ATIS-1000034.2010(S2020)

Next Generation Network (NGN): Security Mechanisms and Procedures

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as 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-1000034.2010(S2020), *Next Generation Network (NGN): Security Mechanisms and Procedures*

Is an American National Standard developed by the ATIS **Packet Technologies and Systems Committee (PTSC)**.

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

ATIS-1000034.2010(S2020)

American National Standard for Telecommunications for

Next Generation Network (NGN): Security Mechanisms and Procedures

Alliance for Telecommunications Industry Solutions

Approved November 18, 2010

(Republished April 2022 with an administrative edit)

American National Standards Institute, Inc.

Abstract

ATIS-1000029.2008, *NGN Security Requirements*, provides security requirements for next generation networks (NGNs) and its interfaces (e.g., UNIs, NNIs and ANIs). This standard describes some security mechanisms that can be used to fulfill the requirements described in ATIS-1000029.2008 and specifies the suite of options for each selected mechanism. Specifically, this standard describes identification, authentication and authorization mechanisms; then discusses transport security for signalling and OAMP, and media security. It then describes audit-trail-related mechanisms and finally describes the provisioning. The security mechanisms described in this standard are based on use of the trust model defined in ATIS 100029.The list of security mechanisms described in this standard is not exhaustive. NGN providers are encouraged to support additional security tools, capabilities and operational measures as needed beyond the mechanisms specified in this standard for NGN security protection.

Foreword

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:

M. Dolly, PTSC Chair (AT&T)

W. Downum, Technical Editor (Telcordia)

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 –

Next Generation Network (NGN): Security Mechanisms and Procedures

1. Scope

ATIS-1000029 (NGN Security Requirements) [ATIS-100029], provides security requirements for next generation networks (NGNs) and its interfaces (e.g., UNIs, NNIs and ANIs), including a trust model. The security mechanisms selected to implement these requirements will contain options, and mismatched options are undesirable because they tend to introduce security vulnerabilities and make it more difficult to achieve interoperability.

This standard therefore highlights some important security mechanisms that can be used to realize the requirements in [ATIS-100029] and specifies the suite of options to be used for each selected mechanism to reduce interoperability and mismatch problems. The list of mechanisms described in this standard is not exhaustive. NGN providers are encouraged to support additional security tools, capabilities and operational measures as needed beyond the mechanisms specified in this standard for NGN security protection.

This standard is intended to be used with [ATIS-100029] and [ITU-T Y.2701] to provide a base for NGN security. It should be used with other security related standards and other specifications as appropriate for specific security areas.

> Note: The mechanisms described in this standard for identification and authentication are part of the broader topic generally known as IdM ("identity management").

1.1 Assumptions

This standard is based on the following assumptions:

1. The bundling of functional entities, as defined in [ATIS-1000018] and [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) to protect itself, b) to assure end-to-end security is not compromised within its network, and c) to assure high availability and integrity of NGN communications.
3. Each network domain will establish and enforce policies of 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 protect the interconnected networks and the communications (signalling/control traffic, bearer traffic and management traffic) across UNIs, ANIs and NNIs.
4. This standard addresses network-based security, which is achieved by applying a layered architecture, consisting of perimeter security to trusted domains, physical security of provider equipment, and potentially the use of encryption

1.2 Overview

This standard is organized as follows:

- Clause 2 (References) – This clause provides normative references.

- Clause 3 (Definitions) – This clause provides definitions used in this standard
- Clause 4(Abbreviations and acronyms) – This clause provides the list of abbreviations and acronyms used in this standard.
- Clause 5 (Convention) – This clause is intentionally left blank.
- Clause 6 (Security risks and threats) – This clause provides reference to security risks and threats applicable to NGN.
- Clause 7 (Security trust model) – This clause provides a summary of the trust model defined in ATIS-100029 and ITU-T Y.2701.
- Clause 8 (Identification, authentication and authorization) – This clause provides mechanisms and security measures for identification, authentication and authorization
- Clause 9 (Transport security for signaling and OAMP) - This. clause provides mechanisms for signaling and OAMP encryption and integrity protection
- Clause 10 (Media security) – This clause provides mechanisms for media (i.e., bearer traffic) protection.
- Clause 11 (OAMP) – This clauses provides information and references for audit trail, trapping and logging of security events.
- Clause 12 (Provisioning of equipment in untrusted zone) – This clause provides information regarding provisioning of subscriber equipment in the un-trusted zone.
- APPENDIX A – Examples of Source-Address Assurance and its application to the mechanism of subscriber identification and authentication
- APPENDIX B – Emergency Telecommunications Service (ETS) Interconnection Security
- APPENDIX C – Security Best Practices
- APPENDIX D – Bibliography.

2. Normative 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 editions indicated were valid. All standards are subject to revision, and parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

2.1 ATIS references[1]

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

[ATIS-1000029] ATIS-1000029.2008, *NGN Security Requirements*

[ATIS-1000030] ATIS-1000030.2008, *Authentication and Authorization Requirements for Next Generation Network (NGN)*

[ATIS-1000035] ATIS-1000035.2009, *Next Generation Network (NGN) Identity Management (IdM) Framework*

[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 >

[ATIS-1000010] ATIS-1000010.2006(R2011), *Support of Emergency Telecommunications Service (ETS) in IP Networks*

[ATIS-0300276] ATIS-0300276.2008, *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane.*

2.2 ITU-T references[2]

[ITU-T Y.2012] ITU-T Recommendation Y.2012 (2006), *Functional Requirements and Architecture of the NGN*

[ITU-T Y.2701] ITU-T Recommendation Y.2701 (2007), *NGN security requirements*

[ITU-T Y.2702] ITU-T Recommendation Y.2702 (2008), *NGN Authentication and authorization requirements.*

[ITU-T Y.2703] ITU-T Recommendation Y.2703 (2009), *The application of AAA service in NGN.*

[ITU-T Y.2720] ITU-T Recommendation Y.2720 (2009), *NGN identity management framework.*

[ITU-T X.509] ITU-T Recommendation X.509 (2008), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

[ITU-T X.660 | ISO/IEC 9834-1] ITU-T Recommendation X.660 (2008) | ISO/IEC 9834-1:2008), *Information Technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the ASN.1 Object Identifier tree.*

[ITU-T X.1035] ITU-T Recommendation X.1035 (2007), *Password-authenticated key exchange (PAK) protocol.*

[ITU-T M.3016] ITU-T Recommendation M.3016 (2005), *Security for the management plane.*

2.3 IETF references[3]

[IETF RFC4302] IETF RFC 4302, *IP Authentication Header.*

[IETF RFC4303] IETF RFC 4303, *IP Encapsulating Security Payload (ESP).*

[IETF RFC5246] IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2.*

3. Definitions

3.1 Terms defined elsewhere

This standard uses the following terms defined elsewhere:

---

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

[3] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

3.1.1 Asset [ATIS-1000029 and ITU-T Y.2701]: Anything that has value to the organization, its business, its operations and its continuity.

3.1.2 Border element [ATIS-1000029 and ITU-T Y.2701]: Network element providing functions connecting different security and administrative domains.

3.1.3 Corporate network [ATIS-1000029 and ITU-T Y.2701]: A private network that supports multiple users and may be in multiple locations (e.g, an enterprise, a campus).

3.1.4 Terminal equipment border element [ATIS-1000029 and ITU-T Y.2701]: Border element providing security functions between customer premises equipment and service provider network.

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

3.1.6 Network border element [ATIS-1000029 and ITU-T Y.2701]: Border element under sole control of the provider, providing security functions with terminal equipment.

3.1.7 Domain border element [ATIS-1000029 and ITU-T Y.2701]: Border element under sole control of the provider, providing security functions with other network domains.

3.1.8 Security domain [ATIS-1000029 and ITU-T Y.2701]: 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**.1.9 Trust** [ATIS-1000029 and ITU-T Y.2701]: 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.

3.1.10 Trusted but vulnerable zone [ATIS-1000029 and ITU-T Y.2701]: 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.

3.1.11 Trusted zone [ATIS-1000029 and ITU-T Y.2701]: 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.

3.1.12 Un-trusted zone [ATIS-1000029 and ITU-T Y.2701]: 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.

3.1.13 Security Token [ITU-T X.810]: A set of data protected by one or more security services, together with security information used in the provision of those security services, that is transferred between communicating entities.

3.1.14 Security zone [ATIS-1000029 and ITU-T Y.2701]: ITU-T Y.2701 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.

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

3.1.16 User Network [ATIS-1000029 and ITU-T Y.2701]: A private network consisting of terminal equipment that may have multiple users.

3.2 Terms defined in this standard

This standard defines the following term:

3.2.1 Authenticator: An Authenticator is a network element that facilitates identification and authentication of subscribers, devices, or end-users. For example, border elements with back-to-back user agent (B2BUA) functionality or proxy call session control functional entity (P-CSC-FE) can be Authenticators of subscribers for SIP-based services.

4 Abbreviations and acronyms

This standard uses the following abbreviations and acronyms.

3G	3rd Generation
ATIS	Alliance for Telecommunications Industry Solutions
AGW	Access Gateway
AH	Authentication Header
AKA	Authentication and Key Agreement
ANI	Application-to-Network Interface
AS/WS	Application Server/Web Server
AuC	Authentication Center
B2BUA	Back-to-Back User Agent
BE	Border Element
BSR	Base Station Server
CA	Certification Authority
COPS	Common Open Policy Service
CRL	Certificate Revocation List
CSC-FE	Call Session Control Functional Entity
DBE	Domain Border Element
DNS	Domain Name System
DoS	Denial of Service
DTMF	Dual-Tone Multi-Frequency
ECC	Elliptic Curve Cryptography (ECC)
ESP	Encapsulating Security Protocol
ETS	Emergency Telecommunications Service
FE	Functional Entity

GBA	Generic Bootstrapping Architecture
GW	Gateway
HMAC	Hash Message Authentication Code (HMAC)
HTTP	Hypertext Transfer Protocol
I-CSC-FE	Interrogating Call Session Control Functional Entity
ID	Identity
IdM	Identity Management
IDPS	Intrusion Detection and Prevention Systems
IDS	Intrusion Detection Systems
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LAN	Local Area Network
MD5	Message Digest 5
MIB	Management Information Base
MPLS	Multi Protocol Label Switching
MRP-FE	Media Resource Processing Functional Entity
MS	Mobile Station
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
OID	Object Identifier
ONU	Optical Network Units
PAK	Password Authenticated Key
P-CSC-FE	Proxy Call Session Control Functional Entity
POTS	Plain Old Telephone Service
PSTN	Public Switch Telephone Network
QoS	Quality of Service
RAC-FE	Resource and Admission Control Functional Entity
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network

RTSP	Real Time Streaming Protocol
SAA-FE	Service Authentication and Authorization Functional Entity
SASL	Simple Authentication and Security Layer
SBC	Session Border Controller
S-CSC-FE	Serving Call Session Control Functional Entity
SDP	Session Description Protocol
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SL-FE	Subscription Locator Functional Entity
SNMP	Simple Network Management Protocol
SRTP	Secure Real Time Protocol
TAA-FE	Transport Authentication and Authorization Functional Entity
TCP	Transmission Control Protocol
TE	Terminal Equipment
TE-BE	Terminal Equipment Border Element
TLS	Transport Layer Security
TMN	Telecommunication Management Network
TRIP	Telephony Routing over IP
UA	User Agent
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
UNI	User-to-Network Interface
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
VLAN	Virtual LAN
VPN	Virtual Private Network
WLAN	Wireless LAN
xDSL	x Digital Subscriber Line

5 Conventions

None.

6 Security risks and threats

See clause 4 in [ATIS-1000029] and [ITU-T Y.2701] for security risks and threats assumed for the NGN environment.

7 Security trust model

The choice by an NGN provider of security mechanisms depends on the applicable trust model. This standard assumes the use of the trust model defined in [ATIS-1000029] and [ITU-T Y.2701]. This clause provides a summary of the NGN security trust model defined in [ATIS-1000029] and [ITU-T Y.2701].

The NGN functional reference architecture defines functional entities (FEs). However, since network security aspects depend heavily on the way that FEs are physically 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 and on the NGN provider.

7.1 Single network trust model

This sub-clause 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 1.

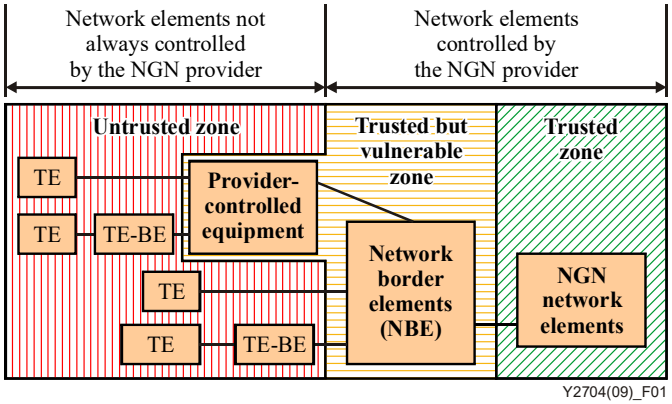

Figure 1 Security trust model/[ATIS-1000029]

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

1). They are under the full control (for provisioning, maintenance, and operational control) of the NGN provider,

2) They are located in the NGN provider domain, and

3) They communicate only with other elements in the “trusted” zone and with elements in the “trusted-but-vulnerable” zone.

It should not be assumed that because a network element is in a trusted zone, it is necessarily secure.

The network elements in 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 management messages, and the use of a separate VPN within the (MPLS/)IP network. The same combination of methods is expected to be applied to secure communication within the “trusted” zone and between NGN network elements in the “trusted” zone and the “trusted-but-vulnerable” zone.

A “trusted but vulnerable network security zone”, or “trusted but vulnerable zone” in short, is a zone where the network elements/devices communicate with elements in the “un-trusted” zone, which is why they are “vulnerable”. In addition, they communicate with elements in the “trusted” zone. Like network elements in the “trusted” zone, the equipment is under the control of the NGN provider, though the equipment may be located within or outside the NGN provider’s premises. Their major security function is to protect the NEs in the trusted zone from the security attacks originated in the un-trusted zone. The combination of methods applied to secure communication between NGN network elements in the “trusted-but-vulnerable” zone and the “untrusted” zone may differ from those used to secure communication in the “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 that interface to 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. Examples of these are access Session Border Controllers (SBCs) at the UNI and interconnect SBCs at the NNI.
- “Domain border elements (DBEs)” that reside on the border between two domains within a single service provider’s network.
- “Device configuration & bootstrap NBEs (DCB-NBEs)” 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-NBEs” that interface with the NGN provider’s OAMP systems in the trusted zone in order to provision and maintain the user’s/subscriber’s device and certain NGN provider’s equipment in the outside plant.
- “Application server/web server NBEs (AS/WS-NBEs)” 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.

Figure 1 shows the relationships among the NBEs and NEs that need to be protected.

