Reference

RTS/TISPAN--07051-NGN-R3

Keywords

Stage2, Stage 3, 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

Important notice

Individual copies of the present document can be downloaded from:

http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2011.
All rights reserved.

DECT™, PLUGTESTS™, UMTS™, TIPHON™, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. LTE™ is a Trade Mark of ETSI currently being registered for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.
## Contents

Intellectual Property Rights ............................................................................................................................................................. 5

Foreword ............................................................................................................................................................................................................................ 5

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Scope</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>References</td>
<td>5</td>
</tr>
<tr>
<td>2.1</td>
<td>Normative references</td>
<td>5</td>
</tr>
<tr>
<td>2.2</td>
<td>Informative references</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>Definitions and abbreviations</td>
<td>10</td>
</tr>
<tr>
<td>3.1</td>
<td>Definitions</td>
<td>10</td>
</tr>
<tr>
<td>3.2</td>
<td>Abbreviations</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>NGN Security</td>
<td>13</td>
</tr>
<tr>
<td>4.0</td>
<td>Overview</td>
<td>13</td>
</tr>
<tr>
<td>4.0a</td>
<td>Security services identified in TS 187 001 and TR 187 002</td>
<td>13</td>
</tr>
<tr>
<td>4.1</td>
<td>NGN security architecture</td>
<td>14</td>
</tr>
<tr>
<td>4.2</td>
<td>Security domains</td>
<td>19</td>
</tr>
<tr>
<td>4.5</td>
<td>PES Security Architecture</td>
<td>20</td>
</tr>
<tr>
<td>4.5.1</td>
<td>Security for H.248 within PES</td>
<td>20</td>
</tr>
<tr>
<td>4.6</td>
<td>Application security architecture</td>
<td>21</td>
</tr>
<tr>
<td>4.6.1</td>
<td>Generic Authentication Architecture (GAA)</td>
<td>21</td>
</tr>
<tr>
<td>4.6.1.1</td>
<td>Generic Bootstrapping Architecture (GBA)</td>
<td>21</td>
</tr>
<tr>
<td>4.6.1.2</td>
<td>Support for Subscriber Certificates (SSC)</td>
<td>22</td>
</tr>
<tr>
<td>4.6.1.3</td>
<td>Access to NAF using HTTPS</td>
<td>22</td>
</tr>
<tr>
<td>4.6.2</td>
<td>HTTP Digest authentication for UICC-less CND</td>
<td>22</td>
</tr>
<tr>
<td>5</td>
<td>Void</td>
<td>24</td>
</tr>
<tr>
<td>6</td>
<td>Void</td>
<td>24</td>
</tr>
<tr>
<td>7</td>
<td>Void</td>
<td>24</td>
</tr>
<tr>
<td>7.1</td>
<td>Void</td>
<td>24</td>
</tr>
<tr>
<td>7.2</td>
<td>Void</td>
<td>24</td>
</tr>
<tr>
<td>8</td>
<td>Void</td>
<td>24</td>
</tr>
<tr>
<td>9</td>
<td>Security Architectures for IPTV</td>
<td>24</td>
</tr>
<tr>
<td>9.1</td>
<td>Content Protection</td>
<td>24</td>
</tr>
<tr>
<td>9.1.2</td>
<td>Reference Points</td>
<td>25</td>
</tr>
<tr>
<td>9.1.2.1</td>
<td>LIF – UE (s-cp-1)</td>
<td>26</td>
</tr>
<tr>
<td>9.1.2.2</td>
<td>KMF – LIF (s-cp-2)</td>
<td>26</td>
</tr>
<tr>
<td>9.1.2.2</td>
<td>KMF – CEF (s-cp-3)</td>
<td>26</td>
</tr>
<tr>
<td>9.1.2.3</td>
<td>CEF – MDF (s-cp-4)</td>
<td>26</td>
</tr>
<tr>
<td>9.2</td>
<td>Service Protection</td>
<td>26</td>
</tr>
<tr>
<td>9.3</td>
<td>Optional solutions</td>
<td>26</td>
</tr>
<tr>
<td>9.3.1</td>
<td>Any Content Protection</td>
<td>27</td>
</tr>
<tr>
<td>9.3.1.1</td>
<td>Reference Points</td>
<td>27</td>
</tr>
<tr>
<td>9.3.1.2</td>
<td>Procedures</td>
<td>27</td>
</tr>
<tr>
<td>9.3.1.2.1</td>
<td>Content Preparation</td>
<td>27</td>
</tr>
<tr>
<td>9.3.1.2.2</td>
<td>Content Delivery</td>
<td>27</td>
</tr>
<tr>
<td>9.3.2</td>
<td>OMA BCAST</td>
<td>28</td>
</tr>
<tr>
<td>9.3.2.1</td>
<td>OMA BCAST Functional Architecture</td>
<td>28</td>
</tr>
<tr>
<td>9.3.2.2</td>
<td>Mapping between TISPAN IPTV Architecture and OMA BCAST Service Protection Functional Architecture</td>
<td>29</td>
</tr>
<tr>
<td>9.3.2.3</td>
<td>Mapping between TISPAN IPTV Service Protection based on 4-layer Key Hierarchy and OMA BCAST Service Protection Functional Architecture</td>
<td>30</td>
</tr>
<tr>
<td>9.3.2.4</td>
<td>OMA BCAST Smart Card Profile adaptation to MPEG-2 TS</td>
<td>31</td>
</tr>
<tr>
<td>9.3.2.4.1</td>
<td>STKM Transport in MPEG-2 TS</td>
<td>32</td>
</tr>
<tr>
<td>9.3.2.4.1</td>
<td>STKM and MPEG-2 TS encryption</td>
<td>34</td>
</tr>
</tbody>
</table>
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/PR/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 stage 2 model for the security architecture of NGN that supports the services required to satisfy the requirements identified in TS 187 001 in accordance with the risk assessment described in TR 187 002.

The present document defines the stage 3 implementation of the stage 2 services using existing mechanisms defined by the IETF and 3GPP.

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".


[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”.


[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)”.


[29] void


[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)”.


[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”.

ETSI
[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 24: "Universal Mobile Telecommunications System (UMTS); 3G security; Wireless Local Area Network (WLAN) interworking security”.


[49] 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”


[51] OMA-AD-BCAST-v1_0: “Open Mobile Alliance: “Mobile Broadcast Services Architecture”

[52] OMA-TS-BCAST_SvcCntProtection – v1_0: “Service and Content Protection for Mobile Broadcast Services”, version 1.0, Open Mobile Alliance

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

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


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”.
3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document the terms and definitions in X.811 [31], X.812 [32], X.814 [33], X.815 [34] and ISO/IEC 11770-1 [28] and following apply:

**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

**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
- **BDS** Broadcast Distribution Service
- **BSD/A** BCAST Service Distribution/Application
- **BGCF** Breakout Gateway Control Function
- **BSF** Bootstrapping Server Functionality
- **BSM** BCAST Subscription Management
- **CA** Certification Authority
- **CA-PID** Conditional Access-Packet Identifier
- **CAS** Conditional Access System
- **C-BGF** Core Border Gateway Function
- **CEF** Content Encryption Function
- **CLF** Connectivity session and repository Location Function
- **CND** Customer Network Device
- **CNG** Customer Network Gateway
- **CONF** CONFidentiality service
- **CPE** Customer Premises Equipment
- **CPN** Customer Premises Network
- **CSCF** Call Session Control Function
- **DoS** Denial-of-Service
- **DRM** Digital Rights Management
- **ESP** Encapsulating Security Protocol
- **ECM** Entitlement Control Message
- **EMM** Entitle Management Message
- **FE** Functional Entity
- **FFS** For Further Study
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FA</td>
<td>File Application Component</td>
</tr>
<tr>
<td>FD</td>
<td>File Delivery Component</td>
</tr>
<tr>
<td>GAA</td>
<td>Generic Authentication Architecture</td>
</tr>
<tr>
<td>GBA</td>
<td>Generic Bootstrapping Architecture</td>
</tr>
<tr>
<td>GE</td>
<td>Generic Entities</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation</td>
</tr>
<tr>
<td>HLR</td>
<td>Home Location Register</td>
</tr>
<tr>
<td>HSS</td>
<td>Home Subscriber Server</td>
</tr>
<tr>
<td>HTTP</td>
<td>HyperText Transport Protocol</td>
</tr>
<tr>
<td>IBCF</td>
<td>Interconnection Border Control Function</td>
</tr>
<tr>
<td>I-BGF</td>
<td>Interconnection Border Gateway Function</td>
</tr>
<tr>
<td>I-CSCF</td>
<td>Interrogating Call Session Control Function</td>
</tr>
<tr>
<td>ID</td>
<td>IDentity</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IF</td>
<td>InterFace</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange</td>
</tr>
<tr>
<td>IMPI</td>
<td>IMS Private User ID</td>
</tr>
<tr>
<td>IMPU</td>
<td>IMS Public User ID</td>
</tr>
<tr>
<td>IMS</td>
<td>IP Multimedia Subsystem</td>
</tr>
<tr>
<td>INT</td>
<td>INTegrity service</td>
</tr>
<tr>
<td>INTF</td>
<td>INTegrity Function</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol security</td>
</tr>
<tr>
<td>IPTV</td>
<td>Internet Protocol TeleVision</td>
</tr>
<tr>
<td>IRG</td>
<td>IMS Residential Gateway</td>
</tr>
<tr>
<td>ISIM</td>
<td>IMS Subscriber Identity Module</td>
</tr>
<tr>
<td>ISUP</td>
<td>ISDN User Part</td>
</tr>
<tr>
<td>IUA</td>
<td>ISDN Q.921-User Adaptation</td>
</tr>
<tr>
<td>KM</td>
<td>Key Management service</td>
</tr>
<tr>
<td>KMF</td>
<td>Key Management Function</td>
</tr>
<tr>
<td>LIF</td>
<td>Licensing Issuing Function</td>
</tr>
<tr>
<td>LTKM</td>
<td>Long Term Key Message</td>
</tr>
<tr>
<td>MAA</td>
<td>Multimedia Auth Answer</td>
</tr>
<tr>
<td>MDF</td>
<td>Media Delivery Function</td>
</tr>
<tr>
<td>ME</td>
<td>Mobile Equipment</td>
</tr>
<tr>
<td>MGC</td>
<td>Media Gateway Controller</td>
</tr>
<tr>
<td>MGCF</td>
<td>Media Gateway Control Function</td>
</tr>
<tr>
<td>MRF</td>
<td>Multimedia Resource Function Controller</td>
</tr>
<tr>
<td>MRFP</td>
<td>Multimedia Resource Function Processor</td>
</tr>
<tr>
<td>n.a.</td>
<td>not applicable</td>
</tr>
<tr>
<td>NACF</td>
<td>Network Access Configuration Function</td>
</tr>
<tr>
<td>NAF</td>
<td>Network Application Function</td>
</tr>
<tr>
<td>NAPT</td>
<td>Network Address and Port Translation</td>
</tr>
<tr>
<td>NASS</td>
<td>Network Access SubSystem</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NBA</td>
<td>NASS Bundled Authentication</td>
</tr>
<tr>
<td>NDS</td>
<td>Network Domain Security</td>
</tr>
<tr>
<td>NE</td>
<td>Network Element</td>
</tr>
<tr>
<td>NGN NT</td>
<td>NGN Network Termination</td>
</tr>
<tr>
<td>NGN</td>
<td>Next Generation Network</td>
</tr>
<tr>
<td>OIR</td>
<td>Originating Identity Presentation</td>
</tr>
<tr>
<td>P-CSCF</td>
<td>Proxy Call Session Control Function</td>
</tr>
<tr>
<td>PDBF</td>
<td>Profile DataBase Function</td>
</tr>
<tr>
<td>PEF</td>
<td>Policy Enforcement Function</td>
</tr>
<tr>
<td>PEK</td>
<td>Programme Encryption Key</td>
</tr>
<tr>
<td>PES</td>
<td>PSTN/ISDN Emulation</td>
</tr>
<tr>
<td>PID</td>
<td>Packet Identifier</td>
</tr>
<tr>
<td>PMT</td>
<td>Programme Map table</td>
</tr>
<tr>
<td>PS</td>
<td>Packet Switched</td>
</tr>
<tr>
<td>RACS</td>
<td>Resource Admission Control Subsystem</td>
</tr>
<tr>
<td>RAND</td>
<td>RANDom</td>
</tr>
<tr>
<td>RGW</td>
<td>Residential GateWay</td>
</tr>
</tbody>
</table>
4 NGN Security services

