ATIS-1000029.2008(R2013)

Security Requirements for NGN

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

As a leading technology and solutions development organization, ATIS brings together the top global ICT companies to advance the industry's most-pressing business priorities. Through ATIS committees and forums, nearly 200 companies address cloud services, device solutions, emergency services, M2M communications, cyber security, ehealth, network evolution, quality of service, billing support, operations, and more. These priorities follow a fast-track development lifecycle – from design and innovation through solutions that include standards, specifications, requirements, business use cases, software toolkits, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of oneM2M, a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications sectors, and a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit < www.atis.org >.

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-1000029.2008(R2013), *Security Requirements for NGN*

Is an American National Standard developed by the **Signaling, Architecture, and Control (SAC)** Subcommittee under the **ATIS Packet Technologies and Systems Committee (PTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

(R2013)

ATIS-1000029.2008

American National Standard for Telecommunications

Security Requirements for NGN

Alliance for Telecommunications Industry Solutions

Approved November 20,2008

American National Standards Institute, Inc.

Abstract

This standard provides security requirements for the Next Generation Network (NGN) against security threats, and to mitigate the effects of security attacks. This standard is aligned with ITU Y.2701, Security Requirements for NGN Release 1.

Foreword

This standard provides security requirements for the Next Generation Network (NGN) and its interfaces (e.g., UNIs, NNIs and ANIs). NGN architectural descriptions can be found in ATIS-1000018, *NGN Architecture* [1] and ITU-T Recommendation Y.2012 [8], *Functional requirements and architecture of the NGN*.

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 standard.

This standard uses trust model based on network elements (physical boxes). NGN providers will be deploying network elements that support the functional entities defined in ATIS-1000018 [1] and ITU-T Recommendation Y.2012 [8]. The bundling of these functional entities to a given network element will vary, depending on the vendor. Therefore, this standard will not attempt to show a strict and fixed bundling between logical functional entities and physical network elements.

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

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, PTSC, which was responsible for its development, had the following roster:

J. Zebarth, PTSC Chair (Nortel)

M. Dolly, PTSC Vice-Chair (AT&T)

R. Singh, Technical Editor (Telcordia)

M. Dolly, Technical Editor (AT&T)

C. Underkoffler, ATIS Chief Editor

The Signalling, Architecture, and Control (SAC) Subcommittee was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

American National Standard for Telecommunications –

Security Requirements for NGN

1 Scope

This standard provides security requirements for the Next Generation Network (NGN) against security threats, and to mitigate the effects of security attacks. This standard is aligned with ITU Y.2701, Security Requirements for 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., signaling, 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).

Adherence to these requirements will 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 standard.

The requirements specified in this standard 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 providers will be deploying “network elements” that support the functional entities described in ATIS-1000018 [1] and ITU-T Recommendation Y.2012 [8]. The bundling of these functional entities to a given network element will vary, depending on the vendor. Therefore, this standard will not attempt to show a strict and fixed bundling of logical functional entities and physical network elements.

The requirements in this standard 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 this standard.

In addition, the requirements in this document cover some of the technical aspects of what is generally known as “Identity Management (IdM).” 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 the identity of a person.

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

Note: In this document, use of the term “NGN provider” includes all types of providers in an NGN environment such as service providers, network providers, access providers and transport providers.

1.1 General security principles

ITU-T Recommendation X.805, *Security architecture for systems providing end-to-end Communications* [6] and ATIS-1000007, *Generic Signaling and Control Plane Security for Evolving Networks* [1] defines the following security dimensions.

- Access control
- Authentication
- Non-repudiation
- Data confidentiality
- Communication security
- Data integrity
- Availability
- Privacy

It also identifies the security threats shown in Figure 1.

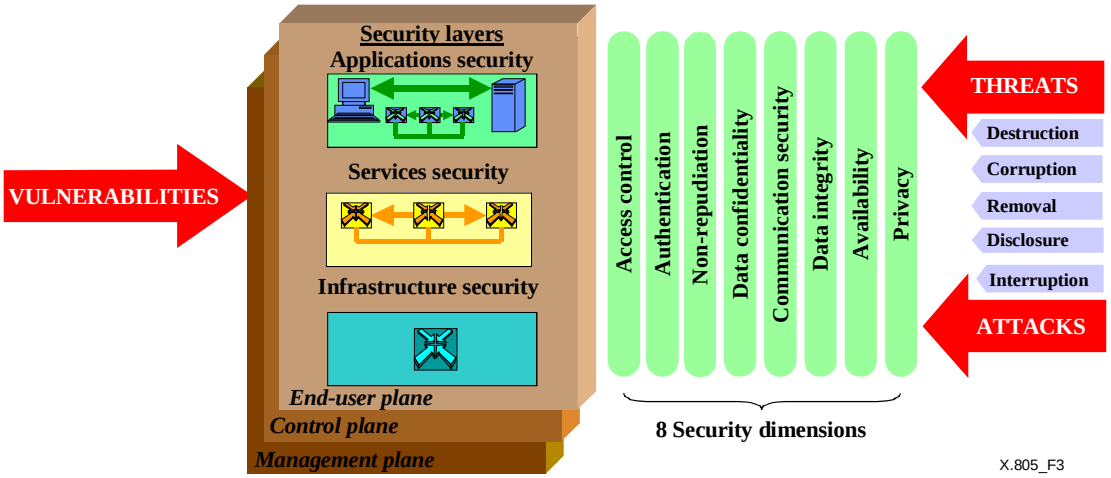

Figure 1 – Security architecture of X.805 (Figure 3/X.805)

These security dimensions and security threats stated above are considered as the basis of this standard.

