ETSI TR 187 002 V3.1.1 (2011-04)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat, Vulnerability and Risk Analysis

Reference

RTR/TISPAN-07037-NGN-R3

Keywords

analysis, security

ETSI

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

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

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

Important notice

Copyright Notification

Contents

Intellectual Property Rights

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

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

Foreword

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

1 Scope

The present document presents the results of the Threat Vulnerability Risk Analysis (TVRA) for the NGN.

The present document follows the method and proforma for carrying out a TVRA defined in TS 102 165-1 [i.4] and incorporates material of the NGN threat and risk analysis herein.

The present document identifies security-relevant interfaces in the NGN, identifies security-relevant scenarios for use in the NGN, analyses NGN in terms of security threats and risks by performing a security threat and risk analysis, and classifies the identified vulnerabilities and the associated risk presented to the NGN.

This threat and risk analysis makes a number of assumptions that are believed to hold for typical deployment scenarios of the NGN.

NOTE 1: Depending on the actual instantiation of the NGN some of the assumptions declared in the present document may not fully hold and this may alter the associated risks.

NOTE 2: Whilst the present document is a technical report it identifies requirements for future work. In all cases these requirements are considered indicative pending their ratification in formal ETSI Technical Specifications within the TISPAN Work Programme.

2 References

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

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

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

2.1 Normative references

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

Not applicable.

2.2 Informative references

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

[i.1] ETSI EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".

[i.2] ETSI TS 181 005: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability Requirements".

[i.3] ISO/IEC 13335: "Information technology - Guidelines for the management of IT security".

[i.4] ETSI TS 102 165-1 (V4.2.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

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

[i.6] ETSI TS 187 001: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[i.7] ETSI TS 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

[i.8] ETSI TR 180 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Release definition".

[i.9] ETSI ES 282 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); Functional architecture".

[i.10] ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture".

[i.11] ETSI ES 283 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); H.248 Profile for controlling Access and Residential Gateways".

[i.12] ETSI EN 383 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control (BICC) Protocol or ISDN User Part (ISUP) [ITU-T Recommendation Q.1912.5, modified]".

[i.13] ETSI TS 133 210: " Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 Release 10)".

[i.14] AS/NZS 4360: "Risk Management".

[i.15] Directive 2002/21/EC of the European Parliament and of the council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[i.16] Directive 2002/58/EC of the European Parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[i.17] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[i.18] IETF RFC 3261: "SIP: Session Initiation Protocol".

[i.19] 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 Release 7)".

[i.20] ETSI TS 133 234: "Universal Mobile Telecommunications System (UMTS); 3G security; Wireless Local Area Network (WLAN) interworking security (3GPP TS 33.234 Release 6)".

[i.21] ITU-T Recommendation H.248: "Gateway control protocol".

[i.22] ETSI TR 102 055: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); ENUM scenarios for user and infrastructure ENUM".

[i.23] ETSI TR 102 420: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Review of activity on security".

[i.24] IETF RFC 2535: "Domain Name System Security Extensions".

[i.25] IETF RFC 3761: "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[i.26] IETF RFC 3403: "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database".

[i.27] IETF RFC 2915: "The Naming Authority Pointer (NAPTR) DNS Resource Record".

[i.28] Draft-ietf-dnsext-dnssec-protocol-06 (2004): "Protocol Modifications for the DNS Security Extensions".

[i.29] Draft-ietf-dnsext-dnssec-records-08 (2004): "Resource Records for DNS Security Extensions".

[i.30] Draft-ietf-dnsext-dnssec-intro-11 (2004): "DNS Security Introduction and Requirements".

[i.31] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.32] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".

NOTE: When referring to all parts of ISO/IEC 15408 the reference above is used.

[i.33] 3GPP TR 33.803: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Coexistence between TISPAN and 3GPP authentication schemes (Release 7)".

[i.34] ETSI TR 187 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples".

[i.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".

[i.36] IETF RFC 1631: "The IP Network Address Translator (NAT)".

[i.37] IETF RFC 1918: "Address Allocation for Private Internets".

[i.38] IETF RFC 3489: "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)".

[i.39] IETF draft, draft-ietf-behave-rfc3489bis-13 (November 2007): "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)".

[i.40] IETF draft, draft-ietf-mmusic-ice-19 (October 2007): "Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols".

[i.41] IETF draft, draft-behave-turn-02 (February 2006): "Obtaining Relay Addresses from Simple Traversal of UDP Through NAT (STUN)".

[i.42] ETSI TR 187 009: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study of prevention of unsolicited communication in the NGN".

[i.43] ETSI SR 002 211: "Electronic communications networks and services; Candidate list of standards and/or specifications in accordance with Article 17 of Directive 2002/21/EC".

[i.44] ETSI TS 181 016: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service Layer Requirements to integrate NGN services and IPTV".

[i.45] Directive 95/46/EC Of The European Parliament And Of The Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.46] ETSI TS 185 006 (V2.3.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Devices architecture and Reference Points".

[i.47] ETSI TS 185 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Premises Networks: Protocol Specification (Stage 3)".

[i.48] ETSI TS 184 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Identifiers (IDs) for NGN".

[i.49] 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 [3GPP TS 24.229 [Release 7], modified]".

[i.50] Void.

[i.51] UK Home Office; R.V.Clark, "Hot Products: understanding, anticipating and reducing demand for stolen goods", ISBN 1-84082-278-3.

[i.52] ETSI TR 187 002 (V1.2.2): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN);TISPAN NGN Security (NGN-SEC);Threat, Vulnerability and Risk Analysis".

[i.53] IEEE 802.11 (2007): "Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications".

[i.54] Void.

[i.55] ETSI TS 187 016: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Identity Protection (Protection Profile)".

[i.56] ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[i.57] ISO/IEC 15408-2: " Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements".

[i.58] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Vocabulary for 3GPP Specifications (3GPP TR 21.905)".

[i.59] ISO/IEC 7498-2: " Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture".

[i.60] ETSI TS 183 019 (V2.3.0): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment; User-Network Interface Protocol Definitions".

[i.61] ETSI TS 133 310 (V9.4.0): "Universal Mobile Telecommunications System (UMTS); LTE; Network Domain Security (NDS); Authentication Framework (AF) (3GPP TS 33.310 version 9.4.0 Release 9)".

[i.62] ETSI TS 133 320 (V9.3.0): "Universal Mobile Telecommunications System (UMTS); LTE; Security of Home Node B (HNB) / Home evolved Node B (HeNB) (3GPP TS 33.320 version 9.3.0 Release 9)".

[i.63] IETF RFC 1661: "The Point-to-Point Protocol (PPP)".

[i.64] IETF RFC 3741: "Exclusive XML Canonicalization, Version 1.0".

[i.65] IETF RFC 1994: "PPP Challenge Handshake Authentication Protocol (CHAP)".

[i.66] ETSI TS 124 234: "Universal Mobile Telecommunications System (UMTS); LTE; 3GPP system to Wireless Local Area Network (WLAN) interworking; WLAN User Equipment (WLAN UE) to network protocols; Stage 3 (3GPP TS 24.234)".

[i.67] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229)".

[i.68] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[i.69] Void.

[i.70] ETSI TS 183 020: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment: Roaming in TISPAN NGN Network Accesses; Interface Protocol Definition".

[i.71] ETSI TS 129 234: "Universal Mobile Telecommunications System (UMTS); LTE; 3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3 (3GPP TS 29.234)".

[i.72] IETF RFC 3539: "Authentication, Authorization and Accounting (AAA) Transport Profile".

[i.73] IETF RFC 4005: "Diameter Network Access Server Application".

[i.74] IETF RFC 4072: "Diameter Extensible Authentication Protocol (EAP) Application".

[i.75] IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".

[i.76] IETF RFC 3580: "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines".

[i.77] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[i.78] IETF RFC 2548: "Microsoft Vendor-specific RADIUS Attributes".

[i.79] IETF RFC 2866: "RADIUS Accounting".

[i.80] IETF RFC 4372: "Chargeable User Identity".

[i.81] IETF RFC 2486bis(6): "The Network Access Identifier".

[i.82] IETF RFC 3162: "RADIUS and IPv6".

[i.83] IETF RFC 3588: "Diameter Base Protocol".

[i.84] 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".

[i.85] 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".

[i.86] ETSI TS 129 329: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Sh interface based on the Diameter protocol; Protocol details (3GPP TS 29.329)".

[i.87] IETF RFC 3554: "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec".

[i.88] IETF RFC 2960: "Stream Control Transmission Protocol".

[i.89] IETF RFC 3309: "Stream Control Transmission Protocol (SCTP) Checksum Change".

[i.90] IETF RFC 4201: "Link Bundling in MPLS Traffic Engineering (TE)".

[i.91] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[i.92] ETSI TR 133 978: "Universal Mobile Telecommunications System (UMTS); Security aspects of early IP Multimedia Subsystem (IMS) (3GPP TR 33.978)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EG 202 387 [i.1] and the following apply:

attack: attempt to bypass security controls on a computer

NAT traversal: term used to describe the problem of establishing connections between hosts in IP networks which use NAT devices (either locally or remotely) to modify their local IP address

Network Address Translation: method by which IP addresses are mapped from one realm to another in order to provide transparent routing to hosts

NOTE: NAT devices are used to connect address domains with private (unregistered) addresses to public domains with globally unique (registered) addresses.

T-*nnn*: numeric identifier for a threat

threat: potential cause of an unwanted incident which may result in harm to a system or organization

NOTE: See ISO/IEC 13335 [i.3].

unwanted incident: incident such as loss of confidentiality, integrity and/or availability

NOTE: See AS/NZS 4360 [i.14].

user equipment: one or more devices allowing a user to access services delivered by TISPAN NGN networks

NOTE: This includes devices when under user control commonly referred to as IAD, ATA, RGW, TE, etc., UE does not include network controlled entities such as network terminations and access gateways.

vulnerability: flaw or weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security policy

NOTE: Vulnerability is often used synonymously with weakness.

3.2 Abbreviations

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

3G	3rd Generation
3GPP	3rd Generation Partnership Project
ADSL	Asymmetric Digital Subscriber Line
AF	Application Function
AGCF	Access Gateway Control Function
AGW	Access GateWay
AH	Authentication Header
A-MGF	Access Media Gateway Function
A-RACF	Access-Resource and Admission Control Function
ARGW	Access Residential media GateWay
AS	Application Server
B2BUA	Back-To-Back User Agent
BGF	Border Gateway Function
BTF	Basic Transport Function
CC	Call Control
CCM	Counter mode with Cipher block chaining Message authentication code
CCMP	Counter mode with Cipher block chaining Message authentication code Protocol

CD	Compact Disc
CHAP	Challenge Handshake Authentication Protocol
CLF	Connectivity session and repository Location Function
CND	Customer Network Device
CNG	Customer Network Gateway
CPE	Customer Premises Equipment
CPN	Customer Premises Network
C-RACF	Core-Resource and Admission Control Function
CRAVED	Concealable, Removable, Available, Valuable, Enjoyable, and Disposable
CSCF	Call Session Control Function
DECT	Digital European Cordless telephony
DNS	Domain Name System
DNSSEC	DNS SECurity
DoS	Denial-of-Service
DSAA	DECT Standard Authentication Algorithm
DSC	DECT Standard Cipher
DTMF	Dual Tone Multi Frequency
EAP	Extensible Authentication Protocol
ECN	Electronic Communication Network
ECN&S	Electronic Communications Networks and Services
ECS	Electronic Communication Service
ESP	Encapsulating Security Payload
FFS	For Further Study
FQDN	Fully Qualified Domain Name
GPRS	GSM Packet Radio System
ICE	Interactive Connectivity Establishment
I-CSCF	Interrogating Call Session Control Function
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IMSI	IMS subscriber Identifier
IP	Internet Protocol
IPsec	Internet Protocol security
IPTV	Internet Protocol TeleVision
ISDN	Integrated Services Digital Network
ISIM	IMS Subscriber Identity Module
ISO	International Standards Organization
ISUP	ISDN User Part
IVR	Interactive Voice Response
MAC	Message Authentication Code
MD	Message Digest
MGC	Media Gateway Controller
MGW	Media GateWay
MRFP	Media Resource Function Processor
NANP	NGN Access Network Provider
NASS	Network Access SubSystem
NAT (1)	Network Address Translator (device)
NAT (2)	Network Address Translation (process)
NAT-T	Network Address Translation Traversal
NBA	NASS-Bundled Authentication
NCP	NGN Connectivity Provider
NGN	Next Generation Network
NT	Network Termination
OSI	Open Systems Interconnection
P-CSCF	Proxy Call Session Control Function
PDBF	Profile Data Base Function
PES	PSTN/ISDN Emulation Subsystem
PNG	Public Network Gateway
PoC	Push to talk over Cellular
PS	Packet-Switched
PSTN	Public Switched Telephone Network
RACS	Resource Admission Control Subsystem

RAMR	Realistic-Achievable-Mesurable-Relevant
RCEF	Resource Control Enforcement Function
RGW	Residential GateWay
R-MGF	Residential Media Gateway Function
ROM	Read-Only Memory
RSN	Robust Security Network
RTCP	Realtime Transport Control Protocol
RTP	Realtime Transport Protocol
RTSP	Real-Time Streaming Protocol
S-CSCF	Serving Call Session Control Function
SDP	Session Description Protocol
SEG	SEcurity Gateway
SGW	Signalling GateWay
SIP	Session Initiation Protocol
SPDF	Service Policy Decision Function
SpoA	Service point of Attachment
STUN	Simple Traversal of UDP through NAT
TCP	Transport Control Protocol
TDM	Time Division Multiplex
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
ToE	Target of Evaluation
TPF	Transport Processing Function
TpoA	Transport point of Attachment
TVRA	Threat Vulnerability Risk Assessment
UAAF	User Access Authorization Function
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card
UML	Unified Modelling Language
UNI	User-Network Interface
UPSF	User Profile Server Function
VLAN	Virtual Local Area Network
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access

4 NGN-relevant Security Interfaces and Scenarios

This clause identifies the NGN use cases and therefore the NGN security environment that the TVRA has been applied to.

4.1 Security-relevant NGN Scenarios

Scenarios are presented following a complexity ordering, from a simple generic model to rather more complex scenarios.

4.1.1 Basic NGN scenario (ECN&S model)

The Electronic Communication Network (ECN) and Electronic Communication Service (ECS) model as shown in figure 1 is the model used in the Framework Directive [i.15] and simplifies the network into a set of provision types. An ECN is a communication network and roughly speaking addresses the lowest 3 layers of the ISO/OSI protocol stack. An ECS is a communication service and roughly speaking addresses the highest layers of the ISO/OSI stack. In order to connect a user connects to both an ECS and an ECN.

The basic model shows that the CPE may consist of more than one equipment type and that the NT has two connection points, one for services (SpoA) and one for Transport (or network) (TpoA).

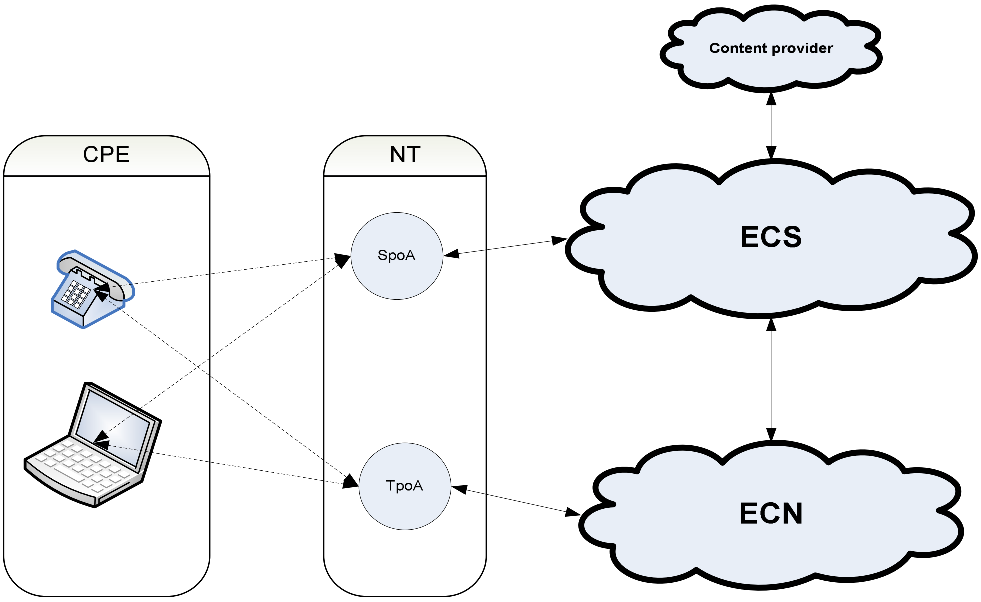


Figure 1: Basic ECN&S model for the NGN

4.1.2 IMS scenarios

4.1.2.1 3GPP IMS

The 3GPP IMS model does not in general distinguish ECS and ECN but there is a broad assumption that IMS lies on top of the PS subsystem which is an implementation of ECN using 3GPP specific access technology. The trusted domain therefore encompasses each of the NT, ECN (the GPRS network) and ECS (the IMS network), see figure 2 for a simplified IMS scenario.

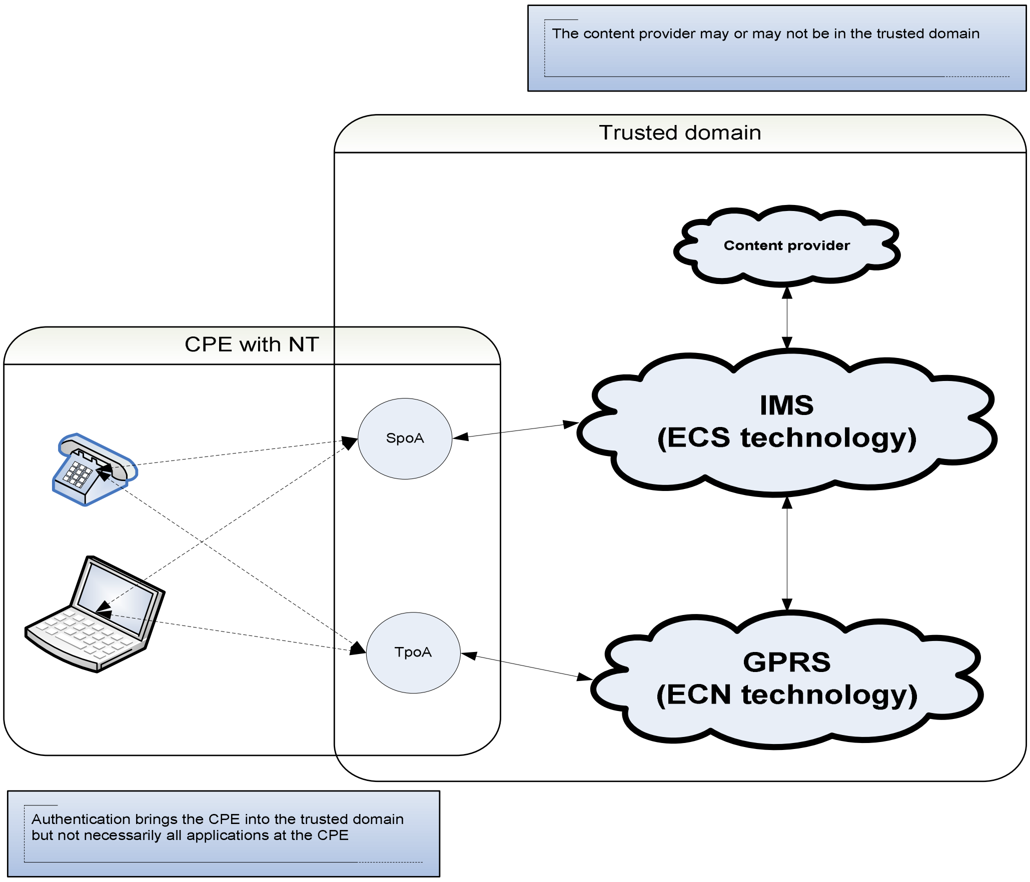

The content provider may or may not be in the trusted domain
Trusted domain
Content provider
CPE with NT
SpoA
IMS
(ECS technology)
TpoA
GPRS
(ECN technology)
Authentication brings the CPE into the trusted domain but not necessarily all applications at the CPE

Figure 2: Simplified view of 3GPP IMS domains mapped to ECNS

The authentication mechanism does not provide separate authentication of each service on the broad assumption that all services are offered to the same identity and therefore there is no need to give authorization and authentication on a per-service basis.

4.1.2.2 Generic or NGN IMS

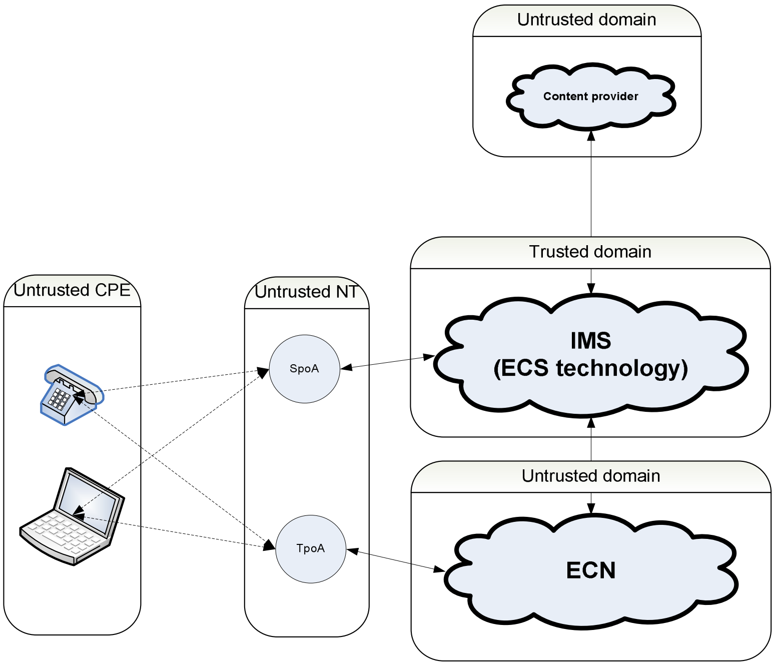


Figure 3: View of IMS where IMS is trusted

In figure 4 the model is extended to show which domains shown in figure 3 contain different element types.

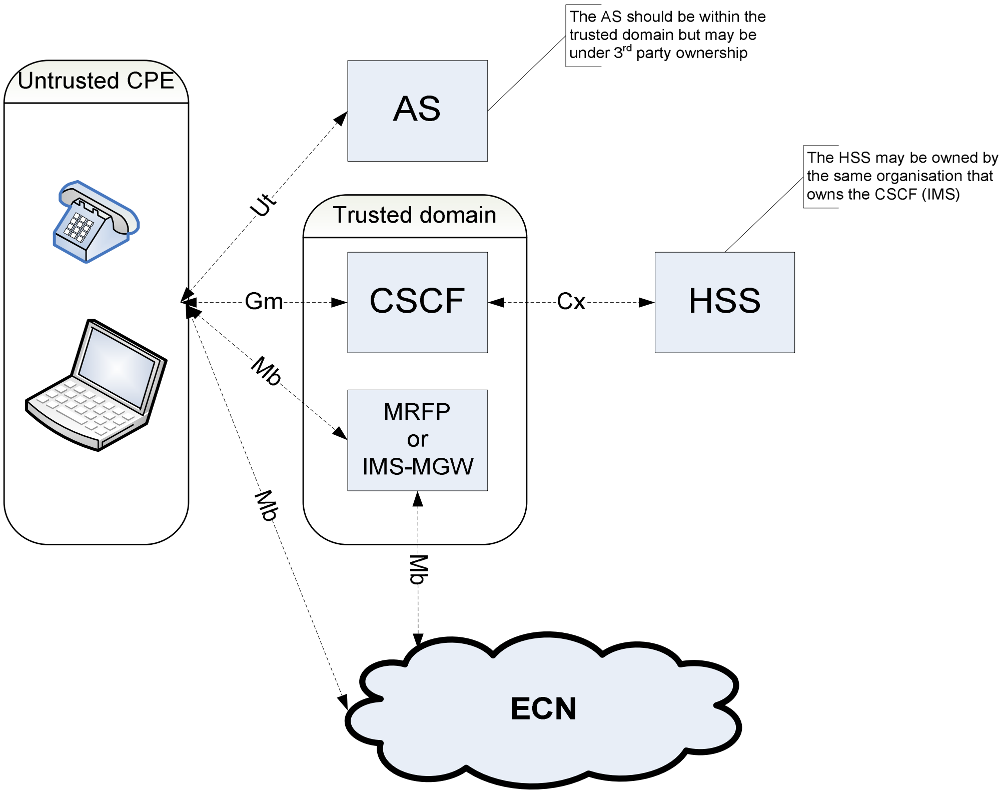

The AS should be within the trusted domain but may be under 3rd party ownership
Untrusted CPE
AS
Ut
The HSS may be owned by the same organisation that owns the CSCF (IMS)
Trusted domain
Gm
CSCF
Cx
HSS
Mb
MRFP or IMS-MGW
Mb
Mb
ECN

Figure 4: Open interfaces in the IMS model for NGN

Figure 5 further extends the model to show a roaming scenario.

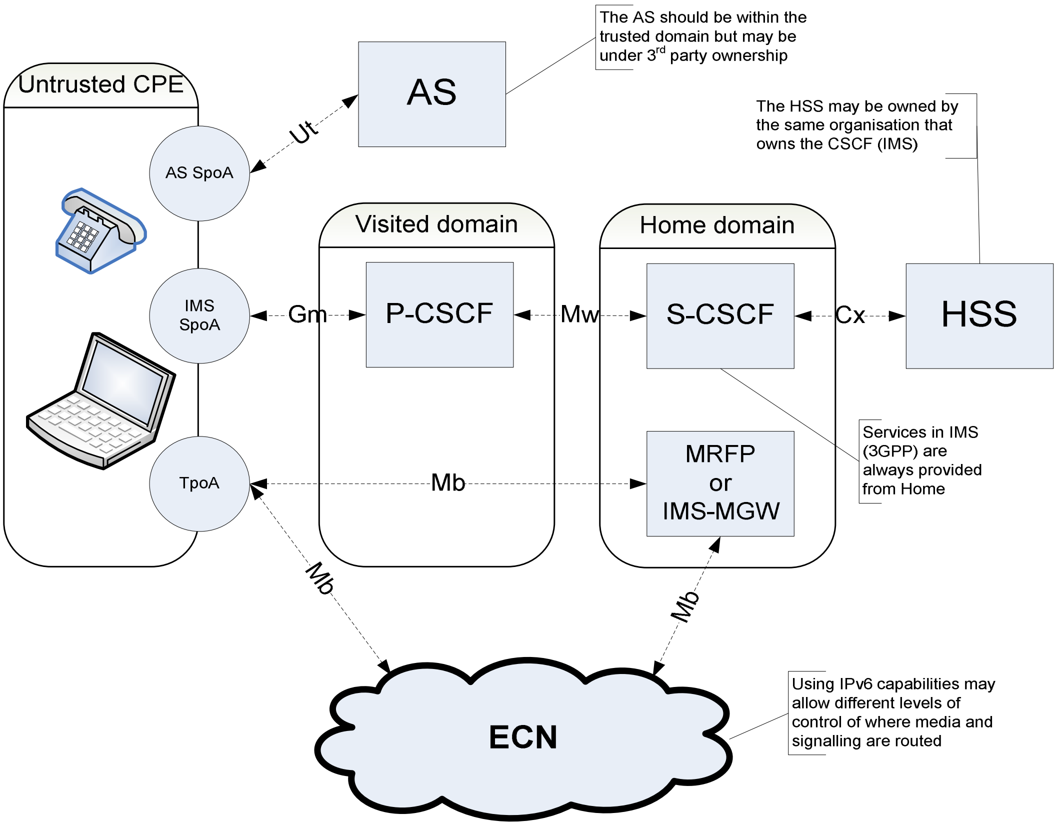

The AS should be within the trusted domain but may be under 3rd party ownership
Untrusted CPE
AS
Ut
AS SpoA
The HSS may be owned by the same organisation that owns the CSCF (IMS)
Visited domain
Home domain
IMS SpoA
Gm
P-CSCF
Mw
S-CSCF
Cx
HSS
Services in IMS (3GPP) are always provided from Home
TpoA
Mb
MRFP or IMS-MGW
Mb
Mb
ECN
Using IPv6 capabilities may allow different levels of control of where media and signalling are routed

Figure 5: Roaming scenario

4.1.3 Nomadic user security scenario

The actors in this scenario (see figure 9) are named Bob and Alice.

Alice has a multi-service terminal she usually uses at home. She normally uses a set of services offered by two service providers (ECS1 and ECS3 in figure 9). She has taken her terminal to a friend's house (Bob) and expects to use her services there as well. Alice connects her terminal to the network at Bob's house via some form of fixed or wireless access (WiFi) and is using services from her own service provider. Bob has a different transport network provider from Alice.

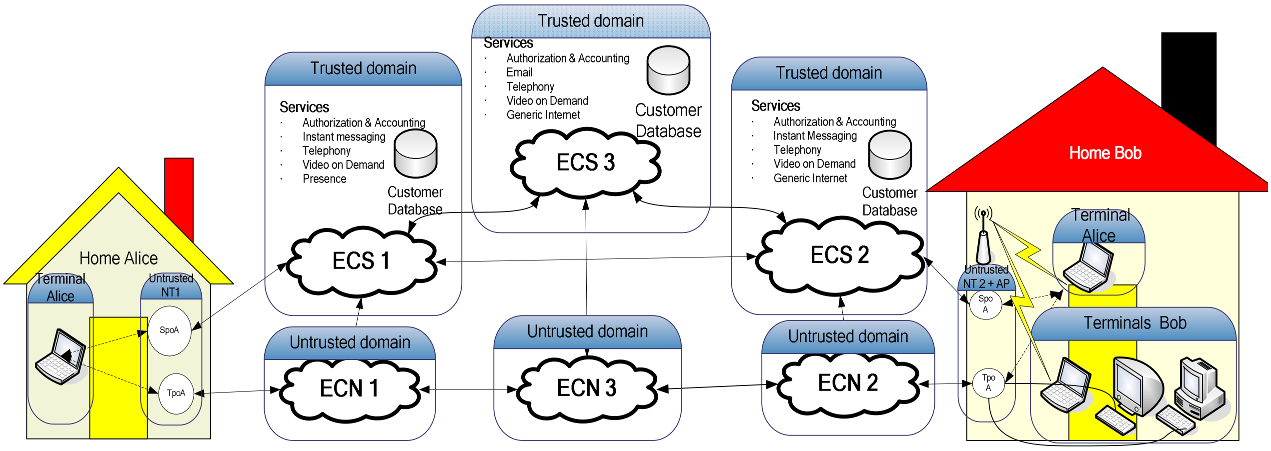


Figure 6: Nomadic user security scenario

Bob wants to be assured that allowing Alice to use his home network does not generate costs for him (Alice has to pay the charges for her service use). Furthermore Bob requires some assurance that Alice, and the actions of Alice's service provider, does not alter the risk of attack to the other terminals at Bob's home. Bob also requires some assurance that Alice and Alice's service provider should not block the other terminals in Bob's home from using their services. Alice requires some assurance that her communication should not be impeded by Bob's terminals. Bob's terminals should not be able to masquerade as Alice either during the time she is in Bob's home or afterwards. Alice may use her terminal to call the local emergency service, be connected to an appropriate emergency centre and provide the appropriate location information.

5 Threat and risk analysis

NOTE: The scope of this clause is only the functionality provided for NGN-R1 and has not been validated for additional functionality provided in NGN-R2 or NGN-R3 other than where specifically indicated in the text.

This clause analyzes NGN in terms of threats and carries out an analysis of risks according to the methodology defined in TS 102 165-1 [i.4].

5.1 PES Analysis

5.1.1 PES objectives and security objectives

The current draft of ES 282 002 [i.9] identifies some of the objectives for PES and these are restated here with respect to the actor making the statement.

Table 1: PES objectives

Actor (note 1)	Objective
Existing PSTN/ISDN service provider (note 2)	Seamless provision of service to customer base in presence of change of technology in the core network.
Packet transport technology provider (note 3)	To offer an alternative to circuit switched transports for point-to-point time critical services.
Aspirant NGN service provider	To adopt NGN ECN technology (packet based) whilst allowing slow changeover to NGN ECS technology.
NOTE 1: The end customer is not considered as an actor in PES although he may be considered a stakeholder. NOTE 2: This is a special case of an ECS. NOTE 3: This is a special case of an ECN.	

The security objectives for PES are bound by the conditions of the Framework Directive [i.15] and the Privacy Directive [i.16].

5.1.2 Stage 2 model of PES (UML)

The UML class diagram representing PES is given below.

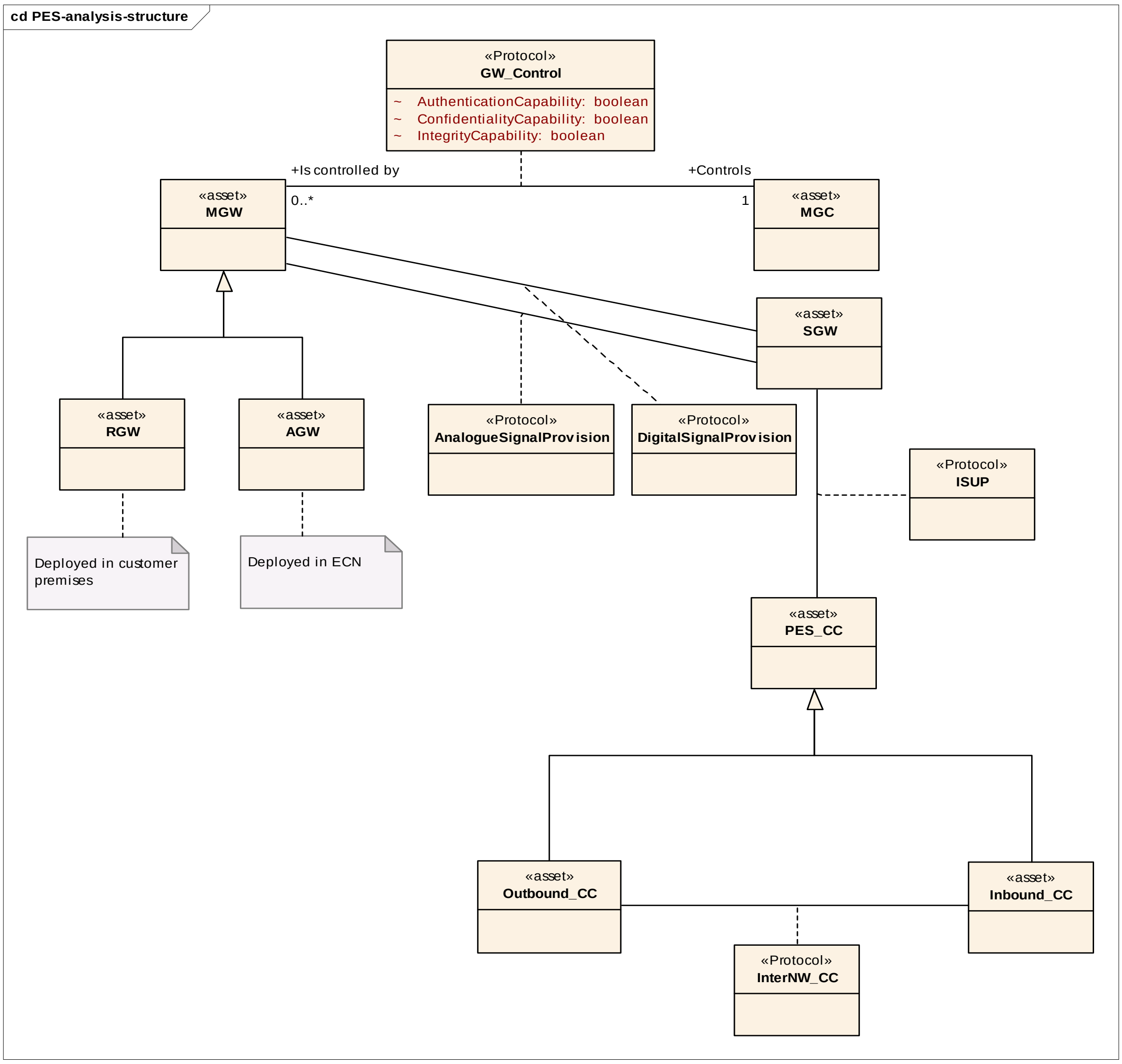


Figure 7: UML class diagram for PES

The UML model in figure 7 identifies the assets and the relationship between them for PES. The model of figure 7 is generic and does not imply a specific implementation. Figure 10 illustrates the specific application of the 2 generic protocols (H.248 as specified in ES 283 002 [i.11] for the Gateway control protocol and for the means of providing signalling from the analogue user line to the PES-CC, and SIP-I [i.12] for the Inter-network call control transfer protocol) in the available PES stage 3 definitions.

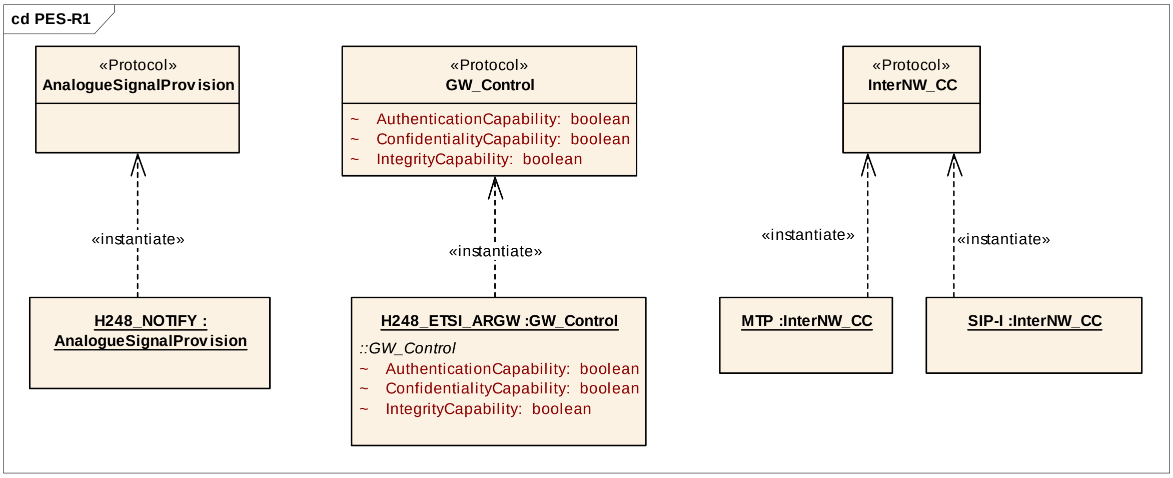

cd PES-R1
«Protocol»
AnalogueSignalProvision
«Protocol»
GW_Control
~ AuthenticationCapability: boolean
~ ConfidentialityCapability: boolean
~ IntegrityCapability: boolean
«Protocol»
InterNW_CC
«instantiate»
«instantiate»
«instantiate»
«instantiate»
H248_NOTIFY : AnalogueSignalProvision
H248_ETSI_ARGW :GW_Control
::GW_Control
~ AuthenticationCapability: boolean
~ ConfidentialityCapability: boolean
~ IntegrityCapability: boolean
MTP :InterNW_CC
SIP-I :InterNW_CC

Figure 8: Instances of the PES protocols

5.1.2.1 Identification of assets

The assets in PES (for stage 2 analysis) are:

- Media Gateway Function (MGW):
  - Residential MGW (RGW) in customer premises.
  - Access MGW (AGW) in network operator premises.
- Media Gateway Control Function (MGC).
- Call controller (CC):
  - Outbound call controller.
  - Inbound call controller.
- Protocols:
  - Between MGC and MGW.
- Between MGC and CC:
  - Between inbound and outbound CC.
  - Between UE and MGW.

5.1.2.2 Missing considerations in PES

5.1.2.2.1 ECN technology

The technology of the ECN is not fully described in the PES. However the NGN as a whole uses IPv4 and/or IPv6 as the core technology in the ECN.

Attacks on IP of any type will affect PES and so are not addressed specifically in the present document.

5.1.2.2.2 Protocol stack

The overall transmission chain and the invocation of protocols at points in the deployment chain is not fully described in PES.

5.1.2.2.3 Cardinality of relationships

The cardinality of relationships between objects in PES is not clear. The UML model in figure 7 addresses these where possible but these should be verified.

5.1.2.2.4 Deployment

There are a number of ways to deploy PES and a number of protocol choices that may be made. For example the MGC and PES_CC entities may be co-located and there will be no visible interface between MGC and PES_CC.

5.1.3 Points of attack in PES

5.1.3.1 Interfaces

The primary points of attack in PES are the open interfaces (considered here as communications paths) where data is transmitted.

NOTE: The secondary point of attack is the application itself which may be corrupt, or malicious. It is assumed for the first pass that the application software functions correctly and that attacks will be on data external to the application (e.g. configuration data) and on the interfaces to the application.

Table 2: Interfaces and their characteristics

Communication paths	Characteristics	Attributes transferred
Customer to MGW	Closed circuit	DTMF tones for called party identity Call continuation tones Call content
MGW to MGC	IP transfer	Responses to control messages
MGW to SGW		Interpreted DTMF tones (H.248 [i.21] package)
SGW to MGW		Instructions for sending call signalling tones
MGC to MGW		Gateway control messages
SGW to CC		ISUP message
Outbound CC to Inbound CC		ISUP message

5.1.3.2 Implicit relationships

There are a number of implicit relationships in PES which may be open to attack. These are explored further here.