4.1 Summary

The NGN shall provide the following suite of security services:

- Identification and authentication;
- Message Integrity:
  - Provision;
  - Validation.
• Confidentiality of communications;
• Confidentiality of signalling.

The NGN shall offer the following security management services:

• Symmetric key distribution
  - To individuals for end to middle symmetric services
  - To groups for end to middle symmetric services
  - To individuals and groups for broadcast services
• Public key distribution and validation
• Public key revocation

The NGN shall offer the following composite security services:

• Consent framework for processing of private data;
• Framework to provide resilience in the NGN.

The stage 2 design for NGN security extends the stakeholder driven requirements model defined in TS 187 001 [1] and identifies security mechanisms, security services, and security policies to provide an overall model for NGN security.

Figure 1: Simple ontological model of security in the NGN

4.2 Mapping security services to requirements use cases

4.0 Overview

This clause provides an overview of the NGN security document.

The NGN security architecture is designed to support the requirements for NGN Security defined in TS 187 001 [1] that have been derived from the results of application of the ETSI Threat, Vulnerability and Risk Analysis (TVRA) method defined in TS 102 165-1 [i.7] and captured in TR 187 002 [49].
4.0a Security services identified in TS 187 001 and TR 187 002

TR 187 002 [49] has identified those threats and threat agents that when enacted against the NGN lead to a level of risk that has to be mitigated. TR 187 002 identifies the security services required to provide mitigation that are then documented as requirements to be met by the NGN in TS 187 001 [1]. Table 1 summarises the services identified in each of TR 187 002 and TS 187 001. The services are implemented using the framework defined in TS 102 165-2 [54].

Table 1: Summary of security services identified in TR 187 002 and TS 187 001

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>T-8</td>
<td>PES: Attack potential for denial-of-service on publicly addressable interfaces</td>
<td>R-AD-1, R-AD-3</td>
<td>Availability</td>
</tr>
<tr>
<td>T-16</td>
<td>NASS-IMS bundled: IP Spoofing</td>
<td>R-AA-24, R-AA-13, R-NF-2</td>
<td>Authentication</td>
</tr>
<tr>
<td>T-11</td>
<td>NASS-IMS bundled: Interception at the customer interface, air interface present</td>
<td>R-CD-18</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>T-14</td>
<td>NASS-IMS bundled: Attack potential for manipulation at the customer interface, air interface present</td>
<td>R-CD-13</td>
<td>Integrity</td>
</tr>
<tr>
<td>T-18</td>
<td>NASS-IMS bundled: Attack potential for manipulation at the customer interface (denial-of-service)</td>
<td>R-AD-1</td>
<td>Availability</td>
</tr>
<tr>
<td>T-19</td>
<td>NASS-IMS bundled: &quot;line-id poisoning&quot; attack</td>
<td>R-AA-24, R-AA-13, R-NF-2</td>
<td>Authentication</td>
</tr>
<tr>
<td>T-5</td>
<td>PES: Attack potential for manipulation between networks (without SEG)</td>
<td>R-CD-2</td>
<td>Integrity</td>
</tr>
<tr>
<td>T-1</td>
<td>PES: Attack potential for interception at the customer interface</td>
<td>R-CD-15, R-CD-16</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>T-3</td>
<td>PES: Attack potential for manipulation at the customer interface</td>
<td>R-CD-13</td>
<td>Integrity</td>
</tr>
<tr>
<td>T-10</td>
<td>NASS-IMS bundled: Attack potential for interception at the customer interface, no air interface</td>
<td>R-CD-20</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>T-13</td>
<td>NASS-IMS bundled: Attack potential for manipulation at the customer interface, No air</td>
<td>R-CD-15</td>
<td>Integrity</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------</td>
<td>-------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>T-9</td>
<td>PES: Attack potential for denial-of-service on non-publicly addressable interfaces</td>
<td>R-AD-3</td>
<td>Availability</td>
</tr>
<tr>
<td>T-4</td>
<td>PES: Attack potential for manipulation in the fixed network</td>
<td>R-CD-16</td>
<td>Integrity</td>
</tr>
<tr>
<td>T-7</td>
<td>PES: Attack potential for manipulation between networks (with SEG)</td>
<td>R-CD-16</td>
<td>Integrity</td>
</tr>
<tr>
<td>T-12</td>
<td>NASS-IMS bundled: Attack potential for interception at the customer interface (e1 IF)</td>
<td>R-CD-8</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>T-2</td>
<td>PES: Attack potential for interception at the customer interface</td>
<td>R-CD-19</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>T-15</td>
<td>NASS-IMS bundled: Attack potential for manipulation at the customer interface (e1 IF)</td>
<td>R-CD-15</td>
<td>Integrity</td>
</tr>
<tr>
<td>T-17</td>
<td>NASS-IMS bundled: Invalidation of IP address not signalled</td>
<td>R-CD-13 R-CD-8</td>
<td>Authentication</td>
</tr>
</tbody>
</table>

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

### 4.1 NGN security architecture

The NGN security architecture extends the abstract security architecture defined in clause 4 of TS 102 165-2 [54] (see Figure 2) and provides the mappings shown in Table 2. In addition the security architecture overlays the core NGN architecture defined in ES 282 001 [2].

![Diagram](image)

**Figure 2: Abstract architecture for security countermeasure application**
NOTE: As considered in TR 187 002 [49] the e1 reference point does not terminate in NASS.

NOTE 2: As considered in TR 187 002 [49] the e3 reference point is a management reference point only and only exists when the UE is a CNG, and has no bearing on the communications architecture.

NOTE 3: As considered in TR 187 002 [49] Ut is an application layer reference point.

NOTE 4: The Gm reference point between the UE and the IMS service platform is not shown.

NOTE 5: The Dj reference point is a media point and is used to carry RTP and RTCP data only.

Figure 3: UE reference points from ES 282 001 [2]
Table 2: Mapping from TS 102 165-2 abstract reference points to NGN architecture

<table>
<thead>
<tr>
<th>Abstract reference point (from TS 102 165-2 [54])</th>
<th>NGN reference point</th>
<th>Security service building block defined</th>
<th>Authentication principal</th>
<th>Location of security association definition</th>
<th>SEGF applies at Za (TS 133 210 [8]) (see note 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TpoA e1</td>
<td>Authentication</td>
<td>Confidentiality</td>
<td>Network Access Identifier (NAI)</td>
<td>IEEE 802.1x as defined in TS 183 019 [20] (Note 1)</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>Integrity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>Key management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dji</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Z</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ST</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SpoA Gm</td>
<td>Authentication</td>
<td>Confidentiality</td>
<td>IMSI, IMPU</td>
<td>TS 133 203 [7] (Note 2)</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>Integrity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>Key management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ApoA Ut</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>T2TpoA e5</td>
<td>Authentication</td>
<td>Confidentiality</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>Integrity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>Key management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S2SpoA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>A2ASpoA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>A2SpoA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>S2TpoA e2</td>
<td>Authentication</td>
<td>Confidentiality</td>
<td>TS 283 035 [21]</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>Integrity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>Key management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gq'</td>
<td>Authentication</td>
<td>Confidentiality</td>
<td>TS 183 017 [35]</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>Integrity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>Key management</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

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

- a1, a2, a3, a4 and thus are assumed to be in the security domain of the transport domain.
The following reference points are wholly within the service domain and are not exposed:

The NGN architecture is described by the following elements:

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

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

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

- Transport instantiated in the NASS security plane;
- Service instantiated in the IMS security plane;
- Application instantiated in the GAA/GBA key management plane.
NOTE 1: The terminology of V-UUAF and H-UAAF is not consistent with that used in the NASS stage 2 document ES 282 004 [5] where the terms UAAF Proxy and UAAF Server are used.

NOTE 2: The interface Zb between BSF and UPSF is defined in 3GPP but not endorsed in TISPAN NGN.

NOTE 3: No functional decomposition of UPSF, PDPF and HSS has been carried out therefore any sharing of functionality between these elements is not considered in the current version of the document.

NOTE 4: In the IMS the HSS and UPSF functions overlap.

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

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

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

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

NOTE 1: In the NGN, an IMS subscriber may register over an IP access session established by a NASS subscriber, which may not be the same as the IMS subscriber. In such cases there is no relation between the profile/credentials used at the NASS level and at the IMS level.

NOTE 2: The PDBF may be co-located with the UPSF.

NOTE 3: The dashed lines between H-UAAF and PDBF and between the NAS/AS and the UPSF indicate interfaces which are not defined in the present document.

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

NOTE: The TISPAN Application Server (AS) could have access to BSF as described in TS 133 220 [11] in which case UPSF takes the role of the HSS and has a connection to the BSF through reference points Zn and Zh.

4.2 Security domains

The following security domains are defined for the NGN:

- **Customer domain**
  - This domain includes the UE which may be either a single terminating device or a customer premises access point such as that defined in TS 185 003 [48] as a Customer Network Gateway (CNG) hosting one or more Customer Network Devices (CND) in the context of a Customer Premises Network. This may also include a corporate network defined as Next Generation Corporate Network (NGCN) defined in …

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

NOTE 2: The NGN IMS Residential Gateway as specified for Release 1 in TS 187 003 [47] has been further elaborated as part of the functionality of the CNG as specified in TS 185 003 [48].