This standard 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 standard 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.

1.2 Assumptions

This standard is based on the following assumptions:

1. The bundling of functional entities defined in ATIS-1000018 [1] and ITU-T Recommendation Y.2012 [8] to a given network element will vary, depending on the vendor.
2. Each NGN provider has specific responsibilities within its domain for security. Examples include implementing applicable security services and practices to a) to protect itself, b) to assure end-to-end security is not compromised within its network, and c) to 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 its 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 (signaling/control traffic, bearer traffic and management traffic) across UNIs, ANIs and NNIs. Policy enforcement is outside the scope of this document.
4. This standard addresses network-based security, for a layered architecture, consisting of perimeter security to trusted domains, physical security of provider equipment, and the potential use of encryption.

1.3 Document overview

This standard is organized as follows:

- Clause 2 (References) – This section 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 ATIS-100018 [1] and ITU-T Recommendation Y.2012 [8] 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 to meet the objectives given in clause 7.
- Bibliography

This standard is defined to provide a basis for NGN security. Various companion standards 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 standards contain provisions which, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the edition indicated was valid. All standards are subject to revision, and the parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent edition of the standard indicated below.

[1] ATIS-1000018, *NGN Architecture.*[1]

[2] ATIS-1000007.2006(R2011), *Generic Signaling and Control Plane Security for Evolving Networks.*[1]

[3] ATIS-1000010.2006(R2011), *Security for Next Generation Networks - An End User.*[1]

[4] ITU-T Recommendation Y.2701, *Security Requirements for NGN Release 1.*[2]

[5] ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*[2]

[6] ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end Communications.*[2]

[7] ITU-T Recommendation Y.2201, *NGN release 1 requirements*.[2]

[8] ITU-T Recommendation Y.2012, *Functional requirements and architecture of the NGN*.[2]

[9] ITU-T Recommendation M.3016.0 (2005), Security for the management plane: Overview.[2]

[10] ITU-T Recommendation M.3016.1 (2005), *Security for the management plane: Security requirements*.[2]

[11] ATIS-0300276.2008,*Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Security Requirements for the Management Plane*. [1]

[12] ATIS-1000019.2007, *Network to Network (NNI) Standard for Signaling and Control Security for Evolving VoP Multimedia Networks*.[1]

[13] ATIS--1000012.2006(R2011), *Signaling Systems No. & (SS7) - SS7 - Network and NNI Interconnection Security Requirements and Guidelines*. [1]

---

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

[2] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

3 Definitions and abbreviations

3.1 Definitions

This standard defines the following terms.

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

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

Corporate Network: Private network that supports multiple users and may be in multiple locations (e.g, an enterprise, a campus).

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

Emergency telecommunications service (ETS): National service, providing authorized priority communications to facilitate the work of emergency personnel in times of disaster. [from ITU-T Recommendation E.107]

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

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

Security domain: 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.

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.

Trusted but vulnerable zone: From the viewpoint of a NGN provider a security zone where the network elements and systems are operated (provisioned and maintained) by the NGN provider. The equipment may be under the control of 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 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 network elements and systems in the trusted zone from the security attacks originated in the un-trusted zone.

Trusted zone: (From the viewpoint of a NGN provider) a security zone consisting of a NGN provider's network elements and systems that 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.

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.

Security zone: A domain defined by operational control, location, and connectivity to other network elements and systems. A security zone is either, (1) trusted, (2) trusted but vulnerable, or (3) un-trusted. A security zone is defined by operational control, location, and connectivity to other device/network elements.

User: An user [Y.2091], person, subscriber, system, equipment, terminal (e.g. FAX, PC), (functional) entity, process, application, provider, or corporate network.

User Network: A private network consisting of terminal equipment that may have multiple users.

3.2 Abbreviations and acronyms

This standard uses the following abbreviations and acronyms.

