability

It is recommended that the following minimum set of capabilities be supported:

- Security mechanisms to protect the availability of ETS telecommunications services (e.g., protection of ETS signalling and control, and bearer/data traffic against denial of service (DoS) and other forms of attacks).
- Security mechanisms to protect the availability of ETS specific resources and information (e.g., authentication/authorization databases, priority information stored in policy decision function, and dedicated network resources against denial of service (DoS) and other forms of attacks).

Bibliography

ITU-T Recommendations

[b-ITU-T E.106] ITU-T Recommendation E.106 (2003), *International Emergency Preference Scheme (IEPS) for disaster relief operations*.

[b-ITU-T E.107] ITU-T Recommendation E.107 (2007), *Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS.*

[b-ITU-T E.115] ITU-T Recommendation E.115 (2007), *Computerized directory assistance*.

[b-ITU-T M.3016.2] ITU-T Recommendation M.3016.2 (2005), *Security for the management plane: Security services*.

[b-ITU-T M.3016.3] ITU-T Recommendation M.3016.3 (2005), *Security for the management plane: Security mechanism*.

[b-ITU-T M.3016.4] ITU-T Recommendation M.3016.4 (2005), *Security for the management plane: Profile proforma*.

[b-ITU-T M.3060] ITU-T Recommendation M.3060/Y.2401 (2006), *Principles for the management of Next Generation Networks*.

[b-ITU-T X.1121] ITU-T Recommendation X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

[b-ITU-T X.1122] ITU-T Recommendation X.1122 (2004), *Guideline for implementing secure mobile systems based on PKI.*

[b-ITU-T Y.1271] ITU-T Recommendation Y.1271 (2004), *Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks.*

[b-ITU-T Y.2000-Sup.1] ITU-T Y.2000-series Recommendations – Supplement 1 (2006), *NGN release 1 scope.*

[b-ITU-T Y.2111] ITU-T Recommendation Y.2111 (2006), *Resource and admission control functions in Next Generation Networks.*

ETSI TISPAN documents

[b-ETSI TR 187.002] ETSI TR 187 002 V.1.1.1 (2006), *Telecommunications and Internet converged services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat and Risk Analysis.*

[b-ETSI TS 187.001] ETSI TS 187 001 V.1.1.1 (2006), *Telecommunications and Internet converged services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements.*

[b-ETSI TS 187.003] ETSI TS 187 003 V.1.1.1 (2006), *Telecommunications and Internet converged services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture.*

ETSI/3GPP documents

[b-3GPP TS 33.102] 3GPP TS 33.102 (2007), *3G security; Security architecture*.

[b-3GPP TS 33.103] 3GPP TS 33.103 (2001), *3G security; Integration guidelines*.

[b-3GPP TS 33.110] 3GPP TS 33.110 (2007), *Key establishment between a UICC and a terminal*.

[b-3GPP TS 33.120] 3GPP TS 33.120 (2001), *Security Objectives and Principles*.

[b-3GPP TS 33.200] 3GPP TS 33.200 (2004), *3G security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security*.

[b-3GPP TS 33.203] 3GPP TS 33.203 (2007), *3G security; Access security for IP-based services*.

[b-3GPP TS 33.204] 3GPP TS 33.204 (2007), *3G security; Network Domain Security (NDS); TCAP user security*.

[b-3GPP TS 33.210] 3GPP TS 33.210 (2007), *3G security; Network Domain Security; IP network layer security*.

[b-3GPP TS 33.220] 3GPP TS 33.220 (2007), *Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.

[b-3GPP TS 33.310] 3GPP TS 33.310 (2007), *Network Domain Security (DNS; Authentication Framework (AF)*.

[b-3GPP TR 33.901] 3GPP TR 33.901 (2001), *Criteria for cryptographic algorithm design process*.

[b-3GPP TR 33.902] 3GPP TR 33.902 (2001), *Formal Analysis of the 3G Authentication Protocol*.