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;
- a base station router (BSR), a network element that integrates the base station, radio network controller and router functionalities for wireless access;
- an optical unit (ONU) 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. An “un-trusted” zone includes all network elements of customer networks and possibly peer networks or other NGN provider domains which are connected to the NGN Provider’s network border elements. In the “un-trusted” zone comprised of terminal equipment, equipment is not under the control of the NGN provider and it may be impossible to enforce the NGN provider’s security policy on the user. Still it is desirable to try to apply some security measures, and to that end, it is recommended that signalling, media, and OAMP interfaces be secured and the TE-BE located in the “un-trusted” zone, be hardened. However, security is less for communication with network elements in the “un-trusted” zone than for communication with network elements in the “trusted” zone.

7.2 Peering network trust model

When an NGN is connected to another network, the presence or absence of trust depends on:

- the physical interconnection, where the interconnection can range from a direct connection in a secure building to a connection between separate (possibly not secured) buildings via shared facilities;
- the peering model, where the traffic can be exchanged directly between the two NGN service providers, or via one or more NGN transport providers;
- the business relationships among network, where there may be penalty clauses in the SLA, and/or a trust in the other NGN provider’s security policies; in general, NGN providers should view other providers as un-trusted.

Figure 2 shows an example when a connected network is judged un-trusted.

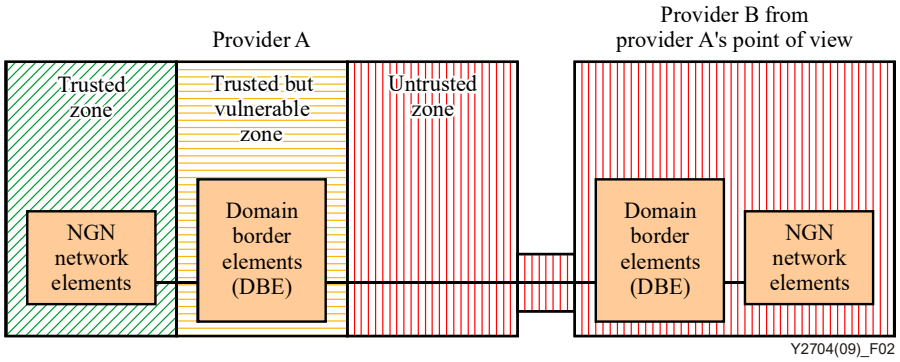

Figure 2 – Peering trust model/[ATIS-1000029]

8 Identification, Authentication and Authorization

Refer to [ATIS-1000029], [ATIS-1000030], [ATIS-1000035], [ITU-T Y.2701], [ITU-T Y.2702], and [ITU-T Y.2720] for information related to identification, authentication, authorization and identity management (IdM).

This clause describes identification, authentication and authorization mechanisms, in particular, those concerning SIP-based services. The mechanisms concerning other services are for further study.

8.1 Subscribers

A request for an NGN service is associated with a subscriber. This association is determined through identification of the request with the subscriber. Further identification (and associated authentication) of the End-User may be necessary depending on the SLA between the NGN provider and the Subscriber.

This process can be achieved by using a functional element that facilitates identification and authentication of subscribers, devices or end-users (called an Authenticator). For example, Network Border Elements (NBE) with back-to-back user agent (B2BUA) functionality or P-CSC-FEs can be Authenticators of subscribers for SIP-based services. Identification and authentication is achieved by exchanging and validating credentials between the Authenticator and the TE.

8.2 Network Element

[ATIS-1000029] and [ITU-T Y.2701] recommends that Network Elements to be identified and authenticated for communications.

If the Border Element receives the request from a NGN Network Element in the Trusted Zone, the identification contained in the request may be considered accurate and not checked further subject to NGN provider security policy.

If the Border Element receives requests from Network Elements in the un-trusted and the trusted-but vulnerable Zone, the Network Elements are recommended to be identified and authenticated and the communication privileges verified. Identification and authentication is achieved by exchanging and validating credentials between the Authenticator and the NE.

8.3 Credential usage in the NGN Security

Credentials are used in NGN Security to identify and authenticate a Device, a Subscriber, or an End-User. These credentials are described in section 8.3.1. These credentials may take one of two different forms, either a X.509 public key certificate (described in clause 8.3.2) or a shared key (described in section 8.3.3). An X.509 public key certificate may be used to establish a secure transport between the TE and the Authenticator (described in section 8.3.1) based on the NGN provider policy. The shared key may be used either to establish a secure transport, or in generating/verifying the response to an Authenticator -initiated challenge (described in section 8.3.1) based on the NGN provider policy.

8.3.1 Device, Subscriber, and End-User Credentials

Three distinct types of credentials are used in the NGN:

1. Device credentials,
2. Subscriber credentials, and
3. End-User credentials.

Device credentials may be supplied by the manufacturer with the device. For example, during the manufacture of the device, the device may have the credentials “burned in” from the manufacturer, which includes such information as the device serial number or the manufacturer. Device credentials identify and authenticate the device. An NGN provider may associate device credentials with a particular subscriber’s service to alleviate the need for subscriber credentials. In such cases requests from the device may be associated with a particular account based on the NGN provider policy.

Subscriber credentials are used for association of the originator of an NGN request with a particular account. Subscriber credentials are entered (e.g., via download, SIM, etc.) in the devices capable of accepting such credentials. Subscriber credentials installed on a device associate the subscriber with that device. All calls made from the device will be associated with the subscriber whose credentials are installed on the device. Multiple sets of credentials may be installed on a single device, in which case the device provides the means to distinguish between requests associated with each subscriber. Note: An NGN customer may have one or more NGN subscription, each associated with zero or more devices. In addition, the NGN subscription may be associated with one or more end users (i.e., the end user is not necessarily the subscriber) that may be using different devices or sharing the same device based on NGN provider policy.

End-User credentials are used to identify and authenticate specific end users to the network. For example, a SIM card can identify the End-User for a service; when the End-User places their SIM card into the phone it becomes associated with (and all calls are identified as being from) that End-User. Another example is a Security Token, a hardware token (a physical device) or a software token (a program installed on a general-purpose device such as a personal computer). It is provided to an authorized user to augment the authentication process. A security token may store cryptographic keys, such as a digital signature, or biometric data, such as a fingerprint. A request originating from a NGN device will be identified and authenticated as being from the End-User associated with that Security Token. In certain scenarios (e.g., in the case of the SIM card above) it may be possible for multiple end-users to use the service associated with a single subscriber (i.e., subscriber account), and calls originated by the end-user are charged to the subscriber account. End users can identify and authenticate themselves with the network to take advantage of personal services. Individual transport layer security associations may be established, using end user credentials, between the TE and NGN Network (Authenticators). The NGN provider associates the end user credentials with a particular subscriber service for billing purposes.

8.3.2 X.509 public key certificates as credentials

An X.509 public key certificate is a digital document that includes an entity’s identifier, its attributes, a public key that belongs to the entity, and other authentication information (e.g., information on the issuer of the certificate, Certificate Revocation List [CRL], starting and ending dates and times of the certificate’s validity, etc.). The description of some of the basic fields and some extensions fields of an X.509 public key certificate is provided in Table 1. Refer to [ITU-T X.509] for detailed descriptions of the fields of X.509 public key certificates. A public key certificate is digitally signed by a trusted third party, which is normally referred to as the Certification Authority (CA) for the public key certificate. The CA computes a hash (e.g., using SHA-1) of all the fields except the *Signature Value field*, encrypts it with its own private key, and then adds the signature together with the signature algorithm applied to the certificate (in the *Signature Value field*).

Table 1– Some basic and extensions fields of an X.509 public key certificate

Name of a field	Description
Subject	Identifies the entity associated with the public-key certificate (the directory distinguished name of certificate subject)
Serial number	A unique identifier of the certificate
Issuer	Identifies the entity that has signed and issued the certificate (the directory distinguished name of the CA)
Valid From	Starting date and time of the certificate validity
Valid To	Ending date and time of the certificate validity
Public Key	The public key of the certificate holder
Version	Version of the encoded X.509 public key certificate
Subject Alternative Name	Another identifier of the certificate holder
CRL Distribution Points	Name or address of the CRL distribution point
Authority Information Access	Name or address for access to information about the CA
Enhanced Key Usage	Description of the purposes that the certificate can be used for (list of the ITU-T | ISO/IEC-defined object identifiers (OIDs) [X.660 | ISO/IEC 9834-1]
Application policies	The applications and services that can use the certificate (specified by the OIDs)
Certificate Policies	Policies and mechanisms used by the CA for receiving a request for, handling, authorizing, issuing, and managing certificates
Signature Algorithm	The algorithm identifier for the algorithm and hash function used by the CA in signing the certificate (e.g., SHA-1 with RSA)
Signature Value	The actual signature of the certificate

Public key certificates specified in [ITU-T X509] may be used by NGN Network elements in establishing security associations with other network elements, and provide the basis for mutual identification and authentication. They can also be used between TE and the Authenticator for the same purposes.

For a subscriber or end-user certificate, the <Subscriber Account Identifier> (see clause 8.4.2), an identifier to fetch subscriber account information, is used by the Authenticator to obtain further information about the credentials through the Service Authentication and Authorization (SAA) and the Transport Authentication and Authorization (TAA) Functional Entities (SAA/TAA-FEs). For a device certificate, if the device has been associated with a subscriber, then the Device Manufacturer and Device Serial Number are used by the Authenticator to determine the associated <Subscriber Account Identifier>, and then the <Subscriber Account Identifier> is used to obtain further information about the credentials through the SAA/TAA-FEs.

End-user, Service and Device certificates may be used in creating TLS connections between the device and the Authenticator (section 9.1.2), or may be used in creating IPsec connections through IKE Authentication (section 9.2.4.3).

8.3.3 Shared keys as credentials

Shared key can be used to enhance the security of NGN access. In that case, a copy of the shared key is given to the subscriber or end-user, and a copy is stored in the appropriate Functional Entities such as the Service User Profile – Functional Entities (SUP-FEs) or Transport User Profile Functional Entities (TUP-FEs). Every key is required to have a unique name, and the name is used by the Authenticator to obtain further information about the credentials.

When using pre-shared keys, the strength of the system is dependent upon the strength of the shared secret. The goal is to keep the shared secret from being the weak link in the chain of security. This implies that the shared secret needs to contain as much entropy (randomness) as the cipher being used. In other words, the shared secret is recommended to have at least 128-160 bits of entropy.

It should be noted that the symmetric key approach has certain differences compared to the asymmetric key approach described in clause 8.3.2 and the following should be considered:

- An entity needs to have a separate set of symmetric keys with each communications partner;
- The keys have to be provisioned, established and stored in a secure way;
- An entity must rely on its partner to keep the shared key secret.

8.3.4 Information provisioned in SUP/TUP-FEs for each set of credentials

The SUP/TUP-FEs are the repositories for all device, subscriber, and end-user credentials to be used to access in the NGN infrastructure. They are typically implemented as an integral part of the Authenticator in order to optimize the handling of authentication requests. However, to support mobility, the Authenticator may need to consult a remote SAA/TAA-FE server to obtain information about credentials. The Subscriber Account Identifier, or the Key Name, is used to fetch this information through the SAA/TAA-FE.

The following security-related information associated with each set of credentials is required to be provisioned in the FEs such as SUP/TUP-FEs storing the credentials: (1) the Subscriber Account Identifier or the Key Name or the, (2) whether end-user identification and authentication is required for this subscriber, (3) whether these credentials describe a subscriber or an end-user, and (4) allowable values of the “From” header in requests.

Following are several examples of the information stored in the credential repositories such as SUP/TUP-FEs.

For a TE NGN device certificate that handles four POTS lines, with numbers 212-555-1111-1113 and 1151:

Subscriber Account: 123-456789
From headers: sip:212-555-111[1-3]@NGN .ngn.com
| sip:212-555-1151@NGN .ngn.com
Identity string: sip:212-555-1111@NGN .ngn.com
Type of credentials: subscriber
End-User ID required: no

For a subscriber certificate assigned to the John Doe family:

Subscriber Account: Doe-family
From headers: sip:*Doe@NGN .ngn.com
Identity string: sip:Doe@NGN .ngn.com
Type of credentials: subscriber
End-User ID required: no

For a pre-shared key assigned to the John Doe family:

Key name: JohnDoe

Key: dfe56131d1958046689d83306477ecc
From headers: sip:*Doe@NGN .ngn.com
Identity string: sip:Doe@NGN .ngn.com
Type of credentials: subscriber
End-User ID required: no

For a TE-BE serving the Acme Widget Company:
Subscriber Account: Acme Widget Company
From headers: sip:*@acme.com
Identity string: sip:acme.com
Type of credentials: subscriber
End-User ID required: no

For an end-user at the Acme Widget Company:
Subscriber Account: Acme Widget Company
From headers: sip:bob@acme.com
Identity string: sip:bob@acme.com
Type of credentials: end-user

8.4 Identification and Authentication of Subscribers

8.4.1 General Strategy

The originator's identity in SIP is generally contained in the "From" header. However, identification of the subscriber through the use of the "From" header in a SIP request is susceptible to spoofing attacks and is therefore not used where higher level of assurance of the subscriber's identity is required. Instead, the value of the "From" header is compared against the subscriber identity obtained by other means.

In order to minimize the effect on call setup delay, the identification and authentication of the subscriber is derived from the Network Source Address (source address in the IP packet header) or the transport security association (association established by e.g., IPsec or TLS between the originating device and the Authenticator) whenever possible. When these techniques do not produce an identification consistent with the "From" header in the SIP request, then a challenge is issued to the originator; if the response contains proper credentials then the request will proceed. Further details of these procedures are described in the following sections.

The procedures in section 8.4.2 describe how the Authenticator determines, based on the Network Source Address, that either (1) the Subscriber can't be determined by this method, (2) a Subscriber is determined and it matches the "From" header in the request, or (3) a Subscriber is determined but it is different than the "From " header in the request.

The procedures in section 8.4.3, describes how the Authenticator determines based on the Transport Security association, that either (1) the Subscriber can't be determined by this method, (2) the Subscriber is determined and it matches the "From" header in the request, or (3) the Subscriber is determined but it is different than the "From" header in the request.

The actions then taken by the Authenticator are given in Table 2.

Table 2 – Authenticator's actions for each authentication result

Source Address determination of Subscriber	Transport Security determination of Subscriber	Authenticator Actions
N/A	N/A[note]	Use Challenge/Response
N/A	Match	OK
N/A	Different	Use Challenge/Response
Match	N/A	OK
Match	Match	OK
Match	Different	Use Subscriber identity from Network Source Address
Different	N/A	Use Challenge/Response
Different	Match	Use Subscriber identity from Transport Security Association
Different	Different	Use Challenge/Response

[Note] N/A means Not Applicable

If the resulting action is to use a challenge/response, the procedures of section 8.4.4 are followed.