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
OS	Operating Systems

OSS	Operations Support System
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
3G	3rd Generation

4 Security threats and risks

This standard assumes that the systems, components, interfaces, information, resources, communications (i.e., signaling, 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 detected by 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;
- 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 premise 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

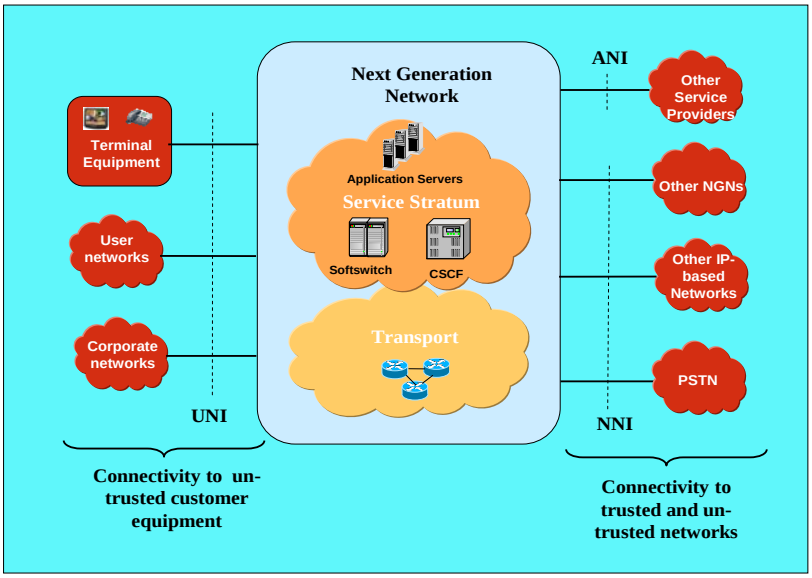

Figure 2 - Connectivity to networks and users

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 via 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 sub-clause defines three security zones;

1. Trusted,
2. Trusted but vulnerable,
3. Un-trusted,

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

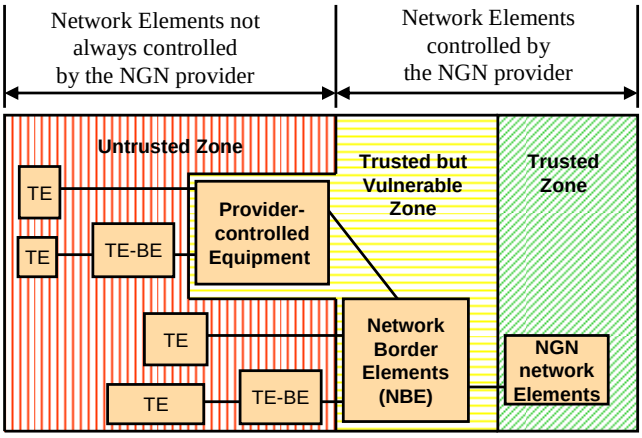

Figure 3 - Security trust model

An “internally 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 signaling, 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), which provide the User-Network Interface 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 on the border between 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.
- Operations, Administration, Maintenance, and Provisioning NBE(OAMP-NBE) that 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 to provide the user/subscriber access to web based services.

.

Examples of devices and systems 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 (and, therefore, may or may not be part of the trusted zone), are:

- Outside plant equipment in the access network/technology;
- Base Station Router (BSR), a wireless network element that integrates the base station, radio network controller and router functionalities;[3]
- Optical Units (ONUs) within a user/subscriber's residence.

The "trusted-but-vulnerable" zone will be protected by a combination of methods. Some examples are physical security of the NGN network elements, general hardening of the systems, , use of secure signaling for all signaling 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 and systems of a customer network, peer network, or other NGN provider security zone outside of the related NGN provider domain. These are connected to the NGN provider's border elements.. The elements in the "un-trusted zone" may not be under the control of the NGN providers and it is effectively impossible to enforce the provider's security policy on the user. Still it is desirable to apply some security measures, and to that end, it is recommended that signaling, media, and OAM&P be secured and that the Terminal Equipment Border Element (TE-BE) located in the "un-trusted zone", is hardened. However, due to the lack of

[3] This is not CPE.

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, whether the other network is trusted depends on:

- Physical interconnection, where the interconnection can range from a direct connection in a secure building to via shared facilities;
- The peering model, whether the traffic is exchanged directly between the two NGN service providers, or via one or more untrusted 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. The relationship shall specify contractual terms stating the obligations each party to the contract agrees to and should also specify any specific security mechanisms, information and procedures also agreed to by the parties.

In general, NGN providers should view other providers as un-trusted.

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

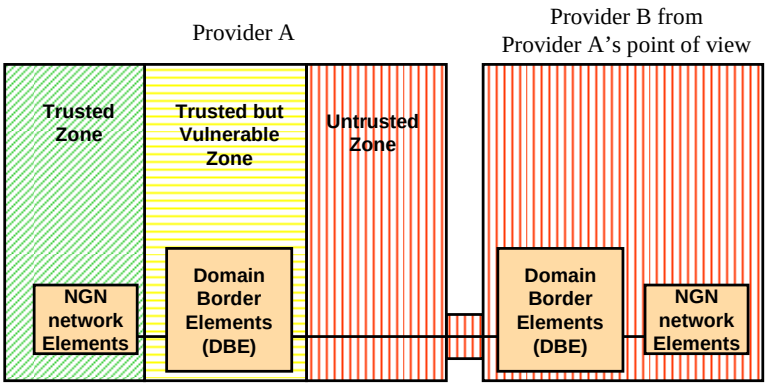

Figure 4 – Peering trust model

6 Security architecture

6.1 Functional NGN architecture reference

Figure 5 shows a functional view of the NGN architecture defined in ATIS-100018 [1] and ITU-T Recommendation Y.2012 [8].

