

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2760

(05/2011)

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

Next Generation Networks – Security

Mobility security framework in NGN

Recommendation ITU-T Y.2760



International
Telecommunication
Union

Documents
Document Sharing Hub

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
Smart ubiquitous networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
Future networks	Y.3000–Y.3099

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

Recommendation ITU-T Y.2760

Mobility security framework in NGN

Summary

Recommendation ITU-T Y.2760 specifies the mobility security framework in next generation network (NGN) transport stratum. It addresses the security requirements, security mechanisms and procedures for mobility management and control in NGN.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2760	2011-05-20	13

Keywords

Mobility security, NGN.

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 2012

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

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	2
5	Security requirements for mobility in NGN	3
5.1	Security threats	5
5.2	Security requirements	5
6	Security capabilities supported by relevant function entities	5
6.1	Transport user profile functional entity (TUP-FE).....	6
6.2	Transport authentication and authorization functional entity (TAA-FE).....	6
6.3	Mobile location management functional entity (MLM-FE).....	6
6.4	Handover decision control functional entity (HDC-FE)	6
6.5	Network information distribution functional entity (NID-FE).....	6
6.6	Access management functional entity (AM-FE).....	6
6.7	Layer3 handover execute function (L3HEF).....	6
6.8	Access node functional entity (AN-FE)	6
7	Key management and authentication.....	7
7.1	Key management framework	7
7.2	Authentication	8
8	Establishment of security context.....	14
8.1	Security context transfer between serving AM-FE and target AM-FE	14
8.2	Security context transfer between serving AR-FE and target AR-FE.....	15
8.3	Security context transfer between UE and HDC-FE	15
9	IP mobility security	16
9.1	Host-based mobility security	16
9.2	Network-based mobility security	17
10	Security between UE and HDC-FE	17
10.1	Host-initiated security association establishment between UE and HDC-FE	17
10.2	Network-initiated security association establishment between UE and HDC-FE.....	18
10.3	Security association pre-establishment between UE and HDC-FE based on PKI.....	19
11	Security between UE and NID-FE	20
11.1	Host-initiated security association establishment between UE and NID-FE	20



	Page
11.2 Network-initiated security association establishment between UE and NID-FE	21
11.3 Security association establishment between UE and NID-FE based on PKI.....	21
12 Security for transport functions	22
12.1 Security between UE and access node function entity	22
12.2 Security between UE and L3HEF (Layer3 Handover Execute Function)	23
Appendix I.....	24
I.1 Example of full authentication procedure	24
I.2 Example of fast re-authentication procedure.....	24
I.3 Example of host-based mobility	25
Bibliography.....	27

Recommendation ITU-T Y.2760

Mobility security framework in NGN

1 Scope

This Recommendation describes the mobility security framework in next generation network (NGN) transport stratum. This Recommendation considers the security requirements in [ITU-T Y.2018]. This Recommendation includes authentication and key management, security context establishment, IP mobility security, and security of mobility management, control and transport in the transport stratum. This Recommendation addresses the scenarios including intra- and inter-technology mobility, intra- and inter-domain mobility.

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 Q.1706]	Recommendation ITU-T Q.1706/Y.2801 (2006), <i>Mobility management requirements for NGN</i> .
[ITU-T X.805]	Recommendation ITU-T X.805 (2003), <i>Security architecture for systems providing end-to-end communications</i> .
[ITU-T Y.2011]	Recommendation ITU-T Y.2011 (2004), <i>General principles and general reference model for Next Generation Networks</i> .
[ITU-T Y.2012]	Recommendation ITU-T Y.2012 (2010), <i>Functional requirements and architecture of next generation networks</i> .
[ITU-T Y.2014]	Recommendation ITU-T Y.2014 (2010), <i>Network attachment control functions in next generation networks</i> .
[ITU-T Y.2018]	Recommendation ITU-T Y.2018 (2009), <i>Mobility management and control framework and architecture within the NGN transport stratum</i> .
[ITU-T Y.2701]	Recommendation ITU-T Y.2701 (2007), <i>Security requirements for NGN release 1</i> .
[ITU-T Y.2704]	Recommendation ITU-T Y.2704 (2010), <i>Security mechanisms and procedures for NGN</i> .
[ITU-T Y-Sup.7]	ITU-T Y-series Recommendations – Supplement 7 (2008), <i>ITU-T Y.2000-series – Supplement on NGN release 2 scope</i> .
[ITU-R M.1645]	Recommendation ITU-R M.1645 (2003), <i>Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000</i> .

Copyright © 2011 ITU-T

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 handover (clause 6.2.2 of [ITU-T Q.1706]): The ability to provide services with some impact on their service level agreements to a moving object during and after movement.

