ETSI TS 187 003 V3.4.1 (2011-03)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture

Reference

RTS/TISPAN-07038-NGN-R3

Keywords

architecture, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document defines the security architecture of NGN.

The present document addresses the security architecture required to fulfil the NGN security requirements defined in TS 187 001 [1] and includes the definition of security architectures to provide protection for each of the NGN functional architecture (ES 282 001 [2]) and its subsystems (NASS ES 282 004 [5], PES ES 282 002 [3], ES 282 007 [15], SIP and SDP call control ES 283 003 [14] and RACS ES 282 003 [4]). Where appropriate the present document endorses security mechanisms defined in other specifications.

The present document addresses the security issues of the NGN core network and the NGN access network(s) and the Customer Premises network (CPN).

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[2] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[3] ETSI ES 282 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); Functional architecture".

[4] ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture".

[5] ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".

[6] ETSI TS 183 033: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia; Diameter based protocol for the interfaces between the Call Session Control Function and the User Profile Server Function/Subscription Locator Function; Signalling flows and protocol details [3GPP TS 29.228 V6.8.0 and 3GPP TS 29.229 V6.6.0, modified]".

[7] ETSI TS 133 203: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Access security for IP-based services (3GPP TS 33.203)".

[8] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)".

[9] ETSI TS 133 222: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) (3GPP TS 33.222)".

[10] ETSI TS 133 220: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (3GPP TS 33.220)".

[11] ETSI ES 283 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Subsystem (PES); NGN Release 1 H.248 Profile for controlling Access and Residential Gateways".

[12] ETSI TS 183 019: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment; User-Network Interface Protocol Definitions".

[13] ETSI ES 283 035: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e2 interface based on the DIAMETER protocol".

[14] ETSI ES 283 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3".

[15] ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".

[16] ETSI TS 182 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Stage 2 description (3GPP TS 23.228 v7.2.0, modified)".

[17] ISO/IEC 11770-1 (2010): "Information technology - Security techniques - Key management - Part 1: Framework".

[18] ITU-T Recommendation X.811: "Information Technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework".

[19] ITU-T Recommendation X.812: "Information Technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework".

[20] ITU-T Recommendation X.814: "Information Technology - Open Systems Interconnection - Security frameworks for open systems: Confidentiality framework".

[21] ITU-T Recommendation X.815: "Information Technology - Open Systems Interconnection - Security frameworks for open systems: Integrity framework".

[22] ETSI TS 183 017: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol specification".

[23] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[24] IEEE 802.1x: "Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control".

[25] ETSI TS 181 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability Requirements".

[26] ETSI TS 187 003 Release 1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

[27] ETSI TS 185 003: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Customer Network Gateway (CNG) Architecture and Reference Points".

[28] ISO/IEC 13818-1 (2007): "Information technology -- Generic coding of moving pictures and associated audio information: Systems".

[29] Open Mobile Alliance OMA-AD-BCAST-v1-0: "Mobile Broadcast Services Architecture".

[30] Open Mobile Alliance OMA-TS-BCAST-SvcCntProtection-v1-0: "Service and Content Protection for Mobile Broadcast Services".

[31] ETSI TS 182 027: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; IPTV functions supported by the IMS subsystem".

[32] ETSI TS 102 165-2: " Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

[33] OMA DRM v2.0: "OMA Digital Rights Management V2.0".

NOTE: Available at: http://www.openmobilealliance.org/Technical/release_program/drm_v2_0.aspx.

[34] DVB: "DVB-SI | CA-System-ID".

NOTE: Available at: http://www.dvbservices.com/identifiers/ca_system_id.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 133 919: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Generic Authentication Architecture (GAA); System description (3GPP TR 33.919)".

[i.2] ETSI TS 133 221: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Support for subscriber certificates (3GPP TS 33.221)".

[i.3] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis ".

[i.4] ETSI TS 103 197: "Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt".

[i.5] ETSI TS 182 028: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN integrated IPTV subsystem Architecture".

[i.6] ETSI TS 183 063: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IMS-based IPTV stage 3 specification".

[i.7] ETSI TS 183 064: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN integrated IPTV subsystem stage 3 specification".

[i.8] DVB bluebook A125: "Digital Video Broadcasting (DVB); Support for use of DVB Scrambling Algorithm version 3 within digital broadcast systems, DVB Document A125", July 2008.

[i.9] ETSI EG 202 238: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Evaluation criteria for cryptographic algorithms".

[i.10] ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN-SEC); Threat, Vulnerability and Risk Analysis ".

[i.11] ETSI ETR 289: "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems"; October 1996.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document the terms and definitions in ITU-T Recommendations X.811 [18], X.812 [19], X.814 [20], X.815 [21], ISO/IEC 11770-1 [17] and the following apply:

content protection: protection of content or content assets during its entire lifetime

NOTE: It ensures that a user can only use the content in accordance with the license that they have been granted, e.g. play/view/hear multiple times or hours, etc.

data: any information conveyed in communication packets as well as any other information such as topology information

license: data package which represents the granted Rights to a specific user and the key related to the protected content

NGN Network Termination (NGN NT): reference point which denotes a logical demarcation point between the residential customer domain and the NGN core via access networks

NOTE: It covers the corresponding interfaces.

Policy Enforcement Function (PEF): security function that enforces policy rules

NOTE: The PEF encompasses functions for filtering and topology hiding such as typically found in firewalls and/or session border controllers.

rights: pre-defined set of usage entitlement to the content

NOTE: The entitlement may include the permissions (e.g. to view/hear, copy, modify, record, distribute, etc.), constraints (e.g. play/view/hear multiple times or hours), etc.

security domain: set of elements made of security policy, security authority and set of security relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain

NOTE: The activities of a security domain involve one or more elements from that security domain and, possibly, elements of other security domains

service protection: protection of content (data or media stream) during the delivery time or the time of transmission

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3G	3rd Generation
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, Accounting
ACK	ACKnowledge
ACR	Anonymous Communications Rejection
AF	Application Functions
AGCF	Access Gateway Control Function
AGW	Access GateWay
AKA	Authentication and Key Agreement

AMF	Access Management Function
AN	Access Network
AP	Access Point
AP	Authentication Proxy
A-RACF	Access-Resource Admission Control Function
ARF	Access Relay Function
AS	Application Server
ASP	Application Service Provider
AUTH	AUTHentication service
AUTHOR	AUTHORization service
AUTN	AUthentication TokeN
BDS	Broadcast Distribution Service
BGCF	Breakout Gateway Control Function
BSD/A	BCAST Service Distribution/Application
BSF	Bootstrapping Server Functionality
BSM	BCAST Subscription Management
CA	Certification Authority
CA-PID	Conditional Access-Packet Identifier
CAS	Conditional Access System
C-BGF	Core Border Gateway Function
CEF	Content Encryption Function
CLF	Connectivity session and repository Location Function
CND	Customer Network Device
CNG	Customer Network Gateway
CONF	CONFidentiality service
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CSCF	Call Session Control Function
DoS	Denial-of-Service
DRM	Digital Rights Management
ECM	Entitlement Control Message
EMM	Entitle Management Message
FA	File Application Component
FD	File Delivery Component
FE	Functional Entity
FFS	For Further Study
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GRE	Generic Routing Encapsulation
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	HyperText Transport Protocol
IBCF	Interconnection Border Control Function
I-BGF	Interconnection Border Gateway Function
I-CSCF	Interrogating Call Session Control Function
ID	IDentity
IETF	Internet Engineering Task Force
IF	InterFace
IKE	Internet Key Exchange
IMPI	IMS Private User ID
IMPU	IMS Public User ID
IMS	IP Multimedia Subsystem
INT	INTegrity service
INTF	INTegrity Function
IP	Internet Protocol
IPsec	Internet Protocol security
IPTV	Internet Protocol TeleVision
IRG	IMS Residential Gateway
ISIM	IMS Subscriber Identity Module
ISUP	ISDN User Part
IUA	ISDN Q.921-User Adaptation
KM	Key Management service

KMF	Key Management Function
LIF	Licensing Issuing Function
LTKM	Long Term Key Message
MBMS	Multimedia Broadcast Multicast Service
MDF	Media Delivery Function
ME	Mobile Equipment
MGC	Media Gateway Controller
MGCF	Media Gateway Control Function
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
NACF	Network Access Configuration Function
NAF	Network Application Function
NASS	Network Access SubSystem
NAT	Network Address Translation
NDS	Network Domain Security
NGCN	Next Generation Corporate Network
NGN NT	NGN Network Termination
NGN	Next Generation Network
OIR	Originating Identity Presentation
P-CSCF	Proxy Call Session Control Function
PDBF	Profile DataBase Function
PEF	Policy Enforcement Function
PEK	Programme Encryption Key
PES	PSTN/ISDN Emulation
PID	Packet Identifier
PMT	Programme Map table
RACS	Resource Admission Control Subsystem
RGW	Residential GateWay
SAA	Service Access Authentication
SCF	Service Control Function
SCP	SmartCard Profile
S-CSCF	Serving Call Session Control Function
SDP	Session Description Protocol
SEG	Security Gateway
SEGF	SEcurity Gateway Function
SEK	Service Encryption Key
SG	Service Guide
SGF	Signalling Gateway Function
SIP	Session Initiation Protocol
SKMF	Service Key Management function
SLF	Subscription Locator Function
SMF	Service Membership Function
SP	Service Protection
SPDF	Service Policy Decision Function
SP-E	Service Protection Encryption Component
SPF	Service Protection function
SP-KD	Service Protection Key Distribution Component
SP-M	Service Protection Management Component
SSC	Support for Subscriber Certificates
SSF	Service Selection Function
STKM	Short Term Key Message
TE	Terminal Equipment
THIG	Topology Hiding Interconnection Gateway
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
TLS	Transport Layer Security
TS	Technical Specification
UA	User Agent
UAAF	User Access Authorization Function
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
UPSF	User Profile Server Function

USIM	UMTS Subscriber Identity Module
WLAN	Wireless Local Area Network
XCAP	XML Configuration Access Protocol
XML	eXtensible Markup Language

4 NGN Security

4.0 Overview

This clause provides an overview of the NGN security document.

The NGN security architecture is designed to support the requirements for NGN Security defined in TS 187 001 [1] that have been derived from the results of application of the ETSI Threat, Vulnerability and Risk Analysis (TVRA) method defined in TS 102 165-1 [i.3] and captured in TR 187 002 [i.10].

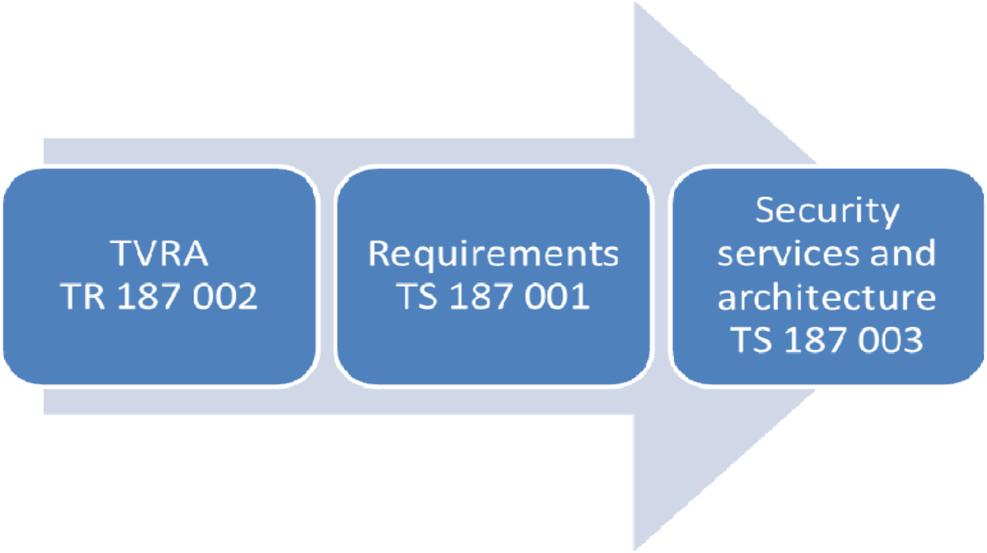


Figure 1: The main documents of the TISPAN Security suite

4.0a Security services identified in TS 187 001 and TR 187 002

TR 187 002 [i.10] has identified those threats and threat agents that when enacted against the NGN lead to a level of risk that has to be mitigated. TR 187 002 [i.10] identifies the security services required to provide mitigation that are then documented as requirements to be met by the NGN in TS 187 001 [1]. Table 1 summarises the services identified in each of TR 187 002 [i.10] and TS 187 001 [1]. The services are implemented using the framework defined in TS 102 165-2 [32].