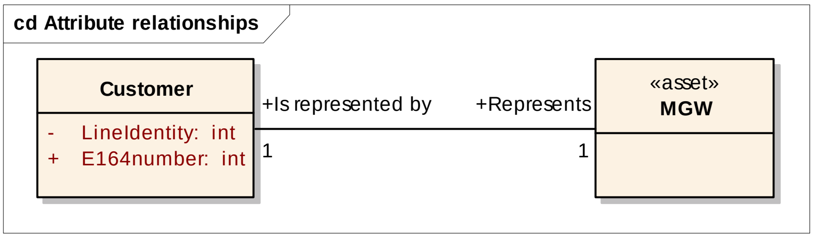


Figure 9: UML representation of customer to MGW relationship

The MGW acts on behalf of the customer and the customer requires that the MGW does not misrepresent the customer by modifying data belonging to (or leased to) the customer. For PES the primary customer identity is his E.164 number.

For analysis it is assumed that there is a one-to-one relationship of MGW and customer.

5.1.4 Risk analysis

5.1.4.1 Overview

This analysis works from the perspective of trying to identify which threats may be possible on the open interfaces. The weighting of risk is defined in the TVRA guidance but for this analysis it is sufficient to identify and quantify the potential of any threat being successful.

5.1.4.2 Interception

This threat means that an unauthorized party may learn information transferred or stored in PES. According to the penetration points the following threats can be distinguished.

5.1.4.2.1 Interception at the customer to MGW interface

There are essentially two scenarios to consider:

- MGW in customer premises.
- MGW in operator's premises.

In both scenarios it is assumed that the MGC is in the operator's premises (i.e. an MGC in the customer premises is not a valid scenario for PES).

For the purpose of attack it is assumed that the user signalling/traffic are sent over non-radiating wires that are routed in difficult to access areas (or where access is physically obvious).

Table 3: T-1: Attack potential for interception at the customer interface

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 week	1
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Moderate	4
Equipment	Standard	0
Total	Moderate - possible	7

5.1.4.2.2 Interception within the fixed network

For the purposes of attack it is assumed that the fixed network is physically difficult to penetrate and will be managed to identify break-ins. It is assumed that the protocols and signalling are defined with respect to publicly available specifications.

Table 4: T-2: Attack potential for interception at the customer interface

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 month	4
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Difficult	12
Equipment	Standard	0
Total	High - unlikely	18

5.1.4.3 Manipulation

NOTE: Extend manipulation for targeted and non-targeted attacks. Review the weightings.

5.1.4.3.1 Manipulation at the customer interface

There are essentially two scenarios to consider:

- MGW in customer premises.
- MGW in operator's premises.

In both scenarios it is assumed that the MGC is in the operator's premises (i.e. an MGC in the customer premises is not a valid scenario for PES).

For the purpose of attack it is assumed that the user signalling/traffic are sent over non-radiating wires that are routed in difficult to access areas (or where access is physically obvious).

Table 5: T-3: Attack potential for manipulation at the customer interface

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 week	1
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Moderate	4
Equipment	Standard	0
Total	Moderate - possible	7

5.1.4.3.2 Manipulation in the fixed parts of the network

In contrast to the customer interface in the fixed parts of the network all kinds of manipulation are possible:

- deletion;
- reordering; and
- insertion of data is possible without restriction.

The underlying attacks can be in principle at least the same as for manipulation at the radio interface, with the following attacks added.

- Manipulations can be done in the following ways:
    - an attacker can use some equipment infiltrated into any interface of the system to manipulate the data and voice signals being transferred there;
    - deletion can be carried out, e.g. by physical action like wire-cutting, but also by rerouting of the data (e.g. by manipulation of the data header);
    - an attacker, who has access to an entity in the system, e.g. the MGC/SGW, can manipulate the data or voice signals being processed or stored.

Table 6: T-4: Attack potential for manipulation in the fixed network

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 month	4
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Moderate	4
Equipment	Specialized	3
Total	Moderate - possible	13

5.1.4.3.3 Manipulation in links between networks

In addition to those manipulations considered in the fixed parts of the network there is further scope for attack between networks (although still "fixed"). These manipulations have different attack potential depending on the implementation of the interface.

Table 7: T-5: Attack potential for manipulation between networks (without SEG)

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 week	0
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Moderate	4
Equipment	Standard	0
Total	Basic - likely	6

Table 8: T-7: Attack potential for manipulation between networks (with SEG)

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 week	0
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Moderate	12
Equipment	Standard	0
Total	Moderate - possible	14

5.1.4.4 Denial-of-Service

This threat means that an unauthorized party may deny system availability to authorized parties.

There are essentially two scenarios to consider:

- Attack of public interfaces.
- Attack of private interfaces.

Table 9: T-8: Attack potential for denial-of-service on publicly addressable interfaces

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 week	0
Expertise	Layman	0
Knowledge of TOE	Public	0
Access to mount attack	Easy	1
Equipment	Standard	0
Total	No rating - Likely	1

Table 10: T-9: Attack potential for denial-of-service on non-publicly addressable interfaces

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 week	0
Expertise	Layman	0
Knowledge of TOE	Public	0
Access to mount attack	Difficult	12
Equipment	Standard	0
Total	Moderate - Possible	12

5.1.5 PES unwanted incidents

The unwanted incidents such as loss of availability, loss of integrity, loss of confidentiality as a result of the PES trust assumptions as given in clause 5.1.4.2.1 are considered to be unlikely.

5.1.6 Existing PES security provisions

The existing PES security model is shown in figure 1 of [i.17] and the security provisions for use of H.248 [i.21] for that model are also described in ES 283 002 [i.11].

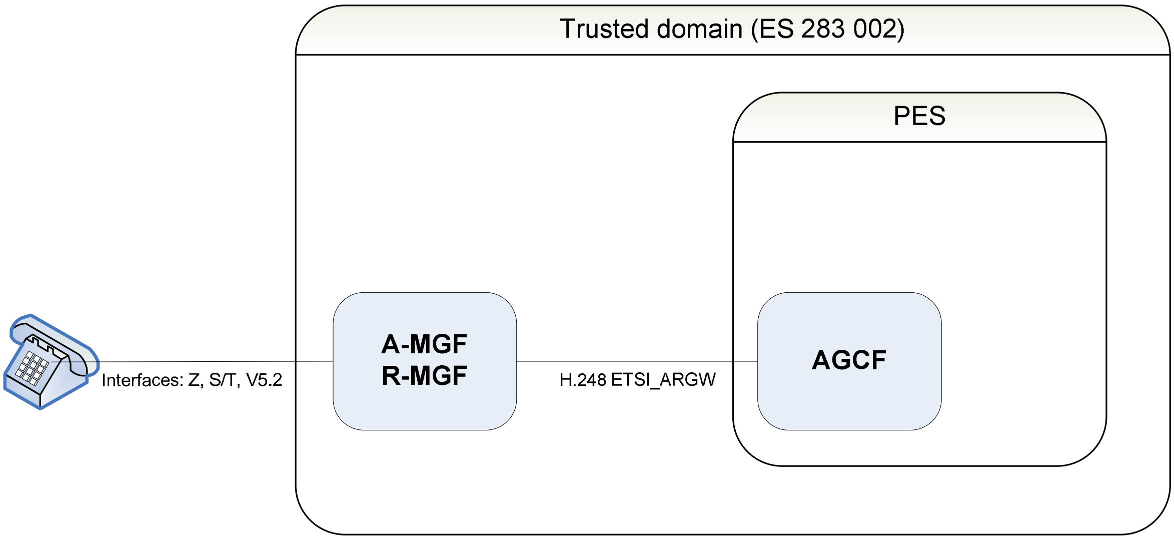


Figure 10: H.248 deployment model as specified in ES 282 002 [i.9]

As shown in figure G.4, the trust domain is assumed to include the AGCF as well as the A-MGF, R-MGF in the in the operator's domain.

5.1.7 Security capabilities in PES

5.1.7.1 H.248 ETSI_ARGW

5.1.7.1.1 Authentication

Not provided.

The rationale for no explicit authentication function/capability in H.248 [i.21] ETSI_ARGW is that the Access Gateway is under the control of the ECN&S providing service. The provisioning mechanism for the telephone line/service establishes the identity of the customer. The means to establish identity vary between providers but may include checks for documentary proof of identity and address. Post provisioning there are no further authentication checks made. The fixed network assumes a "dumb" end-user device (i.e. does not control the protocol state machine and does not send full signalling), and also assumes that access to the physical transmission media is difficult.

5.1.7.1.2 Confidentiality of signalling

Not provided.

Rationale is as for authentication.

5.1.7.1.3 Confidentiality of traffic

Not provided.

Rationale is as for authentication.

5.1.7.1.4 Integrity of signalling

Not provided.

Rationale is as for authentication.

5.1.7.1.5 Integrity of traffic

Not provided.

Rationale is as for authentication.

5.1.8 Role of NGN subsystems in PES

5.1.8.1 Transport plane

5.1.8.1.1 NASS

No explicit role in PES.

5.1.8.1.2 RACS

The RACS lies on the interface between the service plane and the transport plane. RACS is used in PES to ensure that the IP network provides appropriate RTP streams for the carriage of 64k-TDM traffic.

5.1.8.1.3 Transport elements

No role defined for PES in NGN-R1.

5.1.8.2 Service plane

5.1.8.2.1 IMS

No role defined for PES in NGN-R1.

5.1.8.2.2 PSS

No role defined for PES in NGN-R1.

5.1.8.3 Recommendations

The role of the transport network and means to secure it need to be addressed. It is recognized that the Security Gateway (SEG) functions described in TS 133 203 [i.19] can be deployed to protect the signalling links (using IPsec ESP in Tunnel Mode). It is noted that the SEG as currently defined does not protect media but work is underway to address this in 3GPP.

There is a risk to availability not addressed by TS 133 203 [i.19] if the addresses of the point of interconnection are in the public domain. The denial of service attacks are more difficult to mitigate against and work has to be done in this area. In particular the use of public address space at the point of interconnect should be avoided.

5.2 Analysis of NASS

See annex I of the present document.

5.3 Analysis of RACS

See annex A of the present document.

5.4 Analysis of NGN-IMS

FFS.

5.5 Analysis of DNS and ENUM in NGN

See annex C of the present document.

5.6 Analysis of SIP in NGN

Void.

6 Conclusions for NGN-R1

Table 11 shows that all critical threats (attack potential rating less than or equal to 14) have been addressed by either a specific technical countermeasure or by the limited functionality inherent in Release 1. This table will need to be reviewed as a when new functionality is incorporated in further releases of the TISPAN specifications or when the present document is further updated.

For each identified security vulnerability, table 11 identifies some example security requirements. Table 11 also identifies security countermeasures against the security vulnerabilities.

NOTE: The shown requirements in table 11 are not meant to be complete; TS 187 003 [i.7] may provide more security requirements.

Table 11: Mapping of security threats to requirements and to countermeasures

Threat Identifier	Security Threat (0 - 14) Subsystem/Feature: short description	Attack potential rating	Impact	Occurrence likelihood	Risk	Primary NGN Security Requirement [i.6]	Countermeasure as defined
T-8	PES: Attack potential for denial-of-service on publicly addressable interfaces	1 (highly likely)	3 (high)	2 (possible)	6 (Critical)	R-AD-1 R-AD-3	Not applicable according to trust assumption in NGN R1.
T-16	NASS-IMS bundled: IP Spoofing	1 (highly likely)	2 (medium)	2 (possible)	4 (Major)	R-AA-24 R-AA-13 R-NF- 2	See clause 5.2.1.4.4.2.
T-11	NASS-IMS bundled: Interception at the customer interface, air interface present	4 (highly likely)	2 (medium)	2 (possible)	4 (Major)	R-CD-18	Security protection along the e1 IF; see [i.7].
T-14	NASS-IMS bundled: Attack potential for manipulation at the customer interface, air interface present	4 (highly likely)	2 (low)	2 (possible)	4 (Major)	R-CD-13	Security protection along the e1 IF; see [i.7].
T-18	NASS-IMS bundled: Attack potential for manipulation at the customer interface (denial-of-service)	4 (highly likely)	1 (low)	2 (possible)	2 (Minor)	R-AD-1	Not in scope of TISPAN NGN.
T-19	NASS-IMS bundled: "line-id poisoning" attack	4 (highly likely)	2 (medium)	2 (possible)	4 (Major)	R-AA-24 R-AA-13 R-NF- 2	See 3GPP TR 33.803 [i.33].
T-5	PES: Attack potential for manipulation between networks (without SEG)	6 (highly likely)	3 (high)	1 (unlikely)	3 (Minor)	R-CD-2	Use of the Security Gateway (SEG) as defined in [i.13].
T-1	PES: Attack potential for interception at the customer interface	7 (possible)	1 (low)	1 (unlikely)	1 (Minor)	R-CD-15 R-CD-16	Not applicable according to trust assumption in NGN R1.
T-3	PES: Attack potential for manipulation at the customer interface	7 (possible)	1 (low)	1 (unlikely)	1 (Minor)	R-CD-13	Not applicable according to trust assumption in NGN R1.
T-10	NASS-IMS bundled: Attack potential for interception at the customer interface, no air interface	7 (possible)	1 (low)	2 (possible)	2 (Minor)	R-CD-20	Security protection along the e1 IF; see [i.7].
T-13	NASS-IMS bundled: Attack potential for manipulation at the customer interface, No air interface present	7 (possible)	1 (low)	2 (possible)	2 (Minor)	R-CD-15	Security protection along the e1 IF; see [i.8].
T-9	PES: Attack potential for denial-of-service on non-publicly addressable interfaces	12 (possible)	1 (low)	1 (unlikely)	1 (Minor)	R-AD-3	Security protection along the Mj and Mg interfaces; see [i.7].

Threat Identifier	Security Threat (0 - 14) Subsystem/Feature: short description	Attack potential rating	Impact	Occurrence likelihood	Risk	Primary NGN Security Requirement [i.6]	Countermeasure as defined
T-4	PES: Attack potential for manipulation in the fixed network	13 (possible)	1 (low)	1 (unlikely)	1 (Minor)	R-CD-16	Security protection along the Mj and Mg interfaces; see [i.7].
T-7	PES: Attack potential for manipulation between networks (with SEG)	14 (possible)	1 (low)	1 (unlikely)	1 (Minor)	R-CD-16	Use of the Security Gateway (SEG) as defined in [i.13].
T-12	NASS-IMS bundled: Attack potential for interception at the customer interface (e1 IF)	18 (unlikely)	1 (low)	1 (unlikely)	1 (Minor)	R-CD-8	No technical countermeasure defined in Release 1.
T-2	PES: Attack potential for interception at the customer interface	18 (unlikely)	1 (low)	1 (unlikely)	1 (Minor)	R-CD-19	No technical countermeasure defined in Release 1.
T-15	NASS-IMS bundled: Attack potential for manipulation at the customer interface (e1 IF)	18 (unlikely)	2 (low)	1 (unlikely)	2 (Minor)	R-CD-15	No technical countermeasure defined in Release 1.
T-17	NASS-IMS bundled: Invalidation of IP address not signalled	16 (unlikely)	1 (low)	1 (unlikely)	1 (Minor)	R-CD-13 R-CD-8	No technical countermeasure defined in Release 1.

Annex A: TVRA of RACS in NGN-R2

NOTE 1: The scope of this annex is only the functionality provided for NGN-R2.

NOTE 2: The detail requirements identified in this analysis are also stated in TS 187 001 [i.6].

A.1 Scope of the TVRA

The role of the TVRA is to identify the risk presented to the NGN by the RACS and the risk offered to the RACS by the NGN. The TVRA documents and specifies the security objectives for both the RACS and the NGN it exists within, similarly the TVRA documents and specifies the security requirements for the RACS and the NGN it exists within. The means of performing the TVRA is defined in TS 102 165-1 [i.4] and the specific means of defining objectives and requirements is defined in TR 187 011 [i.34]. The role of TVRA in standardization is defined with respect to the "design for assurance" paradigm that has been developed from analysis of the application of the Common Criteria for Information Security Assurance in EG 202 387 [i.1].

The conduct of a TVRA requires a critical analysis of a system and may identify faults in the system design that require correction to meet the system and security objectives.

A.2 Identification of the ToE

A.2.1 Overview

The ToE describes RACS and its environment in sufficient detail to unambiguously identify the internal and external components, information flows, and intended use.

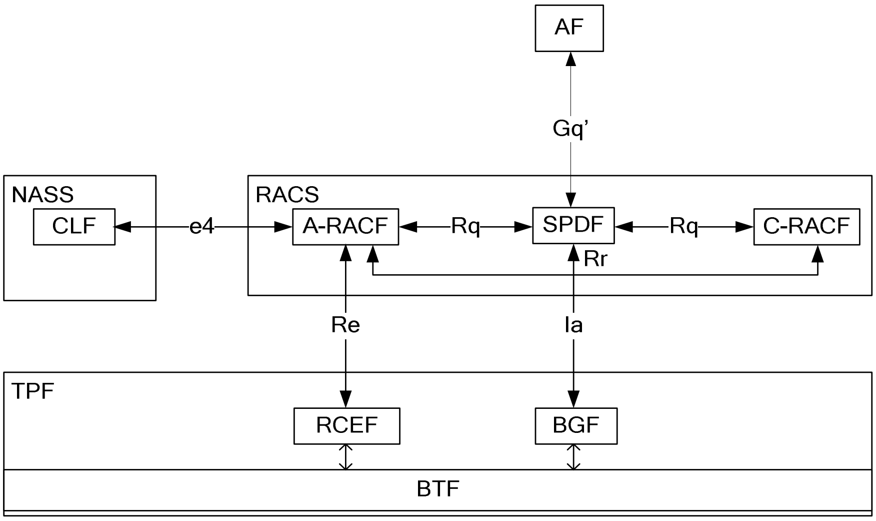
RACS in the NGN offers a suite of procedures and mechanisms to allow:

- policy-based resource reservation;
- policy-based admission control.

NOTE 1: In addition as the resources may be reserved and charging records maintained RACS enables the Accounting dimension of a AAA service.

These procedures and mechanisms apply for both unicast (point to point) and multicast (point to multipoint) traffic, and apply in both access networks and core networks.

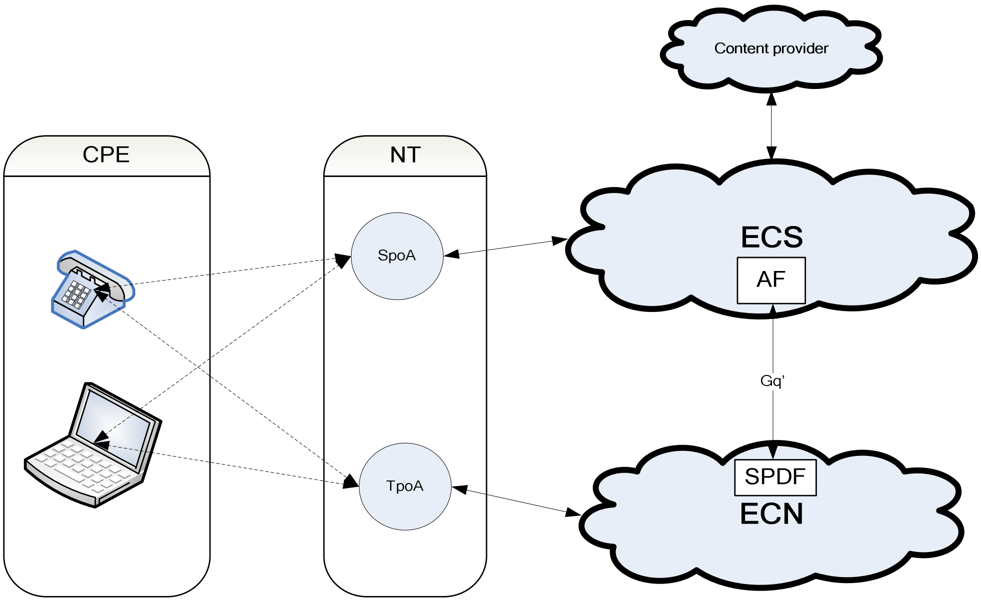
The ToE of RACS are the functional entities Access-Resource and Admission Control Function (A-RACF), Core-Resource and Admission Control Function (C-RACF) and Service Policy Decision Function (SPDF), and the reference points e4, Rr, Re, Rq, Rd', Ri', Gq' and Ia which interconnect them to the ToE environment. The information transferred on these reference points including necessary information from the communicating party are also part of the ToE.



NOTE 1: Reference points Rd' and Ri' between instances of SPDF are not shown.
NOTE 2: The BTF is shown for completeness only, there is no direct link from RACS to BTF.
NOTE 3: The UE is considered on the left hand side of the diagram with the core network at the right hand side.

Figure A.1: RACS functional architecture derived from ES 282 003 [i.10]

In the context of the regulatory model of NGNs, the ECN&S model, shown in figure 1 (clause 4 of the present document) the RACS ToE fits as shown in figure A.2.



NOTE: The RACS, NASS and TPF co-exist within the ECN.

Figure A.2: RACS in context of ECN&S

The ToE environment (security environment) is made up of the Application Function (), Network Access SubSystem (NASS) and the Transport Processing Functions (TPF) which is a grouping of Resource Control Enforcement Function (RCEF), Border Gateway Function () and Basic Transport Function ().

NOTE 2: The AF is in most cases an instance of a SIP-server modelled as an IMS Call Session Control Function (CSCF).

A.2.2 Scenarios for analysis and derivation of ToE

A.2.2.1 Summary

The ToE is considered with respect to the deployment scenarios outlined in table A.1 and given in expanded form in clauses A.2.2.2 through A.2.2.5.

Table A.1: Summary of scenarios for ToE extraction

No.	Scenario description	Exposed reference points (see notes 2 and 3)	Exposed assets (see notes 1 and 4)
1	Service-based Policy Decision and Admission Control Functions performed within a single trust domain	Gq'	AF,SPDF Data in each of Resource reservation request; Resource Modification Request; Resource Request/Modification Confirmation; Resource Release Request; Abort Resource Reservation
2	Service-based Policy Decision and Admission Control Functions handled separately by NGN operators situated in two different trust domains	Gq' Ri'	AF,SPDF Data in each of Resource reservation request; Resource Modification Request; Resource Request/Modification Confirmation; Resource Release Request; Abort Resource Reservation
3	Service-based Policy Decision and Admission Control Functions distributed by NGN operators across two trust domains	Gq' Ri' E4	AF,SPDF, NASS, x-RACF Data in each of Resource reservation request; Resource Modification Request; Resource Request/Modification Confirmation; Resource Release Request; Abort Resource Reservation; Access Profile Push; Access Profile Pull; IP Connectivity Release Indication
4	Service-based Policy Decision and Admission Control Functions distributed by NGN operators across several (more than two) trust domains	Gq' Ri' E4 Re	AF,SPDF, NASS, A-RACF, RCEF. Data in each of Resource reservation request; Resource Modification Request; Resource Request/Modification Confirmation; Resource Release Request; Abort Resource Reservation; Access Profile Push; Access Profile Pull; IP Connectivity Release Indication
NOTE 1: Both push and pull capabilities are considered in the assets that are exposed. NOTE 2: Whilst the Ia reference point was never envisaged to be external the specification does not preclude this. NOTE 3: The Gq' reference point is considered to lie between the facilities of a core operator and a RACS operator and is only exposed if the RACS operator and the Core operator are different. NOTE 4: The NASS is not decomposed in this analysis.			

A.2.2.2 Single trust domain deployment scenario

In this scenario all of the NASS, RACS and TPF entities exist in a single trust domain as would be the case for a conventional single ECN offering all the network services through a single access point. In this scenario the Gq' reference point, and the information transferred across it, is the only exposed reference point and when modelled as an interface represents a single attack interface.

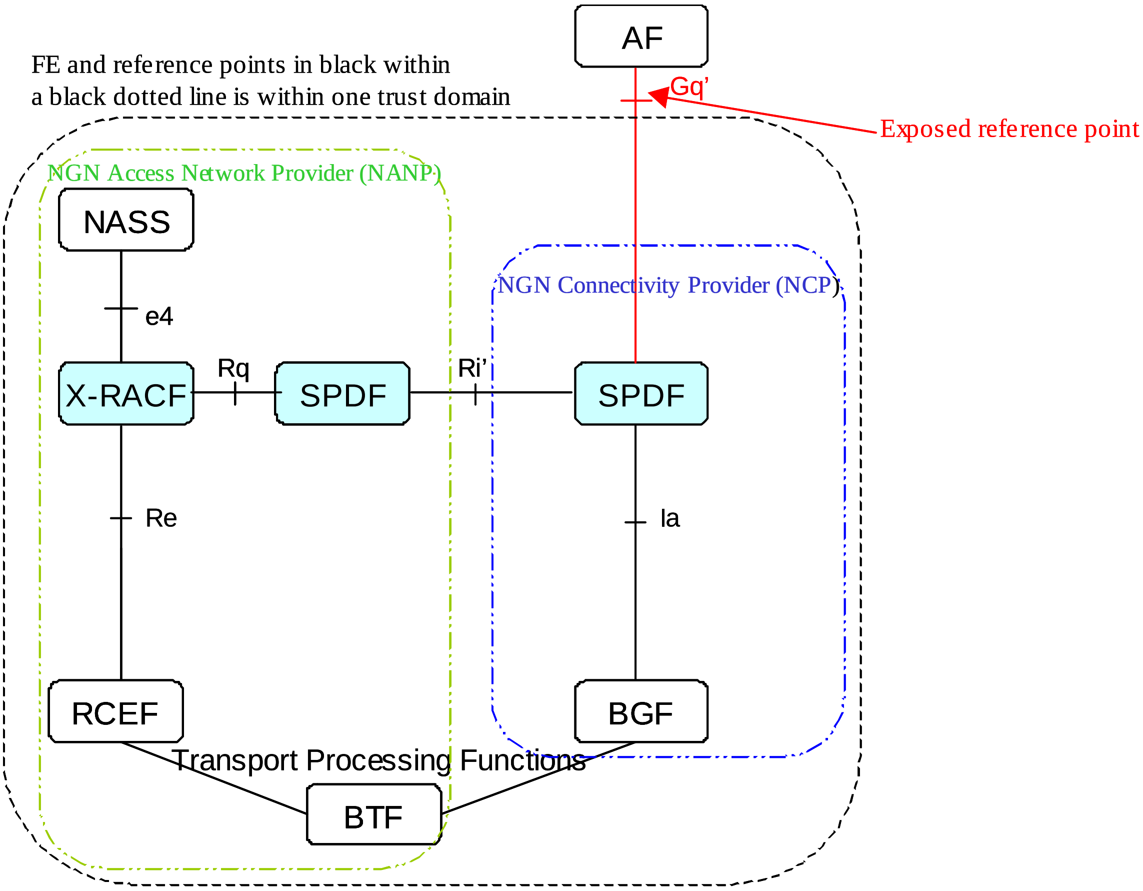

FE and reference points in black within
a black dotted line is within one trust domain
AF
Gq'
Exposed reference point
NGN Access Network Provider (NANP)
NASS
e4
X-RACF
Rq
SPDF
Ri'
NGN Connectivity Provider (NCP)
SPDF
Re
Ia
RCEF
BGF
Transport Processing Functions
BTF

Figure A.3: RACS ToE deployment scenario 1

The information flows visible at the Gq' reference point are:

- Resource reservation request.
- Resource Modification Request.
- Resource Request/Modification Confirmation.
- Resource Release Request.
- Abort Resource Reservation.

A.2.2.3 Two separate trust domains deployment scenario

Deployment scenario 2 represent a deployment of RACS wherein the ECN domain is split between two operators playing the roles of NGN Access Network Provider (NANP) and NGN Connectivity Provider (NCP). Figure A.4 illustrates this scenario with the service-based policy decisions made by the NCP and the admission control functions by the NANP. The admission control functions relevant for this scenario are:

- Admission Control based on access user profile.
- Admission Control based on available resources over the last mile (access network segment).
- Admission Control based on Security Policy profile.
- Admission Control based on available resources over the aggregation network segment.

However, in cases where there is a many to many relationship between NANP and NCP, NANP may have to perform some service-based policy control thus there will be two instances of SPDF (one each in NANP and NCP) and this exposes reference point Ri'.

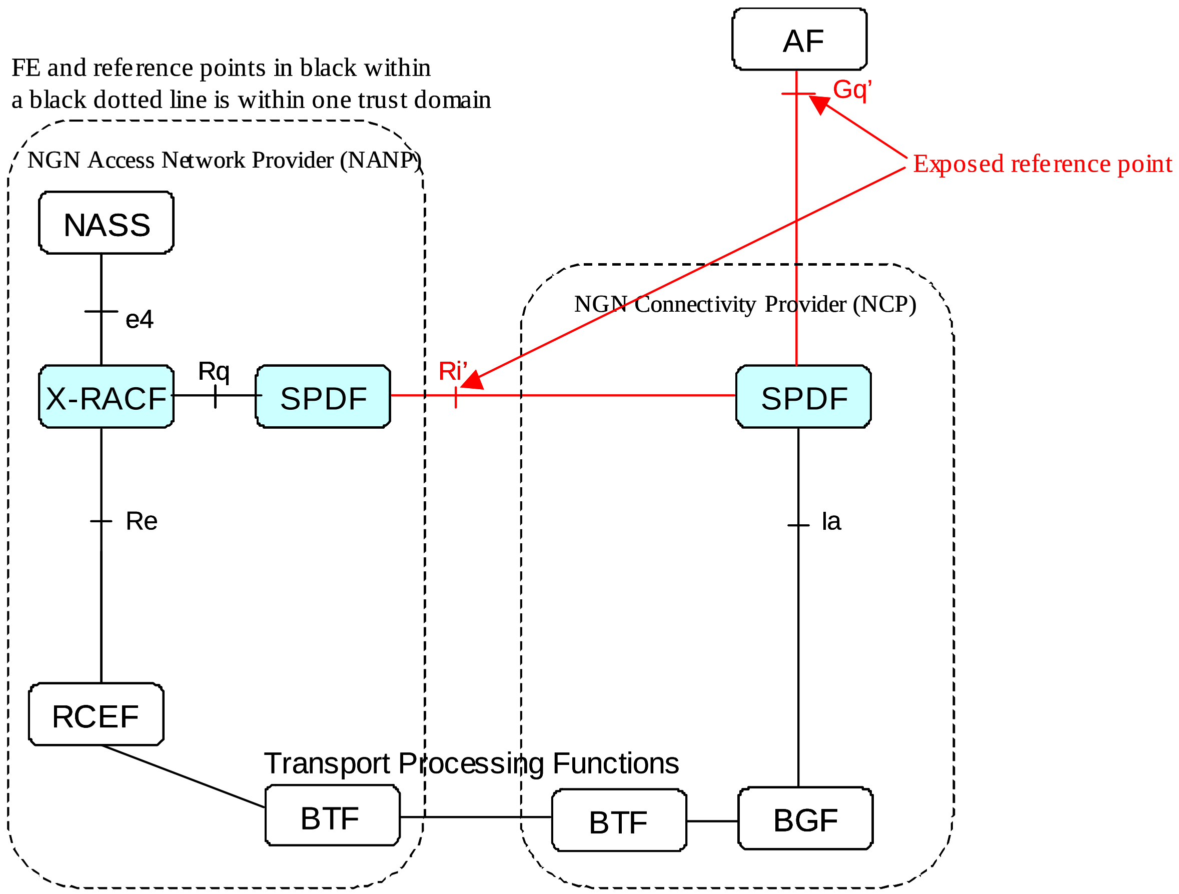

FE and reference points in black within
a black dotted line is within one trust domain
AF
Gq'
Exposed reference point
NGN Access Network Provider (NANP)
NASS
e4
X-RACF
Rq
SPDF
Ri'
NGN Connectivity Provider (NCP)
SPDF
Re
Ia
RCEF
Transport Processing Functions
BTF
BTF
BGF

Figure A.4: RACS ToE deployment scenario 2

A.2.2.4 Two collaborating trust domains deployment scenario

Deployment scenario 3 represents a scheme wherein two different NGN operators take the role of NGN Access Network Provider (NANP) and NGN Connectivity Provider (NCP) respectively. Each operator performs some service-based policy decisions and some admission control functions, i.e. the NANP performs admission control decisions related to the access user profile and the available resources on the access network segment, and the NCP performs admission control decisions based available resources on the core network segment.

In comparison to scenario 2 this scenario introduces a potential exposure of reference point e4 where user profiles are exchanged between the A-RACF and CLF. In this particular scenario e4 is also extended to an exchange between C-RACF and CLF where C-RACF lies in the NCP.

The information flows visible at the e4 reference point are:

- Access Profile Push.
- Access Profile Pull.
- IP Connectivity Release Indication.

The reference points exposed and when implemented in protocol become visible as attack interfaces for this scenario are e4, Gq' and Ri'.

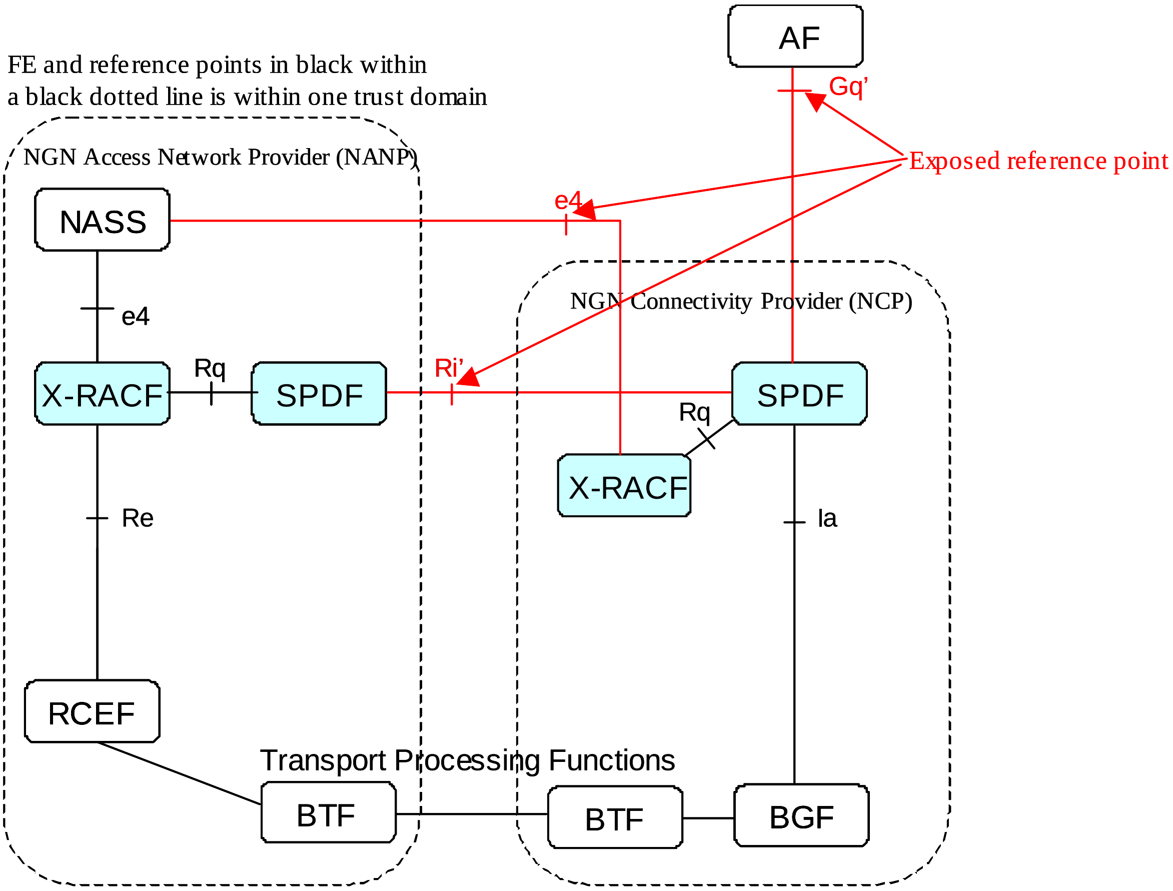
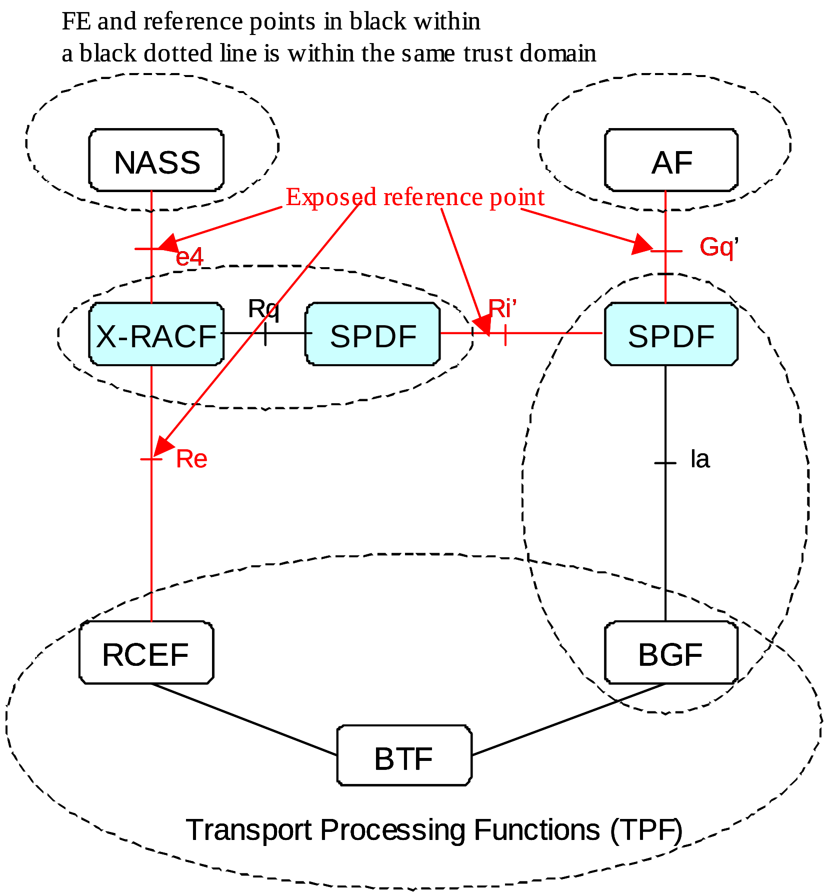

FE and reference points in black within
a black dotted line is within one trust domain
NGN Access Network Provider (NANP)
NASS
e4
X-RACF
Rq
SPDF
Re
RCEF
Transport Processing Functions
BTF
AF
Gq'
Exposed reference point
e4
Ri'
NGN Connectivity Provider (NCP)
SPDF
Rq
X-RACF
Ia
BTF
BGF

Figure A.5: RACS ToE deployment scenario 3

A.2.2.5 Multi trust domain deployment scenarios

Deployment scenario 4 represents the worst-case scenario for the distribution of the functional entities of RACS and the exposure of the relevant reference points as attack interfaces by further separation of responsibility in the ECN. This scenario opens all reference points that may be considered to be deployed between domains (administration, ownership or trust domains) as exposed with the likelihood of them being implemented as attack interfaces. The impact over scenario 3 is to extend the exposed reference points to include Re between RECF and x-RACF.


FE and reference points in black within
a black dotted line is within the same trust domain
NASS
AF
Exposed reference point
e4
Gq'
X-RACF
Rq
SPDF
Ri'
SPDF
Re
Ia
RCEF
BGF
BTF
Transport Processing Functions (TPF)

NOTE: The reference point Ia is in most cases intra trust domain although it is technically possible for Ia to be inter trust domain. However, this is not very likely as this means that NAT functions will be in different administrative domains.

Figure A.6: RACS ToE deployment scenario 4

A.3 Analysis of ToE elements

A.3.1 Transport processing functions

The Transport Processing Functions (TPF) in the NGN are abstractions of the IP network with specific capabilities to provide QoS. Within the TPF functional layer are two entities that act on instruction of RACS:

- RCEF enforces the traffic policies by means of which RACS can assure the use of the resources.

NOTE: The RCEF is usually deployed in IP Edge Nodes (IP Access Nodes) and is therefore sited close to the User Equipment.

- BGF performs policy enforcement functions and NAT functions at the border between two network segments. There are two specializations of the BGF:
  - the Core BGF (C-BGF) that sits at the boundary between an access network and a core network, at the core network side;
  - the Interconnection BGF (I-BGF) that sits at the boundary between two core networks.

A.3.2 SPDF

The SPDF acts as the policy decision point for each administrative domain it resides in. It may also communicate with an interconnected SPDF located in an adjacent administrative domain for a reservation request. Where decisions require the involvement of two or more SPDFs it is important to be able to identify the decision maker and the decision supporter roles.

The SPDF makes policy decisions by using service policy rules defined by the network operator, however the interface between AF and SPDF does not carry these rules and it is understood that they are determined in a commercial agreement between operators of RACS (ECN operators) and providers of services (ECS operators) and thus provided off line. The ability to strongly identify, and to authenticate, providers of services to operators of RACS is not given in the current specifications, hence there is a potential for masquerade of AF to SPDF.

The SPDF acts to hide the underlying network topology from the service (ECS) and from any interconnected ECN. The interface between ECS and ECN enabled by RACS thus is able to offer to the ECS a consistent answer to a reservation request independently of the actual technology of the ECN.

