

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2704

(01/2010)

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

Next Generation Networks – Security

Security mechanisms and procedures for NGN

Recommendation ITU-T Y.2704

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE

General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899

INTERNET PROTOCOL ASPECTS

General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999

NEXT GENERATION NETWORKS

Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Future networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999

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

Recommendation ITU-T Y.2704

Security mechanisms and procedures for NGN

Summary

Recommendation ITU-T Y.2701, *Security requirements for NGN release 1*, provides security requirements for next generation networks (NGNs) and its interfaces (e.g., UNIs, NNIs and ANIs). Recommendation ITU-T Y.2704 describes some security mechanisms that can be used to fulfil the requirements described in Recommendation ITU-T Y.2701 and specifies the suite of options for each selected mechanism. Specifically, this Recommendation describes identification, authentication and authorization mechanisms; then it 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 Recommendation are based on use of the trust model defined in Recommendation ITU-T Y.2701.

The list of security mechanisms described in this Recommendation is not exhaustive. NGN providers are encouraged to support additional security tools, capabilities and operational measures as needed beyond the mechanisms specified in this Recommendation for NGN security protection.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2704	2010-01-29	13

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

© ITU 2010

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

CONTENTS

	Page
1 Scope	1
1.1 Assumptions	1
1.2 Overview	1
2 References.....	2
3 Definitions	3
3.1 Terms defined elsewhere	3
3.2 Terms defined in this Recommendation.....	4
4 Abbreviations and acronyms	4
5 Conventions	7
6 Security risks and threats	7
7 Security trust model.....	7
7.1 Single network trust model.....	7
7.2 Peering network trust model.....	9
8 Identification, authentication and authorization	10
8.1 Subscribers	10
8.2 Network element	10
8.3 Credential usage in the NGN security	10
8.4 Identification and authentication of subscribers.....	14
8.5 Identification and authentication of end-users	18
8.6 Identification and authentication by TE-BE.....	20
8.7 Authenticator-SAA/TAA-FEs interface	20
8.8 Identification and authentication of bearer traffic	21
9 Transport security for signalling and OAMP	23
9.1 TLS	23
9.2 IPsec in trusted and trusted-but-vulnerable zones	27
9.3 Key agreement protocol between untrusted and trusted-but-vulnerable zone.....	31
9.4 IPsec between untrusted and trusted-but-vulnerable zone	31
10 Media security	31
10.1 SRTP.....	33
11 OAMP.....	34
11.1 Network element interface to logging systems	35
11.2 Network element use of SNMP	35
11.3 Security patch management.....	35
11.4 Version management.....	35
11.5 Audit trail, trapping, and logging at TE-BE	36
12 Provisioning of equipment in untrusted zone	36

Appendix I – Examples of source-address assurance and its application to the mechanism of subscriber identification and authentication	37
I.1 Subscriber identification and authentication linked to access-line authentication	37
I.2 Subscriber identification and authentication linked to explicit access authentication at IP connectivity establishment	39
Appendix II – Emergency telecommunications service (ETS) interconnection security	42
II.1 Background.....	42
II.2 Scope/purpose.....	42
II.3 Security objectives and guidelines for interconnection of ETS	42
II.4 Authentication and authorization	42
II.5 Transport security for signalling and OAMP	43
II.6 Media traffic	43
II.7 Support of calling number ID and calling name ID restriction features	43
II.8 Non-traceability	43
II.9 End-to-end peer-to-peer encryption	43
Appendix III – Security best practices	44
III.1 Introduction	44
III.2 Firewalls	44
III.3 Operating system hardening	45
III.4 Vulnerability assessment	45
III.5 Intrusion detection systems	46
Bibliography.....	47

Recommendation ITU-T Y.2704

Security mechanisms and procedures for NGN

1 Scope

[ITU-T Y.2701], *Security requirements for NGN release 1*, 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 Recommendation therefore highlights some important security mechanisms that can be used to realize the requirements in [ITU-T Y.2701] 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 Recommendation is not exhaustive. NGN providers are encouraged to support additional security tools, capabilities and operational measures as needed beyond the mechanisms specified in this Recommendation for NGN security protection.