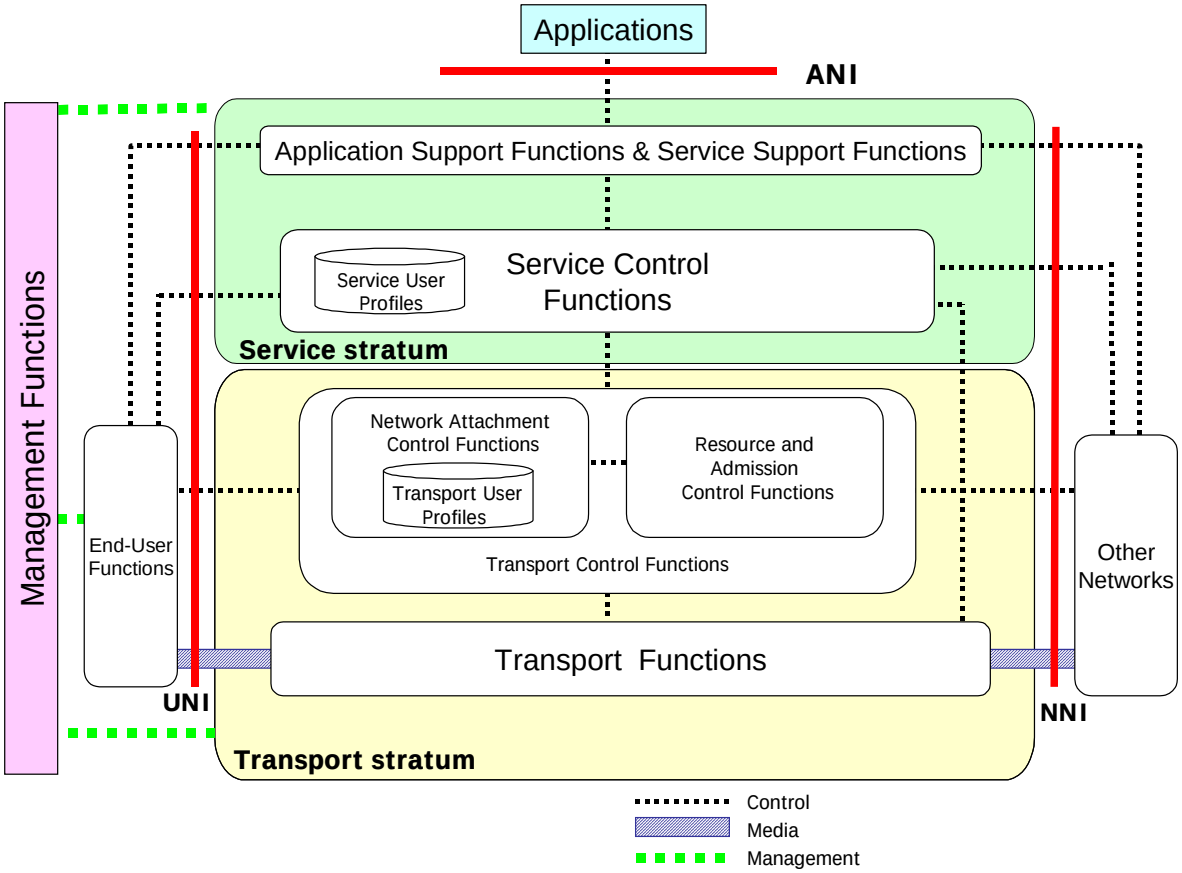

Figure 5 - NGN architecture overview (Figure 1/ATIS-100018 and Figure 1 of ITU-T Y.2012)

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

The NGN 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 ATIS-1000018 [1] and ITU-T Recommendation Y.2012 [8].

6.2 Mapping to NGN functional architecture

This standard describes the method to achieve security by using the trust model shown in clause 5, that is, an NGN composed of a trusted domain, un-trusted domain, and trusted but vulnerable domain in between as shown in Figure 3 and Figure 4. Each NGN provider should use the abstract trust models to plan and implement its security strategy to protect its own assets. One of the key challenges to achieve security with this model is selecting an appropriate method to transmit signaling, media, and 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., B2B-UA for SIP signaling) between the "trusted" zone and the "untrusted" zone. It receives a packet from the "untrusted" zone, examines it, discards it if it is inappropriate, and if it is appropriate copies the necessary part to construct a packet appropriate for the "trusted" zone. In this case, these BNEs traffic becomes part of the "trusted but vulnerable" zone.