- **Access network security domain**
  - with FEs hosted by the access network provider.

- **Visited NGN security domain**
  - with FEs hosted by a visited network provider where the visited network may provide access to some application services (AF). The visited network provider may host some applications and may own an
own database of subscribers. Alternatively, or additionally, the visited network provider may outsource some application services to the home network provider or even to a 3rd application provider.

- **Home NGN security domain**
  - with FEs hosted by the home network provider where the home network may provide some application services (AF). The home network provider hosts some applications and owns a database of subscribers.

- **3rd party application network security domain**
  - with FEs hosted by the ASP where the ASP provides some application services (AF). The ASP may be a separate service provider from the visited or the home network provider. The ASP may need to deploy authorization information offered by the visited or home network provider.

Figure 3 shows the partitioning of the NGN network into security domains.

![Figure 3: NGN security domains](image)

**NOTE:** Although Figure 3 shows the Next Generation Access and the Visited NGN as separate entities, they may, in practice, be co-located.

### 4.5 PES Security Architecture

#### 4.5.1 Security for H.248 within PES

### 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.
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:
- 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 $K_s$.
- 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, $K_s_{NAF}$, is derived in the ME using $K_s$.
- 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 $K_s$, does not leave the UICC. GBA-aware UICC may generate two keys from $K_s$, called $K_{int_{NAF}}$ and $K_{ext_{NAF}}$ (i.e. $K_{ext/int_{NAF}}$). $K_{int_{NAF}}$ is used by the UICC while $K_{ext_{NAF}}$ 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.
4.6.2 HTTP Digest authentication for UICC-less CNDs

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

HTTP Digest authentication, as defined in RFC2617 [36], permits the authentication of a user or CND at application layer.

RFC2617 describes an open framework with different options to be implemented (e.g. single-way vs. mutual authentication, partial integrity protection, and others). According to the local policy, the operator may define different mapping credentials and different ways for the provisioning of the customer credentials to the CND and Application Server. The selection of the proper credentials at running time is performed by means of the “realm” mechanism.

To simplify the provisioning, the Service Access Authentication (SAA) element enables the usage of the user credentials stored in the UPSF also at application layer. The following picture (12a) shows the integration of the SAA in the NGN with the main reference points involved.

![Figure 12a: HTTP digest authentication for UICC-less CNDs](image)

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

This specification identifies the protocols applicable for the following reference points:

- **Au**: HTTP Digest authentication as specified in RFC 2617 [36]. The actual implementation details depend on the local policy of the Operator. The authentication flow can be protected by means of TLS (i.e. HTTPS).
- **Cx (Diameter)**: Cx subset, in order to support the authentication (i.e. the 3GPP TS 29.228 [6] for digest authentication). The SAA behaves like a S-CSCF as defined in 3GPP TS 29.228 [6] clause 6.3. In particular the SAA requests, for each authenticating users, the H(A1) value that is a hash (i.e. MD5) of the username (e.g. IMPI), realm, and the secret shared between the NGN and the customer. The communication between SAA and UPSF via Cx shall follow the rules of Network Domain Security as specified in TS 33.210 [8]. If multiple UPSF
exist in the network, SLF is used to select the appropriate instance as specified in ES 282 001 clause 6.5.2 [2]. For simplification SLF is not represented on the figure.

- As: The communication between SAA and AS via As shall follow the rules of Network Domain Security as specified in TS 33.210 [8].

Security requirements described in clause 4 are identified by a symbolic security requirement identifier (e.g. R-SP-n) for quick reference and along with some textual description. The security requirements are listed without any implied preference or priority. It is pointed out that not all security requirements are mutually exclusive, but there is indeed some unavoidable overlap among them.

ISIM shall be hosted on a UICC. Use of the ISIM on UICC is the preferred solution for achieving the security requirements to access the NGN IMS features. The ISIM may reside within the device itself, or be accessed remotely, via a local interface to the "device holding the UICC".

4.1 Security Policy Requirements

A security policy defines the legitimate users of a system and what they are allowed to do. It states what information must be protected from which threats. In environments with heterogeneous user communities, multiple vendors' equipment, differing threat models, and uneven deployment of security functionality, assurance that security is functioning correctly is extremely difficult without enforceable policies.

(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.

(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.

(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.

(R-SP-5) The UE and the P-CSCF shall negotiate the integrity algorithm that shall be used for the session.

(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.

(R-SP-7) The security gateway functions (SEGF) shall be responsible for enforcing security policies for the interworking between networks.

NOTE: The actual inter-security domain policy is not standardized and is left to the discretion of the roaming agreements of the operators.

(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.

4.2 Authentication, Authorization, Access Control and Accountability Requirements

General Access authentication

(R-AA-1) Access to NGN networks, services, and applications shall be provided for authorized users only.
NGN IMS authentication shall support early deployment scenarios, although it is optional for operators to deploy such scenarios.

In non-early deployment scenarios, IMS authentication shall be independent from access authentication.

An ISIM shall be used to access any IMS service, however, exceptions may be allowed for emergency calls and early deployment scenarios.

ISIM based Authentication between the IMS-subscriber and the network shall comply to the authentication part of Access Security for IP-based services TS 133 203 [2].

ISIM based Re-authentication of an IMS-subscriber shall comply to the authentication part of Access Security for IP-based services TS 133 203 [2].

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.

NGN relevant ISIM specific information shall be protected against unauthorized access or alteration.

User authentication may either be hardware-based (for 3GPP UE: ISIM on UICC; i.e. proof by possession of a physical token) or be software-based (i.e. proof by knowledge of some secret information).

User Authentication to the NGN IMS using SIP Digest mechanisms shall be supported as an early deployment scenario.

Where more than one authentication mechanism are deployed by an NGN IMS operator, that operator shall determine the authentication mechanism (e.g. SIP Digest or ISIM-based) on a per-device 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. Where a terminal supports the ISIM solution and the network operator supports both ISIM and early deployment solutions, ISIM solution shall be used.

Transmitted passwords shall be sufficiently protected; e.g. by encryption or other techniques.

For the special early deployment scenarios (see note 1), 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.

NOTE 1: 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 2: 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.

The NGN subsystems shall be able to be able to define and enforce policy with respect to validity of user authorization.

Mutual authentication shall be supported between the UE and the AS before providing authorization.

It should also be possible to support an Authentication Proxy based architecture.
NOTE 1: The purpose of the AP is to separate the authentication procedure and the AS specific application logic to different logical entities.

(R-AA-17) Mutual authentication shall be supported between the UE and the AP.

(R-AA-18) The AP shall decide whether a particular subscriber (i.e. the UE), is authorized to access a particular AS.

(R-AA-19) If an AP is used, the AS shall only authorize the access request to the requested resource.

NOTE 2: The AS does not need to explicitly authenticate the user.

NASS

(R-AA-20) Mutual authentication should be supported between the CPE and the NASS during access network level registration.

(R-AA-21) The access network shall be able to authenticate and authorize the access subscriber.

(R-AA-22) Authentication and authorization to the Access Network is controlled by the operator of the Access Network.

(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.

(R-AA-24) NASS shall support both the use explicit (e.g. PPP or IEEE 802.1x [1,2]) 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.

(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.

(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.

RACS

(R-AA-27) RACS and AF shall be mutually authenticated prior to resource authorization.

(R-AA-27A) AF and SPDF in RACS shall be able to mutually identify each other when performing the authentication.

CPN - RACS

(R-AA-28) RACS and CPN shall be mutually authenticated prior to resource authorization.

NOTE: For emergency services alternative procedures are required.

Other Specific Requirements

(R-AA-27.1) 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.

(R-AA-28.2) Authentication of NGN users and authentication of NGN terminals shall be separate.

(R-AA-29) 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.
4.3 Identity and Secure Registration Requirements

The following requirements aim to mitigate against masquerading, spoofing, and impersonation of NGN terminals, devices/systems (HW/SW) and users. The requirements aim to provide measures against identity theft, misuse/authorized use of NGN services/applications.

(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).

(R-IR-2) An access identity shall be used for access authentication. This identity may or may not be used for other purposes.

(R-IR-3) The line ID shall be possible to use for line authentication.

4.4 Communications and Data Security Requirements

Clause 4.4 contains such requirements that address communications and data security. Data, in this context, can mean either user data (e.g. voice, video, text stream) or management data.

4.4.1 General Communications and Data Security Requirements

General

(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).

NDS

(R-CD-2) Network Domain Security (NDS) shall be provided at the network layer and comply to TS 133 210 [3].

(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 [3].

(R-CD-4) Security shall be provided within the network domain for the Cx interface.

Access Security

(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.

(R-CD-6) Secure link shall be provided between UE and the P-CSCF for protection of the Gm reference point.

(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.

(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.
(R-CD- 9) ISIM specific information shall be updated in a secure manner.

Ut

(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).

RACS

Other Specific Requirements

(R-CD- 12) All data related to configuring the UE through the e3 reference point shall be protected against loss of confidentiality and against loss of integrity.

4.4.2 Integrity and Replay Protection Requirements

General

(R-CD- 13) Integrity protection of signalling, control communications and of stored data shall be provided.

(R-CD- 14) It shall be possible to ensure the origin, integrity and freshness of authentication data, particularly of the cipher key.

Access Security

(R-CD- 15) Integrity protection shall be applied between the UE and the P-CSCF for protecting the SIP signalling.

NDS

(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 [3].

Ut

(R-CD- 17) Data integrity shall be supported between the UE and the Application Server.

RACS

(R-CD- 18.1) RACS shall ensure integrity of all information exchanged over the e4 reference point.

RACS - CPN

(R-CD- 19.2) RACS shall ensure integrity of all policy related resource information exchanged between CPN and RACS.

NOTE: This requires that RACS is the validator of the integrity of the data exchanged, and that CPN is the generator of the integrity check data.

4.4.3 Confidentiality Requirements

General

(R-CD- 20) Confidentiality of communications should be achieved by cryptographic encryption. Confidentiality of stored data shall be achieved by cryptographic encryption or by access controls.

(R-CD- 21) 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.
**Access Security**

(R-CD-22) IMS specific confidentiality protection shall be provided for the SIP signalling between UE and P-CSCF.

(R-CD-20.1) There shall be means to enable confidentiality protection on all communication over interface e5.

(R-CD-20.2) There shall be means to enable confidentiality protection of all information exchanged over interface e2.

**NDS**

(R-CD-23) 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 [3].

**Other Specific Requirements**

(R-CD-24) It shall be possible to protect the confidentiality of user-related data which is stored or processed by a provider.

**CPN - RACS**

(R-CD-23) RACS shall ensure confidentiality of all policy related resource information exchanged between CPN and RACS.

### 4.5 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 domains to define and implement protection against traffic analysis for signalling and management protocols.

(R-P-2) User location and usage patterns shall be kept from unwanted disclosure.

