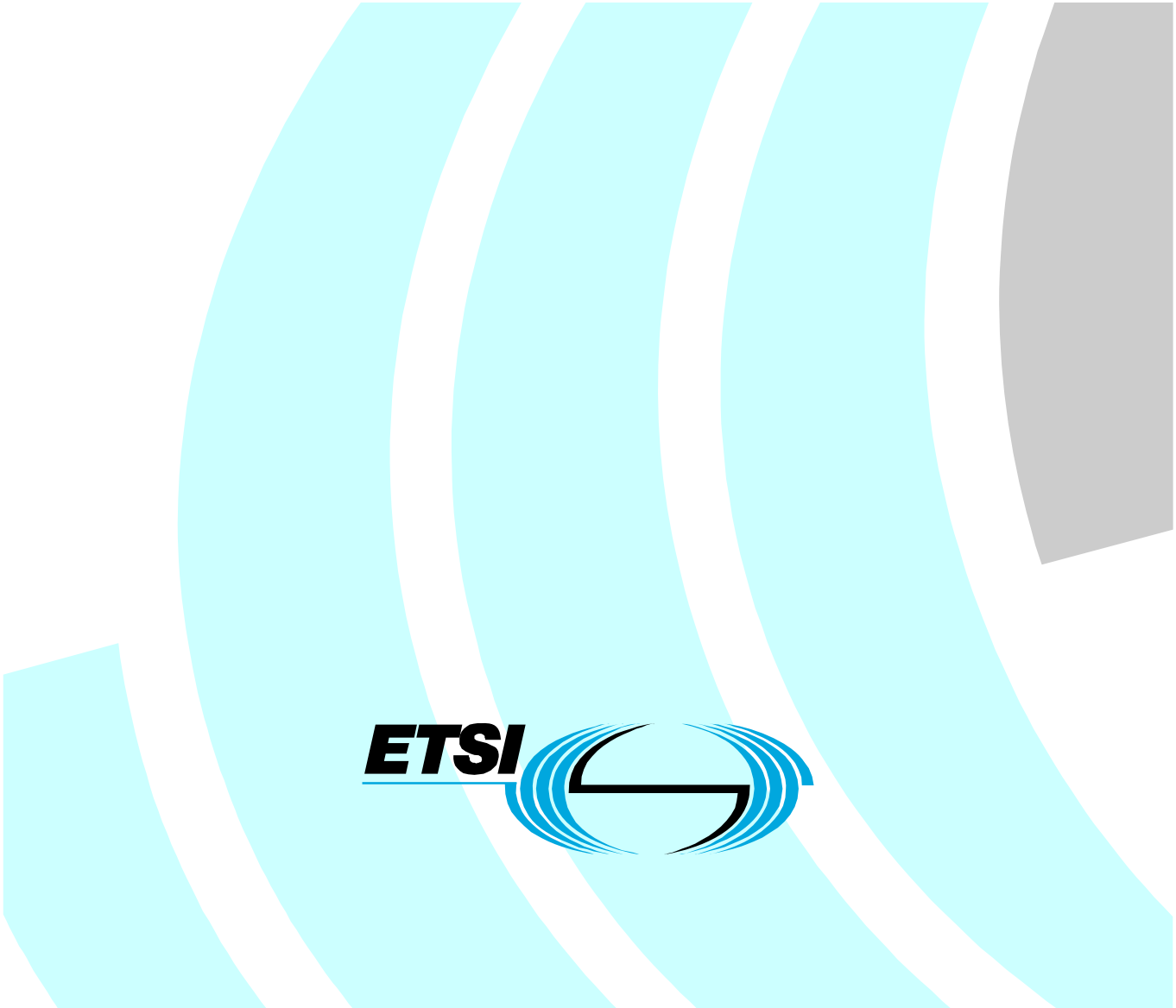
ETSI TS 187 003 V2.1.1 (2009-02)

Technical Specification

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



Reference
RTS/TISPAN-07029-NGN-R2

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

Contents

Intellectual Property Rights 5
Foreword 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 9
3 Definitions and abbreviations 9
3.1 Definitions 9
3.2 Abbreviations 10
4 NGN Security 12
4.1 NGN security architecture 13
4.2 Security domains 15
4.3 NASS and RACS security architecture 16
4.3.1 NASS-IMS Bundled Security 18
4.4 IMS security architecture 19
4.4.1 NASS-IMS Bundled Security 21
4.5 PES Security Architecture 22
4.5.1 Security for H.248 within PES 22
4.5.2 IMS-based PES Security 23
4.6 Application security architecture 23
4.6.1 Generic Authentication Architecture (GAA) 23
4.6.1.1 Generic Bootstrapping Architecture (GBA) 24
4.6.1.2 Support for Subscriber Certificates (SSC) 24
4.6.1.3 Access to NAF using HTTPS 24
5 Mapping of Security Requirements to Security Services and NGN FEs 24
5.1 Security services in NGN security architecture 24
5.2 Security Services in NGN FEs 26
5.3 Security Services on NGN Interfaces 30
5.4 Mapping of 3GPP security FEs to NGN FEs 32
6 NGN IMS Residential Gateway 34
7 Security for H248 35
7.1 R-MGF Context 35
7.2 A-MGF Context 35
8 Security Architectures for Media Security 35
9 Security Architectures for IPTV 35
10 Security Architecture for Customer Premises Networking 35
11 Security Architecture for Fixed Mobile Convergence 35
12 Interfaces out of scope 35
12.1 Interconnect Iz interface I BGF 35
12.2 RI' and Gq' 35
13 Security Architecture for Corporate Networks 36
13.1 Subscription Based Business Trunking 36
13.2 Peering Based Business Trunking 36
14 Security Architecture for Host Enterprise 36
Annex A (informative): NGN-relevant security interfaces 37
A.1 Network attachment security interfaces 37

A.1.1 Reference Point e1 (CNG - AMF) 38
A.1.2 Reference Point e2 (CLF - AF) 38
A.1.3 Reference Point a3 (AMF - UAAF) 38
A.1.4 Reference Point e5 (UAAF - UAAF) 38

A.2 Service layer security interfaces 39
A.2.1 NGN IP Multimedia Subsystem (IMS) 39
A.2.1.1 Reference Point Gm (UE/IMS Residential Gateway - P-CSCF) 39
A.2.1.2 Reference Point Cx (CSCF - UPSF) 40
A.2.1.3 Reference Point Gq' (P-CSCF - RACS) 40
A.2.1.4 Reference Point Iw (IWF - non-compatible SIP) 40
A.2.1.5 Reference Point Ic (IBCF - IMS) 40
A.2.1.6 Void 40
A.2.1.7 Reference Point Ut (UE - AS) 40

A.3 Interconnection security interfaces 41
A.3.1 Interconnecting security at the transport layer 42
A.3.2 Interconnecting security at the service layer 42

Annex B (informative): Mapping of NGN Security Requirements to Security Services 43

Annex C (informative): Implementation notes on the IMS Residential Gateway 50

C.1 B2BUA registration 50

C.2 B2BUA originating session establishment 53

C.3 B2BUA terminating session establishment 54

Annex D (informative): Supplementary Information on NASS-IMS Bundled Authentication 56

D.1 Flow Diagram for NASS Bundled Authentication 56

Annex E (informative): Open Issues in NGN Security 58

Annex F (informative): IPTV content security elements and their interactions 59

F.1 IPTV-Unicast authorized Content Delivery Option A 60

F.2 IPTV-Unicast authorized Content Delivery Option B 60

F.3 IPTV-Multicast Content Delivery 61

F.4 Mapping Content Security to IPTV architecture 62

F.5 Text contributed during release 2 63

Annex G (informative): Bibliography 66

History 67

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 definition complies with the requirements of ITU-T Recommendation I.130 [29] at stage 2.

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 (ES 282 004 [5], ES 282 001 [3], ES 282 007 [24], ES 283 003 [23] and 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) up to and including the NGN Network Termination (NGN NT) in the residential customer domain. The NGN NT denotes a logical demarcation point between the residential customer domain and the NGN core and access networks and covers the corresponding interfaces.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

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 indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

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

[9] ETSI TS 133 141: "Universal Mobile Telecommunications System (UMTS); Presence service; Security (3GPP TS 33.141)".

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

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

[12] 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)".

[13] 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)".

[14] ETSI TS 131 101: "Universal Mobile Telecommunications System (UMTS); UICC-terminal interface; Physical and logical characteristics (3GPP TS 31.101)".

[15] ETSI TS 131 102: "Universal Mobile Telecommunications System (UMTS); Characteristics of the Universal Subscriber Identity Module (USIM) application (3GPP TS 31.102)".

[16] ETSI TS 131 103: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Characteristics of the IP Multimedia Services Identity Module (ISIM) application (3GPP TS 31.103)".

[17] ETSI TS 129 329: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Sh interface based on the Diameter protocol; Protocol details (3GPP TS 29.329)".

[18] 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".

[19] 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".

[20] ETSI TS 183 019: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment; Network Access xDSL and WLAN Access Networks; Interface Protocol Definitions".

[21] 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".

[22] 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".

[23] 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".

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

[25] 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)".

[26] IETF RFC 3261: "SIP: Session Initiation Protocol".

[27] ISO/IEC 10181-1 (1996): "Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview".

[28] ISO/IEC 11770-1 (1996): "Information technology - Security techniques - Key management - Part 1: Framework".

[29] ITU-T Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[30] ITU-T Recommendation X.810 (1995): "Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview".

[31] ITU-T Recommendation X.811: "Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Authentication framework".

[32] ITU-T Recommendation X.812: "Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Access control framework".

[33] ITU-T Recommendation X.814: "Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Confidentiality framework".

[34] ITU-T Recommendation X.815: "Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Integrity framework".

[35] 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".

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

[37] ETSI TS 183 043: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IMS-based PSTN/ISDN Emulation; Stage 3 specification".

[38] 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".

[39] ETSI TS 133 102: "Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture (3GPP TS 33.102)".

[40] 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".

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

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

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

[44] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[45] ETSI TS 123 002: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Network architecture".

[46] ETSI TS 133 234: "Universal Mobile Telecommunications System (UMTS); 3G security; Wireless Local Area Network (WLAN) interworking security".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

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

[i.3] ETSI TS 182 027: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; IPTV functions supported by the IMS subsystem".

[i.4] ETSI TR 183 032: "Telecommunications and Internet converged Services and Protocols for Advanced Networks (TISPAN); Feasibility study into mechanisms for the support of encapsulated ISUP information in IMS".

[i.5] ETSI TR 182 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Organization of user data".

[i.6] ETSI TR 183 014: "Telecommunications and Internet converged Services and Protocols for Advanced Networks (TISPAN); Development and Verification of PSTN/ISDN Emulation".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

AUTHentication service (AUTH): See ITU-T Recommendation X.811 [31].

AUTHORization service (AUTHOR): See ITU-T Recommendation X.812 [32].

CONFidentiality service (CONF): See ITU-T Recommendation X.814 [33].

content protection: protection of content (files or streams) post-delivery

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

INTegrity service (INT): See ITU-T Recommendation X.815 [34].

Key Management service (KM): See ISO/IEC 11770-1 [28].

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
AN	Access Node
AP	Access Point
AP	Authentication Proxy
A-RACF	Access-Resource Admission Control Function
ARF	Access Relay Function
AS	Application Server
ASP	Application Service Provider
AuC	Authentication Centre
AUTH	AUTHentication service
AUTHOR	AUTHORization service
AUTN	AUthentication TokeN
B2BUA	Back-to-Back User Agent
BGCF	Breakout Gateway Control Function
BSF	Bootstrapping Server Functionality
CA	Certification Authority

C-BGF	Core Border Gateway Function
CEF	Content Encryption Function
CLF	Connectivity session and repository Location Function
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
ESP	Encapsulating Security Protocol
FE	Functional Entity
FFS	For Further Study
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GE	Generic Entities
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
MAA	Multimedia Auth Answer
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
n.a.	not applicable
NACF	Network Access Configuration Function
NAF	Network Application Function
NAPT	Network Address and Port Translation
NASS	Network Access SubSystem
NAT	Network Address Translation
NBA	NASS Bundled Authentication
NDS	Network Domain Security
NE	Network Element
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
PES	PSTN/ISDN Emulation
PS	Packet Switched
RACS	Resource Admission Control Subsystem
RAND	RANDom
RGW	Residential GateWay
SA	Security Association
SCF	Service Control Function
SCS	OSA Service Capability Server
S-CSCF	Serving Call Session Control Function
SDO	Standards Development Organisation
SDP	Session Description Protocol
SEG	Security Gateway
SEGF	SEcurity Gateway Function
SGF	Signalling Gateway Function
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SPD	Security Policy Database
SPDF	Service Policy Decision Function
SSC	Support for Subscriber Certificates
SSF	Service Selection Function
TE	Terminal Equipment
THF	Topology Hiding Function
THIG	Topology Hiding Interconnection Gateway
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
TLS	Transport Layer Security
T-MGF	Trunking Media Gateway Function
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
URI	Uniform Resource Identifier
USIM	UMTS Subscriber Identity Module
VGW	Voice over IP GateWay
WLAN	Wireless Local Area Network
XCAP	XML Configuration Access Protocol
XML	eXtensible Markup Language

4 NGN Security

This clause provides an overview of the NGN security document. The entire document can be seen as a documented output of a security process that loops through several stages; see figure 1, where arrows indicate logical steps and dependencies.

The present document assumes existence of a well-defined NGN architecture (see ES 282 001 [2]) that includes the IMS architecture (TS 123 002 [45]), the Network Attachment Subsystem (NASS) architecture (see ES 282 004 [5], the Resource Admission Subsystem (RACS) architecture (see ES 282 003 [4]), and the PSTN/ISDN Emulation (PES) architecture (see ES 282 002 [3]). Likewise, the present document assumes the corresponding IMS security architecture (seeTS 133 102 [39]). IMS architecture and IMS security architecture are shown as dashed boxes; those prerequisites are not specified further in the present document.

The description of the NGN security architecture has been divided in a number of smaller blocks describing the security interfaces, the security functions and security protocols, security building blocks and security components.

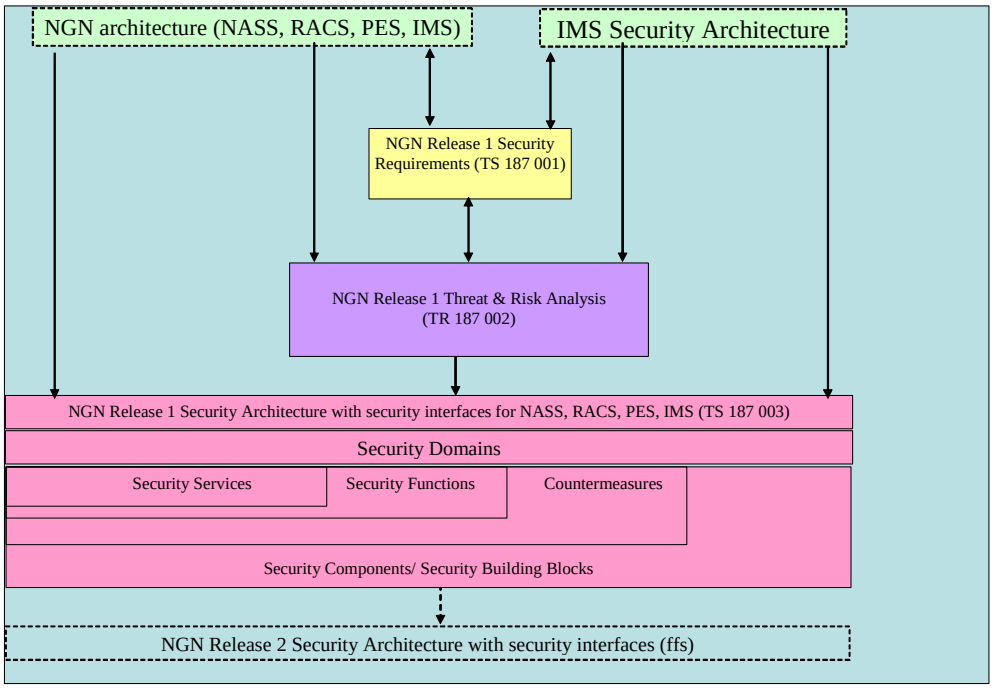


Figure 1: Overview of NGN security documents

4.1 NGN security architecture

The NGN security architecture basically consists of the following major parts:

- NGN security domains (see clause 4.3).
- Security services (see clause 5):
  - authentication;
  - authorization;
  - policy enforcement;
  - key management;
  - confidentiality; and
  - integrity.
- Security protocols including those contained in:
  - IMS Access Security (see TS 133 203[7]);
  - SIP HTTP-digest (see RFC 3261 [26]) (for NGN legacy UE);
  - XCAP (see TS 183 033[6]), presence security (see TS 133 141[9]).
- Application specific key management.
- SEGFs to secure signalling and control communication among network entities/FEs. Security Gateways (SEGs) for IMS network domain security - as defined by TS 133 210 [8] - are considered primarily functional components. The present document endorses SEGs and calls them **Security Gateway Function (SEGF)**.
- IMS Residential Gateway to secure access of legacy UEs (see clause 6).

- NGN-specific security mechanisms at various protocols/logical layers such as:
  - NASS authentication based on explicit line authentication;
  - NASS authentication based on implicit physical line authentication; and
  - NASS-IMS bundled authentication.
- NGN subsystem specific security measures (e.g. for PES).

Figure 2 provides a high level overview of the security FEs within the NGN security architecture. Three logical security planes with respective FEs are distinguished:

- NASS security plane;
- IMS security plane;
- GAA/GBA key management plane.