(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 "trusted" zone. In this case NEs that control traffic become the "trusted but vulnerable" zone NEs.

(c) End-to-end encryption between the sender and the receiver, assuming that the sender is trusted by the receiver.

In the functional architecture shown in ATIS-1000018 [1] (Figure 6 of this standard), SIP signaling 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 the P-CSCF-FE. NEs that contain P-CSCF-FE therefore can be considered as NEs in the "trusted but vulnerable" zone, or as NEs in the "trusted zone" depending on the firewall functions between the end-user function and the P-CSCF-FE. NEs that contain only the S-CSCF-FE, and which are therefore separated from NEs that contains the P-CSCF-FE, they can be considered as NEs in the "trusted zone."

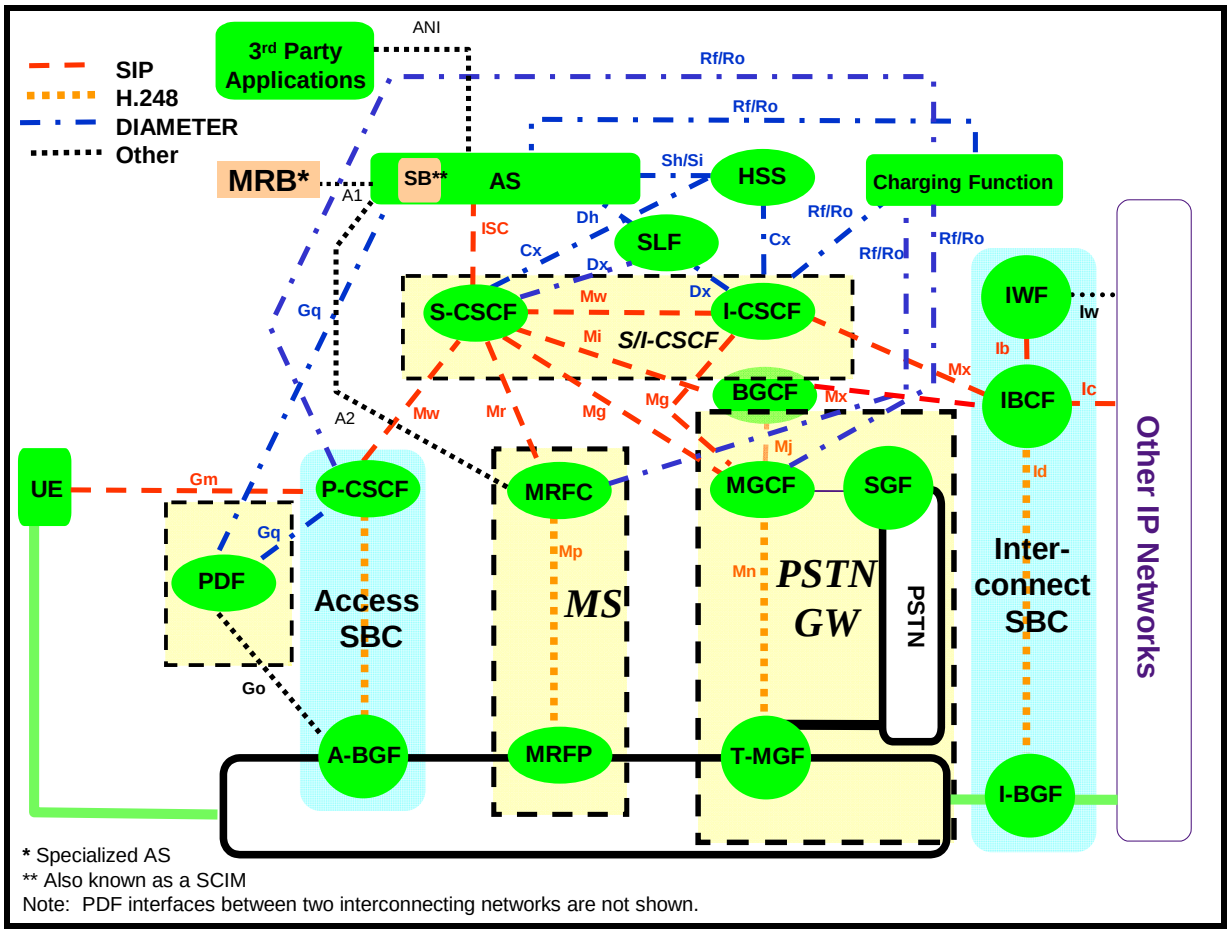

Figure 6 - ATIS NGN functional architecture (Figure 2/ATIS-1000018)

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, signaling, management and media/bearer communications. In identifying NGN resources for security protection against threats, the theoretical layered architecture defined in ATIS-1000018 [1] and ITU-T Recommendation Y.2012 [8] is to be considered together with the 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 1-4 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	(d) Protect against corruption or modification of information. (e) Protect against theft, removal or loss (e.g., identity theft). (f) 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 signaling 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 signaling).