There is an assumption of a discovery mechanism for the SPDF to determine the appropriate entity or entities among A-RACF, BGF and interconnected SPDFs to service the request received from the AF, however this discovery mechanism is not detailed and depending on its implementation may allow data manipulation attacks.

The SPDF does not require access to user profile information although within the ECN as a whole such information is held in NASS and may be made available to RACS to supplement the policy rules in the SPDF. The management of such data in RACS is not explicitly defined and may allow data manipulation attacks (e.g. data modification, data replay).

A.3.3 RACF

The x-RACF are generic functions that maintain resource models specific to an access technology and that provide a common interface to the provision of resources independently of the technology. Although there is only one abstraction of the x-RACF in practice multiple x-RACF may be arranged in an hierarchical structure with the top tier x-RACF providing the e4 reference point.

Data is not explicitly maintained in RACS although the x-RACF may use data from the NASS CLF component to assist in resource reservation enforcement. Such data when stored needs to be protected from manipulation attacks and in particular needs to be kept fresh (a barrier to replay attacks).

A.3.4 Reference points

Each reference point has been analysed with respect to the risk presented when (if) exposed and the analysis is presented in table A.2.

Table A.2: Risk consideration of reference points

Ref.Pt	Risk considerations	Risk analysis recommendation
E4	E4 is the link between NASS and RACS and therefore is considered as open as the link between two subsystems. Access Profile Push: Access Profile Pull: IP Connectivity Release Indication: The main interaction across e4 is that of access profile exchange (either by push or pull) and indication of release of IP connections.	If RACS and NASS both exist within a single ECN (as in scenarios 1,2,3) then e4 should never be exposed.
Gq'	The Gq' reference point is considered to lie between the facilities of a core operator and a RACS operator and is only exposed if the RACS operator and the Core operator are different.	The regulatory framework requires separation of ECN and ECS and as RACS belongs to the ECN domain with the AF belonging to the ECS domain it is expected that Gq' will be exposed on a realized interface.
Rd'	Exists between instances of SPDFs but not defined in NGN-R2 and not believed to be exposed in any scenario.	Not exposed and not analysed further.
Ri'	Exists between instances of SPDFs and may be exposed if two instances of RACS have to communicate to exchange policy data. The Ri' Reference point allows the SPDF in the Originating Domain to relay a reservation request to an SPDF in a serving (connected) domain.	The Ri' reference point is exposed over the DIAMETER based protocol stack in a similar fashion to Gq' and e4. The stage 2 definition of Ri' in ES 282 003 [i.10], and the stage 3 definition in TS 183 017 [i.35] are both incomplete at the time of this analysis. However as the originating SPDF relays the message the risk is of the AF trusting the response received over Gq' and therefore a need for the SDPF connected to AF to be assured of the integrity and source of the relayed response. Similarly the interconnected SDPF has to be assured of the integrity and source of the relayed request.
Rr	Exists between instances of x-RACF and not believed to be exposed in any scenario.	Not exposed and not analysed further.
Re	Re is only exposed in the event that the RACS and transport functions themselves are separated. This seems to contradict the relationships considered for ECNs (where NASS and RACS and the IP network are part of the ECN) but exposes a number of undefined information flows.	There is no data to analyse as the exposure occurs as per scenario 4 where all of RACS and the ECN elements are distributed.
Ia	The BGF lies at the edge of the transport, i.e. at the NNI edge of the ECN and is intended to be an unexposed element of the ECN receiving policy input from the SPDF.	The Ia reference point was never envisaged to be external the specification does not preclude this.

A.3.5 Information flow analysis

The security analysis of information flows considers first of all the stage 2 abstractions and then the stage 3 implementation and the analysis is presented in tables A.3 and A.4.

Table A.3: Stage 2 information flows for RACS

Information flow	Direction	Content	Analysis
Resource reservation request	AF to SPDF	AF Identifier; Resource Reservation Session ID; Subscriber-ID (optional); Globally Unique IP Address (optional) Assigned IP Address, Address Realm, Requestor Name, Service Class; Service Priority (optional); Charging Correlation Information (CCI) (optional); Duration of Reservation (optional); Authorization package ID (optional); Media Description Media Type, Media ID, Media Priority (optional); Traffic Flow Parameters Direction, Flow ID, IP Address, Ports, Protocols, Bandwidth, Reservation Class (optional), Transport Service Class (optional)), Commit Id Overbooking request indicator (optional)	The presence of a subscriber identity requires that this information flow is protected from eavesdropping in order to ensure the non-exposure of personal data on open interfaces. It is noted that the protocol for the AF to SPDF link is DIAMETER which is a AAA framework and that itself relies on the presence of security mechanisms (e.g. IPsec, TLS) to provide security. The presence of the CCI data suggest a requirement to ensure this has not been manipulated to prevent billing fraud.
Resource Modification Request	AF to SPDF	AF Identifier, Resource Reservation Session ID, Requestor Name, Service Class, Duration of Reservation (optional), Charging Correlation Information (optional), Service Priority (optional), Authorization package ID (optional), Media Description; Media Type, Media ID, Media Priority (optional), Traffic Flow Parameters Direction, Flow ID, IP Addresses, Ports, Protocols, Bandwidth, Reservation Class (optional), Transport Service Class (optional), Commit ID	As above
Resource Request Confirmation	SPDF to AF	AF Identifier, Resource Reservation Session ID, Duration of Reservation Granted (optional), Overbooking confirmation indicator (optional)	If this message is blocked the AF will retry and may lead to a denial of service.
Resource Modification Confirmation	SPDF to AF	AF Identifier, Resource Reservation Session ID, Duration of Reservation Granted (optional), Overbooking confirmation indicator (optional)	
Resource Release Request	AF to SPDF	AF Identifier Resource Reservation Session ID	
Abort Resource Reservation	AF to SPDF	AF Identifier, Resource Reservation Session ID Time Stamp	

Information flow	Direction	Content	Analysis
Access Profile Push	NASS to RACS	Subscriber ID, Physical Access ID (optional), Logical Access ID, Access Network Type, Globally Unique IP Address; Assigned IP Address Address Realm, QoS Profile Information (optional); Transport Service Class, Media Type, UL Subscribed Bandwidth, DL Subscribed Bandwidth, Maximum priority, Requestor Name, Initial Gate Setting (optional); List of allowed destinations, UL Default Bandwidth, DL Default Bandwidth	Strictly this is defined in the NASS rather than the RACS documents. In this case data held by the NASS in the CLF is sent to RACS in the A-RACF functional entity. The data is based on subscriber identity and if sent over an exposed interface has to be protected from eavesdropping (from privacy regulation). The underlying mechanism is DIAMETER.
Access Profile Pull	RACS to NASS	IP Address End Point, Address Realm Subscriber ID (optional)	As for push but it is noted that the content of the profile is not explicit for the pull case (although it is assumed the profile is itself exchanged as per the push case).
IP Connectivity Release Indication	NASS to RACS	IP Address End Point, Address Realm Subscriber ID (optional)	Used to indicate user release of IP connectivity and therefore to allow RACS to clear any reservations.

Table A.4: Stage 3 protocol mapping to information flows

Stage 2 Information flow	Direction	Stage 3 protocol	Analysis
Resource reservation request	AF to SPDF	DIAMETER	Fits to the authorization schema of DIAMETER
Resource Modification Request	AF to SPDF	DIAMETER	Fits to the authorization schema of DIAMETER
Resource Request Confirmation	SPDF to AF	DIAMETER	Used as a confirmation of the matching request
Resource Modification Confirmation	SPDF to AF	DIAMETER	As above
Resource Release Request	AF to SPDF	DIAMETER	Fits to the authorization schema of DIAMETER
Abort Resource Reservation	AF to SPDF	DIAMETER	Fits to the authorization schema of DIAMETER
Access Profile Push	NASS to RACS CLF to A-RACF	DIAMETER	Fits to the authorization schema of DIAMETER
Access Profile Pull	RACS to NASS A-RACF to CLF	DIAMETER	Fits to the authorization schema of DIAMETER
IP Connectivity Release Indication	NASS to RACS	DIAMETER	Fits to the authorization schema of DIAMETER

The following notes on the use of DIAMETER should be taken into account:

Diameter clients, such as Network Access Servers (NASes) and Foreign Agents support IP Security, and MAY support TLS. Diameter servers support TLS, but the administrator MAY opt to configure IPSec instead of using TLS. Operating the Diameter protocol without any security mechanism is not recommended.

The secure transport of DIAMETER messages is defined in TS 133 210 [i.13] for application at the abstracted Za/Zb reference points using only IPsec (in tunnel mode although it may be required to use the encapsulated UDP mode for cases where NAT devices exist in the path). For the instance of the AF-SPDF interface being exposed to attack the encryption and integrity provisions of IPsec shall be deployed as in the outline protocol stack shown in figure A.7 for the connection between AF and SPDF and in figure A.8 for the connection between CLF (in NASS) and A-RACF (in RACS).

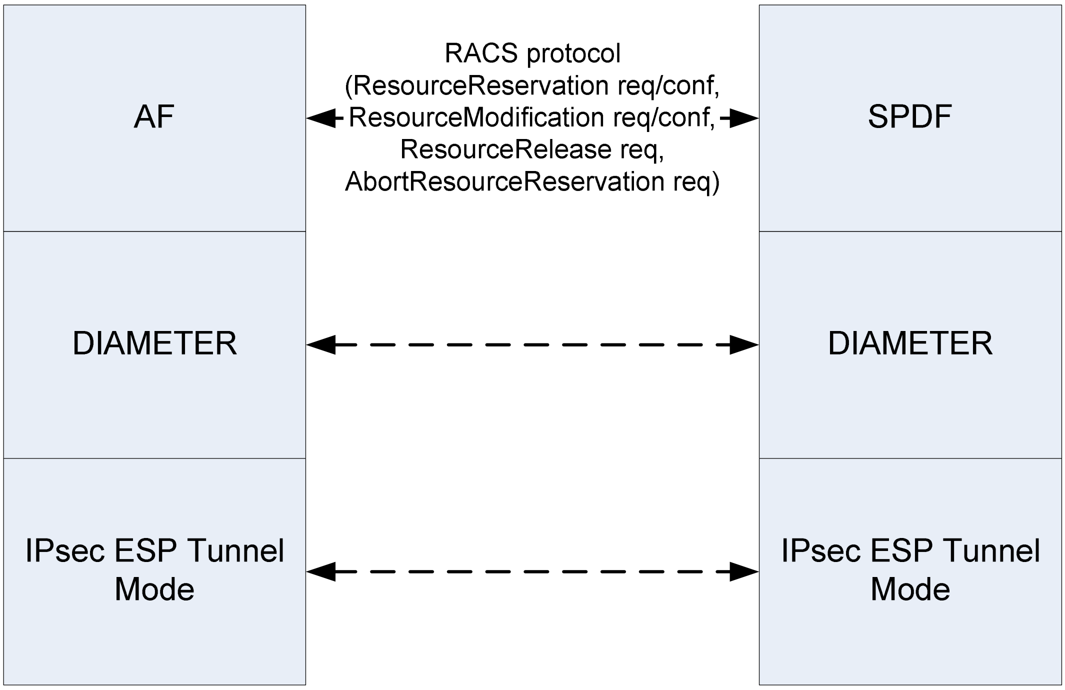


Figure A.7: Protocol stack between AF and SPDF

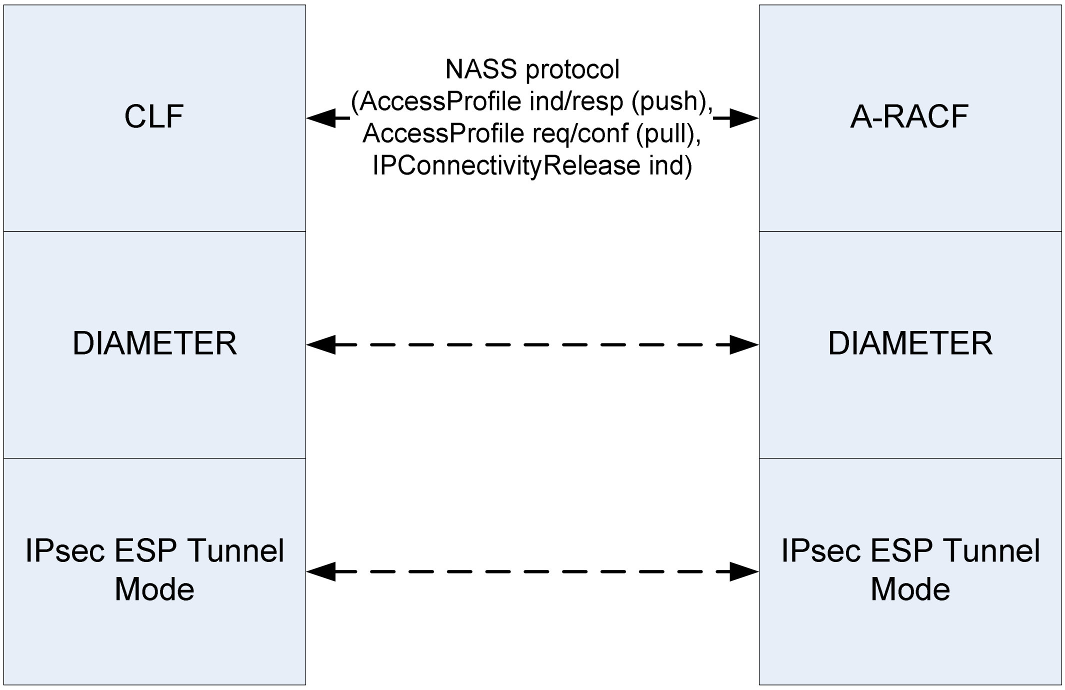

CLF
NASS protocol
(AccessProfile ind/resp (push),
AccessProfile req/conf (pull),
IPConnectivityRelease ind)
A-RACF
DIAMETER
DIAMETER
IPsec ESP Tunnel Mode
IPsec ESP Tunnel Mode

Figure A.8: Protocol stack between CLF and A-RACF

The functional architecture of RACS used in the analysis is that found in ES 282 003 [i.10].

A.4 Security objectives

The security objectives listed in table A.5 are the top most level of requirement for RACS to drive the functional and detail requirements identified as countermeasures for risks from RACS shown in clause A.5.

Table A.5: RACS security objectives

Security Objectives		
OBJ1	The NGN R2 RACS should have a means to identify AF to RACS	Not explicitly available
OBJ2	The NGN R2 RACS should have a means to authenticate AF to RACS	Not explicitly available
OBJ3	The NGN R2 RACS should have a means to authorize AF to RACS	Not explicitly available but implicit through DIAMETER and IPsec
OBJ4	The NGN R2 RACS should have a means to ensure secure communication on all exposed reference points of RACS (e4, Rr, Rq, Gq', Ri', Re and Ia)	Not explicitly available but implicit through DIAMETER and IPsec
OBJ5	The NGN R2 RACS should have a means to ensure confidentiality of all information exchanged over all exposed reference points (e4, Rr, Rq, Gq', Ri', Re and Ia)	Not explicitly available but implicit through DIAMETER and IPsec
OBJ6	The NGN R2 RACS should have a means to ensure integrity of all information exchanged over all exposed reference points (e4, Rr, Rq, Gq', Ri', Re and Ia)	Not explicitly available but implicit through DIAMETER and IPsec
OBJ7	The NGN R2 RACS should have a means to ensure confidentiality of stored data for all relevant functional entities in RACS	Not explicitly available
OBJ8	The NGN R2 RACS should have a means to ensure authorized access to stored data for all relevant functional entities in RACS	Not explicitly available
OBJ9	The NGN R2 RACS should have a means to ensure confidentiality of signalling within RACS	Not explicitly available
OBJ10	The NGN R2 RACS have a means to ensure confidentiality of all user-related data exchanged over all relevant interfaces/reference points in RACS (e4, Rr, Rq, Gq', Ri', Re and Ia interfaces)	Not explicitly available but implicit through DIAMETER and IPsec
OBJ11	The NGN R2 RACS have a means to ensure confidentiality of all user-related data stored on all relevant functional entities in RACS	Not explicitly available
OBJ12	The NGN R2 RACS have a means to only allow authorized disclosure of user location and usage patterns	Not explicitly available
OBJ13	The NGN R2 RACS should have a means to ensure confidentiality of critical or user private information transferred between instances of RACS (x-RACF and SPDF) located in different administrative domains within NGN networks	Not explicitly available but implicit through DIAMETER and IPsec
OBJ14	The NGN R2 RACS should have a means to ensure the integrity (and authenticity) of authorized reserved resources when aggregating these from multiple Transfer Processing Functions	Not explicitly available but implicit through DIAMETER and IPsec
OBJ15	The NGN R2 RACS should have a means to authorize the validity of QoS resource reservations to ensure that they are in line with policies established by the operators and stored in the subsystem, and if appropriate transport resources are available	Not explicitly available
OBJ16	The NGN R2 RACS should have a means for the multicast resource admission control mechanism to authorize multicast services (possible against resource admission policies)	Not explicitly available
OBJ17	The NGN R2 RACS should have a means for the multicast resource mechanism to ensure integrity of rapid modification of resources during fast channel zapping	Not explicitly available
OBJ18	The NGN R2 RACS should have a means to allow only authorized access to topology and resource information from local transport segments	Not explicitly available but implicit through DIAMETER and IPsec
OBJ19	The NGN R2 RACS should have a means to allow only authorized access to topology and resource information from multiple external transport segments	Not explicitly available but implicit through DIAMETER and IPsec
OBJ20	The NGN R2 RACS should have a means to allow only authorized access to topology and resource information from several network entities within one or more transport segments	Not explicitly available but implicit through DIAMETER and IPsec

A.5 Threats to RACS and threat agents to enable them

This clause identifies the threats to RACS and the threat agents that can initiate or perform the threat and materialize it to an security attack.

Attacks are considered with respect to the threat trees identified in TS 102 165-1 [i.4] as follows:

- Interception attacks.
- Manipulation attacks.
- Masquerade attacks.

The ToE has identified Gq' as the primary exposed reference point with a potential of e4 also being exposed. The likelihood of reference points being Re and Ri' being exposed (as per scenarios 2, 3, and 4) are considerably less but the overall structure of attacks is identical as the protocol stacks in use are also identical (RACS over DIAMETER over IPsec).

The following attacks are considered:

- Interception of data transferred across the reference point (Gq', e4, Ri').
- Manipulation of data transferred across the reference point (Gq', e4, Ri'):
    - Blocking response messages from SPDF by alteration of AF identifier.
- Injection of data.

Where data on Gq' is intercepted it may release subscriber data that could be considered as personal data in the context of the data privacy directive. If this is the case the data should be protected from disclosure.

An attacker may be highly motivated to alter (manipulate) data in resource-reservations as this could lead to financial fraud if the link through the Charging Correlation Information is exploitable.

For each of the potentially exposed reference points (Gq'. Ri', e4) the ability of an attacker to make a direct attack is somewhat restricted for access as each of these reference points is exposed within the ECN (Ri', e4) or between the ECN and ECS (Gq')) and thus minimizes the attack potential (see table A.6).

Table A.6: Attack potential for interception at the exposed RACS reference points

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 week	1
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Moderate	4
Equipment	Standard	0
Total	Moderate - possible	7

Prior to mounting any form of manipulation attack the attacker has to be able to gain access to the exposed reference points thus having an initial attack potential the same as for interception. With the protocol stack that exists a direct interception and manipulation is largely countered where the IPsec layer provides confidentiality and integrity protection, if the suite of encryption and integrity algorithms recommended (AES) is deployed the attack potential is modified as shown in table A.7.

Table A.7: Attack potential for information interception at the exposed RACS reference points

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	Beyond reasonable assessment	> 50
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Moderate	4
Equipment	Standard	0
Total	Unlikely	> 50

In order to inject data successfully however the attack lies above the IPsec and DIAMETER layer by direct masquerade of the RACS peer entities. There is no direct authentication to counter any masquerade attack.

A.6 Countermeasures for risk mitigation in RACS

This clause describes the countermeasures to the threats identified in RACS TVRA. The countermeasures formulated as security requirements to RACS for TISPAN NGN R2.

In accordance with the guidance given by TR 187 011 [i.34] the objectives outlined in clause A.5 are refined through functional to detailed requirements (essentially from stage 1 intention to stage 3 deployment). The functional requirements are expressed where possible using the functional capabilities model of ISO/IEC 15408-2 [i.31].

A.6.1 Functional requirements

The following requirements are derived from the security objectives and stated as RACS optimizations of ISO/IEC 15408-2 [i.31].

- Identification (FIA_UID):
  - RACS not allow any media reservation requests from the AF to be acted upon prior to identification of the AF.
  - RACS not allow any media reservation modifications from the AF to be acted upon prior to identification of the AF.
  - RACS not allow any media reservation cancellations from the AF to be acted upon prior to identification of the AF.
- Authentication (FIA_UAU):
  - RACS not allow any media reservation requests from the AF to be acted upon prior to authentication of the AF.
  - RACS not allow any media reservation modifications from the AF to be acted upon prior to authentication of the AF.
  - RACS not allow any media reservation cancellations from the AF to be acted upon prior to authentication of the AF.
- Replay protection (FPT_RPL):
  - RACS detect replay of media reservation requests from the AF.
- Data integrity (FDP_UIT):
  - The RACS enforce the implementation of Gq' to transmit data to the SPDF in a manner protected from modification errors.

  - The RACS enforce the SPDF to be able to receive data from the AF in a manner protected from modification errors.
  - The RACS enforce the implementation of e4 to transmit data to the RACF in a manner protected from modification errors.
  - The RACS enforce the RACF to be able to receive data from the CLF in a manner protected from modification errors.

- Data confidentiality (FDP_UCT):
  - The RACS enforce the implementation of Gq' to transmit data to the SPDF in a manner protected from unauthorized disclosure.
  - The RACS enforce the SPDF to be able to receive data from the AF in a manner protected from unauthorized disclosure.
  - The RACS enforce the implementation of e4 to transmit data to the RACF in a manner protected from unauthorized disclosure.
  - The RACS enforce the RACF to be able to receive data from the CLF in a manner protected from unauthorized disclosure.

A.6.2 Detail requirements

The detail requirements given below are also stated in TS 187 001 [i.6].

(R-AA- 27): RACS and AF be mutually authenticated using application layer identities prior to resource authorization using DIAMETER.

(R-AA- 28): AF and SPDF in RACS have unique application layer identities to be used for mutual authentication.

(R-CD- 17): RACS ensure integrity of all policy related resource information exchanged between NASS and RACS.

NOTE 1: This requires that RACS is the validator of the integrity of the data exchanged, and that NASS is the generator of the integrity check data.

(R-CD- 18): Data integrity validation in RACS be enforced using either Message Digest (MD) or cryptographic Message Authentication Code (MAC) with keys derived from the unique application layer identities of AF and SPDF (as specified in requirement R-AA-28).

NOTE 2: Unique application layer identities as specified in requirement R-AA-28 are a pre-requisite for R-CD-17 and R-CD-18.

Annex B: TVRA of Media transport NGN-R2

NOTE 1: The scope of this annex is only the functionality provided for NGN-R2.

NOTE 2: The detail requirements identified in this analysis are also stated in TS 187 001 [i.6].

B.1 Description of ToE

A model for media security is proposed as the basis of further analysis in figure B.1. The model shows an active class representing the Media Source with an active class representing the Media Transport Encoder. The model shows that the encoding of media transport is dependent upon the actual media transport used. Finally the model shows a media security encoder as a specialization of media transport encoder with additional interfaces for security credential management.

NOTE 1: Media may be encoded prior to transport (e.g. MP3 audio, MPEG-4 video) but the form of direct media encoding is not considered further.

NOTE 2: An active class indicates that, when instantiated, it controls its own execution. Rather than being invoked or activated by other objects, it can operate standalone and define its own thread of behaviour.

The media transport encoder (and its associated specialization media security encoder) are invoked by the media source.

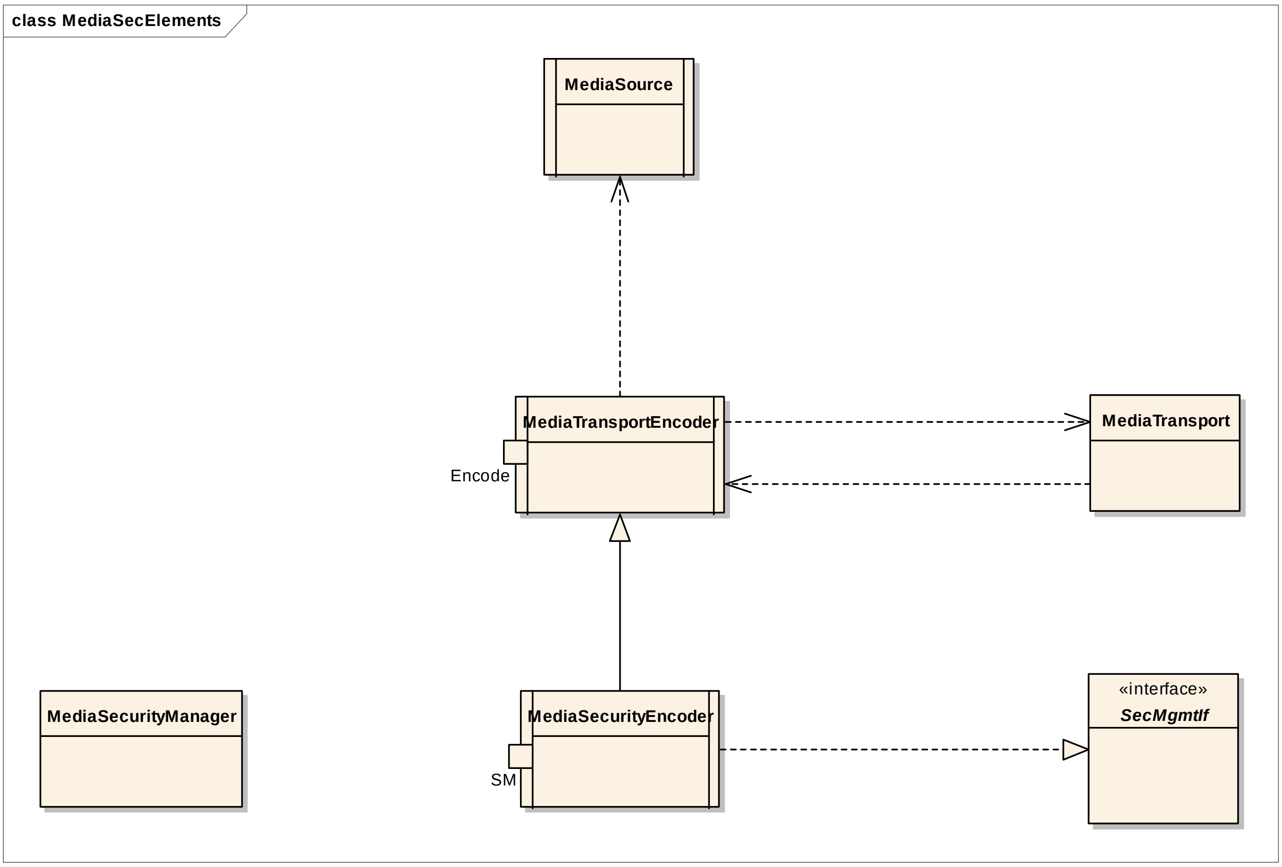


Figure B.1: Abstract model of media security elements (shown as UML classes)

The NGN Media architecture has two phases which can be attacked:

- Path establishment:
    - Redirection.
    - Manipulation of signalling.
- Path active:
    - Eavesdropping.

In order to support media transfer in the NGN a number of sub-systems are used. An attack against these subsystems may result in an attack to the media transfer capabilities.

The assumptions under which media security in the NGN is considered are listed in table B.1.

Table B.1: Assumptions prior to media security risk analysis

a.1.1	Existing fixed access networks do not have cryptographic lower layer protection	Underlying assumption is that cryptographic means are required to achieve media security.
a.1.2	UTRAN networks have cryptographic lower layer protection	Optional. Configured on a site by site basis and subject to national regulation for deployment of cryptographic methods. It is also noted that UTRAN media protection is bound to the authentication procedure.
a.1.3	IMS deployment for fixed networks do not have sufficient underlying security	Sufficient is not defined.
a.1.4	Eavesdropping of media traffic is possible without physical access in WLAN deployment	But there are mechanisms to provide WLAN media protection.
a.1.5	User to user communication is considered in scope of media security	User should be fully defined, e.g. end-user terminal should be used instead.
a.1.6	User to network communication is considered in scope of media security	User should be fully defined, e.g. end-user terminal should be used instead.
a.1.7	User to group communication is considered in scope of media security	User should be fully defined, e.g. end-user terminal should be used instead.
a.1.8	Simplex communication is considered in scope of media security	
a.1.9	Duplex communication is considered in scope of media security	Covers both isochronous and asynchronous media.
a.1.10	Conversational text is considered in scope of media security	

B.2 Identification of objectives

The objectives in a system are high level statements of intent. In general for a media stream the attributes that need to be protected are its confidentiality (to protect from eavesdropping), its integrity (to ensure correctness of the content of the media stream) and the authenticity of the source of the media stream. These objectives are summarized in table B.2.

Table B.2: Objectives to be met by media security provisions

B Security Objectives		
OBJ1	An NGN should allow a received of a media stream to authenticate the source of the stream.	
OBJ2	Media security may be removed on receipt of an authorized request.	
OBJ3	An NGN should allow media to be encrypted end-to-end.	
OBJ4	An NGN should allow media to be encrypted end-to-middle.	
OBJ5	An NGN should allow media to be integrity protected end-to-end.	
OBJ6	An NGN should allow media to be integrity protected end-to-middle.	

B.3 Step 2: Identification of requirements

The system requirements are dependent on the system objectives identified in Step 1 and come in two variants:

- security requirements; and.
- assurance requirements.

The assurance requirements are derived from the assurance objectives as a selection of ISO/IEC 15408-2 [i.31] security assurance components. Security requirements are derived from the security objectives from Step 1. As for the security objectives, the security requirements are categorized into the five categories, here requirement categories, authentication, accountability, confidentiality, integrity and availability.

SR 002 211 [i.43] identifies those aspects of standardization that are required to ensure compliance with the European Framework Directive [i.15]. In some instances the right to privacy can be withheld as suggested in paragraph 2 of article 5 of the privacy directive [i.16] (see clause 5.1). Provisions for the lawful interception of traffic, and for retention of signalling data are allowed exceptions as defined in Article 15(1) of the privacy directive [i.16]:

1) Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC [i.45]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

The obligations from the directive are placed on member states but may be met by the provision of specific capabilities in the NGN. If the requirements are to be met by the NGN these may be stated as follows:

Id	Requirement text
R-MS-REG-1	An NGN provide mechanisms to prevent eavesdropping of traffic
R-MS-REG-2	An NGN provide mechanisms to prevent unauthorized recording and storage of traffic
R-MS-REG-3	An NGN provide mechanisms to prevent unauthorized interception of traffic
R-MS-REG-4 (note)	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
R-MS-REG-5	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
R-MS-REG-6 (note)	An NGN operator should provide mechanisms to ensure the retention and handover of signalling of specific NGN users if required to by a lawful authority
NOTE: This requirement is not strictly related to media but may be correlated to media provision.	

The requirements derived from the regulatory environment in Europe require that the NGN provides protection of media in the following areas: Confidentiality; Integrity.

Prevention of eavesdropping can be achieved in a number of ways:

NOTE 1: For the purposes of analysis it is assumed that the eavesdropping attacker has taken some care to be both anonymous and non-intrusive.

- Broadcast media paths (e.g. radio) should be protected by encryption of media content in such a manner that the encryption key can not be recovered from examination of the media stream or by injection of signals to the media stream (known text attacks). The key used for encryption should only be known to the parties directly involved in the transfer of the media over the broadcast path.

NOTE 2: Broadcast (radio) paths may be visible to an attacker at some considerable distance from the intended path.

- Non-broadcast media paths should be constructed such that eavesdropping cannot be achieved without intrusion to the media path (e.g. by direct access to a cable (fibre-optic or other)).

Id	Requirement text
R-MS-GEN-1	An NGN SHOULD ensure that non-broadcast media paths are constructed such that eavesdropping cannot be achieved without intrusion to the media path.
R-MS-GEN-2	An NGN SHOULD ensure that broadcast media paths (e.g. radio) should be protected by encryption of media content.
R-MS-GEN-3	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.

Provision of security for media may be provided by cryptographic or non-cryptographic means. Where media is exposed in an untrusted domain the general assumption is that attack is more likely than when media is exposed in a trusted domain. For cryptographic media protection to work encryption keys will require to be distributed and managed.

End to end encryption devices may be subject to restriction under the terms of the Wassenaar agreement either in the form of the encryption device or in the effective key length. End-to-end encryption may offer some advantage in minimizing delay (depending on the form of the algorithm and the transport) but may not be allowed by regulation on a national basis to be deployed by the core network. Where the provision of end-to-end encryption includes the selection of keys and algorithms by the end points it cannot be considered as an NGN service thus not be provided by the NGN.

NOTE 3: If users choose to provide their own end-to-end encryption solution it will be a decision of each NGN to support the resultant media service.

The protection of traffic and signalling in most instances is from the end point (terminal) to a fixed point within the trusted network.

Table B.3 lists a number of requirements for media security in NGNs from the preceding analysis.

Table B.3: Requirements for media security in the NGN

(R-MS- 1):	The NGN not provide support for end-to-end media security.
(R-MS- 2):	The NGN provide support for user-to-network media security (for the following security services Confidentiality, Integrity, Authenticity of source and destination end-points).
(R-MS- 3):	The NGN provide support for secure media transfer in point-to-point topologies.
(R-MS- 4):	The NGN provide support for secure media transfer in point-to-multipoint topologies.
(R-MS- 5):	The NGN provide support for secure media transfer in broadcast topologies.
(R-MS- 6):	An NGN provide mechanisms to prevent eavesdropping of traffic.
(R-MS- 7):	An NGN provide mechanisms to prevent unauthorized recording and storage of traffic.
(R-MS- 8):	An NGN provide mechanisms to prevent unauthorized interception of traffic.
(R-MS- 9):	An NGN should ensure that non-broadcast media paths are constructed such that eavesdropping cannot be achieved without intrusion to the media path.
(R-MS- 10):	An NGN should ensure that broadcast media paths (e.g. radio) should be protected by encryption of media content.
(R-MS- 11):	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.

Table B.4 lists a number of requirements for media security in NGCNs from the preceding analysis that are in addition to the NGN requirements found in table B.3.

Table B.4: Requirements for media security in the NGCN

(R-NGCN- 12):	The NGN provide support for secure media transfer between NGCNs and NGNs.
(R-NGCN- 13):	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.
(R-NGCN- 14):	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.
(R-NGCN- 15):	An NGCN should be transparent to the end-to-end encryption of any key exchange required for the purpose of media security.

Annex C:
Example TVRA for use of ENUM in NGN

NOTE 1: The scope of this annex is only the functionality provided for NGN-R1 and has not been validated in the scope of NGN-R2.

NOTE 2: The detail requirements identified in this analysis are also stated in TS 187 001 [i.6].

C.1 Overview and introduction

ENUM is a system for resolving NGN session routing. ENUM is a core component of the NGN and its use is outlined in TR 102 055 [i.22]. The security analysis of ENUM given in this annex reviews the architecture of ENUM and its role within the NGN. A detailed security analysis of ENUM is also provided in TR 102 420 [i.23] but does not make reference to the eTVRA method.

There are a number of assumptions to be made for use of ENUM in the NGN:

- ENUM lies on top of DNS;
- ENUM refers to a system of use and not just to RFC 3761 [i.25] and RFC 3403 [i.26] that define the use of DNS for storage of E.164 numbers and the NAPTR records that populate it;
- ENUM may be deployed in a number of ways (e.g. user-ENUM, infrastructure-ENUM).

NOTE: When reviewing and analysing the security impact of ENUM deployment it is noted that where DNS is public, everything in the DNS records is public. If ENUM is a direct overlay of DNS distinguished only by the use of specific record types then the ENUM records are effectively public.

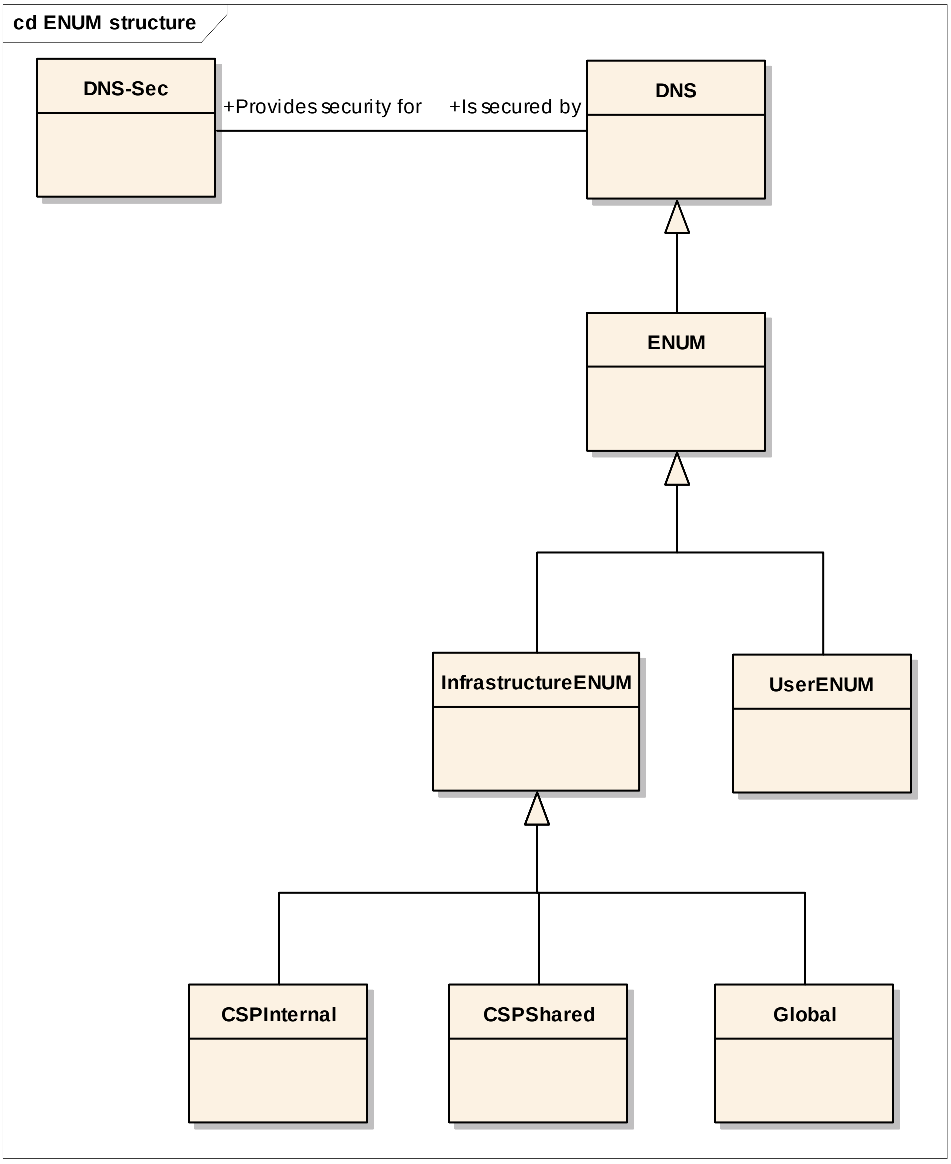


Figure C.1: Hierarchical structure of ENUM showing increasing generalization at top

From a security analysis point of view increasing specialization (i.e. where infrastructure ENUM is a specialization of ENUM which is itself a specialization of DNS) allows layering of security provisions. Figure C.1 identifies DNS-sec as protecting the root DNS system so its provisions can be inherited by all of the specializations of DNS.

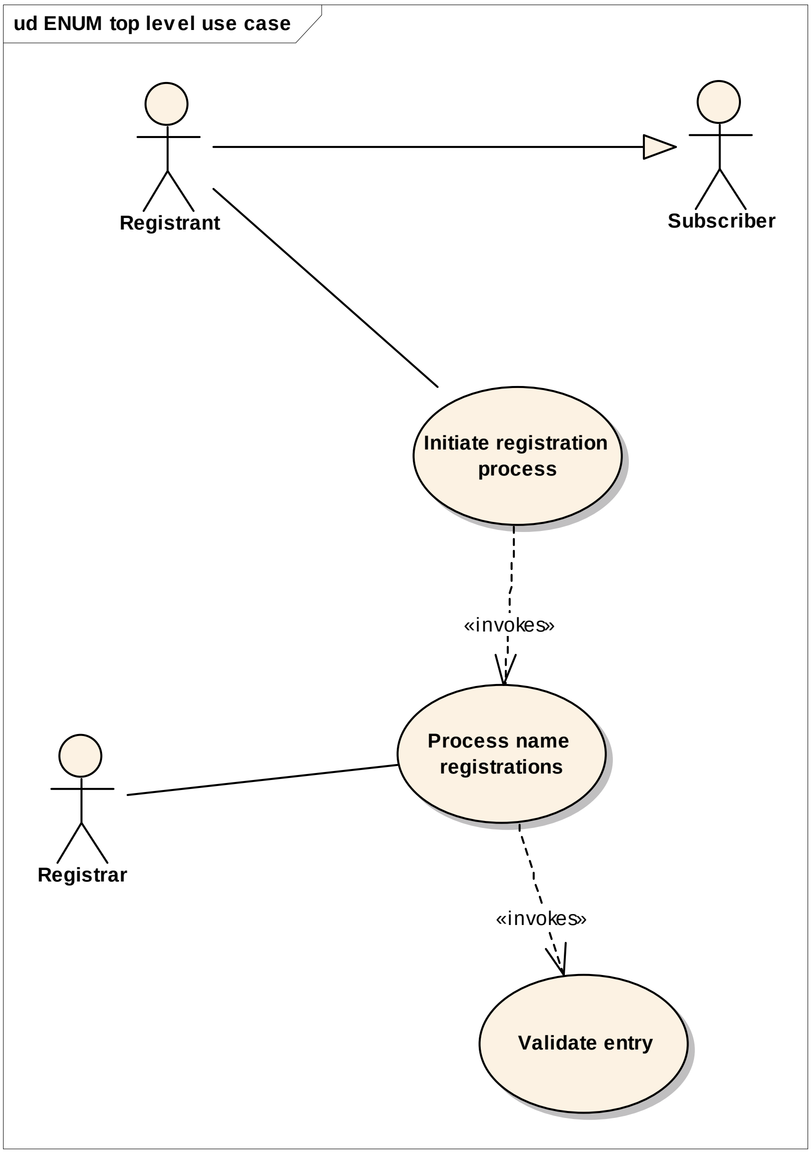

ud ENUM top level use case
Registrant
Subscriber
Initiate registration process
«invokes»
Process name registrations
Registrar
«invokes»
Validate entry

Figure C.2: Main actors and use cases in ENUM

Figure C.2 shows the main actors in ENUM with the registrant shown as a specialization of the subscriber and acting on his behalf to insert his E.164 number into ENUM.