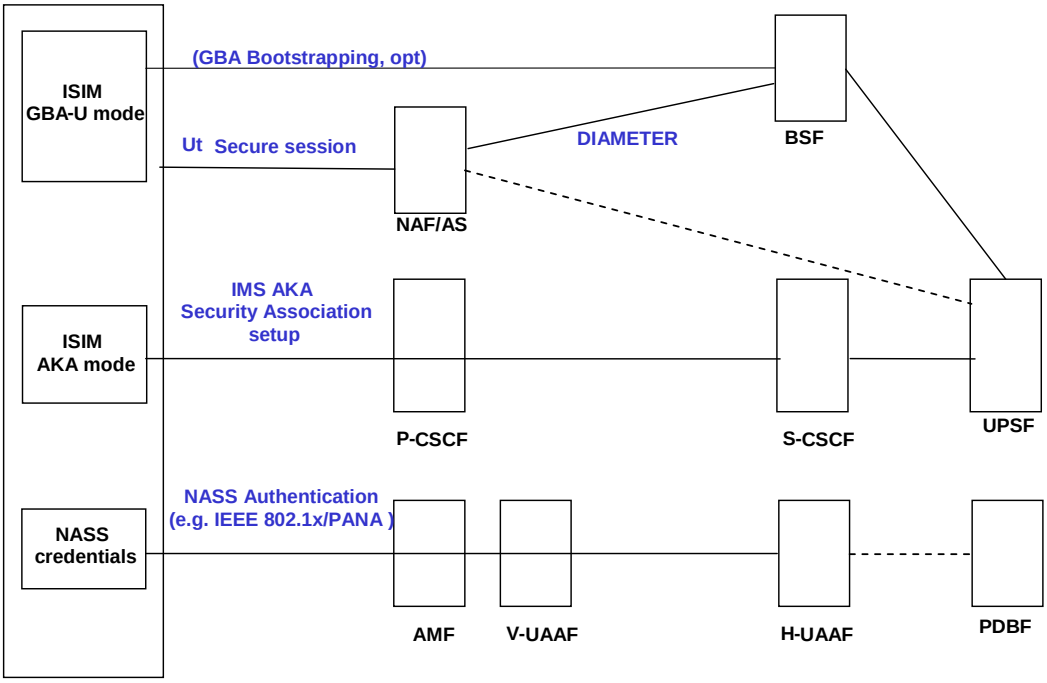


Figure 2: Usage of security FEs in the NGN security architecture

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; the V-UAAF (if present) may be a proxy while the home UAAF (H-UAAF) shall process the authentication message and decide authorization. The H-UAAF takes into account user profile information that is stored in the PDBF. The PDBF shall hold the profiles of the NASS user. In 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. Hence, in such cases, there is no relation at all between the profile/credentials used at the NASS level and at the IMS level. However, the PDBF may be co-located with the UPSF.

NOTE: The dashed lines between H-UAAF and PDBF and between the NAS/AS and the UPSF indicate interfaces which are not defined and standardized in the present document. Specification of such interfaces is left as further study. Nevertheless, such an UAAF-PDBF interface is generally required for carrying out authentication at NASS level.

The IMS security plane encompasses the P-CSCF, S-CSCF, I-CSCF (not shown in figure 2) and the UPSF. P-CSCF, S-CSCF and I-CSCF shall be involved in the IMS security procedures for authenticating UE and core network, deciding authorization, as well as for supplying fresh key material as specified in TS 133 203 [7]. The UPSF shall hold the user profiles used at the IMS level.

The GBA/GAA security plane (optional) encompasses the NAF and BSF FEs for application layer security.

This clause describes the NGN security architecture.

4.2 Security domains

A security domain (see ISO/IEC 10181-1 [27] and ITU-T Recommendation X.810 [30]) is a set of elements under a given security policy administered by a single security authority for some specific security relevant activities. The activities of a security domain involve one or more elements from that domain, however at least one of the elements must be in that domain.

In general, a security domain is required to:

- protect the integrity, and optionally the confidentiality, of its functional elements and activities;
- ensure the availability of, and account for the use of, the elements and activities under its protection.

The following principal security domains are identified in the general case where the visited network provider hosts some IMS services and the core IMS provider in the home network domain further provides IMS services:

- Customer's domain that includes UE (owned by customer or by operator).
- Access network security domain with FEs hosted by the access network provider.
- Visited NGN network 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 network 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 different 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 3 shows the partitioning of the NGN network into security domains.

NOTE: The box labelled "APPL" denotes hosted applications; applications are optional.

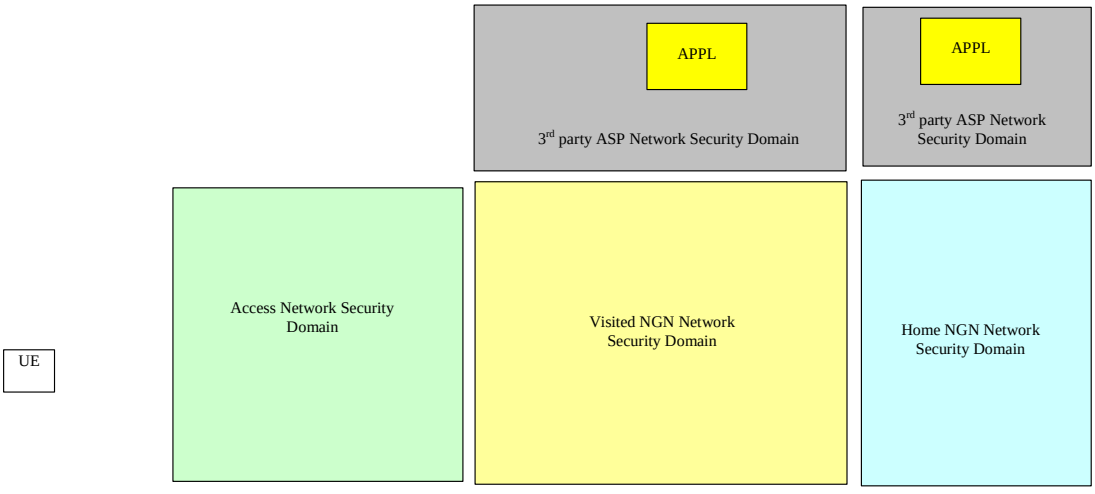


Figure 3: NGN security domains

4.3 NASS and RACS security architecture

Figure 4 shows a high-level view of the NASS and RACS subsystems as mapped to the five NGN security domains.

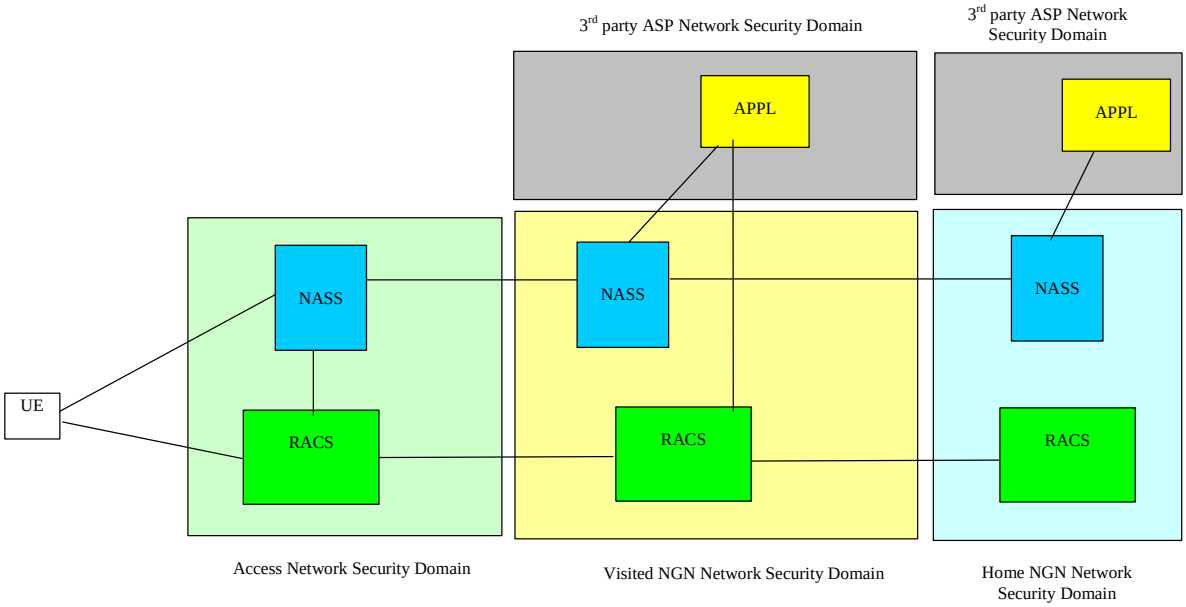


Figure 4: NASS and RACS NGN architecture with security domains

SEGFs security shall protect the interdomain interfaces between the NGN network security domains.

Figure 4 shows the most general case. NASS and RACS functional entities are mapped to the networking domains such as access transport network, visited NGN network and home NGN network. Those networking domains equally represent security domains in the sense of TS 133 210 [8] assuming that each networking domain is being operated by a distinct operator. SEcurity Gateway Functions (SEGFs) within each security domain shall protect the exposed interfaces in-between security domains and ensure that a minimal security policy among security domains is enforced.

SEGFs may also optionally protect the (less exposed, internal) interfaces within a security domain; this is left to the discretion of the network operator. The general security architecture case for NASS and RACS subsystems can be collapsed iteratively into fewer (security) domains (not shown): e.g. home network and visited network within one security domain, or access, visited, home network and ASP network all in one security domain. If 3rd party ASP network security domain and home network security domain coincide, then the home network actually hosts the application. The same holds true for the visited network security and the 3rd party ASP network security domain.

It is noted that not all interfaces might occur:

- In NASS scenario 1, the interface e2 with the branches V-CLF-to-H_CLF, V-CLF-to-AF and V-PDBF do not occur.
- In NASS scenario 2, the interface e2 with the branch V-CLF-to-AF and V-PDBF do not occur.
- In NASS scenario 3, the interfaces e5 and e2 with the branches V-UAAF-to-H-UAAF and V-CLF-to-H-CLF do not occur.
- In NASS scenario 4, the interfaces e5 and e2 with the branches V-UAAF-to-H-UAAF and V-CLF-to-AF do not occur.

It is further noted, that several SEGFs shown as separate functional entities may be co-located; such as for example, the SEGFs around Rq and Di interfaces.

It is noted that there might be further application-specific security protocols (not shown) on top of the Za interfaces. Such security protocols (if any) remain for further study.

NOTE: On the SEG CA in ASP domains it is observed that those CAs are not peering CAs as among the home/visited and access provider. It remains for further study how such SEG CAs could be deployed in the context of NGN.

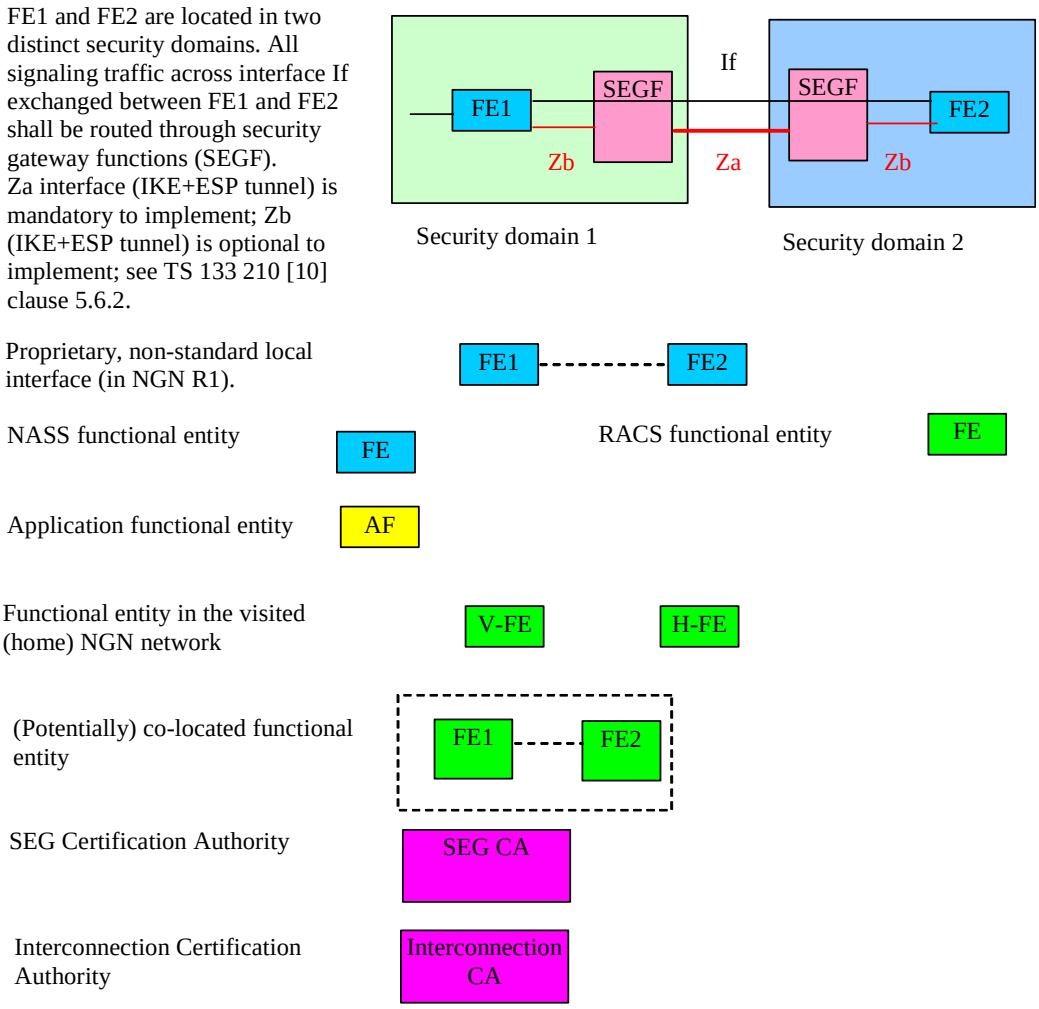


Figure 5: Legend

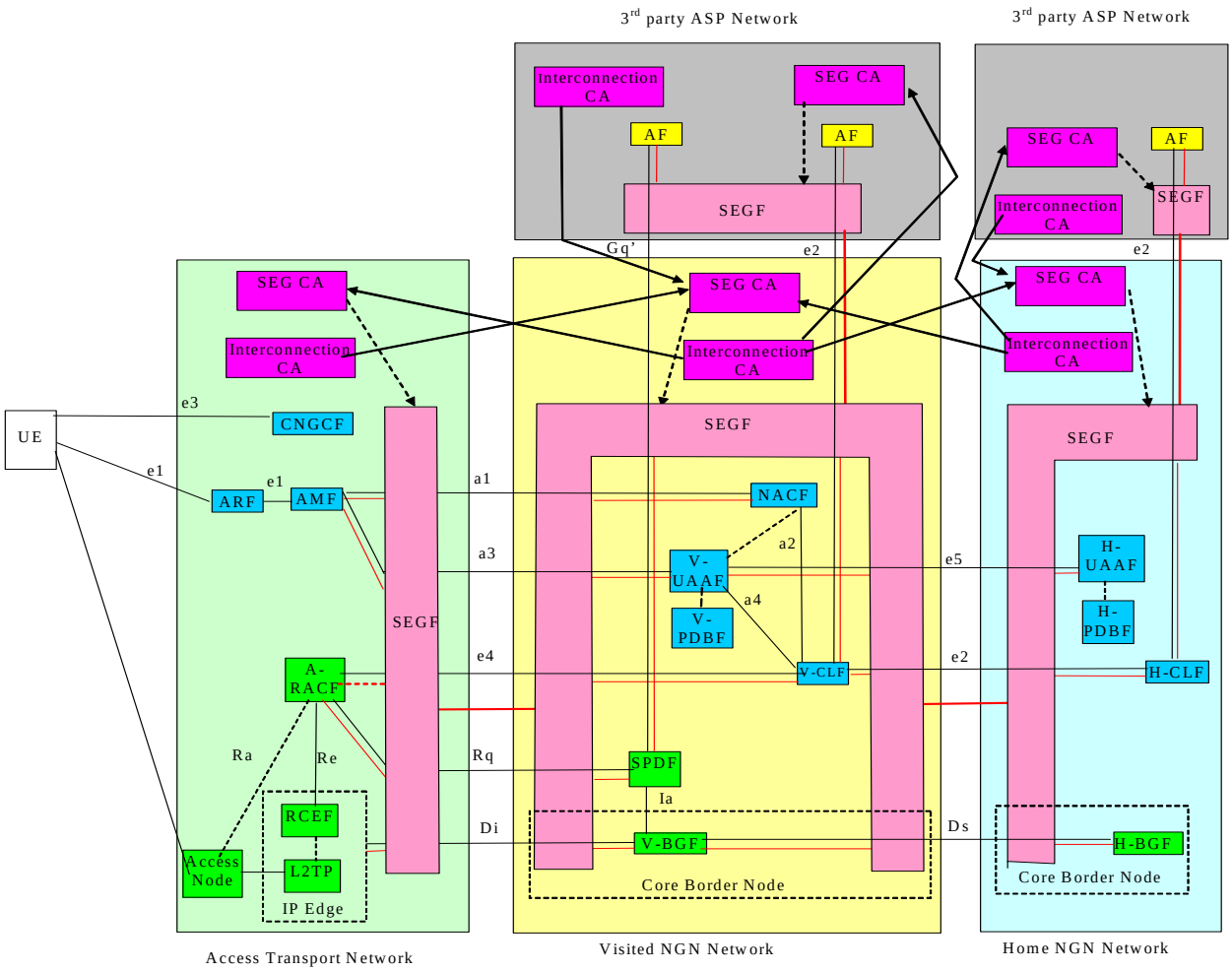


Figure 6: NGN NASS and RACS security architecture with FEs and security gateway functional components around inter-domain interfaces in access, visited, home and other operator's networks

4.3.1 NASS-IMS Bundled Security

Please refer to clause 4.4.1.

4.4 IMS security architecture

The IMS security architecture for both 3G environments and for NGN environments is defined in TS 133 203 [7].

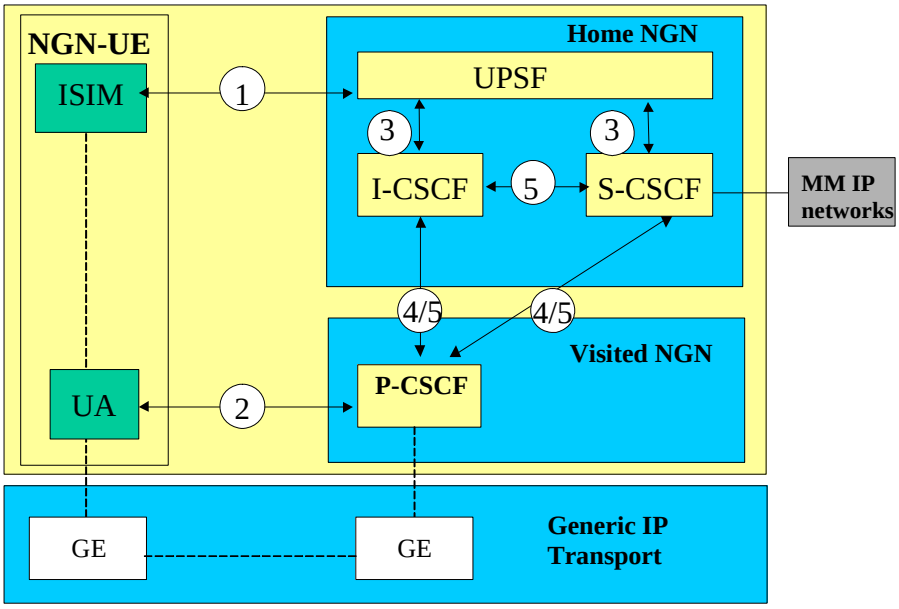


Figure 7: IMS Security architecture in an NGN environment (see TS 133 203 [7])

Figure 7 depicts the IMS security architecture in an NGN environment as defined in TS 133 203 [7], where the 3GPP specific transport domain is replaced by the Generic IP transport domain. The following observations support figure 7.