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.

Examples	Goals and objectives
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) signaling and management within a provider network (c) Provide security of signaling 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) Providing security protection of transport control signaling (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	(a) Provide security protection of inter-system signaling (e.g. SIP, RADIUS, Diameter) within an a network provider network (e.g., CSCF to HSS signaling)
	Interfaces and communications	(a) Provide security protection of signaling and management across UNI, NNI and ANI 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 signaling 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 an 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

Example	Goals and objectives
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 standard.

- 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 the NGN into account.
- Security methods should be based on existing and well-understood security standards where these are available.
- 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 signaling 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 to a domain.
- The principles and general security objectives for secure TMN management as outlined in T1.276 *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane* [11] and ITU-T Recommendation M.3016.0 [9] (clause 7) should be followed.

7.2 Objectives for security across multiple network provider domains

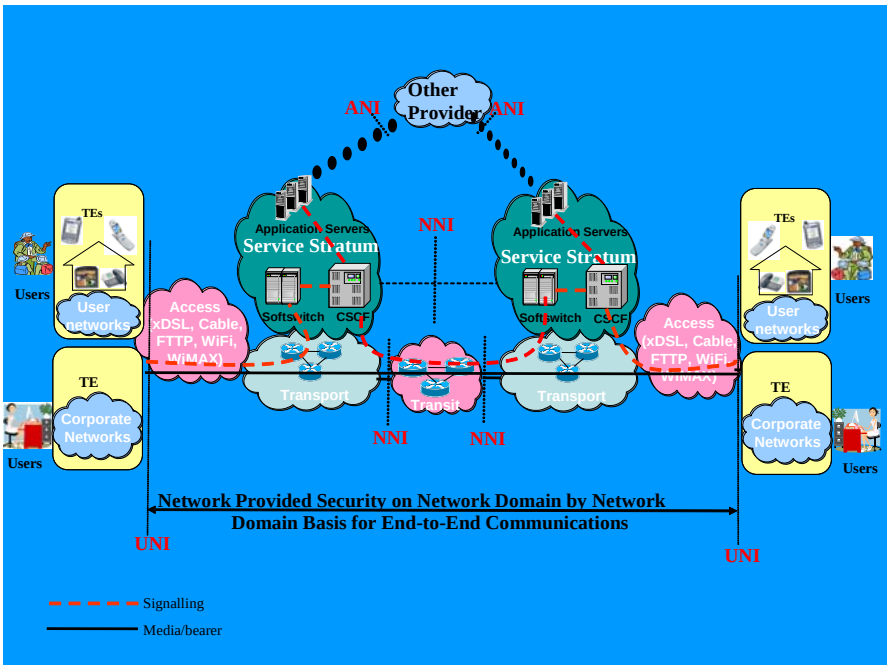

Figure 7 - Security of communications across multiple networks

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.

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 only. Authorization may be given by the provider providing the access or by another provider after validation by an authentication and access control process.

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 to authenticate subscriber, 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 of an end user device, a user-network gateway, or corporate network gateway to obtain access or attachment to the transport network access).
2. Capabilities to authenticate a user 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 needed by network services or features.
5. Capabilities to allow bilateral authentication or mutual authentication between two NGN providers on each stratum for exchange of signaling, 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 standard 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.

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.

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

7.3.7 Availability

The 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.

The 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 standard.

7.3.8 Privacy

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

8 Specific Security requirements

This section 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 the trusted zone and in the 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 the service and the transport strata (user-to-network, network-to-user, network-to-network). This should also be possible in the 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, by blocking unauthorized traffic.

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

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 signaling/control flows and management flows transported on it.

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

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

The security requirements for secure TMN management are to follow those stated in T1.276 [11] and ITU-T Recommendations M.3016.0[9] (clause 10.1) and M.3016.1[10] (clause 6).

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

The NGN elements, especially certain network border elements may perform the logical and/or physical separation of transport. Examples include 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 networks (virtual such as VPNs and VLANs). This shall adhere to the security policies in place

The 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. Protection may be 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 establishing 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. The NGN providers shall prepare an

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” (software access which would circumvent usual access control mechanisms) are permitted 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. The 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.

T1.276 [11] and ITU-T Recommendations M.3016.0 [9] (clause 10.1.2.6.3) and M.3016.1 [10] (clause 6.6, and clause 6.7) detail further the security requirements for security logging and audit.

8.1.4 Time stamping and time source

NGN elements are 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 the 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 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.

T1.276 [11] and ITU-T Recommendation M.3016.0 [9] (clause 10.1.2.6.4) details further 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 “Trojan horses[4]” (that phone home), “worms” (that generate useless traffic or turn systems into “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.

[4] 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.

These analysis would 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.

T1.276 [11] and ITU-T Recommendation M.3016.1 [10] (Appendix I.5.2) provides further considerations on a patching process; Appendix I.5.3.9 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 set allocated from a separate address block. Each internal NGN network element should have a physically or logically separate interface for the exclusive use of 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 NGN element is required to internally track all changes, and provide the opportunity to roll them back.