(R-P-3) It shall be possible to protect the confidentiality of user identity data.

(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.

(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.

(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.

(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).

(R-P-8) The NGN shall provide mechanisms that allow to present the identity of the session originator, if this is not restricted by the session originator.

(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).

(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.
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.

It shall be possible for the sender of the message to request to hide its public ID from the recipient.

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.

It shall be possible to protect the CPN topology from exposure toward the NGN.

The CPN transmitting information to the RACS shall not disclose CPN internal (private or other critical) information to the RACS.

### 4.6 Key Management Requirements

- **(R-KM- 1)** Key management and key distribution between SEGFs shall comply to the Network Domain Security TS 133 210 [3].
- **(R-KM- 2)** The UE and the AS shall be able to resume a previously established secure session.
- **(R-KM- 3)** The key management mechanism must be able to traverse a NAT/NATP device.

### 4.7 Secure Management Requirements

**NOTE:** Security Management requirements are for further study.

### 4.8 NAT/Firewall Interworking Requirements

Firewall is here understood in a generic sense. A firewall could be an Application-Level Gateway (ALG), a proxy, a packet-filter, a NAT/NATP device or a combination of all of those. A Security Gateway Function is an entity on the border of the IP security domain and is used to secure native IP based protocols over the Za interfaces.

- **(R-NF- 1)** NGN security protocols shall work with commonly-used firewalls and shall work in environments with NAT/NATP.
- **(R-NF- 2)** Filters to screen the IP packets to restrict/grant access to specific bearer streams shall be supported.
- **(R-NF- 3)** The SEGFs may include filtering policies and firewall functionality not required in TS 133 210 [3].

### 4.9 Non-Repudiation Requirements

**NOTE:** Non-repudiation requirements are for further study.

### 4.10 Availability and DoS protection Requirements

- **(R-AD- 1)** Mechanisms shall be provided to mitigate denial-of-service attacks.
- **(R-AD- 2)** Provide access control mechanisms to ensure that authorized users only can access the service.
- **(R-AD- 3)** It shall be possible to prevent intruders from restricting the availability of services by logical means.
- **(R-AD- 4)** Availability of and accuracy of location information shall be provided for the EMTEL services.
- **(R-AD- 5)** Availability of EMTEL PSAPs shall not be decreased by DoS attacks. EMTEL PSAPs shall be able to reconnect.
4.11 Assurance Requirements

(R-AS-1) The TISPAN NGN shall provide guidance for evaluating and certifying NGN equipment and systems.

(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.

4.12 Requirements on Strength of Security Mechanisms

The guidelines defined in EG 202 238 [i.12] shall be followed when defining or selecting cryptographic algorithms in TISPAN.

4.13 IPTV Security Requirements

4.13.1 Common IPTV Security Requirements

NOTE: When delivering the security information (e.g. the licenses or keys) to the subscribers (especially large amount of subscribers), the impact to system performance should be taken into account.

(R-IPTV-C-1) The NGN IPTV service shall allow several kinds of users, named groups of users, entities acting on behalf of users and entities acting on behalf of named groups of users.

(R-IPTV-C-2) The NGN IPTV service shall assign unique and non-forgeable user identities to users.

(R-IPTV-C-3) The NGN IPTV service shall allow several (number to be decided) users to be associated with one subscription.

(R-IPTV-C-4) The NGN IPTV service shall uniquely authenticate all users to the IPTV service using unique and non-forgeable authentication credentials on a subscription basis.

(R-IPTV-C-5) The NGN IPTV service shall uniquely authorize all users to the IPTV service on a subscription basis.

(R-IPTV-C-6) The NGN IPTV service shall assign unique and non-forgeable identities to all subscribers and named groups of subscribers.

(R-IPTV-C-7) The NGN IPTV service shall uniquely authenticate all subscribers and named groups of subscribers to the IPTV service using unique authentication credentials.

(R-IPTV-C-8) The NGN IPTV service shall uniquely authorize all subscribers and named groups of subscribers to the IPTV service.

(R-IPTV-C-9) The NGN IPTV service shall assign unique and non-forgeable identities to all user devices.

(R-IPTV-C-10) The NGN IPTV service shall uniquely authorize all devices to the IPTV service.

(R-IPTV-C-11) The NGN IPTV service shall assign unique and non-forgeable identities to all IPTV sessions that are verifiable to users and devices.

(R-IPTV-C-12) The NGN IPTV service shall assign unique and non-forgeable identities to all IPTV service providers that are verifiable to users.

(R-IPTV-C-13) The NGN IPTV service shall provide a mechanism to authenticate and authorize the RTSP control messages from users.

(R-IPTV-C-14) The NGN IPTV service shall assign unique and non-forgeable identities to all IPTV content that are verifiable for users.
4.13.2 IPTV Service Protection Requirements

(R-IPTV-CN-1) The NGN IPTV service protection functions shall support distribution of access keys coming from the network according to the corresponding rights.

(R-IPTV-CN-2) The NGN IPTV service protection functions shall support means to protect the service-associated keys against unauthorized access, and ensure their integrity and confidentiality.

(R-IPTV-CN-3) The NGN IPTV service protection functions shall be able to authenticate and ensure the integrity and confidentiality of communication between the service and the user.

(R-IPTV-CN-4) The NGN IPTV service protection functions shall provide a means for protecting time-restricted services (e.g. subscription and pay-per-view).

(R-IPTV-CN-5) The NGN IPTV service protection functions shall provide an open framework allowing the operator to choose one or more protection solution.

(R-IPTV-CN-6) The NGN IPTV service protection functions applied on a service providing access to IPTV content shall not make any constraint on the way the content is protected.

(R-IPTV-CN-7) The NGN IPTV service protection functions applied on a service providing access to IPTV content should interoperate with Content Protection solutions.

4.13.3 IPTV Content Protection Requirements

(R-IPTV-CP-1) The NGN IPTV content protection shall authenticate and authorize the origin of all IPTV content to the receiving users.

(R-IPTV-CP-2) The NGN IPTV content protection shall verify the authenticity of the origin of all IPTV content to the receiving users.

(R-IPTV-CP-3) The NGN IPTV content protection shall provide end-to-end content confidentiality protection within regulatory constrains.

(R-IPTV-CP-4) The NGN IPTV service should provide end-to-end content integrity protection for an IPTV session.

(R-IPTV-CP-5) The NGN IPTV service shall control and restrict content on a content metadata basis for users.

(R-IPTV-CP-6) The NGN IPTV service and content protection functions shall provide the means for retrieving related rights and/or keys for chosen protected content items.

(R-IPTV-CP-7) The NGN IPTV service shall have a measure to restrict unauthorized usage of content (viewing, re-viewing, copying, etc.) for users.

(R-IPTV-CP-8) The NGN IPTV service shall have a measure to restrict unauthorized distribution of content for users.

(R-IPTV-CP-9) The NGN IPTV content protection functions shall provide a means for protecting time-restricted content usage.

(R-IPTV-CP-10) The NGN IPTV content protection functions shall provide an open framework allowing the operator to choose one or more protection solution.

4.13.4 IMS-based IPTV Security Requirements

NOTE: Reusing the existing IMS security mechanisms as much as possible should be taken into account.

4.13.5 Non-IMS-based IPTV Security Requirements

(R-IPTV-NIMS-1) The NGN IPTV service shall for each IPTV session uniquely link devices, users, named groups of users, entities acting on behalf of users to an IPTV session.
The NGN IPTV service shall for each combined IPTV session uniquely link devices, users to an IPTV session.

The NGN IPTV service shall assign unique identities to critical IPTV service logics on the devices that are verifiable for users.

The NGN IPTV service shall assign non-forgable identities to critical IPTV service logics on the devices that are verifiable for users.

The NGN IPTV service shall authenticate and authorize critical IPTV service logics on the devices to the receiving user.

The NGN IPTV service shall verify the authenticity of critical IPTV service logics on the devices to the receiving users.

Refinement of DSF9: The NGN IPTV service shall uniquely authenticate all subscribers and named groups of subscribers when accessing private or sensitive information using unique authentication credentials.

Refinement of DSF10: The NGN IPTV service shall uniquely authorize all subscribers and named groups of subscribers when accessing private or sensitive information.

The NGN IPTV service shall provide end-to-end encryption of private or sensitive information on an IPTV session basis.

4.13.6 Availability and DoS Protection Requirements

The NGN IPTV service shall be accessible to the authorized users, subscribers and devices according to the requirements of the IPTV service regarding timeliness and quality.

The NGN IPTV service shall have measures to prevent DoS attacks posed upon the IPTV service to ensure fulfilment of the requirements of the IPTV service regarding timeliness and quality.

The NGN IPTV service shall have measures to detect and act upon all DoS attacks posed upon the IPTV service (note that act might mean inform e.g. the system administrator of the event) to ensure fulfilment of the requirements of the IPTV service regarding timeliness and quality.

4.14 DRM

The NGN IPTV service shall provide a general framework open to the integration of content protection solutions (e.g. DRM).

One or more open fully standardized DRM solutions shall be supported with NGN IPTV content protection, including e.g. the key management, the delivery, and encryption and decryption operations of keys and content, and interfaces. All solutions shall be fully specified, permitting well-defined variations in operational behaviour without introducing proprietary elements to any part of the system. All such solutions shall have the same priority.

The fully standardized DRM solution shall fulfil the requirements as stated in clause 4.13.3 "IPTV Content Protection Requirements".

4.15 Media Security Requirements

4.15.1 Common Media Security Requirements

4.15.1.1 Regulatory Requirements

An NGN shall provide mechanisms to prevent eavesdropping of traffic.
An NGN shall provide mechanisms to prevent unauthorized recording and storage of traffic.

An NGN shall provide mechanisms to prevent unauthorized interception of traffic.

An NGN operator should provide mechanisms to ensure the interception and handover of signalling of specific NGN users if required to by a lawful authority.

NOTE 1: This requirement is not strictly related to media but may be correlated to media provision.

An NGN operator should provide mechanisms to ensure the interception and handover of the content of communication of specific NGN users if required to by a lawful authority.

NOTE 2: This requirement is not strictly related to media but may be correlated to media provision.

4.15.1.2 Non-broadcast media paths

An NGN should ensure that non-broadcast media paths are constructed such that eavesdropping cannot be achieved without intrusion to the media path.

An NGN should ensure that broadcast media paths (e.g. radio) should be protected by encryption of media content.

An NGN should ensure that the key used for encryption is only known to the parties directly involved in the transfer of media over the broadcast path.

4.15.1.3 NGN Requirements

The NGN shall not provide support for end-to-end media security.

The NGN shall provide support for user-to-network media security (for the following security services Confidentiality, Integrity, Authenticity of source and destination end-points).

The NGN shall provide support for secure media transfer in point-to-point topologies.

The NGN shall provide support for secure media transfer in point-to-multipoint topologies.

The NGN shall provide support for secure media transfer in broadcast topologies.