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

NOTE – The mechanisms described in this Recommendation for identification and authentication are part of the broader topic generally known as IdM ("identity management").

1.1 Assumptions

This Recommendation is based on the following assumptions:

- 1) The bundling of functional entities, as defined in [ITU-T Y.2012], to a given network element will vary, depending on the vendor.
- 2) Each NGN provider has specific responsibilities within its domain for security. For example, implementing applicable security services and practices 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 for service level agreements (SLAs) to assure the security of its domain and the security of the network interconnections. It is assumed that the SLAs would specify security services, mechanisms and practices to be implemented to protect the interconnected networks and the communications (signalling/control traffic, bearer traffic and management traffic) across UNIs, ANIs and NNIs.
- 4) This Recommendation addresses network-based security, which is a layered architecture, consisting of perimeter security to trusted domains, physical security of provider equipment, and potentially the use of encryption.

1.2 Overview

This Recommendation is organized as follows:

- Clause 2 (References) – This clause provides normative references.
- Clause 3 (Definitions) – This clause provides definitions used in this Recommendation.
- Clause 4 (Abbreviations and acronyms) – This clause provides the list of abbreviations and acronyms used in this Recommendation.
- Clause 5 (Conventions) – 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 [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 signalling and OAMP) – This clause provides mechanisms for signalling 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 clause 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 untrusted zone.
- Appendix I – Examples of source-address assurance and its application to the mechanism of subscriber identification and authentication
- Appendix II – Emergency telecommunications service (ETS) interconnection security
- Appendix III – Security best practices
- Bibliography

2 References

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

- [ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.
- [ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.
- [ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.
- [ITU-T Y.2703] Recommendation ITU-T Y.2703 (2009), *The application of AAA service in NGN*.
- [ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.
- [ITU-T X.509] Recommendation ITU-T X.509 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*.
- [ITU-T X.660] Recommendation ITU-T 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 International Object Identifier tree*.

- [ITU-T X.1035] Recommendation ITU-T X.1035 (2007), *Password-authenticated key exchange (PAK) protocol*.
- [IETF RFC 4302] IETF RFC 4302 (2005), *IP Authentication Header*.
- [IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP)*.
- [IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 asset** [ITU-T Y.2701]: Anything that has value to the organization, its business, its operations and its continuity.
- 3.1.2 border element** [ITU-T Y.2701]: Network element providing functions connecting different security and administrative domains.
- 3.1.3 corporate network** [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 domain border element** [ITU-T Y.2701]: Border element under sole control of the provider, providing security functions with other network domains.
- 3.1.5 emergency telecommunications service (ETS)** [b-ITU-T E.107]: A national service providing priority telecommunications to the ETS authorized users in times of disaster and emergencies.
- 3.1.6 network border element** [ITU-T Y.2701]: Border element under sole control of the provider, providing security functions with terminal equipment.
- 3.1.7 security domain** [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.
- 3.1.8 security token** [b-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.
- 3.1.9 security zone** [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.
- 3.1.10 terminal equipment border element** [ITU-T Y.2701]: Border element providing security functions between customer premises equipment and service provider network.
- 3.1.11 trust** [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.

3.1.12 trusted but vulnerable zone [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.

3.1.13 trusted zone [ITU-T Y.2701]: From the viewpoint of a NGN provider, a security domain where 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.

3.1.14 un-trusted zone [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.

3.1.15 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 [ITU-T Y.2701]: A private network consisting of terminal equipment that may have multiple users.

3.2 Terms defined in this Recommendation

This Recommendation 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 Recommendation uses the following abbreviations and acronyms:

3G	3rd Generation
AGW	Access Gateway
AH	Authentication Header
AKA	Authentication and Key Agreement
ANI	Application-to-Network Interface
AS/WS	Application Server/Web Server
AuC	Authentication Centre
B2BUA	Back-to-Back User Agent
BE	Border Element
BSR	Base Station Router
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
ESP	Encapsulating Security Protocol
ETS	Emergency Telecommunications Service
FE	Functional Entity
GBA	Generic Bootstrapping Architecture
GW	Gateway
HMAC	Hash Message Authentication Code
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	MultiProtocol 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 Switched 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
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	Telecommunications 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 [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 Recommendation assumes the use of the trust model defined in [ITU-T Y.2701]. This clause provides a summary of the NGN security trust model defined in [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 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.