All security relevant use of authorization is required to be logged in the audit trail. The audit trail is required to be retained 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.

8.2 Requirements for NGN elements in the trusted zone

Each NGN element in the “trusted” zone is to be assigned an IP address(s) in the block reserved for internal (i.e., trusted) NGN elements. All signaling is required to use this address(s). The NGN element is also required to be assigned an IP address(s) in the block reserved for OAMP, and all OAMP messaging is required to use this address(s).

In order to preserve the confidentiality and integrity of customer communication signaling and media traffic 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 defense 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 defense against signaling attacks. All signaling traffic from a TE or TE-BE in the “un-trusted zone” is processed at its assigned NBE, which re-transmits the information 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 the “un-trusted zone” from reaching any network element in trusted zone except its assigned NBE(s).

As with signaling, the network border elements (NBE) are also the main defense against media attacks. All media traffic from TE/TE-BE is processed at a NBE, and the NBE relays the media traffic. The NBE routes media packets, towards the destination and through the “trusted” zone, 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 negotiated rate for the session. 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 re-transmitted 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 set (the “internal” address) is to be assigned from the block reserved for internal NGN elements. All signaling and media to and from other internal NGN elements is required to use this address set (or this interface). One IP address set (the “external” address) is to be assigned; it is to be accessible from the TE equipment. All signaling and media to and from the TE is required to use this address set (or this interface). One IP address set (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 signaling traffic, the signaling transport of all signaling 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 signaling information to such NGN elements are required to be established using secure channels with authentication. All signaling 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 signaling exchange), and against the expected source address (based on the session description contained in the signaling 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 channels from a source IP address that is not a valid originator of requests to this NBE are also to be silently discarded.

8.3.1 Requirements for NNI Security

The requirements specified in ATIS-1000019, *Network to Network (NNI) Standard for Signaling and Control Security for Evolving VoP Multimedia Networks* [12] shall be supported for NNI security.

8.3.2 Requirements for PSTN/SS7 Interconnection Security

The requirements specified in clause 10.3 of ATIS-1000012, *Signaling Systems No. & (SS7) - SS7 - Network and NNI Interconnection Security Requirements and Guidelines* [13] shall be supported for security of interconnection to PSTN/SS7.

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 shall 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 signaling traffic, signaling messages are required to use a secure signaling 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 eavesdropping. Since OAMP can be provided either in-band or 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 security functionalities of the NGN provider border elements facing the “untrusted” zone are for further study.

Media traffic should be protected from eavesdropping or modification.

9 Emergency Telecommunications Service (ETS) Security

Special consideration should be given to protect ETS communications and, resources and information related to ETS. The requirements specified in ATIS-1000010, *Support for Emergency Telecommunications Service (ETS) in IP Network* [3] for security of ETS shall be supported.

10 Identity Management (IdM)

A structured IdM approach is necessary to protection the NGN and its resources such as services, applications, and sensitive and private network and subscriber information. By implementing IdM capabilities and best practices for access control and for the use of personal identifiers identity information, NGN providers can drastically reduce cyber crime such as identity theft, hacking and frauds and can protect the NGN infrastructure.

NGN providers shall implement capabilities for IdM and protect IdM functions and information. IdM capabilities include but are not limited to, the following:

- Capabilities to discover authoritative and trusted sources of identity information
- Capabilities to allow secure exchange of identity information for validation and assertion of identities among authorized entities based on trust and security policies.
- Capabilities to allow secure exchange of identity related information between the different systems supporting multiple applications/services (e.g., voice, data and IPTV). For example, the NGN should support single-sign-on to multiple applications/services or should allow different applications/services to use common authentication and authorization functions and resources for efficiency and security.
- Capabilities to control access to network information and subscriber’s private information based on security and trust policies.
- Capabilities to control and protect stored identity information.

Annex A

(informative)

A Informative References

ATIS[5]

ATIS-1000014, *Information & Communications Security for NGN Converged Services IP Networks and Infrastructure* (October, 2007)

ITU-T Recommendations[6]

ITU-T Recommendation Y.2111, *Functional Resource and admission control functions in Next Generation Networks*

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

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

ITU-T Recommendation M.3016.2 (2005), *Security for the management plane: Securityservices*

ITU-T Recommendation M.3016.3 (2005), *Security for the management plane: Securitymechanism*

ITU-T Recommendation M.3016.4 (2005), *Security for the management plane: Profileproforma*

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

ITU-T Recommendation E.115 (2006), *Computerized directory assistance*

ITU-T Recommendation E.106 (2003), *International Emergency Preference Scheme (IEPS) for Disaster Relief Operations*.

ITU-T Recommendation E.107, *Emergency Telecommunications Service (ETS) and Interconnection Framework for National Implementations of ETS*.

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*.