Table 1: Summary of security services identified in TR 187 002 [i.10] and TS 187 001 [1]

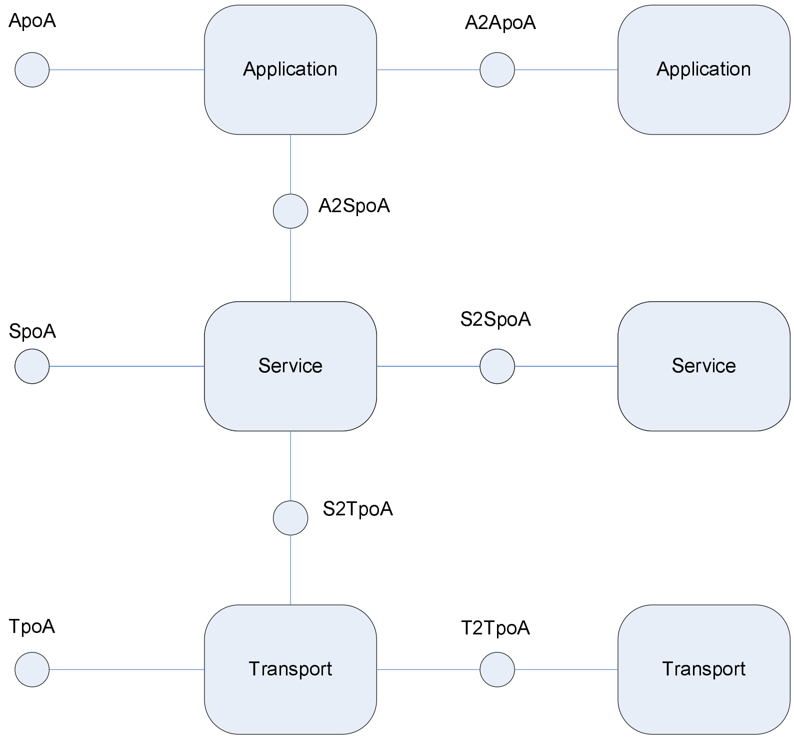
Threat Identifier	Security Threat Subsystem/Feature: short description	Primary NGN Security Requirement [1]	Security service identified
T-8	PES: Attack potential for denial-of-service on publicly addressable interfaces	R-AD-1 R-AD-3	Availability
T-16	NASS-IMS bundled: IP Spoofing	R-AA-24 R-AA-13 R-NF- 2	Authentication
T-11	NASS-IMS bundled: Interception at the customer interface, air interface present	R-CD-18	Confidentiality
T-14	NASS-IMS bundled: Attack potential for manipulation at the customer interface, air interface present	R-CD-13	Integrity
T-18	NASS-IMS bundled: Attack potential for	R-AD-1	Availability

Threat Identifier	Security Threat Subsystem/Feature: short description	Primary NGN Security Requirement [1]	Security service identified
	manipulation at the customer interface (denial-of-service)		
T-19	NASS-IMS bundled: "line-id poisoning" attack	R-AA-24 R-AA-13 R-NF- 2	Authentication
T-5	PES: Attack potential for manipulation between networks (without SEG)	R-CD-2	Integrity
T-1	PES: Attack potential for interception at the customer interface	R-CD-15 R-CD-16	Confidentiality
T-3	PES: Attack potential for manipulation at the customer interface	R-CD-13	Integrity
T-10	NASS-IMS bundled: Attack potential for interception at the customer interface, no air interface	R-CD-20	Confidentiality
T-13	NASS-IMS bundled: Attack potential for manipulation at the customer interface, No air interface present	R-CD-15	Integrity
T-9	PES: Attack potential for denial-of-service on non-publicly addressable interfaces	R-AD-3	Availability
T-4	PES: Attack potential for manipulation in the fixed network	R-CD-16	Integrity
T-7	PES: Attack potential for manipulation between networks (with SEG)	R-CD-16	Integrity
T-12	NASS-IMS bundled: Attack potential for interception at the customer interface (e1 IF)	R-CD-8	Confidentiality
T-2	PES: Attack potential for interception at the customer interface	R-CD-19	Confidentiality
T-15	NASS-IMS bundled: Attack potential for manipulation at the customer interface (e1 IF)	R-CD-15	Integrity
T-17	NASS-IMS bundled: Invalidation of IP address not signalled	R-CD-13 R-CD-8	Authentication

The NGN shall support security associations for each of Authentication, Authorisation (in support of availability), Integrity and Confidentiality.

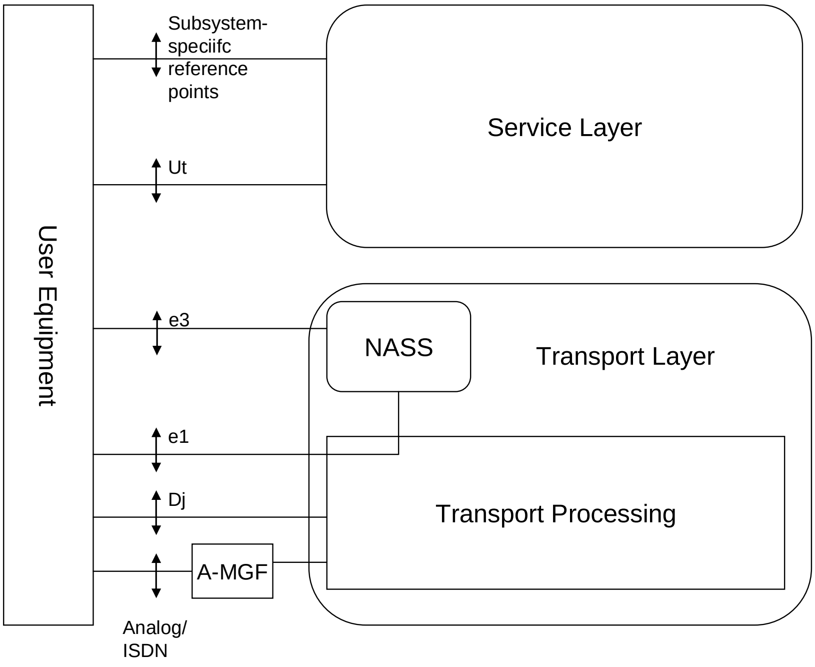
4.1 NGN security architecture

The NGN security architecture extends the abstract security architecture defined in clause 4 of TS 102 165-2 [32] (see Figure 2) and provides the mappings shown in Table 2. In addition the security architecture overlays the core NGN architecture defined in ES 282 001 [2].



NOTE: For NGN an example of the service is Voice over IMS;
For NGN the transport layer is represented by NASS; and
- For NGN an example of the application layer is IPTV.

Figure 2: Abstract architecture for security countermeasure application



NOTE 1: As considered in TR 187 002 [i.10] the e1 reference point does not terminate in NASS.
NOTE 2: As considered in TR 187 002 [i.10] the e3 reference point is a management reference point only and only exists when the UE is a CNG, and has no bearing on the communications architecture.
NOTE 3: As considered in TR 187 002 [i.10] Ut is an application layer reference point.
NOTE 4: The Gm reference point between the UE and the IMS service platform is not shown.
NOTE 5: The Dj reference point is a media point and is used to carry RTP and RTCP data only.

Figure 3: UE reference points from ES 282 001 [2]

Table 2: Mapping from TS 102 165-2 [32] abstract reference points to NGN architecture

Abstract reference point (from TS 102 165-2 [32])	NGN reference point	Security service building block defined	Authentication principal	Location of security association definition	SEGF applies at Za (TS 133 210 [8]) (see note 3)
TpoA	e1	Authentication Confidentiality Integrity Key management	Network Access Identifier (NAI)	IEEE 802.1x [24] as defined in TS 183 019 [12] (note 1)	No
	Dj	n/a			
	Z	n/a			
	ST	n/a			
SpoA	Gm	Authentication Confidentiality Integrity Key management	IMSI, IMPU	TS 133 203 [7] (note 2)	No
ApoA	Ut				No
T2TpoA	e5	Authentication Confidentiality Integrity Key management			Yes
	Iz	n/a			
S2SpoA					Yes
A2ASpoA					Yes
A2SpoA					Yes
S2TpoA	e2	Authentication Confidentiality Integrity Key management		ES 283 035 [13]	Yes
	Gq'	Authentication Confidentiality Integrity Key management		TS 183 017 [22]	Yes

NOTE 1: IEEE 802.1x [24] is defined for use to secure Ethernet access and makes the assumption that the NASS architecture (see ES 282 004 [5]) is modified to combine the ARF/AMF to the authenticator function and the UAAF/SPDF acting as the authentication server.

NOTE 2: TS 133 203 [7] provides support for a number of authentication schemes including SIP/HTTP-digest and the NASS bundled options (i.e. authentication at NASS is accepted by IMS without invoking any IMS specific authentication functions).

NOTE 3: A SEGF is used where the domains are discrete and is mandatory for all exposed inter-domain interfaces providing integrity and confidentiality of signalling content with source address authentication. Connections between the different NGN components within the same NGN network are the "Zb" interfaces. These interfaces are mandatory for implementation and optional for use, depending on operator risk assessment

The following reference points are wholly within the transport domain and are not exposed:

- a1, a2, a3, a4 and thus are assumed to be in the security domain of the transport domain

The following reference points are wholly within the service domain and are not exposed:

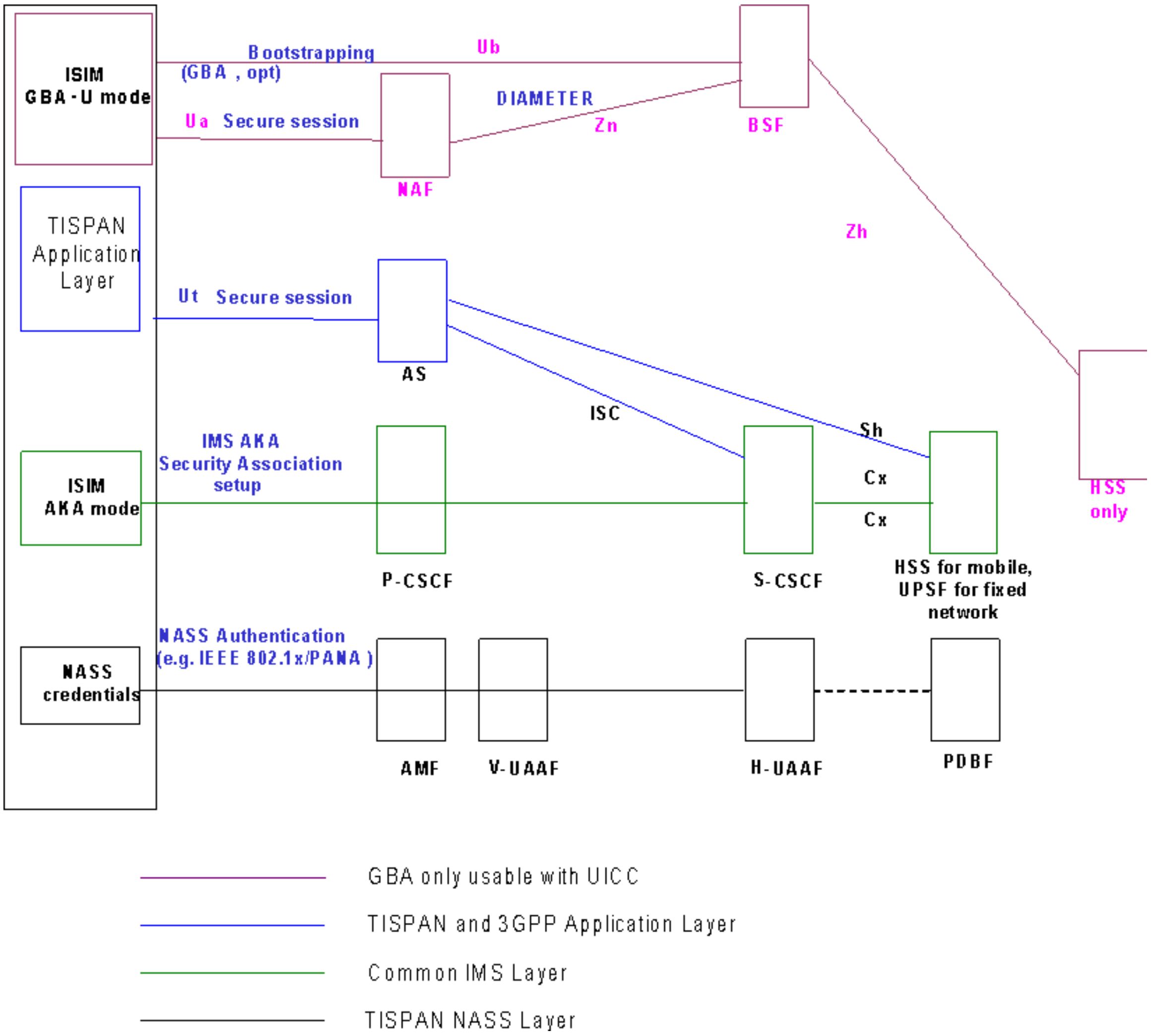
The NGN architecture is described by the following elements:

- NGN security domains
- NGN Security services (see the mappings given in Table 1 and Table 2):
- NGN Security protocols supporting the security services

In addition the security architecture endorses Security Gateways (SEGs) defined by TS 133 210 [8] and renames them for the NGN application as Security Gateway Function (SEGF) to secure signalling and control communication among network entities/FEs.

In addition to security domains the NGN security architecture also defines logical security planes across multiple domains supporting the abstract model of Figure 2 mapped to specific NGN functionality:

- Transport instantiated in the NASS security plane.
- Service instantiated in the IMS security plane.
- Application instantiated in the GAA/GBA key management plane.



NOTE 1: The terminology of V-UUAF and H-UAAF is not consistent with that used in the NASS stage 2 document ES 282 004 [5] where the terms UAAF Proxy and UAAF Server are used.
NOTE 2: The interface Zh between BSF and UPSF is defined in 3GPP but not endorsed in TISPAN NGN.
NOTE 3: No functional decomposition of UPSF, PDPF and HSS has been carried out therefore any sharing of functionality between these elements is not considered in the present document.
NOTE 4: In the IMS the HSS and UPSF functions overlap.

Figure 4: Usage of security FEs in the NGN security architecture

For NASS an authentication security association shall be established between the UE and the PDPF/H-UAAF. The NASS principal shall be the NAI with the role of authenticator being taken by the PDPF/H-UAAF.

NOTE 1: It is assumed that the PDPF hold the credentials for authentication of the NASS with the H-UAAF carrying out the authentication process.

The NASS security plane encompasses the security operations during network attachment for gaining access to the NGN access network. The visited UAAF (V-UAAF) in a visited access network relays authentication message to/from the home NGN network (equivalent in operation to the VSS or VLR in PLMN); the V-UAAF (if present) may be a proxy while the home UAAF (H-UAAF) shall process the authentication message and decide authorization (equivalent in operation to the HSS or HLR in PLMN). The H-UAAF takes into account user profile information that is stored in the PDBF (equivalent to the Authentication Centre in PLMN). The PDBF shall hold the profiles of the NASS user.

NOTE 2: In the NGN, an IMS subscriber may register over an IP access session established by a NASS subscriber, which may not be the same as the IMS subscriber. In such cases there is no relation between the profile/credentials used at the NASS level and at the IMS level.

NOTE 3: The PDBF may be co-located with the UPSF.

NOTE 4: The dashed lines between H-UAAF and PDBF and between the NAS/AS and the UPSF indicate interfaces which are not defined in the present document.

For IMS the required security associations are defined by TS 133 203 [7] and the procedures defined therein shall apply. The UPSF shall hold the user profiles used at the IMS level. The GBA/GAA security plane encompasses the NAF and BSF FEs for application layer security.

NOTE 5: The TISPAN Application Server (AS) could have access to BSF as described in TS 133 220 [10] in which case UPSF takes the role of the HSS and has a connection to the BSF through reference points Zn and Zh.