In Infrastructure ENUM there is no explicit communication between the subscriber and the registrant, and the registrar may be from the same organization as the registrant.

C.1.1 Security critical ENUM operations

There are a large number of ENUM operations identified that either provide protection or which require protection. These are summarized in the operation scenarios below.

C.1.1.1 Registration of an E.164 number in the ENUM database

This clause describes the process for registration of a new ENUM domain name in the ENUM Tier 2 Nameserver Provider and the delegation of the related zone in the Tier 1 Registry. The process is based on the assumption that the request of registration is initiated by the end user to which the E.164 number has been assigned or by a third party (agent) operating on behalf of the end user after its authorization. In the following the entity initiating the registration process (end user or agent) is referred to as the ENUM Registrant.

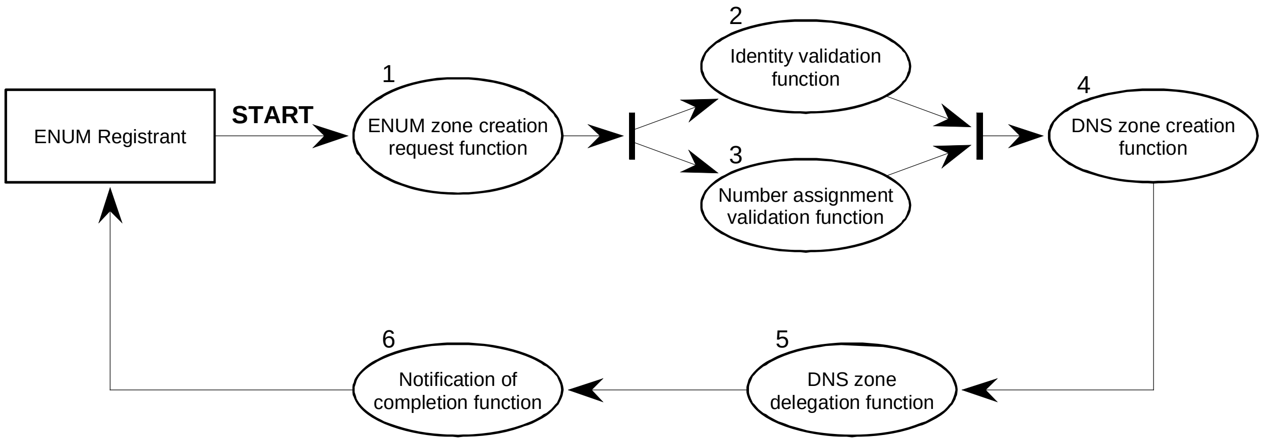

ENUM Registrant
START
1
ENUM zone creation request function
2
Identity validation function
3
Number assignment validation function
4
DNS zone creation function
5
DNS zone delegation function
6
Notification of completion function

Figure C.3: Functional model for Registration

Figure C.3 presents a functional model in which the following process takes place for the registration and provision of NAPTR records:

1) The **ENUM zone creation request** step involves receiving requests from an ENUM Registrant to create a DNS zone for his E.164 number.

2) The **identity validation** step involves confirming the identity of the ENUM Registrant and his authority to act on behalf of an end user.

3) The **number assignment validation** step involves confirming the assignment of the E.164 number to the ENUM end user.

4) **The DNS zone creation** step involves creation of a zone in the ENUM Tier 2 Nameserver Provider.

5) The **DNS zone delegation** step involves delegating DNS authority to the new zone by inserting the appropriate pointers in the Tier 1 Registry to the ENUM Tier 2 Nameserver Provider selected by the end user.

6) The **notification of completion** step involves informing the ENUM Registrant that the registration process has been successfully completed.

C.1.1.2 Processes for creation, modification and deletion of NAPTR Records in the Tier 2 database

This clause describes the process for amendment of NAPTR Resource Records in the Tier 2 database. This could take the form of the creation, modification or deletion of a NAPTR or group of NAPTR records related to a specific E.164 number. A request for amendment is initiated by the ENUM end user or an agent acting on behalf of the ENUM end user (both referred to as the ENUM Registrant).

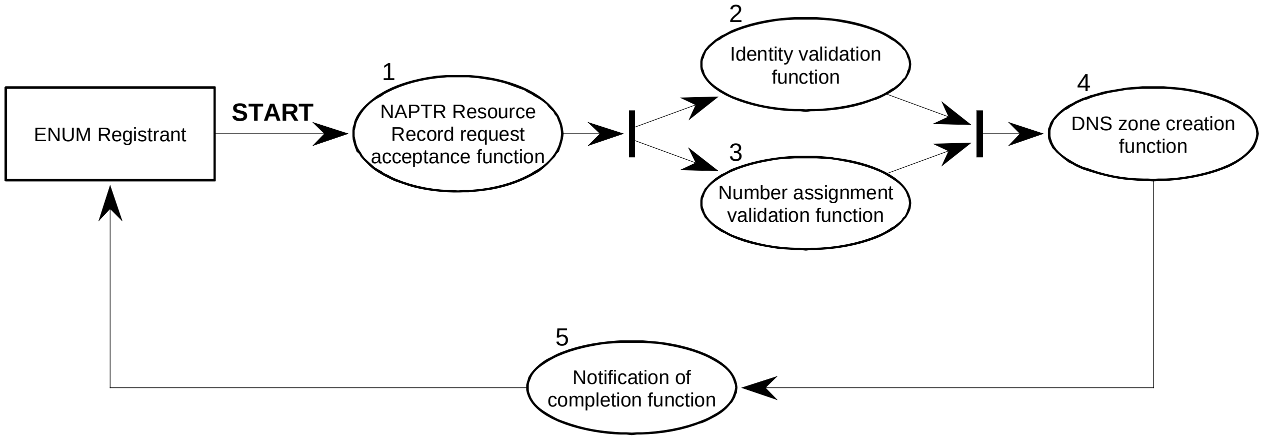

ENUM Registrant
START
1
NAPTR Resource Record request acceptance function
2
Identity validation function
3
Number assignment validation function
4
DNS zone creation function
5
Notification of completion function

Figure C.4: Functional model for amendment of NAPTR Resource Records in Tier 2 database

Figure C.4 presents a functional model which includes the following process take place for the amendment of NAPTR Resource Records in the Tier 2 database:

1) The **NAPTR Resource Record request acceptance** step involves receiving requests from an ENUM Registrant to create, modify or delete a NAPTR Resource Record corresponding to the ENUM end user's E.164 number.

2) The **identity validation** step involves confirming:

   - the identity of an ENUM Registrant who is the ENUM end user; or

   - the identity of an ENUM Registrant who is not the ENUM end user and his authority to make a request on behalf of the ENUM end user.

3) The **number assignment validation** step involves confirming the assignment of the E.164 number to the ENUM end user.

4) The **DNS zone update** step involves updating ENUM service details corresponding to the ENUM end user's E.164 number in the DNS in the required format.

5) The **completion notification** step involves informing the ENUM Registrant that the amendment process has been successfully completed.

C.1.1.3 Processes for removal of E.164 numbers from ENUM databases

This clause describes the process for removal of E.164 numbers and NAPTR Resource Records from ENUM databases. The process is based on the assumption that an ENUM end user should have information corresponding to its E.164 number in ENUM databases until:

- it no longer requires the services that are reliant on ENUM;

- it otherwise relinquishes the number or the number is withdrawn.

In the event of relinquishment or withdrawal of the number, it is important for NAPTR Resource Records corresponding to the number to be removed before any conflict is generated by use of the number by a new end user. In the case that the ENUM end user requires the removal of information relating to its E.164 number from ENUM databases, the ENUM end user or an agent acting on behalf of the ENUM end user (both referred to as the ENUM Registrant) initiates the removal request. In the case that the ENUM end user relinquishes the number or the number is withdrawn, it may be appropriate to allow the Assignment Entity to initiate the request to remove information relating to the E.164 number from ENUM databases, or to periodically verify that ENUM data corresponding to an end user's E.164 number should continue to be maintained.

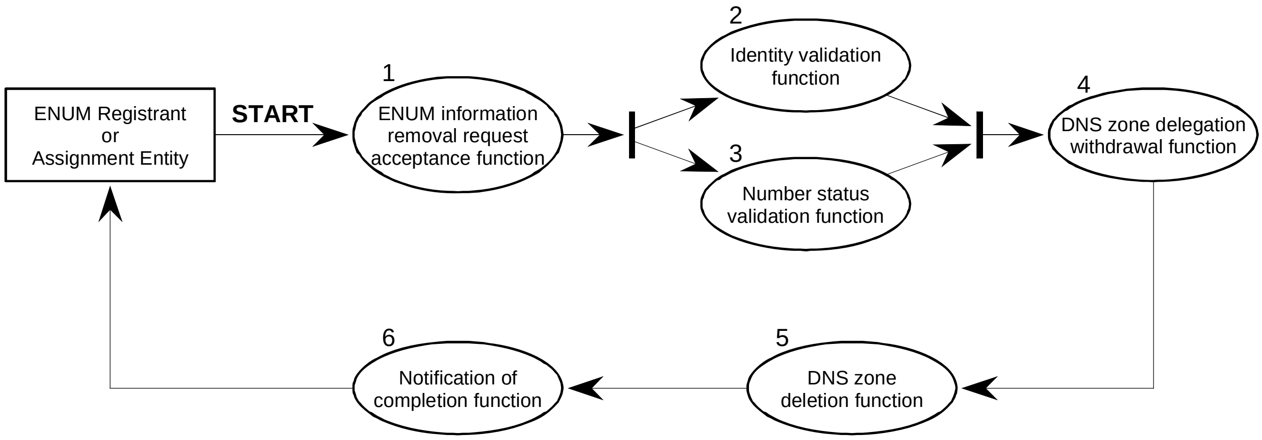

ENUM Registrant or Assignment Entity
START
1
ENUM information removal request acceptance function
2
Identity validation function
3
Number status validation function
4
DNS zone delegation withdrawal function
5
DNS zone deletion function
6
Notification of completion function

Figure C.5: Functional model for removal of E.164 numbers from ENUM databases

Figure C.5 presents a functional model in which the following process take place for the removal of E.164 numbers and NAPTR Resource Records from ENUM databases:

1) The **ENUM information removal request acceptance** step involves accepting requests from an ENUM Registrant (either an end user or an agent acting on behalf of an end user) or an Assignment Entity to remove information relating to an E.164 number from ENUM databases.

2) The **identity validation** step involves confirming:

   - the identity of an ENUM Registrant who is the ENUM end user; or

   - the identity of an ENUM Registrant who is not the ENUM end user and his authority to make a request on behalf of the ENUM end user; or

   - the identity of an Assignment Entity and its authority to make a request in relation to a particular E.164 number.

3) The **number status validation** step involves confirming that the E.164 number is assigned to the ENUM end user or, prior to its relinquishment or withdrawal, was assigned to the ENUM end user.

4) The **DNS zone delegation withdrawal** step involves withdrawing the delegation of DNS authority to the zone corresponding to an E.164 number by removing the pointers to the URI corresponding to the number.

5) The **DNS zone deletion** step involves deleting ENUM information relating to an E.164 number from the DNS.

6) The **notification of completion** step involves informing the originator of the removal request that the removal process has been successfully completed.

C.1.1.4 Processes for changing Registrars

Requirements and procedures should exist to enable an ENUM Registrant to change the Registrar responsible for registration of the domain and creation of the NAPTR records corresponding to an E.164 number. These requirements and procedures should support change of Registrar in such a way that no interruption in an ENUM end user's use of the domain name and NAPTR records.

Where requirements and procedures for change of Registrar exist in a country in respect of normal Internet domain name registrations, these requirements and procedures should be checked to establish whether they meet the additional requirements that apply when an ENUM Registrar changes. Where no such requirements and procedures exist in a country the following points should be considered:

- an ENUM end user should be able to change Registrar at any time;

- an ENUM end user with domain name registrations and NAPTR records for more than one E.164 number should be able to change Registrar in respect of all or some of the numbers;

- a request to change Registrar should be made by an ENUM Registrant to its selected new Registrar (and not the old (current) Registrar);

- the new Registrar should validate the identity of the ENUM Registrant and, if the latter is not the ENUM end user, verify his authority to act on behalf of the ENUM end user;

- the new Registrar should verify that the E.164 number is assigned to the ENUM end user;

- the new Registrar should notify the Tier 1 Registry and ENUM Tier 2 Nameserver Provider and the old Registrar of the intention of the ENUM Registrant to change Registrar;

- within a specified time, the Tier 1 Registry and ENUM Tier 2 Nameserver Provider should amend their Registrant information to identify the new Registrar as the Registrar of record for the particular ENUM Registrant, and notify the old and new Registrars of the amendments. It is the prime responsibility of the Tier 1 Registry to supervise the proper completion of the process; and

- in the case that an unauthorized change of Registrar occurs, the ENUM Tier 2 Nameserver Provider should reverse the amendment of its Registrant information within a specified time.

C.1.2 ENUM assets

C.1.2.1 NAPTR records

As described in RFC 2915 [i.27] in the text of example 3 in clause 7.3 the ENUM application uses a NAPTR record to map an e.164 telephone number to a URI.

EXAMPLE 1: The E.164 phone number "+1-770-555-1212" when converted to a domain-name would be "2.1.2.1.5.5.5.0.7.7.1.e164.arpa."

When an ENUM (DNS) query is executed against this number the following records may be returned:

```
EXAMPLE 2:   $ORIGIN 2.1.2.1.5.5.5.0.7.7.1.e164.arpa.
             IN NAPTR 100 10 "u" "sip+E2U"  "!^.*$!sip:information@tele2.se!"
             IN NAPTR 102 10 "u" "mailto+E2U" "!^.*$!mailto:information@tele2.se!"
```

The returned resource record set contains the information needed to contact that telephone service. The example above states that the available protocols used to access that telephone's service are either the Session Initiation Protocol or SMTP mail.

The NAPTR record is an asset of the ENUM system. The principal attack against ENUM is to the integrity of the NAPTR records. A NAPTR record that is modified either when stored or recovered may lead to failure of the entity that relies upon the data in the record. Routing entities for example may make false routing decisions if the data in the NAPTR record has been corrupted (including unauthorized modification).

C.1.2.2 ENUM query

The purpose of an ENUM query is to return the NAPTR records held against the E164 number.

C.2 DNSSEC

A security framework for DNS has been defined in RFC 2535 [i.24] and is commonly referred to as DNSSEC. The purpose of DNSSEC is to assure the correctness of a query result by means of signed integrity check values to be attached to DNS results.

DNSSEC signatures have a pair of timestamps indicating valid from and to times. This allows a DNSSEC server to guarantee freshness of the data in order to avoid the results being corrupted by an attacker who feeds old data with (then) valid signatures.

The security mechanisms offered to DNS provide data origin authentication and data integrity by use of public key cryptography mechanisms.

When applying DNSSEC [i.28], [i.30] and [i.29] to ENUM the smallest protected unit is a RRSet. Each resource record is digitally signed and a name server query returns both the RRSet and the signature for the set (this is contained in a RRSIG record). Checking of the RRSIG indicates both the integrity of the data contained in the RRSet and the source of the data; the origin authentication is based on a trusted root and a chain of trust by following pointers with proven integrity.

C.3 Unwanted incidents in use of ENUM in NGN (eTVRA Step 1)

The goal of any security system is to reduce the number of unwanted incidents. Table C.1 identifies the unwanted incidents to be countered in ENUM.

Table C.1: ENUM unwanted incidents

ID	Unwanted Incident
1	loss of reliability/loss of service
2	loss of service/theft of service
3	theft of service/ loss of service
4	reduced availability
6	loss of privacy/loss of service
7	loss of service for one user
8	Impersonation of a user
9	loss of service/loss of privacy
10	loss of service/loss of privacy/loss of reliability
11	Free use of the system/Overuse of the system
12	loss of service for many users
13	loss of service for all users
17	loss of availability
19	Loss of privacy
20	loss of revenue/Theft of service/Free use
21	Loss of customer confidence
23	Overuse of the system
24	Loss of reliability
25	loss of privacy/Impersonation of a user
26	Impersonation of a server
NOTE: Ids 5, 14, 15, 16, 18, 22 are not allocated in the ENUM analysis.	

The translation of unwanted incidents to system objectives may be achieved by inspection, often by simple rephrasing of the unwanted incident text. The most obvious method is to equate an unwanted incident to a specific objective whereby the objective is to prevent the realization of the unwanted incidents.

C.4 Security requirements for ENUM in the NGN (eTVRA Step 2)

The NGN-R1 security requirements document (TS 187 001 [i.6]) does not explicitly identify security requirements for ENUM or for the use of DNS. Detail security requirements referred to ISO/IEC 15408 [i.32] functional capabilities are defined in TR 102 420 [i.23] and summarized below.

Table C.2: Security concern classification from RFC 3761 [i.25]

CIA	Security concern	Attack form
Confidentiality	Packet interception	Man-in-the-middle attacks.
		Eavesdropping on requests combined with spoofed responses.
	ID guessing and query prediction	An attack based on ID guessing or query prediction relies on predicting the behaviour of a resolver. It is most likely to be successful when the victim is in a known state, whether because the victim rebooted recently, or because the victim's behaviour has been influenced by some other action by the attacker or because the victim is responding (in a predictable way) to a third party action known to the attacker.
	Masquerade	Masquerading is a type of attack in which one system entity poses illegitimately as another user or administrator.
	Eavesdropping	Reading and interpreting data flowing in either direction. An eavesdropper does not have to be able to spoof data.
Integrity	Spoofing	Modifying data flowing in either direction. Spoofing can lead to modified queries or to modified responses.
	RR Presence denial	Removes complete resource records from a response.
	Cache Poisoning	Feeding bad data into a victim's cache, thus potentially subverting subsequent decisions based on DNS names.
	Name Chaining	Modification of the RDATA portion of RRs that contain DNS names thus diverting the victim's queries to a fraudulent part of the DNS tree.
	DNS server perversion	This attack feeds illegitimate data into the DNS thus perverting (part of) the DNS. The DNS may then be configured to give back answers that are not in the best interest of the user.
	Loss of data integrity	This attack feeds any illegitimate data into the DNS.
	Name-based attacks	Use of the actual DNS caching behaviour to insert bad data into a victim's cache.
	Betrayal By A Trusted Server	The placing of a malicious entry into the database to point to an unexpected URI.
	Authenticated denial of Domain Names	The placing of a malicious entry into the database to ensure that calls cannot be completed for the user.
Integrity and Availability	Administrator Action Repudiation	Removal of audit trails for administrator actions.
Availability	Denial of service	Use of DNS servers as denial of service amplifiers.
	Data Mining	A data mining attack attempts to derive as much data as possible from a database.
	Denial and Degradation of Service	This attack prevents or delays the authorized access to a system resource which should be accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.

The public nature of the DNS service, and of ENUM as a profile of that service, suggest as shown in the above table that the most damaging attacks against ENUM (DNS) are those that attack the integrity of the data and the availability of the service. The attacks against confidentiality are less motivated as the data is already public.

In the context of the Common Criteria (see annex F) the following functional components should be deployed during the identity validation step.

Table C.3: Functional components to be deployed during identity validation

CC entity	Description	Affected ENUM entity	Unwanted incident avoided
FDP_SDI.1	The stored data is continually monitored to detect errors in its integrity.	NAPTR record	Manipulation
FDP_SDI.2	The stored data is continually monitored to detect errors in its integrity and actions to be taken in the event of errors being found are defined.	NAPTR record	Manipulation
FDP_UIT.1	The data that is transferred is monitored to detect errors in its integrity.	NAPTR record	Manipulation
FDP_UIT.2	The data that is transferred is monitored to detect errors in its integrity and actions to be taken in the event of errors being found using assistance from the source are defined (i.e. the error is reported to the source and both source and destination take part in the corrective action).	NAPTR record	Manipulation
FDP_UIT.3	The data that is transferred is monitored to detect errors in its integrity and actions to be taken in the event of errors being found without using assistance from the source (i.e. the corrective action takes place only at the receiver).	NAPTR record	Manipulation
FIA_UAU.2	The user is not allowed to perform any action prior to successful authentication.	ENUM registrant	Masquerade
FIA_UAU.3	The authentication procedure should ensure that forged or copied authentication data cannot be used.		Masquerade
FIA_UID.2	The user is not allowed to perform any action prior to successful identification.	ENUM registrant	Masquerade

NOTE: The results of an ENUM query, and the data in ENUM, are intended to be highly visible so no counters for attacks against confidentiality are required.

C.5 ENUM assets (eTVRA Step 3)

An eTVRA analysis uses one or more scenarios to identify the assets under study. This TVRA ENUM/NNA analysis assumes a PC-based SIP client communicating via a generic broadband Internet connection wherein an ENUM infrastructure is reachable by the customers of the VoIP service provider but not by the rest of the world.

C.5.1 NNA provisioning scenario

Figure C.6 depicts the scenario as necessary for provisioning names into the system. The following steps have been assumed:

- The home network has assigned to the user a private identity to be used during sign-on:
  - This private identity may be used for session establishment as well or may be replaced with a temporary ID (c.f. IMSI and TIMSI). The serving network may or may not be using the secret ID (as in 3GPP).
- The user has somehow bound one or more public IDs (MISDN, SIP URI etc.) to the private ID:
  - The public IDs may be used as presentation ID during outgoing sessions and may be used to reach the user for incoming sessions.

    In this scenario ENUM is used as the mechanism for provisioning and resolving names.

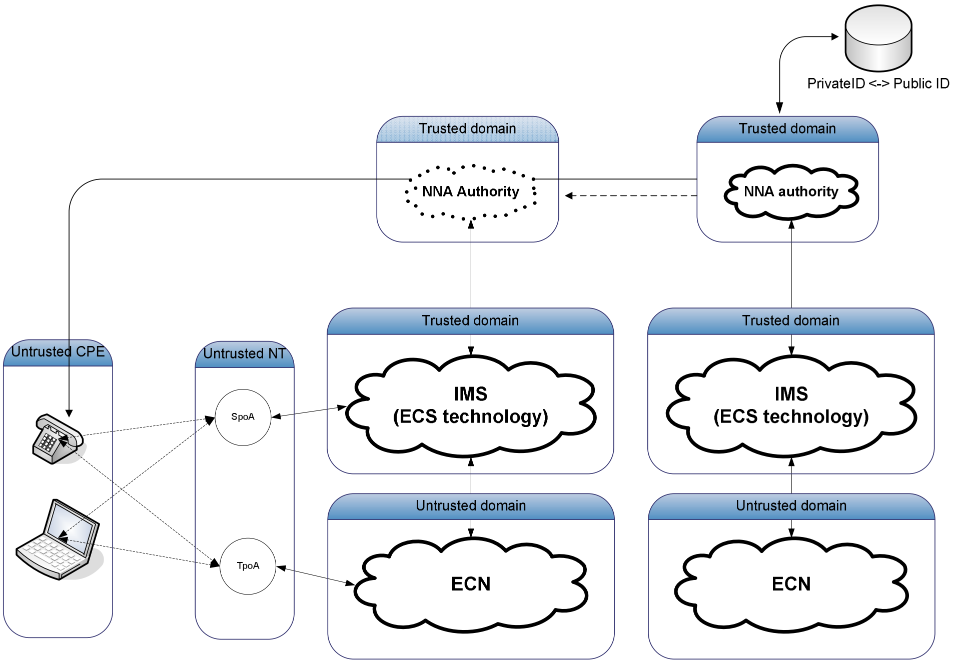


Figure C.6: NNA provisioning scenario

C.5.2 Signalling scenario

Once names, numbers and addresses have been provisioned, they need to be used. Usage happens when a user is being called or messaged. Figure C.7 shows the details of such a scenario. The figure shows two user's terminals each connected to an ECS and an ECN.

When ECS-1 needs to place a call on behalf of CPE-1 to another user, ECS-1 queries its ENUM server. This server is populated with data provided by higher ENUM server and possibly with proprietary data. The ENUM server will provide ECS-1 with either a direct SpoA on CPE-2 or with an SPoA on ECS-2. The signalling is now exchanged to establish the call.

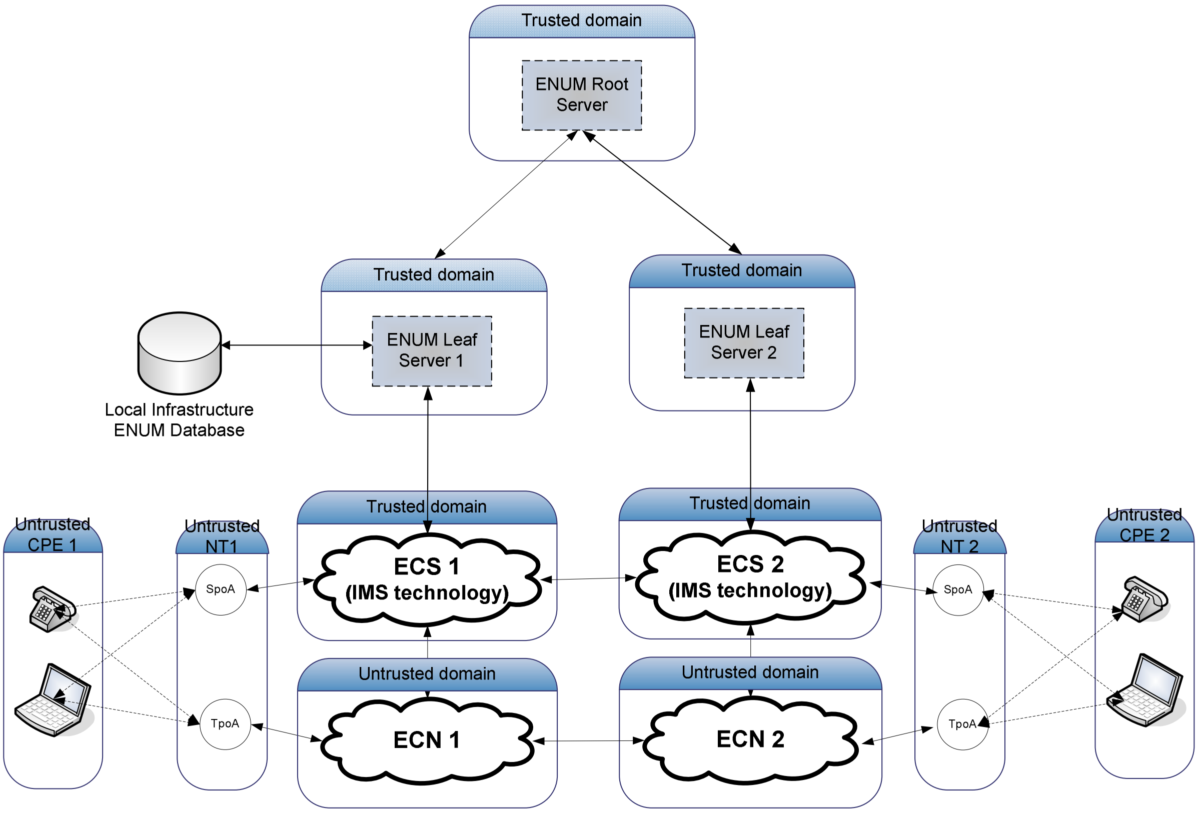


Figure C.7: Signalling scenario

C.5.3 Identification of assets

The assets of the NGN system under analysis are as follows:

- Protocols and their information elements visible at the open interfaces defined in the NGN architecture.
- Protocols and their information elements visible at the interfaces to non-NGN systems.
- Operations required to distribute identity.
- Operations required to secure communication.

Assets can be classified and sub-classified in a number of ways. The top level of classification is the asset type shown in table C.4.

Table C.4: Asset type classification

Asset type
Human
Logical
Physical
System

C.5.4 Logical Assets

The Logical assets of the ENUM system under analysis are:

- Signalling content (DNS results, etc.).
- A user/terminal's Private ID (e.g. IMSI, IP address, MAC address etc.).
- A user's public IDs (e.g. MISDN, SIP-URI, etc.).
- Encryption and trust keys.

Logical assets are deployed or made visible through a number of processes (where the processes themselves form additional logical assets):

- Distribution (from an authority to the terminal/user).
- Storage (in the terminal or the authority).
- Usage (when registration or setting up a session).

Threats may include manipulation, copying/interception (thus breaking privacy), impersonation, DoS.

C.5.5 Physical Assets

The Physical assets of the ENUM system under analysis are:

- Authentication store (database).
- DNS/ENUM servers:
  - ENUM core server;
  - ENUM Leaf server.
- End-user terminal (PC).
- Network links:
  - network link in the residential net (wired);
  - network link in the residential net (wireless);
  - link from access net to service net;
  - link from residence to access net;
  - link to ENUM leaf server.
- Routers:
  - broadband router in residential network;
  - router for ENUM core server;
  - router for ENUM leaf server;
  - router in access net;
  - router in service net.
- ENUM clients such as SIP or other session server.

For these physical assets the following threats are considered:

- DoS on the servers.
- Network disruption.
- Interception.
- Impersonation.
- Modification of the database.

C.5.6 Summary of assets

The assets of the ENUM system under analysis are:

- Access network topology.
- Authentication store (database).
- Broadband router in residential network.
- DNS cache.
- DNS Query.
- DNS response.
- End-user.
- End-user terminal (embedded, e.g. smartphone).
- End-user terminal (PC).
- ENUM core server.
- ENUM DNS records.
- ENUM Leaf server.
- ENUM message.
- ENUM query.
- ENUM response.
- ENUM server keys.
- Firewall.
- Firewall Rule (block DNS port).
- IP address.
- IPsec stack.
- Link from access net to service net.
- Link from residence to access net.
- Link to ENUM core server.
- Link to ENUM leaf server.
- Management credentials.

- Media.
- NAPTR record.
- NAT table.
- Network link in the residential net (wired).
- Network link in the residential net (wireless).
- Network maintenance personnel.
- Private user ID.
- Public user IDs.
- Router for ENUM core server.
- Router for ENUM leaf server.
- Router in access net.
- Router in service net.
- RTP packet.
- Service maintenance personnel.
- Service network topology.
- Signature on NAPTR.
- Stored user credentials (DB).
- Stored user credentials (Term).
- TCP stack.
- TCP/IP packet.
- Terminal IP address.
- Topology information.
- UDP/IP packet.

C.5.7 Relationships between assets

Logical assets (or contained assets) have to be deployed in a physical asset (or container asset) and the combinations considered in the analysis are shown in table C.5.

Table C.5: Pairings of logical (contained) and physical (container) assets

Logical (contained) asset	Physical (container) asset
ENUM data in transit	link to ENUM leaf server
	Network link in the residential net (wired)
	Network link in the residential net (wireless)
ENUM DNS records	ENUM Leaf server
ENUM query	SIP or other session server
ENUM server keys	ENUM Leaf server
NAPTR record	ENUM core server
	ENUM Leaf server
private user ID	end-user terminal (PC)
public user IDs	Authentication store (database)
	end-user terminal (PC)
Service network topology	router in service net
Signature on NAPTR	ENUM Leaf server

C.6 Vulnerabilities in ENUM (eTVRA Step 4)

C.6.1 Weakness in ENUM (eTVRA Step 4a)

The weaknesses of the ENUM system under analysis are:

- Susceptibility to buffer overflow:
  - May be used to attack a server by forcing an operating system exception. Affects physical hardware.
- Customer data in DNS:
  - This weakness is a consequence of the DNS and ENUM link and may lead to violations of data privacy laws.
- Disruptable server call state.
- Illegal message content.
- Illegal message format.
- Limited Internet transport capacity.
- Readable keys.
- Re-usable/predictable credentials.
- Unencrypted LAN communication.
- Use of outdated routing data.
- Use of unauthenticated data.
- Weak encryption keys.
- Writable data records.
- Writable DNS cache.
- Writable router cache.
- Writable server credentials.

C.6.2 Threat agents in ENUM (eTVRA Step 4b)

The threat agents that apply to the ENUM system under analysis are:

- Badly encrypted signalling interception.
- DNS cache poisoning.
- DNS data manipulation in server.
- ENUM credential manipulation.
- Man-in-the-middle attack (rogue DNS replies).
- Overload of communication (DNS flood).
- Overload of communication (illegal SIP packet).
- Overload of communication (IP flood).
- Overload of communication (IPsec flood).
- Reading public DNS data.
- Router IP cache poisoning.
- Social engineering.
- Unencrypted signalling interception.

C.6.3 Identification of vulnerabilities in ENUM (eTVRA Step 4.1)

As identified in the main body of the present document (clause 4.2) to be considered a vulnerability of an asset both a weakness and a viable threat enacted by a threat agent have to exist.

Table C.6: Vulnerabilities in ENUM

ID	Asset Name	Weakness Name	ThreatAgent
97	user credentials in database IN Authentication store (database)	Writable DNS cache	USER credential manipulation in Database
100	user credentials in database IN Authentication store (database)	Writable server credentials	USER credential manipulation in Database
102	topology information IN Residential router	writable router cache	Router IP cache poisoning
125	ENUM data in transit IN link to ENUM leaf server	Limited Internet transport capacity	overload of communication (DNS flood)
126	ENUM data in transit IN link to ENUM leaf server	Unencrypted LAN communication	Unencrypted signalling interception
127	ENUM data in transit IN link to ENUM leaf server	Weak encryption keys	Badly encrypted signalling interception
128	NAPTR record IN ENUM core server	Writable data records	DNS data manipulation in server
137	Signature on NAPTR IN ENUM Leaf server	Writable data records	ENUM credential manipulation
138	ENUM DNS records IN ENUM Leaf server	Writable DNS cache	DNS cache poisoning
139	ENUM server keys IN ENUM Leaf server	Readable keys	ENUM credential manipulation
140	ENUM DNS records IN ENUM Leaf server	Limited Internet transport capacity	overload of communication (DNS flood)
141	ENUM DNS records IN ENUM Leaf server	Unencrypted LAN communication	man-in-the-middle attack (rogue DNS replies)
142	ENUM server keys IN ENUM Leaf server	Writable data records	DNS data manipulation in server
143	ENUM DNS records IN ENUM Leaf server	Writable data records	DNS data manipulation in server
146	NAPTR record IN ENUM Leaf server	Writable data records	DNS data manipulation in server
150	ENUM query IN SIP or other session server	Limited Internet transport capacity	overload of communication (IP flood)
162	NAPTR record IN ENUM Leaf server	customer data in DNS	reading public DNS data
163	NAPTR record IN ENUM core server	customer data in DNS	reading public DNS data
164	NAPTR record IN ENUM core server	Limited Internet transport capacity	overload of communication (IP flood)
173	ENUM data in transit IN Network link in the residential net (wired)	Limited Internet transport capacity	overload of communication (IP flood)
174	ENUM data in transit IN Network link in the residential net (wired)	Unencrypted LAN communication	Unencrypted signalling interception
175	ENUM data in transit IN Network link in the residential net (wired)	Weak encryption keys	Badly encrypted Media interception
188	ENUM query IN SIP or other session server	Use of outdated routing data	man-in-the-middle attack (rogue DNS replies)
189	TCP stack IN SIP or other session server	Disruptable server call state	closing of TCP server sessions (birthday attack)
191	ENUM data in transit IN Network link in the residential net (wired)	Use of unauthenticated data	man-in-the-middle attack (rogue DNS replies)
192	ENUM data in transit IN Network link in the residential net (wireless)	Use of unauthenticated data	man-in-the-middle attack (rogue DNS replies)
193	ENUM query IN SIP or other session server	Use of unauthenticated data	man-in-the-middle attack (rogue DNS replies)

C.7 Risk assessment for ENUM (eTVRA Step 5)

In establishing the risk the likelihood of attack against any vulnerability identified in step 4 is calculated. The result of this step is shown in table C.7.

Table C.7: Risk assessment for ENUM

Vulnerability	Expertise	Access	Equipment	Knowledge	Time
97	Proficient	Difficult	Standard	Public	≤ 1 week
100	Proficient	Difficult	Standard	Public	≤ 1 week
102	Proficient	Moderate	Standard	Public	≤ 1 week
125	Proficient	Unlimited	Standard	Public	≤ 1 day
126	Proficient	Moderate	Standard	Public	≤ 1 day
127	Layman	Moderate	Standard	Public	≤ 1 week
128	Proficient	Difficult	Standard	Public	≤ 1 week
137	Proficient	Difficult	Standard	Public	≤ 1 day
138	Proficient	Unlimited	Standard	Public	≤ 1 day
139	Proficient	Difficult	Standard	Public	≤ 1 day
140	Proficient	Unlimited	Standard	Public	≤ 1 day
141	Proficient	Moderate	Standard	Public	≤ 1 day
142	Proficient	Difficult	Standard	Public	≤ 1 week
143	Proficient	Difficult	Standard	Public	≤ 1 week
146	Proficient	Difficult	Standard	Public	≤ 1 week
150	Proficient	Unlimited	Standard	Public	≤ 1 day
151	Proficient	Moderate	Standard	Public	≤ 1 day
162	Layman	Unlimited	Standard	Public	≤ 1 day
163	Layman	Unlimited	Standard	Public	≤ 1 day
164	Proficient	Unlimited	Standard	Public	≤ 1 day
173	Proficient	Unlimited	Standard	Public	≤ 1 day
174	Proficient	Moderate	Standard	Public	≤ 1 day
175	Layman	Moderate	Standard	Public	≤ 1 week
188	Proficient	Moderate	Standard	Public	≤ 1 day
189	Proficient	Unlimited	Standard	Public	≤ 1 week
191	Proficient	Moderate	Standard	Public	≤ 1 day
192	Proficient	Moderate	Standard	Public	≤ 1 day
193	Proficient	Moderate	Standard	Public	≤ 1 day

C.8 ENUM risk classification (eTVRA Step 6)

The risks from the analysis performed in step 5 are tabulated below ordered by the risk classification.