- The IMS is independent of the transport network.
- Generic Entities (GE) equivalent to the 3GPP transport entities will be present in the Generic IP transport domain.
- In NGN the AuC functionality is performed by UPSF.
- The Security Associations (SA) (referring to the corresponding arrows in figure 7) are retained:
  - SA-1, SA-3, SA-4 and SA-5 are endorsed as described in TS 133 203 [7].
  - SA-2 is endorsed with the extension to ensure transport across NAT/Firewall boundaries.

There exist other interfaces and reference points in IMS, which have not been addressed above. Those interfaces and reference points reside within the IMS, either within the same security domain or between different security domains (see figure 8). The protection of all such interfaces and reference points (which may include subsystems like NASS/RACS) apart from the Gm reference point are protected as specified in TS 133 210 [8].

The present document endorses the interfaces (1) to (5) of TS 133 203 [7].

Figure 8 details figure 7 by showing the IMS functional entities in the NGN that runs over a generic IP transport.

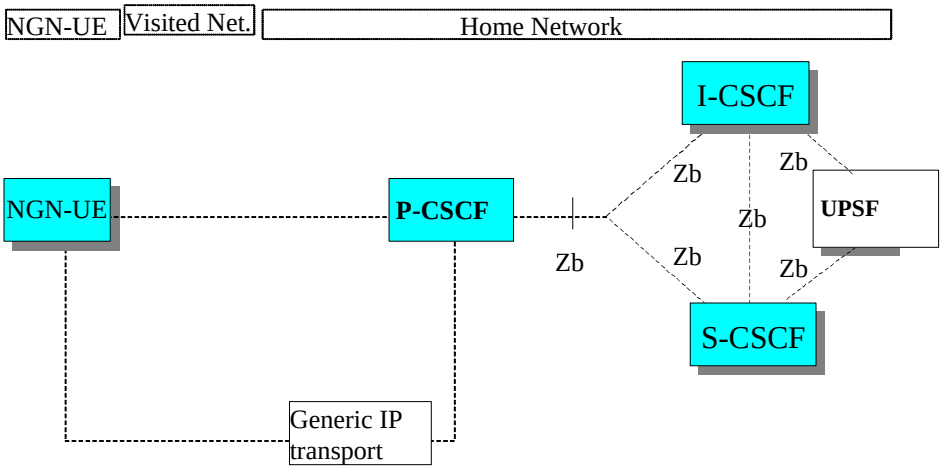


Figure 8: Generic IP Transport underneath IMS (see TS 133 203 [7])

In the following, IMS components are segregated into the different security domains. Figure 9 shows the IMS components in five different domains. The interconnection between the different IMS components is not shown in the figure and it should be in accordance with ES 282 007 [24]. The segregation is explained below.

1) **Customer's domain** includes UE and optionally some Residential Gateways (which may be owned by the user/operator). The Residential Gateway shall have ISIM, which has the credentials for IMS authentication.

2) **Access network domain** is hosted by the access network provider. The access network provider may or may not be the same as the NGN provider.

3) **Visited network domain** is hosted by a visited network provider. The visited network provider may offer multimedia services and may have his own subscribers. Alternatively, the visited network provider may have agreement with some 3rd party Application Service Provider (ASP) to offer services. The visited network domain may encompass IMS functional entities.

4) **Home network domain** is hosted by the home network provider. The home network provider offers multimedia services. Alternatively, the visited network provider may have agreement with some 3rd party Application Service Provider (ASP) to offer services. The home network domain encompasses the IMS network.

5) **3rd party application service provider domain** is hosted by some ASP different from the operator. The ASP may need to deploy its own AAA infrastructure to interpret the information offered by the visited or home network provider. It should have the IMS functional entities.

Figure 9 shows the partitioning of the NGN network with IMS components (pink boxes) into security domains (boxes with curved edge). The figure also shows the two different authentications the clients usually go through for NGN access, in the scope of NGN security architecture.

6) The connection marked "Access Authentication" is the authentication between the UE and NASS in the Access Network.

7) The connection marked "IMS Authentication" is the authentication between the UE and the S-CSCF in the IMS network. After the successful authentication, a security association is created between the UE and the P-CSCF. 3GPP R5/R6 has recommended IPsec in transport mode for this. The 3GPP R5/R6 solution lacks NAT traversal capability and hence the 3GPP R7 solution capable of NAT traversal is to be used.

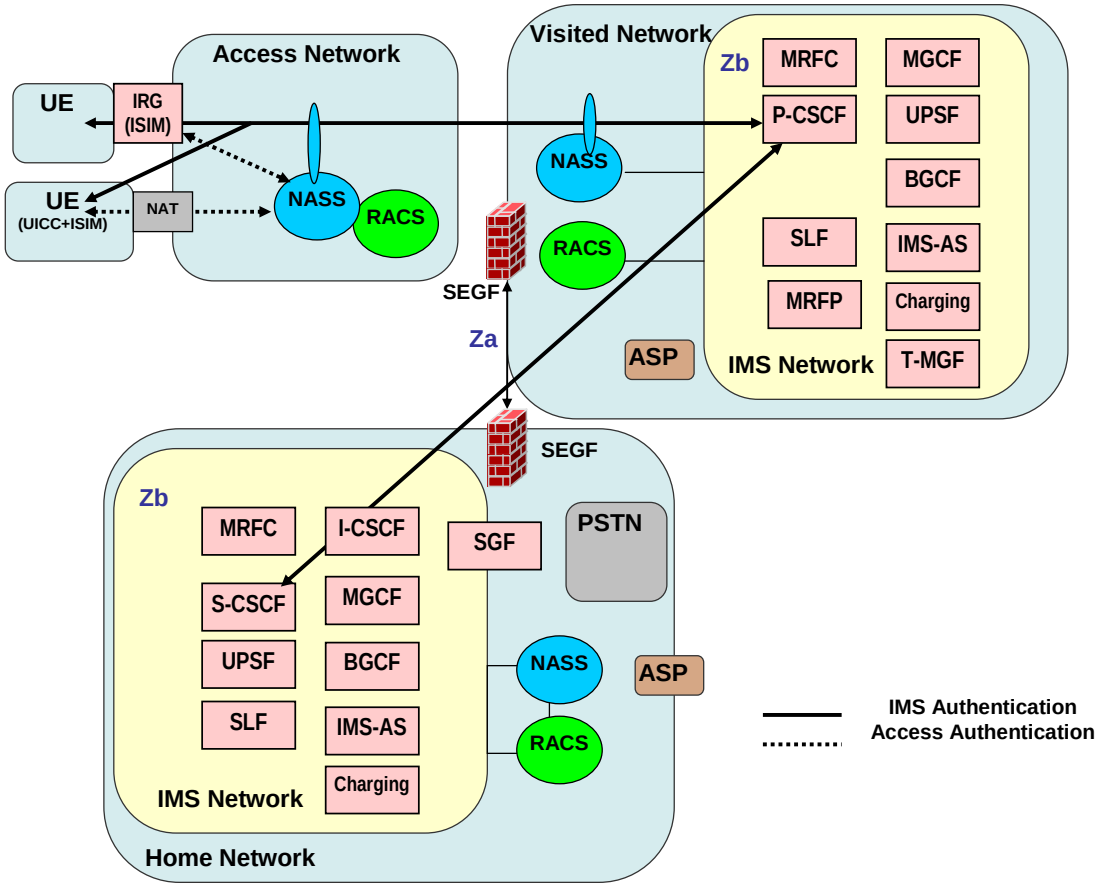
In the figure 9, two distinct interfaces are depicted:

- The connections between the different IMS components (also NGN components) within the same IMS network (NGN network) are the "Zb" interfaces. These interfaces may or may not be protected depending on operator policies.

- The connection between the different Operators, denoted by "Za" in the figure, should be protected (IKE, ESP tunnel). The SEGFs (see TS 133 210 [8]) within each security domain protect the exposed interfaces between operators and ensure that a security policy among security domains is enforced. SEGFs may also optionally protect the (less exposed, internal) interfaces within a security domain; this is left to the discretion of the network operator. The outbound IMS/NGN traffic from an operator cannot by-pass the SEGF. SEGFs are used to protect the traffic between two operators. That means traffic from access network IMS entities to IMS entities in the home network of a different operator shall go through SEGF.

The UE may either have ISIM in it (in which case, it can directly authenticate to the S-CSCF) or the ISIM credentials may be in the IMS residential gateway (IRG) (wherein, the service authentication has to go through the IRG). The ISIM may also be in both the devices.

The Service Providers (ASP) may or may not have the same CA as the visited/home network. This depends on the operator policies.



NOTE: Figure 9 does not show any optional SEGF within a security domain for securing the communication among IMS FEs inside the same security domain.

Figure 9: IMS security domains

4.4.1 NASS-IMS Bundled Security

The NASS Bundled Authentication (NBA) works by extending the successful authentication in the NASS layer to the service layer.

During the network attachment, the NASS authenticates the UE and allocates an IP address. It stores the layer-2 and layer-3 identities in the NASS profile. When UE registers with the P-CSCF, the P-CSCF queries the NASS (actually the CLF functional entity), to obtain its location information. The P-CSCF embeds the location information into the SIP message and forwards it towards the S-CSCF for verification. The S-CSCF verifies this location information with the location information obtained from the UPSF. On successful verification, the user is authenticated at the IMS layer.

At the architectural level, two interfaces are affected:

1) The "e2" interface over which the location info from the NASS is communicated.

2) The "Cx" interface over which the user profile stored in UPSF is transmitted.

This is illustrated in figure 10. See also annex D for a visualization of the network flows.

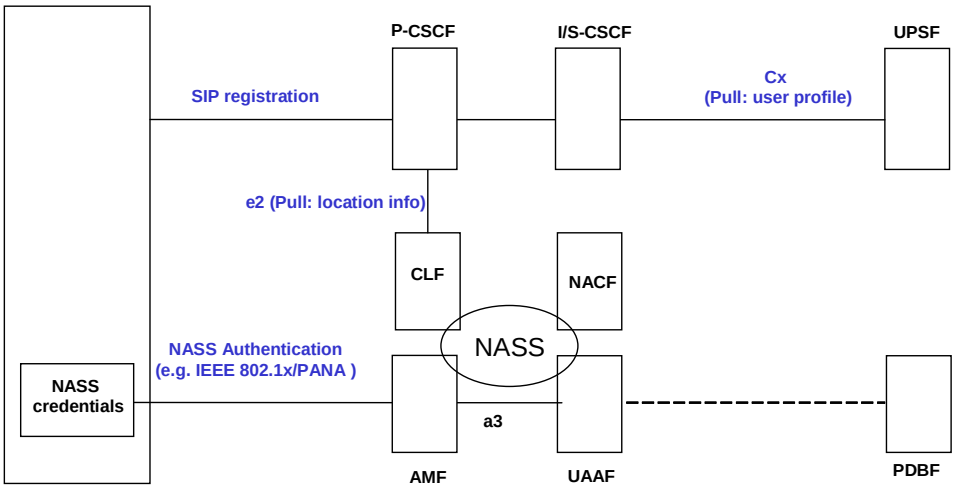


Figure 10: Formal mapping of NASS Bundled Authentication

4.5 PES Security Architecture

4.5.1 Security for H.248 within PES

Figure 11 depicts the security architecture for using H.248.1 for PSTN/ISDN service over IP according to ES 283 002 [18]. 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 [18], 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.

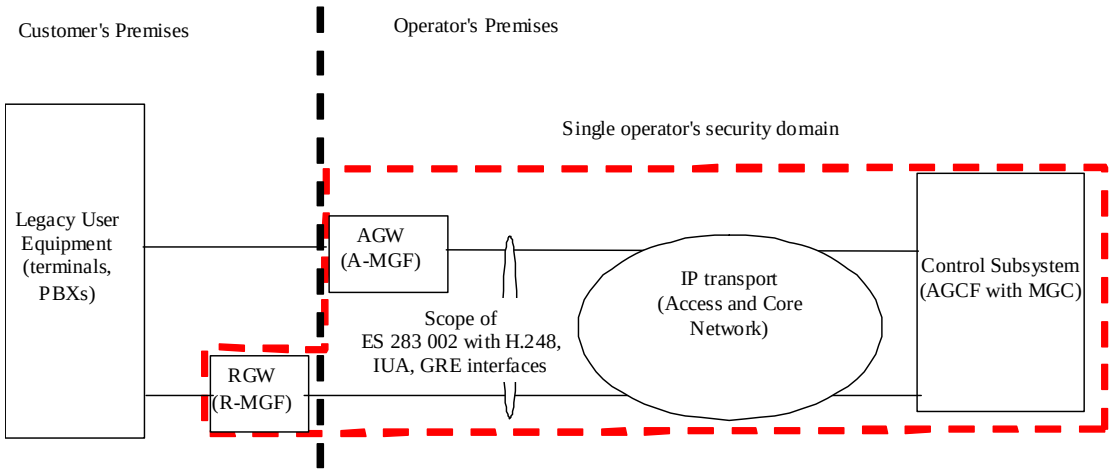


Figure 11: Reference architecture for profile of the Gateway Control Protocol (H.248.1), for controlling access and residential gateways connecting analog lines and ISDN primary and basic accesses, in order to emulate PSTN/ISDN services over IP (see ES 283 002[18])

4.5.2 IMS-based PES Security

TS 182 012[38] defines the functional architecture for the IMS-based PSTN/ISDN emulation subsystem. The MGCF maps the encapsulated ISUP information within SIP messages sent/received to/from the BGCF (Mj interface) and to/from the I/S-CSCF (Mg interface) to the ISDN/PSTN network. The MGCF implements the role of a PES Interworking Application while the IBCF implements the role of a PES Interconnection application, see TS 183 043 [37].

Procedures for filtering ISUP information off from SIP messages are specified in TS 183 043 [37], clauses 5.3.3.5.2.4, 5.3.5.4.2.4 and 5.3.6.2.

In the context of PES, TR 183 032 [i.4], clause 6.2 and TR 183 014 [i.6] provide supplementary information on the feasibility of securing encapsulated ISUP information within SIP.

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 [10]). An authentication proxy may be used optionally for user authentication, as defined in TS 183 033 [6] and TS 133 222 [10], see figure 12.

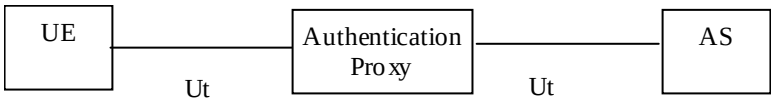


Figure 12: Authentication proxy in the Ut interface path

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 [11].
- Support for Subscriber Certificates (SSC) - TS 133 221 [i.2].
- Access to NAF using HTTPS - TS 133 222 [10].

4.6.1.1 Generic Bootstrapping Architecture (GBA)

GBA is specified in TS 133 220 [11].

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 [10].

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

5 Mapping of Security Requirements to Security Services and NGN FEs

5.1 Security services in NGN security architecture

This clause defines the mapping of security services within the NGN security architecture through security functions. Clause 4.2.3 provides a mapping of security services to NGN FEs.

The following security services are identified for NGN:

- Authentication.
- Authorization.
- Confidentiality.
- Integrity.

Tables 1 to 4 show the security services along with the NGN interfaces between the major NGN subsystems (UE/CNG responsible VGW, NASS, RACS, IMS, PES and AS). The tables only show the interfaces with mandatory security; interfaces with optional security measures are not shown.

NOTE: Since the table is symmetric, the lower left triangular (shaded grey) is supposed to convey the same entries as shown in the upper right triangular.

Table 1: NGN interfaces with required Authentication security services (AUTH)

	UE/CNG, VGW	NASS	RACS	IMS	PES	AS
UE/CNG, VGW	**n.a.**	**e1**	**n.a.**	**Gm**	**Gm**	Ua, Ub, Ut, Zn
NASS		**a3, e5**	**e4**	**n.a**	**n.a.**	e2
RACS			**Rq**	**n.a.**	**n.a.**	Gq'
IMS				**Cx, Dx**	**n.a.**	Sh, Zh
PES					**n.a.**	n.a.
AS						n.a.

Table 2: NGN interfaces with required Confidentiality Security services (CONF)

	UE/CNG, VGW	NASS	RACS	IMS	PES	AS
UE/CNG, VGW	**n.a.**	**e1**	**n.a.**	**Gm**	**Gm**	Ua, Ub, Ut, Zn
NASS		**a3, e5**	**e4**	**n.a.**	**n.a.**	e2
RACS			**Rq**	**n.a**	**n.a.**	Gq'
IMS				**Cx, Dx, Ic**	**n.a.**	Sh, Zh
PES					**n.a.**	n.a.
AS						n.a.

Table 3: NGN interfaces with required Integrity security services (INT)

	UE/CNG, VGW	NASS	RACS	IMS	PES	AS
UE/CNG, VGW	**n.a.**	**e1**	**n.a.**	**Gm**	**Gm**	Ua, Ub, Ut, Zn
NASS		**a3, e5, Za**	**e4**	**n.a**	**n.a.**	e2
RACS			**Rq**	**n.a**	**n.a.**	Gq'
IMS				**Cx, Dx**	**n.a.**	Sh, Zh
PES					**n.a.**	n.a.
AS						n.a.

Table 4: NGN interfaces with required Key Management security services (KM)

	UE/CNG, VGW	NASS	RACS	IMS	PES	AS
UE/CNG, VGW	**n.a.**	**e1**	**n.a.**	**Gm**	**Gm**	Ua, Ub, Ut, Zn
NASS		**a3, e5, Za**	**e4**	**n.a**	**n.a.**	e2
RACS			**Rq**	**n.a**	**n.a.**	Gq'
IMS				**Cx, Dx**	**n.a.**	Sh, Zh
PES					**n.a.**	n.a.
AS						n.a.

5.2 Security Services in NGN FEs

Table 5 identifies the security services with the security mechanism(s) and countermeasures for each NGN FE.

NOTE: Security functions of security services may actually be specified in documents that are referenced indirectly only.