4.2 Security domains

The following security domains are defined for the NGN:

- Customer domain:
  - This domain includes the UE which may be either a single terminating device or a customer premises access point such as that defined in TS 185 003 [27] as a Customer Network Gateway (CNG) hosting one or more Customer Network Devices (CND) in the context of a Customer Premises Network. This may also include a corporate network defined as Next Generation Corporate Network (NGCN).

NOTE 1: The UE may be owned by the customer or by the operator.

NOTE 2: The NGN IMS Residential Gateway as specified for Release 1 in TS 187 003 [26] has been further elaborated as part of the functionality of the CNG as specified in TS 185 003 [27].

- Access network security domain:
  - with FEs hosted by the access network provider.
- Visited NGN security domain:
  - with FEs hosted by a visited network provider where the visited network may provide access to some application services (AF). The visited network provider may host some applications and may own an own database of subscribers. Alternatively, or additionally, the visited network provider may outsource some application services to the home network provider or even to a 3rd application provider.
- Home NGN security domain:
  - with FEs hosted by the home network provider where the home network may provide some application services (AF). The home network provider hosts some applications and owns a database of subscribers.
- 3rd party application network security domain:
  - with FEs hosted by the ASP where the ASP provides some application services (AF). The ASP may be a separate service provider from the visited or the home network provider. The ASP may need to deploy authorization information offered by the visited or home network provider.

Figure 5 shows the partitioning of the NGN network into security domains.

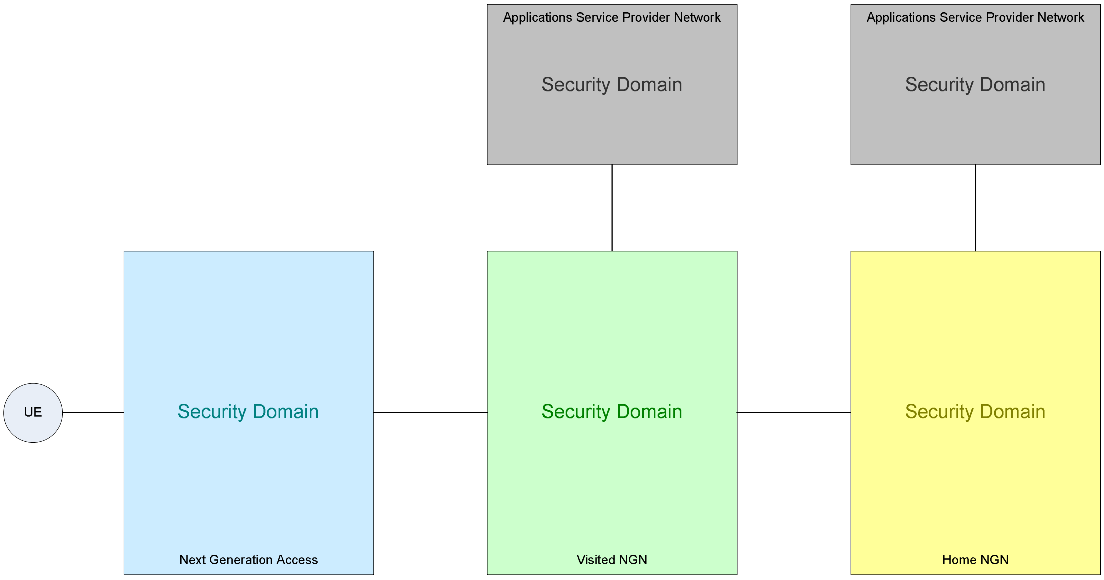


Figure 5: NGN security domains

NOTE: Although Figure 5 shows the Next Generation Access and the Visited NGN as separate entities, they may, in practice, be co-located.

4.3 Void

4.4 Void

4.5 PES Security Architecture

4.5.1 Security for H.248 within PES

Figure 6 depicts the security architecture for using H.248.1 for PSTN/ISDN service over IP according to ES 283 002 [11]. Access Gateway (AGW), Residential Gateway (RGW), the control subsystem (AGCF with MGC) and the control protocols are considered to belong entirely to a single operator's security domain as indicated by the dashed, red line.

The specified H.248 security options should not be used, as these interfaces are considered to be within a security domain. ES 283 002 [11], clause 5.1.3 specifies that no security measures, either IPsec or TLS, are used on the IUA interfaces and no specific countermeasures are applied to the GRE interface carrying packet data.

NOTE: In any other case when the H.248, IUA and GRE interfaces do not fall within a single operator's security domain, a different risk may apply and appropriate countermeasures may be needed. A security architecture for such cases is left as for further study.

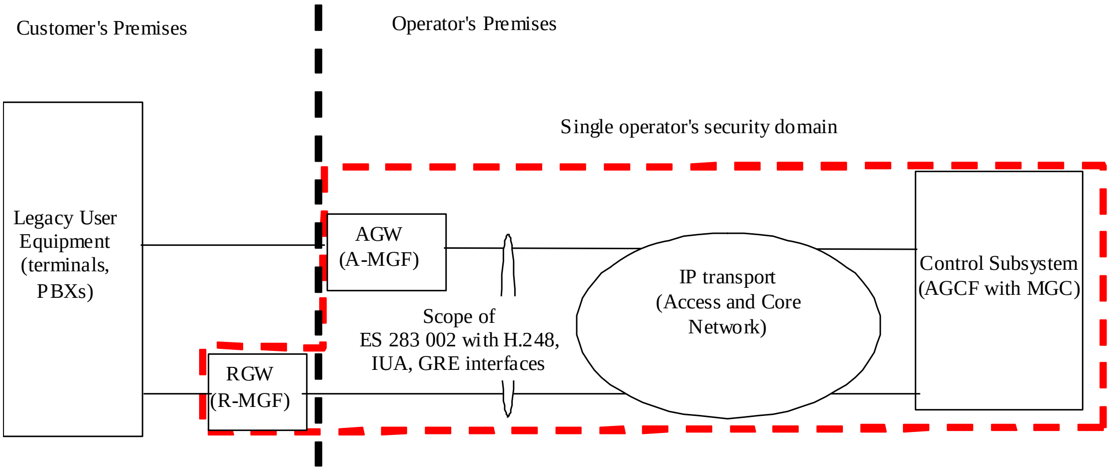

Customer's Premises
Operator's Premises
Single operator's security domain
Legacy User Equipment (terminals, PBXs)
AGW (A-MGF)
RGW (R-MGF)
Scope of ES 283 002 with H.248, IUA, GRE interfaces
IP transport (Access and Core Network)
Control Subsystem (AGCF with MGC)

Figure 6: Reference architecture for profile of the Gateway Control Protocol (H.248.1), for controlling access and residential gateways connecting analog lines and ISDN primary and basic accesses, in order to emulate PSTN/ISDN services over IP (see ES 283 002[11])

4.6 Application security architecture

The AS architecture enables the user to manage information related to his services, such as creation and assignment of Public Service Identities, management of authorization policies that are used e.g. by Presence service, conference policy management, etc.

The XCAP architecture and security architecture is endorsed by TS 183 033 [6]. This defines the usage of a set of security protocols for protection of XCAP traffic on the Ut interface between UE and AS. The two optional method endorsed are HTTP digest over TLS and GAA (see TS 133 222 [9]). An authentication proxy may be used optionally for user authentication, as defined in TS 183 033 [6] and TS 133 222 [9], see figure 7.

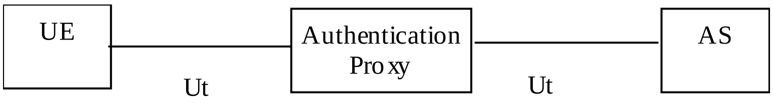


Figure 7: Authentication proxy in the Ut interface path

4.6.1 Generic Authentication Architecture (GAA)

3GPP has defined "Generic Authentication Architecture" (GAA), confer TR 133 919 [i.1]. This is a framework for mutual authentication of user applications and network elements/applications (called Network Application Function or NAF).

3GPP GAA consists of three parts:

- Generic Bootstrapping Architecture (GBA) -TS 133 220 [10].
- Support for Subscriber Certificates (SSC) - TS 133 221 [i.2].
- Access to NAF using HTTPS - TS 133 222 [9].

4.6.1.1 Generic Bootstrapping Architecture (GBA)

GBA is specified in TS 133 220 [10].

GBA enables:

- The establishment of initial secret between the User Equipment and a network element (called Bootstrapping Server Function) in the 3GPP home network. This phase is called "Bootstrapping":
  - The bootstrapping is based on UMTS AKA, i.e. HTTP Digest AKA, it requires the use of USIM or ISIM application on UICC. At the end of the bootstrapping phase, the UE and the BSF share the master key Ks.
- The derivation of application specific keys (called NAF-specific keys).

There are two options for the derivation of those application specific keys:

- GBA_ME: it does not require any change to the UICC:
  - The application specific key, Ks_NAF, is derived in the ME using Ks.
- GBA_U: it requires changes to the UICC, but it provides enhanced security by storing certain keys on the UICC:
  - In GBA_U, the bootstrapped key Ks, does not leave the UICC. GBA-aware UICC may generate two keys from Ks, called K_int_NAF and Ks_ext_NAF (Ks_ext/int_NAF). Ks_int_NAF is used by the UICC while Ks_ext_NAF is sent to the ME.

4.6.1.2 Support for Subscriber Certificates (SSC)

Support for subscriber certificates is specified in TS 133 221 [i.2].

GBA is one possible solution to secure certificate issuance to subscribers. Ua protocol is PKCS#10 with HTTP Digest Authentication.

4.6.1.3 Access to NAF using HTTPS

It is specified in TS 133 222 [9].

It specifies how to access over HTTP is secured using TLS (i.e. HTTPS) in GAA.

4.6.2 HTTP Digest authentication for UICC-less CNDs

GAA/GBA framework cannot be applied in TISPAN deployment scenarios where CNDs do not have access to the UICC. To address these scenarios, this clause defines an authentication architecture allowing the re-use of SIP digest credentials also at the application layer.

HTTP Digest authentication, as defined in RFC 2617 [23], permits the authentication of a user or CND at application layer.

RFC 2617 [23] describes an open framework with different options to be implemented (e.g. single-way vs. mutual authentication, partial integrity protection, and others). According to the local policy, the operator may define different mapping credentials and different ways for the provisioning of the customer credentials to the CND and Application Server. The selection of the proper credentials at running time is performed by means of the "realm" mechanism.

To simplify the provisioning, the Service Access Authentication (SAA) element enables the usage of the user credentials stored in the UPSF also at application layer. Figure 8 shows the integration of the SAA in the NGN with the main reference points involved.

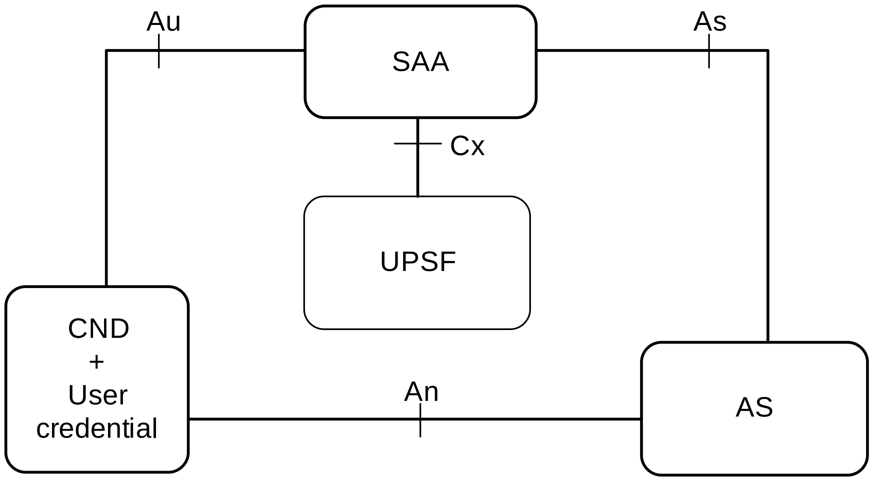


Figure 8: HTTP digest authentication for UICC-less CNDs

The Application Server (AS, such as IPTV or Web portals) communicates to the customer (i.e. CND) by using the An reference point, which implements the application specific protocol (e.g. XML over HTTP) and to the SAA by using the As reference point. Many options are available on the As interface for the synchronization and coordination of the information needed for the authentication and authorization of the customers.

The present document identifies the protocols applicable for the following reference points:

- Au: HTTP Digest authentication as specified in RFC 2617 [23]. The actual implementation details depend on the local policy of the Operator. The authentication flow can be protected by means of TLS (i.e. HTTPS).
- Cx (Diameter): Cx subset, in order to support the authentication (i.e. TS 183 033 [6] for digest authentication). The SAA behaves like a S-CSCF as defined in TS 183 033 [6] clause 6.3. In particular the SAA requests, for each authenticating users, the H(A1) value that is a hash (i.e. MD5) of the username (e.g. IMPI), realm, and the secret shared between the NGN and the customer. The communication between SAA and UPSF via Cx shall follow the rules of Network Domain Security as specified in TS 133 210 [8]. If multiple UPSF exist in the network, SLF is used to select the appropriate instance as specified in ES 282 001 [2], clause 6.5.2. For simplification SLF is not represented on figure 8.
- As: The communication between SAA and AS via As shall follow the rules of Network Domain Security as specified in TS 133 210 [8].

5 Void

6 Void

7 Void

7.1 Void

7.2 Void

8 Void

9 Security Architectures for IPTV

There are two kinds of media protection mechanisms: content protection and service protection. Media content protection is required for the content owner for the control of how the content is used, in particular, on what conditions it can be played, replayed, stored for reuse and copied. Service protection is used to control who can receive the media but it does not control how that media is used after it is delivered to the recipient. It is important to note that service protection is for the service provider's interests and content protection for the content owner's interests. The service provider may implement one or both kinds of protection. The actual content protection solution used by the content owner is not specified by TISPAN but the integration of such content protection is described in clause 9.1.

NOTE As an example, a content protection solution can be offered by a DRM or by a Conditional Access System (CAS).

9.1 Content Protection

For content protection the following elementary functions are used:

- Content licensing: This elementary function handles the licenses issuing related functions, including generation and distribution of the licenses to the desired entities. This shall be known as LIF.
- Key management: This elementary function handles the management of the security keys on behalf of the content usage profiles as defined in the content licensing, including generate and provide the keys and corresponding parameters to the desired entities. This shall be known as KMF.
- Content encryption: This elementary function handles the content protection related operations, e.g. content encryption and encapsulation operations, etc. This shall be known as CEF.