Besides the strategy described in sections 8.4.2 through 8.4.4, the Generic Bootstrapping Architecture (GBA) can also be used for Identification and Authentication of Subscribers. It is described in section 8.4.5.

The authentication strategies described in this document are typical examples, and each NGN provider may select which of these other strategies to use (e.g., using just one procedure described in the following clauses.)

8.4.2 Identification of the Subscriber through Network Source Address

This is the simplest form of subscriber identification, based solely on the source address provided with the IP packets. The Authenticator consults a pre-provisioned mapping of IP address ranges to <Subscriber Account Identifier>, and if the source address of the request is within one of these ranges, the Authenticator considers the request to be originated from that subscriber. The <Subscriber Account Identifier> is then used to obtain the subscriber credentials through the SAA/TAA-FEs and check for consistency with the value of the "From" header.

If the value of the "From" header is consistent with the subscriber, then it is considered a "Match"; if the value of the "From" header is not consistent with the subscriber, then it is considered "Different"; if the source IP address is not contained in any of the pre-provisioned address ranges, then it is considered "N/A".

The strength of this method of subscriber identification depends on providing Source-Address Assurance. The Source-Address Assurance means that the IP address can be used only by the legitimate subscriber to whom the address is assigned. To achieve this, the following two mechanisms are necessary for transport-processing or transport-control FEs, and they must be properly coordinated: 1) strict management of a mapping between a subscriber and his/her assigned address, and 2) prevention of address spoofing based on this managed information. See Appendix A for examples of the above mechanisms and their coordination.

8.4.3 Identification of the Subscriber through TLS/IPsec Security Association

If a secure TLS transport was established for the signalling traffic between the originating device and the Authenticator, and that secure transport was authenticated with a X.509 TE-BE certificate (see section 8.3.2), the Authenticator checks that the “From” header is consistent with the allowed values for the subscriber identified in the <Subscriber Account Identifier>..

If a secure transport (either IPsec or TLS) was established for the signalling traffic between the originating device and the Authenticator, and that secure transport was authenticated with a X.509 TE NGN device certificate (see section 8.3.1 and 8.3.2), then if the device has been associated with a subscriber), the Authenticator utilizes the Device Manufacturer and Device Serial Number to determine the associated <Subscriber Account Identifier> . The <Subscriber Account Identifier> is used to obtain the subscriber credentials and those credentials are checked for consistency with the value in the “From” header.

If a secure transport (either IPsec or TLS) was established for the signalling traffic between the originating device and the Authenticator, and that secure transport was authenticated with a X.509 TE NGN subscriber certificate (see section 8.3.1and 8.3.2) then the Authenticator utilizes the <Subscriber Account Identifier> to obtain the subscriber credentials through the SAA/TAA-FEs. The Authenticator then checks for consistency between the subscriber credentials and the value in the “From” header.

If a secure transport (either IPsec or TLS) was established for the signalling traffic between the originating device and the Authenticator, and that secure transport was authenticated with a X.509 TE NGN End-User certificate (see section 8.3.1 and 8.3.2), then the Authenticator utilizes the <Subscriber Account Identifier> to obtain the subscriber credentials through the SAA/TAA-FEs. The Authenticator then checks for consistency between the subscriber credentials and the value in the “From” header.

If a secure transport (either IPsec or TLS) was established for the signalling traffic between the originating device and the Authenticator, and that secure transport was authenticated with a pre-shared key (see section 9.2.4.3.1), the Authenticator utilizes the Key Name to obtain the subscriber credentials through the SAA/TAA-FEs. The Authenticator then checks for consistency between the subscriber credentials and the value in the “From” header.

If a secure transport was not used between the originating device and the Authenticator, or an “anonymous client” TLS connection was used, then this method is “N/A”.

8.4.4 Identification of the Subscriber through Challenge/Response

Challenge/response is a more secure version of the old style userid/password scheme (i.e. sending of a user identification and password as part of a request for service, and the problem being that it was easily replayed to obtain fraudulent service later). In a challenge/response scheme, the server sends a challenge to the client, asking the client to perform some encryption task using a shared key. The result of that calculation is included in the response, which is then verified by the server. If the exchange were intercepted by others, it cannot be replayed as long as the server never reuses an old challenge.

There is one important type of the challenge-response methods that combines convenience of the password-based authentication methods and security of the methods that are based on the challenge-response scheme. The Password Authenticated Key (PAK) Exchange protocol, presents this type. The PAK protocol ensures mutual authentication of both parties in the act of establishing a symmetric cryptographic key via Diffie-Hellman exchange. The use of Diffie-Hellman exchange ensures the *Perfect Forward Secrecy* – a property of a key establishment protocol that guarantees that compromise of a session key or long-term private key after a given session does not cause the compromise of any earlier session**.** In addition**,** the PAK authentication method protects the exchange from *man-in-the-middle* attacks. The authentication relies on a pre-shared secret, which is protected (i.e., remains unrevealed) to an eavesdropper preventing an off-line dictionary attack.

Thus, the protocol can be used in a wide variety of applications where pre-shared secrets based on the possibly weak password exist. The PAK protocol is specified in [ITU-T X.1035] and [b-TIA 683-D].

A challenge/response involves an additional message exchange between the Authenticator and the originating endpoint, and a calculation done by the originating endpoint. It therefore may have an impact on the delay perceived by the user. It is the goal of the NGN Security to use a challenge/response only when absolutely necessary to achieve the necessary level of identification and authentication.

If a secure transport connection (either IPsec or TLS) was established for the signalling traffic between the originating device and the Authenticator, and a previous request within a configurable time period with the same “From” header contents was successfully authenticated by the Authenticator, then the authentication is considered successful and the request is accepted. In the case of call setup signalling, since the typical first request over a new connection is a “Register”, this challenge/response will be done at a time that will not affect call setup delay.

Since authentication requests are computationally-intensive, it is essential that the Authenticator limit the frequency of queries to the SAA/TAA-FEs. The limits defined in this paragraph may be followed whether the SAA/TAA-FEs is an integral part of the Authenticator or if it is a separate element. A simple Denial-of-Service attack is for an endpoint to simply flood the Authenticator with incorrect requests – if each requires a cryptographic calculation in the SAA/TAA-FEs then service is essentially delayed or halted for all (valid and invalid) requests. To counter such attacks, the Authenticator may locally reject a request if there is a pending authorization request from the same endpoint. A slightly more complex variant of this is for the Authenticator to locally reject a request if there have been at least XXX total requests within the past YYY seconds (both XXX and YYY values to be configurable in the Authenticator). In addition, the Authenticator may deliberately wait a configurable period of time before responding to a failed authorization request. This also weakens various kinds of “password cracking” attacks.

8.4.4.1 Challenge/Response with SIP signalling from originating device

If the originating device is using the SIP signalling protocol, then the Proxy-Authenticate mechanisms defined in [b-IETF RFC3261] can optionally be used to implement a challenge/response. See section 22.2 of [b-IETF RFC3261], section 3 of [b-IETF RFC2617], and section 3 of [b-IETF RFC3310].

The Authenticator responds to the SIP request with a 407 (Proxy-Authentication-Required) response. In this response it includes a Proxy-Authenticate header with: Authentication Scheme of “Digest”, Realm of “NGN .ngn.net”, qop of “auth”, Nonce of a cryptographically random 16-octet value (in hex), optionally a value of the “Opaque” parameter, and Algorithm of “MD5” or “AKAv1-MD5” depending on service agreement with the Customer.

An example of a Proxy-Authenticate header in a 407 response is:

> Proxy-Authenticate: Digest realm=“NGN .ngn.com", qop="auth",
> nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", stale=FALSE, algorithm=MD5

The originating device responds to the 407 with a regenerated request, containing a Proxy-Authentication header. This header is verified to contain the following information: Authentication scheme of “Digest”, Realm identical to that in the 407 response, Nonce identical to that in the 407 response, and Opaque identical to that in the 407 response. In addition, the Proxy-Authentication header includes a “Username” parameter giving the key name, a “Uri” parameter matching the Request-URI of the request, and a “Response” parameter being the hash as specified in [b-IETF RFC2617] or [b-IETF RFC3310].

An example of a Proxy-Authorization header in a re-issued request is:

Proxy-Authorization: Digest username="bob", realm="NGN .ngn.com",
nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", uri="sip:5551212@ngn.com",
response="dfe56131d1958046689d83306477ecc"

The "User-to-User Authentication" mechanisms defined in [b-IETF RFC3261] may also be used to implement a challenge/response. See section 22.2 of [b-IETF RFC3261], section 3 of [b-IETF RFC2617], and section 3 of [b-IETF RFC3310] for details.

If a request is forked, various NGN NEs (e.g. MGC-FE) and/or TEs may wish to challenge the originating device. The forking NE (e.g. S-CSC-FE) aggregates these challenges and places them into a single response that is sent by the forking NE to the originating device. When receiving the response that contains multiple challenges, the originating device supplies multiple credentials in a request and resubmits it.

8.4.4.2 Challenge/Response with signaling other than SIP from originating device

If the originating device is expected to use SIP, but issues its request using a signalling protocol other than SIP, then the challenge/response is considered to have failed. The request is rejected.

8.4.5 Generic Bootstrapping Architecture (GBA)

The Generic Bootstrapping Architecture (GBA) specifies an access-independent bootstrapping procedure. It provides a framework for mutual authentication of End-Users and Network Application Function (NAF) that can be used for identification and authentication of subscribers in the NGN. Refer to [b-ETSI TS133220] for information on GBA.

8.5 Identification and Authentication of End-Users

8.5.1 General Strategy

While identification of the subscriber is absolutely required for the NGN infrastructure, identification of the end-user is an optional service that may be requested by the subscriber or required by the service. Typically this would be to provide additional services, e.g. personal mobility and presence, where the identity of the requesting user is required to enable the service. If a subscriber desires this additional level of identification, it is necessary that all the relevant endpoint devices support the ability to enter additional end-user credentials or to use an end-user instead of a subscriber certificate.

Two methods exist for the Authenticator to identify and authenticate the end-user. The first is through the transport level security association used for the signalling exchange. If that security association was established with an end-user certificate (or a pre-shared key associated with a single end-user), then the end-user identification is complete. The second method is through a challenge/response, where the key name given in the response is associated with a single end-user. These two methods are described further in the following sections.

Advanced NGN devices may have multiple identifiers, e.g. a subscriber certificate and also one or more end-user certificates for the person(s) currently using the device. Such a device would create multiple TLS connections to the Authenticator, one separate connection for each certificate. The device would then send requests to the Authenticator over the appropriate signalling connection based on the desired identity for the call.

There is a concern about credentials for a single user being valid long after the user has "left". If the transport security association was based on an end-user certificate, the subscriber may require continuous activity to maintain the validity of the authentication. Without such activity, the Authenticator closes the secure transport connection, and requires the originating device to re-

establish it with the current end-user certificate (or subscriber certificate or device certificate if no end-user certificate is available). The detailed requirements for this behaviour of Authenticator are given in section 9.1.2 and 9.2.4.3.1, and are based on two timers: one that limits the absolute amount of time for which end-user credentials can be valid for a security association, and the second that limits the idle time between successive requests. Timeout values may be provisioned per subscriber or per end-user, but have to be limited by the maximum values set by the NGN provider.

8.5.2 Identification of the End-User through TLS/IPsec Security Association

If a secure TLS transport was established for the signalling traffic between the originating device and the Authenticator, and that secure transport was authenticated with a X.509 TE-BE certificate (see section 8.6), the Authenticator verifies that the “From” header is consistent with the allowed values for the subscriber identified in the <Subscriber Account Identifier> contained in the certificate.

If a secure transport (either IPsec or TLS) was established for the signalling traffic between the originating device and the Authenticator, and that secure transport was authenticated with a X.509 TE NGN End-User certificate (see section 8.6), then the Authenticator utilizes the <Subscriber Account Identifier> to obtain the subscriber credentials through the SAA/TAA-FEs. The Authenticator then checks for consistency between the subscriber credentials and the value in the “From” header If a secure IPsec transport was established for the signalling traffic between the originating device and the Authenticator, section 8.44 and that secure transport was authenticated with a pre-shared key (see section 9.2.4.3.1), the Authenticator utilizes the Key Name to obtain the subscriber credentials through the SAA/TAA-FEs., The Authenticator then checks for consistency between the subscriber credentials and the value in the “From” header. Identification of the End-User through Challenge/Response.

The challenge/response procedures for identification of an end-user are identical to those used to identify the subscriber, as given in section 8.4.4.

The only extension is that the Authenticator checks the information retrieved through the SAA/TAA-FEs for the key name for an indication that the key is associated with an end-user. If so, then the end-user identification is successful.

If the Authenticator had already done a challenge/response to identify the subscriber, and the named key returned in the response did not identify an end-user, then the end-user identification fails. If a challenge/response was not needed to identify the subscriber, a challenge is issued now.

8.6 Identification and Authentication by TE-BE

The identification and authentication procedures performed by a TE-BE are identical to those performed by an Authenticator with two differences:

1. The TE-BE may be provisioned with all the credentials needed to identify and authenticate the subscriber(s) and end-users that it serves, since it has no access to the distributed SAA/TAA-FEs function available to an Authenticator.
2. The request re-issued in response to a challenge from the Authenticator, containing the “Proxy-Authorization” header, is passed to the Authenticator rather than processed at the TE-BE.

8.6.1 Use of X.509 Certificates

There is a security association between every TE-BE and at least one NBE, established with the X.509 certificate issued to the TE-BE. Requests received at the NBE follow the identification and

authentication procedures given in section 8.4.3, which result in minimal verification of the identification performed by the TE-BE. When a challenge/response is needed (e.g. for a “roaming” user), the exchange will be between the originating endpoint and the NBE, and transparently passed through the TE-BE.

A secure transport between the end-point and the TE-BE is optional. It is anticipated that the network source address will adequately identify most requests.

End-points register to the NBE via TE-BE.

8.7 Authenticator-SAA/TAA-FEs Interface

8.7.1 Use of RADIUS and its extensions

The SAA/TAA-FEs contains the decision point and the SUP/TUP-FEs are the repositories for all end-user and device credentials in the NGN infrastructure. Some SAA/TAA-FEs functions, like authentication, may be distributed in order to optimize authentication request performance.

Two competing choices are commonly used for the protocol for Authenticator to SAA/TAA-FEs communication. RADIUS [b-IETF RFC2865] (well-known and well-supported) and Diameter [b-IETF RFC3588] (defined to fix several deficiencies of RADIUS). It is the eventual goal of the NGN infrastructure to migrate to Diameter; however it is recognized that current implementations of servers are based on RADIUS, and that numerous ad hoc extensions of the basic RADIUS protocol have been developed to meet the needs of this authentication function. While this release of this standard is based on RADIUS with the extension described in [b-IETF RFC5090], a future release of this standard will likely change this interface to be based on Diameter with the extension described in [b-IETF RFC4740].