Table C.8: Vulnerability ordered by vulnerability-id for critical risks only

Id	Asset Name	Asset Weakness	Unwanted Incident	Threat name	Risk classification
102	topology information IN Residential router	writable router cache	loss of reliability/loss of service	Router IP cache poisoning	Critical
125	ENUM data in transit IN link to ENUM leaf server	Limited Internet transport capacity	loss of reliability/loss of service	overload of communication (DNS flood)	Critical
126	ENUM data in transit IN link to ENUM leaf server	Unencrypted LAN communication	loss of privacy/loss of service	Unencrypted signalling interception	Critical
127	ENUM data in transit IN link to ENUM leaf server	Weak encryption keys	Loss of privacy	Badly encrypted signalling interception	Critical
138	ENUM DNS records IN ENUM Leaf server	Writable DNS cache	loss of service for many users	DNS cache poisoning	Critical
140	ENUM DNS records IN ENUM Leaf server	Limited Internet transport capacity	loss of reliability/loss of service	overload of communication (DNS flood)	Critical
141	ENUM DNS records IN ENUM Leaf server	Unencrypted LAN communication	loss of privacy/loss of service	man-in-the-middle attack (rogue DNS replies)	Critical
150	ENUM query IN SIP or other session server	Limited Internet transport capacity	loss of reliability/loss of service	overload of communication (IP flood)	Critical
162	NAPTR record IN ENUM Leaf server	customer data in DNS	Loss of privacy	reading public DNS data	Critical
163	NAPTR record IN ENUM core server	customer data in DNS	Loss of privacy	reading public DNS data	Critical
164	NAPTR record IN ENUM core server	Limited Internet transport capacity	loss of reliability/loss of service	overload of communication (IP flood)	Critical
173	ENUM data in transit IN Network link in the residential net (wired)	Limited Internet transport capacity	loss of reliability/loss of service	overload of communication (IP flood)	Critical
174	ENUM data in transit IN Network link in the residential net (wired)	Unencrypted LAN communication	loss of privacy/loss of service	Unencrypted signalling interception	Critical
175	ENUM data in transit IN Network link in the residential net (wired)	Weak encryption keys	Loss of privacy	Badly encrypted Media interception	Critical
188	ENUM query IN SIP or other session server	Use of outdated routing data	loss of privacy/loss of service	man-in-the-middle attack (rogue DNS replies)	Critical
191	ENUM data in transit IN Network link in the residential net (wired)	Use of unauthenticated data	Impersonation of a server	man-in-the-middle attack (rogue DNS replies)	Critical
192	ENUM data in transit IN Network link in the residential net (wireless)	Use of unauthenticated data	Impersonation of a server	man-in-the-middle attack (rogue DNS replies)	Critical
193	ENUM query IN SIP or other session server	Use of unauthenticated data	Impersonation of a server	man-in-the-middle attack (rogue DNS replies)	Critical

Table C.9: Vulnerability ordered by vulnerability-id

Id	Asset Name	Asset Weakness	Unwanted Incident	Threat name	Risk classification
97	user credentials in database IN Authentication store (database)	Writable DNS cache	loss of service for many users	USER credential manipulation in Database	Minor
100	user credentials in database IN Authentication store (database)	Writable server credentials	Impersonation of a server	USER credential manipulation in Database	Minor
102	topology information IN Residential router	writable router cache	loss of reliability/loss of service	Router IP cache poisoning	Critical
125	ENUM data in transit IN link to ENUM leaf server	Limited Internet transport capacity	loss of reliability/loss of service	overload of communication (DNS flood)	Critical
126	ENUM data in transit IN link to ENUM leaf server	Unencrypted LAN communication	loss of privacy/loss of service	Unencrypted signalling interception	Critical
127	ENUM data in transit IN link to ENUM leaf server	Weak encryption keys	Loss of privacy	Badly encrypted signalling interception	Critical
128	NAPTR record IN ENUM core server	Writable data records	loss of reliability/loss of service	DNS data manipulation in server	Minor
137	Signature on NAPTR IN ENUM Leaf server	Writable data records	loss of reliability/loss of service	ENUM credential manipulation	Minor
138	ENUM DNS records IN ENUM Leaf server	Writable DNS cache	loss of service for many users	DNS cache poisoning	Critical
139	ENUM server keys IN ENUM Leaf server	Readable keys	loss of privacy/Impersonation of a user	ENUM credential manipulation	Minor
140	ENUM DNS records IN ENUM Leaf server	Limited Internet transport capacity	loss of reliability/loss of service	overload of communication (DNS flood)	Critical
141	ENUM DNS records IN ENUM Leaf server	Unencrypted LAN communication	loss of privacy/loss of service	man-in-the-middle attack (rogue DNS replies)	Critical
142	ENUM server keys IN ENUM Leaf server	Writable data records	loss of reliability/loss of service	DNS data manipulation in server	Minor
143	ENUM DNS records IN ENUM Leaf server	Writable data records	loss of reliability/loss of service	DNS data manipulation in server	Minor
146	NAPTR record IN ENUM Leaf server	Writable data records	loss of reliability/loss of service	DNS data manipulation in server	Minor
150	ENUM query IN SIP or other session server	Limited Internet transport capacity	loss of reliability/loss of service	overload of communication (IP flood)	Critical
156	NAT table IN Residential router	Writable DNS cache	loss of service for many users	Router IP cache poisoning	Major
162	NAPTR record IN ENUM Leaf server	customer data in DNS	Loss of privacy	reading public DNS data	Critical
163	NAPTR record IN ENUM core server	customer data in DNS	Loss of privacy	reading public DNS data	Critical
164	NAPTR record IN ENUM core server	Limited Internet transport capacity	loss of reliability/loss of service	overload of communication (IP flood)	Critical
173	ENUM data in transit IN Network link in the residential net (wired)	Limited Internet transport capacity	loss of reliability/loss of service	overload of communication (IP flood)	Critical
174	ENUM data in transit IN Network link in the residential net (wired)	Unencrypted LAN communication	loss of privacy/loss of service	Unencrypted signalling interception	Critical

Id	Asset Name	Asset Weakness	Unwanted Incident	Threat name	Risk classification
175	ENUM data in transit IN Network link in the residential net (wired)	Weak encryption keys	Loss of privacy	Badly encrypted Media interception	Critical
176	SIP data in transit IN Network link in the residential net (wireless)	Unencrypted LAN communication	loss of privacy/loss of service	interception of SIP credentials	Critical
188	ENUM query IN SIP or other session server	Use of outdated routing data	loss of privacy/loss of service	man-in-the-middle attack (rogue DNS replies)	Critical
191	ENUM data in transit IN Network link in the residential net (wired)	Use of unauthenticated data	Impersonation of a server	man-in-the-middle attack (rogue DNS replies)	Critical
192	ENUM data in transit IN Network link in the residential net (wireless)	Use of unauthenticated data	Impersonation of a server	man-in-the-middle attack (rogue DNS replies)	Critical
193	ENUM query IN SIP or other session server	Use of unauthenticated data	Impersonation of a server	man-in-the-middle attack (rogue DNS replies)	Critical

C.9 ENUM countermeasure framework (eTVRA Step 7)

As identified in clause C.4 the main requirements are to counter masquerade and to provide proof of integrity (i.e. to detect, prevent and correct) errors in data transmission caused by malicious attack. The provisions of DNSSEC go some way to achieving these goals and the provision of generic integrity and authentication countermeasures have been analysed to show removal of critical risks in ENUM.

In addition to DNSSEC it is also possible to limit the access to the ENUM infrastructure as described for infrastructure ENUM (TR 102 055 [i.22]), which restricts access to the ENUM infrastructure to only trusted clients (SIP servers etc.). This addresses the threats that deal with interception, impersonation, DoS, etc.

Application of these Infrastructure ENUM as countermeasure requires that the risks are re-computed to allow for the presence of the countermeasure as described in clause 6.8.3. The risks to ENUM drop dramatically after the application of these countermeasures as shown in table C.10.

Table C.10: Residual risk by restriction of ENUM to infrastructure ENUM

Asset Name	Asset Weakness	Threat name	Classification
ENUM DNS records IN ENUM Leaf server	Writable data records	DNS data manipulation in server	Minor
ENUM DNS records IN ENUM Leaf server	Unencrypted communication	man-in-the-middle attack (rogue DNS replies)	Minor
ENUM DNS records IN ENUM Leaf server	Limited Internet transport capacity	overload of communication (IP flood)	Minor
ENUM data in transit IN Network link in the residential net (wireless)	Limited Internet transport capacity	overload of communication (IP flood)	Minor
ENUM data in transit IN Network link in the residential net (wireless)	Use of unauthenticated data	man-in-the-middle attack (rogue DNS replies)	Minor
ENUM data in transit IN Network link in the residential net (wired)	Use of unauthenticated data	man-in-the-middle attack (rogue DNS replies)	Minor
ENUM data in transit IN Network link in the residential net (wired)	Unencrypted communication	Unencrypted signalling interception	Minor
ENUM data in transit IN Network link in the residential net (wired)	Limited Internet transport capacity	overload of communication (IP flood)	Minor
ENUM data in transit IN link to ENUM leaf server	Limited Internet transport capacity	overload of communication (IP flood)	Minor
ENUM query IN SIP or other session server	Use of outdated routing data	man-in-the-middle attack (rogue DNS replies)	Minor
User Agent IN end-user terminal (PC)	Use of outdated routing data	man-in-the-middle attack (rogue DNS replies)	Minor
ENUM data in transit IN link to ENUM leaf server	Unencrypted communication	Unencrypted signalling interception	Minor
NAPTR record IN ENUM Leaf server	Writable data records	DNS data manipulation in server	Minor
NAPTR record IN ENUM core server	Limited Internet transport capacity	overload of communication (IP flood)	Minor
NAPTR record IN ENUM core server	Writable data records	DNS data manipulation in server	Minor
Signature on NAPTR IN ENUM Leaf server	Writable data records	ENUM credential manipulation	Minor
ENUM query IN SIP or other session server	Limited Internet transport capacity	overload of communication (IP flood)	Minor
ENUM server keys IN ENUM Leaf server	Writable data records	DNS data manipulation in server	Minor
ENUM server keys IN ENUM Leaf server	Readable keys	ENUM credential manipulation	Minor
ENUM query IN SIP or other session server	Use of unauthenticated data	man-in-the-middle attack (rogue DNS replies)	Minor
ENUM Leaf server	Limited server processing capacity	overload of communication (DNS flood)	Minor
ENUM core server	Limited server processing capacity	overload of communication (DNS flood)	Minor
ENUM DNS records IN ENUM core server	Writable DNS cache	DNS cache poisoning	Minor
ENUM DNS records IN ENUM Leaf server	Writable DNS cache	DNS cache poisoning	Minor
NAPTR record IN ENUM core server	customer data in DNS	reading public DNS data	Minor
NAPTR record IN ENUM Leaf server	customer data in DNS	reading public DNS data	Minor

C.10 Completed eTVRA proforma for ENUM

A Security Environment		
A.1 Assumptions		
a.1.1	ENUM lies on top of DNS	
a.1.2	ENUM refers to a system of use and not just to RFC 3761 [i.25] and RFC 3403 [i.26] that define the use of DNS for storage of E.164 numbers and the NAPTR records that populate it	
a.1.3	ENUM may be deployed in a number of ways (e.g. user-ENUM, infrastructure-ENUM)	
A.2 Assets		
1	ENUM Leaf server	(NONE)
3	Authentication store (database)	(NONE)
4	SIP or other session server	(NONE)
5	Network link in the residential net (wired)	(NONE)
7	end-user terminal (PC)	(NONE)
8	end-user	(NONE)
9	Network link in the residential net (wireless)	(NONE)
10	link from residence to access net	(NONE)
11	router in access net	(NONE)
12	link from access net to service net	(NONE)
13	router in service net	(NONE)
14	router for ENUM leaf server	(NONE)
15	router for ENUM core server	(NONE)
16	link to ENUM leaf server	(NONE)
17	ENUM core server	(NONE)
18	broadband router in residential network	(NONE)
19	service maintenance personnel	(NONE)
20	network maintenance personnel	(NONE)
22	NAPTR record	(NONE)
23	Stored user credentials (DB)	(NONE)
24	call state	RFC 3261 [i.18] SIP
25	SIP message	RFC 3261 [i.18] SIP
26	ENUM message	(NONE)
27	topology information	(NONE)
28	Stored user credentials (Term)	(NONE)
29	Stored credentials (user)	(NONE)
31	management credentials	(NONE)
32	Signature on NAPTR	(NONE)
33	ENUM server keys	(NONE)
34	ENUM DNS records	(NONE)
35	ENUM query	(NONE)
36	private user ID	(NONE)
37	public user IDs	(NONE)
38	call state perception	(NONE)
39	DNS cache	(NONE)
40	NAT table	(NONE)
41	IP address	(NONE)
42	Terminal IP address	(NONE)
43	DNS Query	(NONE)
44	DNS response	(NONE)
45	ENUM response	(NONE)
46	SIP payload	(NONE)
47	service network topology	(NONE)
48	access network topology	(NONE)
49	call state machine	(NONE)
50	media	(NONE)
51	User Agent	(NONE)
52	TCP stack	(NONE)
53	IPsec stack	(NONE)
56	SIP+ENUM test system	(NONE)
58	Firewall	(NONE)
59	Firewall Rule (block DNS port)	(NONE)

60	link to ENUM core server		(NONE)
61	end-user terminal (embedded, e.g. smartphone)		(NONE)
62	TCP/IP packet		(NONE)
63	UDP/IP packet		(NONE)
64	RTP packet		(NONE)
A.3Threat agents			
1	DNS cache poisoning		*Citation for full text*
2	USER credential manipulation in Database		
3	interception of SIP credentials		
4	closing of SIP server sessions (rogue bye request)		
5	overload of communication (IP flood)		
6	Unencrypted Media interception		
7	DNS data manipulation in server		
8	man-in-the-middle attack (rogue DNS replies)		
11	theft of customer data		
14	Impersonation of a SIP user (forged responses)		
16	Hacking/Cracking into the system		
17	Hacking/Cracking into the system		
22	closing of SIP client sessions (roque bye request)		
23	closing of TCP server sessions (birthday attack)		
24	Rogue DHCP messages		
25	closing of SIP server sessions (Repeated INVITE)		
26	closing of SIP server sessions (roque CANCEL)		
27	ENUM credential manipulation		
28	USER credential manipulation in PC		
29	Router IP cache poisoning		
30	Badly encrypted Media interception		
31	Unencrypted signalling interception		
32	Badly encrypted signalling interception		
33	overload of communication (SIP flood)		
34	overload of communication (illegal SIP packet)		
35	overload of communication (DNS flood)		
36	theft of management data		
37	reading public DNS data		
39	sending illegal IPsec messages		
40	overload of communication (IPsec flood)		
41	theft of credentials on net		
42	USER credential manipulation in embedded terminal		
43	theft of credentials from PC		
44	theft of credentials from embedded terminal		
45	Social engineering		
a.4 Threats			
a.4.1	*Short text describing threat*		*Citation for full text*
a.4.2			
a.5 Security policies (OPTIONAL)			
a.5.1	*Short text describing security policy*		*Citation for full text*
a.5.2			
B Security Objectives			
b.1 Security objectives for the asset			
b.1.1	*Short text describing objective for the asset*		*Citation for full text*
b.1.2			
b.2 Security objectives for the environment			
b.2.1	*Short text describing objective for the requirement*		*Citation for full text*
b.2.2			
C IT Security Requirements			
c.1 asset security requirements			
c.1.1 asset security functional requirements			
c.1.1.1	The stored data is continually monitored to detect errors in its integrity.	FDP_SDI.1	*Citation for full text*

c.1.1.2	The stored data is continually monitored to detect errors in its integrity and actions to be taken in the event of errors being found are defined.	FDP_SDI.2	
c.1.1.3	The data that is transferred is monitored to detect errors in its integrity.	FDP_UIT.1	
c.1.1.4	The data that is transferred is monitored to detect errors in its integrity and actions to be taken in the event of errors being found using assistance from the source are defined (i.e. the error is reported to the source and both source and destination take part in the corrective action).	FDP_UIT.2	
c.1.1.5	The data that is transferred is monitored to detect errors in its integrity and actions to be taken in the event of errors being found without using assistance from the source (i.e. the corrective action takes place only at the receiver).	FDP_UIT.3	
c.1.1.6	The user is not allowed to perform any action prior to successful authentication.	FIA_UAU.2	
c.1.1.7	The authentication procedure should ensure that forged or copied authentication data cannot be used.	FIA_UAU.3	
c.1.1.8	The user is not allowed to perform any action prior to successful identification.	FIA_UID.2	
c.1.2 asset security assurance requirements			
c.1.2.1	*Short text describing security assurance requirement*	*ISO15408 [i.32] class*	*Citation for full text*
c.1.2.2			
c.2 Environment security requirements (OPTIONAL)			
c.2.1	*Short text describing security environment requirement*	*ISO15408 [i.32] class*	*Citation for full text*
c.2.2			
D Application notes (OPTIONAL)			
E Rationale			
The eTVRA should define the full rational, if this is true only a citation (reference) to the full text is required			

Annex D: TVRA of IPTV in NGN-R2

NOTE 1: The scope of this annex is only the functionality provided for NGN-R2.

NOTE 2: The detail requirements identified in this analysis are also stated in TS 187 001 [i.6].

D.1 Step 0: Description of ToE (IPTV)

Internet Protocol Television (IPTV) is a system where a digital television service is delivered using the Internet Protocol (IP) over a network infrastructure. For the NGN the network infrastructure is provided by NASS and RACS.

D.1.1 IPTV stakeholders

For the TVRA of IPTV to be focused, the stakeholders of IPTV in a NGN context be identified and described. There are six main stakeholders in IPTV for NGN described below:

Content Provider: the entity that owns or is licensed to sell content or content assets. Although the IPTV Service Provider is the primary source for the Consumer, a direct logical information flow may be set up between Content Provider and Consumer, for example for rights management and content protection. How the Content Provider receipts content from its owners is outside the scope of the present document. Consumers may also be originators of content.

IPTV Service Provider: the entity that prepares the content bundle provided by the content provider for delivery to the consumer by providing metadata, content encryption and physical binaries. How the IPTV Service Provider receipts content from the Content Provider is outside the scope of the present document.

NGN Service Provider: the entity offering IP based services, which shares a consistent set of policies and common technologies. It handles user authentication/identification, Service Control and security, Charging, IPTV common functions, etc. Several IPTV Service Providers could use the same NGN Service Provider to delivery contents to the consumer. The NGN Service Provider may also provide IPTV service.

Access Service Provider: the entity that provides the underlying IP transport connectivity between the consumer and the NGN entities.

Consumer: The domain where the IPTV services are consumed. The consumer domain may consist of a single terminal, used directly for service consumption, or may be a network of terminals and related devices, including mobile devices. Note that a single consumer domain may be connected obtaining content from multiple Content providers.

End-user: The domain where free of charge and controlled IPTV services are consumed. The control is performed by the consumer. An example of controlled IPTV services is parental control. An example of free of charge IPTV services is a limited time free of charge Broadcast TV due to advertisement purposes or similar.

Figure D.1 shows the IPTV stakeholders and the categories of service involved in IPTV for NGN.

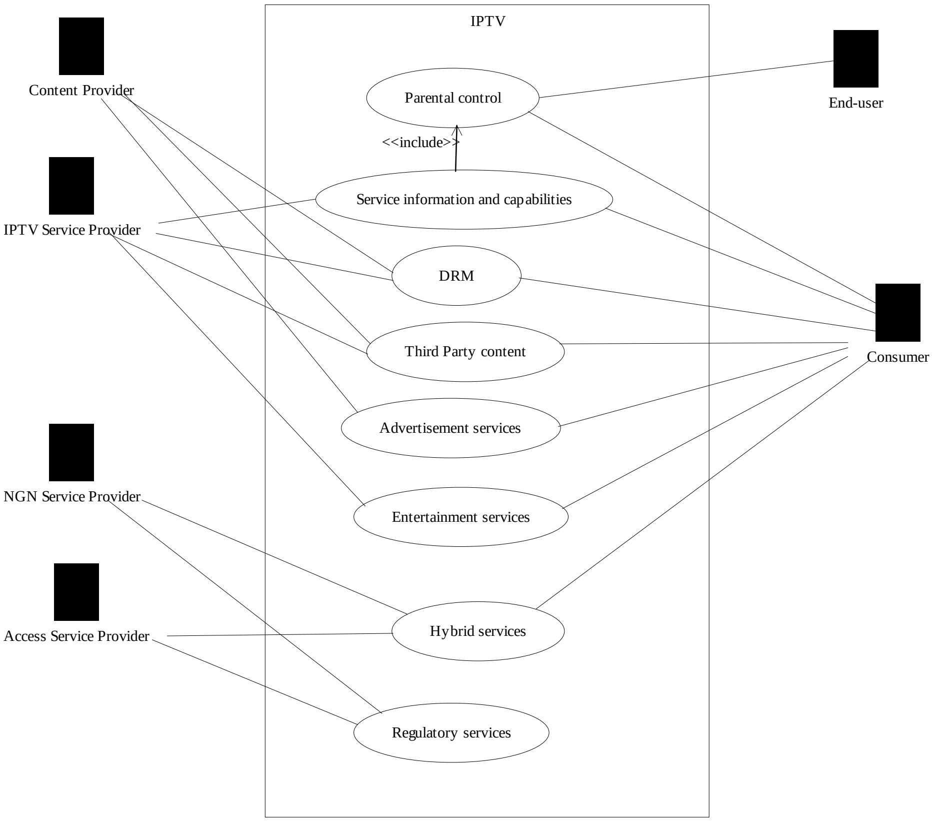


Figure D.1: IPTV stakeholders and main service categories

According to TS 181 016 [i.44] there are six main service categories within IPTV. These are entertaining, advertising, regulatory, hybrid service, third party content and service information. Figure D.1 outlines these categories and how they relate to the stakeholders of IPTV.

Entertainment services include:

- Broadcast TV;
- Trick Modes using PVR;
- Pay Per View;
- Video on Demand (VoD);
- Near VoD;
- Interactive TV;
- Push VoD; and
- Audio.

Regulatory services include:

- Emergency Information;
- Application for the disabled;
- Content Advisories; and
- Educational facilities.

Service information and capabilities include:

- Electronic Programme Guide (EPG);
- Service Discovery and Selection;
- IPTV User Profile;
- Parental Control Service; and
- Notification Services.

Figure D.2 presents the high-level and general service architecture of IPTV.

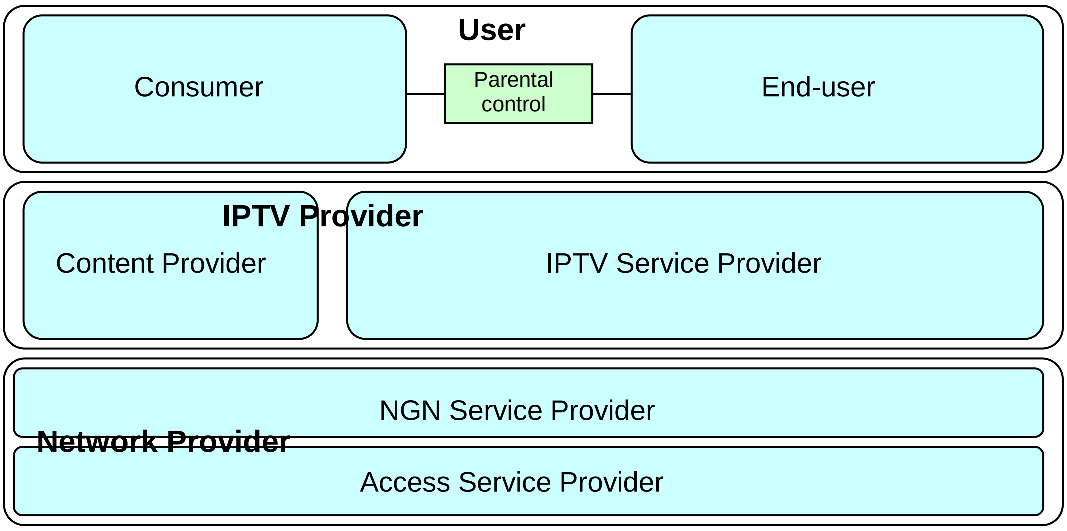


Figure D.2: General IPTV architecture

The high-level service architecture is comprised of the three layers Network Provider, IPTV Provider and User. The lowest service layer contains the various capabilities of the underlying network. The middle service layer is where the value of IPTV to the consumer is provided. The highest layer is comprised of the two main user types, which is consumer and end-user.

D.2 Step 1: Identification of objectives

In TVRA, system objectives are composed of security objectives and assurance objectives. The assurance objectives concern the desired confidence level needed in the results provided of the fulfilment of the security objectives. In practise, this refers to the level of details, rigour and coverage that the results of the TVRA need to provide. The security objectives are used to specify the desired goal for the capabilities of the system (security) attributes authentication, accountability, confidentiality, availability and integrity.

D.2.1 Void

D.2.2 (System) Security Objectives

D.2.2.1 Security objective category authentication

- OBJ1 - A NGN R2 IPTV should allow end-to-end authentication of content to consumers and end-users.
- OBJ2 - A NGN R2 IPTV should allow authentication of consumers and end-users or named groups of consumers or end-users.

- OBJ3 - A NGN R2 IPTV should allow authentication of relevant devices.
- OBJ4 - A NGN R2 IPTV should allow authentication of content such that it can be separated and such that consumers and end-users can distinguish between various types of contents to allow e.g. parent controls.

D.2.2.2 Security objective category accountability

- OBJ5 - A NGN R2 IPTV allow for proper accountability of consumers for billing purposes.

D.2.2.3 Security objective category confidentiality

- OBJ6 - A NGN R2 IPTV should allow sufficient level of privacy for consumers, end-users, involved providers and their private or sensitive *information.*
- OBJ7 - A NGN R2 IPTV should allow proper level of confidentiality of content.
- OBJ8 - A NGN R2 IPTV should permit proper level of confidentiality of relevant devices.

D.2.2.4 Security objective category integrity

- OBJ9 - A NGN R2 IPTV should allow end-to-end integrity protection of content.
- OBJ10 - A NGN R2 IPTV should allow integrity of billing related events and information.

D.2.2.5 Security objective category availability

- OBJ11 - A NGN R2 IPTV should allow availability of IPTV services upon request to consumers and end-users and prevent both unintentional and intentional DoS attacks against IPTV services.

D.3 Step 2: Identification of requirements

The system requirements are dependent on the system objectives identified in Step 1 and come in two variants:

- security requirements; and
- assurance requirements.

The assurance requirements are derived from the assurance objectives as a selection of ISO/IEC 15408-2 [i.31] security assurance components. Security requirements are derived from the security objectives from Step 1. As for the security objectives, the security requirements are categorized into the five categories, here requirement categories, authentication, accountability, confidentiality, integrity and availability.

D.3.1 Security requirements category authentication

From OBJ1 the following security requirements are derived.

(OBJ1 - A NGN R2 IPTV should allow end-to-end authentication of content to consumers and end-users):

- A NGN R2 IPTV support means to uniquely identify objects and named groups of objects.
- A NGN R2 IPTV support means to authenticate objects and named groups of objects.
- A NGN R2 IPTV support means to authorize objects and named groups of objects to consumers and named groups of consumers.
- A NGN R2 IPTV support means to authorize objects and named groups of objects to end-users and named groups of end-users.

From OBJ2 the following security requirements are derived.

(OBJ2 - A NGN R2 IPTV should allow proper authentication of consumers and end-users or named groups of consumers or end-users):

- A NGN R2 IPTV support means to uniquely identify consumers and named groups of consumers.
- A NGN R2 IPTV support means to uniquely identify end-users and named groups of end-users (subscriber groups).
- A NGN R2 IPTV support means to authenticate consumers and named groups of consumers.
- A NGN R2 IPTV support means to authenticate end-users and named groups of end-users (subscriber groups).
- A NGN R2 IPTV support means to authorize consumers and named groups of consumers.
- A NGN R2 IPTV support means to authorize end-users and named groups of end-users (subscriber groups).

From OBJ 3 the following security requirements are derived.

(OBJ3 - A NGN R2 IPTV should permit proper authentication of relevant devices):

- A NGN R2 IPTV support means to uniquely identify devices and named groups of devices.
- A NGN R2 IPTV support means to authenticate devices and named groups of devices.
- A NGN R2 IPTV support means to authorize devices and named groups of devices.

From OBJ4 the following security requirements are derived.

(OBj4 - A NGN R2 IPTV should allow proper authentication of content such that it can be separated and such that consumers and end-users can diverse between various types of contents to allow e.g. parent controls and alike):

- A NGN R2 IPTV support means to uniquely identify content and named groups of content.
- A NGN R2 IPTV support means to authenticate content and named groups of content.
- A NGN R2 IPTV support means to authorize content and named groups of content to consumers and named groups of consumers.
- A NGN R2 IPTV support means to authorize content and named groups of content to end-users and named groups of end-users.

D.3.2 Security requirement category accountability

From OBJ5 the following security requirements are derived.

(OBJ5 - A NGN R2 IPTV allow for proper accountability of consumers for billing purposes):

- A NGN R2 IPTV support means to uniquely identify billing relevant information (events and messages).
- A NGN R2 IPTV support means to record billing relevant information and ensure proper integrity control of these pieces of information.
- A NGN R2 IPTV support proper audit control (mechanism) for the recorded billing relevant information.
- A NGN R2 IPTV should support proper confidentiality of the recorded billing relevant information (need to consider if this is necessary).

D.3.3 Security requirement category confidentiality

From OBJ6 the following security requirements are derived.

(OBJ6 - A NGN R2 IPTV should allow proper level of privacy for consumers, end-users, involved providers and their private or sensitive information):

- A NGN R2 IPTV support means to uniquely identify consumers.
- A NGN R2 IPTV support means to uniquely identify end-users.
- A NGN R2 IPTV support means to uniquely identify providers.
- A NGN R2 IPTV support means to restrict and control access to stored information or similar objects to only authorized subjects using some sort of access control mechanism:
    - A NGN R2 IPTV should support means to classify information in terms of *information types*, such as e.g. private, sensitive, public etc. (assignment: *information types* to be specified) or similar.
    - A NGN R2 IPTV provide proper access control mechanism in line with the above.
- A NGN R2 IPTV support means for end-to-end encryption of sensitive or private information while being transferred between logical communicating parties:
    - A NGN R2 IPTV should support means for cryptographic key management.
    - A NGN R2 IPTV support cryptographic operations.

From OBJ7 the following security requirements are derived.

(OBJ7 - A NGN R2 IPTV should allow proper level of confidentiality of):

- A NGN R2 IPTV support means of uniquely identify content (and in particular content that needs protection against theft or which needs to be identified for parenting control reasons or similar).
- A NGN R2 IPTV support means to restrict and control access to stored objects (information) to only authorized subjects using some sort of access control mechanism:
    - A NGN R2 IPTV should support means to classify information in terms of *content types* or similar.
    - A NGN R2 IPTV provide proper access control mechanism in line with the above.
- A NGN R2 IPTV support means for end-to-end encryption of content while being transferred between logical communicating parties:
    - A NGN R2 IPTV should support means for cryptographic key management.
    - A NGN R2 IPTV support cryptographic operations.

From OBJ8 the following security requirements are derived.

(OBJ8 - A NGN R2 IPTV should permit proper level of confidentiality of relevant devices):

- A NGN R2 IPTV support means of uniquely identify devices.
- A NGN R2 IPTV support means to restrict and control access to devices to authorized subjects only using some sort of access control mechanism:
    - A NGN R2 IPTV should support means to classify devices in terms of *device types* or similar.
    - A NGN R2 IPTV provide proper access control mechanism in line with the above.

D.3.4 Security requirement category integrity

From OBJ9 the following security requirements are derived.

(OBJ9 - A NGN R2 IPTV should allow end-to-end integrity of content):

- A NGN R2 IPTV support means to restrict and control access to content to authorized subjects only:
    - A NGN R2 IPTV support means of uniquely identify subjects.
    - A NGN R2 IPTV support means of authenticate and authorize subjects.
    - A NGN R2 IPTV support means of control and restrict operations that authorized subjects can perform on content (object).
- A NGN R2 IPTV should support means of audit control of operations performed on content by authorized and unauthorized subjects.
- A NGN R2 IPTV support means of preventing manipulation (such as reproduction, copying, replay) of content while stored on media:
    - A NGN R2 IPTV should support means for cryptographic key management for stored content.
    - A NGN R2 IPTV support cryptographic operations for integrity purposes of stored content.
- A NGN R2 IPTV support means of preventing manipulation (such as reproduction, copying, replay) of content while being transferred between logical communicating parties:
    - A NGN R2 IPTV should support means for cryptographic key management for transferred content.
    - A NGN R2 IPTV support cryptographic operations for integrity purposes for transferred content.

From OBJ10 the following security requirements are derived.

(OBJ10 - A NGN R2 IPTV should allow integrity of billing related events and information):

- A NGN R2 IPTV should support means of preventing and/or detecting modification of billing related events and information.
- A NGN R2 IPTV should support means of detecting fraudulent billing related events and information.
- A NGN R2 IPTV should support means of audit control for billing related events and information.

D.3.5 Security requirement category availability:

From OBJ11 the following security requirements are derived.

(OBJ11 - A NGN R2 IPTV should allow availability of network to consumers and end-users):

- A NGN R2 IPTV should support means of detecting unauthorized use of resources (such as various DoS and virus attacks).
- A NGN R2 IPTV should support means of allocating proper resources to authorized use (QoS).

D.4 Step 3: Inventory of the assets

In Step 3 usage scenarios should be provided and assets should be derived from those:

- A family has four children of various ages from 4 to 22. The parents want to make four different parental controls to allow each child to have content tailored to their needs and age. This is only possible if the parents can associate different identities and thus authentication to the various parental control profiles.

- One or more content providers and an IPTV service provider decide to open a selection of the contents for a limited time frame to attract new consumers. No registration is needed for the use of the service. In this case there might be more practical to have the ability to separate between paying customers (consumers) and drop-in customers (end-users).

Annex E: TVRA of NAT and NAT-T in NGN-R2

NOTE 1: The scope of this annex is only the functionality provided for NGN-R2.

NOTE 2: The detail requirements identified in this analysis are also stated in TS 187 001 [i.6].

E.1 Step 0: Description of NAT and NAT-T in NGN-R2

Network Address Translators (NATs) translate addresses between one IP addressing "realm" and another. This mapping is most commonly done between a private address space using addresses set aside for that purpose described in RFC 1918 [i.37] and a public address space. This mapping is commonly referred to as a NAT binding as the NAT has bound together the tuple of PrivateIPAddress:Port to the tuple of PublicIPAddress:Port to allow the subsequent response packets from the external endpoint to be forwarded to the proper internal host. The term NAT in the present document also refers to Network Address Port Translation (NAPT) devices which also translate port addresses in order to reduce the number of public addresses used on the public address side of the NAT (i.e. PrivateIPAddress:PrivatePort to PublicIPAddress:PublicPort).

In addition to address translation, NAT devices may also exhibit firewall characteristics wherein traffic coming across the NAT (from "outside" to "inside" the NAT/FW device) is passed or blocked based on filtering rules.

Functionally NAT includes the following operations:

- Address binding;
- Address lookup and translation;
- Address unbinding;
- Recalculation of checksums in the IP header (as described in clause 3.3 of RFC 1631 [i.36]).

The use of NAT in both IPv4 and IPv6 is likely, in the former as a response to address shortage, in the latter as a method for address privacy.

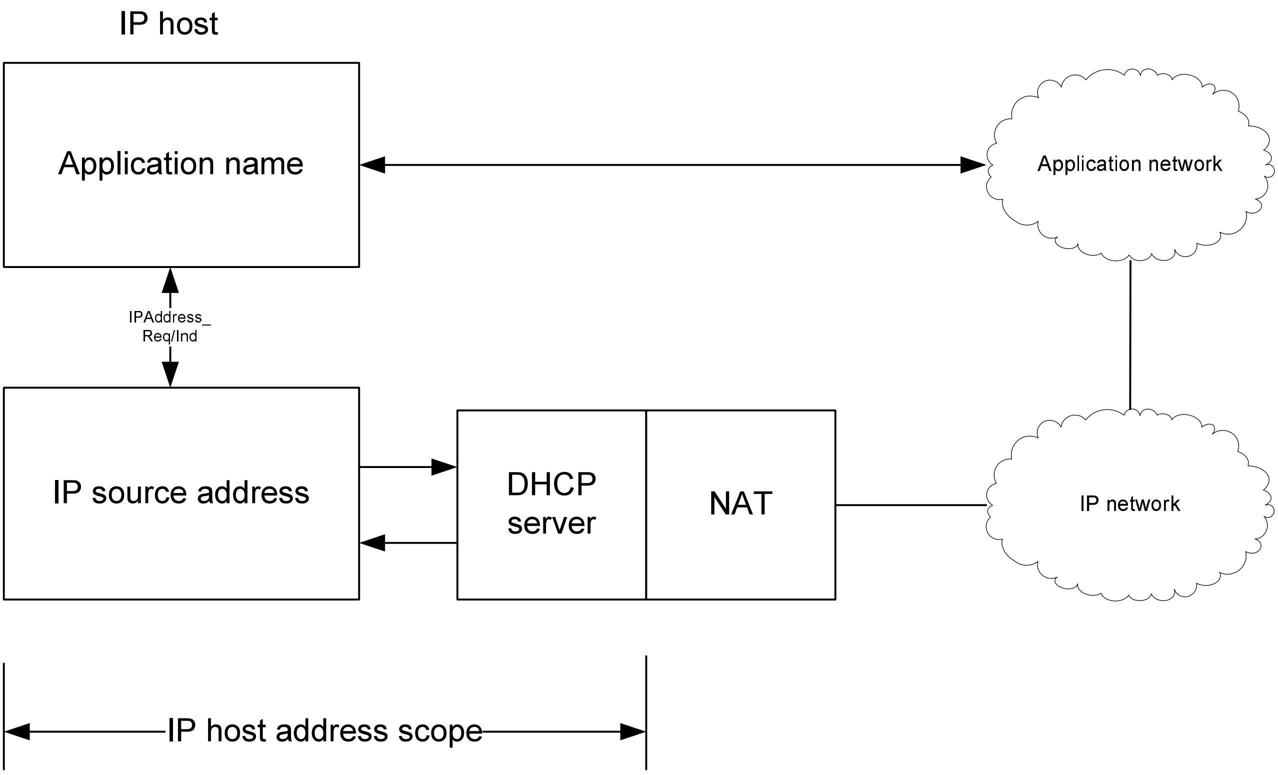


Figure E.1: NAT Traversal problem

When an application uses the Host IP Address in establishing a session with an application network outside the scope of host's IP address then any use of that IP address by the application network is invalid.

NAT traversal is a term used to describe the problem of establishing connections between hosts in private IP networks which use NAT devices (either locally or remotely) to mask their local IP address (i.e. the IP address assigned in the private IP network) whilst giving themselves global connectivity by sharing the public IP address of the gateway to the global IP network.

The techniques used to solve the NAT Traversal problem are of two main types (although mechanisms combining these are also promoted):

- NAT traversal protocols and techniques based on NAT behaviour.
- NAT traversal based on NAT control.

The result of NAT Traversal is that the source-address presented by an application protocol (e.g. SIP) is valid in the application domain for the presented name without requiring that the application name be a Fully Qualified Domain Name (FQDN) and without relying on resolution protocols to determine the address associated with a name.

Figure E.2 depicts the NGN R2 NAT traversal reference architecture.

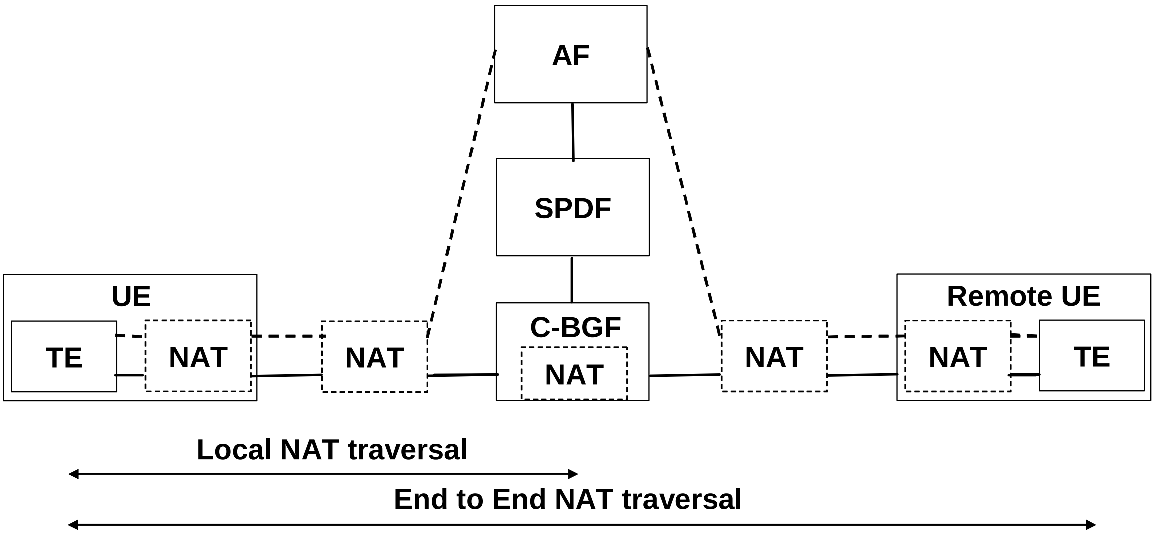


Figure E.2: Reference architecture for NGN R2 NAT

Within NGN-R2 a NAT may be found at a number of locations on both media and signalling paths:

- in UE;
- between the UE and the C-BGF; and
- in C-BGF.

E.2 Step 1: Identification of objectives

E.2.1 (System) Security Objectives

The security objectives to be met by NAT-T in the NGN are tabulated in table E.1. Each objective is analysed with respect to the criteria found in TR 187 011 [i.34] and copied below. The analysis is presented as conformance to RAMR (Realistic-Achievable-Measurable-Relevant):

- Realistic:
  - The objective does not make unjustifiable demands on the target system. For example, in a secure environment it would be unrealistic to set an objective that all users should be able to view the secret passwords of all other users.
- Achievable:
  - It should be possible to meet the objective within the bounds of current or emerging technology without unreasonable cost.
- Measurable:
  - Once an objective has been met, it should be possible to view or otherwise validate its effect on the target system either directly or indirectly.
- Relevant:
  - The objective should be directly related to the general security of the target system and its environment;
  - the objective should not detract from the overall purpose of the target system.

If a security objective is unable to meet all of these criteria, it should be revised or rejected.

Table E.1: Security objectives for NAT-T in the NGN

Security Objectives		
Id	**Statement**	**RAMR analysis**
OBJ21	NGN R2 NAT-T should maintain confidentiality of data on both sides of the NAT device	RAMR
OBJ22	A NGN R2 NAT-T should maintain any proof of authenticity between NGN entities where the proof of authenticity has to traverse a NAT	RAMR
OBJ23	A NGN R2 NAT-T should maintain the integrity of data that traverses a NAT device	RAMR For IPsec in tunnel mode the checksum may be corrupted by some NAT and NAT-T devices
OBJ24	The application of NAT Traversal should not restrict the communications capability of the NGN	RAMR If filtering is enabled in the NAT-T device the NAT-T device may have the ability to restrict the communications capability of the NGN
OBJ25	The presence of NAT devices in the communications path should be detected	RAMR
OBJ26	The form of NAT devices in the communications path should be detected	RAMR
OBJ27	The presence of filtering devices in the communications path should be detected	RAMR
OBJ28	The form of filtering devices in the communications path should be detected	RAMR

E.3 Step 2: Identification of requirements

Security requirements in a true top down design approach should be derived from the security objectives identified in Step 1, however in practical systems the requirements and objectives are developed in iterative steps The security requirements should be identified as belonging to one of the following categories:

- authenticity;
- Accountability;
- Confidentiality;
- Integrity; and
- availability.