These three elementary functions may be flexibly located in existing functional entities or new ones as a whole or in independent parts.

NOTE: Some of these elementary functions may be executed on-line (in real-time) or off-line (in this case could be part of the management).

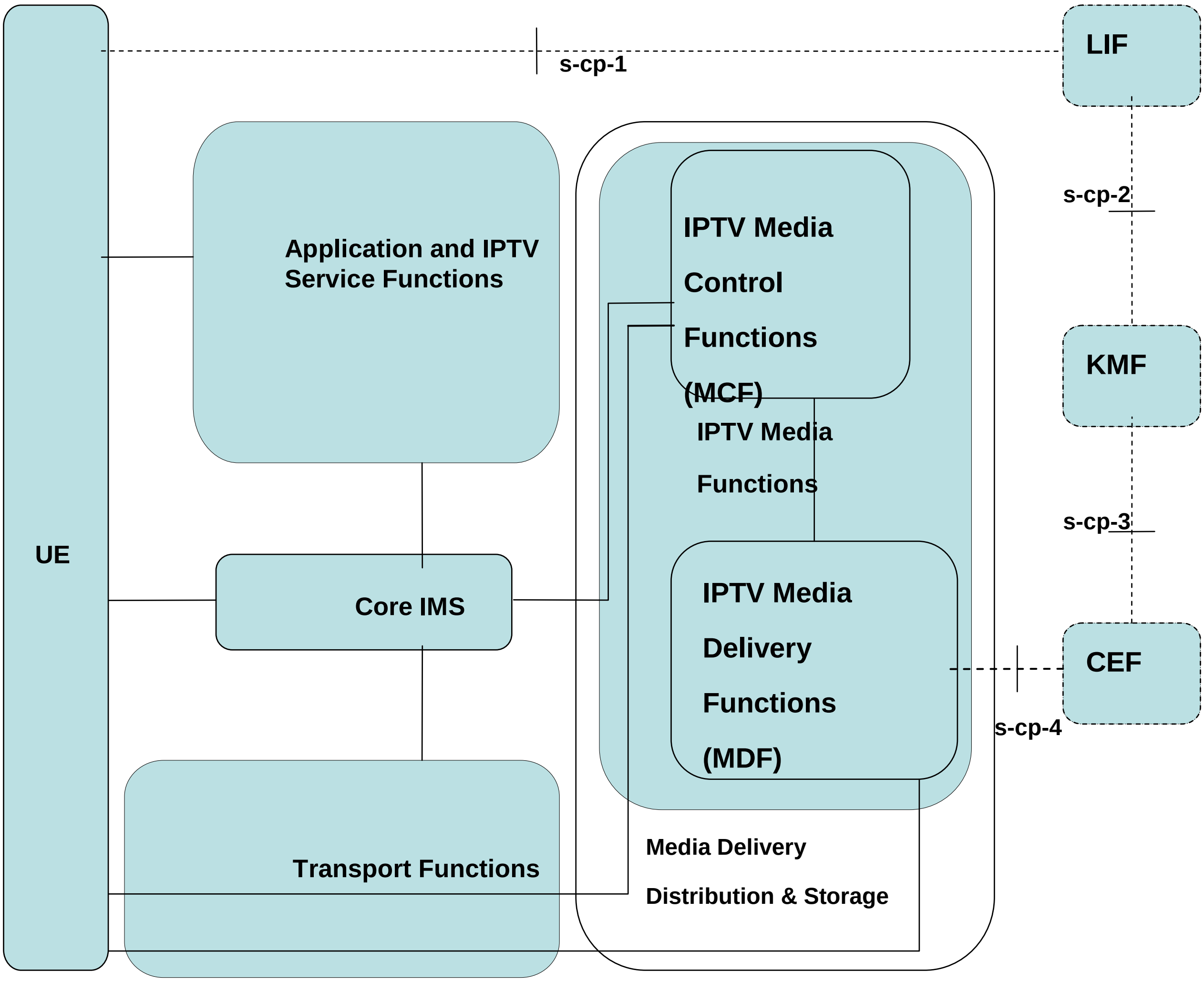

s-cp-1
LIF
s-cp-2
KMF
s-cp-3
CEF
s-cp-4
UE
Application and IPTV Service Functions
IPTV Media Control Functions (MCF)
IPTV Media Functions
Core IMS
IPTV Media Delivery Functions (MDF)
Transport Functions
Media Delivery Distribution & Storage

Figure 9: IPTV Content Protection Architecture

The content protection architecture illustrated above is based on the IPTV service architecture defined in TS 182 027 [31] and TS 182 028 [i.5].

9.1.2 Reference Points

NOTE: This clause describes the content protection reference points. Reference points that are not security specific can be referred to TS 182 027 [31] and TS 182 028 [i.5].

9.1.2.1 LIF – UE (s-cp-1)

This reference point between LIF and UE is used for the delivery of keys and license/rights to UE.

9.1.2.2 KMF – LIF (s-cp-2)

This reference point between KMF and LIV LIF is used for the delivery of keys to LIF.

9.1.2.3 KMF – CEF (s-cp-3)

This reference point between KMF and CEF is used for key exchange.

9.1.2.4 CEF – MDF (s-cp-4)

This reference point between CEF and MDF is used for the transmission of the protected content and possibly content protection messages to MDF.

NOTE: Content Encryption is part of Content Preparation and Content Preparation is not in the scope of TISPAN IPTV Architecture.

9.2 Service Protection

The service membership (SMF), service key management (SKMF) and service protection (SPF) functions described in this clause each involve a set of elementary functions required as part of a generic model for service protection. The SMF, SKMF, and SPF do not duplicate, but collaborate and interact with existing elementary functions in order to perform service protection.

For service protection the following sets of elementary functions are used:

- Service membership elementary functions (SMF): This set of elementary functions handles the granting and revoking of service access rights to access the IPTV services. Metadata related to the service rights management are maintained by the SMF.

NOTE 1: The SMF is handled in an array of existing elementary functions (e.g. service key triggering function) and functional entities. For example, service authorization may be provided by the SCF, and meta-data is maintained in the UPSF.

- Service key management function (SKMF): This set of elementary functions acts on behalf of the Service Membership Function and as such manages service security keys, including generating and providing keys and corresponding parameters to the desired entities.

- Service protection function (SPF): This (set of elementary) function(s) handles the service protection related options, e.g. service confidentiality, integrity operations and authorization at the service access point, etc, using the keys generated in SKMF.

NOTE 2: The SPF includes group association, e.g. multicast group.

9.3 Optional solutions

The following optional solutions are defined:

- Any Content Protection combined with existing NGN Security Architecture

- OMA BCAST as Service Protection

9.3.1 Any Content Protection

Service protection as defined in TISPAN can be ensured with the NGN security architecture as defined in clause 4 in conjunction with any content protection solution complying with the architecture described in this clause.

NGN security architecture defined in clause 4 provides the following features:

- User Authentication

- Service Authorisation based on user authentication

- Service Confidentiality

This clause will describe the constraints which apply to a content protection solution in order to integrate with TISPAN IPTV Architecture.

9.3.1.1 Reference Points

All reference points are proprietary to the content protection system or out of scope of TISPAN IPTV Architecture.

9.3.1.2 Procedures

9.3.1.2.1 Content Preparation

Content Preparation is not in the scope of TISPAN IPTV Architecture. Content Encryption is part of Content Preparation. This clause is provided for information and is not normative.

Two main cases can be distinguished:

- For Live delivery: DVB-Simulcrypt [i.4] has defined a standard interface to integrate content protection solution to a TV head end. DVB-Simulcrypt architecture allows furthermore several content protection solutions to be integrated and used simultaneously on the same IPTV content.

- For Content On Demand delivery: When using content protection, content is usually encrypted offline and the interface between CEF and MDF is a file transfer interface.

9.3.1.2.2 Content Delivery

For IMS-based IPTV, as specified in TS 183 063 [i.6], a TISPAN UE shall support at least one of the following IPTV transport technologies:

- MPEG-2 TS encapsulation over UPD or RTP.

- Direct RTP transport.

For NGN integrated IPTV subsystem, as specified in TS 183 064 [i.7], a TISPAN UE shall be able to receive content encapsulated into MPEG-2 TS over RTP and MPEG-2 TS over UDP.

MDF shall send content compliant to these IPTV transport technologies.

As a consequence, TISPAN IPTV Architecture, when using MPEG-2 TS encapsulation, supports any content protection applied within MPEG-2 TS, in particular content protection compliant with ISO/IEC 13818-1 [28]. ISO/IEC 13818-1 [28] defines how to signal a content protection solution and transport content protection solution specific messaging information, i.e. ECM transporting Control Words / Transport Encryption Keys and EMM transporting Rights management messages in MPEG-2 TS.

Content protection solution applied on MPEG-2 TS and compliant to signalling and transport as defined in ISO/IEC 13818-1 [28] may be used in conjunction with the NGN security architecture as defined in clause 4.

NOTE: Such a content protection solution might need to exchange additional information with UE via s-cp-1 reference point (see Right and Key Delivery)

9.3.1.2.3 Right and Key Delivery

This interface is proprietary between the content protection solution and the content protection client in the UE and the security of this interface is managed by the content protection solution.

NOTE: This interface is not always needed when content protection messaging is transported via MDF (for example when content protection messages (EMM) are transported in-band within MPEG2-TS streams as defined in [28]).

9.3.2 OMA BCAST

TISPAN IPTV Service Protection can be ensured by means of OMA BCAST as specified in [29] and [30].

OMA BCAST is a 4-layer model allowing two key management profiles: the Smartcard Profile and the DRM Profile.

The SmartCard Profile (SCP) is a key management system based on symmetric key model. It uses either 3GPP MBMS security model relying on the (U)SIM on UICC or 3GPP BCMCS security model relying on R-UIM/CSIM.

The DRM Profile is key management system based on the Public Key Infrastructure provided by OMA DRM v2.0 [33].

TISPAN IPTV Service Protection can be ensured by means of the Smartcard Profile or the DRM Profile.

In order to ensure maximum interoperability, OMA BCAST defines a common layer for traffic encryption and allows the other layers of key management to be implemented using either the SmartCard Profile or the DRM Profile.

OMA BCAST Subscription Management that support service or content protection shall support Interface SP-4. Interface SP-4 may support DVB Simulcrypt, allowing the deployment of several service protection solutions in parallel and that could be already deployed on the field. The description of DVB Simulcrypt support is described in clause of Service and Content Protection for Mobile Broadcast Services specification [30].

9.3.2.1 OMA BCAST Functional Architecture

The OMA BCAST logical entities are described in [29].

Table 3: Descriptions of Logical Entities

Logical Entity	Major Functionality
Entities in-scope of OMA BCAST	
BCAST Service Application	Represents the service application of the BCAST Service, such as, streaming audio/video or movie file download. It encompasses the functionality of media encoding and interaction related to BCAST Service. It also provides the BCAST service attributes to the BCAST Service Distribution/Adaptation and BCAST Subscription Management. It may generate charging information, for example, according to the user charging information that it obtains from the BCAST subscription management and the content creator. Legacy mechanisms may be used for charging information generation and delivery.
BCAST Service Distribution/Adaptation	Responsible for the aggregation and delivery of BCAST Services, and performs the adaptation of the BCAST Enabler to underlying BCAST Distribution Systems. It provides the functionality of File and Stream Distribution, Service Aggregation, Service and Content Protection (i.e. data encryption, TEK generation, and protection key message distribution), Service Guide generation and delivery, Notification Delivery, and the adaptation to the underlying BDS. The functionality of adaptation to each BDS may vary depending on the underlying BDS.
BCAST Subscription Management	Responsible for service provisioning such as subscription and payment related functions, the provision of information used for BCAST Service reception, and BCAST Terminal management. It provides the functionality of Notification, Service Protection management, Content Protection management, Service Guide generation support, Terminal Provisioning and interaction with the BDS Service Distribution/Adaptation to communicate/manage subscription information with the Terminal. It may send the user charging information to the BCAST service application.
Terminal	The user device that receives broadcast content as well as the BCAST service related information, such as, service guide, content protection information. The user device may support the interactive channel in which case it would be able to directly communicate to the network regarding the available services.
Entities out-of-scope of OMA BCAST	
Content Creation	Source of content, may provide support for delivery paradigms (e.g. streaming servers); provides base material for content descriptions.
BDS Service Distribution/Adaptation	Responsible for the coordination and delivery of broadcast services to the BDS for delivery to the terminal, including file and stream distribution, and Service Guide distribution. It may also include key distribution, broadcast subscription management, and accounting functionalities. BDS Service Distribution/Adaptation may not exist in certain BDSs. In that case it would be considered a "Null Function". It works with the interactive network to perform service discovery, BDS-specific service protection and handles other interaction functions. It also works with the BDS for content delivery to the terminal.
Broadcast Network	Specific support for the distribution of content over the broadcast channel. This may involve the same or different radio network from that used by the interactive channel.
Interaction Network	Specific support for the interaction channel. This may involve the same or different radio network from that used by the broadcast channel.

9.3.2.2 Mapping between TISPAN IPTV Architecture and OMA BCAST Service Protection Functional Architecture

The TISPAN IPTV architecture is specified in TS 182 027 [31].

Table 4: Mapping between TISPAN IPTV and OMA BCAST logical entities

TISPAN IPTV entities			BCAST entities		
High level entity	**Name**	**Function**	**High level entity**	**Name**	**Function**
Application and IPTV service functions	SDF	Generates and provides service attachment information; provides personalized service discovery	BSD/A	SG (access fragment, SDP)	This fragments are used by the terminal to retrieve the content and associated streams in the broadcast or unicast network. Typically the SDP contains multicast address to retrieve the content.
Application and IPTV service functions	SSF	Provides the service selection information; provides service selection presentation information	BSD/A	SG (service, content, schedule fragments, purchase fragments… displayed to user)	These fragments are used for the selection by the user of content. Information in these fragments are displayed to the user
Application and IPTV service functions	SCF	Service authorisation; Credit limit and credit control.	BSM	SP-M for service protection function	Service Protection Management Component (SP-M) in the BSM is responsible for the registration of Terminal and the authentication/authorization of User; Generation of Key messages.
Media Delivery, distribution & storage	MCF		BSD/A	FD and FA	
Media Delivery, distribution & storage	MDF	Handling media flows delivery; May additionally process, encode or transcode (if required) media to different required media formats (e.g. TV resolution depending on terminals capabilities or user preferences); May perform content protection functionalities (e.g. content encryption).	BSD/A	FD and FA	The File Delivery Component (FD) in the network is responsible for the delivery, aggregation, and adaptation of a file or a bundle of files; If the service protection is done by BCAST, the FD may cooperate with the Service Protection function to encrypt the bearer to be used for file delivery. The File Application Component (FA) in the network is responsible for receiving a file or a bundle of files to be broadcast from the Content Creation and sending the file as well as file attributes and additional information; If the content protection is done by BCAST, the FA may cooperate with the Content Protection function to encrypt the file.