The Authenticator becomes a RADIUS client, and the SAA/TAA-FEs server becomes a RADIUS server, as defined in [b-IETF RFC2865]. Both may implement the extensions for SIP Digest Authentication, as given in [b-IETF RFC5090]. The connection between the Authenticator and SAA/TAA-FEs server may be secured with IPsec with mutual authentication.

With the [b-IETF RFC4590] extensions, the Authenticator makes a RADIUS request with the parameters from the Proxy-Authentication header; the RADIUS server calculates the expected response and returns it to the Authenticator. The Authenticator then validates the request by comparing the actual response from the endpoint to the expected response.

An example of the message sent from the Authenticator to the SAA/TAA-FEs server is:

Code = 1 (Access-Request)

Identifier = 1

Length = 164

Authenticator = 56 7b e6 9a 8e 43 cf b6 fb a6 c0 f0 9a 92 6f 0e

Attributes:

NAS-IP-Address = d5 89 45 26 (213.137.69.38)

NAS-Port-Type = 5 (Virtual)

User-Name = “bob"

Digest-Response (206) = "2ae133421cda65d67dc50d13ba0eb9bc"

Digest-Attributes (207) = [Realm (1) = “NGN .ngn.com"]

Digest-Attributes (207) = [Nonce (2) = " ea9c8e88df84f1cec4341ae6cbe5a359 "]

Digest-Attributes (207) = [Method (3) = "INVITE"]

Digest-Attributes (207) = [URI (4) = " sip:5551212@ngn.com "]

Digest-Attributes (207) = [Algorithm (5) = "md5"]

Digest-Attributes (207) = [User-Name (10) = “bob"]

An example of the response sent from the SAA/TAA-FEs server to the Authenticator is:

Code = 2 (Access-Accept)

Identifier = 1

Length = 20

Authenticator = 6d 76 53 ce aa 07 9a f7 ac b4 b0 e2 96 2f c4 0d

Attributes:

Digest-Response (206) = "dfe56131d1958046689d83306477ecc"

8.7.2 Transport Signalling Security Association

When an X.509 Certificate is used in the establishment of the transport signalling security association, the SUP/TUP-FEs stores (indexed by the <Subscriber Account Identifier>) the set of acceptable “From” headers that may appear in requests from that source, which will be matched against the “From” header provided in the request.

If a pre-shared key is used in the establishment of the transport signalling security association (e.g. peering service provider), then the SUP/TUP-FEs stores (indexed by the Key name) the set of acceptable “From” headers that may appear in requests from that source, which will be matched against the “From” header provided in the request.

8.8 Identification and Authentication of bearer traffic

There are times when it is desirable to identify individual bearer traffic flow for security enhancement, for example, to counter fraudulent attacks such as spoofing or RTP injection. In the NGN, the bearer traffic can be identified by a quintuple that contains

- source IP address,
- destination IP address,
- source port,
- destination port, and
- protocol number.

The identification mechanism described in this section uses this identifier for authentication of every packet. The mechanism is based on a shared secret and the use of the cryptographic hash function, keyed-Hash Message Authentication Code (HMAC). See [b-NIST FIPS 198] for information.

The entities involved in the process of authentication – the End-User Function and the Access Node FE – are described in [ATIS-1000029] and [ITU-T Y.2701] and are depicted in Figure 3 using the UNI as an example.

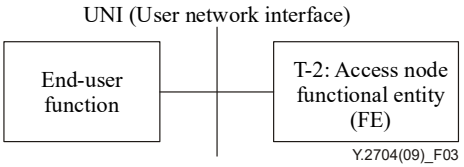

Figure 3 - NGN Entities involved in authentication procedure – UNI example.

The description of the mechanism uses the following conventions:

- *F* is a identifier (quintuple) of bearer traffic
- *K* is a shared secret that both the End-User Function and the Access Node FE possess
- *P* is a packet that the End-User Function intends to send to the Access Node FE
- *i* is a sequence number of a packet that is being incremented by both communicating parties. It is a 64-bit value.
- *t* is a time stamp - a 64 bit value that indicates time in seconds. Alternatively it could be a nonce.
- *(P', Q)* is a packet that the Access Node FE has received

When the End-User Function intends to send a packet *P* to the Access Node FE, it first computes a quantity *H(F, t+i, K)*, which is a hash function of a concatenation of *F*, *t+i,* and *K*, and then attaches this quantity to the packet *P.* Therefore, the full packet sent from the End-User Function to the Access Node FE is *[P, H(F, t+i, K)].* When the Access Node FE receives a packet *(P', Q)*, it computes the quantity *H(F, t+i, K).* If a time stamp is used, the Access Node FE computes the hashes for all values of *t* that are in the agreed upon range for the difference between the times on the End-User Function and the Access Node FE (this needs to be done only once at the beginning of a session). In this case the Access Node FE looks for a match between *Q* and any one of the computed values of hashes. If a match is found then the packet is authenticated. The corresponding value of *t* will be used for the packets of the flow.

If a nonce is used, then the Access Node FE simply checks whether the computed value of the hash is equal to *Q*. If it is, the packet is authenticated.

In an environment where packet loss may occur, simply incrementing i from packet to packet may not suffice. In this case, the Access Node FE may search from i through i+d (where d is a small number) to resynchronize i.

The use of this authentication mechanism helps counter fraudulent attacks such as spoofing or RTP injections.

The mechanism also allows for authentication of the user-generated traffic without revealing the user's identity.

For this implementation, it is suggested for the End-user function and the Access node FE to agree on the format of identifier F, shared secret K, hash function H, exact synchronized time to start time stamp t, where the hashed quantity can be added to the packet P and how, the value of d, and what starts to resynchronize i.

The use of this mechanism is a subject of a network operator's security policy. There are other mechanisms that can be used for authenticating the flows, e.g., IPsec. The advantage of this mechanism in comparison to IPsec is that while IPsec requires encryption of the entire IP packet (in the tunnel mode), or the payload (in the transport mode), this mechanism requires computation only of the hash *H(F, t+i, K),* which can be done faster and using less computing resources.

9 Transport security for signalling and OAMP

Transport security is used in the NGN infrastructure to provide confidentiality and integrity guarantees of the signalling data and the OAMP messages. This section specifies the profile of TLS and IPsec to be used by the NGN infrastructure network elements as two important security mechanisms. The lists of mechanisms are not exhaustive and other implementations may be adopted depending on the NGN provider policies.

Within the Trusted Zone and Trusted-but-Vulnerable Zone, VPN tunnel (e.g., IPsec or TLS) is required for securing the OAMP messages. Section 9.1 gives the profile for TLS use cases, and Section 9.2 gives the corresponding profile for IPsec use cases. Between the TE-BE and OAMP-NBE (i.e. between the Untrusted Zone and Trusted-but-Vulnerable Zone), IPsec is used for creating a VPN tunnel. Section 9.3 gives the applicable profile of IPsec.

While media security is not required within the NGN infrastructure, some Border elements implement media security for service to specific endpoints. For these elements, a later section contains a profile of media security protocols.

9.1 TLS

In the NGN infrastructure, TLS is often used to secure various types of signalling traffic (e.g. SIP, COPS, TRIP, HTTP) between network elements within the trusted zone. It is also supported in Border Elements that might receive encrypted signalling from customer endpoints, and by the TE-BE for communicating to a NBE. Specific requirements for each type of network element are given in [ATIS-1000029] and [Y.2701].

The TLS protocol is defined in [IETF RFC5246]. It provides privacy and data integrity over a reliable transport layer protocol such as TCP or SCTP.

Unless specified otherwise in this section, it is desirable that NGN infrastructure network elements requiring TLS be compliant with the TLS specification [IETF RFC5246] and any requirements specified in [IETF RFC3261] relating to its usage in SIP. While TLS supports the negotiation and use of compression methods, compression may NOT be used within the NGN infrastructure, due to performance degradation.

9.1.1 Cipher suites

The cipher suite includes the authenticated key agreement method used in the TLS handshake, as well as encryption and authentication ciphers used to secure the record layer. Cipher suites are negotiated with the TLS client presenting a list of supported cipher suites in the Client Hello message, and the server responding with the selected cipher suite in the Server Hello message.

There are many factors influencing the choice of encryption algorithm. Example common factors influencing the choice of encryption algorithm includes:

1. Required security
   - Value of the data (to either the organization and/or other entities—the more valuable the data, the stronger the required encryption)
   - Time value of data (if data is valuable but for only a short time period [e.g., days as opposed to years], then a weaker encryption algorithm could be used)
   - Threat to data (the higher the threat level, the stronger the required encryption)

- Other protective measures that are in place and that may reduce the need for stronger encryption—for example, using protected methods of communications, such as dedicated circuits as opposed to the public Internet

2. Required performance (higher performance requirements may require procurement of additional system resources, such as a hardware cryptographic accelerator, or may necessitate weaker encryption)
3. System resources (fewer resources [e.g., process, memory] may necessitate weaker encryption)
4. Import, export, or usage restrictions
5. Encryption schemes supported by network elements
6. Encryption schemes supported by user devices.

Table 3 shows a list of candidate cipher suites suitable for NGN, though the table is not exhaustive.

Table 3 - Candidate cipher suites for NGN

Cipher suite name	Reference	Key exchange	Cipher	Hash
TLS_RSA_WITH_AES_128_CBC_SHA	b-IETF RFC 5246	RSA	AES-128 in CBC mode	SHA-1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman Ephemeral mode with RSA signatures	AES-128 in CBC mode	SHA-1
TLS_RSA_WITH_3DES_EDE_CBC_SHA	b-IETF RFC 2246	RSA	3DES in CBC mode	SHA-1
TLS_DHE_WITH_3DES_EDE_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman Ephemeral mode with RSA signatures	3DES in CBC mode	SHA-1
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	b-IETF RFC4132	RSA	Camellia-128 in CBC mode	SHA-1
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	b-IETF RFC4132	Diffie-Hellman Ephemeral mode with RSA signatures	Camellia-128 in CBC mode	SHA-1

The cipher suits in Table 4 depicted from [b-IETF RFC5246], [b-IETF RFC4132] and [b-IETF RFC 4492] can also be optionally be used by any NEs.

Table 4 - Candidate cipher suites (optional) for NGN

Cipher suite name	Reference	Key Exchange	Cipher	Hash
TLS_DH_DSS_WITH_AES_128_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman with DSS signature	AES-128 in CBC mode	SHA-1
TLS_DH_RSA_WITH_AES_128_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman with RSA signature	AES-128 in CBC mode	SHA-1
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman Ephemeral mode with DSS signature	AES-128 in CBC mode	SHA-1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman Ephemeral mode with RSA signatures	AES-128 in CBC mode	SHA-1
TLS_RSA_WITH_AES_256_CBC_SHA	b-IETF RFC 5246	RSA	AES-256 in CBC mode	SHA-1
TLS_DH_DSS_WITH_AES_256_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman with DSS signature	AES-256 in CBC mode	SHA-1
TLS_DH_RSA_WITH_AES_256_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman with RSA signature	AES-256 in CBC mode	SHA-1
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman Ephemeral mode with DSS signature	AES-256 in CBC mode	SHA-1
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman Ephemeral mode with RSA signatures	AES-256 in CBC mode	SHA-1
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman with DSS signature	Camellia-128 in CBC mode	SHA-1
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman with RSA signature	Camellia-128 in CBC mode	SHA-1
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman Ephemeral mode with DSS signature	Camellia-128 in CBC mode	SHA-1
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	b-IETF RFC 4132	RSA	Camellia-256 in CBC mode	SHA-1
TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman with DSS signature	Camellia-256 in CBC mode	SHA-1
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman with RSA signature	Camellia-256 in CBC mode	SHA-1
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman Ephemeral mode with DSS signature	Camellia-256 in CBC mode	SHA-1
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman Ephemeral mode with with RSA signatures	Camellia-256 in CBC mode	SHA-1
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman with ECDSA signature	3DES in CBC mode	SHA-1
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman with ECDSA signature	AES-128 in CBC mode	SHA-1
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman with ECDSA signature	AES-256 in CBC mode	SHA-1
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman Ephemeral mode with ECDSA signature	3DES in CBC mode	SHA-1
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman Ephemeral mode with ECDSA signature	AES-128 in CBC mode	SHA-1
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman Ephemeral mode with ECDSA signature	AES-256 in CBC mode	SHA-1

Cipher suite name	Reference	Key Exchange	Cipher	Hash
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman with RSA signature	3DES in CBC mode	SHA-1
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman with RSA signature	AES-128 in CBC mode	SHA-1
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman with RSA signature	AES-256 in CBC mode	SHA-1
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman Ephemeral mode with RSA signature	3DES in CBC mode	SHA-1
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman Ephemeral mode with RSA signature	AES-128 in CBC mode	SHA-1
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman Ephemeral mode with RSA signature	AES-256 in CBC mode	SHA-1

Note: RC-4 is a popular and well used cipher. However, it is not included in the above list because it is not an open standard.

Note: Elliptic Curve Cryptography (ECC) is a public-key cryptosystem that may be desirable for certain applications in NGN. Specifically, ECC would be appealing for certain applications because of efficiency benefits. Compared to other prevalent cryptosystems such as RSA, ECC offers equivalent security with significantly smaller key sizes. In addition, ECC offers computational efficiency and advantages over certain other public key techniques achieve the same level of protection.

9.1.2 TLS Use of Certificates

TLS is a client-server based protocol with optional client authentication. However, within the Trusted Zone of the NGN infrastructure, and between the Trusted Zone and the Trusted-but-Vulnerable Zone, mutual authentication may be accomplished using TLS. In that case the TLS server sends a Certificate Request to the Client. If a client in the Trusted Zone or Trusted-but-Vulnerable Zone does not provide a client certificate, then the connection request may be rejected by the server. Both the TLS client and server certificates should conform to the NGN infrastructure certification specifications given in section 8.3. Certificates may be verified as specified in section 8.3. Before continuing with a TLS connection, the TLS server or client may validate the remote system matches its certificate.

Between the Trusted-but-Vulnerable Zone and the Untrusted Zone, the TLS server may send a Certificate Request to the Client. If the client has no certificate, it responds with an empty Client Certificate message, and the session proceeds as an anonymous client.

When a NBE accepts an authenticated connection with an endpoint based on a NGN end-user certificate (see section 8.5.2), then the NBE may implement two timers on the connection. The first timer, T1, is started when the connection is established. The second timer, T2, is started when the connection is established and is reset to zero every time a request is received at the NBE over the connection. Whenever either timer reaches its limit value (which may depend on values contained in the certificate), the connection is reset by the NBE and will be re-established by the endpoint to refresh the NGN end-user certificate.

9.1.3 Session Key Management

TLS sessions between NGN infrastructure network elements are expected to be long-lasting. It is therefore important that the session keys be changed periodically. Session keys for TLS sessions may be changed after a configurable period of time.