[b-3GPP TR 33.908] 3GPP TR 33.908 (2001), *3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms*.

[b-3GPP TR 33.909] 3GPP TR 33.909 (2001), *3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions*.

[b-3GPP TR 33.918] 3GPP TR 33.918 (2007), *Generic Authentication Architecture (GAA); Early implementation of Hypertext Transfer Protocol over Transport Layer Security (HTTPS) connection between a Universal Integrated Circuit Card (UICC) and a Network Application Function (NAF)*.

[b-3GPP TR 33.919] 3GPP TR 33.919 (2007), *3G Security; Generic Authentication Architecture (GAA); System description*.

[b-3GPP TR 33.920] 3GPP TR 33.920 (2007), *SIM card based Generic Bootstrapping Architecture (GBA); Early implementation feature*.

[b-3GPP TR 33.980] 3GPP TR 33.980 (2007), *Liberty Alliance and 3GPP security interworking; Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA)*.

[b-ETSI TR 133.901] ETSI TR 133.901 V4.0.0 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security – Criteria for cryptographic Algorithm design process*.

[b-ETSI TR 133.902] ETSI TR 133.902 V4.0.0 (2001), *Universal Mobile Telecommunications System (UMTS); Formal Analysis of the 3G Authentication Protocol*.

[b-ETSI TR 133.908] ETSI TR 133.908 (2001), *Universal Mobile Telecommunications System (UMTS); Security Algorithms Group of Experts (SAGE); General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms*.

[b-ETSI TR 133.909] ETSI TR 133.909 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions*.

[b-ETSI TR 133.919] ETSI TR 133.919 V6.2.0 (2005), *Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); System description*.

[b-ETSI TS 133.102] ETSI TS 133 102 V7.1.0 (2006), *Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture*.

[b-ETSI TS 133.103] ETSI TS 133 103 V4.2.0 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Integration Guidelines*.

[b-ETSI TS 133.120] ETSI TS 133 120 V4.0.0 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Security Principles and Objectives*.

[b-ETSI TS 133.200] ETSI TS 133 200 V6.1.0 (2005), *Universal Mobile Telecommunications System (UMTS); 3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security*.

[b-ETSI TS 133.203] ETSI TS 133 203 V6.10.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services*.

[b-ETSI TS 133.210] ETSI TS 133 210 V7.2.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS)*.

[b-GPP TS 133.220] ETSI TS 133 220 V7.8.0 (2007), *Digital cellular telecommunications system; (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.

[b-ETSI TS 133.310] ETSI TS 133 310 V7.1.0 (2006), *Universal Mobile Telecommunications System (UMTS); Network domain security; Authentication framework (NDS/AF)*.

ATIS/3GPP2 documents

[b-GPP2 S.S0086] 3GPP2 S.S0086 (2004), *IMS Security Framework*.

IPsec related IETF RFCs

[b-IETF RFC 2085] IETF RFC 2085 (1997), *HMAC-MD5 IP Authentication with Replay Prevention*.

[b-IETF RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*.

[b-IETF RFC 2404] IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and AH*.

[b-IETF RFC 2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm With Explicit IV*.

[b-IETF RFC 2410] IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use With IPsec*.

[b-IETF RFC 2411] IETF RFC 2411 (1998), *IP Security Document Roadmap*.

[b-IETF RFC 2451] IETF RFC 2451 (1998), *ESP CBC-Mode Cipher Algorithms*.

[b-IETF RFC 2709] IETF RFC 2709 (1999), *Security Model with Tunnel-mode IPsec for NAT Domains*.

[b-IETF RFC 2857] IETF RFC 2857 (2000), *The Use of HMAC-RIPEMD-160-96 within ESP and AH*.

[b-IETF RFC 3526] IETF RFC 3526 (2003), *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*.

[b-IETF RFC 3602] IETF RFC 3602 (2003), *The AES-CBC Cipher Algorithm and Its Use with IPsec*.