TISPAN IPTV entities			BCAST entities		
High level entity	**Name**	**Function**	**High level entity**	**Name**	**Function**
Application and IPTV service functions	UPSF	The UPSF holds the IMS user profile and possibly IPTV specific profile data	BSM	Equivalent to HSS for Smartcard profile	

Transport functions	Transport control function			BDS Service Distribution/Adaptation;
				Broadcast Network;
				Interaction Network	

Transport functions	Transport processing function			BDS Service Distribution/Adaptation;
				Broadcast Network;
				Interaction Network	

9.3.2.3 Mapping between TISPAN IPTV Service Protection based on 4-layer Key Hierarchy and OMA BCAST Service Protection Functional Architecture

Table 5: Mapping between TISPAN IPTV and OMA BCAST for IPTV key management

TISPAN IPTV entities			BCAST entities		
High level entity	**Name**	**Function**	**High level entity**	**Name**	**Function**
	KMF	KMF execute bootstrapping procedures to establish a shared User Root Key; encrypted with URK is transferred from KMF to UE	BSM	SP-M	The Service Protection Management Component (SP-M) in the BSM is responsible for the registration of Terminal and the authentication/authorization of User. SP-M is also responsible for the LTKM generation and the LTKM delivery over Interaction Channel. LTKM contains SEK and PEK and it is delivered to SP-C in Smartcard
	CEF	CEF encrypts the content and interacts with KMF to acquire TEKs encrypted with SEK; CEF transfers the TEKs encrypted with SEK and content encrypted with TEKs to MCF/MDF; TEKs encrypted with SEK and content encrypted with TEKs are delivered from MCF/MDF	BSD/A	SP-Encryption; SP Key distribution	• The Service Protection Encryption Component (SP-E) in the BSD/A is responsible for encrypting file or stream for delivery over the broadcast channel or the interaction channel. • The Service Protection Key Distribution Component (SP-KD) in the BSD/A is responsible for the distribution over the broadcast channel of the STKM, generation of TEK and the optional generation of STKM.
	MCF/MDF		BSD/A		
Transport functions	Transport control function			BDS Service Distribution/Adaptation; Broadcast Network; Interaction Network	
Transport functions	Transport processing function			BDS Service Distribution/Adaptation; Broadcast Network; Interaction Network	

9.3.2.4 OMA BCAST Smart Card Profile adaptation to MPEG-2 TS

In OMA BCAST, content streams are sent in UDP/RTP packets and may be encrypted at different layers:

- IP layer using IPSEC;
- RTP layer using SRTP; or
- at applicative layer using ISMACrypt.

In TISPAN IPTV:

- When the RTP transport is used for the transport of the content, one of the encryption protocol defined in OMA BCAST shall be used and the STKM shall be transported over UDP/RTP as defined in OMA BCAST.
- When the content is transported in MPEG2 TS encapsulated in UDP/RTP the STKM may be transported in the MPEG2 TS and the following adaptation of OMA BCAST Smartcard profile applies.

9.3.2.4.1 STKM Transport in MPEG-2 TS

In OMA BCAST, the audio and video streams are transported in RTP multicast packets on the IP stack integrated in the broadcast bearer. This bearer depends on the technology used. For example, in case of DVB-H, the IP stack is transported in the MPEG2 TS of the DVB-H bearer.

In case of TISPAN IPTV, audio and video streams may be transported in MPEG2 TS on the IP network.

To guarantee the synchronization of the delivery of keys used to encrypt the content and the encrypted content itself, an adaptation of STKM message to the MPEG2 TS is defined in this clause. This is especially important when the Quality of Service is not guarantee as for unmanaged networks.

OMA BCAST has defined short term key messages (STKM) to vehicle the content key (TEK) on MIKEY messages from the server to the terminal or the Smartcard using RTP protocol in multicast mode.

In the context of systems where the services are transported in a MPEG2 Transport stream (TS), messages dedicated to the conditional access system like the ECM are transported in the MPEG2 TS in specific packets identified by the CA_PID.

The PID of the ECM packet associated to a program is retrieved in the PMT of this program in the CA-descriptor (Descriptor-tag = 0x09).

In case of OMA BCAST SCP (Smart Card Profile), the following adaptation is defined to permit the broadcast of TEK in the MPEG2 TS in ECM defined by DVB.

Signaling of ECM in PMT for OMA BCAST SCP:

The CA-descriptor retrieved in the PMT shall contain the following data for OMA BCAST SCP

- the CA-system-ID associated to OMA BCAST SCP (OMA BCAST 1.0 (U)SIM Smartcard Profile using 3GPP GBA_U) and defined by DVB [34] (http://www.dvbservices.com/identifiers/ca_system_id); and
- the CA-PID associated to the ECM

The STKM shall be transported in the associated CA-PID in private section.

Integration of ECM in private section of the CA packet

ECMs are integrated in PES packets with the stream-id set to "1111 0000".

These PES packets are encoded as private section as defined in MPEG2 TS specification ISO/IEC 13818-1 [28].

The table_id for the ECM is given in the ETR 289 [i.11] and shall be 0x80 or 0x81 the last bit is the toggle bit indicating that the section has been changed.

To ensure that TEK are present when the corresponding encrypted content is broadcasted, the TEK shall be broadcasted in advance during the previous crypto period. When the user zaps to a new channel, to ensure that the Smartcard is able to compute the TEK without waiting for the next crypto period, the ECM containing the current TEK shall be broadcasted during the crypto period corresponding of its use in the encrypted content. The ECM shall then contain the current and the next TEK during a crypto period.

The MIKEY message defined in OMA BCAST SCP is integrated in the CA_data_bytes defined in ETR 289 [i.11] as follows.

Table 6: CA_message_section

Syntax	No. of bits	Identifier
CA_message_section() {		
table_id	8	uimsbf
section_syntax_indicator	1	bslbf
DVB_reserved	1	bslbf
ISO_reserved	2	bslbf
CA_section_length	12	uimsbf
for(i=0; I<N; i++) {		
CA_data_byte	8	bslbf
}		
}		

All the fields except CA_data_bytes are defined in ETR289 [xx]. CA_data_bytes contain the MIKEY message defined in OMA BCAST specification for the STKM of the Smartcard profile for the TEK$_{n}$ and the TEK$_{n+1}$

Table 7: CA_data_bytes for TEK$_{n}$ and the TEK$_{n+1}$

Common HDR (TEK$_{n}$)
EXT MBMS (TEK$_{n}$)
EXT BCAST (TEK$_{n}$)
TS (TEK$_{n}$)
KEMAC (TEK$_{n}$)
Common HDR (TEK$_{n+1}$)
EXT MBMS (TEK$_{n+1}$)
EXT BCAST(TEK$_{n+1}$)
TS (TEK$_{n+1}$)
KEMAC (TEK$_{n+1}$)

The payloads depicted in table above are defined OMA-TS-BCAST_SvcCntProtection [30].

The terminal shall filter the ECM using the toggle bit and send the corresponding STKMs to the smartcard when the toggle bit has changed or when the user zaps to another channel.

The terminal shall send the STKMs contained in the ECM separately using the AUTHENTICATE Command as defined in OMA BCAST specification.

The terminal shall send the STKM corresponding to the TEK$_{n}$ only once to avoid a replay detection error in the Smartcard.

The STKM corresponding to the TEK$_{n}$ shall be sent before the STKM corresponding to the TEK$_{n+1}$ to avoid a playback processing in the Smartcard.

This adaptation minimizes the impact on the standard OMA BCAST terminal and Smartcard.

Example of ECM processing

Figure 10 shows which STKM are transmitted to the Smartcard by the terminal with an example:

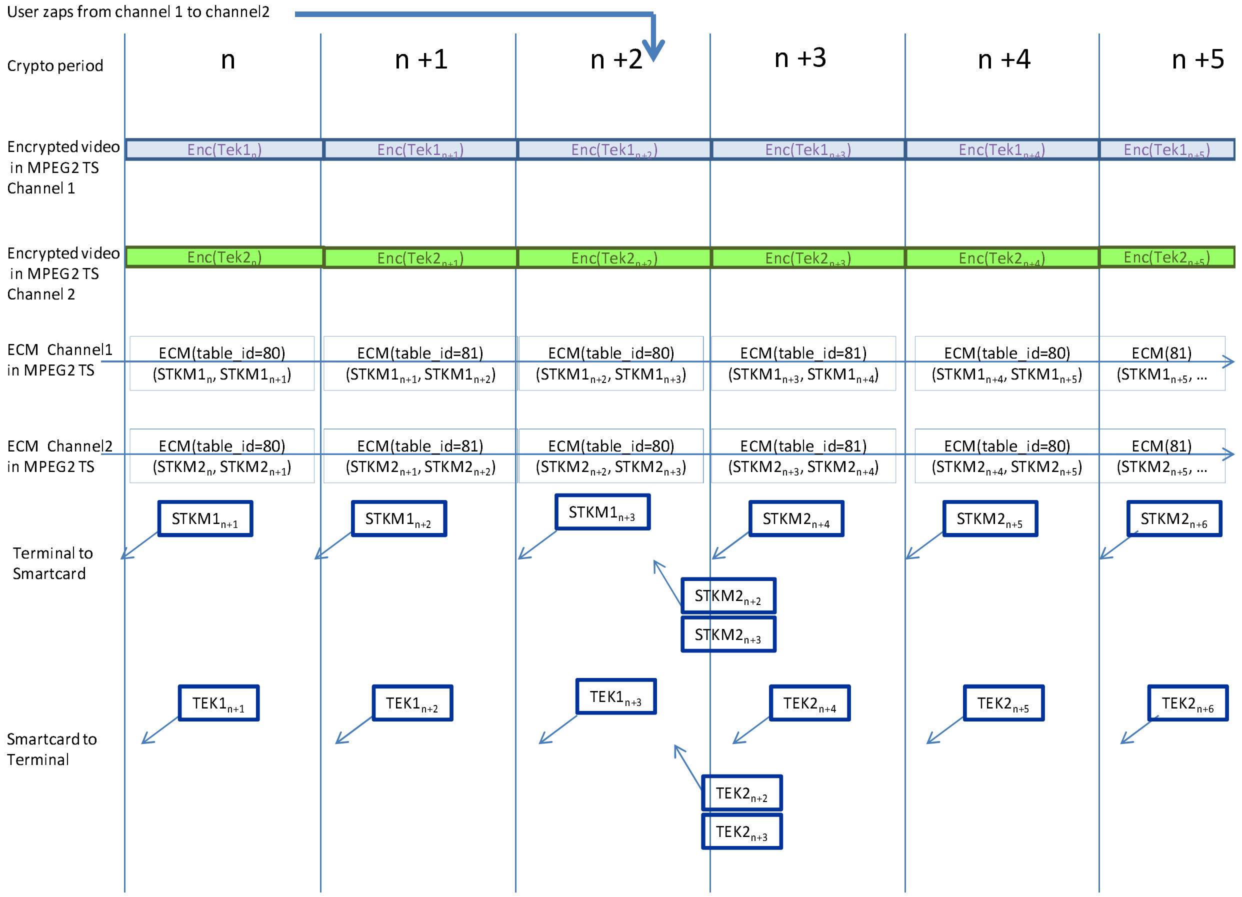

User zaps from channel 1 to channel2
Crypto period
n
n +1
n +2
n +3
n +4
n +5
Encrypted video in MPEG2 TS Channel 1
Enc(Tek1n)
Enc(Tek1n+1)
Enc(Tek1n+2)
Enc(Tek1n+3)
Enc(Tek1n+4)
Enc(Tek1n+5)
Encrypted video in MPEG2 TS Channel 2
Enc(Tek2n)
Enc(Tek2n+1)
Enc(Tek2n+2)
Enc(Tek2n+3)
Enc(Tek2n+4)
Enc(Tek2n+5)
ECM Channel1 in MPEG2 TS
ECM(table_id=80) (STKM1n, STKM1n+1)
ECM(table_id=81) (STKM1n+1, STKM1n+2)
ECM(table_id=80) (STKM1n+2, STKM1n+3)
ECM(table_id=81) (STKM1n+3, STKM1n+4)
ECM(table_id=80) (STKM1n+4, STKM1n+5)
ECM(81) (STKM1n+5, …
ECM Channel2 in MPEG2 TS
ECM(table_id=80) (STKM2n, STKM2n+1)
ECM(table_id=81) (STKM2n+1, STKM2n+2)
ECM(table_id=80) (STKM2n+2, STKM2n+3)
ECM(table_id=81) (STKM2n+3, STKM2n+4)
ECM(table_id=80) (STKM2n+4, STKM2n+5)
ECM(81) (STKM2n+5, …
Terminal to Smartcard
STKM1n+1
STKM1n+2
STKM1n+3
STKM2n+4
STKM2n+5
STKM2n+6
STKM2n+2
STKM2n+3
Smartcard to Terminal
TEK1n+1
TEK1n+2
TEK1n+3
TEK2n+4
TEK2n+5
TEK2n+6
TEK2n+2
TEK2n+3

Figure 10: Example of ECM Processing

9.3.2.4.2 STKM and MPEG-2 TS encryption

In case the content is transported in MPEG2 TS, the encryption algorithm used is defined by the Scrambling Descriptor of the program signalled in the PMT. The possible values for this scrambling descriptor are defined in the DVB bluebook A125 [i.8].

The key used for the encryption is signalled in the TS header in the transport_scrambling_control field if the TS payload is scrambled at TS level, or in the PES header in the PES_scrambling_control field if the TS payload is scrambled at PES level.

Two keys may be used, the odd key or the even key.

In the STKM of the OMA BCAST Smartcard profile, a TEK_ID in the EXT-MBMS extension is used to identify the content key.

When the TEK_ID has an even value, the key transported in the KEMAC corresponds to the even key, and when the TEK_ID has an odd value, the key transported in the KEMAC corresponds to the odd key,

An odd key returned by the smartcard will replace the previous odd key stored in the terminal, and the even key returned by the smartcard will replace the previous even key stored in the terminal. Only two keys, an even and odd keys are present in the terminal and used to decrypt the content.