Supplement 1 to Y.2000-series Recommendations, NGN release 1 scope

---

[5] These documents are available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

[6] These documents are available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

ETSI TISPAN documents[7]

ETSI TS 187 001, *NGN Release 1 Security Requirements*

ETSI TR 187 002, *Threat and Risk Analysis*

ETSI TS 187 003, *Security Architecture*

ETSI/3GPP documents[8][9]

3GPP TS 33.102, *3G security; Security architecture*.

3GPP TS 33.103, *3G security; Integration guidelines*.

3GPP TS 33.110, Key *establishment between a UICC and a terminal*.

3GPP TS 33.120, *Security Objectives and Principles*.

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

3GPP TS 33.201, *Access domain security*.

3GPP TS 33.203, *3G security; Access security for IP-based services*.

3GPP TS 33.204, *Network Domain Security (NDS); TCAP user security*.

3GPP TS 33.210, 3G *security; Network Domain Security (NDS); IP network layer security*.

3GPP TS 33.220, *Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.

3GPP TS 33.310, *Network domain security; Authentication framework (NDS/AF)*.

3GPP TR 33.900, *Guide to 3G security*.

3GPP TR 33.901, *Criteria for cryptographic Algorithm design process*.

3GPP TR 33.902, *Formal Analysis of the 3G Authentication Protocol*.

3GPP TR 33.903, *Access Security for IP based services*.

3GPP TR 33.908, *3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms*.

3GPP TR 33.909, *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*.

3GPP TR 33.918, *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)*.

3GPP TR 33.919, Generic Authentication Architecture (GAA); System description.

---

[7] These documents are available from the European Telecommunications Standards Institute (ETSI). < http://www.etsi.org/getastandard/home.htm >

[8] These documents are available from the Third Generation Partnership Project (3GPP) at < http://www.3gpp.org/specs/specs.htm >.

[9] These documents are available from the European Telecommunications Standards Institute (ETSI). < http://www.etsi.org/getastandard/home.htm >

3GPP TR 33.920, *SIM card based Generic Bootstrapping Architecture (GBA); Early Implementation Feature*.

3GPP TS 33.980, *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)*.

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*.

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*.

ETSI TR 133 919 (2005), *Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); System description*.

ETSI TS 133 120 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Security Principles and Objectives*.

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

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

ETSI TS 133 220 (2006), *Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.

ETSI TS 133 310 (2006), *Universal Mobile Telecommunications System (UMTS); Network domain security; Authentication framework (NDS/AF)*.

ETSI TS 133 901 (2001), *Universal Mobile Telecommunications System (UMTS);3G Security - Criteria for cryptographic Algorithm design process*.

ETSI TS 133 902 (2001), *Universal Mobile Telecommunications System (UMTS); Formal Analysis of the 3G Authentication Protocol*.

ETSI TS 133.210 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security*.

ETSI TS 133 102 (2006), *Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture*.

ETSI TS 133 103 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Integration Guidelines*.

ATIS/3GPP2 documents[10]

3GPP2 S.S0086 (2004), *IMS Security Framework*.

[10] This document is available from the Third Generation Partnership Project (3GPP) at < http://www.3gpp.org/specs/specs.htm >.

IPsec related IETF RFCs[11]

IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*.

IETF RFC 4302 (2005), *IP Authentication Header*.

IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP)*.

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

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

ETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol*.

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

IETF RFC 4308 (2005), *Cryptographic Suites for IPsec* .

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

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

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

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

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

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

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

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

IETF RFC 2411 (1998), *IP Security Document Roadmap*.

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

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

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

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

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

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

[11] These documents are available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

S/MIME related IETF RFCs[12]

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

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

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

IETF RFC 3851 (2004), *S/MIME Version 3.1 Message Specification*.

IETF RFC 3852 (2004), *Cryptographic Message Syntax*.

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

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

IETF RFC 4134 (2005), *Examples of S/MIME Messages*.

TLS related IETF RFCs[13]

IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

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

IETF RFC 2818 (2000), *HTTP Over TLS*.

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

IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.

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

Miscellaneous IETF security related RFC[14]

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

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

IETF RFC 3948 (2005), *UDP Encapsulation of IPsec ESP Packets*.

IETF RFC 3847 (2004), *Restart Signalling for Intermediate System to Intermediate System (IS-IS).*

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

---

[12] These documents are available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[13] These documents are available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[14] These documents are available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

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*.

DNS related IETF RFCs[15]

IETF RFC 4033 (2005), *DNS Security Introduction and Requirements*.

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

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

TIA documents[16]

TIA Standard TIA-683-D (2005), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*.

TIA Standard TIA-1053 (2005), *Broadcast/Multicast Service Security Framework*.

TIA Standard TIA-1091, *IMS Security Framework*.

ARIB documents[17]

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

---

[15] These documents are available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[16] These documents are available from the Telecommunications Industry Association (TIA). < http://www.tiaonline.org/standards/overview.cfm >

[17] This document is available from http://www.arib.or.jp/english/