An NGN shall provide mechanisms to prevent eavesdropping of traffic.

An NGN shall provide mechanisms to prevent unauthorized recording and storage of traffic.

An NGN shall provide mechanisms to prevent unauthorized interception of traffic.

An NGN should ensure that non-broadcast media paths are constructed such that eavesdropping cannot be achieved without intrusion to the media path.

An NGN should ensure that broadcast media paths (e.g. radio) should be protected by encryption of media content.

An NGN should ensure that the key used for encryption is only known to the parties directly involved in the transfer of media over the broadcast path.

4.15.1.4 NGCN Requirements

The NGN shall provide support for secure media transfer between NGCNs and NGNs.

An NGCN should permit media to be secured (encrypted, authenticated and integrity protected) transparently end-to-end or end to PSTN/ISDN gateway, except where requested or authorized intervention in media occurs.
An NGCN should be transparent to key management for the purpose of media security to take place between the end devices (or end device to PSTN/ISDN gateway), with cryptographic evidence that the peer involved in key exchange or key agreement is the expected communication partner.

An NGCN should be transparent to the end-to-end encryption of any key exchange required for the purpose of media security.

4.16 Security Requirements to Counter Unsolicited Communications

(R-UC-1) The NGN shall provide a means for NGN-users to report calls as UC.
(R-UC-2) Reports of UC made by NGN-users shall be auditable by the NGN.
(R-UC-3) The NGN should provide the ability for an affected user to request the rating of an UC call.
(R-UC-4) The NGN should provide the ability for an affected user to challenge the ratings made by the UC detection system.
(R-UC-5) The NGN should provide the ability to the affected CSP to extract from the call signalling sufficient information to provide a UC rating for the call.
(R-UC-6) The NGN should provide a mechanism to convey the UC rating in the call signalling.
(R-UC-7) The NGN should provide a mechanism to allow variation in the call handling for calls with particular UC ratings.

4.18 NAT Traversal Security Requirements

(R-NAT TRAV-1) TISPAN NGN R2 NAT traversal shall support the traversal of the following type of NATs behaviour between the UE and the IMS Core Network:
- Endpoint Independent Mapping.
- Address Dependent Mapping.
- Address and Port Dependent Mapping.
(R-NAT TRAV-2) TISPAN NGN R2 NAT traversal shall support the following type of filtering behaviour between the UE and the IMS Core Network:
- Endpoint Independent Filtering.
- Address Independent Filtering.
- Address and Port Dependent Filtering.
(R-NAT TRAV-3) TISPAN NGN R2 NAT traversal shall support both inbound and outbound requests to and from UEs through one or more NAT device(s).
(R-NAT TRAV-4) TISPAN NGN R2 NAT traversal shall support uni-directional and bi-directional RTP traffic.
(R-NAT TRAV-5) TISPAN NGN R2 NAT traversal shall support TCP connections initiated externally and internally.
(R-NAT TRAV-6) TISPAN NGN R2 NAT traversal shall support residential networks.
(R-NAT TRAV-7) TISPAN NGN R2 NAT traversal shall support IPv4.
(R-NAT TRAV-8) TISPAN NGN R2 NAT traversal shall support IPv6.
(R-NAT TRAV-9) TISPAN NGN R2 NAT traversal shall support unicast traffic.
(R-NAT TRAV-10) TISPAN NGN R2 NAT traversal should minimize the number of messages that are transmitted solely for NAT traversal.

(R-NAT TRAV-11) TISPAN NGN R2 NAT traversal shall support multiple UEs (on one or more devices) behind a single NAT.

(R-NAT TRAV-12) TISPAN NGN R2 NAT traversal should minimize additional session setup delay.

(R-NAT TRAV-13) TISPAN NGN R2 NAT traversal shall support the traversal for IMS.

(R-NAT TRAV-14) TISPAN NGN R2 NAT traversal shall support SIP signalling encrypted with Ipsec.

(R-NAT TRAV-15) TISPAN NGN R2 NAT traversal shall take into account the scalability, complexity and compatibility with other relevant NGN requirements.

(R-NAT TRAV-16) Any solution recommended for NAT traversal shall not impact the inherent ability of TLS to operate across NAT.

4.19 Home Networking Security Requirements

The security attacks identified in the CPN TVRA that pose either a major or critical risk to the CNG, and thus the CPN, should be protected against by standard measures that operators and service providers of CNGs shall establish and apply a security policy for by default in deployed equipment.

NOTE: The following requirements are in addition to those applying to an NGN terminal.

4.19.1 Confidentiality requirements

(R-CPN-CR-1) For shared credentials and media on wireless connections between the CND and the CNG, the minimum confidentiality protocol shall be WPA2.

(R-CPN-CR-2) Internally to the CPN, a CNG transmitting private or other critical information (i.e. to a CND) shall protect the data from unauthorised disclosure.

(R-CPN-CR-3) Internally to the CPN, a CNG receiving private or other critical information (i.e. from a CND) should verify that the data was protected from unauthorised disclosure.

(R-CPN-CR-4) The CNG shall detect the end of the life of the key used for cryptographic protection of the wireless communication between the CND and the CNG.

4.19.2 Identification, authentication and authorization requirements

(R-CPN-IAAR-1) A CPN-user or external NGN user attempting to invoke a CNG-mediated service, including transparent routing, shall be identified and authenticated by the CNG before being granted access to the service.

(R-CPN-IAAR-2) The CNG shall implement an authentication failure handling policy.

(R-CPN-IAAR-3) The CNG shall take action according to local authentication failure handling policy (which may include silently discarding the authentication and explicit failure notification, or in the case of a replay of credentials may include notification of the true owner of the credentials) upon detection of failure during identification, authentication and authorization.

(R-CPN-IAAR-4) The CNG should detect replayed user and/or device credentials.

(R-CPN-IAAR-5) When the CNG detects replayed user and/or device credentials, the CNG shall stop the relevant processes.

(R-CPN-IAAR-6) The CNG shall implement a privacy protection policy specifying as a minimum private and critical information.

(R-CPN-IAAR-7) When the CNG detects violation of the privacy protection policy the CNG shall discard all signalling, including signalling from the NGN.
The CNG shall implement an authorization management handling policy.

NOTE: This could be used to allow the CNG and the CPN to support parental control related functionalities limiting the use of the broadband connection on a user or time basis. Limitations on a content basis may be shared with devoted network servers.

On reception at the CNG of a message to access configuration information for update and detection of authorization failure the CNG shall reject the request and manage the failure in accordance with the CPN authorization management handling policy.

Where a CND invokes a session at the CNG the CNG shall record the association of session-id, invoking device identity and invoking user-id.

4.19.3 Integrity requirements

On transmission of management information from the CNG to a CND the CNG shall append a timestamp or sequence number to the outgoing message.

On reception at the CNG of a message containing management information the CNG shall extract the timestamp or sequence number and verify that the message has not been replayed.

On reception at the CNG of a message to access or update configuration information the CNG shall allow access only if the sender is an administrator.

On detection of a message integrity error at the CNG the CNG shall discard the message.

On reception at the CNG of a message to access configuration information for update and detection of authorization failure the CNG shall reject the request and manage the failure in accordance with the CPN authorization management handling policy.

On indication received at the CNG of a resource allocation expiry the CNG shall delete all residual data associated with the invocation of the resource.

4.19.4 Availability and DoS protection requirements

On receipt of a valid (i.e. authorized) request for data stored in the CNG the CNG shall return the requested data to the requesting user.

On receipt of a valid (i.e. authorized) request for access to a CNG hosted service or application the CNG shall provide the requested service or application to the requesting user.

On detection of any system failure or discontinuity not specifically handled by other mechanisms the CNG shall revert to a known safe state.

4.19.5 Service protection and/or content protection software upgrade security requirements

Service protection and/or content protection software upgrade allows adaptation of a CND to the protection mechanisms used by a specific relevant stakeholder (in the secure SP and/or CP software upgrade IPTV model). As service protection and/or content protection is a pivotal element in the secure distribution of protected content, upgrading such part of the system needs to be protected against malicious parties trying to attack such upgrade procedure. The motivation for attackers may be diverse. Therefore the supporting software functions for the upgrade of CND’s service and content protection functions (CND-SPF and CND-CPF) need to comply with the following security requirements:

The CND’s software upgrade function shall offer means to proof the validity of the CND’s trusted environment for service protection and/or content protection software upgrade.

The CND shall authenticate the relevant stakeholder to verify if it is entitled to perform an service protection and/or content protection software upgrade.

During the upgrade, all security sensitive data (especially keys, passwords, credentials) shall be transported confidentiality and integrity protected between the CND and the relevant stakeholder.
Before new service protection and/or content protection software upgrades (e.g. the upgrade of software in the CND-SPF or software in the CND-CPF) are installed or activated their authenticity (proof of origin and data integrity) and their validity (e.g. credentials) shall be verified.

Handover of the CND from one relevant stakeholder to another shall be performed in a manner that only an entitled relevant stakeholder may initiate an upgrade of the CND service protection and/or content protection relevant software (the stakeholder must be authenticated by the CND and authorized to do this).

The CND-SPF and CND-CPF shall be implemented in a trusted execution environment. Such an environment shall be tamperproof and contain a secure storage environment for security sensitive information that these protection systems need to store and which shall not be revealed outside the CND.

NOTE: The specification of the implementation of the CND's trusted environment for service protection and/or content protection software upgrade and the secure storage environment is outside the scope of TISPAN.

The service protection and/or content protection system(s) in the relevant stakeholder domain shall be offered the possibility to authenticate the service protection and/or content protection software that is in operation in the CND as being authentic software provided by the service protection and/or content protection provider.

9 Security Architectures for IPTV

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

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

9.1 Content Protection

For content protection the following elementary functions are used:

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

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

NOTE: Some of these elementary functions may be executed on-line (in real-time) or off-line (in this case could be part of the management).
The content protection architecture illustrated above is based on the IPTV service architecture defined in TS 182 027 [i.3] and TS 182 028 [i.9].

9.1.2 Reference Points

Editor's note: this section describes the content protection reference points. Reference points that are not security specific can be referred to TS 182 027 [i.3] and TS 182 028 [i.9].

9.1.2.1 LIF – UE (s-cp-1)

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

9.1.2.2 KMF – LIF (s-cp-2)

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

9.1.2.2 KMF – CEF (s-cp-3)

This reference point between KMF and CEF is used for key exchange.
9.1.2.3 CEF – MDF (s-cp-4)

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

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

9.2 Service Protection

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

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

- Service membership elementary functions (SMF): This set of elementary functions handles the granting and revoking of service access rights to access the IPTV services. Metadata related to the service rights management are maintained by the SMF.
  
  NOTE: The SMF is handled in an array of existing elementary functions (e.g., service key triggering function) and functional entities. For example, service authorization may be provided by the SCF, and meta-data is maintained in the UPSF.