The requirements have been tabulated in table E.2. An analysis of the requirements against the criteria given in TR 187 011 [i.34] is given in the "analysis" column of the table. TR 187 011 [i.34] identifies requirements as of two types:

- Functional requirements:
  - high-level requirements (F.1);
  - behavioural building blocks (F.2);

NOTE: The capabilities specified in ISO/IEC 15408-2 [i.31] are the preferred method of specifying the functional requirements.

  - may refer to existing protocol and service standards (F.3).

- Detailed requirements:
  - low-level requirements (D.1);
  - expressed in a structured form:
    - preconditions;
    - stimulus;
    - response.
  - may be a simple reference to an existing standard (D.2).

Table E.2: Requirements for NAT-T solutions in NGN-R2

Id	Text	F/D	Analysis	Class
R-NATT-1	TISPAN NGN R2 NAT traversal support the traversal of Endpoint Independent Mapping NAT behaviour between the UE and the IMS Core Network	F.1	Requires identification of NAT-T type	🟩
R-NATT-2	TISPAN NGN R2 NAT traversal support the traversal of Address Dependent Mapping NAT behaviour between the UE and the IMS Core Network	F.1	Requires identification of NAT-T type	🟩
R-NATT-3	TISPAN NGN R2 NAT traversal support the traversal of Address and Port Dependent Mapping NAT behaviour between the UE and the IMS Core Network	F.1	Requires identification of NAT-T type	🟩
R-NATT-4	TISPAN NGN R2 NAT traversal support Endpoint Independent Filtering behaviour between the UE and the IMS Core Network	F.1	Requires identification of NAT-T type	🟩
R-NATT-5	TISPAN NGN R2 NAT traversal support Address Independent Filtering behaviour between the UE and the IMS Core Network	F.1	Requires identification of NAT-T type	🟩
R-NATT-6	TISPAN NGN R2 NAT traversal support Address and Port Dependent Filtering behaviour between the UE and the IMS Core Network	F.1	Requires identification of NAT-T type	🟩
R-NATT-7	TISPAN NGN R2 NAT traversal support inbound requests to and from UEs through one or more NAT device(s)		🟩	Availability
R-NATT-8	TISPAN NGN R2 NAT traversal support outbound requests to and from UEs through one or more NAT device(s)		🟩	Availability
R-NATT-9	TISPAN NGN R2 NAT traversal support TCP connections initiated internally			Availability
R-NATT-10	TISPAN NGN R2 NAT traversal support TCP connections initiated externally			Availability
R-NATT-11	TISPAN NGN R2 NAT traversal support residential networks			
R-NATT-12	TISPAN NGN R2 NAT traversal support corporate networks			
R-NATT-13	TISPAN NGN R2 NAT traversal support IP v4	F.3	🟩	🟩
R-NATT-14	TISPAN NGN R2 NAT traversal support IP v6	F.3	🟩	🟩
R-NATT-15	TISPAN NGN R2 NAT traversal support unicast traffic	F.1	Assumes unicast is defined with respect to address type	🟩
R-NATT-16	TISPAN NGN R2 NAT traversal support multicast traffic	F.1	Assumes multicast is defined with respect to address type	
R-NATT-17	TISPAN NGN R2 NAT traversal support uni-directional RTP traffic	F.1		🟥
R-NATT-18	TISPAN NGN R2 NAT traversal support bi-directional RTP traffic	F.1		
R-NATT-19	TISPAN NGN R2 NAT traversal should minimize the number of messages that are transmitted solely for NAT traversal	F.1		
R-NATT-20	TISPAN NGN R2 NAT traversal support multiple UEs (on one or more devices) behind a single NAT	F.1	🟩	🟩
R-NATT-21	TISPAN NGN R2 NAT traversal should minimize additional session setup delay	F.1		
R-NATT-22	TISPAN NGN R2 NAT traversal support the traversal for IMS	F.1		
R-NATT-23	TISPAN NGN R2 NAT traversal support SIP signalling encrypted with IPsec	F.1		🟩
R-NATT-24	TISPAN NGN R2 NAT traversal take into account the scalability, complexity and compatibility with other relevant NGN requirements	F.1		
R-NATT-25	Any solution recommended for NAT traversal not impact the inherent ability of TLS to operate across NAT	F.1		
R-NATT-26	TISPAN NGN R2 NAT traversal support the traversal for non IMS applications including IP TV and PSTN/ISDN emulation	F.1		

E.4 Step 3: Inventory of the assets

Assets are entities in the TOE, here NAT(-T)/NAPT), that has value to the organization, its business operations and its continuity. Assets are identified in Step 3 of TVRA. The goal of TVRA Step 3 is to derive at a systematic inventory list of the valuable entities in the TOE.

An TVRA analysis uses one or more scenarios to identify the assets under study. This NAT(-T)/NAPT analysis uses the TISPAN NGN R2 NAT traversal reference architecture in figure E.1 and the NAT traversal scenarios.

The objective of this clause is to document significant NAT traversal scenarios. For example:

- Residential with unidirectional RTP traffic.
- RACS R2 wholesale with NAT provided by the Access Network operator.
- Business trunking.
- IPTV with dedicated subsystem and RTSP signalling.

In TVRA, assets are identified according to asset categories. The asset categories used in this analysis are physical assets, human assets and logical assets. Physical assets are equipment, software and applications. Logical assets are information and other contained logical constructs in or in relation to physical assets.

The asset lists given below represent a minimum inventory of TISPAN NGN R2 NAT traversal (NAT-T/NAPT).

- Physical assets:
    - UE
    - Remote UE
    - AF
    - SPDF
    - C-BGF
    - Communication links
- Human assets:
    - End-user
    - Remote end-user
- Logical assets:
    - NAT service on UE
    - NAT service on Remote UE
    - NAT service on AF
    - NAT service on SPDF
    - NAT service on C-BGF
    - Private IP address of UE
    - Private IP address of Remote UE
    - TCP/UDP port information of communication
    - Identity of End-user
    - Identity of Remote end-user

Table E.3 describes the relationships between the assets.

Table E.3: Pairings of logical (contained) and physical (container) assets

Logical (contained) assets	Physical (container) assets
UE	NAT service on UE
	Private IP address of UE
	Identity of End-user
Remote UE	NAT service on Remote UE
	Private IP address of Remote UE
	Identity of Remote end-user
Communication links	TCP/UDO port information
AF	NAT service on AF
SPDF	NAT service on SPDF
C-BGF	NAT service on C-BGF

E.5 Vulnerabilities in R2 NAT traversal (eTVRA Step 4)

E.5.1 Weakness in R2 NAT traversal (eTVRA Step 4a)

The weaknesses of the R2 NAT traversal are:

- Unprotected Register message.
- Unprotected Response message.
- No true end-to-end communication.
- Multi-NAT device system to achieve end-to-end communication.
- Problems with tunnelling of communication such as VPN and IPsec.

E.5.2 Threat agents in R2 NAT traversal (eTVRA Step 4b)

Threats are the potential cause of an incident that may result in harm to a system or organization, and hence threats describe how the threat agents use the weaknesses in the TOE to do harm to the system. Threats that apply to R2 NAT traversal are:

- Man-in-the-middle attack masking as either one of the participating physical assets in the R2 NAT traversal such that the authenticity of the end-users are affected.
- Interception on Register and Response message while transmitted on the communication link between UE and Remote UE to gain knowledge such that the confidentiality of data is affected.
- Interception of identity of end-user or Remote end-user by affiliate knowledge gained by intercepting the Register and/or Response message such that the confidentiality of data is affected and/or such that the authenticity of end-users are affected.
- Manipulation of NAT service on one or more of UE, Remote UE, AF, SPDF, or C-BGF such that the message gets sent to the attacker's computer and such that the confidentiality of data and/or authenticity of end-users are affected.
- Intentional altering of data during transmission on the communication link such that the integrity of data is affected.
- Accidental or intentional diverting of messages on the communication link such that the message does not reach its destination and such that the integrity of data is affected.

Threat agents that apply to R2 NAT traversal are:

- Man-in-the-middle attack.
- Interception of source and destination IP address and/or TCP/UDP communication port.
- Interception of identity of end-user and Remote end-user.
- Manipulation of NAT services on one or more of UE, Remote UE, AF, SPDF, and C-BGF.
- Manipulation of data during transmission.
- Accidental and intentional diverting of messages.

E.6 Threats to NAT-T and threat agents to enable them (TVRA steps 4 and 5)

This clause gives a summary of the threats identified with a description of the threat agents that can initiate or perform the threat and materialize it to an security attack. This clause also contains a description of the likelihood and impact of all threats identified.

E.6.1 Identification of threats and threat agents in STUN

The latest draft of STUN [i.39] identifies a number of attack types using specific threat agents to perform manipulation and masquerade attacks. The STUN draft does not categorize the risk presented to a system, nor does it categorize the likelihood of the attack. STUN has been recognized as a platform for NAT-T and not as a NAT-T solution in its own right and as such it underpins both ICE [i.40] and SIP-Outbound [i.41].

E.6.1.1 Manipulation threats and threat agents

E.6.1.1.1 Attacker in NAT-T path

The STUN protocol employs a message integrity mechanism that will detect any modification of a STUN message made by a third party (man in the middle attack vector). In order to launch a manipulation attack the attacker needs to be able to intercept a STUN packet, therefore for analysis manipulation attacks performed by external parties are viewed with respect to the ability to intercept STUN packets.

E.6.1.1.1.1 Interception of STUN messages.

STUN messages appear on specific ports for both UDP and TCP, port number 3478 has been assigned.

```
stun   3478/tcp   Session Traversal Utilities for NAT (STUN) port
stun   3478/udp   Session Traversal Utilities for NAT (STUN) port
```

Knowing how to recognize a STUN message leads to a high likelihood of interception, however the impact of interception is low by itself but may increase when used as the basis of manipulation attacks.

E.6.1.1.1.2 Manipulation of STUN messages.

An intercepted STUN message may be manipulated.

Table E.4: Attack potential for manipulation of STUN messages

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 week	0
Expertise	Layman	0
Knowledge of TOE	Public	0
Access to mount attack	Easy	1
Equipment	Standard	0
Total	No rating - Likely	1

If the message integrity check feature of STUN is deployed any manipulation will be detected and no further countermeasures are required. However the message integrity check feature requires a key to be exchanged and there is some risk that those messages exchanged prior to the establishment of a key are manipulated without detection.

E.6.1.1.1.3 Construction of integrity check value

The Integrity Check Value (ICV) in STUN uses two mechanisms. The first is based on pre-exchanged short-term credentials where the credentials are username and password and where the validity of the credentials is the duration of the media session (for ICE). The second is based on pre-exchanged long-term credentials where the credentials are username and password and where the validity is the duration of the subscription.

In both cases the ICV is constructed as keyed hash (HMAC-SHA1) of the STUN message with the key being determined by the credential type. For short term credentials the key is the password, for long term credentials the key is formed from the MD5 transform of username, realm and password.

There is an inherent weakness for short term credentials if the password has to be exchanged per session across the network. If the session duration is short the means of ensuring no replay of passwords requires some memory to be retained in the STUN agents The means to transfer credentials and the risk introduced by such methods is for further study.

The use of the long term credentials invokes a challenge-response mechanism that introduces a small delay in resolving NAT-T issues.

E.6.1.1.1.4 Manipulation of STUN protocol

An intercepted STUN message may be used to manipulate the behaviour of STUN clients or servers (direction of intercepted message acts as a determinant in the resultant attack). The intended behaviour is denial of service of either the client or server.

Table E.5: Attack potential for manipulation of STUN protocol

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 week	0
Expertise	Layman	0
Knowledge of TOE	Public	0
Access to mount attack	Easy	1
Equipment	Standard	0
Total	No rating - Likely	1

The impact of manipulating the STUN protocol is variable and is countered for many messages by use of an authenticated integrity mechanism (i.e. the integrity check value should be appended by an authenticated party) and thus any message coming from an unauthenticated source is detected. However some STUN messages are sent in clear (i.e. without an authentication check applied) and can only be protected by underlying mechanisms (say TLS or IPsec).

E.6.1.1.2 Attacker in NAT-T endpoint

Where the NAT-T (STUN) endpoints are directly manipulated, for example by maliciously modifying the behaviour of an endpoint though the introduction of modified software, the range of attacks can be extended. In such cases the client is itself not trustworthy and is expected to apply the basic security provisions in the NAT-T application correctly (i.e. message manipulation attacks will not be detected by checking the message integrity check value.

E.6.1.2 STUN usage attacks

The attacks described here are considered as specific examples to validate the behaviour of particular usages of STUN and are taken and generalized from the latest draft of the STUN work [i.39]. ICE or SIP-Outbound may counter these attacks differently with different degrees of success.

A STUN usage defines how STUN is actually utilized - when to send requests, what to do with the responses, and which optional procedures are to be used. A usage should also define:

- Which STUN methods are used;
- What authentication and message integrity mechanisms are used;
- What mechanisms are used to distinguish STUN messages from other messages;
- How a STUN client determines the IP address and port of the STUN server;
- Whether backwards compatibility to RFC 3489 [i.38] is required;
- What optional attributes are required.

The approaches of ICE and SIP-Outbound are instances of STUN usage.

E.6.1.2.1 DDoS Against a Target

In this attack, the attacker provides one or more clients with the same faked reflexive address that points to the intended target. This will trick the STUN clients into thinking that their reflexive addresses are equal to that of the target. If the clients hand out that reflexive address in order to receive traffic on it (for example, in SIP messages), the traffic will instead be sent to the target. This attack can provide substantial amplification, especially when used with clients that are using STUN to enable multimedia applications.

Assumption: This attack can only be launched against targets for which packets from the STUN server to the target pass through the attacker.

E.6.1.2.2 Silencing a Client

In this attack, the attacker provides a STUN client with a faked reflexive address which is a transport address that is non-routing (i.e. goes nowhere).

Assumption: This attack is only possible when the attacker is on path for packets sent from the STUN server towards this unused IP address.

E.6.1.2.3 Masquerade as a known Client

The faked reflexive address points to the attacker itself. This allows the attacker to receive traffic which was destined for the client.

E.6.1.2.4 Eavesdropping

The attacker forces the client to use a reflexive address that routes to the attacker and then forwards any received packets to the client. The attacker is able to observe all packets sent to the client.

Prerequisite for the attack: the attacker have already been able to observe packets from the client to the STUN server.

Assumption: The attacker is on the path between the client and the STUN server, but not necessarily on the path of packets being routed towards the client.

E.6.1.2.5 Risk analysis for use of ICE

The ICE usage of STUN introduces the same underlying risks from STUN and modifies the application of STUN messages. The likelihood of interception of ICE messages is therefore the same as for STUN as is the likelihood of manipulation with the same remarks for countering such attacks by use of the built in message integrity check feature.

E.6.1.2.6 Risk analysis for use of Outbound

The SIP-Outbound approach to NAT-T using a number of carefully crafted SIP messages to detect a NAT in the path and introduces a keep alive mechanism based on SIP to ensure NAT-T for the media defined in the SIP signalling.

The SIP-Outbound usage of STUN introduces the same underlying risks from STUN and modifies the application of STUN messages. The likelihood of interception of SIP-Outbound messages is therefore the same as for STUN as is the likelihood of manipulation with the same remarks for countering such attacks by use of the built in message integrity check feature.

E.6.2 Risk analysis for use of IMS-ALG

The operation of the IMS-ALG for NAT-T is to compare the value of the IP address contained in the SIP-Register "via" header to the source address contained in the IP packet delivering the SIP message. If the address values are different the IMS-ALG **assumes** that a NAT device is in the path. There is no explicit identification of a NAT or the form of NAT device in the path when using IMS-ALG. There is no explicit identification of a filter or the form of filter in the path when using IMS-ALG.

Annex F:
TVRA of UC in NGN-R2

NOTE: The scope of this annex is only the functionality provided for NGN-R2.

Please refer to TR 187 009 [i.42].

Annex G: TVRA of CPN in NGN-R3

NOTE: Whilst the present document is a technical report it identifies requirements for future work as a direct consequence of the analysis and should not be interpreted as mandates in the scope of the present document. In all cases these requirements are considered indicative pending their ratification in formal ETSI Technical Specifications within the TISPAN Work Programme.

G.1 Customer Premises Network (CPN) Threat Vulnerability and Risk Analysis (TVRA)

Risk analysis based security provision is at the heart of the "design for assurance" approach adopted in TISPAN to security standards development. In the NGN environment a Customer Premises Network is a loosely managed entity in the customer premises equipment offering both local services and connectivity (e.g. connecting the PCs, media centres, gaming platforms, printers and other ICT equipment of the household) and offering a gateway to the services of the NGN from the household.

The present document provides the documented output of the TVRA exercise performed against the CPN as defined in TISPAN WG5.

The content of the present document is intended to drive solutions for securing the CPN in the context of the NGN.

G.2 Identification of CPN for TVRA analysis

G.2.1 Overall description of the CPN

The Customer Premises Network (CPN) offers a subset of NGN functionality within the domain of the subscriber whilst also allowing full access to the NGN by terminal/client emulation. In simple terms the CPN comprises a number of user terminals, referred to as Customer Network Devices (CNDs), connected to a Customer Network Gateway (CNG) which provides local routing, local services and access to the NGN.

There are a large number of technologies that may be used to connect CNDs to the CNG and the current analysis includes due consideration of how to apply some of the security capabilities of these to the abstract technologies of the modelled CPN.

NOTE: Existing home ADSL devices may share some of the functionality of CNGs and the set of devices in existing home networks may share some of the functionality of CPNs but should not be considered as NGN CPNs as defined by ETSI.

A CPN is intended to operate in a low cost and low maintenance environment and these factors have been taken into consideration in the preparation of the security recommendations made in the present document.

G.2.2 The security analysis process

The security analysis follows the process described in TS 102 165-1 [i.4] as illustrated below.

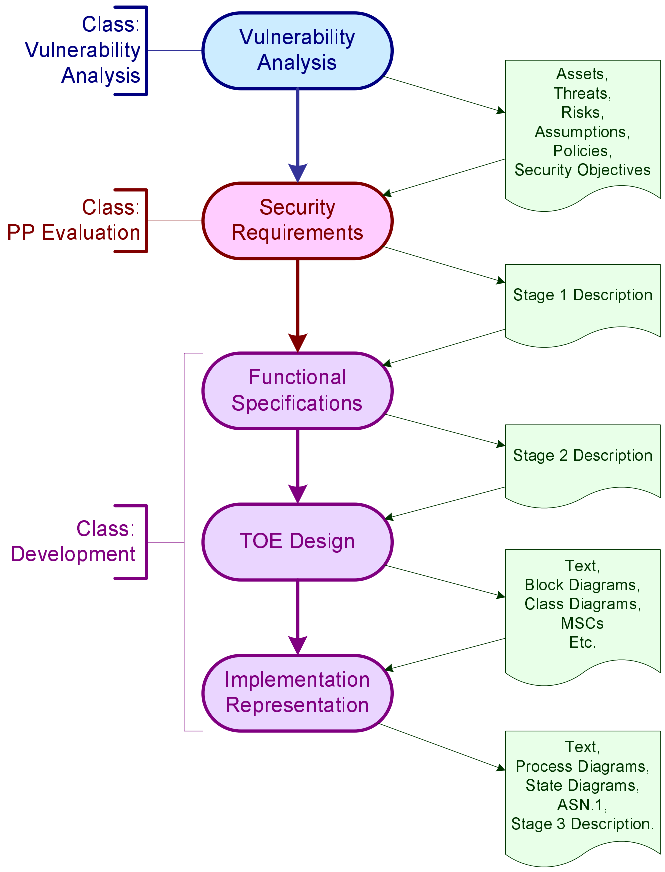

Class: Vulnerability Analysis
Vulnerability Analysis
Assets, Threats, Risks, Assumptions, Policies, Security Objectives
Class: PP Evaluation
Security Requirements
Stage 1 Description
Functional Specifications
Stage 2 Description
Class: Development
TOE Design
Text, Block Diagrams, Class Diagrams, MSCs Etc.
Implementation Representation
Text, Process Diagrams, State Diagrams, ASN.1, Stage 3 Description.

Figure G.1: Structure of security analysis and development in standards documents

The TVRA method consists of the following steps:

1) Identification of the security objectives resulting in a high-level statement of the security goals.

NOTE 1: All assumptions made when formulating security objectives should be explicitly stated as the assumptions may dictate the direction and focus of the analysis and as the assumptions will have to be verified.

2) Specification of the security functional requirements, derived from the objectives developed in step 1.

3) Compilation of an inventory of system assets.

4) Identification and classification of the vulnerabilities in the system, the threats that can exploit them and the unwanted incidents that may result.

5) Quantification of the likelihood of occurrence and the impact of the threats.

6) Establishment of the risks.

7) Specification of countermeasures as detailed security requirements.

NOTE 2: There should be a clear mapping from objectives (step 1) through functional requirements (step 2) to detailed requirements (step 7).

G.2.2.1 Initial security analysis

G.2.2.2 Assumptions

The following pre-conditions have been assumed to be valid within the CPN TVRA (security analysis):

- A CNG is able to perform networking functions from physical connection to bridging and routing capabilities (L1-L3) but may also be able to implement functions related to the service support (up to L7);

- The UNI connection to NGN-IMS services is provided at the Gm reference point;
- The Ut reference point may act as a UNI connection to non-IMS NGN services (where the services are in the application server space);
- e3 reference point is used for remote registration to the CPN as described in ETSI TS 185 006 [i.46]
- The CNG may host an application server on behalf of the CND;
- Physical access to either the CND or the CNG to acquire security-related information (for example, the reading of keystroke sequence mechanically) is out of scope for this analysis;
- Where an IMS terminal uses the CNG in "pass through" mode the CNG is considered to be a network controlled access gateway and not a CNG in the normal sense. It is, therefore, out of scope of the CPN analysis;
- A CNG and a network controlled access gateway may co-exist in the same physical hardware but are maintained in separate security domains. This is somewhat similar to a single PC acting both as a database server and as a web server where some attacks on the base hardware or operating system will affect both capabilities equally but attacks specific to the server types will affect only the attacked server type;
- The CNG acts on behalf of the CNDs in communicating with the NGN;
- The CNG is a full NGN terminal with an NGN identity as defined in TS 184 002 [i.48]:
    - the NGN is assumed to be protected by a full security association with the CNG created using any specified method including IMS-AKA in order to provide authentication of the CNG-identity, and which may also provide confidentiality of the communications between the CNG and the NGN and protection of the integrity of signalling between the CNG and the NGN
- The CND may be a full NGN terminal with an NGN identity as defined in TS 184 002 [i.48] or a non-NGN terminal attached to the CNG via an appropriate terminal adaptor;
- The CNG only connects to the NGN by a fixed line connection (i.e. not by a UMTS radio connection);
- The NGN does not distinguish between a CNG and any other NGN terminal;
- The NGN includes IMS as a service platform.
- The CNG hardware may allow the coexistence of Public Network Gateway (PNG) services and the CPN CNG service. It is assumed that in this case the CPN-CNG service is distinct from the PNG service.

G.2.2.3 Security Objectives

The security objectives shown in table G.1 are categorized according to the guidelines specified in annex D of TS 187 001 [i.6]. A CPN is comprised of one or more CND and a CNG. As a CND can be any user equipment and is unspecified it is excluded from the CPN security analysis. A CND represents an important threat interface to the CPN and is considered to be an un-trusted entity.

Table G.1: CPN Security objectives

OBJ ID	Security Objective Description
Confidentiality	
O-Co1	Information sent to or from a registered user of a CPN should not be revealed to any unauthorized party
O-Co2	Information held within a CNG should be protected from unauthorized access
O-Co3	Details relating to the identity and service capabilities of a CPN user should not be revealed to any unauthorized 3rd party within the CPN or in the wider NGN
O-Co4	Management Information sent to or from a CPN should not be revealed to any unauthorized party
O-Co5	Management Information held within a CNG should be protected from unauthorized access
Integrity	
O-In1	Information held within a CNG should be protected from unauthorized modification and destruction
O-In2	Information sent to or from a registered user of a CPN should be protected against unauthorized or malicious modification or manipulation during transmission
O-In3	Management Information held within a CNG should be protected from unauthorized modification and destruct
O-In4	Management Information sent to or from a CPN should be protected against unauthorized or malicious modification or manipulation during transmission
Availability	
O-Av1	Services provided within a CPN should be available to authorized users of the CPN upon request whether they are attached to an access point within the CPN or to an access point within the wider NG
O-Av2	Services provided within a CPN should be available only to authorized users of the CPN
Authenticity	
O-Au1	It should not be possible for an unauthorized user to pose as an authorized user when communicating with an CPN application or other users of a CPN
O-Au2	It should not be possible for a CPN to receive and process management and configuration information from an unauthorized user
O-Au3	Access to and the operation of services by authorized CPN users should not be prevented by malicious activity within the CPN or in the wider NGN
Accountability	
O-Ac1	The owner of a CPN should only be billed for legitimate use of chargeable CPN and NGN services
Non-Repudiation	
O-NR1	none
Reliability	
O-Re1	none

G.2.2.4 Security functional requirements derived from the security objectives

The following security functional requirements have been derived from the objectives specified in clause G.2.2.3 following the guidelines given in TR 187 011 [i.34].

a) All CPN users shall be required to register (log in) to a CNG before being provided with CPN services

b) A CPN user shall be able to register to the CPN using either local registration or remote registration

c) As part of the registration process, a CPN user (either local or remote) shall provide sufficient information to uniquely identify that user within the CPN

d) Each individual CPN user shall be granted a defined level of access to CPN services upon registration

e) It shall not be possible for a user to invoke CPN services unless the user is currently registered either locally or remotely to the CPN

f) Each individual CPN user shall be granted a defined level of access to CPN data held within the CNG upon registration

g) Access to CPN data held within the CNG should be assigned to individual users according to at least the following three categories:

- no access other than for operation of services (execute access)
- read-only access (includes execute access)
- read and write access (administrator)

h) All CPN users who have read-only access or read and write access to CPN data held within the CNG shall be authenticated and authorized as part of the user registration process (whether local registration or remote registration)

i) It shall not be possible for a user who is not currently registered to the CPN to have any access to CPN data held within the CNG

j) As an option, it shall be possible for signalling and media exchanged between the CNG and the NGN to be encrypted

k) As an option, it shall be possible for management information exchanged between the CNG and the NGN to be encrypted

l) A CNG shall implement or activate mechanisms for detecting changes en route to data (signalling and media) exchanged with the NGN

m) A CNG shall implement mechanisms for detecting possible denial-of-service attacks from within the CPN

n) A CNG shall implement mechanisms for detecting possible denial-of-service attacks originating within the NGN

o) All CPN users shall be authenticated by the CNG as part of the user registration process before invoking any NGN services

p) All CPN users shall be authenticated as part of the user registration process before invoking any CPN services

q) The CNG shall assign unique and non-forgeable identities to all CPN sessions that are verifiable to users and to devices

r) For each CPN session a CNG shall maintain a record of the devices and users linked to that CPN session

s) As an option, it shall be possible to record parts of or all outgoing data transmission from a CNG

t) As an option, it shall be possible to record parts of or all incoming data transmission for a CNG

u) As an option, it shall be possible to record parts of or all access to data held within a CNG

v) As an option, it shall be possible to record parts of or all modifications of data held within a CNG

G.2.2.5 Mapping from objectives to functional requirements

TVRA examines the relevant security associations at several abstraction layers. The two upper abstraction layers are security objectives and functional requirements. Functional requirements are the implementation of the security objectives and refine the security associations introduced in the objectives. The relation between the objectives and the functional requirements are the following: one objective may be fulfilled by one or more functional requirements and one functional requirement may address one or more security objectives. To visualize the relations between these security associations, the following table maps each functional requirement to the objective(s) that they address.

Table G.2: Mapping of functional requirements to objectives

Ref	Functional requirement	Objective implemented
a	All CPN users shall be required to register (log in) to a CNG before being provided with CPN services	O-Co1, O-Co2 O-In2 O-Av1
b	A CPN user shall be able to register to the CPN using either local registration or remote registration	O-Co1, O-Co2 O-In2 O-Av1
c	As part of the registration process, a CPN user (either local or remote) shall provide sufficient information to uniquely identify that user within the CPN	O-Co2, O-Co3, O-Co5 O-In1, O-In3 O-Av1 O-Au1, O-Au2
d	Each individual CPN user shall be granted a defined level of access to CPN services upon registration	O-Co2 O-In1 O-Av1 O-Ac1
e	It shall not be possible for a user to invoke CPN services unless the user is currently registered either locally or remotely to the CPN	O-Av1
f	Each individual CPN user shall be granted a defined level of access to CPN data held within the CNG upon registration	O-Co2, O-Co5 O-In1, O-In3 O-Av1
g	Access to CPN data held within the CNG should be assigned to individual users according to at least the following three categories: - no access other than for operation of services - read-only access - read and write access (administrator)	O-Co2, O-Co3, O-Co5 O-In1, O-In3 O-Av1 O-Au1, O-Au1
h	All CPN users who have read-only access or read and write access to CPN data held within the CNG shall be authenticated and authorized as part of the user registration process (whether local registration or remote registration)	O-Co2, O-Co3, O-Co5 O-In1, O-In3 O-Av1 O-Au1, O-Au2, O-Au2
i	It shall not be possible for a user who is not currently registered to the CPN to have any access to CPN data held within the CNG.	O-Co2, O-Co3, O-Co5 O-In1, O-In3 O-Av1 O-Au1, O-Au2
j	As an option, it shall be possible for signalling and media exchanged between the CNG and the NGN to be encrypted	O-Co1, O-Co4 O-In2, O-In4
k	As an option, it shall be possible for management information exchanged between the CNG and the NGN to be encrypted	O-Co4 O-In4
l	A CNG shall implement or activate mechanisms for detecting changes en route to data (signalling and media) exchanged with the NGN	O-In2 O-In4
m	A CNG shall implement mechanisms for detecting possible denial-of-service attacks from within the CPN	O-Av2
n	A CNG shall implement mechanisms for detecting possible denial-of-service attacks originating within the NGN	O-Av2
o	All CPN users shall be authenticated by the CNG as part of the user registration process before invoking any NGN services	O-Co2, O-Co4 O-In1, O-In3 O-Av1 O-Ac1
p	All CPN users shall be authenticated as part of the user registration process before invoking any CPN services	O-Co2, O-Co4 O-In1, O-In3 O-Av1 O-Au1 O-Ac1
q	The CNG shall assign unique and non-forgeable identities to all CPN sessions that are verifiable to users and devices	O-In2, O-In4
r	For each CPN session a CNG shall maintain a record of the devices and users linked to that CPN session	O-In2, O-In4
s	As an option, it shall be possible to record parts of or all outgoing data transmission from a CNG	O-Ac1
t	As an option, it shall be possible to record parts of or all incoming data transmission for a CNG	O-Ac1
u	As an option, it shall be possible to record parts of or all access to data held within a CNG	O-Ac1 O-Au2
v	As an option, it shall be possible to record parts of or all modifications of data held within a CNG	O-Ac1 O-Au2

G.2.3 Identification of the ToE

The concept of a Target of Evaluation (ToE) in security analysis [i.31] is used to set the boundary for an analysis and for specifying the goal, purpose and scope of the analysis. The identification of the ToE is part of producing the inventory of the assets (step 3) of the TVRA method.

The ToE specifies the scope of the analysis, describes the assets and their relations, and provides a focus for the analysis. For the purposes of the CPN TVRA, the ToE has been identified as the CNG.

The ToE environment is used to specify the communicating entities associated with possible attack interfaces into the ToE. For the purposes of the CPN TVRA, the ToE environment has been identified as the NGN on one side and the CNDs on the other. This is shown in figure G.2. This figure identifies only the primary signalling interfaces from CNDs to the CNG (Gm'), and from the CNG to the NGN ('Gm). The possible attack interfaces into CNG are the interfaces between the CNDs and the CNG and between the NGN and the CNG.

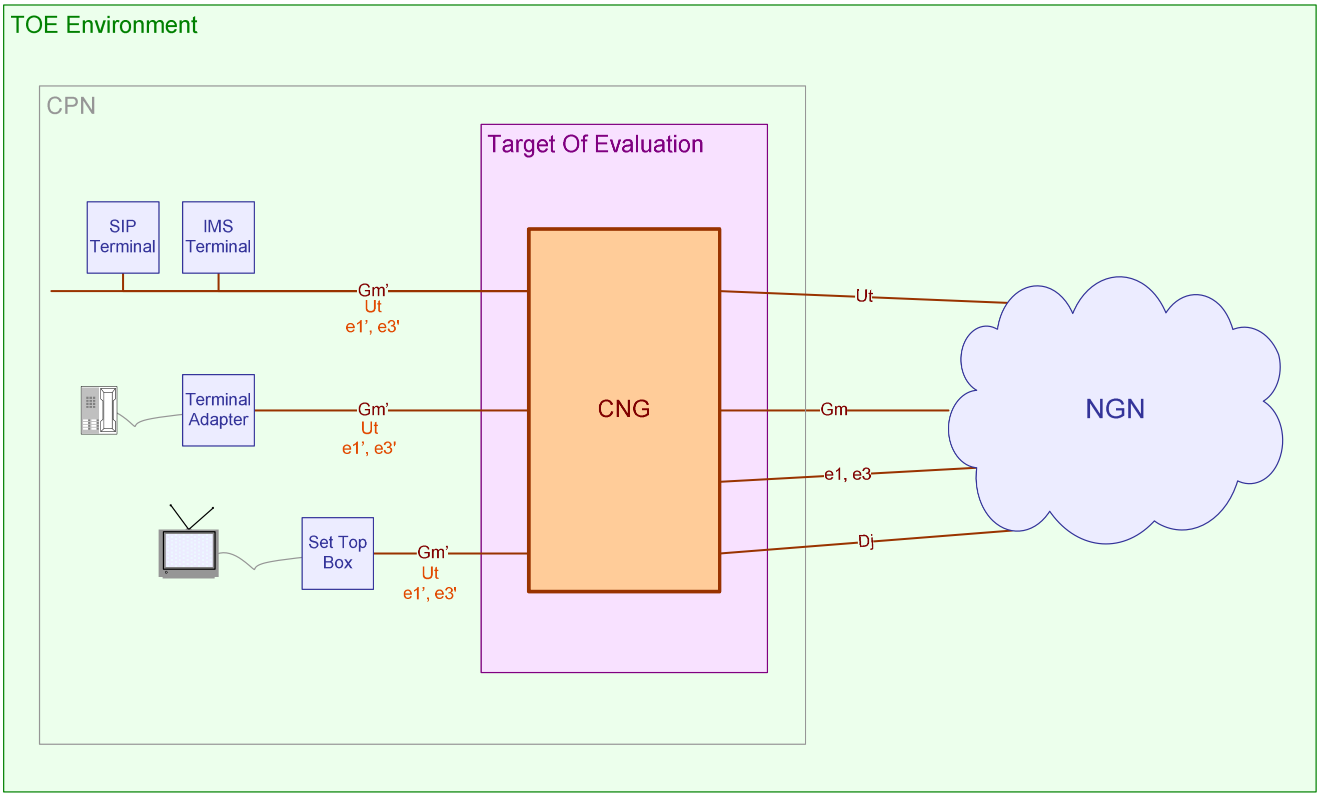


Figure G.2: Identification of ToE

The interfaces between the CNG and the NGN are at the following NGN reference points:

- e1 and e3 for address allocation, authentication and authorization;
- Dj for sending and receiving media and media control flows;
- Gm for access to IMS;
- Ut for those cases where the CND is non-IMS terminal connected to the NGN through a CNG.

Although there is no requirement for a CND to be an IMS terminal, the CNG offers each CND a range of IMS-like services by connecting through a terminal adapter where necessary. In this way, a CNG is able to provide a signalling connection from the CND to the NGN, thus:

- an IMS CND interfaces directly to the SIP Application Servers in the NGN at the Ut reference point;
- a non-IMS SIP CND interfaces directly to the SIP Application Servers in the NGN at the Ut reference point;
- a CND interfaces with the CNG for configuration and management functions at the e3' reference point;
- a CND interfaces with the CNG for network attachment functions at the e1' reference point;
- a CND interfaces with the CNG for SIP services over the B2BUA at the Gm' reference point.

G.2.3.1 Inherent weakness in the ToE

Analysis of the NGN CPN specifications [i.46], [i.47] has identified the following weaknesses in the CNG:

1) SIP is the primary signalling system used within the CPN and previous studies have demonstrated a number of core weaknesses in the SIP protocol [i.52];
2) SIP is semantically and syntactically imprecise although best practice guidelines have made significant efforts to address these issues;
3) It is possible for the connection between a CND and the CNG to be wireless which would mean that all communication between the CND and the CNG is exposed to interception attack;
4) The physical environment in which the CPN is placed is unlikely to be controlled and thus may open the physical elements of the CPN (the CNDs and the CNG) to theft (it is assumed that all CPN equipment fit the criminal criteria of CRAVED [i.51]);
5) The CNG operates in an un-trusted domain;
6) A home installation of a CPN is unlikely to be protected against interruptions of power or against electromagnetic interference;
7) The CNG connects to the NGN at three distinct logical points (Transport, IMS/Service, Application) and the transport attachment is a normal IP termination it is possible to invoke end-user services directly at the transport layer and by that bypassing any equivalent service normally connected at either the IMS/Service or Application layers.

NOTE: The impact of any attack that exploits this weakness varies from the point of observation of the attack whereas the likelihood is constant.

G.2.3.2 Assets inside the ToE

A functional decomposition of the CNG (the ToE) identifies a number of interoperating entities (assets) as shown in figure G.3.

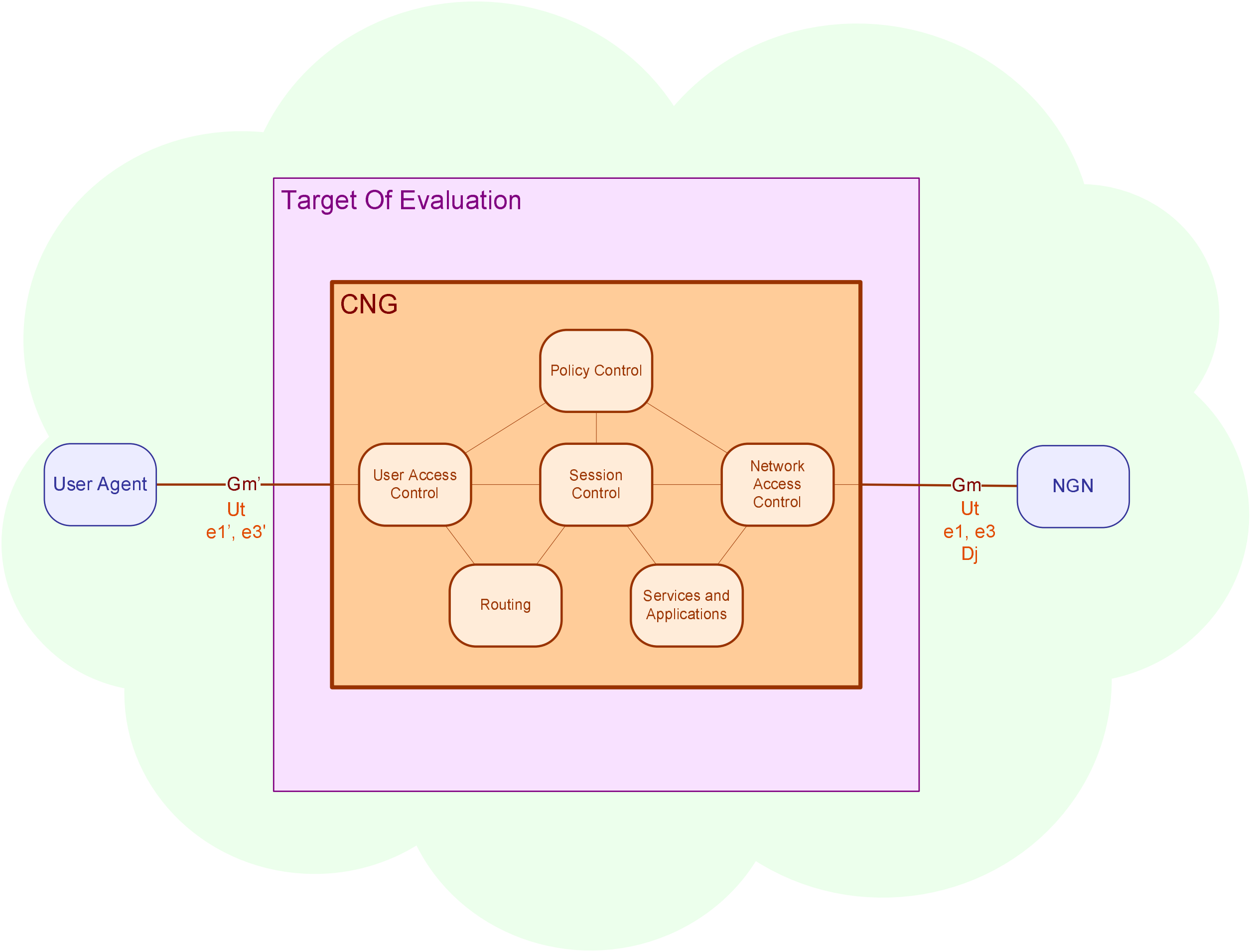


Figure G.3: Decomposition of ToE to visualize the functional entities inside a CNG

The functional assets within the CNG/ToE are described in table G.3.