Table 5: Security services and countermeasures provided by NGN FEs

NGN FE	Security Services	Countermeasure and security mechanism in NGN
Access Point (AP)	AUTH	Authentication functions for AP are as specified by TS 183 019 [20].
	AUTHOR	Authorization functions for AP are as specified by TS 183 019 [20].
	CONF	Confidentiality functions for AP are as specified by TS 183 019 [20].
	INT	Integrity functions for AP are as specified by TS 183 019 [20].
	KM	Key management functions for AP are as specified by TS 183 019 [20].
	PEF	n.a.
AGCF, AGW, RGW	AUTH	Assumed to be in the trusted domain, see ES 283 002 [18].
	AUTHORF	Assumed to be in the trusted domain, see ES 283 002 [18].
	CONF	Assumed to be in the trusted domain, see ES 283 002 [18].
	INT	Assumed to be in the trusted domain, see ES 283 002 [18].
	KM	Assumed to be in the trusted domain, see ES 283 002 [18].
	PEF	Assumed to be in the trusted domain, see ES 283 002 [18].
A-RACF	AUTH	Authentication functions for securing the e4 interface for A-RACF are as specified by ES 283 034 [22]. Authentication functions for securing the Rq interface for A-RACF are as specified by ES 283 026 [40].
	AUTHOR	Authorizations functions for securing the e4 interface for A-RACF are as specified by ES 283 034 [22]. Authorizations functions for securing the Rq interface for A-RACF are as specified by ES 283 026 [40].
	CONF	Confidentiality functions for securing the e4 interface for A-RACF are as specified by ES 283 034 [22]. Confidentiality functions for securing the Rq interface for A-RACF are as specified by ES 283 026 [40].
	INT	Integrity functions for securing the e4 interface for A-RACF are as specified by ES 283 034 [22]. Integrity functions for securing the Rq interface for A-RACF are as specified by ES 283 026 [40].
	KM	Key management functions for securing the e4 interface for A-RACF are as specified by ES 283 034 [22]. Key management functions for securing the Rq interface for A-RACF are as specified by ES 283 026 [40].
	PEF	Policy enforcement functions for securing the e4 interface for A-RACF are as specified by ES 283 034 [22]. Policy enforcement functions for securing the Rq interface for A-RACF are as specified by ES 283 026 [40].
AS	AUTH	Authentication functions for AS are as specified by TS 133 141 [9] and by TS 183 033 [6]. Authentication functions for securing the DIAMETER protocol for AS are as specified by TS 129 329 [17] and by TS 133 210 [8].
	AUTHOR	Authorization functions for AS are as specified by TS 133 141 [9] and by TS 183 033 [6]. Authorization functions for securing the DIAMETER protocol for AS are as specified by TS 129 329 [17] and by TS 133 210 [8].
	CONF	Confidentiality functions for AS are as specified by TS 133 141 [9] and by TS 183 033 [6]. Confidentiality functions for securing the DIAMETER protocol for AS are as specified by TS 129 329 [17] and by TS 133 210 [8].
	INT	Integrity functions for AS are as specified by TS 133 141 [9] and by TS 183 033 [6]. Integrity functions for securing the DIAMETER protocol for AS are as specified by [17] and by TS 133 210 [8].
	KM	Key management functions for AS are as specified by TS 133 141 [9] and by TS 183 033 [6]. Key management functions for securing the DIAMETER protocol for AS are as specified by TS 129 329 [17] and by TS 133 210 [8].

NGN FE	Security Services	Countermeasure and security mechanism in NGN
	PEF	Policy enforcement functions for filtering encapsulated ISUP within SIP in the AS are specified by TS 183 043 [37] clauses 5.3.3.5.2.4 and 5.3.5.4.2.4.
Authentication Proxy (AP)	AUTH	Authentication functions for AP are as specified by TS 183 033 [6] and TS 133 222 [10].
	AUTHOR	Authorization functions for AP are specified by TS 183 033 [6] and TS 133 222 [10].
	CONF	Confidentiality functions for AP are specified by TS 183 033 [6] and TS 133 222 [10].
	INT	Integrity functions for AP are specified by TS 183 033 [6] and TS 133 222 [10].
	KM	Key management functions for AP are as specified by TS 183 033 [6] and TS 133 222 [10].
	PEF	Policy enforcement functions for AP are as specified by TS 183 033 [6] and TS 133 222 [10].
BGCF	AUTH	n.a.
	AUTHOR	n.a.
	CONF	n.a.
	INT	n.a.
	KM	n.a.
	PEF	n.a.
BSF	AUTH	Authentication functions for BSF are as specified by TS 133 220 [11].
	AUTHOR	Authorization functions for BSF are as specified by TS 133 220 [11].
	CONF	Confidentiality functions for BSF are as specified by TS 133 220 [11].
	INT	Integrity functions for BSF are as specified by TS 133 220 [11].
	KM	Key management functions for BSF are as specified by TS 133 220 [11].
	PEF	n.a.
CLF	AUTH	Authentication functions for securing the e2 interface of the CLF are as specified by ES 283 035 [21].
	AUTHOR	Authorizations functions for securing the e2 interface of the CLF are as specified by ES 283 035 [21].
	CONF	Confidentiality functions for securing the e2 interface of the CLF are as specified by ES 283 035 [21].
	INT	Integrity functions for securing the e2 interface of the CLF are as specified by ES 283 035 [21].
	KM	Key management functions for securing the e2 interface of the CLF are as specified by ES 283 035 [21].
	PEF	Policy enforcement functions for securing the e2 interface of the CLF are as specified by ES 283 035 [21].
IBCF	AUTH	n.a.
	AUTHOR	Authorization functions for IBCF are as specified by TS 182 006 [25].
	CONF	Confidentiality functions for IBCF are as specified by TS 182 006 [25].
	INT	n.a.
	KM	n.a.
	PEF	Policy enforcement functions for IBCF are as specified by TS 182 006 [25]. Policy enforcement functions for filtering encapsulated ISUP within SIP in the IBCF are specified byTS 183 043 [37], clause 5.3.6.2.
IRG	AUTH	IMS-AKA authentication functions for IRG shall be as specified in TS 133 203 [7]. Authentication functions for IPsec packet authentication in the IRG are as specified in TS 133 203 [7]. Optional authentication functions for SIP HTTP-digest in the IRG are as defined in [26].
	AUTHOR	Authorization functions in the IRG are as specified in TS 133 203 [7].
	CONF	Confidentiality functions in the IRG protect IMS-AKA key distribution against loss of confidentiality as specified in TS 133 203 [7]. Confidentiality functions in the IRG encrypt IPsec packets as specified in TS 133 203 [7].
	INT	Integrity functions in the IRG protect IMS-AKA key distribution against loss of integrity as specified in TS 133 203 [7]. Integrity functions in the IRG protect IPsec packets against loss of integrity as specified in TS 133 203 [7].
	KM	Key management functions in the IRG provide IMS-AKA as specified in TS 133 203 [7].
	PEF	n.a.
MGCF	AUTH	n.a.

NGN FE	Security Services	Countermeasure and security mechanism in NGN
	AUTHOR	n.a.
	CONF	n.a.
	INT	n.a.
	KM	n.a.
	PEF	Policy enforcement functions for filtering encapsulated ISUP within SIP in the MGCF are specified by TS 183 043 [37].
NAF	AUTH	Authentication functions in NAF are as specified by TS 133 222 [10].
	AUTHOR	Authorization functions in NAF are specified by TS 133 222 [10].
	CONF	Confidentiality functions in NAF are specified by TS 133 222 [10].
	INT	Integrity functions in NAF are specified by TS 133 222 [10].
	KM	Key management functions in NAF are as specified by TS 133 222 [10].
	PEF	n.a.
PDBF	AUTH	Authentication functions in the PDBF retrieve authentication data (e.g. user identity, list of supported authentication methods, authentication keys etc.) as outlined in ES 282 004 [5].
	AUTHOR	Authorization functions in the PDBF access PDBF to retrieve authorization data (e.g. user network profile) as outlined in ES 282 004 [5].
	CONF	n.a.
	INT	n.a.
	KM	n.a.
	PEF	n.a.
P-CSCF	AUTH	Authentication functions in the P-CSCF provide IMS-AKA as specified in TS 133 203 [7]. Authentication functions in the P-CSCF provide IPsec packet authentication as specified in TS 133 203 [7]. Optional authentication functions in the P-CSCF provide NASS-IMS bundled authentication as specified in ES 283 003 [23] and TS 183 033 [6]. Optional authentication functions in the P-CSCF support SIP HTTP-digest as defined in RFC 3261 [26]. Authentication functions in the P-CSCF secure the e2 interface as specified by ES 283 035 [21]. Authentication functions in the P-CSCF secure the e4 interface as specified by ES 283 034 [22].
	AUTHOR	Authorization functions in the P-CSCF provide authorization functions as specified in TS 133 203 [7]. Authorization functions in the P-CSCF provide authorizations functions for securing the e2 interface as specified by ES 283 035 [21]. Authorization functions in the P-CSCF provide authorizations functions for securing the e4 interface as specified by ES 283 034 [22]. Optional authorization functions in the P-CSCF for NASS-IMS bundled authentication feature as specified in ES 283 003 [23] and TS 183 033 [6]. Optional authorization functions in the P-CSCF support SIP HTTP-digest as defined in RFC 3261 [26].
	CONF	Confidentiality functions in the P-CSCF provide IMS-AKA key distribution against loss of confidentiality specified in TS 133 203 [7]. Confidentiality functions in the P-CSCF provide IPsec packet encryption as specified in TS 133 203 [7]. Confidentiality functions in the P-CSCF secure the e2 interface as specified by ES 283 035 [21]. Confidentiality functions in the P-CSCF secure the e4 interface as specified by ES 283 034 [22].
	INT	Integrity functions in the P-CSCF protect IMS-AKA key distribution against loss of integrity as specified in TS 133 203 [7]. Integrity functions in the P-CSCF protect IPsec packets against loss of integrity as specified in TS 133 203 [7]. Integrity functions in the P-CSCF secure the e2 interface as specified by ES 283 035 [21]. Integrity functions in the P-CSCF secure the e4 interface as specified by ES 283 034 [22].
	KM	Key management functions in the P-CSCF provide IMS-AKA as specified in TS 133 203 [7]. Key management functions in the P-CSCF shall secure the e2 interface as specified by ES 283 035 [21]. Key management functions in the P-CSCF secure the e4 interface as specified by ES 283 034 [22].

NGN FE	Security Services	Countermeasure and security mechanism in NGN
	PEF	Policy enforcement functions in the P-CSCF secure the e2 interface as specified by ES 283 035 [21]. Policy enforcement functions in the P-CSCF secure the e4 interface as specified by ES 283 034 [22]. Policy enforcement functions for filtering encapsulated ISUP within SIP in the P-CSCF are specified by TS 183 043 [37], clause 5.3.3.5.2.4.
S-CSCF	AUTH	Authentication functions for securing DIAMETER over SCTP using IPsec in the S-CSCF are as specified by TS 183 033 [6] and by TS 133 210 [8].
	AUTHOR	Authorization functions for securing DIAMETER over SCTP using IPsec in the S-CSCF are as specified by TS 183 033 [6] and by TS 183 033 [8].
	CONF	Confidentiality functions for securing DIAMETER over SCTP using IPsec in the S-CSCF are as specified by TS 183 033 [6] and by TS 183 033 [8].
	INT	Integrity functions for securing DIAMETER over SCTP using IPsec in the S-CSCF are as specified by [6] and by TS 183 033 [8].
	KM	Key management functions for securing DIAMETER over SCTP using IPsec in the S-CSCF are as specified by TS 183 033 [6] and by TS 183 033 [8].
	PEF	n.a.
SEGF	AUTH	Authentication functions in the SEGF provide IKE as specified in [8]. Authentication functions in the SEGF provide IPsec packet authentication as specified in TS 183 033 [8].
	AUTHOR	Authorization functions in the SEGF provide IKE/IPsec SPD as specified in TS 183 033 [8].
	CONF	Confidentiality functions in the SEGF provide IPsec packet encryption as specified in TS 133 141 [9].
	INT	Integrity functions in the SEGF provide IPsec packet integrity as specified in TS 133 141 [9].
	KM	Key management functions in the SEGF provide IKE as specified in TS 133 141 [9].
	PEF	Policy enforcement for AUTH, AUTHOR, CONF, INT and KM in the SEGF are as specified in TS 133 141 [9].
THF, I-CSCF (THIG)	AUTH	n.a.
	AUTHORF	n.a.
	CONF	n.a.
	INTF	n.a.
	KM	n.a.
	PEF	Topology hiding functions in THF, I-CSCF (THIG) are as specified in ISO/IEC 10181-1 [27] (see TS 124 229 [44]).
UAAF	AUTH	Explicit and/or implicit authentication functions for NASS in the UAAF are as specified by TS 183 019 [20]; see also ES 282 004 [5]. The UAAF terminates the AAA protocol (RADIUS or DIAMETER) as a AAA server, see ES 282 004 [5].
	AUTHOR	Authorization functions for NASS (supported by PDBF) in the UAAF are as specified by TS 183 019 [20].
	CONF	n.a.
	INT	n.a.
	KM	n.a.
	PEF	The UAAF supports the Privacy Indicator to indicate whether location information can be exported to services and applications; ES 282 004 [5].
UPSF (see note)	AUTH	For IMS, the authentication function in the UPSF accesses authentication data stored in the UPSF (see also ES 282 001 [2], TR 182 005 [i.5], see also clause A.2).
	AUTHOR	For IMS, the authorization function in the UPSF accesses authorization data stored in the UPSF (see also ES 282 001 [2], TR 182 005 [i.5], see also clause A.2).
	CONF	For IMS, the confidentiality function in the UPSF accesses keys stored in the UPSF (see also ES 282 001 [2], TR 182 005 [i.5], see also clause A.2).
	INT	For IMS, the integrity function in the UPSF accesses integrity data stored in the UPSF (see also ES 282 001 [2], TR 182 005 [i.5], see also clause A.2).
	KM	For IMS, the key management function accesses key management data stored in the UPSF (see also ES 282 001 [2], TR 182 005 [i.5], see also clause A.2).
	PEF	For IMS, the policy enforcement function in the UPSF accesses policy information stored in the UPSF (see also ES 282 001 [2], TR 182 005 [i.5], see also clause A.2).
NOTE: UPSF does not directly correspond to a security function, nor does UPSF provide a security service.		

5.3 Security Services on NGN Interfaces

Table 6 identifies the security services (AUTH, INT, CONF, KMF) with the security mechanism(s) and countermeasures for each NGN interface.

NOTE 1: Interfaces are not listed in this clause where no security functions are identified.

NOTE 2: Security functions of the security services may actually be specified in documents that are referenced indirectly only.

Table 6: Security services and countermeasures provided by NGN interfaces

NGN IF	Security Services	Countermeasure and security mechanism in NGN
a3 (UAAF - AMF)	AUTH	Authentication functions for the a3 IF are as specified by TS 183 019 [20].
	CONF	Confidentiality functions for the a3 IF are as specified by TS 183 019 [20].
	INT	Integrity functions for the a3 IF are as specified by TS 183 019 [20].
	KM	Key management functions for the a3 IF are as specified by TS 183 019 [20].
a4 (UAAF - CLF)	AUTH	n.a.
	CONF	n.a.
	INT	n.a.
	KM	n.a.
Cx (S-CSCF - UPSF)	AUTH	Authentication functions for securing DIAMETER over SCTP using IPsec for the CX IF are as specified by TS 183 033 [6] and by TS 133 210 [8].
	CONF	Confidentiality functions for securing DIAMETER over SCTP using IPsec for the CX IF are as specified by TS 183 033 [6] and by TS 133 210 [8].
	INT	Integrity functions for securing DIAMETER over SCTP using IPsec for the CX IF are as specified by TS 183 033 [6] and by TS 133 210 [8].
	KM	Key management functions for securing DIAMETER over SCTP using IKE for the CX IF are as specified by TS 183 033 [6] and by TS 133 210 [8].
Dx (S-CSCF - UPSF - SLF)	AUTH	Authentication functions for securing DIAMETER for the DX IF are as specified by TS 183 033 [6] and by TS 133 210 [8].
	CONF	Confidentiality functions for securing DIAMETER for the DX IF are as specified by TS 183 033 [6] and by TS 133 210 [8].
	INT	Integrity functions for securing DIAMETER for the DX IF are as specified by [6] and by TS 133 210 [8].
	KM	Key management functions for securing DIAMETER for the DX IF are as specified by TS 183 033 [6] and by TS 133 210 [8].
e1 (CNG-AMF)	AUTH	Authentication functions for e1 IF are as specified by TS 183 019 [20] and by TS 133 210 [8].
	CONF	Confidentiality functions for e1 IF are as specified by TS 183 019 [20].
	INT	Integrity functions for e1 IF are as specified by TS 183 019 [20].
	KM	Key management functions for e1 IF are as specified by TS 183 019 [20].
e2 (CLF - AF)	AUTH	Authentication functions for securing the e2 interface are as specified by ES 283 035 [21].
	CONF	Confidentiality functions for securing the e2 interface are as specified by ES 283 035 [21].
	INT	Integrity functions for securing the e2 interface are as specified by ES 283 035 [21].
	KM	Key management functions for securing the e2 interface are as specified by ES 283 035 [21].
e4 (CLF - A-RACF)	AUTH	Authentication functions for securing the e4 interface are as specified by ES 283 034 [22].
	CONF	Confidentiality functions for securing the e4 interface are as specified by ES 283 034 [22].
	INT	Integrity functions for securing the e4 interface are as specified by ES 283 034 [22].
	KM	Key management functions for securing the e4 interface are as specified by ES 283 034 [22].
e5 (UAAF - UAAF)	AUTH	Authentication functions for the e5 IF are as specified by TS 183 019 [20]. e5 provides the AAA protocol (RADIUS or DIAMETER) as specified by ES 282 004 [5].
	CONF	Confidentiality functions for the e5 IF are as specified by TS 183 019 [20].
	INT	Integrity functions for the e5 IF are as specified by TS 183 019 [20].
	KM	Key management functions for the e5 IF are as specified by TS 183 019 [20].