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

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

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

Editor's note: this section should be completed with functional architecture overview figure with these functions

9.3 Optional solutions

The following optional solutions are defined:

- Any Content Protection combined with existing NGN Security Architecture
- OMA BCAST as Service Protection

9.3.1 Any Content Protection

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

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

- User Authentication
- Service Authorisation based on user authentication
- Service Confidentiality
This section will describe the constraints which apply to a content protection solution in order to integrate with TISPAN IPTV Architecture.

9.3.1.1 Reference Points

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

9.3.1.2 Procedures

9.3.1.2.1 Content Preparation

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

Two main cases can be distinguished:

- For Live delivery: DVB-Simulcrypt [i.8] has defined a standard interface to integrate content protection solution to a TV head end. DVB-Simulcrypt architecture allows furthermore several content protection solutions to be integrated and used simultaneously on the same IPTV content.

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

9.3.1.2.2 Content Delivery

For IMS-based IPTV, as specified in TS 183 063 [i.10], a TISPAN UE shall support at least one of the following IPTV transport technologies:

- MPEG-2 TS encapsulation over UDP or RTP.
- Direct RTP transport.

For NGN integrated IPTV subsystem, as specified in TS 183 064 [i.11], a TISPAN UE shall be able to receive content encapsulated into MPEG-2 TS over RTP and MPEG-2 TS over UDP.

MDF shall send content compliant to these IPTV transport technologies.

As a consequence, TISPAN IPTV Architecture, when using MPEG-2 TS encapsulation, supports any content protection applied within MPEG-2 TS, in particular content protection compliant with ISO/IEC 13818 [50], ISO/IEC 13818 defines how to signal a content protection solution and transport content protection solution specific messaging information, i.e. ECM transporting Control Words / Transport Encryption Keys and EMM transporting Rights management messages in MPEG-2 TS.

Content protection solution applied on MPEG-2 TS and compliant to signalling and transport as defined in ISO/IEC 13818 [50] may be used in conjunction with the NGN security architecture as defined in clause 4.

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

9.3.1.2.3 Right and Key Delivery

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

Note: This interface is not always needed when content protection messaging is transported via MDF (for example when content protection messages (EMM) are transported in-band within MPEG2-TS streams as defined in [50]).
9.3.2 OMA BCAST

TISPAN IPTV Service Protection can be ensured by means of OMA BCAST as specified in [51] and [52].

OMA BCAST is a 4-layer model allowing two key management profiles: the Smartcard Profile and the DRM Profile. The SmartCard Profile (SCP) is a key management system based on symmetric key model. It uses either 3GPP MBMS security model relying on the (U)SIM on UICC or 3GPP BCMCS security model relying on R-UIM/CSIM. The DRM Profile is key management system based on the Public Key Infrastructure provided by OMA DRM v2.0.

TISPAN IPTV Service Protection can be ensured by means of the Smartcard Profile or the DRM Profile. In order to ensure maximum interoperability, OMA BCAST defines a common layer for traffic encryption and allows the other layers of key management to be implemented using either the SmartCard Profile or the DRM Profile.

OMA BCAST Subscription Management that support service or content protection shall support Interface SP-4. Interface SP-4 may support DVB Simulcrypt, allowing the deployment of several service protection solutions in parallel and that could be already deployed on the field. The description of DVB Simulcrypt support is described in clause of Service and Content Protection for Mobile Broadcast Services specification [52].

9.3.2.1 OMA BCAST Functional Architecture

The OMA BCAST logical entities are described in [51].

<table>
<thead>
<tr>
<th>Logical Entity</th>
<th>Major Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCAST Service Application</td>
<td>Represents the service application of the BCAST Service, such as, streaming audio/video or movie file download. It encompasses the functionality of media encoding and interaction related to the BCAST Service. It also provides the BCAST service attributes to the BCAST Service Distribution/Adaptation and BCAST Subscription Management. It may generate charging information, for example, according to the user charging information that it obtains from the BCAST subscription management and the content creator. Legacy mechanisms may be used for charging information generation and delivery.</td>
</tr>
<tr>
<td>BCAST Service Distribution/Adaptation</td>
<td>Responsible for the aggregation and delivery of BCAST Services, and performs the adaptation of the BCAST Enabler to underlying BCAST Distribution Systems. It provides the functionality of File and Stream Distribution, Service Aggregation, Service and Content Protection (i.e., data encryption, TEK generation, and protection key message distribution), Service Guide generation and delivery, Notification Delivery, and the adaptation to the underlying BDS. The functionality of adaptation to each BDS may vary depending on the underlying BDS.</td>
</tr>
<tr>
<td>BCAST Subscription Management</td>
<td>Responsible for service provisioning such as subscription and payment related functions, the provision of information used for BCAST Service reception, and BCAST Terminal management. It provides the functionality of Notification, Service Protection management, Content Protection management, Service Guide generation support, Terminal Provisioning and interaction with the BDS Service Distribution/Adaptation to communicate/manage subscription information with the Terminal. It may send the user charging information to the BCAST service application.</td>
</tr>
<tr>
<td>Terminal</td>
<td>The user device that receives broadcast content as well as the BCAST service related information, such as, service guide, content protection information. The user device may support the interactive channel in which case it would be able to directly communicate to the network regarding the available services.</td>
</tr>
</tbody>
</table>
Entities out-of-scope of OMA BCAST

<table>
<thead>
<tr>
<th>Content Creation</th>
<th>Source of content, may provide support for delivery paradigms (e.g., streaming servers); provides base material for content descriptions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BDS Service Distribution/Adaptation</td>
<td>Responsible for the coordination and delivery of broadcast services to the BDS for delivery to the terminal, including file and stream distribution, and Service Guide distribution. It may also include key distribution, broadcast subscription management, and accounting functionalities. BDS Service Distribution/Adaptation may not exist in certain BDSs. In that case it would be considered a “Null Function”. It works with the interactive network to perform service discovery, BDS-specific service protection and handles other interaction functions. It also works with the BDS for content delivery to the terminal.</td>
</tr>
<tr>
<td>Broadcast Network</td>
<td>Specific support for the distribution of content over the broadcast channel. This may involve the same or different radio network from that used by the interactive channel.</td>
</tr>
<tr>
<td>Interaction Network</td>
<td>Specific support for the interaction channel. This may involve the same or different radio network from that used by the broadcast channel.</td>
</tr>
</tbody>
</table>

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

The TISPAN IPTV architecture is specified in TS 182 027 [53].

**Table 8: Mapping between TISPAN IPTV and OMA BCAST logical entities**

<table>
<thead>
<tr>
<th>TISPAN IPTV entities</th>
<th>BCAST entities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High level entity</strong></td>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>Application and IPTV service functions</td>
<td>SDF</td>
</tr>
<tr>
<td></td>
<td>SSF</td>
</tr>
<tr>
<td></td>
<td>SCF</td>
</tr>
<tr>
<td>Media Delivery, distribution &amp; storage</td>
<td>MCF</td>
</tr>
<tr>
<td>Media Delivery, distribution &amp; storage</td>
<td>MDF</td>
</tr>
</tbody>
</table>

Service Protection Management Component (SP-M) in the BSM is responsible for the registration of Terminal and the authentication/authorization of User; Generation of Key messages.

The File Delivery Component (FD) in the network is responsible for the delivery, aggregation, and adaptation of a file or a bundle of files; If the service protection is done by BCAST.
resolution depending on terminals capabilities or user preferences); May perform content protection functionalities (e.g. content encryption).

- May perform content protection functionalities (e.g. content encryption).
- The File Application Component (FA) in the network is responsible for receiving a file or a bundle of files to be broadcast from the Content Creation and sending the file as well as file attributes and additional information: If the content protection is done by BCAST, the FA may cooperate with the Content Protection function to encrypt the file.

<table>
<thead>
<tr>
<th>Application and IPTV service functions</th>
<th>UPSF</th>
<th>The UPSF holds the IMS user profile and possibly IPTV specific profile data</th>
<th>BSM</th>
<th>Equivalent to HSS for Smartcard profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport functions</td>
<td>Transp ort control function</td>
<td>BDS</td>
<td>Service Distribution/Adaptation; Broadcast Network; Interaction Network</td>
<td></td>
</tr>
<tr>
<td>Transport functions</td>
<td>Transp ort processing function</td>
<td>BDS</td>
<td>Service Distribution/Adaptation; Broadcast Network; Interaction Network</td>
<td></td>
</tr>
</tbody>
</table>

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

Table 9: Mapping between TISPAN IPTV and OMA BCAST for IPTV key management

<table>
<thead>
<tr>
<th>TISPAN IPTV entities</th>
<th>BCAST entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>High level entity</td>
<td>Name</td>
</tr>
<tr>
<td>KMF</td>
<td>KMF</td>
</tr>
<tr>
<td>CEF</td>
<td>CEF</td>
</tr>
</tbody>
</table>
9.3.2.4 OMA BCAST Smart Card Profile adaptation to MPEG-2 TS

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

- IP layer using IPSEC,
- RTP layer using SRTP or,
- at applicative layer using ISMACrypt

In TISPAN IPTV,

- When the RTP transport is used for the transport of the content, one of the encryption protocol defined in OMA BCAST shall be used and the STKM shall be transported over UDP/RTP as defined in OMA BCAST.

- When the content is transported in MPEG2 TS encapsulated in UDP/RTP the STKM may be transported in the MPEG2 TS and the following adaptation of OMA BCAST Smartcard profile applies.

9.3.2.4.1 STKM Transport in MPEG-2 TS

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

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

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

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

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

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

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

**Signaling of ECM in PMT for OMA BCAST SCP:**

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

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

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

**Integration of ECM in private section of the CA packet**

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

These PES packets are encoded as private section as defined in MPEG2 TS specification 13818-1 [50].

The table_id for the ECM is given in the ETR 289 [55] and shall be 0x80 or 0x81 the last bit is the toggle bit indicating that the section has been changed.

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

The MIKEY message defined in OMA BCAST SCP is integrated in the CA_data_bytes defined in ETR 289 [xx] as follows:
All the fields except CA_data_bytes are defined in ETR289 [xx]. CA_data_bytes contain the MIKEY message defined in OMA BCAST specification for the STKM of the Smartcard profile for the TEK_n and the TEK_{n+1}.

The payloads depicted in table above are defined OMA-TS-BCAST_SvcCntProtection [52].
The terminal shall filter the ECM using the toggle bit and send the corresponding STKMs to the smartcard when the toggle bit has changed or when the user zaps to another channel.

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

The terminal shall send the STKM corresponding to the TEK_n only once to avoid a replay detection error in the Smartcard.

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

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

Example of ECM processing

The figure below shows which STKM are transmitted to the Smartcard by the terminal with an example:

9.3.2.4.1 STKM and MPEG-2 TS encryption
In case the content is transported in MPEG2 TS, the encryption algorithm used is defined by the Scrambling Descriptor of the program signalled in the PMT. The possible values for this scrambling descriptor are defined in the DVB bluebook A125 [i.yy].