10 Void

11 Void

12 Void

12.1 Void

12.2 Void

13 Security Architecture for Corporate Networks

13.1 Subscription Based Business Trunking

The same Security Architecture for connection between the NGCN and NGN will apply as between an NGN UE and NGN, please refer to clause 4.

13.2 Peering Based Business Trunking

TS 133 210 [8] shall apply to the interconnection between the NGCN and the NGN.

14 Security Architecture for Host Enterprise

The same security architecture for connection between the NGCN UE and NGN shall apply as between an NGN UE and NGN, please refer to clause 4.

Annex A (informative): NGN-relevant security interfaces

This clause identifies the security interfaces that are relevant in NGN. This annex extracts relevant material from other NGN specifications.

A.1 Network attachment security interfaces

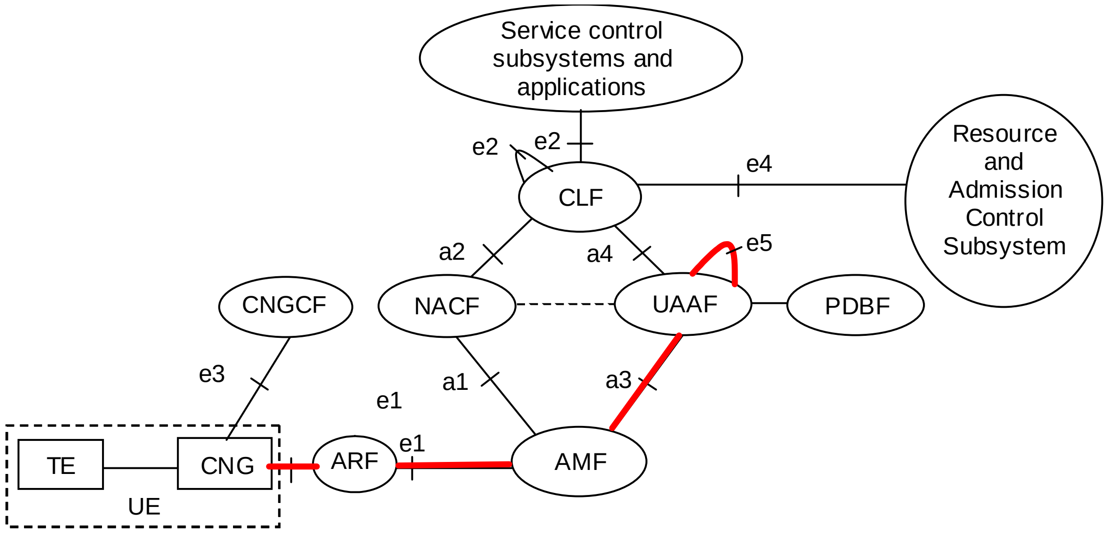
The Network Attachment Subsystem provides the following security functionalities; see ES 282 004 [5], clause 4.1:

- User authentication taking place prior or during the IP address allocation procedure.
- Authorization of network access based on user profiles.

The Network Attachment Subsystem (NASS) comprises the following security related functional entities that are relevant for Access Domain Security:

- **Customer Network Gateway (CNG)** requests access from the network.
- The **Access Management Function (AMF)** (see ES 282 004 [5], clause 5.2.2) forwards requests to the User Access Authorization Function (UAAF) to authenticate the user, authorize or deny the network access, and retrieve user-specific access configuration parameters.
  In case PPP is applied, the AMF terminates the PPP connection and provides the inter-working with the reference point to the network attachment subsystem e.g. using an AAA protocol (RADIUS or Diameter). The AMF acts as a RADIUS client if the UAAF is implemented in a RADIUS server (the AMF terminates the PPP and translates it to signalling on the a3 reference point).
- **User Access Authorization Function (UAAF)** (see ES 282 004 [5], clause 5.2.4) performs user authentication, as well as authorization checking, based on user profiles, for network access. For each user, the UAAF retrieves authentication data and access authorization information from the user network profile contained in the Profile Data Base Function (PDBF). The UAAF also collects accounting data for the changing of the service usage. The User Access Authorization Function (UAAF) acting as proxy can locate and communicate with the UAAF acting as server which can visit the PDBF user authentication data stored in, and forward access and authorization requests, as well as accounting messages, received from the AMF, to the UAAF acting as server. Responses received back in return from the UAAF acting as server will be forwarded to the AMF.
- The **Profile Database Function (PDBF)** (see ES 282 004 [5], clause 5.2.5) is the functional entity that contains user authentication data (e.g. user identity, list of supported authentication methods, authentication keys, etc.) and information related to the required network access configuration: these data are called "user network profile".
  In this release the reference point between UAAF and PDBF is not specified, i.e. UAAF and PDBF are either collocated or connected by a non-standardized interface.
  The PDBF can be co-located with the UPSF (described in ES 282 001 [2]) where this makes sense in the context on the business models being supported (e.g. if the same provider operates both the IP connectivity services and the IMS services).

Figure A.1 provides an overview of the relationships between these functional entities and related reference points. Further details about these and other NASS functionalities and the complete NASS architecture can be found in ES 282 004 [5], clause 5.1.


Service control subsystems and applications
e2
e2
CLF
e4
Resource and Admission Control Subsystem
a2
a4
e5
CNGCF
NACF
UAAF
PDBF
e3
a1
a3
e1
TE
CNG
ARF
e1
AMF
UE

NOTE: UAAF and PDBF are either co-located, or an interface exists among both FEs. This interface is not specified in NGN and is left as for further study.

Figure A.1: NASS functions involved with secure network attachment (see ES 282 004 [5])

A.1.1 Reference Point e1 (CNG - AMF)

This reference point enables the user equipment to provide user credentials (password, token, certificate, etc.) to the Network Attachment Subsystem (NASS) in order to perform network access authentication. This reference point may also enable the NASS to provide authentication parameter to the UE to perform the network authentication when mutual authentication procedure is required. Based on the authentication result, the NASS authorizes or denies the network access to the user equipment; see also ES 282 004 [5], clause 5.5.2.

A.1.2 Reference Point e2 (CLF - AF)

This reference point enables applications and service control subsystems to retrieve from the CLF network location information. The primary parameter to retrieve the location information shall be the Assigned IP address allocated to the UE; see also ES 282 004 [5], clause 5.5.1.

The form of location information that is provided by the CLF depends on the requestor.

The following information flows are used on the CLF to AF reference point:

- Location Information Query.
- Location Information Response.

A.1.3 Reference Point a3 (AMF - UAAF)

This reference point allows the AMF to request the UAAF for user authentication and network subscription checking; see also ES 282 004 [5], clause 5.5.3.

A.1.4 Reference Point e5 (UAAF - UAAF)

This reference point is intended to be used by a UAAF proxy and a UAAF server, which may be in different administrative domains. This reference point allows the UAAF-proxy to request the UAAF-server for user authentication and authorization, based on user profiles. It also allows the UAAF-proxy to forward accounting data for the particular user session to the UAAF-server; see also ES 282 004 [5], clause 5.3.6.

The UAAF-proxy will forward access and authorization requests, as well as accounting messages, received over reference point a3 from the AMF, to the UAAF-server over reference point e5. Responses received back in return from the UAAF-server over interface e5 will be forwarded to the AMF over reference point a3. A bilateral trust relationship will need to be setup between the UAAF-proxy and the UAAF-server in order to facilitate this exchange.

This reference point therefore supports AAA message exchange between the UAAF-proxy and the UAAF-server. RADIUS and Diameter are two possible options for carrier protocols on this reference point.

A.2 Service layer security interfaces

A.2.1 NGN IP Multimedia Subsystem (IMS)

The IP Multimedia Subsystem (IMS) core component of the NGN architecture (Core IMS) supports the provision of SIP-based multimedia services to NGN terminals. It also supports the provision of PSTN/ISDN simulation services.

The architecture of this subsystem is further described in ES 282 002 [3]. Figure A.2 provides an overview of the architecture, interfaces related to Access Security Domain are marked by dashed line.

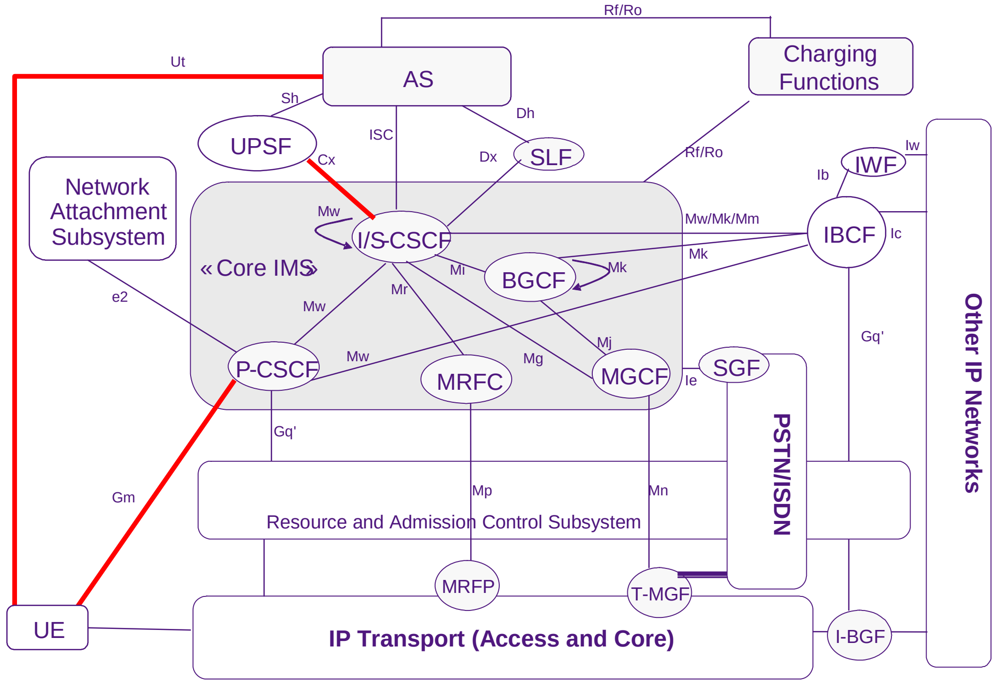


Figure A.2: NGN IMS architecture - Access security (see ES 282 002 [3])

A.2.1.1 Reference Point Gm (UE - P-CSCF)

The Gm reference point supports secure communication between an UE and the IMS, e.g. related to registration and session control; see ES 282 007 [15], clause 9.2. The security association between UE and P-CSCF is established during IMS registration procedure. All subsequent session control messages will use this security association.

NOTE 1: Exact security mechanism for Gm interface is FFS.

NOTE 2: According to TS 181 005 [25], early implementations may use the so-called "NASS-IMS bundled" or digest authentication mechanism. This mechanism is optional for implementation.

A.2.1.2 Reference Point Cx (CSCF - UPSF)

The Cx reference point supports information transfer between CSCF and UPSF. Further information on the Cx reference point is provided in ES 282 007 [15], clause 9.3.2. The following security related procedures are supported:

1) Procedures related to authorization (e.g. checking of roaming agreement).

2) Procedures related to authentication: transfer of security parameters of the subscriber between UPSF and CSCF.

Cx reference point shall support IMS AKA as mandatory authentication mechanism.

A.2.1.3 Reference Point Gq' (P-CSCF - RACS)

The Gq' reference point is used by P-CSCF to reserve resources from the transport layer; see ES 282 007 [15], clause 5.3.2. Important security functionality is related to traffic filtering. C-BGF filters unauthorized media streams, i.e. it only passes media packets through if P-CSCF has authorized them. P-CSCF uses the content of SDP payload of existing SIP sessions when making the authorization decisions.

A.2.1.4 Reference Point Iw (IWF - non-compatible SIP)

Interconnection with external networks supporting a non-compatible version of SIP is performed at the Iw reference point, via the IWF, see ES 282 007 [15]. This interface may support TLS as specified in TS 133 210 [8].

A.2.1.5 Reference Point Ic (IBCF - IMS)

IP-based interconnection with external networks supporting IMS is performed at the Ic reference point, via the IBCF; see ES 282 007 [15] and TS 182 006 [16]. Ic interface is protected using 3GPP Network Domain Security as specified in TS 133 210 [8].

Network Domain Security refers to security within a NGN operator domain and between NGN operator domains that have a fixed roaming agreement. NGN Domains are networks that are managed by a single administrative authority. The same level of security and usage of security services will be typical within a NGN Domain. A network operated by a single operator will typically constitute one NGN Domain although an operator may subsection its network into separate sub-networks.

A.2.1.6 Void

A.2.1.7 Reference Point Ut (UE - AS)

This interface enables the user to manage information related to his services, such as creation and assignment of Public Service Identities, management of authorization policies that are used e.g. by Presence service, conference policy management, etc.

TS 183 033 [6] defines the Ut interface between a UE and an AS for the purpose of manipulating user controlled setting and variables at the AS; see figure A.3.

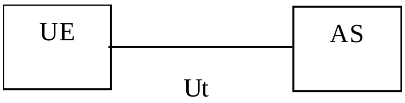


Figure A.3: Ut interface

Ut interface is protected with TLS. Authentication may be based on the Generic Authentication Architecture (GAA) as defined in TS 133 222 [9] or the HTTP Digest mechanisms defined in RFC 2617 [23].

A.3 Interconnection security interfaces

NGN may interconnect with several types of networks, e.g. at the service layer with SS7-based networks or IP-based networks, and at the transfer level with TDM-based or with IP-based networks. Interconnection may take place within the NGN trust domain, or between NGN and non-NGN trust domains. More details of NGN interconnections are available in ES 282 001 [2] and in ES 282 007 [15]. Figure A.4 represents IP-based interconnection.