NGN IF	Security Services	Countermeasure and security mechanism in NGN
Gm (UE/IRG - P-CSCF) (VGW - P-CSCF)	AUTH	Authentication functions for the Gm IF provide IMS-AKA as specified in TS 133 203 [7]. Authentication functions for the Gm IF provide IPsec packet authentication as specified in TS 133 203 [7]. Optional authentication functions for the Gm IF provide SIP HTTP-digest as defined in RFC 3261 [26]. Optional authentication functions for the Gm IF provide NASS-IMS bundled authentication as specified in ES 283 003 [23] and TS 183 033 [6].
	CONF	Confidentiality functions for the Gm IF protect IMS-AKA key distribution against loss of confidentiality specified in TS 133 203 [7]. Confidentiality functions for the Gm IF protect IPsec packet encryption as specified in TS 133 203 [7].
	INT	Integrity function for the Gm IF protects IMS-AKA key distribution against loss of integrity as specified in TS 133 203 [7]. Integrity function for the Gm IF protects IPsec packet integrity as specified in TS 133 203 [7].
	KM	Key management functions for the Gm IF provide IMS-AKA as specified in TS 133 203 [7].
Gq' (AF - SPDF)	AUTH	Authentication functions for securing DIAMETER for Gq' are as defined by TS 183 017 [35].
	CONF	Confidentiality functions for securing DIAMETER for Gq' are as defined by TS 183 017 [35].
	INT	Integrity functions for securing DIAMETER for Gq' are as defined by TS 183 017 [35].
	KM	Key management functions for securing DIAMETER for Gq' are as defined by TS 183 017 [35].
Ia (SPDF - BGF)	AUTH	Ia IF does not provide any authentication functions; see ES 283 018 [19].
	CONF	Ia IF does not provide any confidentiality functions; see ES 283 018 [19].
	INT	Ia IF does not provide any integrity functions; see ES 283 018 [19].
	KM	Ia IF does not provide any key management functions; see ES 283 018 [19].
Ic (IBCF - IBCF)	AUTH	n.a.
	CONF	Confidentiality functions for Ic are as specified by TS 182 006 [25].
	INT	n.a.
	KM	n.a.
ISC (CSCF - AS)	AUTH	n.a.
	CONF	n.a.
	INT	n.a.
	KM	n.a.
Mg (CSCF - MGCF)	AUTH	n.a.
	CONF	n.a.
	INT	n.a.
	KM	n.a.
Mj (BGCF - MGCF)	AUTH	n.a.
	CONF	n.a.
	INT	n.a.
	KM	n.a.
Rq (SPDF - A-RACF)	AUTH	Authentication functions for securing the DIAMETER protocol for the Rq IF are as specified by ES 283 026 [40].
	CONF	Confidentiality functions for securing the DIAMETER protocol for the Rq IF are as specified by ES 283 026 [40].
	INT	Integrity functions for securing the DIAMETER protocol for the Rq IF are as specified by ES 283 026 [40].
	KM	Key management functions for securing the DIAMETER protocol for the Rq IF are as specified by ES 283 026 [40].
Sh (AS - UPSF) (SCS - UPSF)	AUTH	Authentication functions for securing the DIAMETER protocol for the Sh IF are as specified by TS 129 329 [17] and by TS 133 210 [8].
	CONF	Confidentiality functions for securing the DIAMETER protocol for the Sh IF are as specified by TS 129 329 [17] and by TS 133 210 [8].
	INT	Integrity functions for securing the DIAMETER protocol for the Sh IF are as specified by TS 129 329 [17] and by TS 133 210 [8].
	KM	Key management functions for securing the DIAMETER protocol for the Sh IF are as specified by TS 129 329 [17] and by TS 133 210 [8].
Ua (NAF - UE)	AUTH	Authentication functions for Ua IF are as specified by TS 133 220 [11].
	CONF	Confidentiality functions for Ua IF are as specified by TS 133 220 [11].

NGN IF	Security Services	Countermeasure and security mechanism in NGN
	INT	Integrity functions for Ua IF are as specified by TS 133 220 [11].
	KM	Key management functions for Ua IF are as specified by TS 133 220 [11].
Ub (BSF - UE)	AUTH	Authentication functions for Ub IF are as specified by TS 133 220 [11].
	CONF	Confidentiality functions for Ub IF are as specified by TS 133 220 [11].
	INT	Integrity functions for Ub IF are as specified by TS 133 220 [11].
	KM	Key management functions for Ub IF are as specified by TS 133 220 [11].
Ut (UE - (AP) - AS)	AUTH	Authentication functions for Ut IF are as specified by TS 133 141 [9], TS 133 222 [10] and by TS 183 033 [6].
	CONF	Confidentiality functions for Ut IF are as specified by TS 133 141 [9], TS 133 222 [10] and by TS 183 033 [6].
	INT	Integrity functions for Ut IF are as specified by TS 133 141 [9], TS 133 222 [10] and by TS 183 033 [6].
	KM	Key management functions for Ut IF are as specified by TS 133 222 [10], TS 133 141 [9] and by TS 183 033 [6].
Za (SEGF - SEGF)	AUTH	Authentication functions for Za IF are as specified in TS 133 210 [8].
	CONF	Confidentiality functions for Za IF are as specified in TS 133 210 [8].
	INT	Integrity functions for Za IF are as specified in TS 133 210 [8].
	KM	Key management functions for Za IF are as specified in TS 133 210 [8].
Zb (SEGF - FE)	AUTH	Optional authentication functions for Zb IF areas specified in TS 133 210 [8].
	CONF	Optional confidentiality functions for Zb IF are as specified in TS 133 210 [8].
	INT	Optional integrity functions for Zb IF are as specified in TS 133 210 [8].
	KM	Optional key management functions for Zb IF are as specified in TS 133 210 [8].
Zh (BSF - UPSF)	AUTH	Authentication functions for Zh IF are as specified by TS 133 220 [11].
	CONF	Confidentiality functions for Zh IF are as specified by TS 133 220 [11].
	INT	Integrity functions for Zh IF are as specified by TS 133 220 [11].
	KM	Key management functions for Zh IF are as specified by TS 133 220 [11].
Zn (BSF - UE)	AUTH	Authentication functions for Zn IF are as specified by TS 133 220 [11].
	CONF	Confidentiality functions for Zn IF are as specified by TS 133 220 [11].
	INT	Integrity functions for Zn IF are as specified by TS 133 220 [11].
	KM	Key management functions for Zn IF are as specified by TS 133 220 [11].

5.4 Mapping of 3GPP security FEs to NGN FEs

NGN shall re-use 3GPP security entities (AuC, HLR and HSS; see TS 123 002 [45]) as follows; see also figure 13 that illustrates a mapping of 3GPP FEs to NGN FEs:

- The PDBF at the NASS level shall conceptually encompass the same functionality that is provided by the AuC, see TS 123 002 [45], clause 4.1.1.1.2. Additionally, the PDBF shall contain the NASS level profiles needed for the NASS layer authentication.

NOTE 1: Conceptually means that the functionality is not the same as AuC operates at IMS level while PDBF operates at NASS level. Thus, the functions of the AuC need to be transposed into some conceptually equivalent functions at the PDBF.

- When mapping the 3GPP PS domain architecture to the NASS architecture, the H-UAAF conceptually covers the part of the HLR that is used to access the AuC; see figure 13, see TS 123 002 [45], clause 4.1.1.1.1. When mapping the 3GPP WLAN architecture to the NASS architecture, the H-UAAF is equivalent to the WLAN H-AAA server, while the V-UAAF is equivalent to a WLAN AAA proxy; see figure 14, see TS 133 234 [46], clause 4.1.4.

- The UPSF as a generic FE shall encompass:

  - Authentication data for the IMS are held in the non-HLR part of the HSS. However, this part of the HSS is not explicitly termed AuC. This part is shown as AuC' to represent the AuC functionality for the IMS (i.e. ISIM-based). This AuC' functionality is inherited by the UPSF.

  - Some other HSS functionality (different from AuC and HLR).

NOTE 2: The HSS is defined in TS 123 002 [45], clause 4.1.1.1.

Generally, NGN FEs shall not encompass any 3GPP functionality that relates to supporting the CS and PS domain.

Figures 13 and 14 show interfaces:

- PDBF - UAAF: This interface is not defined.
- Components and interfaces within UPSF are not defined.
- Internal interfaces within HSS are not defined in 3GPP.

NOTE 3: Figures 13 and 14 show relationships at a high level and are not meant to imply exact correspondences. Some details can of course not be mapped precisely. Some details can of course not be mapped precisely. This is because the architectural assumptions on the environment of user data in 3GPP and in NGN are somewhat different. In particular, the scopes of UAAF and HLR are different.

NOTE 4: IMS data also contains AuC data related to ISIM.

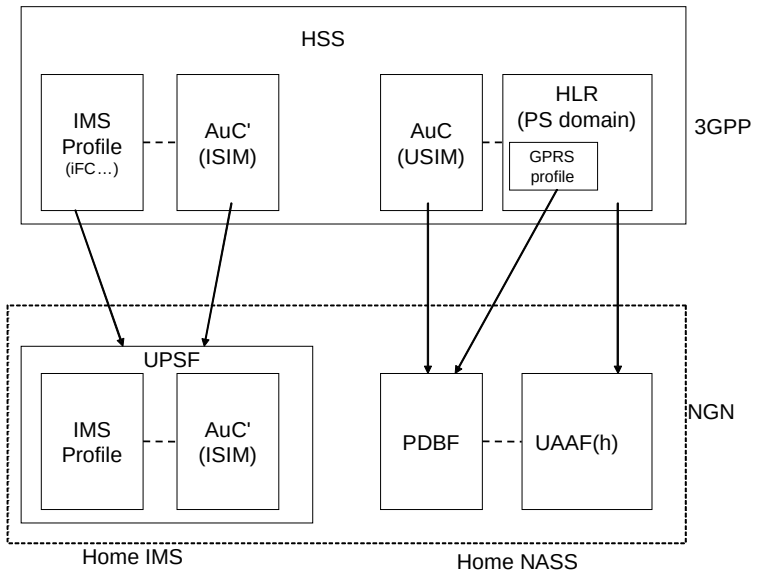


Figure 13: Mapping of HSS (AuC, HLR) to PDBF, UPSF, UAAF (PS domain)

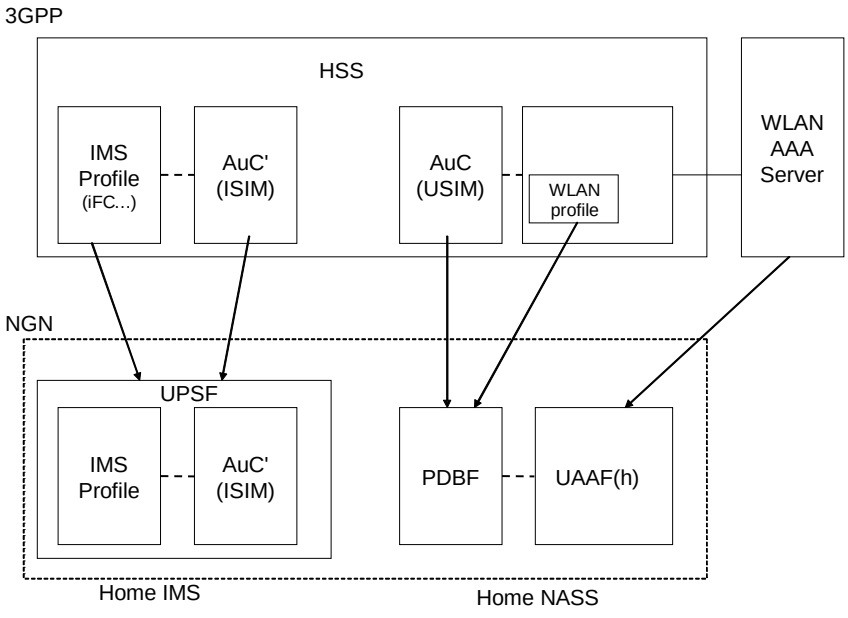


Figure 14: Mapping of HSS (AuC, HLR) to PDBF, UPSF, UAAF (WLAN case)

6 NGN IMS Residential Gateway

User may gain access to NGN IMS services by using a non-ISIM capable SIP UA via a NGN IMS Residential Gateway (IRG). NGN IMS Residential Gateway is an optional functional element within the NGN architecture and serves the purpose to securely connect legacy, non-NGN UE equipment to the NGN that does not have the capability of using an ISIM/UICC. The IRG holds a SIP B2BUA, which has a full NGN IMS UA interface towards the NGN IMS network. The interface towards to the local user is not specified by the present document; however, it could be for example IETF compatible SIP UA (see RFC 3261[26]), softphone, IP phone, IAD/DECT or some other possibly proprietary phone system. The IMS Residential Gateway is placed in the customer's domain. One potential realization of IMS Residential Gateway is presented in figure 15.

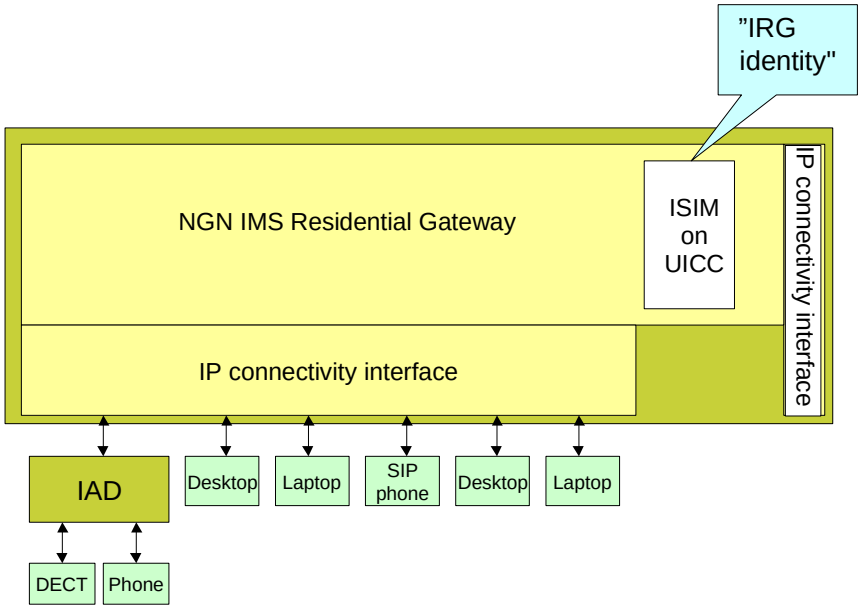


Figure 15: Potential realization of NGN IMS Residential Gateway

The ISIM within the IRG represents the required security functionality for IMS in NGN. In NGN, the ISIM (see TS 131 103 [16]) shall be deployed in conjunction with a UICC (see TS 122 048 [12], TS 123 048 [13], TS 131 101 [14] and TS 131 102 [15]).

The operator shall disable all implicit registrations sets from the HSS, on behalf of those ISIMs that are dedicated to IMS Residential Gateways. If there are implicit registrations sets defined in the HSS, then the implementation of IMS Residential Gateway gets a lot harder. It is recommended that the ISIM include only one Public User Identity.

IMS Residential Gateway when implemented in a device should be robust, and therefore it should store the registrations states (local and IMS registration states) and security connections states to a memory that is not erased during outages. It is recommended that the IMS Residential Gateway and the local UAs authenticate each other, and communicate using some security mechanism. The content of these security measures are out of the scope of the present document.

If the IMS Residential Gateway has phone capabilities by itself, then that phone should be treated like any other local phone.

NOTE 1: A typical IMS Residential Gateway would work as follows. When the IMS Residential Gateway device is switched on, and the first local UA is registered, then the IMS Residential Gateway registers the IMS Residential Gateway identity. The gateway identity is one of the public user identities that are stored to the ISIM. IMS Residential Gateway gets all the associated URIs from P-Associated-URI header field during the registration of explicit line identity. Then the IMS Residential Gateway continues processing the local registration request, assuming that the local registration request is related to one of the associated Public User Identities. After these steps the IMS Residential Gateway should monitor the registration state by subscribing to the registration event package in S-CSCF. Subsequent local registration requests do not initiate the registration of explicit line identity. The incoming calls that are directed to the IMS Residential Gateway identity are automatically directed to all connected UAs. Personal identities are always explicitly registered, and incoming calls to them are always directed only to associated UAs.

NOTE 2: Devices that have an ISIM do not have to use IMS Residential Gateway.

NOTE 3: How to secure the link(s) between UE and IRG is outside the scope of the present document.

Annex B includes some informative implementation notes on the IMS Residential Gateway.

7 Security for H248

7.1 R-MGF Context

Void.

7.2 A-MGF Context

Void.

8 Security Architectures for Media Security

Void.

9 Security Architectures for IPTV

See annex Ffor a description of the potential architectures for IPTV that will be developed for the next release.

10 Security Architecture for Customer Premises Networking

Void.

11 Security Architecture for Fixed Mobile Convergence

Void.

12 Interfaces out of scope

12.1 Interconnect Iz interface I BGF

Void.

12.2 RI' and Gq'

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

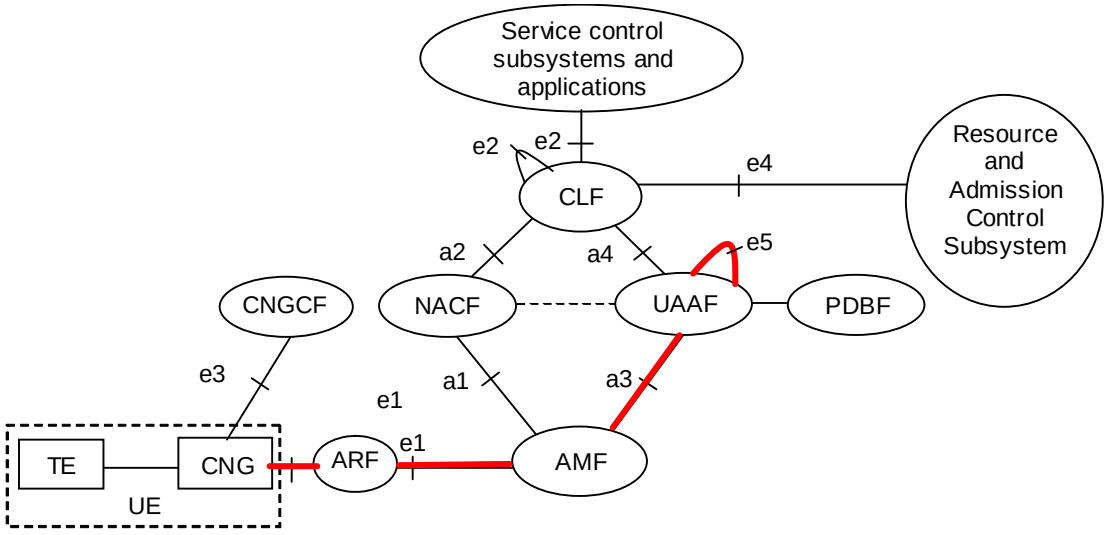
The Network Attachment Subsystem provides the following security functionalities; see ES 282 004 [5], clause 4.1:

- 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.



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.