3.1.2 horizontal mobility (clause 6.2.3 of [ITU-T Q.1706]): Mobility on the same layer as defined in [ITU-R M.1645]. Generally, it is referred to as the mobility within the same access technology.

3.1.3 mobility (clause 3.2 of [ITU-T Q.1706]): The ability for the user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment.

3.1.4 NGN transport stratum (clause 3.10 of [ITU-T Y.2011]): That part of the NGN which provides the user functions that transfer data and the functions that control and manage transport resources to carry such data between terminating entities.

3.1.5 trust (clause 3.2.9 of [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.

3.1.6 vertical mobility (clause 6.2.3 of [ITU-T Q.1706]): Mobility between different layers as defined in [ITU-R M.1645]. Generally, it is referred to as the mobility between different access technologies.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 inter-technology mobility: See "Vertical mobility" in clause 3.1.

3.2.2 intra-technology mobility: See "Horizontal mobility" in clause 3.1.

3.2.3 security context: A set of security parameters including identifier, key material, key algorithm, etc.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3G	3rd Generation
ABG-FE	Access Border Gateway Functional Entity
AE	Authentication Extension
AKA	Authentication and Key Agreement
AM-FE	Access Management Functional Entity
AN-FE	Access Node Functional Entity
ANI	Application to Network Interface
AR-FE	Access Relay Functional Entity
DDoS	Distributed Deny of Service
EAP	Extensible Authentication Protocol
EN-FE	Edge Node Functional Entity
FA	Foreign Agent

HA	Home Agent
HDC-FE	Handover Decision Control Functional Entity
IP	Internet Protocol
L3HEF	Layer 3 Handover Execution Function
MIP	Mobile IP
MIPv4	Mobile IP for IP version 4. See [b-IETF RFC 3220]
MIPv6	Mobile IP for IP version 6. See [b-IETF RFC 3775]
MLM-FE	Mobile Location Management Functional Entity
MMCF	Mobility Management Control Functions
MN	Mobile Node
MOBIKE	IKEv2 Mobility and Multihoming Protocol. See [b-IETF RFC 4555]
NACF	Network Attachment Control Functions
NGN	Next Generation Network
NID-FE	Network Information Distribution Functional Entity
NNI	Network to Network Interface
PKI	Public Key Infrastructure
PMIPv6	Proxy Mobile IPv6. See [b-IETF RFC 5213]
RAN	Radio Access Network
RRP	Registration Reply
RRQ	Registration Request
TAA-FE	Transport Authentication and Authorization Functional Entity
TLM-FE	Transport Location Management Functional Entity
TLS	Transport Layer Security
TTLS	Tunnelled Transport Layer Security
TUP-FE	Transport User Profile Functional Entity
UE	User Equipment
UNI	User to Network Interface
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless LAN

5 Security requirements for mobility in NGN

NGN supports multiple access technologies, such as WLAN, WiMax, and 3G RAN, etc. [ITU-T Y.2012]. Mobility support is one of the features in NGN, which includes nomadicity and handover. In NGN release 2, handover covers inter-access networks and intra-access networks scenarios [ITU-T Y-Sup.7].

NGN supports the following features:

- 1) Trust model: NGN security trust model defines three security zones: trusted, trusted but vulnerable and un-trusted [ITU-T Y.2701]. It shows that access network has to go through the security gateway before accessing the core network.

- 2) NGN supports multiple access technologies.
- 3) NGN supports several mobility protocols, such as MIPv4, MIPv6, DSMIPv6, PMIPv6 and MOBIKE.
- 4) NGN supports multi-radio UE, such as WLAN, WiMax, 3G RAN, etc.
- 5) NGN supports service continuity when handover between heterogeneous access systems.