Table G.3: Decomposition of CNG logical assets

CNG logical asset	Functionality	Reference Points	
		CND to CNG	CNG to NGN
User Access Control	The primary point at which a CND accesses the facilities of the CNG and through which they may access the NGN	Ut, Gm'	Ut, Gm
Network Access Control	Offers NASS like services	au, e1', e3'	e1, e3
Session Control	Manage sessions and negotiate session resources (bandwidth, screen resolution, codecs etc.)	Gm'	Gm
Routing	Network address translation and routing	e1'	e1
Policy Control	Security policy, rights management and QoS policy.	Directly between CND and NGN	Ut
Services and Applications	Communication services (SIP, IMS-based services), IPTV services and customer applications	Ut, Gm'	Ut, Gm

Each of these logical assets has been further decomposed and analysed to better understand what detailed functional entities and data exist in each and the relationships between them, particular any containment and dependency relationships.

Table G.4: Information transferred across reference points between CND and CNG

RP	Information passed
au	Authentication and authorization information pertaining to attachment, encryption and security processes (WEP, WPA2, etc.)
e1'	CNDand CNG hardware identities (MAC address, device ID etc.)
e3'	Information related to: auto-configuration and dynamic service provisioning; software/firmware management; status and performance monitoring; diagnostics
Gm'	Registration and session control data (e.g. parameters)

Table G.5: Information transferred directly between CND and NGN

RP	Information passed
Ut	Information related to user service management, management of public service identities and management of service authorization policies (e.g. used by Presence service, conference policy management)

Table G.6: Information transferred across reference points between CNG and NGN

RP	Information passed
e1	CNG hardware identities (MAC address, device ID etc.)
e3	Information related to: auto-configuration and dynamic service provisioning; software/firmware management; status and performance monitoring; diagnostics
Dj	Information related to media reception and media control such as IPTV functions
Gm	Registration and session control data (e.g. parameters) for SIP through the B2BUA; IMS services; SIP Application Servers

G.2.3.2.1 Decomposition of the CNG functional entities

User Access Control shares much of its functionality with the NGN User Profile Server Function (UPSF) and is responsible for holding the following user related information:

- service-level user identification, numbering and addressing information;
- service-level user security information;
- service-level user location information;
- service-level user profile information.

The data stores involved are modelled in figure G.4 as a User Descriptor and User Authentication Parameters In addition any user specific parameters for signalling and content validation are shown.

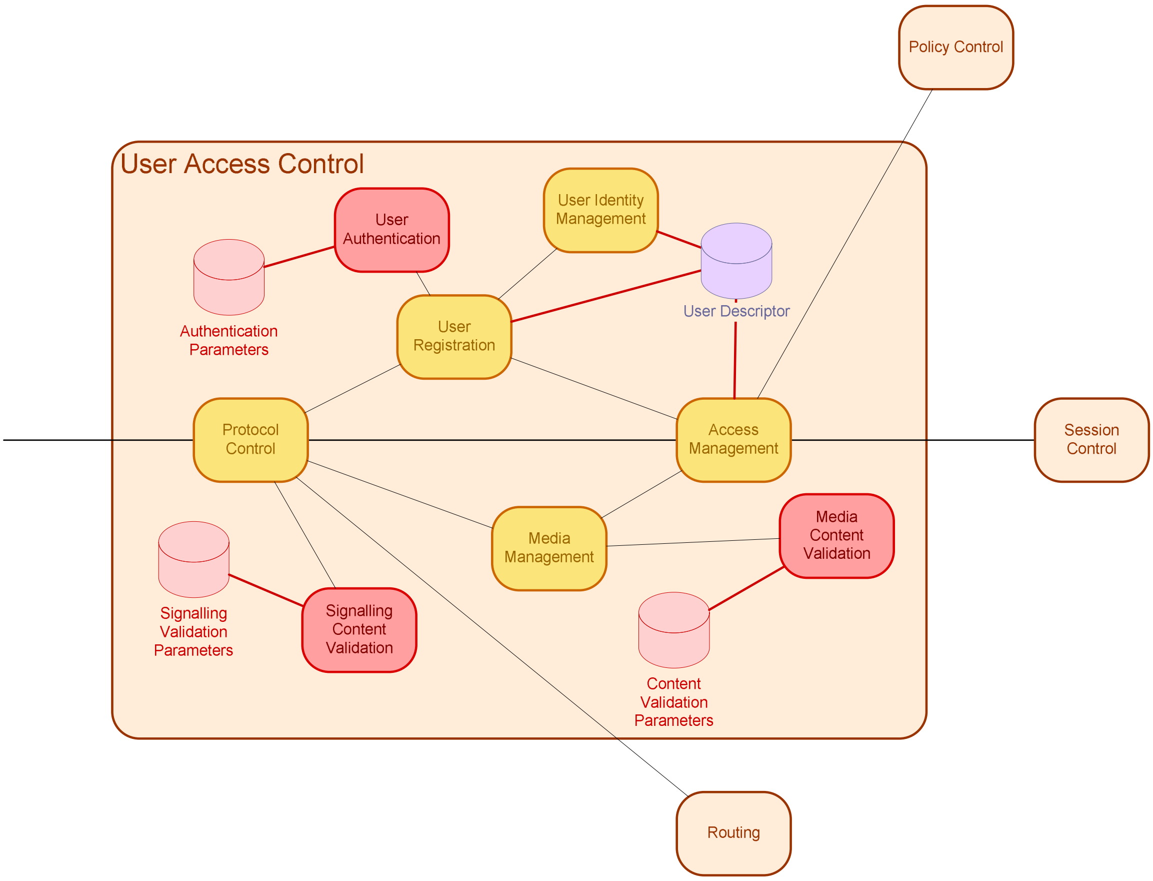


Figure G.4: Decomposition of User Access Control

The remaining functional elements within the CNG have been decomposed in a similar way and the results of this are shown in figures G.5 to G.8.

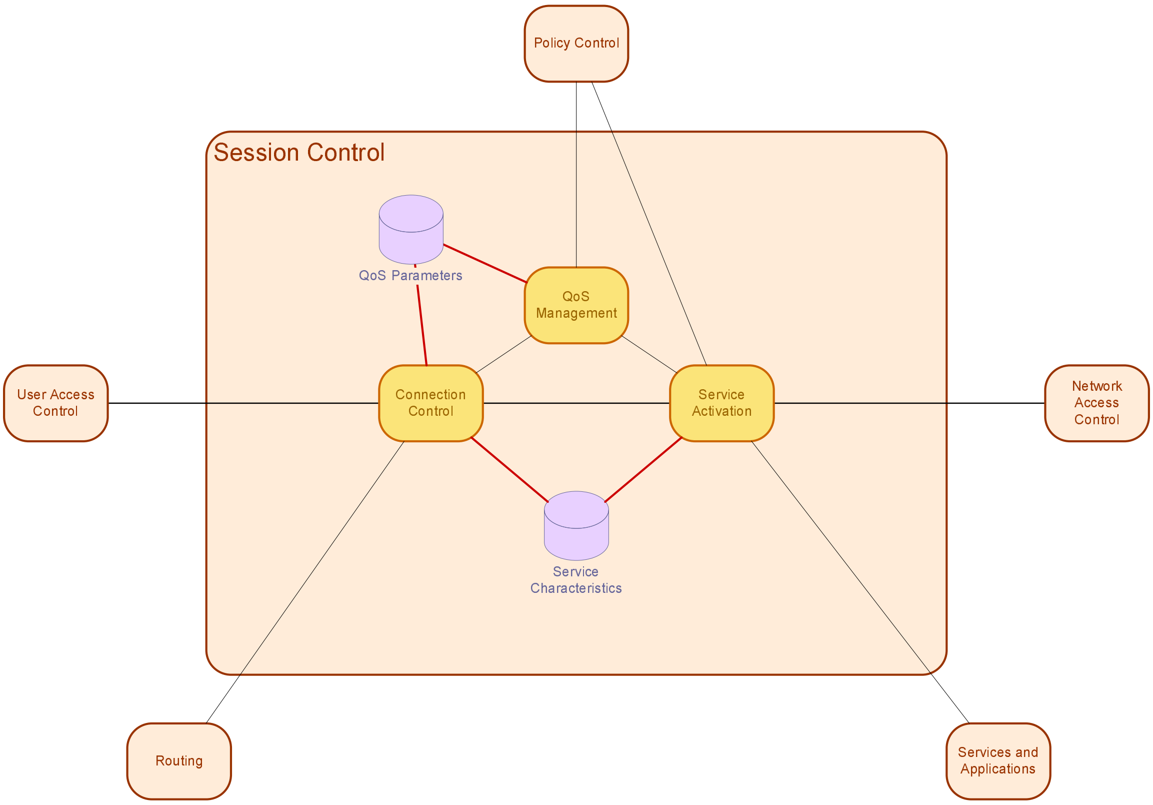


Figure G.5: Decomposition of Session Control

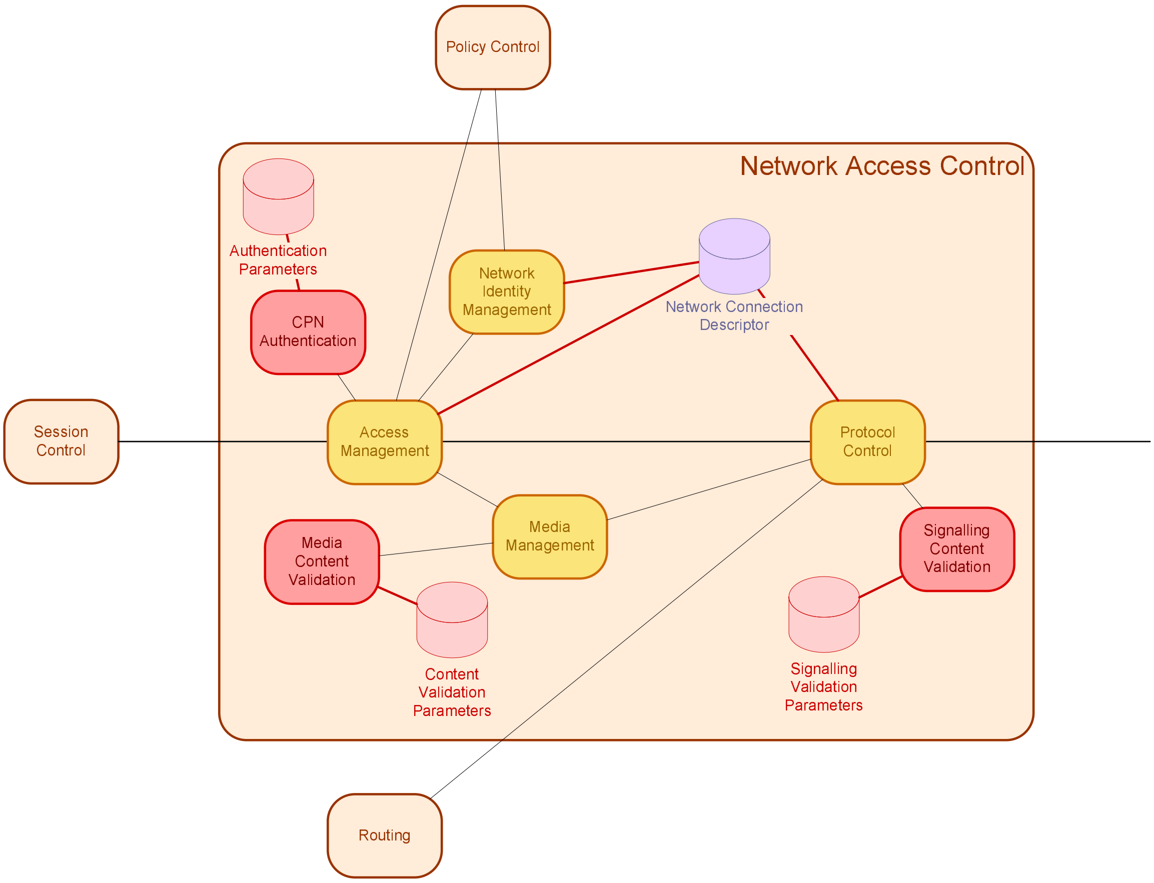

Policy Control
Network Access Control
Authentication Parameters
Network Identity Management
Network Connection Descriptor
CPN Authentication
Session Control
Access Management
Protocol Control
Media Management
Signalling Content Validation
Media Content Validation
Content Validation Parameters
Signalling Validation Parameters
Routing

Figure G.6: Decomposition of Network Access Control

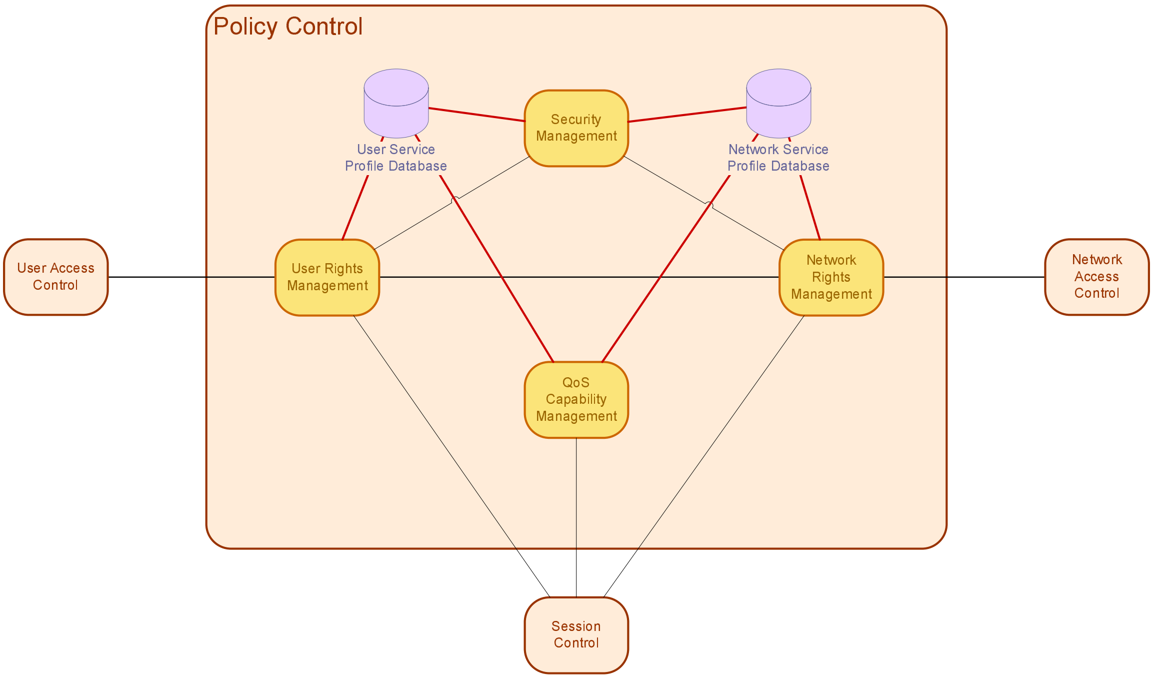

Policy Control
User Service Profile Database
Security Management
Network Service Profile Database
User Access Control
User Rights Management
Network Rights Management
Network Access Control
QoS Capability Management
Session Control

Figure G.7: Decomposition of Policy Control

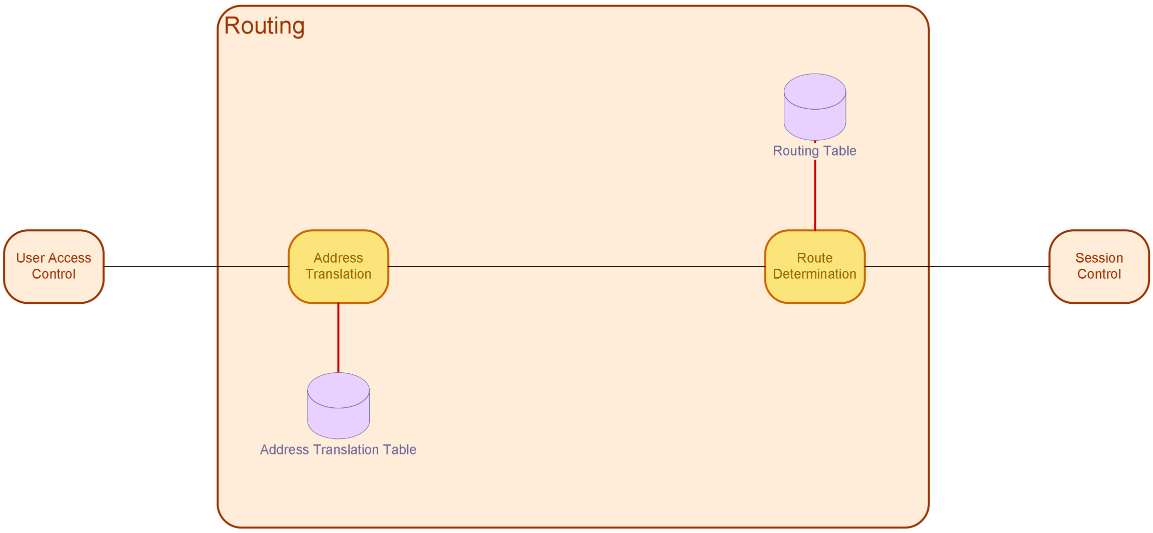


Figure G.8: Decomposition of Routing

G.2.4 Mapping of functional requirements to assets in the ToE

Each of the functional requirements specified in clause G.2.2.4 has an impact on one or more of the functional or data entities identified as assets of the CNG in clause G.2.3.2.1. These relationships are shown in table G.7.

Table G.7: Mapping of functional requirements to ToE assets

Ref	Functional requirement	ToE asset impacted
a	All CPN users shall be required to register (log in) to a CNG before being provided with CPN services	User Access Control, Services and Applications
b	A CPN user shall be able to register to the CPN using either local registration or remote registration	User Access Control, Services and Applications, Session Control
c	As part of the registration process, a CPN user (either local or remote) shall provide sufficient information to uniquely identify that user within the CPN	User Access Control, Services and Applications, Session Control
d	Each individual CPN user shall be granted a defined level of access to CPN services upon registration	User Access Control, Policy Control, Services and Applications, Network, Access Control
e	It shall not be possible for a user to invoke CPN services unless the user is currently registered either locally or remotely to the CPN	User Access Control, Policy Control, Network Access Control, Services and Applications
f	Each individual CPN user shall be granted a defined level of access to CPN data held within the CNG upon registration	User Access Control, Policy Control, Network Access Control, Session Control, Routing information, Services and Applications
g	Access to CPN data held within the CNG should be assigned to individual users according to at least the following three categories: - no access other than for operation of services - read-only access - read and write access (administrator)	User Access Control, Policy Control, Network Access Control, Session Control, Routing information, Services and Applications
h	All CPN users who have read-only access or read and write access to CPN data held within the CNG shall be authenticated and authorized as part of the user registration process (whether local registration or remote registration)	User Access Control, Policy Control, Network Access Control, Session Control, Routing information, Services and Applications
i	It shall not be possible for a user who is not currently registered to the CPN to have any access to CPN data held within the CNG	User Access Control, Policy Control, Network Access Control, Session Control, Routing information, Services and Applications
j	As an option, it shall be possible for signalling and media exchanged between the CNG and the NGN to be encrypted	User Access Control, Network Access Control, Policy Control Function, Session Control, Services and Applications, Routing
k	As an option, it shall be possible for management information exchanged between the CNG and the NGN to be encrypted	Network access Control, Policy Control Function, Routing, Session Control, Services and Applications, User Access Control
l	A CNG shall implement or activate mechanisms for detecting changes en route to data (signalling and media) exchanged with the NGN	Network access Control, Policy Control Function, Routing, Session Control, Services and Applications, User Access Control

Ref	Functional requirement	ToE asset impacted
m	A CNG shall implement mechanisms for detecting possible denial-of-service attacks from within the CPN	Network access Control, Policy Control Function, Routing, Session Control, Services and Applications
n	A CNG shall implement mechanisms for detecting possible denial-of-service attacks on the CPN originated from within the NGN	Network access Control, Policy Control Function, Routing, Session Control, Services and Applications
o	All CPN users who are authorized to invoke NGN services shall be authenticated by the CNG as part of the user registration process (whether local registration or remote registration)	User Access Control, Services and Applications, Session Control,
p	All CPN users who are authorized to invoke internal CPN applications shall be authenticated as part of the user registration process (whether local registration or remote registration)	User Access Control, Services and Applications, Session Control, B2BUA
q	All CPN users who are authorized to communicate directly with other users of the same CPN shall be authenticated as part of the user registration process (whether local registration or remote registration)	User Access Control, Services and Applications, Session Control
r	All CPN users who are authorized to view and modify CPN management and configuration information shall be authenticated as part of the user registration process (whether local registration or remote registration)	User Access Control, Services and Applications, Session Control Network Access Control, Routing information
s	The CNG shall assign unique and non-forgeable identities to all CPN sessions that are verifiable to users and devices	Services and Applications
t	The CNG shall for each CPN session uniquely link devices, users, and CPN sessions	Services and Applications
u	As an option, it shall be possible to record parts of or all outgoing data transmission from a CNG	CNG
v	As an option, it shall be possible to record parts of or all incoming data transmission for a CNG	CNG
w	As an option, it shall be possible to record parts of or all access to data held within a CNG	CNG
x	As an option, it shall be possible to record parts of or all modifications of data held within a CNG	CNG

G.2.5 Weaknesses of assets in the ToE

G.2.5.1 Wireless access devices

G.2.5.1.1 Wireless Ethernet (IEEE 802.11 series)

CNDs may attach to the CNG using wireless Ethernet technologies (IEEE 802.11a/b/g/n) that have a number of built in security features with variable cryptographic strength and capability. Authentication and authorization data may be visible at the au reference point where it is transferred between the CND and the CNG. However the CPN specifications [i.46], [i.47] do not explicitly tie any specific authentication method to the au reference point.

G.2.5.1.1.1 Wired Equivalent Privacy (WEP)

There are a number of well-documented flaws in WEP mainly relating to the management of keys and the cryptographic parameters. In particular WEP is susceptible to the following attacks:

- passive attacks to decrypt traffic based on statistical analysis;
- active attacks to inject new traffic from unauthorized mobile stations, based on known plaintext;
- active attacks to decrypt traffic, based on tricking the access point;
- dictionary-building attack that, after analysis of about one days-worth of traffic, allows real-time automated decryption of all traffic.

The cryptographic provision of confidentiality in WEP uses 64-bit and 128-bit key implementations of the RC4 algorithm but the use of repeated (re-used) initialisation vectors brings the effective key length down to 40 and 104 bits respectively. It is possible to recover the key within a few thousand transactions using known plaintext and signal injection, thus negating any security of the RC4 algorithm itself. An attack can be performed over the air in real-time with easily accessible tools.

WEP only provides confidentiality when used in WiFi applications and does not purport to offer any support of identification. Furthermore, WEP installations use a shared secret that may be susceptible to directory attacks.

G.2.5.1.1.1.1 Notes on RC4

RC4 is a two-stage key stream generator comprising a key scheduling algorithm (stage 1) and a random number generator (stage 2). RC4 was designed in 1987 to be very simple to implement and, whilst this goal is achieved, practical implementations (such as in WEP) often fail.

Perfect secrecy can be achieved using methods based upon the One Time Pad in which *n* bits of plain text are protected by an absolutely random key of length *n* to give a cipher text also of length *n*. However, RC4 uses a key that is shorter than the plain text length *n* and a pseudo-random number derived from an initialisation vector (seed) to generate a key stream sequence of length *n*. If the generator is good and the seed information is sufficiently long with respect to the key and changed for every instance of key stream generation, a key stream generator should approach the secrecy levels of the One Time Pad.

G.2.5.1.1.2 WiFi Protected Access (WPA)

In order to address the weaknesses in WEP, the WiFi Alliance proposed a revision to IEEE 802.11 [i.53], of which WPA implements a sub-set. WPA retains the use of RC4 as the encryption algorithm but improves on the key management sub-system by proposing the Temporal Key Integrity Protocol (TKIP) that uses inputs of the initialisation vector and the key to create a cryptographically modified key as input to RC4. TKIP also introduces an anti-replay counter as only the single hop anti-replay mechanisms are immune to store and forward errors and attacks.

WPA only provides confidentiality and does not purport to offer any support to identification. Furthermore, WPA installations use a shared secret that may be susceptible to directory attacks.

G.2.5.1.1.3 WPA-2 or Robust Security Network (RSN)

WPA-2 is a full implementation of 802.11 security and replaces RC4 with an algorithm derived from AES known as CCM (Counter Mode with Cipher Block Chaining Message Authentication Code).

WPA-2 provides confidentiality and integrity but does not purport to offer any support to identification. Furthermore, WPA-2 installations use a shared secret that may be susceptible to directory attacks although some modes provide rudimentary support for challenge-response authentication extensions that inhibit such attacks.

G.2.5.1.2 DECT devices

DECT has been specified in ETSI and contains built-in authentication and confidentiality countermeasures. There have been no successful attacks reported on the DECT Standard Authentication Algorithm (DSAA) or on the DECT Standard Cipher (DSC). However, the source of both these algorithms is private (i.e. not public in the way that AES is). Depending on manufacturer and specific devices the keys are shared between handsets and base stations and may be discoverable by an enterprising attacker although this probably requires physical access to the DECT base-station.

G.2.5.1.3 Bluetooth devices

There is significant historical evidence of the vulnerabilities in Bluetooth and on tools that can be used to exploit them (btscanner, btxml, Gnokki, OpenOBEX, Redfang and others). The number of Bluetooth attacks recorded is extensive and some are due to the extended physical range achievable on some Bluetooth devices (750m has been reported with unmodified equipment). Some well-known Bluetooth attacks are:

- Theft or alteration of personal information;
- Mobile phone IMEI number availability;
- Privacy, tracking;

- Complete control of certain devices;
- Denial of Service (DoS);
- Airborne viruses and worms.

Most attack tools are able to counter the conventional responses of placing the Bluetooth device in non-discoverable mode and of requiring the explicit pairing of devices. The Bluetooth specification does includes authentication of the devices and confidentiality protection of the radio interface transmissions although this is often based on default (published) PIN codes. Bluetooth specifies a 128-bit cryptographic confidentiality mechanism but the key is derived from the user-entered PIN code which are often only 4 digits (6 bits in BCD format) and that is often set to "0000" by default at installation and rarely changed.

G.2.5.2 SIP signalling

The vulnerabilities of SIP are well documented [i.52] and whilst many of these are resolvable, the core protocol still exhibits several weaknesses. In addition, because of the popularity and relative simplicity of SIP, there are a large number of attack tools available.

The CPN supports two variants of SIP each of which share attributes including extensibility:

- The Gm reference point supports IMS-SIP as defined in ES 283 003 [i.49].
- The Gm' reference point supports other variants of SIP as defined in RFC 3261 [i.18].

The concept of the CNG as a SIP B2BUA (i.e. acting as a SIP server to the CND and as a SIP client to the NGN) may require a mapping of IETF SIP to IMS SIP, or may allocate any non-IMS SIP signalling to the Ut reference point or directly to an uncontrolled SIP server across the root IP connection.

G.2.5.3 Lack of DoS Protection

SIP, IMS and the wireless connection security protection measures do not include any particular DoS protection capabilities. Generally, It is difficult to protect against even simple DoS attacks other than stack overflow. There are a number of automated DoS attack tools available and the likelihood of a DoS attack is high regardless of the protocol used.

Denial of Service attacks can be mounted by saturating a destination device with irrelevant, incorrect or malicious messages. As the protocol stack will attempt process all received messages as if valid, there is a significant danger that the device will have insufficient resources to process genuine messages. It is possible to add address filtering mechanisms, such as Firewalls, prior to the receiving entity to pre-process messages and block those that are received from source addresses that are black-listed or otherwise denied access.

G.2.5.4 Summary of ToE weaknesses

Table G.8 summarizes the weaknesses described in clauses G.2.5.1 to G.2.5.3. It also identifies potential unwanted incidents that may be the result of each weakness and specifies the knowledge required to successfully mount an attack.

Table G.8: Overview of Weaknesses

Weakness			Unwanted Incidents	Attack system knowledge
ID	**Name**	**Description**		
W-1	WEP protocol flaws	WEP is susceptible to the following attacks: • passive and active decryption attacks; • active attacks to inject new traffic; • dictionary-building attacks.	Disclosure of sensitive information; Manipulation of private or other critical information (such as signalling); Masquerade	Public: Automated attack tools are available; attacks can be performed over the air in real-time.
W-2	WPA protocol flaws	WPA installations use a shared secret that may be susceptible to directory attacks	Disclosure of sensitive information; Manipulation of private or other critical information (such as signalling); Masquerade	Public: There are known attacks and attack tools available.
W-3	WPA-2 protocol flaws	WPA-2 installations use a shared secret that may be susceptible to directory attacks although some modes provide rudimentary support for challenge-response authentication extensions that inhibit such attacks.	Disclosure of sensitive information; Manipulation of private or other critical information (such as signalling); Masquerade	Restricted: Particular expertise is needed to carry out directory attacks against WPA-2. Critical: No attacks recorded against a WPA-2 implementation that includes directory attacks protection. An attacker would need to know very specific details of the particular implementation.

W-4	General SIP protocol weaknesses	The stateless architecture of SIP makes it possible for message flows to be disrupted by the receipt of spurious messages such as "BYE", "Invite", "Cancel" and "Refer"	Loss of service;
			Service instability;
			Masquerade
				Public:
				There are a wide number of attack tools available.

W-5	No clear separation of CNG and NGN identities	The concept of the CNG as a SIP B2BUA (i.e. acting as a SIP server to the CND and as a SIP client to the NGN) may require a mapping of IETF SIP to IMS SIP, or may allocate any non-IMS SIP signalling to the Ut reference point or directly to an uncontrolled SIP server across the root IP connection.	Masquerade, Disclosure and manipulation of private or critical information	Public The general and well-known SIP attacks are applicable. In addition, depending on the implementation, information may also be accidentally leaked or changes due to B2BUA design flaws. In cases where an attacker gains access to B2BUA, any attack is in principle possible to launch both against the CNG and the NGN

Weakness			Unwanted Incidents	Attack system knowledge
ID	Name	Description		
W-6	HTTP digest for access to SIP/IMS	Authentication is a password based identification method. User identity and password protected by means of TLS for which there are known attack. Furthermore, digest authentication does not protect IMS signalling. It should be difficult to determine the original secret input key value by knowing only the algorithm output value. However, it is plausible that a brute force attack would find a matching output. If user password is too simple then attacker has a good chance of finding it	Masquerade; Fraudulent use of service	Restricted: There are some relevant attack tools available, but some knowledge (more than layman) is needed to launch the attack.
W-7	NBA for access to IMS	NASS bundled authentication (NBA) relies on the underlying access network authentication method. The access network identity and the IP address are sent to the IMS network as proof of authentication. The security level of the IMS network corresponds to the security level of underlying access network.	Fraudulent use of service	Public: The knowledge needed to attack a WEP-based system is available in the public domain Restricted: Some knowledge (more than layman) needed is required to launch an attack on a WPA-based system
W-8	Lack of DoS protection	The CNG protocol stack will attempt to process all received messages as if valid. There is a significant danger that the device will have insufficient resources to process genuine messages	DoS	Public: No particular knowledge is needed to launch a DoS attack as it is inherently difficult to protect against even simple DoS attacks. Automated DoS attack tools are easily accessible.

G.2.6 Threats to the weaknesses of assets in the ToE

NOTE: The CPN security analysis (TVRA) examines threats on CPN network elements and reference points from a generic point of view and does not reflect a particular physical implementation and configuration.

Analysis of the CPN identified seven threat categories (threat families):

- Denial of service;
- Eavesdropping and interception;
- Masquerade;
- Unauthorized access;
- Loss of information;
- Corruption of information and manipulation;
- Repudiation;

G.2.6.1 Denial of service (DoS)

DoS is a category of attack that is difficult to protect against. The result of such an attack is generally that the attacked entity fails to perform its function or prevents other entities from performing their functions. Attack vectors include the use of UDP, ICMP echo, SYN packets and other methods to flood the target with the goal of consuming all of the target's network capacity and other resources including processing, CPU time, disk space, nodes, ports and directories. Alternative and valid attack vectors include the physical removal of resources (e.g. theft of equipment) and the modification of stored information (e.g. user profile, routing information). A DoS attack can be mounted directly on network elements by or indirectly on system services, thus:

- Denial of Service on network elements:
  - made by continuously sending data to the CNG network elements so that no more resources are available to the CNDs.
- Denial of access to Services:
  - the relevant network elements have insufficient resources to perform a user request and so CPN services cannot be offered to the users. This threat might be a result of the previous one.

G.2.6.2 Eavesdropping

Unauthorized monitoring of communication may be invoked in a number of ways including attaching a protocol analyser to any accessible link, illegal use of lawful interception facilities (not applicable in the ToE but may be applicable in the CNG to NGN connection) and illicit activation of optional features or tools such as conferencing. The impact of any eavesdropping attack on a connection between the CNG and a CND is considered to be "High" (value 3) regardless of the connection technology implemented.

G.2.6.2.1 Eavesdropping of content of communication

The likelihood of eavesdropping an unprotected IEEE 802.11 [i.53] wireless connection between a CND and the CNG is very high as several attack tools are available for download on the Internet. However, the likelihood of such an attack depends on the protection measures available in the security package implemented. As an example of how the method described in TS 102 165-1 [i.4] can be used to determine risk factors, tables G.9 to G.11show the calculations for the likelihood of attack on IEEE 802.11 [i.53] CNDs protected by WEP, WPA and WPA-2 respectively. Table G.12 then summarizes the risk factors derived for each of these.

Table G.9: Resistance of a WEP-based IEEE 802.11 [i.53] system to an eavesdropping attack

Factor	Range	Value
Time	≤1 day	0
Expertise	Proficient	2
Knowledge	Public	0
Opportunity	Easy	1
Equipment	Standard	0
	Total (Resistance)	**3 = Basic**
	Likelihood of attack (based upon Resistance value)	**Likely = 3**

Table G.10: Resistance of a WPA based IEEE 802.11 [i.53] system to an eavesdropping attack

Factor	Range	Value
Time	≤1 week	1
Expertise	Proficient	2
Knowledge	Restricted	1
Opportunity	Moderate	4
Equipment	Standard	0
	Total (Resistance)	**8 = Moderate**
	Likelihood of attack (based upon Resistance value)	**Possible = 2**

Table G.11: Resistance of a WPA-2 based IEEE 802.11 [i.53] system to an eavesdropping attack

Factor	Range	Value
Time	≤1 week	1
Expertise	Proficient	2
Knowledge	Critical	10
Opportunity	Difficult	12
Equipment	Specialized	3
	Total (Resistance)	**28 = Beyond High**
Likelihood of attack (based upon Resistance value)		**Unlikely = 1**

Table G.12: Summary of risks associated with IEEE 802.11 [i.53] CNDs

Security Package	Impact of Attack	Likelihood of Attack	Risk Factor	Classification
IEEE 802.11 [i.53] with WEP	3 (High)	3 (Likely)	9	Critical
IEEE 802.11 [i.53] with WPA	3 (High)	2 (Possible)	6	Critical
IEEE 802.11 [i.53] with WPA-2	3 (High)	1 (Unlikely)	3	Minor

The adoption of WPA-2 as the security measure for WiFi moves the risk to an acceptable level. Whilst there is no change in the impact of an eavesdropping attack, the use of link encryption significantly increases the CNDs resistance to interception and, consequently, reduces the likelihood of such an attack. It is assumed for this analysis that an attacker is aware of the presence of a wireless enabled CNG and is able to get close enough to intercept the transmissions (typically within 100 m).

The likelihood of interception on a connection between the CNG and a Bluetooth CND is very high (value 3) but not considered further in this analysis as the role of Bluetooth in the CPN is not defined.

The likelihood of interception on a connection between a CNG and a DECT CND depends on the invocation of the native security capabilities of DECT. If mutual authentication and encryption are enabled and used with appropriate keys then an interception attack can be classified as "Unlikely" and, thus, the residual risk is "Minor" (value 3).

G.2.6.2.2 Eavesdropping of network element IDs

Network element IDs may be used by entities to authenticate each other prior to an exchange of data. If an attacker has gained knowledge of these IDs, they can later be used to mount a masquerade attack on network elements. This may also be the precursor of other masquerade, modification or DoS attacks. Many protocols exchange identity data in clear text, which in practise means that the level of vulnerability for wireless connections is the same as for eavesdropping of content of communication.

G.2.6.3 Masquerade

Masquerading is the pretence of an entity to be a different entity and several masquerade attacks have been identified as possible within a CPN:

- Masquerade as a legitimate user during the registration process;
- Masquerade as a network entity during the registration process;
- Masquerade as a legitimate user during the authentication process;
- Masquerade as a network entity during the authentication process;
- Masquerade as a calling party during call setup;
- Masquerade as a called party during call setup;
- Masquerade as a non-terminating network entity during call setup;
- Masquerade as a non-terminating network entity during an active connection.

The principal countermeasure to any form of masquerade is authentication of the identity (user or device identity). Both the identity and the credentials used for authentication have to be authoritative within the domain of use and the authority for the identity must be recognised as such. In the NGN masquerade is countered using the IMS-Authentication and Keying Agreement protocols (IMS-AKA), where IMS-Identity and authentication credentials are assigned to the end-user by the IMS provider (and authority in this case).

Identifiers in the CPN that may be attacked by masquerade are listed in tables G.13 and G.14.

Table G.13: CND Identifiers

Identifier	Format	Notes	Authority

Device identifier	IMEI etc.	Hard-coded identifier associated with the specific CND.	IMEI = Manufacturer
			MAC = Manufacturer

CPN User Identifier	IMS Address	Private number only known within the CPN.	CPN supervisor
CPN User Aliases	CPN specific	Other identifier(s) by which the CPN user can be addressed within the CPN. May be given in short form of e.g. 2 or 3.	CPN supervisor
NGN Directory Number	IMS Address	Optional public address that is used for routing, e.g. DDI calls to the user's terminal.	NGN operator

Table G.14: Network Access Identifiers

Identifier	Format	Notes	Authority

Access Identifier	IMEI etc.	Hard-coded identifier associated with the specific access point between the CNG and the NGN.	IMEI = Manufacturer
			MAC = Manufacturer

NGN Access Identifier	IMS address	Private number used for routing calls from CPN users to the NGN access point. This identity is only known within the CPN.	CNP supervisor
NGN Directory Number	IMS Address	Public address of the network access point.	NGN operator

G.2.6.4 Unauthorized access

An attacker gains access to a system or application without permission by exploiting system weaknesses or by masquerading as an entity with higher access permission.

G.2.6.5 Loss of information

Loss of information refers to the destruction of information either stored or in transit along a path of communication.

G.2.6.6 Corruption of information

Corruption of information is the compromise of data integrity by unauthorized insertion, modification or reordering.

In principle it is not possible to prevent users from deliberately manipulating data or destroying a database within the scope of the access rights allocated to them. However, if access rights can be circumvented (e.g. due to incorrect administration of the DBMS), then even unauthorized parties can gain access to the database and manipulate the data contained therein.

- Modification of Terminal Ids:
  - If this ID would be changed this could lead to other attacks such as denial of service attacks, which may be used in connection with a masquerade attack.
- Modification of call setup information:
  - The following are some examples of attacks that are possible when modifying the call setup information:
    - modification of the calling ID could result in masquerade attacks and in billing fraud against the calling party;

    - modification of the called ID could result in denial of service attacks on the called party;
    - modification of the service number might result in billing fraud against the NGN CSP (e.g. replacing a PRS number with a low rate number).

- Modification of routing information:
    - Routing information has to be stored in each domain (e.g. either in the CNG or the NGN). Modification of this information may lead to denial of service attacks or to billing fraud against NGN CSPs as well as against legitimate CPN users.
- Modification of user access authentication data (e.g. for subsequent use):
    - The service profile of each user stored in the CNG contains identification and authentication data. If this data is modified, it could lead to denial of service attacks on a legitimate CPN user attempting to access the environment of the CPN.
- Modification of data exchanged in the registration process:
    - A user is required to register to the CPN before being able to make a call. Modifying registration data could lead to other threats such as denial of service, masquerade or fraud.
- Modification of content of communication:
    - Not relevant for voice communication.
- Modification of network element Ids:
    - Each network element must have a domain unique ID so that it can be identified in the CPN.
- Modification of service authentication data (i.e. part of content of communication):
    - An ITSP may provide different kinds of services. For each subscriber of these services the service profile specifies which services the subscriber is allowed to use and the charging and billing information related to each service. A legitimate CPN user may find it attractive to change the entries in the service profile to enable use of special services that the user currently does not have access to or to change the charging rates for using the services.

G.2.6.7 Repudiation

Repudiation involves a user denying participation in a particular communication by one or more of the following:

- denial of transmission;
- denial of data receipt;
- denial of data access;
- denial of modification of data.

The level of risk presented by denial of involvement depends on a number of factors. If no audit records are maintained, the likelihood of plausible denial is increased but the impact depends on the value to the attacked party of the supposed infringement. Where log records are maintained the likelihood of plausible denial is reduced but again the impact to the attacked party depends on the value of the infringement. In cases where there is no financial element involved and where the parties in the CPN are mostly trusted, the implementation of legally assured non-repudiation countermeasures may not be necessary. It should be sufficient for a CPN network to maintain simple logs of both successful and failed access attempts and to make these available for expert interpretation to support analysis of other attacks.