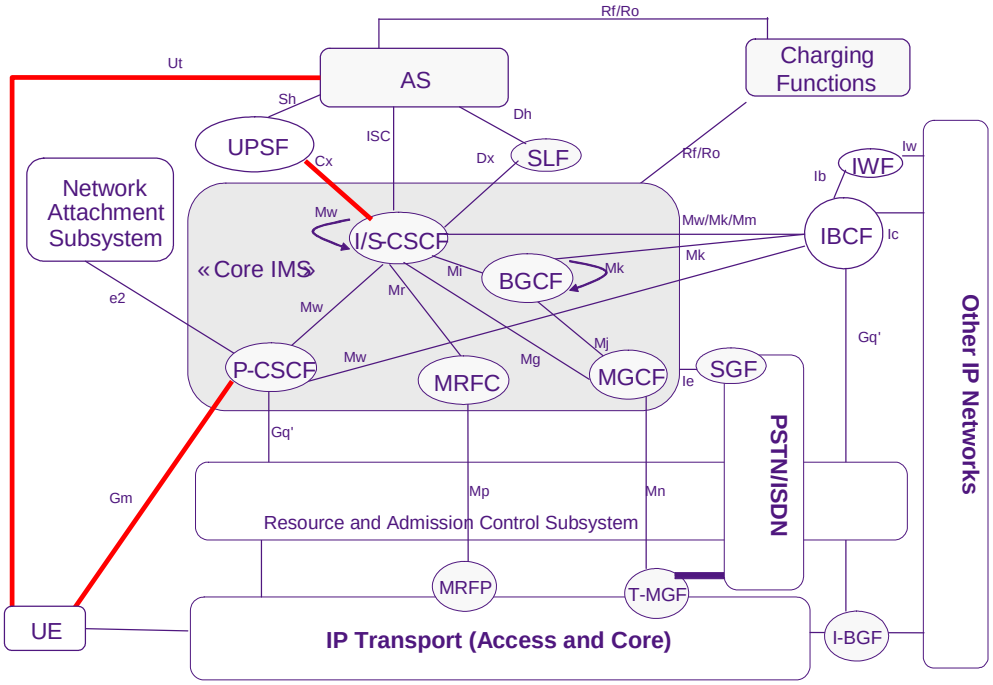


Figure A.2: NGN IMS architecture - Access security (see ES 282 002 [3])

A.2.1.1 Reference Point Gm (UE/IMS Residential Gateway - P-CSCF)

The Gm reference point supports secure communication between an UE or an IMS Residential Gateway and the IMS, e.g. related to registration and session control; see ES 282 007 [24], clause 9.2. Security set-up shall be possible using an ISIM application TS 131 103 [16].

The security association between UE or IMS Residential Gateway 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 [43], early implementations may use the so-called "line authentication" mechanism. This mechanism is optional for implementation.

An interface between the UE and the IMS Residential Gateway is considered outside the scope of the present document.

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 [24], 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 [24], 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 [24]. 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 [24] and TS 182 006 [25]. 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

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.

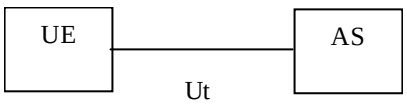


Figure A.3: Ut interface

Ut interface is protected with TLS. Authentication may be based on the Generic Authentication Architecture (GAA) as defined in TS 133 222 [10] or the HTTP Digest mechanisms defined in RFC 2617 [36].

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 [24]. Figure A.4 represents IP-based interconnection.

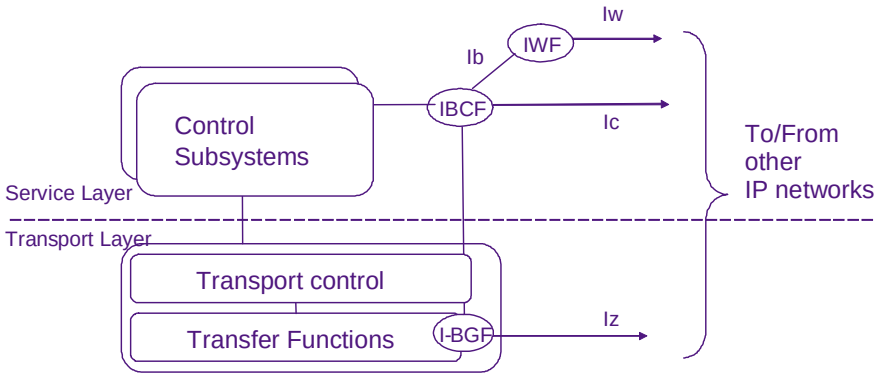


Figure A.4: IP Interconnection (see ES 282 001 [2])

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 [24].

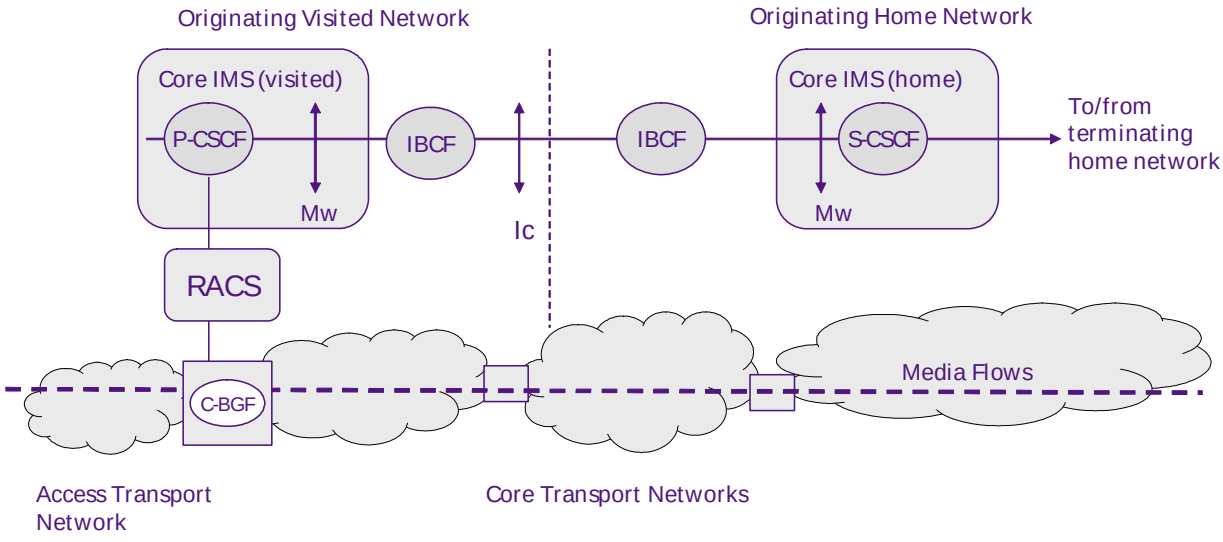
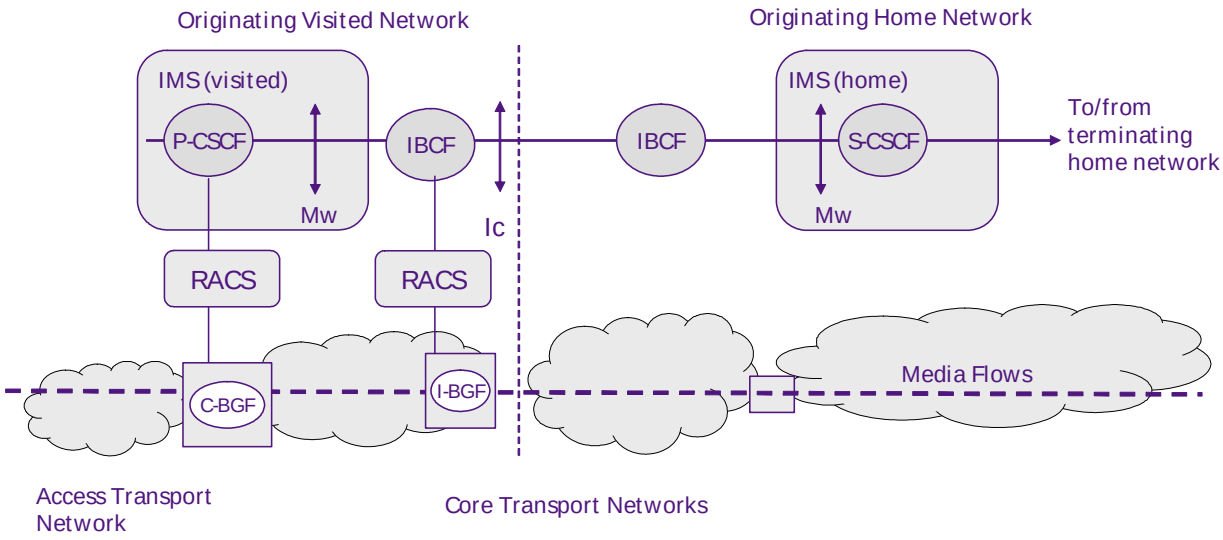


Figure A.5: IMS interconnect scenario without I-BGF (see ES 282 007 [24])



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 on the above figures.

Figure A.6: IMS interconnect scenario with I-BGF (see ES 282 007 [24])

TS 182 006 [25] 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)	
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	

Requirement Reference	Statement of Requirement	Specific Security Function required?	Security Functional Element
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
R-AA-24	NASS shall support both the use explicit (e.g. PPP or IEEE 802.1x [42]) 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

Requirement Reference	Statement of Requirement	Specific Security Function required?	Security Functional Element
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
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

Requirement Reference	Statement of Requirement	Specific Security Function required?	Security Functional Element
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)
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

Requirement Reference	Statement of Requirement	Specific Security Function required?	Security Functional Element
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
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

Requirement Reference	Statement of Requirement	Specific Security Function required?	Security Functional Element
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 ES 202 238 [41] 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 (informative): Implementation notes on the IMS Residential Gateway

The following use cases describe how a non-ISIM SIP User Agent (UA) can register and establish calls via the SIP B2BUA within an IMS Residential Gateway. The use cases are based on TS 183 033 [6]. The different parts are how the UA is connected and how the SIP B2BUA maps the identities and the messages.

It must be noted, that the operator must not define any implicit registration sets in HSS, on behalf of those ISIMs that are dedicated to B2BUAs.

C.1 B2BUA registration

The I-CSCF has been excluded in the use case just for simplification. It is still there in the real use case.

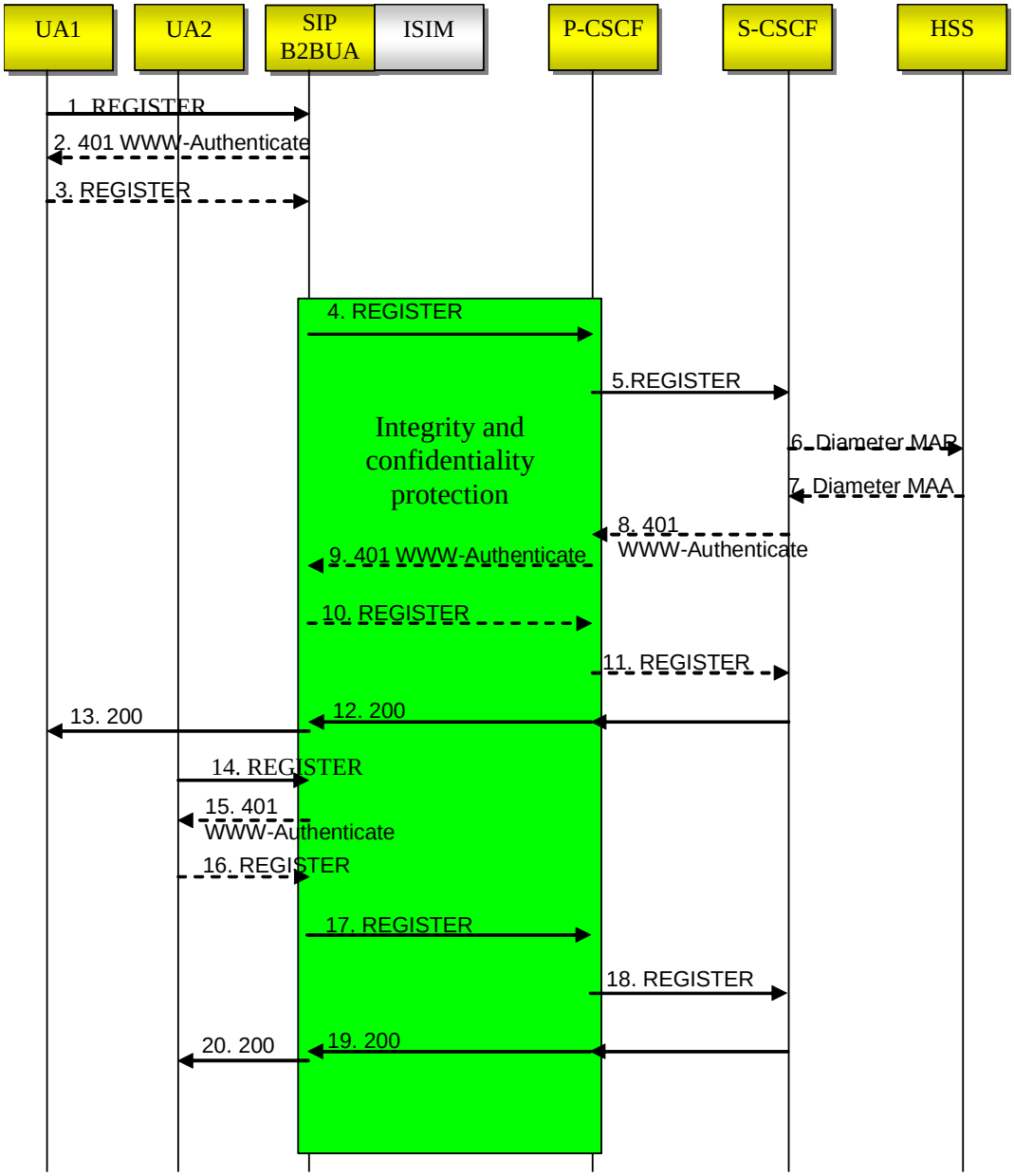


Figure C.1: IMS Residential Gateway registration message flow

1) The UA1 registers to the SIP B2BUA with a To header including a local username (bob) that is associated to the subscription for the ISIM.
example message:
REGISTER To: <sip:bob>

2) The B2BUA optionally challenges the user. The subscriber can for example locally configure if local users should be challenged and the passwords to use for the local users.
Example message:
401 WWW-Authenticate Digest

3) The UA1 resends the register message if challenged. The message then contains an Authorization header including the identity (bob) of the challenged user included in the username parameter.
Example message:
REGISTER Authorization Digest username=bob

4) The B2BUA use the Private User Identity stored in the ISIM as the username. The Contact header contains the IP address (or domain name) of the B2BUA. The selected Public User Identity in the To header is the value in the To header from the UA1 or a mapped name (bob.smith@operator.net) where a local username used by the UA1 is mapped to a Public User Identity. The subscriber can locally configure this mapping.
Example message:
REGISTER Authorization Digest username=IMPI, Security-Client To:<sip:bob.smith@>operator.net>

5) The P-CSCF sends the request to the S-CSCF after excluding some headers (Proxy-Require and Security-Client) and some header information (e.g. sec-agree from the Require header).
Example message:
REGISTER Authorization Digest username=IMPI
To:<sip:bob.smith@>operator.net>

6) The S-CSCF request authentication vectors from HSS in case the client must be authenticated and there are no authentication vectors. The client must initially be authenticated (indicated e.g. by the lack of a downloaded service profile).
Example message:
Diameter MAR

7) The HSS then returns one or several authentication vectors.
Example message:
Diameter MAA

8) The S-CSCF challenges the B2BUA/ISIM with a 401 including RAND and AUTN in case client authentication is necessary.
Example message:
401 WWW-Authenticate (RAND, AUTN)

9) The P-CSCF adds some headers to the 401 before sending it to the B2BUA.
Example message:
401 WWW-Authenticate (RAND, AUTN) Security-Server

10) The B2BUA calculates a RES and verifies the AUTN if challenged by a 401. The B2BUA then sends a new REGISTER including an Authorization header with the digest where RES has been used as the shared key.
Example message:
REGISTER Authorization username=IMPI, RES Security-Client, Security-Verify
To:<sip:bob.smith@>operator.net>

11) The P-CSCF sends the request to the S-CSCF after excluding some headers (Proxy-Require, Security-Verify and Security-Client) and some header information (e.g. sec-agree from the Require header). The S-CSCF verifies the digest based on RES from the B2BUA with the digest calculated with XRES. This is only necessary if the B2BUA has been challenged.
Example message:
REGISTER Authorization Username=IMPI, RES
To:<sip:bob.smith@>operator.net>

12) The S-CSCF responds with a 200 including Path, Service-Route and P-Associated-URI headers.
Example message:
200 Path Service-Route P-Associated-URI

13) The B2BUA stores the content of the Service-Route and P-Associated-URI headers and then removes the Path, Service-Route and P-Associated-URI headers before sending a 200 to the UA1.
Example message:
200

14) The UA2 registers to the SIP B2BUA with a To header including a local username (alice) that is associated to the subscription for the ISIM.
Example message:
REGISTER To: <sip:alice>

15) The B2BUA optionally challenges the user.
Example message:
401 WWW-Authenticate Digest

16) The UA2 resends the register message if challenged. The message then contains an Authorization header including the identity (alice) of the challenged user included in the username parameter.
Example message:
REGISTER Authorization Digest username=alice

17) The B2BUA use the Private User Identity stored in the ISIM as the username. The selected Public User Identity in the To header is the mapped name (alice.smith@operator.net).
Example message:
REGISTER Authorization username=IMPI, Security-Client Security-Verify
To:<sip:alice.smith@operator.net>

18) The P-CSCF sends the request to the S-CSCF after excluding some headers (Proxy-Require, Security-Verify and Security-Client) and some header information (e.g. sec-agree from the Require header).
Example message:
REGISTER Authorization: username=IMPI,
To: <sip:alice.smith@operator.net>

19) Since the S-CSCF has already authenticated the Private User Identity (there is a service context) there is no need to do it again. The S-CSCF responds with a 200 including Path, Service-Route and P-Associated-URI headers.
Example message:
200 Path Service-Route P-Associated-URI

20) The B2BUA stores the content of the Service-Route and P-Associated-URI headers and then removes the Path, Service-Route and P-Associated-URI headers before sending a 200 to the UA1.
Example message:
200