9.2 IPsec in Trusted and Trusted-but-Vulnerable Zones

In the NGN infrastructure IPsec may be used to secure various types of traffic (e.g. SNMP, RADIUS) between network elements within the trusted zone. Specific requirements for each type of network element are given in [ATIS-1000029] and [ITU-T Y.2701].

As described generally in [b-IETF RFC4301], IPsec is composed of a number of different pieces. These can be used to provide confidentiality, integrity, and replay protection. Some of these can be configured manually, but in general a key management component is used. Additionally, the decision on the use of IPsec is typically controlled by a policy database. This section describes the mandatory-to-implement subset of the components of IPsec.

In network elements that use IPsec, it is recommended to ensure that TLS-secured connections are not run over IPsec.

Note: Network elements that use IPsec should ensure that media streams secured with SRTP or RC4 are not run over IPsec. This is to ensure that no double-encryption is done, which would be wasteful of NGN resources. It should also be noted that tunnelling of encryption may occur from the end user.

9.2.1 AH and ESP

The Authentication Header (AH), described in [IETF RFC4302, b-IETF RFC4835], and the Encapsulating Security Protocol (ESP), described in [IETF RFC4303], are the two choices of over-the-wire security protocols. Both optionally provide replay protection. ESP typically is used to provide confidentially, integrity, and authentication of traffic. ESP also can provide integrity and authentication without confidentiality. ESP can also be used to provide confidentiality alone. AH protects portions of the preceding IP header, including the source and destination address. AH can also protect those IP options that need to be seen by intermediate routers, but is required to be intact and authentic when delivered to the receiving system, though use of such IP options is extremely rare.

NGN infrastructure network elements may support the Encapsulating Security Protocol (ESP), as defined in [IETF RFC4303]. ESP_DES (both 40 and 56 bits), ESP_3DES, ESP_AES [b-IETF RFC3602], and ESP_CAMELLIA [b-IETF RFC4312] may be supported in Cipher Block Chaining (CBC) mode. Network Elements that support ESP_NULL may NOT use ESP_NULL when communicating with another NGN infrastructure network element. The actual encryption algorithm used within ESP is negotiated during key management.

All implementations of ESP are required by [b-IETF RFC4301] to support the concept of Security Associations (SAs), and [b-IETF RFC4301] provides a general model for processing IP traffic relative to SAs. Although particular IPsec implementations need not follow the details of this general model, the external behaviour of any IPsec implementation may match the external behaviour of the general model. This ensures that components do not accept traffic from unknown addresses and do not send or accept traffic without security (when security is required). NGN infrastructure network elements that implement IPsec may provide behaviour that matches the general model described in [b-IETF RFC4301].

9.2.2 Transport and Tunnel Mode

Both AH and ESP can be used in either transport mode or tunnel mode. In tunnel mode, the IPsec header is followed by an inner IP header. This is the normal usage for Virtual Private networks (VPNs), and is generally required when either end of the IPsec-protected path is not the ultimate destination, e.g. when IPsec is implemented in a firewall, or router. Transport mode is preferred for point-to-point communication.

NGN infrastructure network elements may support IPsec in Transport Mode.

9.2.3 Replay Protection

NGN infrastructure network elements may use the IPsec optional replay-protection service (anti-replay service). Within NGN infrastructure network elements, the IPsec anti-replay service may be turned on at all times. An IPsec sequence number outside of the current anti-replay window is flagged as a replay and the packet is rejected. When the anti-replay service is turned on, an IPsec sequence number cannot overflow and roll over to 0. Before that happens, a new Security Association should be created as specified in [IETF RFC4303].

9.2.4 Key Management

All cryptographic systems require key management. While IPsec provides for both manual and automatic key management schemes, manual schemes don't scale as well as automatic schemes and do not offer replay protection. All key management schemes provide authentication. NGN infrastructure network elements should implement one of the automated key exchange mechanisms described in this section.

When IKE is not used for key management, an alternative key management protocol needs an interface to the IPsec layer in order to create/update/delete IPsec Security Associations. IPsec Security Associations may be automatically established or re-established as required. This implies that the IPsec layer also needs a way to signal a key management application when a new Security Association needs to be set up (e.g. the old SA is about to expire or there is no SA on a particular interface). In addition, some Border Elements may be required to run multiple key management protocols (e.g. IKE for securing connections for OAMP, and PKINIT for securing connections). In these cases the PF_KEY [b-IETF RFC2367] interface is recommended to be used.

9.2.4.1 Transform Identifiers

The IPsec Transform Identifier is used by the key management procedures to negotiate an encryption algorithm that is used by ESP in IPsec. The transform identifier is also used by IKE to secure its phase-1 and phase-2 messages. A list of available IPsec transform identifiers is given in [b-IETF RFC5282]. Within the NGN infrastructure, the transform IDs ESP_3DES (value 0x03, with key size of 192 bits, CBC mode) and ESP_CAMELLIA (value 0x16, with 128 bits key, CBC mode) [b-IETF RFC4312] may be supported. The Transform ID ESP_AES (value 0x0C, with 128 bit key, CBC mode) is recommended to be supported. IKE allows negotiation of the encryption key size, so if in the future it is desired to increase the key size for one of the above algorithms, IKE will use this built-in function.

For all of these transforms the CBC Initialization Vector (IV) is carried in the clear inside each ESP packet payload [b-IETF RFC2451]. AES-128, defined in [b-NIST FIPS197, b-IETF RFC3602] may be used in CBC mode with a 128-bit block size and a randomly generated Initialization Vector. AES-128 requires 10 rounds of cryptographic operations [b-IETF RFC3602]. Camellia-128, defined in [b-IETF RFC3713 and b-IETF RFC4312] may be used in CBC mode with a 128-bit block size and a randomly generated Initialization Vector. It requires 18 rounds of cryptographic operations [b-IETF RFC3713]

9.2.4.2 Authentication Algorithms

The IPsec Authentication Algorithm is used by the key management procedures to negotiate a packet-authentication algorithm that is used. A list of available IPsec authentication algorithms is given in [b-IETF RFC5282]. Within the NGN infrastructure, the authentication algorithms HMAC-

MD5-96 (value 0x01, key size of 128 bits, defined in [b-IETF RFC2403]) and HMAC-SHA-1-96 (value 0x02, key size 160 bits, defined in [b-IETF RFC4835]) may be supported.

9.2.4.3 Internet Key Exchange (IKE)

One automated key exchange mechanism is described in [b-IETF RFC2409], and is known as IKE. IKE key management is completely asynchronous to data messages and does not contribute to any delays during communications setup. The only exception would be some unexpected error, where the Security Association is unexpectedly lost by one of the endpoints.

IKE is a peer-to-peer key management protocol. It consists of two phases. In the first phase, a shared secret is negotiated via a Diffie-Hellman key exchange. It is then used to authenticate the second IKE phase. The second phase negotiates another secret, used to derive keys for the IPsec ESP protocol.

9.2.4.3.1 First IKE Phase

Three different modes are defined for authentication during the first IKE phase. IKE authentication with Public-Key Encryption SHALL NOT be used in the NGN infrastructure, as this requires the initiator to already know the responder's public key. IKE Authentication with Signatures and IKE Authentication with Pre-Shared Keys may be supported.

IKE defines specific sets of Diffie-Hellman parameters (i.e. prime and generator) that may be used for the phase 1 IKE exchange. The first group may be supported in NGN infrastructure network elements, and the remaining groups are recommended to be supported.

If IKE Authentication with signatures is used, both client and server may exchange X.509 certificates (see section 8.3.2). Certificates may be verified as specified in section 8.3.

When a Network Border Element accepts an authenticated connection with an endpoint based on a NGN end-user certificate, then the NBE may implement two timers on the connection. The first timer, T1, is started when the connection is established. The second timer, T2, is started when the connection is established and is reset to zero every time a request is received at the NBE over the connection. Whenever either timer reaches its limit value (which may depend on values contained in the certificate), the connection is reset by the NBE and will be re-established by the endpoint to refresh the NGN end-user certificate.

If IKE Authentication with Pre-Shared keys is used, a key derived by some out-of-band (e.g. manual) mechanism is used to authenticate the exchange. Implementations may allow a pre-shared key of at least 128 octets. Verification of the requirements for the pre-shared keys is not required in the network elements. Implementations may support Aggressive Mode, defined in Section 5.4 of [b-IETF RFC2409], and use the key name as the identity of the initiator/responder. The aggressive mode of IKE v1 [IETF RFC 2409] in combination with pre-shared-key is known to be insecure. With this mode, a hash of the secret is transmitted in clear over the network; if the IP traffic is intercepted by an attacker, then the key can be retrieve with an off-line brute force attempt. It is recommended that at least 128-bit long PSK shall be used to prevent the brute-force calculation of the PSK based on its hash.

When using pre-shared keys, the strength of the system is dependent upon the strength of the shared secret. The goal is to keep the shared secret from being the weak link in the chain of security. This implies that the shared secret needs to contain as much entropy (randomness) as the cipher being used. In other words, the shared secret is recommended to have at least 128-160 bits of entropy.

9.2.4.3.2 Second IKE Phase

In the second IKE phase, an IPsec ESP Security Association is established, including the ESP keys and ciphersuites. First, a shared second-phase secret is established, and then all the IPsec keying material is derived from it using the one-way function specified in [b-IETF RFC2409]. The second-phase secret is built from encrypted nonces that are exchanged by the two parties. Another Diffie-Hellman exchange is allowed by [b-IETF RFC2409] in addition to the encrypted nonces, but may NOT be used in NGN infrastructure network elements. This is to avoid the associated performance penalties.

9.3 Key agreement protocol between Untrusted and Trusted-but-Vulnerable Zone

The Key Agreement (AKA) protocol specified for IMS network may also be used as applicable. The Universal Mobile Telecommunications System (UMTS) Authentication and Key Agreement (AKA) protocol supports mutual authentication of the Mobile Station (MS) and the network. The UMTS AKA is a challenge-response protocol, which uses a long-term key K shared between Universal Subscriber Identity Module (USIM) and Authentication Center (AuC). These entities reside on the Universal Integrated Circuit Card (UICC) of the MS and in the mobile station's home network respectively. The AKA protocol is specified in 3GPP.33.102V710-2007, Security Architecture [b-3GPP.33.102V710-2007].

Although the AKA mechanism is typically used for authentication of the wireless devices that are equipped with the smart cards (e.g., UICC), there is nothing in the AKA specifications that would prevent the use of the mechanism for authentication of the fixed devices that are capable of running the USIM application.

9.4 IPsec between Untrusted and Trusted-but-Vulnerable Zone

The TE-BE is a NGN Network Element that resides in the Untrusted Zone. However, it is still managed by the NGN Carrier and needs access to the OAMP systems located within the Trusted Zone. Therefore there is a OAMP-SE that resides in the Trusted-but-Vulnerable Zone that acts as a relay point for the OAMP messages.

The TE-BE may ensure that TLS-secured connections are not run over the IPsec VPN Tunnel. The TE-BE may ensure that media streams that are secured with SRTP media Security are not run over the IPsec VPN Tunnel.

The IPsec VPN Tunnel may use IPsec ESP [IETF RFC4303] in Tunnel mode [b-IETF RFC4301].

The IPsec anti-replay service may be enabled at all times.

The IPsec VPN Tunnel may support Transform Identifiers ESP_3DES (with key size of 192 bits, in CBC mode) and ESP_CAMELLIA (with 128-bit key and CBC mode) [b-IETF RFC4312]. The IPsec VPN Tunnel is recommended to support Transform Identifier ESP_AES (with 128-bit key and CBC mode).

The IPsec VPN Tunnel may support Authentication Algorithms HMAC-MD5-96 (key size of 128 bits), and HMAC-SHA-1-96 (key size 160 bits).

Key generation and management for the IPsec VPN Tunnel may be done with IKE [b-IETF RFC2409], using IKE Authentication with Digital Signatures, or IKE authentication with a pre-shared key. If IKE authentication with Digital Signatures is used, both client and server may exchange X.509 certificates, and certificates may be verified.

10 Media Security

Media encryption is not required within the NGN infrastructure, but it may be required to be supported for customers that desire its use. Such support may include the support of media encryption protocols, SRTP [b-IETF RFC3711]. In the rest of this section Network Border Elements (i.e., the edge of the network provider's domain) are assumed to implement encryption/decryption although it is possible to do the same in a separate platform shared among NBEs. In either case, the encryption and decryption is required to be collocated with other media processing capabilities such as Dual-Tone Multi-Frequency (DTMF) detection and transcoding.

With the requirement to connect subscribers desiring media encryption on their access link with those that do not (or don't support it), there are five separate cases that need to be considered as shown in Figure 4.

The first and simplest case is where neither endpoint desires encryption. The media will flow from source to destination, through the border elements, without any encryption on any of the links. Neither Network Border Element (NBE)#1 (serving the originator) nor Network Border Element (NBE) #2 (serving the destination) does any encryption or decryption.

The second case occurs if the originator desires an encrypted media stream but the destination doesn't, NBE #1 acts as a encryption/decryption relay point. NBE #1 receives the encrypted stream from the originator, decrypts it and passes it through the NGN infrastructure to NBE #2, who passes it (still unencrypted) to the destination. In the reverse direction NBE #1 receives unencrypted media through the NGN infrastructure and encrypts it before sending it to the originator. Thus the media over leg#1 (from the originator to NBE #1) is encrypted, leg#2 (between NBE #1 and NBE #2) is not, and leg#3 (between NBE #2 and the destination) is not.

The third case occurs if the destination desires an encrypted media stream but the originator doesn't. NBE #2 acts as an encryption/decryption relay point. NBE#1 receives unencrypted media from the originator and passes it (still unencrypted) through the NGN infrastructure to NBE #2. NBE #2 encrypts it and passes it to the destination. In the reverse direction NBE #2 receives the encrypted media stream from the destination endpoint and decrypts it before forwarding through the NGN infrastructure. NBE #1 passes the unencrypted media to the originator. Thus the media over legs #1 and #2 are unencrypted, and the media over leg#3 is encrypted.

The fourth case occurs if the originator and destination both desire encrypted media, but either they do not support compatible encryption schemes or there is some enhanced service being provided by the NGN infrastructure (such as Dual-Tone Multi-Frequency (DTMF) detection for calling card applications). Both NBE #1 and NBE #2 act as encryption/decryption relay points. NBE #1 receives the encrypted stream from the originator, decrypts it and passes it through the NGN infrastructure to NBE #2. NBE #2 encrypts it and passes it to the destination. In the reverse direction, NNBE #2 receives encrypted media from the destination endpoint and decrypts it before forwarding through the NGN infrastructure. NBE #1 receives unencrypted media and encrypts it before sending it to the originator. Thus the media over legs #1 and #3 are encrypted, and the media through the NGN infrastructure (leg #2) is not.