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

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

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

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

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

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.

![NGN IMS architecture - Access security (see ES 282 002 [3])](image)

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

The Gm reference point supports secure communication between an UE and the IMS, e.g. related to registration and session control; see ES 282 007 [24], clause 9.2. The security association between UE and P-CSCF is established during IMS registration procedure. All subsequent session control messages will use this security association.

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

NOTE 2: According to TS 181 005 [43], early implementations may use the so-called "NASS-IMS bundled" or digest authentication mechanism. This mechanism is optional for implementation.
A.2.1.2 Reference Point Cx (CSCF - UPSF)

The Cx reference point supports information transfer between CSCF and UPSF. Further information on the Cx reference point is provided in ES 282 007 [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](image)

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])](image1)

Figure A.4 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])](image2)
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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Policy Requirements</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R-SP-1</td>
<td>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.</td>
<td>No (see note 1)</td>
<td></td>
</tr>
<tr>
<td>R-SP-2</td>
<td>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.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-SP-3</td>
<td>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.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-SP-4</td>
<td>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.</td>
<td>No (see note 2)</td>
<td></td>
</tr>
<tr>
<td>R-SP-5</td>
<td>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.</td>
<td>Yes</td>
<td>PEF, AUTH</td>
</tr>
<tr>
<td>R-SP-6</td>
<td>The Security Gateway Functions (SEGF) shall be responsible for enforcing security policies for the interworking between networks (see note 3).</td>
<td>Yes</td>
<td>PEF</td>
</tr>
<tr>
<td>R-SP-7</td>
<td>SEGF are responsible for security sensitive operations and shall offer capabilities for secure storage of long-term keys used for IKE authentication.</td>
<td>Yes</td>
<td>SEGF, AUTH</td>
</tr>
<tr>
<td><strong>Authentication, Authorization, Access Control and Accountability Requirements</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R-AA-1</td>
<td>Access to NGN networks, services, and applications shall be provided for authorized users only.</td>
<td>Yes</td>
<td>PEF, AUTH</td>
</tr>
<tr>
<td>R-AA-2</td>
<td>NGN IMS authentication shall support early deployment scenarios (with support for legacy equipments).</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-AA-3</td>
<td>In non-early deployment scenarios, IMS authentication shall be independent from access authentication.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-AA-4</td>
<td>An ISIM shall be used to access any IMS service, however, exceptions may be allowed for emergency calls and early deployment scenarios.</td>
<td>No. Insofar as ISIM is not detectable at the interface between UE and NGN. (see note 4)</td>
<td></td>
</tr>
<tr>
<td>R-AA-5</td>
<td>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]).</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-AA-6</td>
<td>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]).</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-AA-7</td>
<td>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.</td>
<td>Yes</td>
<td>PEF</td>
</tr>
<tr>
<td>R-AA-8</td>
<td>NGN relevant ISIM specific information shall be protected against unauthorized access or alteration.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------</td>
<td>-------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>R-AA-9</td>
<td>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).</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-AA-10</td>
<td>User Authentication to the NGN IMS using SIP Digest mechanisms shall be supported as an early deployment scenario.</td>
<td>Yes</td>
<td>AUTH</td>
</tr>
<tr>
<td>R-AA-11</td>
<td>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.</td>
<td>Yes</td>
<td>PEF</td>
</tr>
<tr>
<td>R-AA-12</td>
<td>Transmitted passwords shall be sufficiently protected; e.g. by encryption or other techniques.</td>
<td>Yes</td>
<td>CONF, INTF</td>
</tr>
<tr>
<td>R-AA-13</td>
<td>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)</td>
<td>Yes</td>
<td>AUTH</td>
</tr>
<tr>
<td>R-AA-14</td>
<td>The NGN subsystems shall be able to define and enforce policy with respect to validity of user authorization.</td>
<td>Yes</td>
<td>PEF</td>
</tr>
<tr>
<td>R-AA-15</td>
<td>Mutual authentication shall be supported between the UE and the AS before providing authorization.</td>
<td>Yes</td>
<td>AUTH, AUTHOR</td>
</tr>
<tr>
<td>R-AA-16</td>
<td>It SHOULD also be possible to support an Authentication Proxy based architecture (see note 7).</td>
<td>Yes</td>
<td>AUTH</td>
</tr>
<tr>
<td>R-AA-17</td>
<td>Mutual authentication shall be supported between the UE and the AP.</td>
<td>Yes</td>
<td>AUTH</td>
</tr>
<tr>
<td>R-AA-18</td>
<td>The AP shall decide whether a particular subscriber (i.e. the UE), is authorized to access a particular AS.</td>
<td>Yes</td>
<td>AUTHOR</td>
</tr>
<tr>
<td>R-AA-19</td>
<td>If an AP is used, the AS shall only authorize the access request to the requested resource (see note 8).</td>
<td>Yes</td>
<td>AUTHOR</td>
</tr>
<tr>
<td>R-AA-20</td>
<td>Mutual authentication should be supported between the UE and the NASS during access network level registration.</td>
<td>Yes</td>
<td>AUTH</td>
</tr>
<tr>
<td>R-AA-21</td>
<td>The access network shall be able to authenticate and authorize the access subscriber.</td>
<td>Yes</td>
<td>AUTH, AUTHOR</td>
</tr>
<tr>
<td>R-AA-22</td>
<td>Authentication and authorization to the Access Network is controlled by the operator of the Access Network.</td>
<td>Yes</td>
<td>AUTH, AUTHOR, PEF</td>
</tr>
<tr>
<td>R-AA-23</td>
<td>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.</td>
<td>Yes</td>
<td>AUTHOR</td>
</tr>
<tr>
<td>R-AA-24</td>
<td>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.</td>
<td>Yes</td>
<td>AUTH</td>
</tr>
<tr>
<td>R-AA-25</td>
<td>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.</td>
<td>Yes</td>
<td>AUTH, PEF</td>
</tr>
<tr>
<td>R-AA-26</td>
<td>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.</td>
<td>Yes</td>
<td>AUTH</td>
</tr>
<tr>
<td>R-AA-27</td>
<td>As the interface between the Application Function (AF) and RACS can be inter-operator, the RACS shall authenticate and authorize the Application Function (AF).</td>
<td>Yes</td>
<td>AUTH, AUTHOR</td>
</tr>
</tbody>
</table>
### Identity and Secure Registration Requirements

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>R-AA-28</td>
<td>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.</td>
<td>Yes</td>
<td>AUTH</td>
</tr>
<tr>
<td>R-AA-29</td>
<td>Authentication of NGN users and authentication of NGN terminals shall be separate.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-AA-30</td>
<td>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.</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### Communications and Data Security Requirements