C.2 B2BUA originating session establishment

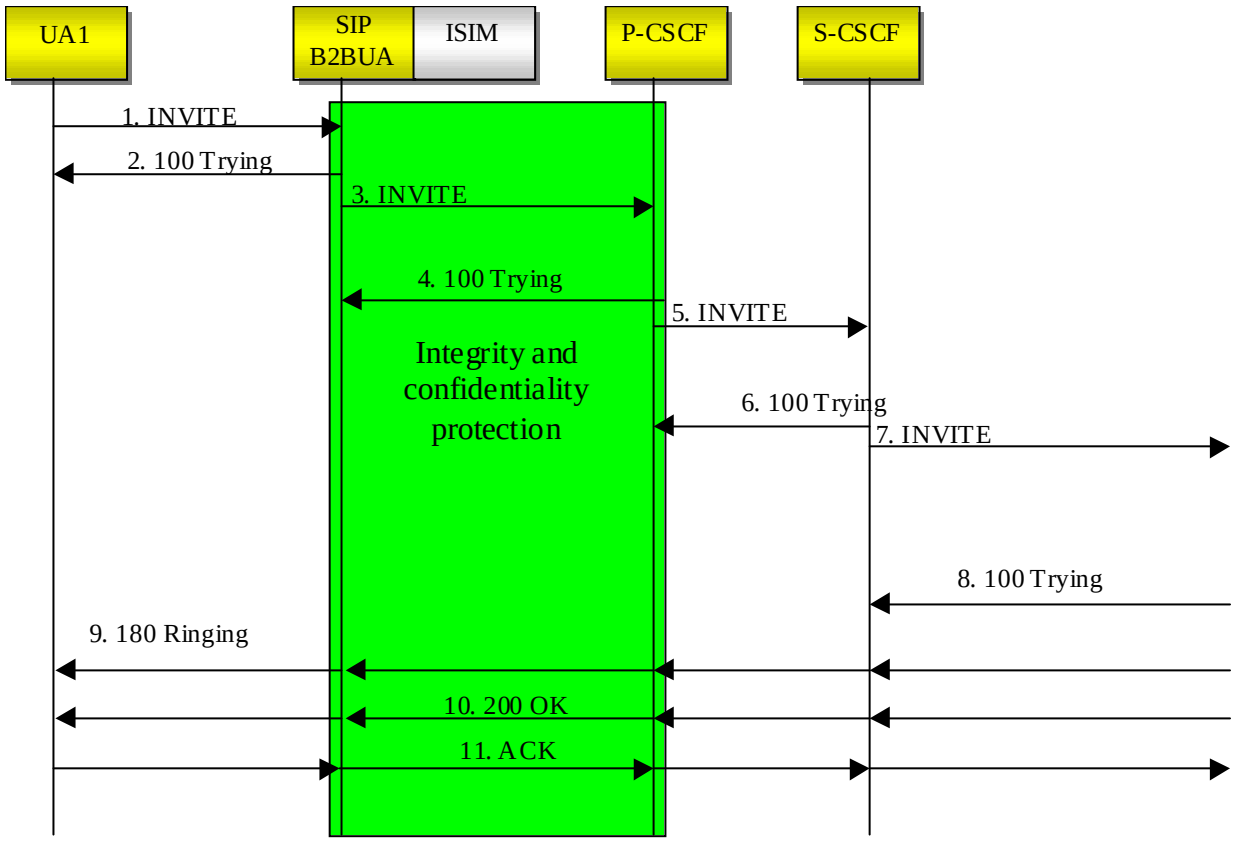


Figure C.2: B2BUA originating session establishment message flow

1) The UA1 sends an INVITE to the B2BUA:
Example message:
INVITE sip:carl.jones@otheroper.net Contact <sip:192.168.1.2> From: <sip:bob>

2) The B2BUA responds with a 100 Trying.

3) The B2BUA adds some headers to the INVITE message. The From header is converted to the Public User Identity that is equal to the personal identity for the user. The P-Preferred-Identity header contains as well the personal identity. The B2BUA changes the Contact header and sends the INVITE to the P-CSCF.
Example message:
INVITE sip:carl.jones@otheroper.net Contact <sip:130.1.2.3 :5678>
From:<sip:bob.smith@operator.net>

4) The P-CSCF responds with 100 Trying.
Example message:
100 Trying

5) The P-CSCF removes the P-Preferred-Identity and inserts instead a P-Asserted-Identity that contains the content of P-Preferred-Identity if that was authorized from the network point of view. The P-CSCF then sends the INVITE to the S-CSCF.
Example message:
INVITE sip:carl.jones@otheroper.net Contact <sip: 130.1.2.3 :5678>
From:<sip:bob.smith@operator.net>

6) The S-CSCF responds with 100 Trying.
Example message:
100 Trying

7) The S-CSCF removes the P-Access-Network-Info before the INVITE is sent out from the network.
Example message:
INVITE sip:carl.jones@otheroper.net
Contact <sip: 130.1.2.3 :5678>
From:<sip:bob.smith@operator.net>

8) A remote CSCF responds with 100 Trying.
Example message:
100 Trying

9) The other party sends a 180 Ringing
Example message:
180 Ringing Record-Route

10) The other party sends a 200 OK
Example message:
200 OK Record-Route SDP

11) The UA1 acknowledges the 200 OK with an ACK.
Example message:
ACK

C.3 B2BUA terminating session establishment

The I-CSCF and HSS are excluded for simplicity. The I-CSCF is the initial point of contact.

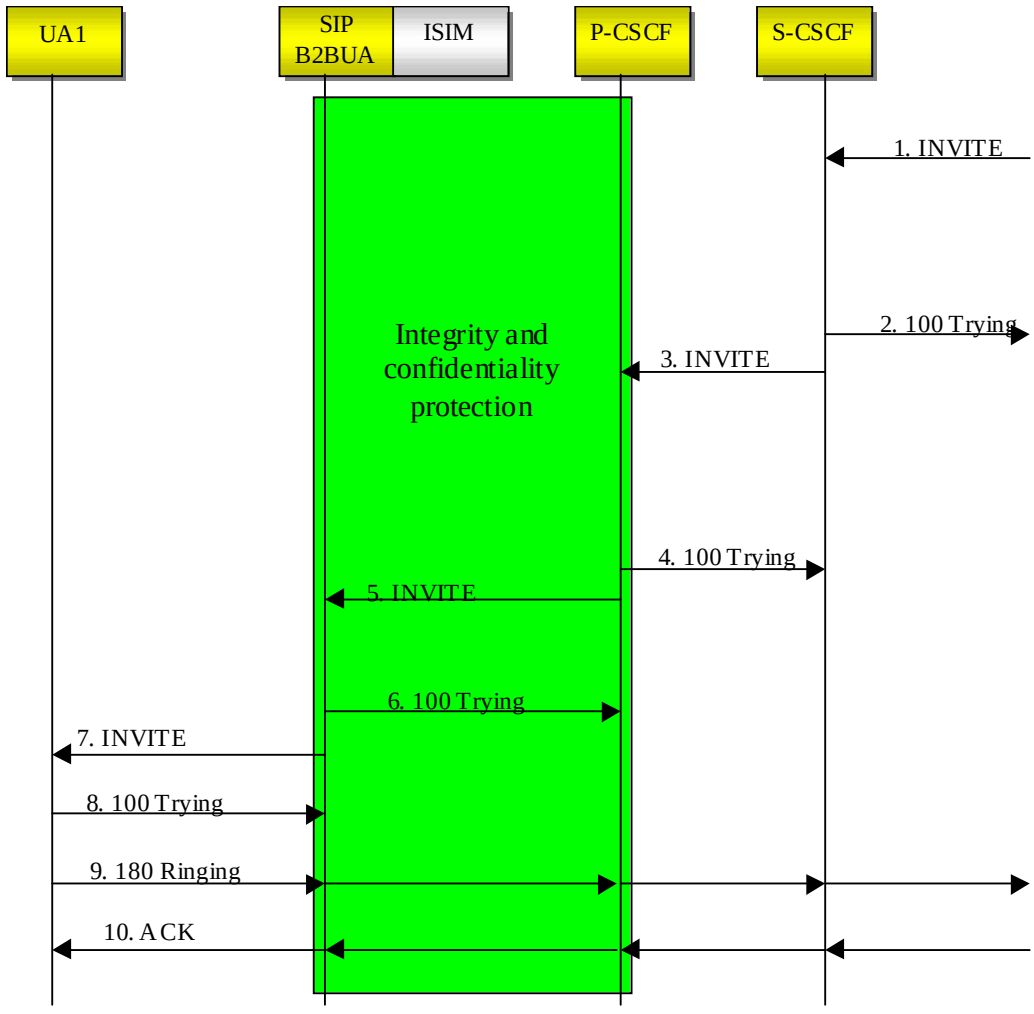


Figure C.3: B2BUA terminating session establishment message flow

1) The remote UA sends an INVITE to the S-CSCF.
Example message:
INVITE sip:bob.smith@operator.net
Contact <sip:132.100.101.102 :7654>
From:<sip:carl.jones@otheroperator.net>

2) The S-CSCF responds with 100 Trying.
Example message:
100 Trying

3) The S-CSCF picks the contact address stored at registration and inserts it as the Request-URI. The S-CSCF inserts the original Request-URI is inserted in the P-Called-Party-ID header and sends the INVITE to the P-CSCF.
Example message:
INVITE sip:130.1.2.3 :5678
Contact <sip:132.100.101.102 :7654>
From:<sip:carl.jones@otheroperator.net>

4) The P-CSCF responds with 100 Trying.
Example message:
100 Trying

5) The P-CSCF removes the P-Charging-Vector and sends the INVITE to the B2BUA.
Example message:
INVITE sip:130.1.2.3 :5678 Contact <sip:132.100.101.102 :7654>
From:<sip:carl.jones@otheroperator.net>

6) The B2BUA responds with 100 Trying.
Example message:
100 Trying

7) The B2BUA uses the Request-URI in the received request to find the home user that has previously registered. The Request-URI is replaced with the locally stored contact address. The B2BUA sends the INVITE to the UA1.
Example message:
INVITE sip:192.168.1.2 Contact <sip:192.168.1.1> From:<sip:carl.jones@otheroperator.net>

8) The UA1 responds with 100 Trying.
Example message:
100 Trying

9) The UA1 responds with 180 Trying.
Example message:
180 Trying

10) The remote UA sends an ACK to the UA1 via the S-CSCF and P-CSCF.
Example message:
180 Ringing

Annex D (informative): Supplementary Information on NASS-IMS Bundled Authentication

D.1 Flow Diagram for NASS Bundled Authentication

This clause describes how clients authenticate to NASS and simultaneously also gain service layer authentication using the "single-sign-on" NASS bundled authentication. The sequence diagram is depicted in figure D.1.

1) The UE gets network attachment after the authentication at the NASS level. The CLF in the NASS (network attachment subsystem) holds a binding between the IP address and the location information (contains the Line Identifier), which the user holds per the xDSL connectivity. The selection of the authentication (whether NBA is possible or not) is done at UPSF level on IMS-user basis.

2) As the SIP REGISTER message reaches P-CSCF, the P-CSCF knows whether or not a security association is required at this point, based on:

   - the SIP signalling;
   - presence of local policies (such as network interface);
   - L3/L2 address.

   During the SIP registration, the P-CSCF locates the CLF based on the UE's IP address or/and based on the information of the access network from which the P-CSCF receives the IP packet (P-CSCF may have several logical/physical interfaces toward different Access Networks). P-CSCF performs a "Location Information Query" towards the CLF over the e2 interface. The key for the query is the IP address used by the UE.

3) The CLF sends the response to the P-CSCF including the location information of the UE.

4) The P-CSCF appends the NASS location information to the SIP REGISTER message and forwards the REGISTER message to I-CSCF and eventually to S-CSCF.

5) S-CSCF queries the UPSF over the Cx interface using MAR request.

6) The UPSF returns a message with the location information of the user identified by the IMPI and IMPU (if NASS Bundling is preferred authentication scheme).

7) S-CSCF finally authenticates by comparing the location info embedded in REGISTER message with location information received from the UPSF. If they match the user is successfully authenticated.

8) The S-CSCF sends SAR message to the UPSF and the UPSF sends SAA message back to the S-CSCF.

9) The S-CSCF sends 200 OK message to the UE.

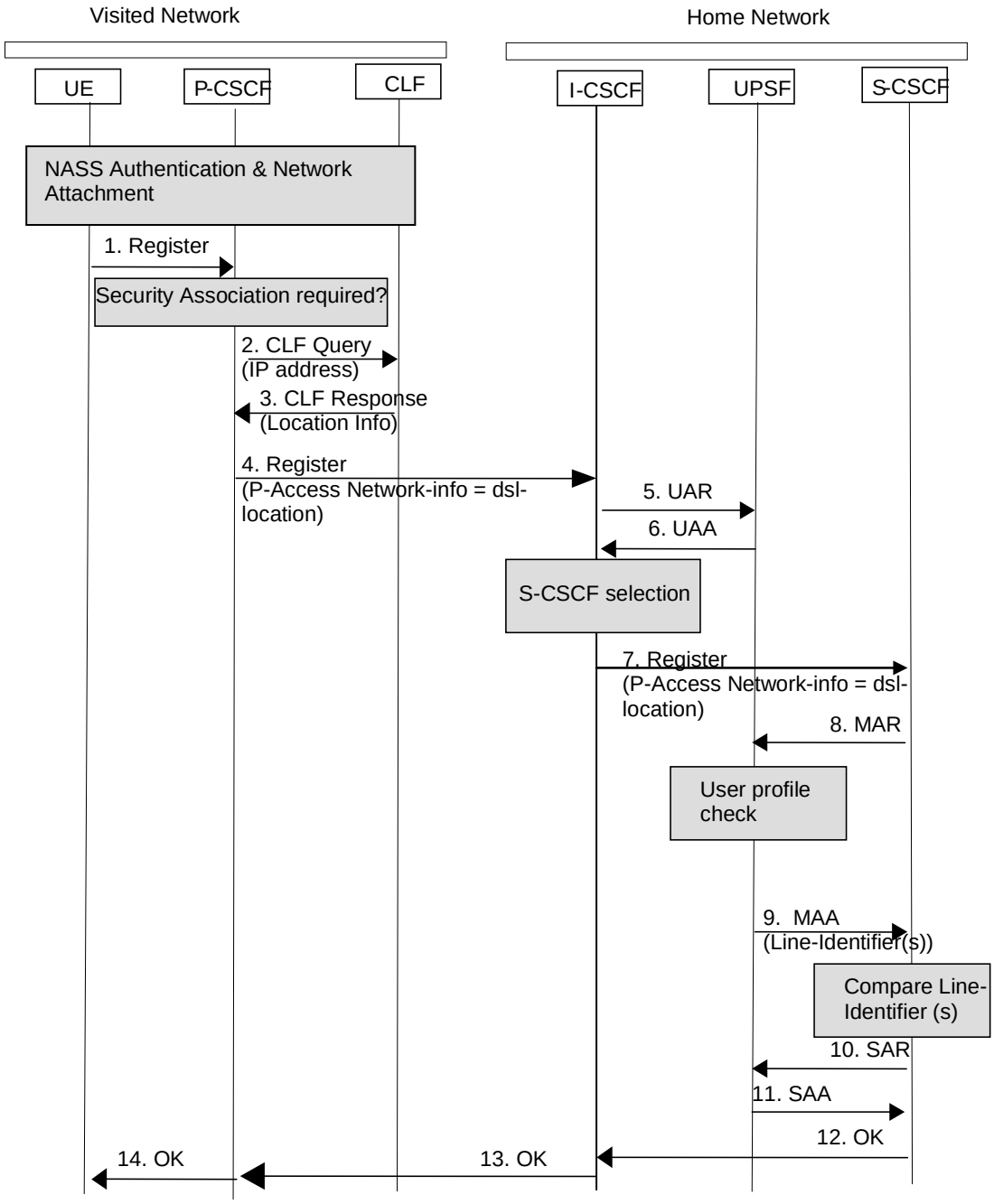


Figure D.1: Flow Diagram for NASS Bundled Authentication (see TS 183 033 [6])

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. IRG).

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 (informative): IPTV content security elements and their interactions

This information material is output from drafting session of WG7 about IPTV content security model discussed on TISPAN 15ter. It presents several possible ways of how should WG7 look to content security elements and their interaction as well as interaction with existing elements of IPTV functional architecture (WI2048/WI2049) (for simplifying complexity for this purpose just with MDF & UE).

The presented models are just example of possible behaviour and have no aim to apply any preferred model. As was accepted during discussion in WG7 drafting session topic required much more future to analyse all relevant models and also models from other SDOs to not develop specific model (more as make general framework or adaptation of existing models). Therefore this information could be used just as guidance for future studies.

The following figures are included:

- Two from several potential behaviours of steps for content security model for unicast services such a CoD (2 options) (not limited to just those).
- One from several potential behaviours of steps for content security model for multicast services such a BC services (2 options - for step 8 was identify different way how could be keys data) (not limited to just those).
- Possible mapping of relation between content security elements and existing TISPAN IPTV functional architecture elements (not limited list, just initial one).

Findings from WG7 drafting session and offline discussions:

The future contributions are welcome and invited to this field:

- We need to make analyses of existing content security model.
- We need to identify mapping of discussed interaction to existing interfaces and IPTV procedures.
- We identify that the content security model for multicast services could have higher priority as unicast service scenarios.
- Special informative annex could be part of document WI 7029 (towards WI2048/WI2049) for purpose of synchronization with WG2 documents.
- There should be required additional functionalities or tasks to existing content security functions.