The fifth case occurs if the originator and destination both desire encrypted media, support compatible encryption schemes, and there is no enhanced service being provided by the NGN infrastructure. NBE #1 receives encrypted media from the originator and passes it unchanged through the NGN infrastructure to NBE #2, who passes it unchanged to the destination. In the reverse direction NBE #2 receives encrypted media from the destination and passes it unchanged through the NGN infrastructure to NBE #1 who passes it unchanged to the originator. Thus the media over all three legs is encrypted. The signalling needed to achieve this case is beyond the scope of this document.

Media encryption described in this section provides authentication, confidentiality, and message integrity.

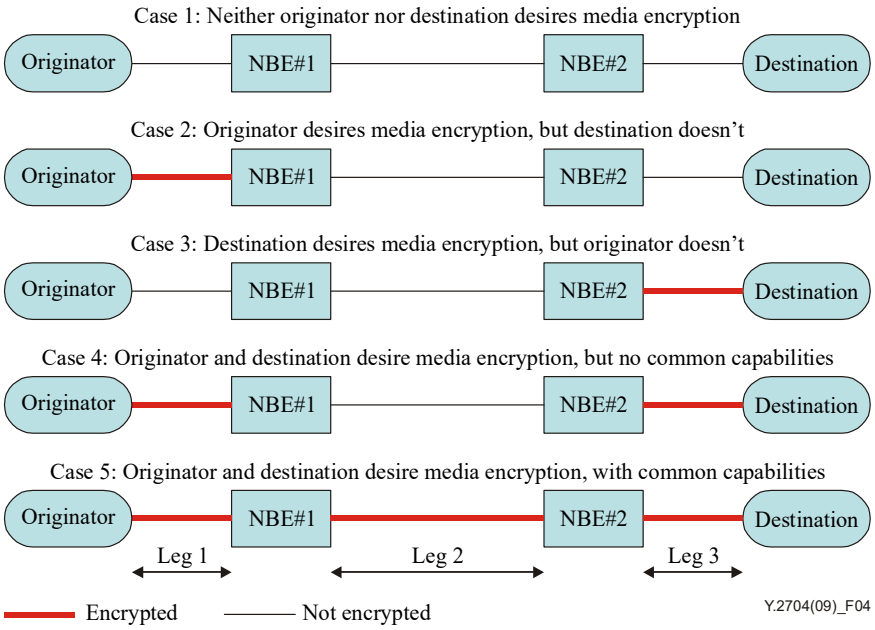

Figure 4 - The relationship of media encryption, BE's capabilities, and originator/destination's desire

10.1 SRTP

Secure RTP is described in [b-IETF RFC3711], and is defined as a profile of RTP [b-RFC3550]. It is intended to be implemented between the RTP application and the transport layer in the protocol stack – intercepting an RTP packet and forwarding an equivalent SRTP packet on the transmit side, and intercepting SRTP packet and passing equivalent RTP packet up the stack on the receiving side. It basically encrypts the payload of the RTP packet and adds an authentication tag to the end of the packet on the transmit side, and verifies the authentication tag and decrypts the payload on the receive side.

10.1.1 Encryption and Authentication Algorithms

An NBE supporting SRTP may support AES in Counter Mode [b-IETF RFC3711]. Also see [b-NIST FIPS SP 800-38a] for more information. The NBE may support HMAC-SHA1 for message integrity check generation, with tag length of 80 bits.

10.1.2 Cipher Suite Negotiation and Key Generation

Key generation for SRTP can be done in several ways: (1) via provisioning (via TE Provisioning Element), (2) by using key material generated by the endpoint device and included in Session Description Protocol (SDP) [b-IETF RFC4566] in the INVITE requests, (3) key material is exchanged using separate key management protocol and piggybacked with SDP.

For each subscriber, the NBE may obtain from the SAA/TAA-FEs the SRTP Master Key, and from this derive preliminary encryption and authentication session keys. An SRTP Master Key of length 128 may be supported. The key derivation algorithm described in [b-IETF RFC3711] may be supported. The preliminary encryption key length may be 128 bits, the preliminary session salt key length may be 112 bits, and the preliminary authentication key may be 160 bits. When a new SRTP Master key is issued to a subscriber, the NBE may be able to use it immediately.

NOTE: The term Master can be interpreted to have unfortunate connotations in current usage. This terminology has been used in the approved IETF References and is being retained solely to assist the reader in understanding the principles and when referring to the referenced text.

If the SDP contained in the INVITE request has “RTP/SAVP” as the media protocol value in the “m=” line, and no key value in a “k=” line, and no “a=crypto” attribute, then the NBE may use the preliminary keys generated from the provisioning system as the actual keys for the session. The cipher suite is not negotiable in this case.

If the SDP contained in the INVITE request has “RTP/SAVP” as the media protocol value in the “m=” line, and no “a=crypto” attribute, and a key value in a “k=” line, then the NBE may use the key contained in the “k=” line as the SRTP Master Key and generate the session and authentication keys from it. The cipher suite is not negotiable in this case.

If the SDP contained in the INVITE request has “RTP/SAVP” as the media protocol value in the “m=” line, and a “a=crypto” attribute, then the NBE may follow the requirements of [b-IETF RFC 4568] to generate the session and authentication keys. For example, the SDP entry “a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4” indicates the cipher-suite is AES_CM_128_HMAC_SHA1_80, and the key_param is defined by the text starting with “inline:”. Within the key_param, the first field is the master key appended with the master salt, concatenated and then base64 encoded. The list of valid cipher suites is given in section 5.2 of [b-IETF RFC 4568], from which one is chosen as part of the SDP offer/answer exchange.

If the SDP contained in the INVITE request has “RTP/SAVP” as the media protocol value in the “m=” line, and a “a=key-mgmt” attribute, then NBE may follow the requirements of [b-IETF RFC4567] to generate keys and security parameters. For example, “a=key-mgmt:mikey AQAFgM0XflABAAAAAAAAAAAAA...” indicates that the key management protocol is mikey [b-IETF RFC3830], and the remainder text is the key management data which is base64 [b-IETF RFC4648] encoded.

10.1.3 Authentication interface between NGN Network Element and Secure Token Server

NGN Network Elements may implement SASL [b-IETF RFC4422] protecting their OAMP functions. The SASL layer may include an authentication check based on Secure Token, as defined in [b-IETF RFC2808]. This is identified with the SASL key “Secure Token”. The user desiring OAMP access provides (1) an authorization identity (which allows system administrators to log in with a different user identity; if empty it defaults to the authentication identity), (2) an authentication identity (an identity whose passcode will be used), (3) the pin value of the user and 6-digit passcode on the Secure Token.

The NGN Network Element may implement an SAA/TAA-FE compliant client as part of the SASL handling of Secure Token. The NGN Network Element collects the presented user credentials and then sends them to the Secure Token server. Collected fields include the username, pin code, and currently-displayed Secure Token value. The Network Element receives back an Accept/Deny/Retry status message. If successful, the SASL enables the user to access the OAMP functions, based on the level of access associated with that username.

11 OAMP

An audit trail should be taken for all OAMP access attempts (whether successful or not), all OAMP changes made, and all OAMP signoffs. In addition, events considered significant by the NGN provider’s policy are logged.

In this section some mechanisms on important features are described. They are not exhaustive and other implementations may be adopted depending on the NGN provider policies.

Note: Security of event logging is necessary. For additional information refer to [ATIS-1000029], ATIS-0300276, [ITU-T Y.2701] and [ITU-T M.3016].

11.1 Network Element interface to Logging Systems

The Network Elements is recommended to send their logging information to a remote log host. Such elements that utilize the Syslog protocol [b-IETF RFC5424] to achieve this function may follow the requirements of this section.

Network Elements that utilize the Syslog protocol may include a timestamp, with the time based on the value received via SNTP/NTP from a trusted time source, and may give the timestamp in UTC. Elements may include their Hostname (if one has been provisioned) or their IP address in the syslog message header.

11.2 Network Element Use of SNMP

It is essential that the NGN Network Elements be able to be managed from a remote platform. SNMP is the industry standard mechanism to do this. While SNMPv3 [b-IETF RFC3413, b-IETF RFC3414, b-IETF RFC3415] solves many of the security faults present in SNMPv2, it is becoming increasingly widely available.

The Network Elements are recommended to send their logging information to a remote log host. Such elements may utilize the SNMP protocol to achieve this function, noting the caveats elsewhere in this document relating to SNMP v3.

SNMP is defined by an overall architecture [b-IETF RFC3411], the mechanism for naming objects and events (MIBs) [b-IETF RFC1155, b-IETF RFC1212, b-IETF RFC1215, b-IETF RFC2578, b-IETF RFC2579, and b-IETF RFC2580], and protocol operations [b-IETF RFC3416, b-IETF RFC3417]. For a more detailed overview of the documents that describe the current Internet-Standard Management Framework, see section 7 of [b-IETF RFC3410].

Each NGN Network Element may implement an SNMP client. If SNMP v1 or v2 are used, and if required by security policy of the NGN provider, they are required to use UDP over IPSec as the transport. Each instance of a message may be encoded using the Basic Encoding Rules of ASN.1 [ITU-T X.690] into a single UDP datagram. The client may listen on port 161 for Command Responder Applications, and may listen on port 162 for Notification Receiver Applications.

NGN Network Elements are required to implement all necessary MIBs for reporting security events and audit trails.

11.3 Security Patch Management

Regular installation of maintenance and security patches on NGN network elements and servers minimizes their vulnerabilities to attacks and unintentional failures. A comprehensive patch management strategy is required to be deployed including Installation and Verification processes and platforms.

11.4 Version management

Network Elements configurations and changes are required to be backed up. The primary goal of system backup is to allow system recovery in the event of hardware or software troubles that result

in corruption of a software load and/or the associated system data. The following types of information may be included in a system backup load:

- Customer data and logic
- Network traffic connectivity such as facilities and trunks
- The NGN Carrier and vendor-provided application software
- Operating system
- Hardware configuration

An on-going record of provisioning work is required to be maintained so that any Network Element (NE) can be brought up to date with provisioning actions that have occurred since a backup image was taken.

The Provisioning Platform may provide the following capabilities.

- A journal of provisioning activities for each of the Network Elements (NEs) that directly provisions.
- At least one week's worth of Provisioning activities for each NE.

The Provisioning Platform may allow users to manually review the stored provisioning activities for each NE. The activity description provided to the user is required to summarize the size, number, and types of transactions for a given time interval.

The Provisioning Platform may provide a utility to allow re-provisioning of a designated NE by re-entering data into a specified NE. This utility should allow selection of begin and end dates/times for the data to be re-provisioned. Based on the specified begin and end dates/times, the Provisioning Platform should automatically re-enter all of the intervening data into the specified NE.

11.5 Audit Trail, Trapping, and Logging at TE-BE

All of the Audit Trail, Trapping, and Logging requirements for NGN Network Elements apply to the TE-BE.

The TE-BE is connected to the OAMP systems through a VPN tunnel. It therefore sends its logging messages, receives SNMP requests and sends SNMP responses through this VPN. The TE-BE is not recommended to accept any OAMP requests on any other interface.

The requirements for the VPN tunnel are given in section 9.3.

12 Provisioning of equipment in untrusted zone

All customer premise equipments are configured by the TE Provisioning Element. TE Provisioning Element resides in the trusted zone and may only communicate with the TEs via the Network Border Element (NBE) as shown in Figure 2. A TE or TE-BE may authenticate and establish a security association with the NNBE before it can obtain configuration file from the TE Provisioning Element. NNBE may support both TLS and IPsec for establishing SA with the TEs (including TE-BE). Refer to sections 9.1 and 9.2 for more detail.

Provider controlled Equipment can be treated as a part of NBE in this context.

The TE Provisioning Element includes the address of a NBE in the configuration data downloaded to the authenticated device. The TE Provisioning Element may also include a certificate that is used to authenticate the subscriber with the NNBE as described in section 8.4.

A TE device will request provisioning from NGN service provider. The NBE will receive this request and authenticate the TE with the SAA/TAA-FEs. When the device is authenticated, the Border Element will forward the provisioning request to TE Provisioning Element. The TE Provisioning Element then downloads the configuration and/or firmware to the TE. If the TE cannot be authenticated, the failure is logged.

APPENDIX A: Examples of Source-Address Assurance and its application to the mechanism of subscriber identification and authentication

[Informative]

This Appendix provides concrete examples of the Source-Address Assurance mechanisms and its application to the subscriber identification and authentication through Network Source Address described in Clause 8.4.2.

A.1. Subscriber identification and authentication linked to access-line authentication

This clause provides an example of the subscriber identification and authentication, in which an IP address is assigned as the result of access-line authentication. In this example, each subscriber is statically associated with his/her access line. Hence, the mechanism described in this example is applicable only to non-nomadic (i.e. fixed) services.

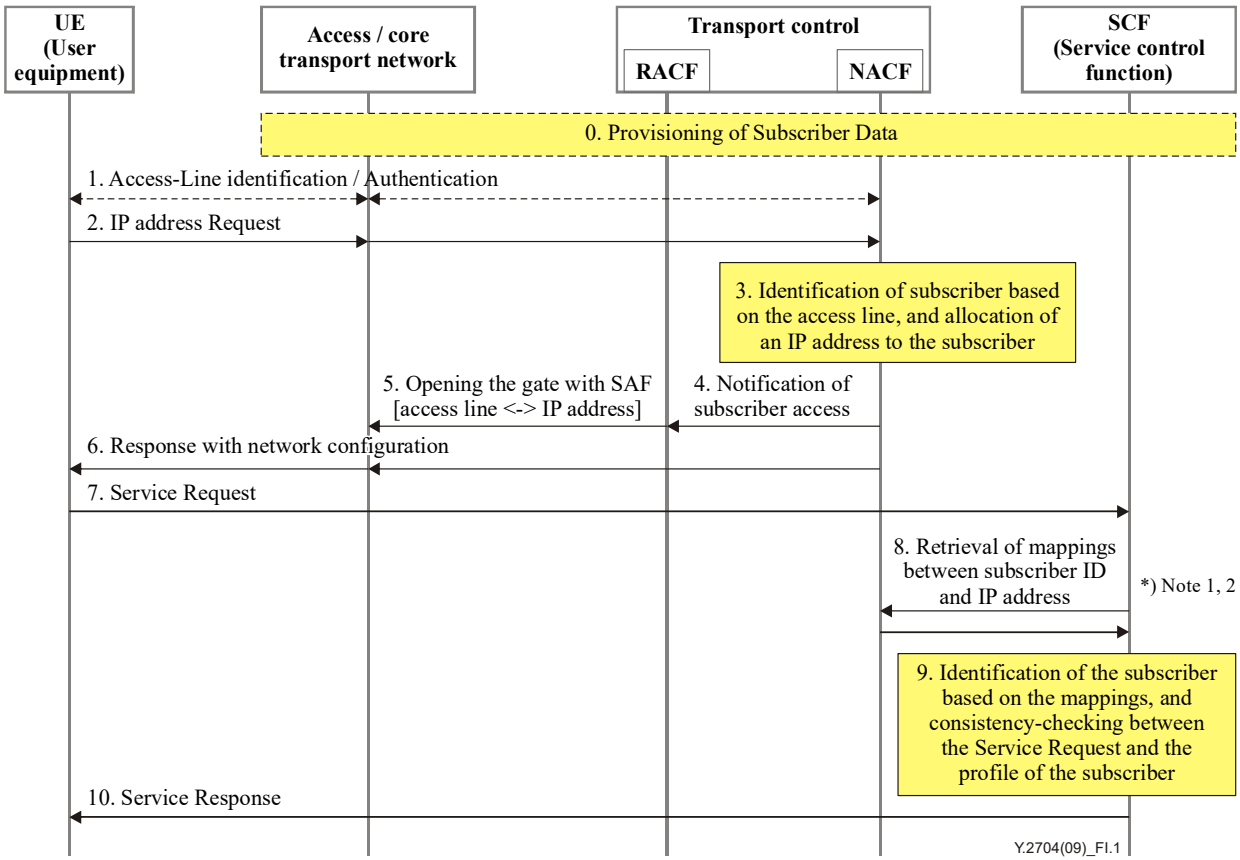

Figure A. 1 - High-level message flows of example 1

NOTE 1 – The mapping information between the IP address and the Subscriber ID may be provided from the NACF to the SCF at the time of address allocation by the NACF.