[b-IETF RFC 3664] IETF RFC 3664 (2004), *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*.

[b-IETF RFC 4109] IETF RFC 4109 (2005), *Algorithms for Internet Key Exchange version 1 (IKEv1)*.

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*.

[b-IETF RFC 4302] IETF RFC 4302 (2005), *IP Authentication Header*.

[b-IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP)*.

[b-IETF RFC 4304] IETF RFC 4304 (2005), *Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)*.

[b-IETF RFC 4305] IETF RFC 4305 (2005), *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*.

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol*.

[b-IETF RFC 4307] IETF RFC 4307 (2005), *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*.

[b-IETF RFC 4308] IETF RFC 4308 (2005), *Cryptographic Suites for IPsec*.

[b-IETF RFC 4309] IETF RFC 4309 (2005), *Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)*.

[b-IETF RFC 4312] IETF RFC 4312 (2005), *The Camellia Cipher Algorithm and Its Use With IPsec*.

S/MIME related IETF RFCs

[b-IETF RFC 2311] IETF RFC 2311 (1998), *S/MIME Version 2 Message Specification*.

[b-IETF RFC 2312] IETF RFC 2312 (1998), *S/MIME Version 2 Certificate Handling*.

[b-IETF RFC 3565] IETF RFC 3565 (2003), *Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)*.

[b-IETF RFC 3657] IETF RFC 3657 (2004), *Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS)*.

[b-IETF RFC 3850] IETF RFC 3850 (2004), *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling*.

[b-IETF RFC 3851] IETF RFC 3851 (2004), *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*.

[b-IETF RFC 3852] IETF RFC 3852 (2004), *Cryptographic Message Syntax*.

[b-IETFB RFC 4134] IETF RFC 4134 (2005), *Examples of S/MIME Messages*.

TLS related IETF RFCs

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[b-IETF RFC 2817] IETF RFC 2817 (2000), *Upgrading to TLS Within HTTP/1.1*.

[b-IETF RFC 2818] IETF RFC 2818 (2000), *HTTP Over TLS*.

[b-IETF RFC 3268] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*.

[b-IETF RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.

[b-IETF RFC 4132] IETF RFC 4132 (2005), *Addition of Camellia Cipher Suites to Transport Layer Security (TLS)*.

Miscellaneous IETF security related RFC

[b-IETF i-d.SIPUAP] IETF internet-draft work in progress, draft-ietf-sipping-config-framework-08.txt (March 6, 2006), *A Framework for Session Initiation Protocol User Agent Profile Delivery*.

[b-IETF RFC 3489] IETF RFC 3489 (2003), *STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*.

[b-IETF RFC 3711] IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP)*.

[b-IETF RFC 3715] IETF RFC 3715 (2004), *IPsec-Network Address Translation (NAT) Compatibility Requirements*.

[b-IETF RFC 3847] IETF RFC 3847 (2004), *Restart Signaling for Intermediate System to Intermediate System (IS-IS)*.

[b-IETF RFC 3948] IETF RFC 3948 (2005), *UDP Encapsulation of IPsec ESP Packets*.

DNS related IETF RFCs

[b-IETF RFC 4033] IETF RFC 4033 (2005), *DNS Security Introduction and Requirements*.

[b-IETF RFC 4034] IETF RFC 4034 (2005), *Resource Records for the DNS Security Extensions*.

[b-IETF RFC 4035] IETF RFC 4035 (2005), *Protocol Modifications for the DNS Security Extensions*.

TIA documents

[b-TIA-683-D] TIA Standard TIA-683-D (2006), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*.

[b-TIA-1053] TIA Standard TIA-1053 (2005), *Broadcast/Multicast Security Framework*.

[b-TIA-1091] TIA Standard TIA-1091 (2006), *IMS Security Framework*.

ARIB documents

[b-ARIB-SS0078] ARIB STD-T64 S.S0078-0 v1.0 (2002), *Common Security Algorithms*.

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, 2008