F.1 IPTV-Unicast authorized Content Delivery Option A

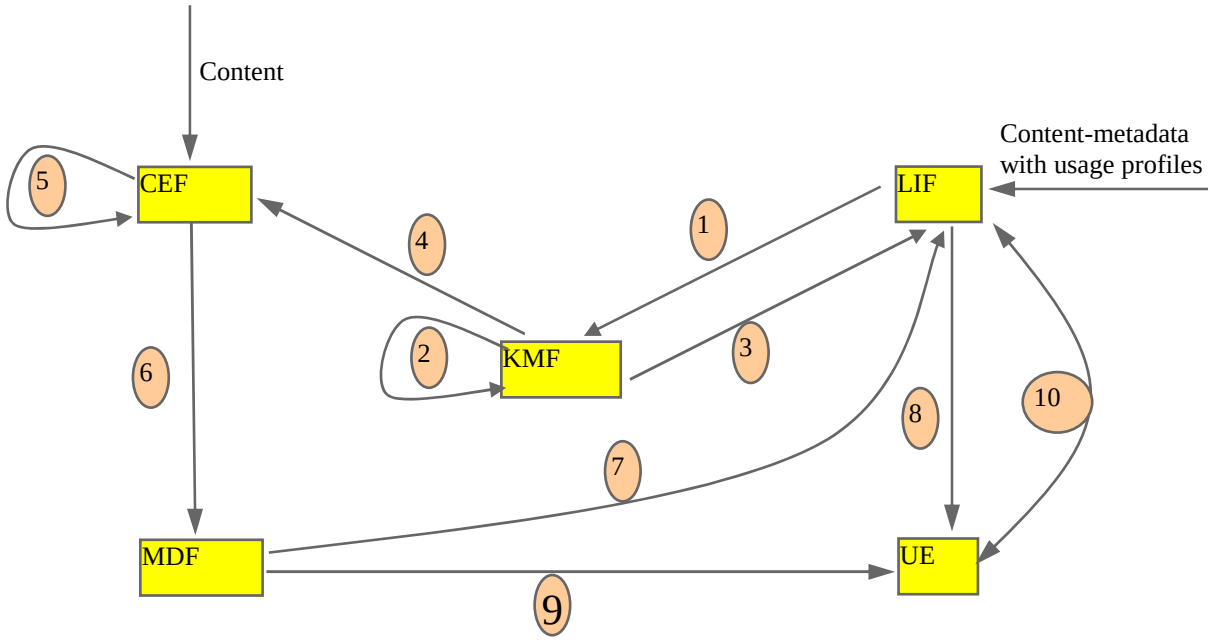


Figure F.1: IPTV-Unicast authorized Content Delivery Option A

F.2 IPTV-Unicast authorized Content Delivery Option B

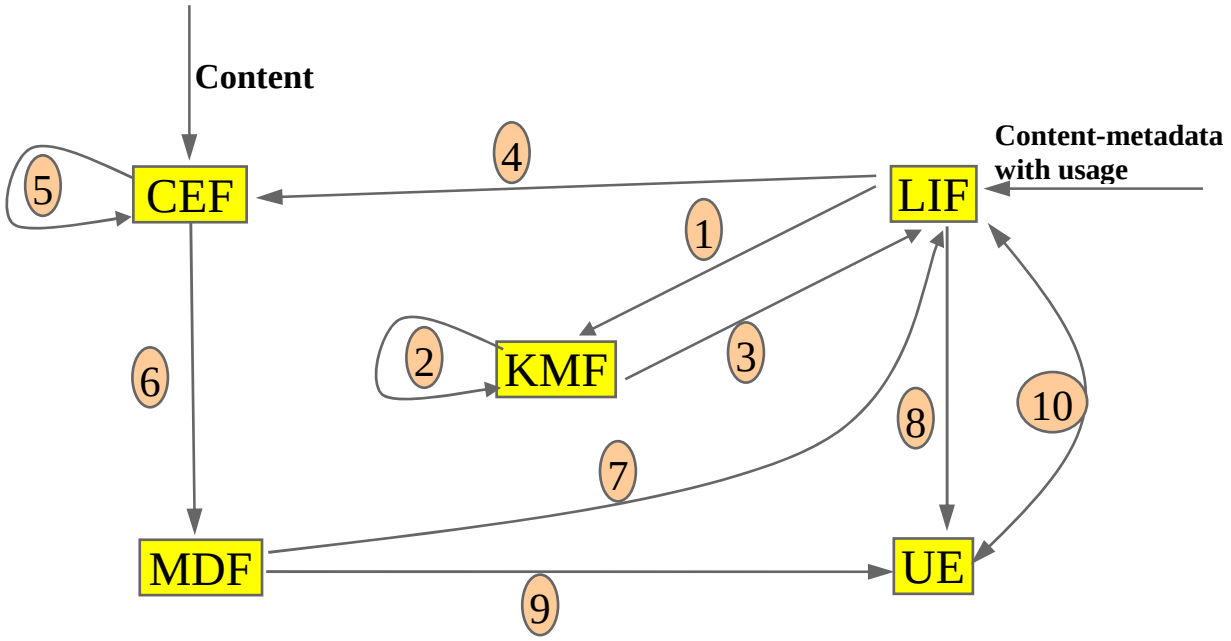


Figure F.2: IPTV-Unicast authorized Content Delivery Option B

1) LIF Requests Auth.Key at KMF.
2) KMF Generates Keying data according to the metadata policy sent by LIF.
3) KMF Sends Keying data to LIF.
4) KMF Sends Keying data to CEF.
5) CEF encrypts content.
6) CEF Sends encrypted content to MDF.
7) MDF informs LIF "content ready for sending".
8) LIF sends corresponding Keying data with metadata to UE.
9) MDF delivers encrypted content to UE.
10) UE confirms the successful receipt of content and decryption.

F.3 IPTV-Multicast Content Delivery

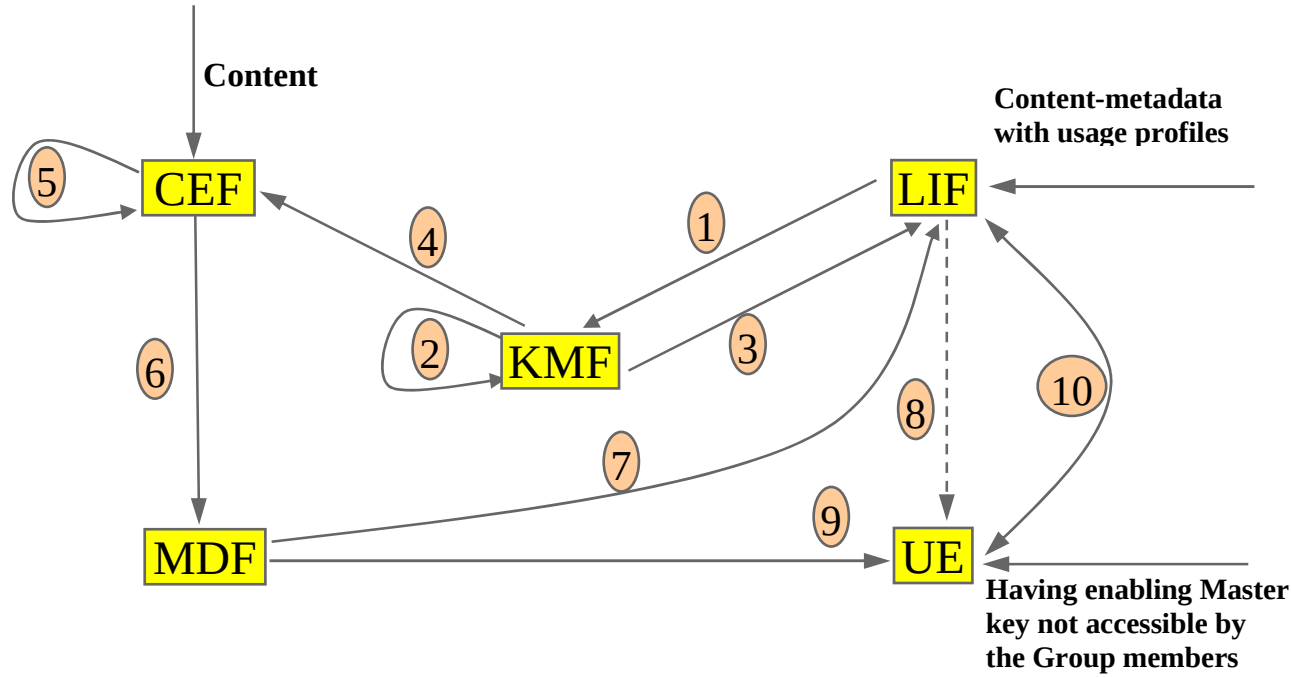


Figure F.3: IPTV-Multicast Content Delivery

1) LIF Requests Auth.Key at KMF.
2) KMF Generates Keying data according to the metadata policy.
3) KMF Sends Key to LIF.
4) KMF Sends Key to CEF.
5) CEF encrypts content in real-time. (The key material consists in multicast case of a session-based key related to the temporary usage of the content combined with the enabling master key, which enables only the authorized members of a group to decrypt the content. This master key must be protected from distribution by the authorized users to unauthorized users).
6) CEF sends content to MDF.
7) MDF notifies "content ready for sending" to LIF.

8) LIF Sends Key to UE (Keys may be send within content itself as well).

9) MDF sends "live content" to authorized Group of UEs.

10) UE decrypts and confirms the successful receipt of content.

F.4 Mapping Content Security to IPTV architecture

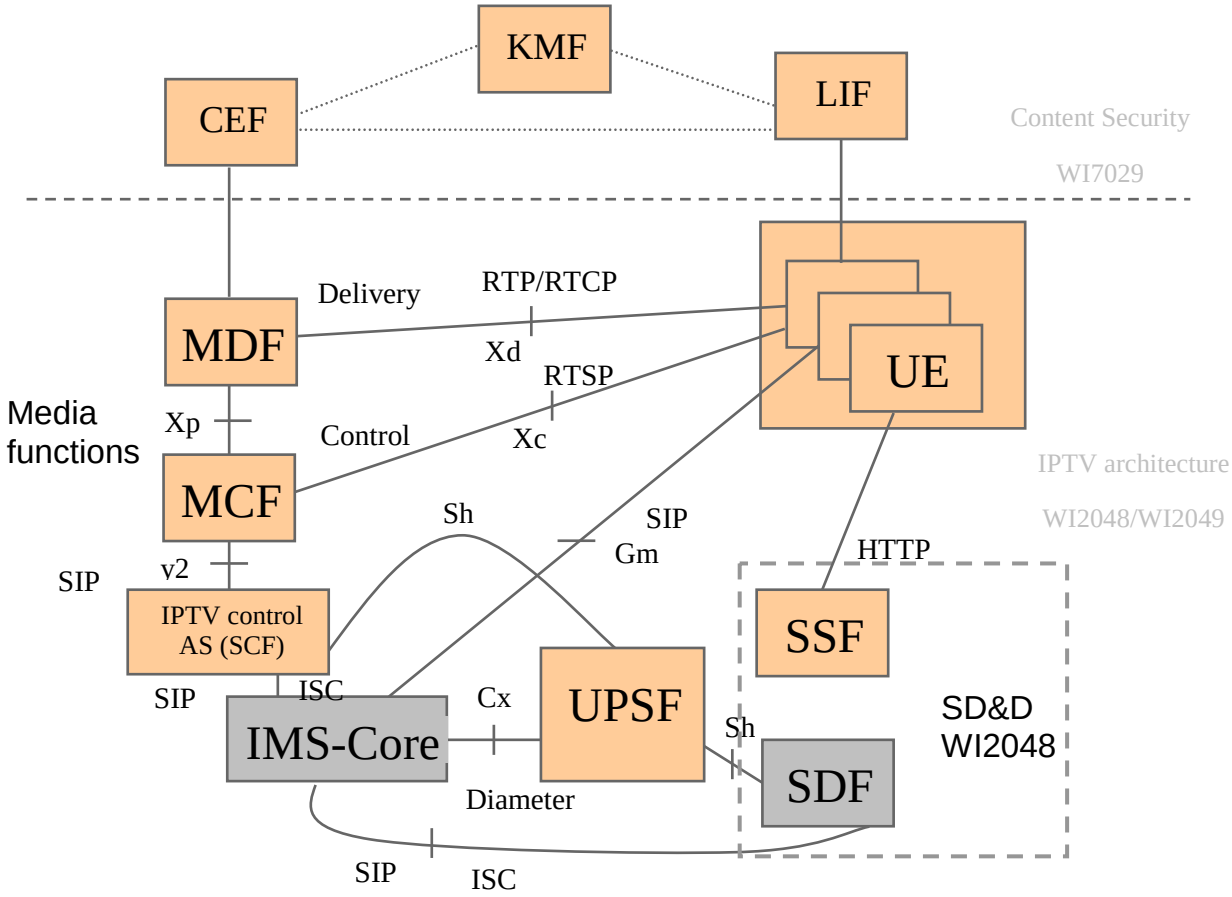


Figure F.4: Mapping Content Security to IPTV architecture

Potential relation between content security entities and IPTV functional architecture entities:

LIF - KMF

KMF - CEF

LIF - CEF

CEF - MDF

LIF - SCF

LIF - UE

LIF - UPSF

LIF - SCF (IPTV Service Control/IPTV AS)

CEF - Preparation function (2049)

LIF - SSF (Service Selection Function)

F.5 Text contributed during release 2

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 content protection provided by the content owner is out of the scope of the present document.

The two kinds of protection can be treated independently of each other, but in order to provide security for all services in the IPTV system, we may need to use service protection in combination with content protection:

9.1 Common IPTV security entities

9.1.1 Security assumptions

9.1.1.1 Link layer security assumptions

9.1.1.2 Network layer security assumptions

9.1.1.3 Service layer security assumptions

9.1.1.4 Application layer security assumptions

9.1.2 Overview of security functional entities

NOTE: Currently, the security elementary function entities are assumed the same in the WI2048 and WI2049, so the corresponding function entities are assumed the same.

9.1.2.1 Content security functions definition

For content security 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.
- **Key management:** This elementary function handles the management of the security keys, including generate and provide the keys and corresponding parameters to the desired entities.
- **Content encryption:** This elementary function handles the content protection related operations, e.g. content encryption and encapsulation operations, etc.

NOTE 1: 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).

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

NOTE 2: These definitions are copied from Security clauses of WI2048 and also WI2049 with same text. If WG7 need to change text in this section then will be required request to change also definition in WI2048/WI2049 documents as change request. If actual definition will be not changed whole text from this section could be replaced by reference to final document and their security section in WI2048/2049.

9.1.2.2 Content security functions location

The locations of those elementary functions are as follows:

- **Content encryption:** Should be integrated into MDF (which is already defined in TS 182 027 [i.3] as optional functionality for MDF).
- **Key management:** Shall be located as a standalone function entity for media stream protection; it may also provide keys for media content protection. This shall be known as KMF.
- **Content licensing:** Is located as a standalone function entity. This shall be known as LIF.

NOTE 1: The interface to the content licensing is in the scope of NGN, but the internal operation is left FFS.

NOTE 2: In order to provide flexibility, the content encryption elementary function may also be located as a new entity in the content preparation functions; this is out of the scope of the present document.

NOTE 3: For media content protection, the actual deployed DRM system may use its own key management module; this is out of the scope of the present document.

NOTE 4: The reference points of those functions are for FFS in the present document, it should be addressed in the present document to leave flexibility not restrictive to any applicable DRM model.

NOTE 5: The tasks of LIF with regards to licensing and authorisation are FFS.

9.1.3 Key Management models

9.1.4 Content Protection and service protection models

9.1.4.1 Media content protection model

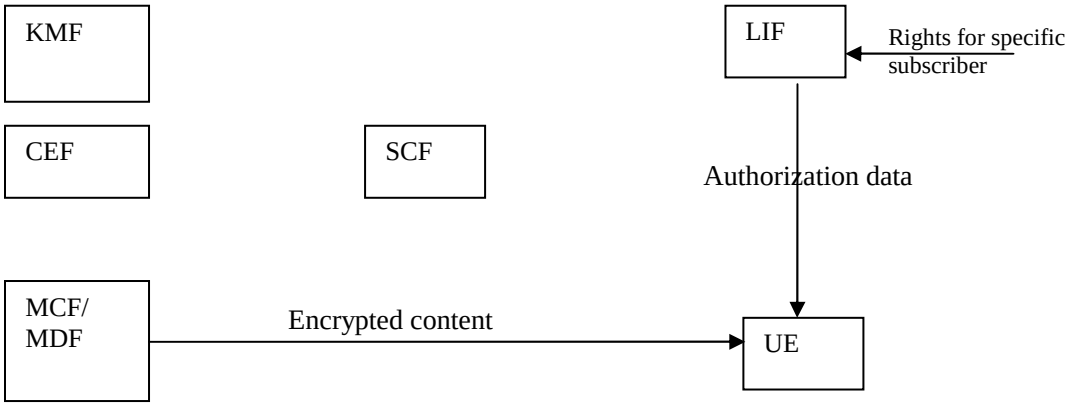


Figure F.5: IPTV media content protection model

Figure F.5 illustrates the model.

1) Relationship between LIF, KMF and MCF/MDF

NOTE 1: The descriptions of relationship requires further contributions to provide analysis.

NOTE 2: The realization of LIF is related to specific DRM system.

2) Relationship between content security elementary functions and existing functions

MCF/MDF delivers the encrypt content to user equipments.

User equipment receives the encrypted content from MCF/MDFs and fetches the license from the LIF, then use the keys from the license to release the key to decrypt the content, and use the content according to the rights defined in the license.

NOTE 3: If the content is offline pre-encrypted, the operations of CEF encryption and the operations of license acquisition of UE may be asynchronous.

NOTE 4: The generation of license in LIF may be started by several methods, e.g. the user equipment request for license or service control functions, further analysis is required.

NOTE 5: The relationship between content security elementary functions and SCF (Service Control Function) and other related existing functions require contributions to provide further analysis.

NOTE 6: The authorization data in this model needs further analysis.

9.1.4.2 Media stream protection model

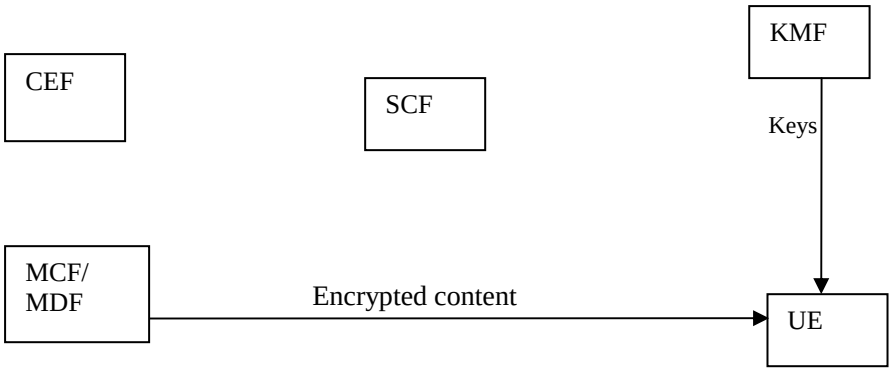


Figure F.6: IPTV media stream protection model

The figure above illustrates the model;

MCF/MDF delivers the encrypt content to user equipments.

The KMF provides keys for the user equipment to decrypt the content.

NOTE 1: UE may not request the keys directly from the KMF, because the KMF keeps all the keys for the content encryption, directly access increases the risks of attacks towards the KMF, this may render the KMF to directly face the attack from UEs, once the KMF is broken, all the keys may be acquired by the attacker, which is a severe problem.

NOTE 2: Contributions are required to provide use cases for media content protection and media stream protection.

IMS-based IPTV subsystem

9.2.1 Security architecture

9.2.2 Reference points

9.2.3 Media stream protection mechanisms

9.2.4 Media content protection mechanisms

9.3 Dedicated IPTV subsystem

9.3.1 Security architecture

9.3.2 Reference points

9.3.3 Media stream protection mechanisms

9.3.4 Media content protection mechanisms

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".

History

Document history		
V2.1.1	February 2009	Publication