NOTE 2 – The NACF may provide the mapping between the IP address and the location information (e.g. Line Identifier) instead of the mapping between the IP address and the subscriber ID. In that case, the SCF is required

to maintain the mappings between subscriber IDs and locations and derive the subscriber ID from the location information sent from the NACF.

Descriptions

0. The subscriber profiles are preconfigured to the corresponding FEs (e.g. TUP-FE, SUP-FE) in the NACF or the SCF.

   The most important setting issues in this scenario are: 1) The NACF (typically TUP-FE) maintains the mappings between subscriber IDs (Subscriber Account Identifiers) and logical/physical access-line IDs (e.g. VLAN ID or access port), and 2) The SCF (typically SUP-FE) maintains the mappings between subscriber IDs and the attributes or profiles of the corresponding subscribers (e.g. values of “From” header in case of SIP-based services). In cases where the name space of subscriber IDs in the SCF is different from that in the NACF, the SCF is recommended also to maintain the mappings between these IDs.

   Alternatively, the NACF does not have to maintain the mappings between subscriber IDs and access-line IDs. In such scenarios, the SCF is recommended to maintain the mappings between subscriber IDs and access-line IDs, so the SCF can retrieve a corresponding subscriber ID from an access-line ID.

   On the gateways in the Access/Core Transport, all gates for subscriber's access lines are initially configured to be closed so that any incoming IP packets, except for the packets necessary for UE to attach the network (e.g. sending address requests or authentication requests), are dropped.

1. A UE attaches to the Access Network through its access line to get IP connectivity to the NGN. This example assumes that access authentication by the NACF is implicit and is executed at step 3. However, the NACF may alternatively employ an explicit access authentication method (e.g. IEEE 802.1X). In that case, network access authentication is executed in this phase, i.e. before IP address assignment.

2. The UE requests allocation of an IP address. This is typically performed by sending DHCP Discover and Request, and these messages are relayed to the NACF by the gateways.

3. In this example, Access Network authenticates the access line and provides the authenticated access-line ID (e.g. VLAN ID or access port) to the NACF. Hence, the NACF can identify the subscriber ID of the UE based on the access-line ID, which the IP address request is sent through. Then, the NACF allocates an IP address to the requesting UE and stores the mapping between the subscriber ID and the allocated IP address.

   This mapping information may be pushed from the NACF to the SCF and be stored (cached) in the SCF. In that case, the 8th step below can be skipped.

4. The NACF notifies the RACF that the subscriber has been connected. This notification includes the subscriber ID, the access-line ID (physical/logical), the allocated IP address, and QoS profiles.

5. The RACF makes a policy decision on network resource allocation to the subscriber and orders the gateways to open the gate for the access line with packet-filtering rules, which are defined to accept and forward incoming IP packets whose source address is the IP address assigned to the subscriber, and to drop other incoming packets.

   The enforcement of source IP address filtering coordinated with access-line authentication by the NACF, which is described above, ensures that an IP address can be used only by the subscriber to whom the address is assigned.

6. The NACF returns the allocated IP address to the UE with other network configuration parameters (e.g. the addresses of DNS servers and P-CSC-FE). This is typically done by sending DHCP Offer and Response messages.

7. After getting IP-connectivity, the UE sends a Service Request (e.g., REGISTER signal in case of SIP-based services) to the SCF. The Service Request is passed by the gateways (firewalls with source-address filtering) to the SCF only if the source address of the Request is one assigned by the NACF.
8. The SCF retrieves the mapping information (i.e., the subscriber ID and its assigned IP address) corresponding to the source address of the Service Request, from the NACF.
9. The SCF considers the Service Request to be originated from the subscriber who assigned the subscriber ID contained in the retrieved mapping information. In cases where the name space of subscriber IDs in the SCF is different from that in the NACF, the retrieved subscriber ID is required to be translated into the subscriber ID in the name space used by the SCF based on the mappings between these IDs.

   The SCF extracts the value of attributes regarding the subscriber's identity (e.g. the value of the "From" header in case of SIP-based services) from the Service Request and checks consistency between those values and the corresponding subscriber's profile.
10. If the authentication and the authorization succeed, the SCF returns the normal reply to offer the requested service (e.g. "200 OK" in case of SIP-based services).

A.2. Subscriber identification and authentication linked to explicit access authentication at IP Connectivity Establishment

This clause provides an example of the subscriber identification and authentication, in which an IP address is assigned as the result of explicit access authentication at the establishment of IP connectivity. In this example, each subscriber is dynamically associated to a L2 session, which is established at the time of access authentication. Hence, the mechanism described in this example is applicable to both nomadic and non-nomadic services.

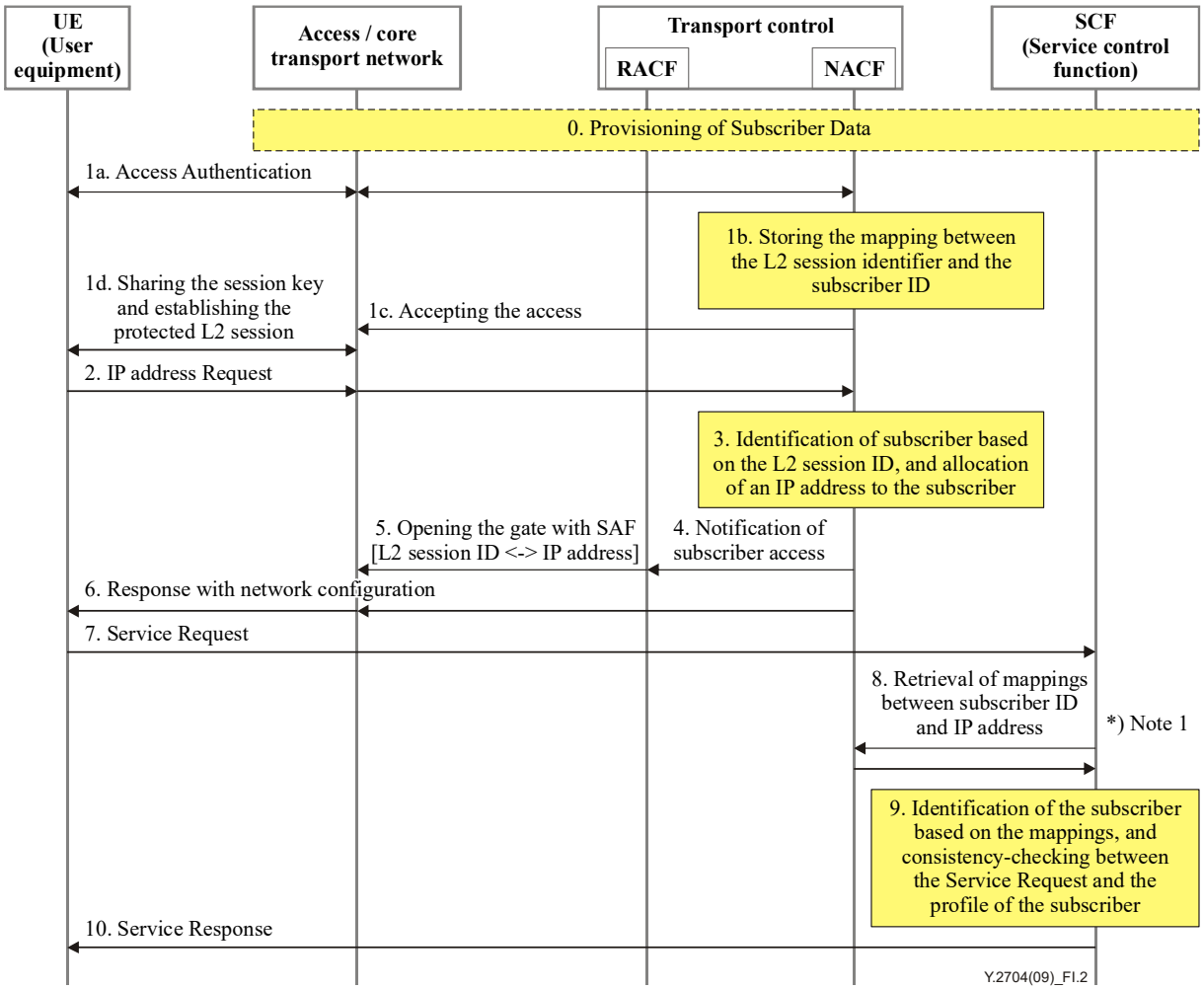

Figure A. 2 - High-level message flows of example 2

NOTE 1 – The mapping information between the IP address and the Subscriber ID may be provided from the NACF to the SCF at the time of address allocation by the NACF.

Descriptions

0. The subscriber profiles are preconfigured to the corresponding FEs (e.g. TUP-FE, SUP-FE) in the NACF or the SCF. In contrast with the previous example, the NACF does not need to maintain the mappings between subscriber IDs and access-line IDs.

   On the gateways in the Access/Core Transport, all gates for L2 access sessions with UEs are initially configured to be closed so that any incoming IP packets, except for the packets necessary for UE to attach the network (e.g. sending address requests or authentication requests), are dropped.

1a. When a UE requests connectivity to the NGN, the Access Network dynamically creates an L2 session with the UE, and an Access Authentication procedure is performed between the UE and the NACF based on the subscriber's credential (typically with an explicit authentication method such as IEEE 802.1X and RADIUS/Diameter). The signalling messages for authentication are forwarded by the gateways.

1b. During the authentication procedure, the identifier of the L2 session (e.g. VLAN-ID, L2 address of the UE, etc) assigned to the UE is sent to the NACF. When the authentication

succeeds, the NACF stores this L2 session identifier with the authenticated subscriber ID.

1c. The NACF notifies the Access Network that the UE has been successfully authenticated and the access to the network has been authorized (e.g. an ACCESS ACCEPT message in case of RADIUS protocol).

1d. Upon receiving the notification of successful authentication of the subscriber from the NACF, the Access Network establishes a security association (SA) with the UE to protect the integrity and confidentiality of the L2 session. Typically, these are achieved by the session-keys derivation mechanisms defined in IEEE 802.1X and the protection procedure defined for each L2 technology (e.g. TKIP/CCMP defined in IEEE 802.11i for 802.11 Wireless-LAN.)

The security mechanisms described above protect the L2 session from being used by other subscribers and provides necessary grounds for the prevention of IP-address spoofing.

2. The UE requests allocation of an IP address. This is typically performed by sending DHCP Discover and Request, and these messages are relayed to the NACF by the gateways.

3. The NACF identifies the subscriber ID of the UE based on the identifier of the L2 session, which the request is sent through. Then, the NACF allocates an IP address to the requesting UE and stores the mapping between the subscriber ID and the allocated IP address.

This mapping information may be pushed from the NACF to the SCF and stored (cached) in the SCF. In that case, the 8th step below can be skipped.

4. The NACF notifies the RACF that the subscriber has been connected. This notification includes the subscriber ID, the L2 session ID (physical/logical), the allocated IP address, and QoS profiles.

5. The RACF makes a policy decision on network resource allocation to the subscriber and orders the gateways to open the gate for the L2 session with packet-filtering rules, which are defined to accept and forward incoming IP packets whose source address is the IP address assigned to the subscriber, and to drop other incoming packets.

The enforcement of source IP address filtering coordinated with access authentication the by NACF, which is described above, ensures that an IP address can be used only by the subscriber to whom the address is assigned.

Steps 6 - 10 are identical to those explained in the previous example described in Clause A.1.

APPENDIX B - Emergency Telecommunications Service (ETS) Interconnection Security [Informative]

B.1 Background

Emergency Telecommunications Service (ETS) is a national service, providing priority services to authorized ETS 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 bi-lateral and/or multi-lateral 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 bi-lateral and/or multi-lateral agreements in times of disaster and emergencies. Assurance and availability of ETS communications will depend on the security capabilities and measures enforced in each national network involved in an end-to-end communication.

B.2 Scope/purpose

This Appendix provides guidance to allow support of network provided security for ETS communications 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 communications across multiple networks on a hop-by-hop basis. However, the NGN is recommended to be capable of transparently supporting such peer-to-peer functions.

This Appendix is not intended to impose conditions on national implementations of ETS. It primary purpose is to allow network provided security for ETS communications (i.e., priority voice, video, data, and messaging communications) across different national networks (i.e., countries / administrations).

B.3 Security Objectives and Guidelines for Interconnection of ETS

Refer to section 7 of [ATIS-1000010] and Appendix I of [ITU-T Y.2701] for information on security objectives and guidelines for interconnection of ETS.

B.4 Authentication and Authorization

It is recommended that national networks support and implement mechanisms and capabilities to authenticate and authorize the ETS user, device, or user and device combination based on the assurance level needed for access to specific service (e.g., voice, data, video) and applicable policy.

It is recommended that the security mechanisms described in the body on this standard for identification and authentication of users and user devices be utilized as appropriate to support ETS implementations in national networks:

- IPsec/TLS associations
- SIP Challenge/Response and X.509 certificates,
- Generic Booth Strapping Architecture.

In addition it is recommended that security measures monitoring access to ETS resources be implemented to detect and prevent denial of services types of attacks.

Also, refer to Appendix I of [ITU-T Y.2702] for information on example ETS authentication and authorizations approaches.

B.5 Transport Security for Signaling and OAMP

It is recommended that the security mechanisms, IPsec and TLS, as described in the body of this standard be utilized as appropriate to protect ETS signaling and OAMP traffic in national networks.

B.6 Media Traffic

It is recommended that the security mechanisms to identify and protect media traffic as described in the body of this standard be utilized as appropriate to protect ETS media traffic in national networks.