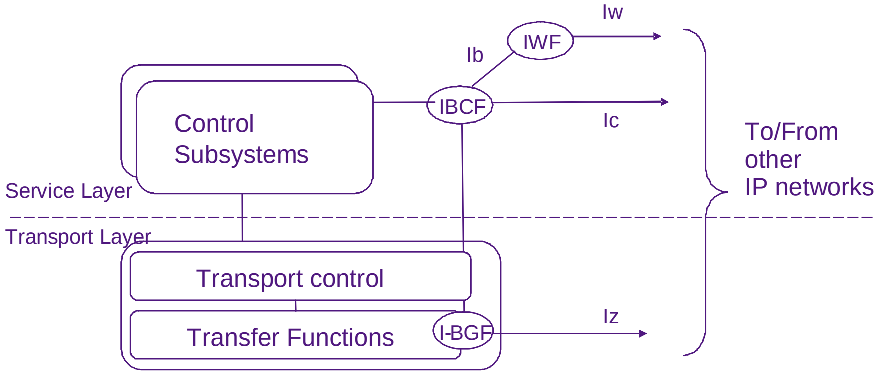


Figure A.4: IP Interconnection (see ES 282 001 [2])

Figure A.5 illustrates the case where no I-BGF is inserted. Figure A.6 illustrates the case where an I-BGF is inserted by the visited network; see also ES 282 007 [15].

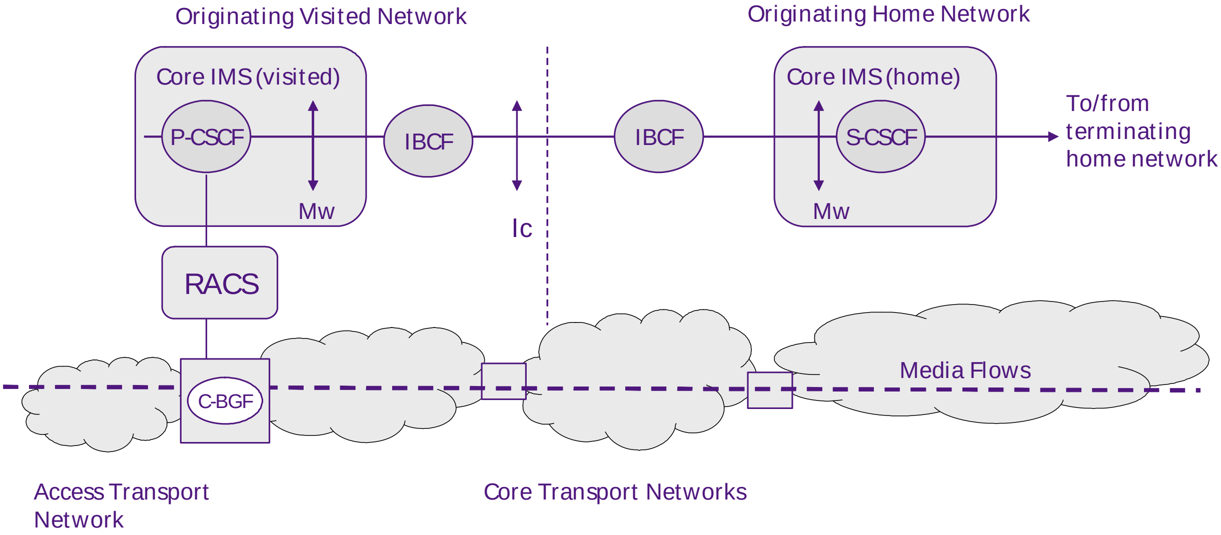
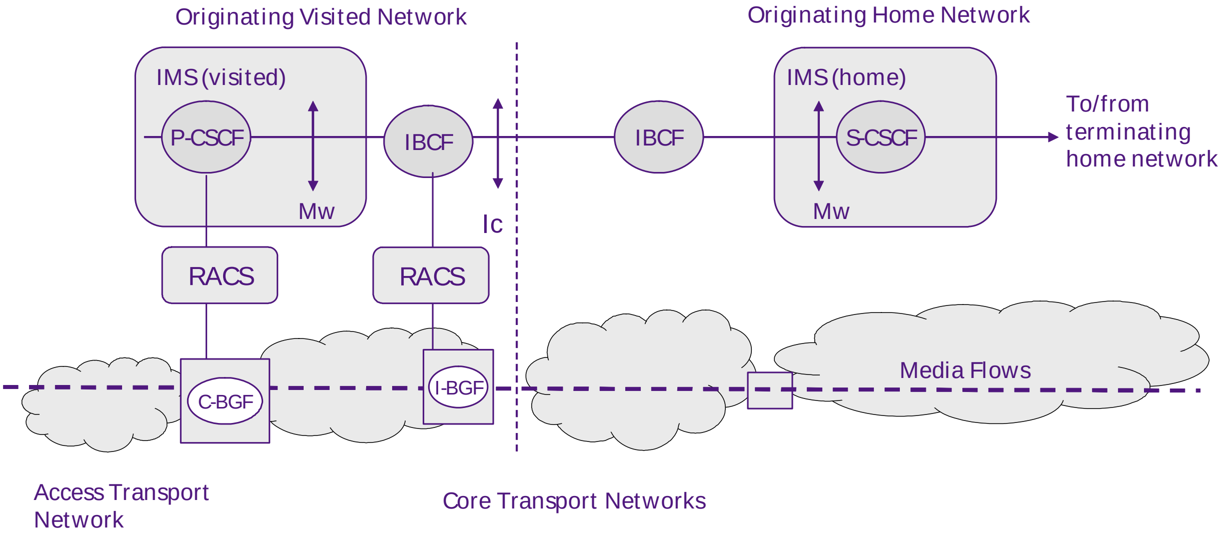


Figure A.5: IMS interconnect scenario without I-BGF (see ES 282 007 [15])



NOTE: As a network operator's option, an I-CSCF with encryption-based topology hiding capabilities (THIG) may also be inserted in the IMS before the IBCF. This is not represented in figures A5 and A.6.

Figure A.6: IMS interconnect scenario with I-BGF (see ES 282 007 [15])

TS 182 006 [16] describes further interconnect scenarios showing usage of the optional IBCF.

A.3.1 Interconnecting security at the transport layer

The security of the Iz reference point is out of the scope of the present document.

A.3.2 Interconnecting security at the service layer

Security measures when interconnecting with SS7 networks are out of the scope of the present document.

IP-based interconnection with external networks supporting is performed at the Ic reference point, via the IBCF.

Annex B (informative): Mapping of NGN Security Requirements to Security Services

Table B.1 identifies which security functions (AUTH, AUTHOR, KM, CONF, INT, PEF) are required in the NGN security architecture to fulfil the NGN security requirements (see TS 187 001 [1]).

Table B.1: Mapping of NGN - Requirements to security functions

Requirement Reference	Statement of Requirement	Specific Security Function required?	Security Functional Element
Security Policy Requirements			
R-SP-1	The NGN network shall be logically and physically divided into security domains allowing for separation of application (e.g. IMS) and transport (e.g. ADSL or UMTS). Also different operators of similar networks (e.g. IMS) shall be able to operate their own security policies.	No (see note 1)	
R-SP-2	Security mechanisms and other parameters beyond default security mechanisms shall be configurable. This shall be static for NNI interface and may be negotiated for UNI interfaces. The security mechanism negotiation shall have a certain minimum level to be defined by the security domain; e.g. avoid bidding-down attacks. Users shall be able to reject communications that do not conform to their minimum security policy.	No	
R-SP-3	The security mechanisms shall be partitioned such that the functions of authentication, data integrity, replay detection, and confidentiality may be implemented and selected independently of each other, insofar as this makes sense.	No	
R-SP-4	The UE shall always offer encryption algorithms for P-CSCF to be used for the session and the P-CSCF policy shall define whether to use encryption or not.	No (see note 2)	
R-SP-5	UE and the P CSCF shall negotiate the integrity algorithm that shall be used for the session.	Yes	KM
R-SP-6	The policy of the HN shall be used to decide if an authentication shall take place for the registration of different IMPUs e.g. belonging to same or different service profiles.	Yes	PEF, AUTH
R-SP-7	The Security Gateway Functions (SEGF) shall be responsible for enforcing security policies for the interworking between networks (see note 3).	Yes	PEF
R-SP-8	SEGFs are responsible for security sensitive operations and shall offer capabilities for secure storage of long-term keys used for IKE authentication.	Yes	SEGF, AUTH
Authentication, Authorization, Access Control and Accountability Requirements			
R-AA-1	Access to NGN networks, services, and applications shall be provided for authorized users only.	Yes	PEF, AUTHORF
R-AA-2	NGN IMS authentication shall support early deployment scenarios (with support for legacy equipments).	No	
R-AA-3	In non-early deployment scenarios, IMS authentication shall be independent from access authentication.	No	
R-AA-4	An ISIM shall be used to access any IMS service, however, exceptions may be allowed for emergency calls and early deployment scenarios.	No. Insofar as ISIM is not detectable at the interface between UE and NGN. (see note 4)	

Requirement Reference	Statement of Requirement	Specific Security Function required?	Security Functional Element
R-AA-5	ISIM based Authentication between the IMS-subscriber and the network shall comply with the authentication part of Access Security for IP-based services (see TS 133 203 [7]).	No	
R-AA-6	ISIM based Re-authentication of an IMS-subscriber shall comply with the authentication part of Access Security for IP-based services (see TS 133 203 [7]).	No	
R-AA-7	It shall be possible to prevent the use of a particular ISIM to access NGN networks and services and it should be possible to revoke a specific ISIM.	Yes	PEF
R-AA-8	NGN relevant ISIM specific information shall be protected against unauthorized access or alteration.	No	
R-AA-9	User authentication may either be hardware-based (for 3GPP UE: ISIM; i.e. proof by possession of a physical token) or be software-based (i.e. proof by knowledge of some secret information).	No	
R-AA-10	User Authentication to the NGN IMS using SIP Digest mechanisms shall be supported as an early deployment scenario.	Yes	AUTH
R-AA-11	Where both Digest and ISIM solutions are deployed by an NGN IMS operator, that operator shall determine the authentication mechanism (SIP Digest or ISIM-based) on a per-user basis. The authentication mechanism shall be enforced according to both the subscription information in the user's service profile and the specific policies of the NGN IMS operator.	Yes	PEF
R-AA-12	Transmitted passwords shall be sufficiently protected; e.g. by encryption or other techniques.	Yes	CONF, INTF
R-AA-13	For the special early deployment scenarios (see note 5), where IMS authentication is linked to access authentication, it shall be possible to gain access to IMS services after an authentication procedure. This authentication provides simultaneous access to the access network and IMS services. (see note 6)	Yes	AUTH
R-AA-14	The NGN subsystems shall be able to define and enforce policy with respect to validity of user authorization.	Yes	PEF
R-AA-15	Mutual authentication shall be supported between the UE and the AS before providing authorization.	Yes	AUTH, AUTHOR
R-AA-16	It SHOULD also be possible to support an Authentication Proxy based architecture (see note 7).	Yes	AUTH
R-AA-17	Mutual authentication shall be supported between the UE and the AP.	Yes	AUTH
R-AA-18	The AP shall decide whether a particular subscriber (i.e. the UE), is authorized to access a particular AS.	Yes	AUTHOR
R-AA-19	If an AP is used, the AS shall only authorize the access request to the requested resource (see note 8).	Yes	AUTHOR
R-AA-20	Mutual authentication should be supported between the UE and the NASS during access network level registration.	Yes	AUTH
R-AA-21	The access network shall be able to authenticate and authorize the access subscriber.	Yes	AUTH, AUTHOR
R-AA-22	Authentication and authorization to the Access Network is controlled by the operator of the Access Network.	Yes	AUTH, AUTHOR, PEF
R-AA-23	The attributes required for authentication of a user by the access network maybe provided by the network operator to whom the user has a NGN IMS subscription.	Yes	AUTHOR

Requirement Reference	Statement of Requirement	Specific Security Function required?	Security Functional Element
R-AA-24	NASS shall support both the use explicit (e.g. PPP or IEEE 802.1x [24]) and/or implicit line authentication (e.g. MAC address authentication or line authentication) of the users/subscribers. In the case of the implicit access authentication, it shall rely only on an implicit authentication through physical or logic identity on the layer 2 (L2) transport layer.	Yes	AUTH
R-AA-25	In case the CNG is a routing modem and the Customer Premises Network (CPN) is a private IP realm, authentication shall be initiated from the CNG.	Yes	AUTH, PEF
R-AA-26	In case the CNG is a bridge, each UE shall authenticate with the NASS as the IP realm in the CPN is known to the Access Network.	Yes	AUTH
R-AA-27	As the interface between the Application Function (AF) and RACS can be inter-operator, the RACS shall authenticate and authorize the Application Function (AF).	Yes	AUTH, AUTHOR
R-AA-28	A media gateway controller must be able to handle authentication of multiple media gateways, i.e. to maintain multiple security associations with different media gateways.	Yes	AUTH
R-AA-29	Authentication of NGN users and authentication of NGN terminals shall be separate.	No	
R-AA-30	Caller id and location information shall be stored according to the Common European regulatory framework by the EMTEL Service Provider. Caller ID and location information shall be validated by the EMTEL Service Provider.	No	
Identity and Secure Registration Requirements			
R-IR-1	It shall be possible to implicitly register IMPU(s). The implicitly registered IMPU(s) all belong to the same Service Profile. All the IMPU(s) being implicitly registered shall be delivered by the HSS to the S-CSCF and subsequently to the P-CSCF. The S-CSCF shall regard all implicitly registered IMPU(s) as registered IMPU(s).	No	
R-IR-2	An access identity shall be used for access authentication. This identity may or may not be used for other purposes.	No	
R-IR-3	The line ID shall be possible to use for line authentication.	No (see note 9)	
Communications and Data Security Requirements			
R-CD-1	Confidentiality and integrity of IMS signalling shall be applied in a hop-to-hop fashion. (UE-to-P-CSCF and among other NEs).	Yes	CONF, INTF
R-CD-2	Network Domain Security (NDS) shall be provided at the network layer and comply with TS 133 210 [8].	Yes	SEGF(AUTH, AUTHOR, KM, CONF, INT, PEF)
R-CD-3	All NDS/IP traffic shall pass through a SEGF (Security Gateway Function) before entering or leaving the security domain. IMS operators shall operate NDS/IP Za interface between SEGFs according to TS 133 210 [8].	Yes	SEGF(AUTH, AUTHOR, KM, CONF, INT, PEF)
R-CD-4	Security shall be provided within the network domain for the Cx interface.	Yes	SEGF(AUTH, AUTHOR, KM, CONF, INT, PEF)
R-CD-5	An ISIM based solution for IMS access security (authentication, confidentiality and integrity protection) of signalling to and from the user, shall be supported.	Yes	AUTH, INT, CONF
R-CD-6	Secure link shall be provided between UE and the P-CSCF for protection of the Gm reference point.	Yes	AUTH, AUTHOR, CONF, INT