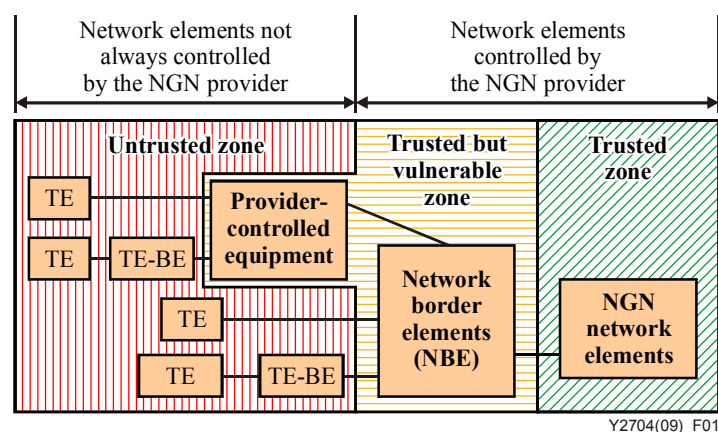


Figure 1 – Security trust model/[ITU-T Y.2701]

A "trusted network security zone", or "trusted zone" in short, is a zone where 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 (NBEs)" at the UNI that provide the 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.
- "Domain border elements (DBEs)" that are similar to the network border elements except that they reside on the border between two domains.
- "Device configuration and 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 interface 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 network 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 that includes all network elements of customer networks or 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. It is still desirable to try to apply some security measures, and to that end, it is recommended that signalling, media, and OAMP be secured and the TE-BE located in the "un-trusted" zone be hardened. However, due to communication with network elements in the "un-trusted" zone, security is less than 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 networks, 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.

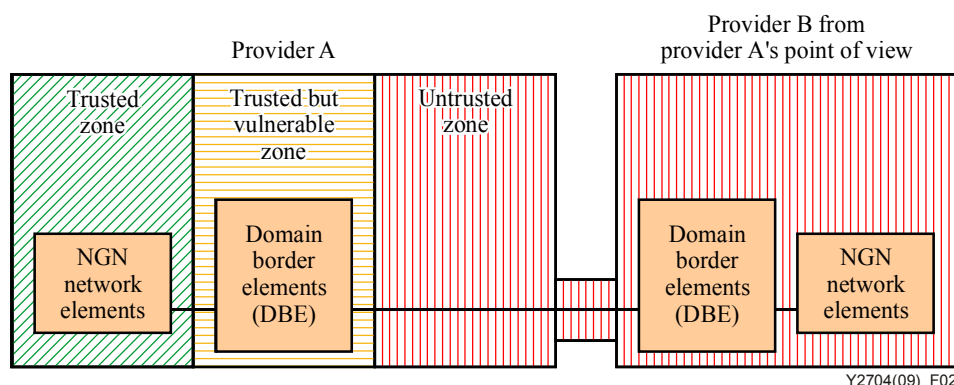


Figure 2 – Peering trust model/[ITU-T Y.2701]

8 Identification, authentication and authorization

Refer to [ITU-T Y.2701], [ITU-T Y.2702], [ITU-T Y.2703] 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

[ITU-T Y.2701] recommends that network elements be identified and authenticated for communications.

If the border element received 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 the NGN security to identify and authenticate a device, a subscriber, and/or an end-user. The credentials to identify and authenticate a device, a subscriber, and/or an end-user are described in clause 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 clause 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 clause 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 clause 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 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 subscriptions 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 its 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. The subscriber and end-user may be the same, or there may be many end-users for a single subscriber. 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 extension 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 extension 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)) [ITU-T X.660]
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 X.509] 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 SAA/TAA-FEs. For a device certificate, the Device Manufacturer and Device Serial Number are used by the Authenticator to determine the associated <Subscriber Account Identifier> (valid only if the device has been associated with a subscriber), 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 (clause 9.1.2), or may be used in creating IPsec connections through IKE Authentication (clause 9.2.4.3).