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>R-IR-1</td>
<td>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).</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-IR-2</td>
<td>An access identity shall be used for access authentication. This identity may or may not be used for other purposes.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-IR-3</td>
<td>The line ID shall be possible to use for line authentication.</td>
<td>No</td>
<td>(see note 9)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>R-CD-1</td>
<td>Confidentiality and integrity of IMS signalling shall be applied in a hop-to-hop fashion. (UE-to-P-CSCF and among other NEs).</td>
<td>Yes</td>
<td>CONF, INTF</td>
</tr>
<tr>
<td>R-CD-2</td>
<td>Network Domain Security (NDS) shall be provided at the network layer and comply with TS 133 210 [8].</td>
<td>Yes</td>
<td>SEGF(AUTH, AUTHOR, KM, CONF, INT, PEF)</td>
</tr>
<tr>
<td>R-CD-3</td>
<td>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].</td>
<td>Yes</td>
<td>SEGF(AUTH, AUTHOR, KM, CONF, INT, PEF)</td>
</tr>
<tr>
<td>R-CD-4</td>
<td>Security shall be provided within the network domain for the Cx interface.</td>
<td>Yes</td>
<td>SEGF(AUTH, AUTHOR, KM, CONF, INT, PEF)</td>
</tr>
<tr>
<td>R-CD-5</td>
<td>An ISIM based solution for IMS access security (authentication, confidentiality and integrity protection) of signalling to and from the user, shall be supported.</td>
<td>Yes</td>
<td>AUTH, INT, CONF</td>
</tr>
<tr>
<td>R-CD-6</td>
<td>Secure link shall be provided between UE and the P-CSCF for protection of the Gm reference point.</td>
<td>Yes</td>
<td>AUTH, AUTHOR, CONF, INT</td>
</tr>
<tr>
<td>R-CD-7</td>
<td>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.</td>
<td>Yes</td>
<td>CONF, INT, AUTH, AUTHOR</td>
</tr>
<tr>
<td>R-CD-8</td>
<td>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.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-CD-9</td>
<td>ISIM specific information shall be updated in a secure manner.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-CD-10</td>
<td>It shall be possible to protect sensitive data (such as Presence information and notifications) from attacks (e.g. eavesdropping, tampering, and replay attacks).</td>
<td>Yes</td>
<td>CONF, INT, AUTH, AUTHOR</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------</td>
<td>------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>R-CD-11</td>
<td>The Rq and Gq’ reference points shall provide mechanism to assure security of the information exchanged.</td>
<td>Yes</td>
<td>SEGf(AUTH, AUTHOR, KM, CONF, INT, PEF)</td>
</tr>
<tr>
<td>R-CD-12</td>
<td>All data related to configuring the UE through the e3 if shall be protected against loss of confidentiality and against loss of integrity.</td>
<td>Yes</td>
<td>AUTH, AUTHOR, KM, CONF, INT, PEF</td>
</tr>
<tr>
<td><strong>Integrity and Replay Protection Requirements</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R-CD-13</td>
<td>Integrity protection of signalling, control communications and of stored data shall be provided.</td>
<td>Yes</td>
<td>INT, AUTH, AUTHOR</td>
</tr>
<tr>
<td>R-CD-14</td>
<td>It shall be possible to ensure the origin, integrity and freshness of authentication data, particularly of the cipher key.</td>
<td>Yes</td>
<td>INT, AUTH, AUTHOR</td>
</tr>
<tr>
<td>R-CD-15</td>
<td>Integrity protection shall be applied between the UE and the P-CSCF for protecting the SIP signalling.</td>
<td>Yes</td>
<td>INT, AUTH, AUTHOR</td>
</tr>
<tr>
<td>R-CD-16</td>
<td>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].</td>
<td>Yes</td>
<td>SEGf(AUTH, AUTHOR, KM, CONF, INT, PEF)</td>
</tr>
<tr>
<td>R-CD-17</td>
<td>Data integrity shall be supported between the UE and the Application Server.</td>
<td>Yes</td>
<td>INT, AUTH, AUTHOR</td>
</tr>
<tr>
<td><strong>Confidentiality Requirements</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R-CD-18</td>
<td>Confidentiality of communications should be achieved by cryptographic encryption. Confidentiality of stored data shall be achieved by cryptographic encryption or by access controls.</td>
<td>Yes</td>
<td>CONF</td>
</tr>
<tr>
<td>R-CD-19</td>
<td>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.</td>
<td>Yes</td>
<td>CONF</td>
</tr>
<tr>
<td>R-CD-20</td>
<td>IMS specific confidentiality protection shall be provided for the SIP signalling between UE and P-CSCF.</td>
<td>Yes</td>
<td>CONF</td>
</tr>
<tr>
<td>R-CD-21</td>
<td>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].</td>
<td>Yes</td>
<td>SEGf(AUTH, AUTHOR, KM, CONF, INT, PEF)</td>
</tr>
<tr>
<td>R-CD-22</td>
<td>It shall be possible to protect the confidentiality of user-related data which is stored or processed by a provider.</td>
<td>Yes</td>
<td>CONF</td>
</tr>
<tr>
<td><strong>Privacy Requirements</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R-P-1</td>
<td>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.</td>
<td>Yes</td>
<td>PEF</td>
</tr>
<tr>
<td>R-P-2</td>
<td>User location and usage patterns shall be kept from unwanted disclosure.</td>
<td>Yes</td>
<td>PEF</td>
</tr>
<tr>
<td>R-P-3</td>
<td>It shall be possible to protect the confidentiality of user identity data.</td>
<td>Yes</td>
<td>CONF</td>
</tr>
<tr>
<td>R-P-4</td>
<td>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.</td>
<td>Yes</td>
<td>PEF</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>R-P-5</td>
<td>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.</td>
<td>Yes</td>
<td>PEF</td>
</tr>
<tr>
<td>R-P-6</td>
<td>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.</td>
<td>Yes</td>
<td>PEF</td>
</tr>
<tr>
<td>R-P-7</td>
<td>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).</td>
<td>Yes</td>
<td>PEF, AUTH</td>
</tr>
<tr>
<td>R-P-8</td>
<td>The NGN shall provide mechanisms that allow presenting the identity of the session originator, if this is not restricted by the session originator.</td>
<td>Yes</td>
<td>PEF</td>
</tr>
<tr>
<td>R-P-9</td>
<td>The privacy aspect of presence information and the need for authorization before providing presence information shall be configurable by the user (i.e. presentilly).</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-P-10</td>
<td>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.</td>
<td>Yes</td>
<td>PEF, AUTHOR</td>
</tr>
<tr>
<td>R-P-11</td>
<td>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.</td>
<td>Yes</td>
<td>PEF</td>
</tr>
<tr>
<td>R-P-12</td>
<td>It shall be possible for the sender of the message to request to hide its public ID from the recipient.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-P-13</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Key Management Requirements</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R-KM-1</td>
<td>Key management and key distribution between SEGFs shall comply with the Network Domain Security (see TS 133 210 [8]).</td>
<td>Yes</td>
<td>KM</td>
</tr>
<tr>
<td>R-KM-2</td>
<td>The UE and the AS shall be able to resume a previously established secure session.</td>
<td>Yes</td>
<td>KM</td>
</tr>
<tr>
<td>R-KM-3</td>
<td>The key management mechanism must be able to traverse a NAT/NATP device.</td>
<td>Yes</td>
<td>KM</td>
</tr>
<tr>
<td>R-NF-1</td>
<td>NGN security protocols shall work with commonly-used firewalls and shall work in environments with NAT/NATP.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-NF-2</td>
<td>Filters to screen the IP packets to restrict/grant access to specific bearer streams shall be supported.</td>
<td>Yes</td>
<td>PEF</td>
</tr>
<tr>
<td>R-NF-3</td>
<td>The SEGFs may include filtering policies and firewall functionality not required in TS 133 210 [8].</td>
<td>Yes</td>
<td>PEF</td>
</tr>
<tr>
<td></td>
<td><strong>Availability and DoS protection Requirements</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R-AD-1</td>
<td>Mechanisms shall be provided to mitigate denial-of-service attacks.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-AD-2</td>
<td>Provide access control mechanisms to ensure that authorized users only can access the service.</td>
<td>Yes</td>
<td>AUTHOR, PEF</td>
</tr>
<tr>
<td>R-AD-3</td>
<td>It shall be possible to prevent intruders from restricting the availability of services by logical means.</td>
<td>Yes</td>
<td>AUTHOR, PEF</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------</td>
<td>--------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>R-AD-4</td>
<td>Availability of and accuracy of location information shall be provided for the EMTEL services.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-AD-5</td>
<td>Availability of EMTEL PSAPs shall not be decreased by DoS attacks. EMTEL PSAPs shall be able to reconnect.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td><strong>Assurance Requirements</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R-AS-1</td>
<td>The NGN shall provide guidance for evaluating and certifying NGN equipment and systems.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>R-AS-2</td>
<td>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.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td><strong>Requirements on Strength of Security Mechanisms</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R-SS-1</td>
<td>The guidelines defined in ES 202 238 [41] shall be followed when defining or selecting cryptographic algorithms in NGN.</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**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 nomadicty).
- b) IMS authentication is linked to access authentication for IP Connectivity (limited nomadicty 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 nomadicty may be available. No IMS specific authentication is therefore required from the CPE/Terminal to gain access to IMS services.

**NOTE 7:** The purpose of the AP is to separate the authentication procedure and the AS specific application logic to different logical entities.

**NOTE 8:** The AS does not need to explicitly authenticate the user.

**NOTE 9:** Identity and the association of identity to service do not imply an FE but may imply an information element within an information flow.
Annex C: Void

Void.
Annex D: 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])
Annex E (informative):
Open Issues in NGN Security

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

1) ISIM chaining: Usage of ISIM in terminals connected through other ISIM-enabled entities (e.g. CNG).
2) PES/H.248 security: Investigate the H.248 security in case the NGN assumptions do not apply.
3) Usage/licensing of 3GPP security algorithms in NGN context.
4) How to secure the Ic IF? SEGFs could be one possibility; security functions (e.g. integrated SEGF) as part of the IBCF could be another possibility. The current text is not clear on this.
5) Security aspects of Emergency Telecommunications are not addressed yet in the present document.

Annex F (informative): Void
Annex G (informative):

Bibliography

- 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".
### Annex H (informative):
#### Change history

<table>
<thead>
<tr>
<th>Date</th>
<th>WG Doc.</th>
<th>CR</th>
<th>Rev</th>
<th>CAT</th>
<th>Title / Comment</th>
<th>Current Version</th>
<th>New Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>02-10-08</td>
<td>19WTD028</td>
<td>001</td>
<td>F</td>
<td></td>
<td>WG7 and WG5 terminology alignment “IRG”/“CNG”</td>
<td>2.1.1</td>
<td>3.0.1</td>
</tr>
<tr>
<td>29-10-09</td>
<td>21bTD197</td>
<td>001</td>
<td>A</td>
<td>F</td>
<td>CR001 TB approved at TISPAN#19</td>
<td>3.1.0</td>
<td>3.1.1</td>
</tr>
<tr>
<td>29-10-09</td>
<td>21bTD197</td>
<td>002</td>
<td>F</td>
<td></td>
<td>Addition of references for update of architecture description</td>
<td>3.1.0</td>
<td>3.1.1</td>
</tr>
<tr>
<td>29-10-09</td>
<td>21bTD197</td>
<td>003</td>
<td>F</td>
<td></td>
<td>Update of architecture diagrams and associated text</td>
<td>3.1.0</td>
<td>3.1.1</td>
</tr>
<tr>
<td>28-11-09</td>
<td>22bTD135</td>
<td>004</td>
<td>F</td>
<td></td>
<td>Update of security services in NGN FEs (table 5)</td>
<td>3.1.0</td>
<td>3.1.1</td>
</tr>
<tr>
<td>12-04-10</td>
<td>TISPAN07(10)0049</td>
<td>006</td>
<td>B</td>
<td></td>
<td>Any Content Protection for IPTV Security</td>
<td>3.1.0</td>
<td>3.1.1</td>
</tr>
<tr>
<td>07-04-10</td>
<td>TISPAN07(10)0051</td>
<td>007</td>
<td>B</td>
<td>F</td>
<td>OMA BCAST</td>
<td>3.1.0</td>
<td>3.2.0</td>
</tr>
<tr>
<td>29-04-10</td>
<td>TISPAN07(10)0043</td>
<td>008</td>
<td>B</td>
<td></td>
<td>Application Layer Authentication Architecture for UICC-less CNDs</td>
<td>3.1.0</td>
<td>3.2.0</td>
</tr>
<tr>
<td>26-11-10</td>
<td>TISPAN07(10)0157</td>
<td>009</td>
<td>B</td>
<td>F</td>
<td>Zb interface between NGN components in an NGN network made mandatory for implementation, but still optional for use by operators.</td>
<td>3.2.0</td>
<td>3.3.0</td>
</tr>
<tr>
<td>06-12-10</td>
<td>TISPAN07(10)0166</td>
<td>010</td>
<td>C</td>
<td></td>
<td>Clarifications and deletion of duplicated material</td>
<td>3.3.0</td>
<td>3.4.0</td>
</tr>
<tr>
<td>06-12-10</td>
<td>TISPAN07(10)0191</td>
<td>011</td>
<td>F</td>
<td>F</td>
<td>IPTV: OMA BCAST STKM and MPEG-2 TS (transport and encryption)</td>
<td>3.3.0</td>
<td>3.4.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>F</td>
<td>Update of Change history table</td>
<td>3.4.0</td>
<td>3.4.1</td>
</tr>
</tbody>
</table>
## History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2.1.1</td>
<td>February 2009</td>
<td>Publication</td>
</tr>
<tr>
<td>V3.0.1</td>
<td>March 2009</td>
<td>R3 baseline CR 001 19WTD028r2 implemented - Clause 10 request for contributions</td>
</tr>
<tr>
<td>V3.1.0</td>
<td>August 2009</td>
<td>CR001 TB approved at TISPAN#19</td>
</tr>
<tr>
<td>V3.1.1</td>
<td>October 2009</td>
<td>CR001,002,003 approved at TISPAN#22</td>
</tr>
<tr>
<td>V3.2.0</td>
<td>May 2010</td>
<td>22TD135r1, at TISPAN#23 (10)0043r1,(10)0049r2,(10)051r2 at TISPAN#24 Implemented</td>
</tr>
<tr>
<td>V3.3.0</td>
<td>November 2010</td>
<td>TISPAN(10)0190 CR pack against WI-07038 – Sec. Arch. Implemented (making Zb mandatory for implementation but still optional for use)</td>
</tr>
<tr>
<td>V3.4.0</td>
<td>December 2010</td>
<td>TISPAN(10)0166r2_CR_TS_187_003_Tidying_and_corrections TISPAN(10)0191r3 IPTV: OMA BCAST STKM and MPEG-2 TS (transport and encryption Implemented</td>
</tr>
</tbody>
</table>