Requirement Reference	Statement of Requirement	Specific Security Function required?	Security Functional Element
R-CD-7	In case access authentication is independent from IMS authentication: Solutions for access to the NGN core shall provide for secure transfer of signalling to the NGN core independent of the access technology. Solutions for access to the NGN core shall provide for secure transfer of signalling to the NGN core independent of the presence of intermediate IP networks connecting the NGN access with the NGN core. Solutions for access to the NGN core shall allow for mutual authentication of end user and NGN core. It shall be possible for the terminal to authenticate the user.	Yes	CONF, INT, AUTH, AUTHOR
R-CD-8	In the case where IMS authentication is linked to access line authentication the underlying access technology shall provide protection of NGN signalling and user data.	No	
R-CD-9	ISIM specific information shall be updated in a secure manner.	No	
R-CD-10	It shall be possible to protect sensitive data (such as Presence information and notifications) from attacks (e.g. eavesdropping, tampering, and replay attacks).	Yes	CONF, INT, AUTH, AUTHOR
R-CD-11	The Rq and Gq' reference points shall provide mechanism to assure security of the information exchanged.	Yes	SEGF(AUTH, AUTHOR, KM, CONF, INT, PEF)
R-CD-12	All data related to configuring the UE through the e3 if shall be protected against loss of confidentiality and against loss of integrity.	Yes	AUTH, AUTHOR, KM, CONF, INT, PEF
Integrity and Replay Protection Requirements			
R-CD-13	Integrity protection of signalling, control communications and of stored data shall be provided.	Yes	INT, AUTH, AUTHOR
R-CD-14	It shall be possible to ensure the origin, integrity and freshness of authentication data, particularly of the cipher key.	Yes	INT, AUTH, AUTHOR
R-CD-15	Integrity protection shall be applied between the UE and the P-CSCF for protecting the SIP signalling.	Yes	INT, AUTH, AUTHOR
R-CD-16	Integrity protection between Network Elements (e.g. between CSCFs, and between CSCFs and the HSS) shall rely on mechanisms specified by Network Domain Security in TS 133 210 [8].	Yes	SEGF(AUTH, AUTHOR, KM, CONF, INT, PEF)
R-CD-17	Data integrity shall be supported between the UE and the Application Server.	Yes	INT, AUTH, AUTHOR
Confidentiality Requirements			
R-CD-18	Confidentiality of communications should be achieved by cryptographic encryption. Confidentiality of stored data shall be achieved by cryptographic encryption or by access controls.	Yes	CONF
R-CD-19	Confidentiality of signalling and control messages shall be enforced if required by the application or in environments where the security policy demands confidentiality. The mechanism should allow a choice in the algorithm to be used.	Yes	CONF
R-CD-20	IMS specific confidentiality protection shall be provided for the SIP signalling between UE and P-CSCF.	Yes	CONF
R-CD-21	Confidentiality protection between Network Functions (e.g. between CSCFs, or between CSCFs and the HSS) shall rely on mechanisms specified by Network Domain Security in TS 133 210 [8].	Yes	SEGF(AUTH, AUTHOR, KM, CONF, INT, PEF)

Requirement Reference	Statement of Requirement	Specific Security Function required?	Security Functional Element
R-CD-22	It shall be possible to protect the confidentiality of user-related data which is stored or processed by a provider.	Yes	CONF
Privacy Requirements			
R-P-1	It shall be possible to protect the network topology from exposure toward other domains. It shall also be possible for a security domain to define and implement protection against traffic analysis for signalling and management protocols.	Yes	PEF
R-P-2	User location and usage patterns shall be kept from unwanted disclosure.	Yes	PEF
R-P-3	It shall be possible to protect the confidentiality of user identity data.	Yes	CONF
R-P-4	Anonymous communication sessions shall be supported in NGN either in a permanent mode or in a temporary mode communication by call. In this case the originating party identity shall not be presented to the destination party. The network to which the destination party is connected to is responsible to handle this service.	Yes	PEF
R-P-5	NGN shall support the specific case where the destination party has an override right (e.g. emergency communication sessions), and the originating party identity is provided to the destination party independent whether or not this communication session is anonymous.	Yes	PEF
R-P-6	The Anonymous Communications Rejection (ACR) simulation service shall allow the served user to reject incoming communication from users or subscribers who have restricted the presentation of their originating identity according to the OIR simulation service.	Yes	PEF
R-P-7	The NGN shall support mechanisms for the network operator to guarantee the authenticity of a user identity presented for an incoming call to a user where the call is wholly within that operator's network (i.e. originating and terminating parties are subscribers to, and resident in, a single NGN).	Yes	PEF, AUTH
R-P-8	The NGN shall provide mechanisms that allow presenting the identity of the session originator, if this is not restricted by the session originator.	Yes	PEF
R-P-9	The privacy aspect of presence information and the need for authorization before providing presence information shall be configurable by the user (i.e. presentity).	No	
R-P-10	A principal of a presentity shall, at any time, be able to control to whom, for how long and what (all or part of) presence information of the presentity is provided, and a principal of a watcher shall, at any time, be able to control to whom, for how long and what (all or part of) watcher information of the watcher is provided.	Yes	PEF, AUTHOR
R-P-11	Any services using the presence information shall ensure privacy agreement before releasing presence information. The presence service does not address deployment specific issues (e.g. where agreements are stored or how they are negotiated). It only gives requirements for privacy management.	Yes	PEF
R-P-12	It shall be possible for the sender of the message to request to hide its public ID from the recipient.	No	
R-P-13	Users may select the Identity presented when starting a session or sending a message. It shall be possible to verify this identity and to initiate a session or message in reply.		
Key Management Requirements			
R-KM-1	Key management and key distribution between SEGFs shall comply with the Network Domain Security (see TS 133 210 [8]).	Yes	KM
R-KM-2	The UE and the AS shall be able to resume a previously established secure session.	Yes	KM
R-KM-3	The key management mechanism must be able to traverse a NAT/NATP device.	Yes	KM

Requirement Reference	Statement of Requirement	Specific Security Function required?	Security Functional Element
NAT/Firewall Interworking Requirements			
R-NF-1	NGN security protocols shall work with commonly-used firewalls and shall work in environments with NAT/NATP.	No	
R-NF-2	Filters to screen the IP packets to restrict/grant access to specific bearer streams shall be supported.	Yes	PEF
R-NF-3	The SEGFs may include filtering policies and firewall functionality not required in TS 133 210 [8].	Yes	PEF
Availability and DoS protection Requirements			
R-AD-1	Mechanisms shall be provided to mitigate denial-of-service attacks.	No	
R-AD-2	Provide access control mechanisms to ensure that authorized users only can access the service.	Yes	AUTHOR, PEF
R-AD-3	It shall be possible to prevent intruders from restricting the availability of services by logical means.	Yes	AUTHOR, PEF
R-AD-4	Availability of and accuracy of location information shall be provided for the EMTEL services.	No	
R-AD-5	Availability of EMTEL PSAPs shall not be decreased by DoS attacks. EMTEL PSAPs shall be able to reconnect.	No	
Assurance Requirements			
R-AS-1	The NGN shall provide guidance for evaluating and certifying NGN equipment and systems.	No	
R-AS-2	Security implications of potential misuse of protocols used in NGN shall be documented through a TVRA. This enables users to assess the security they need before deploying the given protocol.	No	
Requirements on Strength of Security Mechanisms			
R-SS-1	The guidelines defined in EG 202 238 [33] shall be followed when defining or selecting cryptographic algorithms in NGN.	No	
NOTE 1: The split is a mandate of the regulatory regime but of itself does not require security functional entities, however at deployment the logical and physical separation requires that at the FE level some consideration has to be made for the existence of relay or proxy functions. NOTE 2: The detail definition of the UE is considered out of scope of NGN. However for confidentiality functions the configuration protocol should be capable of algorithm selection. NOTE 3: The actual inter-security domain policy is not standardized and is left to the discretion of the roaming agreements of the operators. NOTE 4: In the provision phase rather than in the activation phase the role of ISIM is clearer. NOTE 5: The two special early deployment scenarios are (also referred to as NASS Bundled authentication): a) IMS authentication is linked to access line authentication (no nomadicity). b) IMS authentication is linked to access authentication for IP Connectivity (limited nomadicity can be provided). NOTE 6: Access authentication may result in IMS services being tied to the access point (line) or to the current IP Connectivity (device). In the latter case limited nomadicity may be available. No IMS specific authentication is therefore required from the CPE/Terminal to gain access to IMS services. NOTE 7: The purpose of the AP is to separate the authentication procedure and the AS specific application logic to different logical entities. NOTE 8: The AS does not need to explicitly authenticate the user. NOTE 9: Identity and the association of identity to service do not imply an FE but may imply an information element within an information flow.			

Annex C: Void

Void.

Annex D:
Void

Annex E (informative): Open Issues in NGN Security

The following open issues are identified and remain as for further study:

1) ISIM chaining: Usage of ISIM in terminals connected through other ISIM-enabled entities (e.g. CNG).

2) PES/H.248 security: Investigate the H.248 security in case the NGN assumptions do not apply.

3) Usage/licensing of 3GPP security algorithms in NGN context.

4) How to secure the Ic IF? SEGFs could be one possibility; security functions (e.g. integrated SEGF) as part of the IBCF could be another possibility. The current text is not clear on this.

5) Security aspects of Emergency Telecommunications are not addressed yet in the present document.

Annex F: Void

Annex G (informative): Bibliography

- G. Horn, D. Kröselberg, K. Müller: "Security for IP multimedia services in the 3GPP third generation mobile system", Internet Research: Electronic Networking Applications and Policy, Vol. 13 No.2, 2003, pp. 100-106.
- Geir M. Køien et al: "Introduction to Access Security in UMTS", IEEE Wireless Communications Magazine, Feb 2004.
- ITU-T Recommendation X.800: "Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure And Applications Security Architecture For Open Systems Interconnection For CCITT Applications"; 1991.
- 3GPP2: "IMS Security Framework; S.R0086-A_v1.0_040614; 06/2004".
- ETSI TR 133 919: "3rd Generation Partnership Project; 3G Security; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); System Description (3GPP TR 33.919)".
- ETSI ETR 232: "Security Techniques Advisory Group (STAG); Glossary of security terminology".
- ETSI TS 133 310: "Universal Mobile Telecommunications System (UMTS); Network domain security; Authentication framework (NDS/AF) (3GPP TS 33.310)".
- ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat, Vulnerability and Risk Analysis".
- ETSI TS 133 141: "Universal Mobile Telecommunications System (UMTS); LTE; Presence service; Security (3GPP TS 33.141)".
- ETSI TS 122 048: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Security Mechanisms for the (U)SIM application toolkit; Stage 1 (3GPP TS 22.048)".
- ETSI TS 123 048: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Security mechanisms for the (U)SIM application toolkit; Stage 2 (3GPP TS 23.048)".
- ETSI TS 131 101: "Universal Mobile Telecommunications System (UMTS); UICC-terminal interface; Physical and logical characteristics (3GPP TS 31.101)".
- ETSI TS 131 102: "Universal Mobile Telecommunications System (UMTS); LTE; Characteristics of the Universal Subscriber Identity Module (USIM) application (3GPP TS 31.102)".
- ETSI TS 131 103: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Characteristics of the IP Multimedia Services Identity Module (ISIM) application (3GPP TS 31.103)".
- ETSI TS 129 329: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Sh interface based on the Diameter protocol; Protocol details (3GPP TS 29.329)".
- ETSI ES 283 018: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: H.248 Profile for controlling Border Gateway Functions (BGF) in the Resource and Admission Control Subsystem (RACS); Protocol specification".
- ETSI ES 283 034: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol".
- IETF RFC 3261: "SIP: Session Initiation Protocol".

- ISO/IEC 10181-1 (1996): "Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview".
- ITU-T Recommendation X.810 (1995): "Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview".
- ETSI TS 183 043: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IMS-based PSTN/ISDN Emulation; Stage 3 specification".
- ETSI TS 182 012: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IMS-based PSTN/ISDN Emulation Sub-system (PES); Functional architecture".
- ETSI TS 133 102: "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Security architecture (3GPP TS 33.102)".
- ETSI ES 283 026: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specification".
- ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".
- ETSI TS 123 002: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Network architecture".
- ETSI TS 133 234: "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Wireless Local Area Network (WLAN) interworking security".
- ETSI TR 183 032: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study into mechanisms for the support of encapsulated ISUP information in IMS".
- ETSI TR 182 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Organization of user data".
- ETSI TR 183 014: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation; Development and Verification of PSTN/ISDN Emulation".

Annex H (informative): Change history

Date	WG Doc.	CR	Rev	CAT	Title / Comment	Current Version	New Version
02-10-08	19WTD028r2	001		F	WG7 and WG5 terminology alignment "IRG"/"CNG"	2.1.1	3.0.1
					CR001 TB approved at TISPAN#19	3.0.1	3.1.0
29-10-09	21bTD197	001A	1	F	Addition of references for update of architecture description	3.1.0	3.1.1
29-10-09	21bTD197	002		F	Update of architecture diagrams and associated text	3.1.0	3.1.1
29-10-09	21bTD197	003		F	Update of security services in NGN FEs (table 5)	3.1.0	3.1.1
28-11-09	22bTD135r1	004		F	Updating Scope	3.1.1	3.2.0
12-04-10	TISPAN07(10)0049r2	006		B	Any Content Protection for IPTV Security	3.1.1	3.2.0
07-04-10	TISPAN07(10)0051r2	007	1	B	OMA BCAST	3.1.1	3.2.0
29-04-10	TISPAN07(10)0043r1	008		B	Application Layer Authentication Architecture for UICC-less CNDs	3.1.1	3.2.0
26-11-10	TISPAN07(10)0157r1	009		B	Zb interface between NGN components in an NGN network made mandatory for implementation, but still optional for use by operators.	3.2.0	3.3.0
06-12-10	TISPAN07(10)0166r2	010		C	Clarifications and deletion of duplicated material	3.3.0	3.4.0
06-12-10	TISPAN07(10)0191r3	011		F	IPTV: OMA BCAST STKM and MPEG-2 TS (transport and encryption)	3.3.0	3.4.0
					Update of Change history table	3.4.0	3.4.1

History

Document history		
V2.1.1	February 2009	Publication
V2.3.2	March 2011	Publication
V3.4.1	March 2011	Publication