B.7 Support of Calling Number ID and Calling Name ID Restriction Features

Calling Number ID and Calling Name ID are two legacy PSTN features that permit users to know who is calling. ETS calls may serve different national communities of users with different sensitivities to the disclosure of such information to the called party. Therefore, it is recommended that appropriate mechanism be supported to enforce policy regarding display or disclosure of ETS user information.

B.8 Non-traceability

For certain ETS communications it is important that location information associated with the calling party and called party be unavailable to all parties to the maximum extent feasible. In particular, any location related information is recommended to be suppressed or, if necessary, have un-meaningful information substituted as appropriate based on applicable policy. Location related information includes, but may not be limited to:

1. Calling and called party NPA-NXX or URI;
2. Calling and called party geographic address;
3. Calling and called party x-y coordinates;
4. Calling and called party cell information of possible use in narrowing location down to a cell;
5. Calling and called party IP address;
6. Calling and called party End Office or other facility information enabling geographic proximity of the calling party to be determined.

B.9 End-to-End Peer-to-Peer Encryption

Selected users may require User Equipment (UE) encrypted ETS calls/sessions. For these calls/sessions, normal ETS call/session establishment procedures would apply and the end-to-end encryption process is provided by the UE for the bearer information (e.g., voice) to the terminating UE. This encryption process is transparent to the NGN. However, the NGN is recommended to be capable of transparently supporting such peer-to-peer functions.

APPENDIX C - Security Best Practices

[Informative]

C.1 Introduction

To meet the requirements specified in [ATIS-1000029] and [ITU-T Y.2701], additional security mechanisms beyond those specified in this standard may be needed. Best practice security mechanisms such as the use of firewalls, operating system hardening, vulnerability scanning, and Intrusion Detection Systems (IDS) may be employed to secure the NGN infrastructure. Refer to [b-NIST SP 800-94] for guide on intrusion detection and prevention systems (IDPS) and [b-NIST SP 800-83] NIST for guidance on malware incident prevention and handling.

This Appendix provides a summary of some example best practice security mechanisms that should be employed.

C.2 Firewalls

Firewalls are fundamental security building blocks that provide network isolation at boundaries between network segments or between different networks. Firewalls perform isolation based on specific traffic filtering rules configured onto the firewalls. Firewalls may be used in conjunction with other security mechanisms to provide an additional layer of security. The addition of firewalls helps provide “defense in depth” security whereby multiple security mechanisms are overlaid to achieve stronger security.

A firewall examines both inbound and outbound traffic, and should be configured to deny all traffic unless specifically allowed by the firewall rules. A firewall may also provide logging of traffic and trigger alarms when unauthorized packets are detected. Firewalls can physically be provided as separate appliances or may be provided as software on the host machines themselves. Types of firewalls include static packet filtering, application layer, and state aware packet filtering firewalls, and the choice will depend on particular customer needs and preferences.

Static packet filtering firewalls examine incoming and outgoing packets and apply a set of rules to determine whether packets will be allowed to transit the firewall or be dropped. This determination is typically based on the packet source and destination IP addresses, the protocol type, and the TCP source and destination ports. Depending on the packet and the criteria, the firewall will drop or forward the packet, and possibly create a log entry and/or raise an alarm. Some static packet filtering firewalls may also provide deeper inspection of packets, possibly up to the application layer.

Application layer firewalls run applications on behalf of the machines in the network they are protecting, and are often called “proxy” firewalls. When performing the applications, application layer firewalls will detect any anomalous activity and if any is found will not pass the data on to the machines they are protecting. Application layer firewalls must be enabled with all necessary application and must run these applications on behalf of all protected machines. Because of this, application layer firewalls have a high impact on network performance.

State aware firewalls perform packet filtering functions similar to static packet filtering firewalls, and in addition maintain information about the state of traffic connections. The state information allows the firewall to make better decisions about whether to allow or deny particular traffic. For example, a state aware firewall may be configured to only allow traffic from machines on one side of the network to initiate communications. This is particularly useful where private networks connected to public networks.

When using firewalls as an additional signalling and control plane security, the firewalls should be configured to allow only desired signalling and control communication between a set of machines.

Any other traffic on the network other than the desired communications should be denied, thereby providing a layer of protection for these machines.

Note that providing firewalls may have system engineering and product impacts, and some applications may have to be made firewall aware. Also note that firewalls will not protect against all security attacks such as an attacker spoofing legitimate signalling packet information.

C.3 Operating System Hardening

Servers and network elements used for signalling and control plane functions are vulnerable to any number of attacks including the following:

- Backdoor programs
- Sniffing programs
- Password grabber and cracking tools
- Exploitation of defects in operating system services
- Denial of service (DoS).

Some of these attacks are based on well-publicized techniques, with scripts and other tools available to make it possible for less knowledgeable crackers to apply exploits against systems. Once a system has been compromised, an intruder can do a number of things, among which are:

- Modify or destroy information
- Disclose sensitive information
- Install malicious code to gather information
- Use the compromised server to attack other systems.

Operating system hardening procedures may be used to improve the resistance of operating systems to attacks. Operating system hardening procedures are essentially sound practices that are followed during the installation and configuration of an operating system. While no system is absolutely secure, following operating system hardening procedures will result in systems that are harder for crackers to compromise.

Operating system hardening essentially involves the restriction of services, ports, and access to applications and files. Operating system hardening also involves only running applications from a restricted access privilege account and with only absolutely necessary ports and services running only. Operating system manufacturers should be consulted to obtain the latest OS hardening procedures and security patches.

C.4 Vulnerability Assessment

The goal of performing a vulnerability assessment on network elements is to discover security vulnerabilities, weaknesses, and areas of risk. Vulnerability testing is designed to try and make systems fail by interrupting services, circumventing devised security controls, capturing confidential data, obtaining unauthorized access to the system, or stealing or denying service. Vulnerability assessment may be included for NGN elements in order to ensure even stronger security.

Vulnerability assessment for network elements may be conducted at the product verification stage, and then ongoing as part of network maintenance. Including security vulnerability testing at the product verification stage is advantageous since there is already a pre-established procedure to record and submit requests for changes. Ongoing routine vulnerability assessments are useful to identify new threats and vulnerabilities and initiate action to mitigate the issues identified.

C.5 Intrusion Detection Systems

Intrusion detection systems can be used provide protection against intrusions and unauthorized actions. For example, intrusion detection systems can be used to warn network administrators of the possibility of a security incident such as a SIP server compromise or denial-of-service attack.

Intrusion detection systems (IDS) can be broadly categorized according to the following criteria:

- Real Time or Off Line Incident Detection: A real time IDS network traffic and logs as events take place. An off-line IDS system analyzes intrusions in batch mode after incidents have occurred.
- Network Based or Host Based Installation: A network-based IDS typically involves multiple monitors installed at choke points on the network where all traffic between two points can be monitored. A host-based IDS requires that software be installed directly on the servers to be protected, and monitors the network connections and user activity on those servers.
- Reactive of Passive: A reactive IDS actively intervenes to head off attacks by modifying firewall rules or router filters or other measures. A passive IDS system only notifies administrators or other network systems of the problem.

Most commercial IDS products provide a combination of network and host-based monitoring capabilities, with a central management device to receive the reports from the various monitors and alert the network administrators.

APPENDIX D – Bibliography
[Informative]

The following informative references are used in this document:

[b-IETF RFC1155] IETF RFC 1155, *Structure and identification of management information for TCP/IP-based internets.*[4]

[b-IETF RFC1212] IETF RFC 1212, *Concise MIB definitions.* [4]

[b-IETF RFC1215] IETF RFC 1215, *Convention for defining traps for use with the SNMP.* [4]

[b-IETF RFC2578] IETF RFC 2578, *Structure of Management Information Version 2 (SMIv2).* [4]

[b-IETF RFC2579] IETF RFC 2579, *Textual Conventions for SMIv2.* [4]

[b-IETF RFC2580] IETF RFC 2580, *Conformance Statements for SMIv2.* [4]

[b-IETF RFC2246] IETF RFC 2246, *The TLS Protocol Version 1.0.* [4]

[b-IETF RFC2367] IETF RFC 2367, *PF_KEY Key Management API, Version 2.* [4]

[b-IETF RFC2403] IETF RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH.* [4]

[b-IETF RFC 2409] IETF RFC 2409, *The Internet Key Exchange (IKE).* [4]

[b-IETF RFC2451] IETF RFC 2451, *The ESP CBC-Mode Cipher Algorithms.* [4]

[b-IETF RFC2617] IETF RFC 2617, *HTTP Authentication: Basic and Digest Access Authentication.* [4]

[b-IETF RFC2808] IETF RFC 2808, *The SecurID® SASL Mechanism.* [4]

[b-IETF RFC2865] IETF RFC 2865, *Remote Authentication Dial In User Service (RADIUS).* [4]

[b-IETF RFC3261] IETF RFC 3261, *SIP: Session Initiation Protocol.* [4]

[b-IETF RFC3310] IETF RFC 3310, *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA).* [4]

[b-IETF RFC3410] IETF RFC 3410, *Introduction and Applicability Statements for Internet-Standard Management Framework.* [4]

[b-IETF RFC3411] IETF RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.* [4]

[b-IETF RFC3413] IETF RFC 3413, *Simple Network Management Protocol (SNMP) Applications.* [4]

[b-IETF RFC3414] IETF RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).* [4]

[b-IETF RFC3415] IETF RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).* [4]

[4] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[b-IETF RFC3416] IETF RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP).* [4]

[b-IETF RFC3417] IETF RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP).* [4]

[b-IETF RFC3550] IETF RFC 3550, *RTP: A Transport Protocol for Real-Time Applications.* [4]

[b-IETF RFC3588] IETF RFC 3588, *Diameter Base Protocol.* [4]

[b-IETF RFC3602] IETF RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec.* [4]

[b-IETF RFC3711] IETF RFC 3711, *The Secure Real-time Transport Protocol (SRTP).* [4]

[b-IETF RFC3713] IETF RFC 3713, *A Description of the Camellia Encryption Algorithm.* [4]

[b-IETF RFC3830] IETF RFC 3830, *MIKEY: Multimedia Internet KEYing.* [4]

[b-IETF RFC 4132] IETF RFC 4132, *Addition of Camellia Cipher Suites to Transport Layer Security (TLS).* [4]

[b-IETF RFC 4279] IETF RFC 4279, *Pre-Shared Key Ciphersuites for Transport Layer Security* (TLS) [4]

[b-IETF RFC4301] IETF RFC 4301, *Security Architecture for the Internet Protocol.* [4]

[b-IETF RFC 4306] IETF RFC 4306, *Internet Key Exchange (IKEv2) Protocol.* [4]

[b-IETF RFC 4312] IETF RFC 4312, *The Camellia Cipher Algorithm and Its Use with IPsec.* [4]

[b-IETF RFC4422] IETF RFC 4422, *Simple Authentication and Security Layer (SASL).*

[b-IETF RFC 4492] IETF RFC 4492, *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).* [4]

[b-IETF RFC 4566] IETF RFC 4566, *SDP: Session Description Protocol*. [4]

[b-IETF RFC4567] IETF RFC 4567, *Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP).* [4]

[b-IETF RFC4568] IETF RFC 4568, *Session Description Protocol (SDP) Security Descriptions for Media Streams.* [4]

[b-IETF RFC 4590] IETF RFC 4590, *RADIUS Extension for Digest Authentication.* [4]

[b-IETF RFC 4648] IETF RFC 4648, *The Base16, Base32, and Base64 Data Encodings.* [4]

[b-IETF RFC4740] IETF RFC 4740, *Diameter Session Initiation Protocol (SIP) Application.* [4]

[b-IETF RFC 4835] IETF RFC 4835, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).* [4]

[b-IETF RFC5077] IETF RFC 5077, *Transport Layer Security (TLS) Session Resumption without Server-Side State.* [4]

[b-IETF RFC5090] IETF RFC 5090, *Radius Extension for Digest Authentication.* [4]

[b-IETF RFC 5246] IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2.* [4]

[b-IETF RFC5282] IETF RFC 5282, *Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol.* [4]

[b-IETF RFC5424] IETF RFC 5424, *The Syslog Protocol.* [4]

[b-ISO/IEC 15946-5-1] *Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves. Part 1: General*[5]

[b-ISO/IEC 15946-5-2] *Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves. Part 2: Digital Signatures (ECDA)* [5]

[b-ISO/IEC 15946-5-3] *Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves. Part 3 Key Establishment (ECDH)* [5]

[b-ISO/IEC 15946-5-4] *Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves. Part 4: Digital signatures giving message recovery*[5]

[b-ISO/IEC 15946-5-5] *Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves. Part 5: Elliptic curve generation Cryptographic techniques based elliptic Curves.* [5]

[b-ISO/IEC 18033-3] International Organization for Standardization, *"Information technology - Security techniques - Encryption algorithms – Part 3: Block ciphers", ISO/IEC 18033-3, July 2005.* [5]

[b-NIST FIPS SP800-38a] NIST Federal Information Processing Standard (FIPS) Special Publication 800-38: *Recommendation for Block Cipher Modes of Operations. Methods and Techniques, December 2001.*[6]

[b-NIST FIPS 197] NIST Federal Information Processing Standard (FIPS) 197: *Advanced Encryption Standard, November 2001.* [6]

[b-NIST FIPS 198] NIST Federal Information Processing Standard (FIPS) 198, *The Keyed-Hash Message Authentication Code.* [6]

[b-NIST SP 800-44 v2] NIST Special Publication 800-44 Version 2, *Guidelines on Securing Public Web Servers* [6]

[b-NIST SP 800-57] NIST Special Publication 800-57, *Recommendation for Key Management – Part 1: General (Revised).* [6]

[b-NIST SP 800-94] NIST Special Publication 800-94, *Guide to Intrusion detection and Prevention Systems (IDPS)* [6]

[b-NIST SP 800-83] NIST Special Publication 800-83, *Guide to Malware Incident Prevention and Handling.* [6]

[b-TIA 683-D] TIA Standard TIA-683-D (2005), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*[7]

[b-ETSI TS133220] ETSI TS 133 220, 03/2006, *Generic Authentication Architecture (GAA); Generic bootstrapping architecture.*[8]

---

[5] This document is available from the International Organization for Standardization. < http://www.iso.ch/iso/en/prods-services/ISOstore/store.html >

[6] This document is available from the National Institute of Standards and Technology (NIST) at < http://csrc.nist.gov/publications/fips/ >.

[7] This document is available from the Telecommunications Industry Association (TIA). < http://www.tiaonline.org/standards/overview.cfm >

[b-3GPP. TS 33.102] *3G Security: Security Architecture.*[9]

[b-3GPP TS 33.328] *IP Multimedia System (IMS) media plane security.* [9]

[8] This document is available from the European Telecommunications Standards Institute (ETSI).
< http://www.etsi.org/getastandard/home.htm >

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