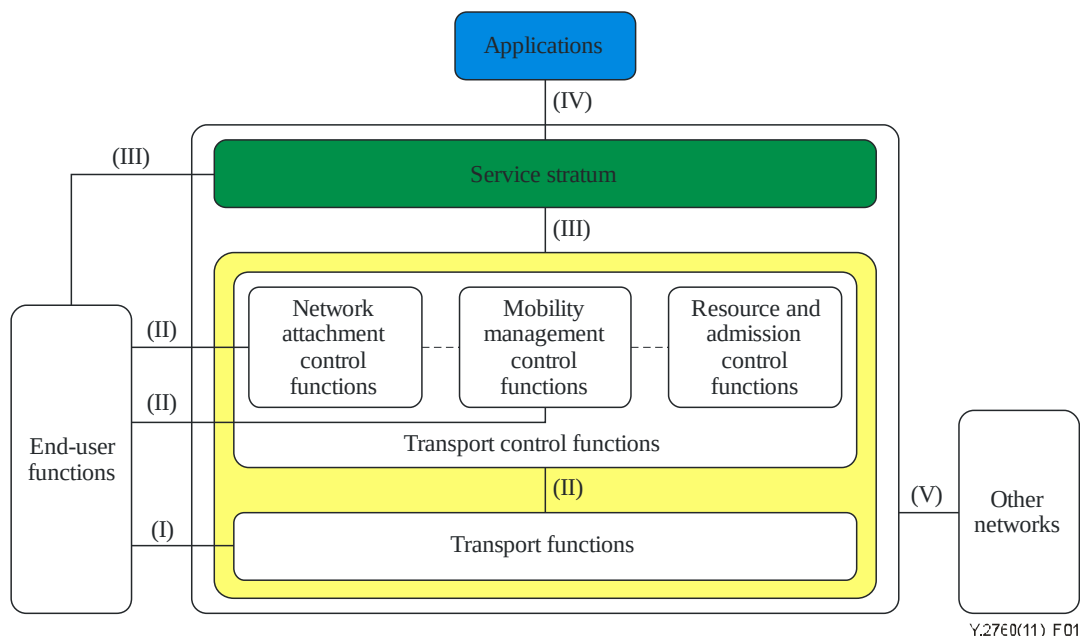


Figure 1 – Mobility security architecture in NGN

Five security feature groups are defined to:

- (I) focus on security in transport layer between end-user functions and transport functions, such as access security which may be protected physically or logically between end-user functions and access network entity in transport functions. (I) also concerns the security of UNI between end-user functions and transport functions.
- (II) focus on security in the control layer between end-user functions and the transport control function entity. (II) also focuses on security in the control message interface between transport functions entity and transport control function entity. (II) concerns the security of UNI between end-user functions and transport control functions.
- (III) focus on security of interface between end-user functions and service stratum. (III) also focuses on security in control message interface between transport control functions entity and service stratum. (III) concerns the security of UNI between end-user functions and service stratum.
- (IV) focus on security of interface between service stratum and application entity. (IV) concerns the security of ANI between end-user functions and transport functions.
- (V) focus on security of interface between NGN and other networks which include both transport layer and control layer. (V) concerns the security of NNI between NGN network and other networks.

The principles of [ITU-T X.805] are applicable to the security threats and security requirements identified in this Recommendation.

5.1 Security threats

The following security threats are identified in [ITU-T Y.2018]:

- T1 UE can be unauthorized to initiate the mobility signalling with MLM-FE.
- T2 Mobility signalling can be tampered with by intruders.
- T3 MLM-FE can be impersonated to provide false information to the UE.
- T4 The UE location can be eavesdropped by intruders.
- T5 Traffic redirection attack can happen.
- T6 Attacker can insert itself on-path by man-in-the-middle attack.
- T7 DDoS attack can consume a large quantity of network resources.
- T8 UE can be unauthorized to get information from HDC-FE or NID-FE.
- T9 HDC-FE or NID-FE can be impersonated to push false information to UE.
- T10 The signalling between the UE and the HDC-FE or the NID-FE can be modified or eavesdropped.
- T11 The user plane data can be eavesdropped or modified.

5.2 Security requirements

The following security requirements are identified in [ITU-T Y.2018]:

- R1 The UE and NID-FE are required to be mutually authenticated.
- R2 Signalling between the UE and the MLM-FE is required to be integrity- and confidentiality-protected.
- R3 Signalling between the UE and the MLM-FE is required to be protected against replay attacks.
- R4 The location privacy of the UE is required to be provided.
- R5 The UE and HDC-FE are required to be mutually authenticated.
- R6 Signalling between the UE and the HDC-FE is required to be integrity- and confidentiality-protected.
- R7 Signalling between the UE and the HDC-FE is required to be protected against replay attacks.
- R8 Low-latency authentication and signalling protection is required to be provided.
- R9 Security context transfer is required to be optimized.
- R10 The mobility security solution is required to be media independent.
- R11 Mechanisms are required to be available to protect user plane traffic between the UE and the EN-FE when the user profile so indicates.

In addition to the security requirements identified in [ITU-T Y.2018], the following security requirement is also concerned:

- R12 The security for multi-connection is required to be supported.

6 Security capabilities supported by relevant function entities

The functional entities related to mobility security in NGN are as follows:

- Transport user profile functional entity (TUP-FE)
- Transport authentication and authorization functional entity (TAA-FE)
- Mobile location management functional entity (MLM-FE)
- Handover decision control functional entity (HDC-FE)