G.2.6.8 Threat list

Tables G.15 to G.20 list the threats identified for the ToE, i.e. the CNG.

Table G.15: List of DoS threats to the CNG

ID	Threat Name	Threat Description	Weakness	Countermeasures
T-1	DoS on CNG network elements	Carried out by one or more threat agents that continuously send data to CNG network elements causing an overflow state that reduces the resources available to the CNDs potentially to zero.	W-4 W-8	DoS attack detection capabilities DoS attack prevention measures.
T-2	Denial of access to services	Possibly a result of a DoS attack on CNG network elements (T-1). May also be carried out by one or more threat agents, such as automatic attack software, continuously sending fake but valid service requests to the CNG. Both threats result in an overflow state that reduces the ability of the CNG to provide services or to respond to authorized service requests The attack could also be carried out by a threat agent that changes user access parameters, thus denying access to the user.	W-4 W-8	DoS attack detection capabilities DoS attack prevention measures.
T-3	Denial of access by malicious application injected to the CNG a priori	Carried out by one or more malicious applications (such as Trojans or similar) pre-injected into the CNG to prevent the CNG from responding either partially or completely to authorized service and application requests	W-5 W-8	Measures to allow only authorized software updates and management activities.
T-4	Denial of service due to messaging overloading	Carried out by one or more malicious applications (such as Trojans or similar) pre-injected into the CNG to cause several entities to overload the CNG with, for instance, reconnection requests after un-scheduled and un-controlled restarts.	W-4 W-8	DoS attack detection capabilities. Dos attack prevention measures. Measures to allow only authorized software and firmware updates and management activities.
T-5	Denial of service due to B2BUA software simulation	This attack is carried out by e.g. previous malicious software update to the B2BUA or by masquerading as a valid B2BUA that prevents the establishment of the SIP session etc.	W-8	The CNG should have measures to allow only authorized software updates of the B2BUA. It should be possible to validate the authenticity of a B2BUA. For details, see list of functional requirements, which will be refined into detailed requirements in TVRA step 7.

Table G.16: List of eavesdropping threats to the CNG

ID	Threat Name	Threat Description	Weakness	Countermeasures
T-6	Signalling interception	Carried out by one or more threat agents monitoring the signalling in order to gain knowledge or information about traffic patterns and communication behaviour.	W-1 W-2 W-3	Encryption of signalling Encryption of lower-layer protocol
T-7	Unauthorized monitoring of the behaviour of the CNG	Carried out by one or more threat agents monitoring the behaviour of the CNG in order to deduce the activities undertaken by the CNG.	W-1 W-2 W-3	For details, see list of functional requirements, which will be refined into detailed requirements in TVRA step 7.
T-8	Unauthorized monitoring of the behaviour of the B2BUA	This attack is carried out by one or more threat agents (attackers, software agents, etc.) monitoring the behaviour of the B2BUA and by that deducing the activities undertaken by the B2BUA. Note that a threat agent is by definition an unauthorized entity.	W-1 W-2 W-3	For details, see list of functional requirements, which will be refined into detailed requirements in TVRA step 7.
T-9	Eavesdropping of identity of network element(s)	Carried out by one or more threat agents that eavesdrop on communication and able to deduce and trace the identities of network elements which may be used to reveal network structures or service usage.	W-1 W-2 W-3 W-4	Use of temporary network element IDs. Encryption of communication with pre-shared key.
T-10	Design flaw in network elements that opens up for interception	This attack is carried out by one or more threat agents eavesdropping on communication and by that disclosing equipment identities, and tracking the traffic patterns in and out from the specific equipment.	W-4 W-5	The design flaw is to not provide unique identities to the network equipments (boxes). Note: Many vendors do not provide unique identities for their network equipments as they view these as revealing too much information about their products. Countermeasure: The information should be meaningful only to the specific equipment. For details, see list of functional requirements, which will be refined into detailed requirements in TVRA step 7.
T-11	Eavesdropping/Interception on network/traffic routes due to ARP cache poisoning	This attack is carried out by ARP cache poisoning that puts the CNG in an overload state causing the CNG to change its behaviour and to act like a Hub sending out information in all directions. The Hub behaviour enables route sniffing.	W-1 W-2 W-3	Countermeasure: ARP cache protection schemes. For details, see list of functional requirements, which will be refined into detailed requirements in TVRA step 7.
T-12	Interception of IMS SIP routing	Carried out by one or more threat agents intercepting IMS SIP signalling in order to gain routing information that can later be used to launch a MiM attack or to re-route traffic.	W-4 W-6 W-7	

ID	Threat Name	Threat Description	Weakness	Countermeasures
T-13	Interception of TCP/UDP	Carried out by one or more threat agents intercepting firewall information to discover which TCP/UDP ports that are open and, thus, gain knowledge about the services supported in a particular CPN or the services that the "user" is subscribed to.	W-1 W-2 W-3 W-4	Only allow controlled and authorised updates of the network firewall. Use application aware network firewall functionality.
T-14	Interception of registration information	Carried out by intercepting communication to extract registration information that can be used in subsequent masquerade attacks	W-4 W-6 W-7	Registration information should not be revealed to unauthorized parties (this is difficult though as the initial registration messages (SIP) are sent in clear text).

Table G.17: List of masquerade threats to the CNG

ID	Threat Name	Threat Description	Weakness	Countermeasures
T-15	Masquerade as legitimate service during the registration process	Carried out by a malicious service masquerading as a legitimate service with the aim of redirecting authorized service requests to the malicious service.	W-4 W-5	Registration information should not be revealed to unauthorized parties (this is difficult though as the initial registration messages (SIP) are sent in clear text).
T-16	Masquerade as network entity during the service authentication and registration process	Carried out by a malicious network entity masquerading as a legitimate network entity to obtain user data, e.g. authentication information	W-4 W-5	It should be possible to validate the authenticity of a network entity.
T-17	Masquerade as legitimate user during the authentication process	Carried out by a malicious user who is masquerading as a legitimate user to obtain unauthorised access to services.	W-4 W-5 W-6 W-7	CPN users should be registered and authenticated before granting access to CPN services, application or any data held within the CNG.
T-18	Masquerade as a legitimate calling party during call setup	Carried out by a threat agent performing calls on behalf of a legitimate user and who by that is able to charge the calls to the legitimate user.	W-4 W-5 W-6 W-7	For the use of SIP for call setup, the B2BUA should have means to validate the authenticity of the calling party.
T-19	Masquerade as a legitimate called party during call setup	Carried out by a threat agent that actively re-routes calls to: perform subscription fraud; and enable MiM attacks by rerouting to the MiM attacker machine that sits between the calling and called party.	W-4 W-5 W-6 W-7	For the use of SIP for call setup, the B2BUA should have means to validate the authenticity of the called party.
T-20	Masquerade as non-terminating network entity during an active connection	Carried out by a threat agent that masquerades as either a legitimate network entity or a legitimate service entity in order to gain access to parts of the content of communication (e.g. password) in an established connection for use in fraudulent activities	W-4 W-5	For the use of SIP, the B2BUA should have means to validate the authenticity of the involved network entities.
T-21	Hijacking a link after authentication has been performed.	Carried out by a threat agent hijacking a link after authentication has been successfully performed to gain unauthorized access to CPN services.	W-4 W-5	Session Control should be handled such that it is difficult to hijack a link or to quickly detect hijacked links. It is possible to derive a session id based on the communicating parties or one that has a short time to live.

Table G.18: List of unauthorized access threats to the CNG

ID	Threat Name	Threat Description	Weakness	Countermeasures
T-22	Unauthorised access to Management functions and elements	Carried out by a threat agent that modifies the routing tables to enable, for example, re-routing of traffic	W-4 W-5 W-6 W-7	Policy control and routing information held within the CNG should be protected from unauthorized modification.
T-23	Unauthorised access to network and/or services	Carried out by a threat agent that modifies information in the network elements, services or application to enable fraudulent use of CPN resources and services	W-4 W-5 W-6 W-7	Information held within the CNG, CNP services and applications should be protected from unauthorized modification.

Table G.19: List of manipulation threats to the CNG

ID	Threat Name	Threat Description	Weakness	Countermeasures
T-24	Modification of stored information	Carried out by a threat agent that performs unauthorized modification of stored IDs, such as allowed MAC addresses of CNDs, to deny access for authorized users Also carried out by a threat agent that changes user access parameters, thus denying access to the user. For example, this may involve obtaining access to and the changing of username and password so that the user is no longer able to authenticate for service use.	W-5 W-6 W-7 W-8	ID information should only be meaningful to authorized parties. ID information held within the CNG should be protected against unauthorized modification.
T-25	Modification of stored information	Carried out by a threat agent that performs unauthorized modification of stored information by adding IDs to enable unauthorized access to CPN	W-5 W-6 W-7	Information held within the CNG should be protected against unauthorized modification
T-26	Modification of call setup information	Carried out by a threat agent that performs unauthorized modification of call setup information to enable fraudulent access to CPN services	W-5 W-6 W-7	Information relating to call setup and sessions held within the CNG should be protected against unauthorized modification.
T-27	Modification of call setup information	Carried out by a threat agent that performs unauthorized modification of call setup information to deny legitimate users access to specific CPN services	W-5 W-6 W-7	Information relating to call setup and sessions held within the CNG should be protected against unauthorized modification.
T-28	Modification of routing information	Carried out by a threat agent performing unauthorized modification of routing information to enable billing fraud against NGN communication service providers and/or against legitimate CPN users	W-4	Routing information held within the CNG should be protected against unauthorized modification.
T-29	Modification of routing information	Carried out by a threat agent performing unauthorized modification to routing information to deny access to services for legitimate users of the CPN	W-4 W-8	Routing information held within the CNG should be protected against unauthorized modification.
T-30	Modification of user access authentication data to restrict access for legitimate CPN users	Carried out by a threat agent that modifies user access authentication data such that it becomes invalid and by that restricts and maybe also prevents access to the CNP services, the transport layer, or the NGN services, for legitimate CPN users	W-5 W-6 W-7	User access authentication data held within the CNG should be protected against unauthorized modification.
T-31	Modification of user access authentication data to gain unauthorized access	Carried out by a threat agent that modifies user access authentication data with the aim to gain unauthorized access to the CPN services, transport network, and/or NGN services	W-5 W-6 W-7	User access authentication data held within the CNG should be protected against unauthorized modification.

Table G.20: List of repudiation threats to the CNG

ID	Threat Name	Threat Description	Weakness	Countermeasures
T-32	Denial of transmission	Denial of participation in transmission	W-5 W-6 W-7	Local log to ensure accountability.
T-33	Denial of data receipt	Denial of receipt of data	W-5 W-6 W-7	Local log to ensure accountability.
T-34	Denial of data access	Denial of access to data	W-5 W-6 W-7	Local log to ensure accountability.
T-35	Denial of modification of data	Denial of modification of data	W-5 W-6 W-7	Local log to ensure accountability.

G.2.7 Risk factor calculation

NOTE: This threat analysis identifies and analyses threats on network elements and reference points from a generic point of view and thus it does not reflect possible physical implementations and configurations.

Table G.21: Risk factors for CPN ToE

	Attack scenario	Threats	Motivation for attack	Likelihood	Impact	Risk
1	Flooding the target for Denial of Service	T-1 T-2 T-4	Sabotage, Attacker satisfaction	Likely (3)	High (3)	Critical (9)
2	Modifying stored information	T-2 T-3 T-5 T-24 T-30	Sabotage, Disabling and harming of individual subscribers, Attacker satisfaction	Unlikely (1)	High (3)	Minor (3)
3	Attaching a protocol analyser to any accessible link or other types of illegal monitoring of the CNG	T-6 T-7 T-8 T-9 T-11 T-12 T-13 T-14	Espionage, Getting information, Attacker satisfaction	Likely (3)	High (3)	Critical (9)
4	Design flaw or illegal activation of optional features/tools	T-10	Espionage, Getting information, Attacker satisfaction	Possible (2)	High (3)	Critical (6)
5	Hijacking a link after authentication has been performed.	T-21	Fraud, Harming subscribers, Sabotage, Getting information, Attacker satisfaction	Possible (2)	High (3)	Critical (6)
6	Masquerade using authentication information, obtained by eavesdropping or similar	T-15 T-16 T-17 T-18 T-19 T-20	Fraud, Harming subscribers, Sabotage, Getting information, Attacker satisfaction	Possible (2)	High (3)	Critical (6)
7	Unauthorised access to data and services/applications	T-22 T-23	Fraud, Harming providers, Sabotage, Getting information, Attacker satisfaction	Unlikely (1)	High (3)	Minor (3)
8	Modification of information	T-24 T-25 T-26 T-27 T-28 T-29 T-30 T-31	Fraud, Harming providers, Sabotage, Getting information, Attacker satisfaction	Possible (2)	High (3)	Critical (6)
9	Deletion of stored information	T-27 T-29 T-30	Sabotage, Harming providers and individual subscribers, Fraud	Likely (3)	High (3)	Critical (9)
10	Deletion of data in transfer	T-27 T-29 T-30	Sabotage, Harming providers and individual subscribers, Fraud	Likely (3)	High (3)	Critical (9)
11	Modification of access rights of other parties	T-24 T-26 T-28 T-31	Harming providers and individual subscribers	Possible (2)	High (3)	Critical (6)
12	Modification of stored information	T-3	Sabotage, harming providers and individual subscribers	Possible (2)	High (3)	Critical (6)

	Attack scenario	Threats	Motivation for attack	Likelihood	Impact	Risk
13	Denial of data transmission	T-32	Fraud, Harming providers and subscribers	Likely (3)	Medium (2)	Critical (6)
14	Denial of data receipt	T-33	Fraud, Harming providers and subscribers	Likely (3)	Medium (2)	Critical (6)
15	Denial of data access	T-34	Fraud, Sabotage	Likely (3)	Medium (2)	Critical (6)
16	Denial of modification of data	T-35	Fraud, Sabotage	Likely (3)	Medium (2)	Critical (6)

G.3 Countermeasures in the form of detailed requirements

G.3.1 General countermeasures

G.3.1.1 Wireless connection measures (CND to CNG)

Where IEEE 802.11 [i.53] (WiFi) connection of CNDs to the CNG is provided mechanisms to provide protection from interception should be deployed. Because of the inherent weaknesses in WEP and WPA these mechanisms should be avoided. WPA-2 (also known as RSN) should be installed and configured as default.

NOTE: The CNG may act as a key management and distribution centre for CNDs.

For both DECT and Bluetooth connections link encryption should be enabled and for Bluetooth the key should be of significant length (i.e. such that if the key is made by concatenation of the user entered PIN code it should exhibit very high entropy).

G.3.1.2 Connection measures (CNG to NGN)

In order to insulate itself from the NGN the CNG should ensure that there is a security association established between itself and the NGN providing authentication of the NGN-identity and, ideally, differentiated protection of signalling integrity and confidentiality.

NOTE: In this context, "differentiated" implies the ability of having cryptographic separation of messages sent to or received from the NGN if cryptographic protection mechanisms are deployed.

G.3.1.3 Anti-masquerade countermeasures

Masquerade is countered by authentication. A pre-requisite of authentication is the establishment of authoritative identity and the credential set to allow validation of the identity (through authentication). However authentication by itself does not remove the likelihood of masquerade and in addition the identity itself should be concealed as much as possible in signalling. This may be achieved by either encrypting the identity (e.g. the ESI scheme defined in EN 300 392-7 [i.56]) or the Temporary Identity scheme used in GSM (TMSI), and where a protected cache/store is maintained of the concealed identity subsequent transmissions can conceal the identity thus minimising the exposure and making it more difficult for an attacker to time an attack.

Specific authentication countermeasures fall into one of (at least) 3 categories:

- Challenge response countermeasures
  - The model used in DECT, TETRA, GSM and others in which a random challenge is offered and based on a shared secret a cryptographic response calculated. The strength of the measure lies in the inability of an attacker to correctly guess the response without the knowledge of the key.
- Signature countermeasure
  - Applies to symmetric keying schemes whereby a document (data package) hash is signed by the private key of the claimant and verified as true by verifying the signed hash with the public key of the claimant. The strength of the measure relies on the inability of an attacker to find the private exponent of the key-pair.
- Message Authentication Code countermeasures
  - Similar to the signature countermeasure but using symmetric keys to encrypt the hash of a document.

NOTE: Many pen-test environments allow MAC addresses to be masqueraded.

Table G.22 lists general countermeasures for the CNG and associate these to the earlier identified weaknesses. Clause G.3.2 lists the detailed security requirements to the CNG.

Table G.22: List of countermeasures for the CNG

CO ID	Countermeasure Name	Countermeasure Description	Countermeasure Method	ISO/IEC 15408-2 [i.57] Component	Weakness Name
CO-1	WPA-2	Wireless Connection Security Protection	Encryption and Key Management	FCS_CKM.1 FCS_CKM.2 FCS_CKM.3 FCS_CKM.4 FCS_COP.1	WEP protocol flaws (W-1) NBA for access to IMS (W-7)
CO-2	Identify Management	Separation of NGN and CNG identify and separation between authorized and unauthorized users	Identity management	FIA_AFL.1 FIA_ATD.1 FIA_SOS.1 FIA_SOS.2 FIA_UAU.1/2 FIA_UAU.3 FIA_UAU.4 FIA_UAU.7 FIA_UID.1/2 FIA_USB.1	HTTP digest access to SIP/IMS (W-5)
CO-3	Confidentiality Protection	Measure to ensure that private or other critical information is not revealed to any unauthorized parties	Encryption	FCS_CKM.1 FCS_CKM.2 FCS_CKM.3 FCS_CKM.4 FCS_COP.1 FDP_UCT.1	WEP protocol flaws (W-1) WPA protocol flaws (W-2) General SIP protocol weaknesses (W-4) No clear separation of CNG and NGN identities (W-5) NBA for access to IMS (W-7)
CO-4	Information integrity	Measure that checks whether the information received confirms with the information sent	Message Digest	FDP_IFC.1 FDP_ITT.3 FDP_RIP.1/2 PDF_UIT.1	WEP protocol flaws (W-1) WPA protocol flaws (W-2) General SIP protocol weaknesses (W-4) NBA for access to IMS (W-7)
CO-5	Signalling integrity	Measure that checks whether signalling is accidentally or intentionally changed during transmission		FDP_IFF.1/2/3/4/5/6 FDP_ITT.3 FDP_UIT.1	WEP protocol flaws (W-1) WPA protocol flaws (W-2) General SIP protocol weaknesses (W-4) NBA for access to IMS (W-7) Lack of DoS protection (W-8)
CO-6	Anti-Masquerade-del1	Measure to protect authentication credentials from being revealed to any unauthorized party	Identification and Authentication credential information protection	FIA_AFL.1 FIA_ATD.1 FIA_SOS.1 FIA_SOS.2 FIA_UAU.1/2 FIA_UAU.3 FIA_UAU.4 FIA_UAU.7 FIA_UID.1/2 FIA_USB.1	WEP protocol flaws (W-1) WPA protocol flaws (W-2) WPA-2 protocol flaws (W-3) General SIP protocol weaknesses (W-4) HTTP digest for access to SIP/IMS (W-6) NBA for access to IMS (W-7)

CO ID	Countermeasure Name	Countermeasure Description	Countermeasure Method	ISO/IEC 15408-2 [i.57] Component	Weakness Name
CO-7	Anti-Masquerade-del2	Measure to protect against an entity unauthorized posing on behalf of another entity	Authentication Mechanism Protection	FIA_AFL.1 FIA_ATD.1 FIA_SOS.1 FIA_SOS.2 FIA_UAU.1/2 FIA_UAU.3 FIA_UAU.4 FIA_UAU.7 FIA_UID.1/2 FIA_USB.1	WEP protocol flaws (W-1) WPA protocol flaws (W-2) WPA-2 protocol flaws (W-3) General SIP protocol weaknesses (W-4) HTTP digest for access to SIP/IMS (W-6) NBA for access to IMS (W-7)
CO-8	DoS Protection	Measure to either detect or protect against at least well-known DoS attacks	Stack overflow protection, protocol management	FPT_FLS.1 FPT.ITA.1 FPT_RCV.1/2/3 FPT_RCV.4 FPT_RPL.1 FTA.SSL.1 FTA.SSL.2 FTA.SSL.3 FTA.SSL.4	Lack of DoS protection (W-8)
CO-9	Authorization before use of CPN service	Measure to uniquely establish security associations between user identities and services within the CPN	Access Control	FIA_ATD.1 FIA_SOS.1 FIA_UAU.1/2 FIA_UAU.3 FIA_UAU.4 FIA_UAU.7 FIA_USB.1	No clear separation of CNG and NGN identities (W-5) NBA for access to IMS (W-7) HTTP digest for access to SIP/IMS (W-6) General SIP protocol weaknesses (W-4)
CO-10	Protection of Authorization Associations	Measure to protect the authorization associations from unauthorized modification or use	Authorization Protection	FIA_USB.1 FMT_MOF.1 FMT_MSA.1/2/3/4 FMT_SMF.1 FPR_PSE.1	No clear separation of CNG and NGN identities (W-5)
CO-11	Protection of stored data	Measure to uniquely establish security associations between CPN identities and actions on stored objects within the CPN and detection and recording of potential irregular changes	Access Control and Audit Control	FIA_SOS.1 FIA_SOS.2 FIA_USB.1 FDP_ACC.2 FDP_SDI.2	WEP protocol flaws (W-1) WPA protocol flaws (W-2) WPA-2 protocol flaws (W-3) General SIP protocol weaknesses (W-4) HTTP digest for access to SIP/IMS (W-6) NBA for access to IMS (W-7)
CO-12	Session Control and Associations	Measure to uniquely assign non-forgeable identities to all CPN sessions and to link session ID, device ID and user ID	Identity Management Security Associations	FIA_SOS.1 FIA_SOS.2 FIA_UID.1/2 FIA_USB.1 FPT_STM.1	No clear separation of CNG and NGN identities (W-5)
CO-13	Non-repudiation measures	Measure to record data transmission, receipt, access and modification of data in a non-forgeable manner	Non-repudiation	FAU_GEN.1 FAU_GEN.2 FAU_SAA.1/2/3/4 FAU_SAR.1/2/3 FAU_SEL.1 FAU_STG.1 FCO_NRO.1 FCO_NRR.1	No clear separation of CNG and NGN identities (W-5)

G.3.2 Detailed security requirements

G.3.2.1 Confidentiality requirements

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

- 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.

- 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.

G.3.2.2 Identification, authentication and authorization requirements

- A CPN-user attempting to invoke a CNG-mediated service shall be identified and authenticated by the CNG before being granted access to the service.

- The CNG shall implement an authentication failure handling policy.

- 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.

- The CNG should detect replayed user and/or device credentials.

- When the CNG detects replayed user and/or device credentials, the CNG shall stop the relevant processes.

- The CNG shall implement a privacy protection policy specifying as a minimum private and critical information.

- 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.

- 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.

G.3.2.3 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 indication received at the CNG of a resource allocation expiry the CNG shall delete all residual data associated with the invocation of the resource.

G.3.2.4 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.

Annex H: Identity and privacy protection TVRA for NGN-R3

Please refer to TS 187 016 [i.55].

Annex I: TVRA of NASS in NGN-R3

NOTE: Whilst the present document is a technical report it identifies requirements for future work as a direct consequence of the analysis and should not be interpreted as mandates in the scope of the present document. In all cases these requirements are considered indicative pending their ratification in formal ETSI Technical Specifications within the TISPAN Work Programme.

I.1 Scope of NASS TVRA

The NASS TVRA is based on the stage 2 definitions of NASS from ES 282 004 [i.5] and the stage 3 specifications referred to in ES 282 004 [i.5]. In cases where other stage 3 specifications have been examined as part of the analysis they are explicitly cited in the present document.

The NASS TVRA identifies the exposed interfaces between NASS and the NGN and NASS and the UE, and describes how these can be exploited as attack interfaces.

The purpose of the NASS TVRA is to identify whether the NASS specifications fulfil the security requirements as defined in TS 187 001 [i.6] and to identify gaps, if there are any, between the NASS stage 2 and stage 3 specifications and the NGN security requirements as specified in TS 187 001 [i.6] and the NGN security architecture as specified in TS 187 003 [i.7]. The analysis also identifies potential security problems arising from the NASS stage 2 and stage 3 specifications.

I.2 NASS TVRA Target of Evaluation (ToE)

This clause defines the Target of Evaluation (ToE) for the NASS TVRA, the ToE environment, the internal interfaces (internal to the target) and the external interfaces (interfaces between the ToE and the ToE environment).

I.2.1 Definitions

ES 282 004 [i.5] provides a number of definitions that are essential to the understanding of the ToE description.

authentication: property by which the correct identity of an entity or party is established with a required assurance

NOTE: The party being authenticated could be a user, subscriber, home environment or serving network (see TR 121 905 [i.58]).

authorization: granting of permission based on authenticated identification (see ISO/IEC 7498-2 [i.59])

NOTE: In some contexts, authorization may be granted without requiring authentication or identification e.g. emergency call services.

Customer Network Gateway (CNG): gateway between the Customer Premises Network (CPN) and the Access Network

NOTE: A Customer Network Gateway may be in its simplest form a bridged or routed modem, and in a more advanced form be an IAD.

explicit authentication: authentication that requires that the party to be authenticated performs an authentication procedure (to verify the claimed identity of the party)

NOTE: For example, in IMS security (TS 133 203 [i.19]), explicit authentication is provided with full AKA directed towards the IMS client entity (represented by IMPI/IMPU and USIM/ISIM) and also implicit authentication is provided by means of the IPsec security associations.

implicit authentication: authentication based on a trusted relationship already established between two parties, or based on one or more outputs of an authentication procedure already established between two parties

line identification: process that establishes the identity of the line based on the trusted configuration

NASS user: entity requesting authorization, authentication and allocation of the IP-Address from the NASS

User Equipment (UE): one or more devices allowing a user to access services delivered by TISPAN NGN networks

NOTE: This includes devices under user control commonly referred to as CPE, IAD, ATA, RGW, TE, etc., but not network controlled entities such as access gateways.

I.2.2 ToE Description

The Network Attachment Subsystem (NASS) provides registration at access level and initialisation of User Equipment (UE) for accessing the TISPAN NGN services. The NASS provides network level identification and authentication, manages the IP address space of the Access Network and authenticates access sessions. The NASS also announces the contact point of the TISPAN NGN Service/Applications Subsystems to the UE.

Network attachment through NASS is based on implicit or explicit user authentication using credentials stored in the NASS (NASS user identity, NAI).

More specifically and as defined in ES 282 004 [i.5] the Network Attachment Subsystem (NASS) provides the following functionalities:

- Dynamic **provision of IP address** and other user equipment configuration parameters (e.g. using DHCP).
- **User authentication**, prior or during the IP address allocation procedure.
- **Authorization** of network access, based on **user profile**.
- **Access network configuration**, based on **user profile**.
- **Location management**.

The items in **bold** in the list are those that have a direct bearing on security functions and on privacy protection.

The location of the NASS in the overall TISPAN architecture is described in ES 282 001 [i.17] and shown in figure I.1.

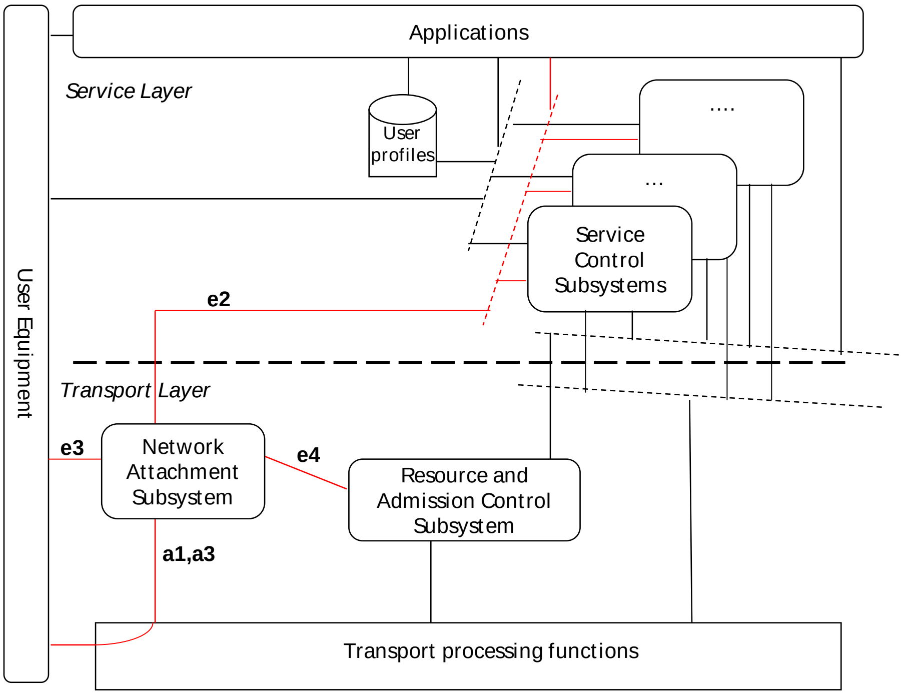

Applications
Service Layer
User profiles
....
...
Service Control Subsystems
e2
User Equipment
Transport Layer
e3
Network Attachment Subsystem
e4
Resource and Admission Control Subsystem
a1,a3
Transport processing functions

Figure I.1: TISPAN NGN Architecture overview

ES 282 004 [i.5] gives an overview of the relationships between the functional entities of NASS and other subsystems of the NGN architecture, as shown in figure I.2.

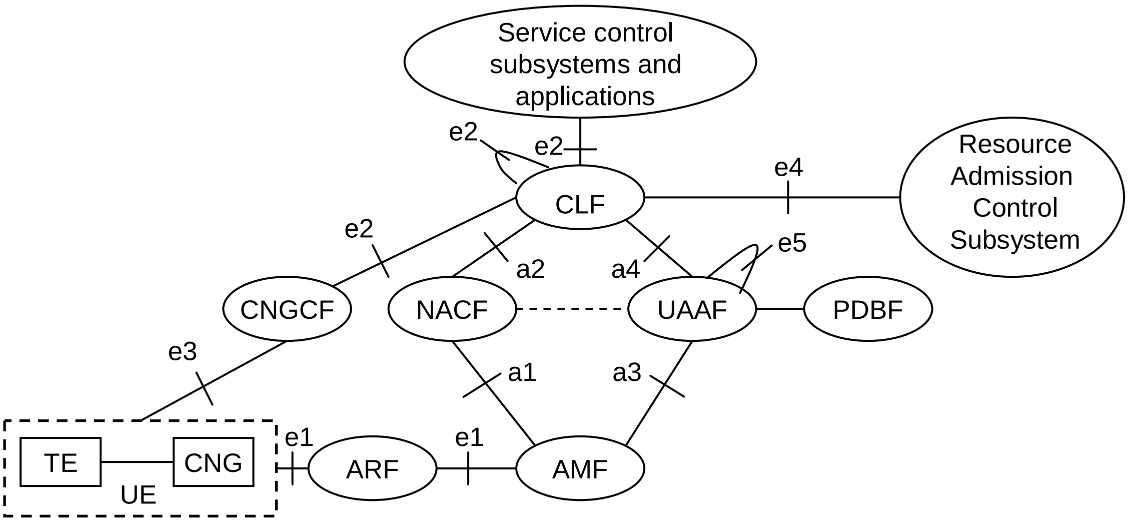

Service control subsystems and applications
e2
e2
Resource Admission Control Subsystem
e4
CLF
e2
a2
a4
e5
CNGCF
NACF
UAAF
PDBF
e3
a1
a3
TE
CNG
UE
e1
ARF
e1
AMF

Figure I.2: Network Attachment Subsystem architecture

The NASS functional entities of figure I.2 are:

- Network Access Configuration Function (NACF).
- Connectivity session Location and repository Function (CLF).
- User Authentication and Authorization Function (UAAF).
- Profile Data Base Function (PDBF).
- CNG Configuration Function (CNGCF).

I.2.3 Analysis of Interfaces

There are 9 interfaces of relevance for the NASS TVRA. These are:

- a2 - reference point between the NACF and the CLF
- a4 - reference point between the UAAF and the CLF
- a1 - reference point between the NACF and the AMF
- a3 - reference point between the UAAF and the AMF
- e5 - reference point between the V-UAAF and the H-UAAF (UAAF-proxy and UAAF-server)
- e4 - reference point between the CLF and RACS (RACF)
- e2 - reference point between the CLF and the Application Functions (AF)
- e1 - reference point between the ARF/AMF and the UE
- e3 - reference point between the CNGCF and the CNG

Of these 9 interfaces, 6 are considered as exposed interfaces in the context of NASS TVRA. Table I.1 summarizes the analysis of the reference points.

Table I.1: Summary of analysis of relevant reference points

Reference point	Description	Internal/External	Exposed/Not Exposed
a2	Reference point between the NACF and the CLF internal to the NASS. This reference points allows the NACF to register in the CLF the association between the allocated IP address of the NASS user identity and the related location information.	Internal	Not exposed
a4	Reference point between the UAAF and the CLF internal to the NASS. This reference point allows the CLF to register the association between the NASS user identity and the NASS user preferences regarding the privacy of location information provided by the UAAF.	Internal	Not exposed (see note 1)
a1	Reference point between the NACF and the AMF. This reference point allows the AMF to request the NACF for the allocation of an IP address to user equipment as well as other network configuration parameters. a1 may be internal or across security domains.	External	Exposed
a3	Reference point between the UAAF and the AMF. This reference point allows the AMF to request the UAAF for NASS user authentication and network subscription checking. a3 may be internal or across security domains.	External	Exposed
e5	Reference point between the V-UAAF and the H-UAAF.	Internal (see note 2) and External (see note 3)	Both (see note 4)
e4	Reference point between the CLF and the RACF entity in RACS. This reference point is used to pass the association between the Globally Unique Address and/or NASS User ID, and the Access Identifier (logical and physical) from the CLF to the RACS.	External	Exposed
e2	Reference point between the CLF and the AF. This reference point enables the AF to retrieve information about the characteristics of the IP/connectivity session used to access such applications from the CLF. It may also be used by a CNGCF to retrieve information from the CLF.	External	Exposed
e1	Reference point between the ARF/AMF and the UE. There is no direct reference point between the NASS and the UE for supporting authentication and IP address allocation. Communication between the NASS and the UE takes place via the ARF and the AMF.	External	Exposed
e3	Reference point between the CNGCF and the CNG. This reference point allows the CNGCF to configure the CNG, trigger maintenance tests, monitoring the performance, and receive notifications. This interface is used during initialisation and update of the CNG to provide the CNG with additional network configuration information when such information are not available over the e1 interface, in order to allow the CNG access to the TISPAN services/applications.	External	Exposed - Management Interface
NOTE 1: The UAAF holds information regarding the privacy of location information for a specific NASS user identity. It should be investigated whether entities internally to NASS are capable of accidental or intentional (via e.g. virus or Trojan) to disclose or change these privacy preferences. NOTE 2: The e5 reference point between V-UAAF and H-UAAF is internal in cases where both are located within the same security domain (trust boundaries). NOTE 3: The e5 reference point between V-UAAF and H-UAAF is external in cases where they are located in different security domains. In such cases, a bilateral trust relationship will need to be established between the V-UAAF and the H-UAAF. ES 282 004 [i.5] does not specify the nature of such a trust relationship. NOTE 4: e5 is an exposed interface in cases where V-UAAF and H-UAAF is located in different security domains. e5 is not exposed in cases where V-UAAF and H-UAAF is located in the same security domain.			

Of these 6 exposed reference points, 2 are defined between configuration entities and thus can be considered as management interfaces (e3, a1). The PDPF is not exposed externally to the NASS and could be seen as an internal trusted entity within the ToE. The AMF has two points of connection the NASS (across a1 and a3).

It is explicitly stated in ES 282 004 [i.5] that there is no reference point between the UE and UAAF but this is wrong as the security association must be between the UE and the UAAF, hence there is a reference point. What is more correct to state is that the reference point (security association) is realised across a number of protocols that do not provide direct connectivity of UE and UAAF.

The CNGCF offers authentication and identification service for the CNG thus suggesting that e3 is a reference point for authentication but that this authentication is not controlled by the UAAF (i.e. it appears that the CNG is not viewed by the NGN as an UE).

I.2.4 Assumptions on the ToE

The following assumptions related to the NASS itself have been made in carrying out this analysis:

- The CNGCF functional entity and its associated e2 reference points are part of the NGN network management system entirely and are, consequently, not part of the communications system to be analysed;
- For the purposes of this analysis, the NASS is modelled at the Transport Layer of the OSI;
- In order to support roaming:
    - the CLF is modelled as a Visited CLF (V-CLF) and a Home CLF (H-CLF) with a new reference point, e2' (based upon reference point e2) between them;
    - the H-CLF can be collocated with the V-CLF or remote from it;
    - the UAAF is modelled as a Visited UAAF (V-UAAF) and a Home UAAF (H-UAAF) with reference point e5 between them;
    - the H-UAAF can be collocated with the V-UAAF or remote from it.
- The threats, vulnerabilities and risks associated with reference point e4 have been previously analysed in the RACS TVRA described in annex A of TR 187 002 [i.52].
- Interfaces a1 and e3 are management interfaces and defined as out of scope for NASS TVRA.
- Interfaces a1 and a3 are not specified in ES 282 004 [i.5] and defined as out of scope for NASS TVRA.

I.2.5 Assumptions of the ToE Environment

The following assumptions related to the NASS environment have been made in carrying out this analysis:

- For the purposes of analysis, the ARF is modelled in the Network Layer of the OSI model.
- For the purposes of analysis, the ARM is modelled at the Link Layer of the OSI model.

I.2.6 Revised NASS architecture

On the basis of the assumptions expressed in clauses I.2.4 and I.2.5, the NASS architecture is revised as shown in figure I.3 for the purposes of the NASS TVRA.

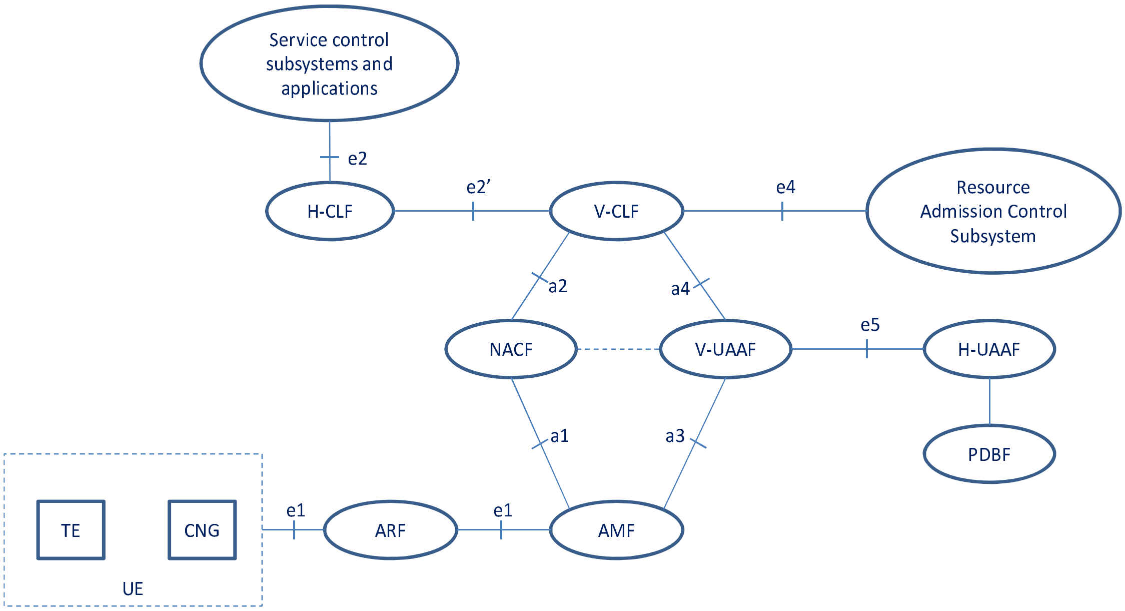

Service control subsystems and applications
e2
H-CLF
e2'
V-CLF
e4
Resource Admission Control Subsystem
a2
a4
NACF
V-UAAF
e5
H-UAAF
PDBF
a1
a3
TE
CNG
UE
e1
ARF
e1
AMF

Figure I.3: Revised NASS architecture

I.2.7 Analysis of exposed interfaces

Table I.2 summarizes the analysis of the exposed interfaces considered in this analysis. Of the 6 identified exposed interfaces from table I.1, only 3 are analysed further and these are: e1, e2, and e5.

NOTE 1: Interfaces a1 and e3 are management interfaces and defined as out of scope for NASS TVRA.

NOTE 2: Interfaces a1 and a3 are not specified in ES 282 004 [i.5] and defined as out of scope for NASS TVRA.

Table I.2: Summary of analysis of exposed reference points

No.	Scenario description	Exposed reference points	Protocol	Exposed assets
1	V-UAAF and H-UAAF across security domains.	e5	DIAMETER or RADIUS	NASS User ID, Privacy Indicator, Globally Unique Address, QoS Profile Information (optional), and Initial Gate Setting (List of allowed destinations, list of denied destinations and default bandwidth).
2	Information Query Request between AF and CLF	e2	DIAMETER	Globally Unique IP Address, NASS User ID, and AF Identity
3	Information Query Response between CLF and AF	e2	DIAMETER	NASS User ID, Location Information (optional), RACS contact point (optional), Terminal Type (optional), Access Network Type (optional), Physical Access ID (optional), and Logical Access ID (optional)
4	Event Registration Request between AF and CLF	e2	DIAMETER	Subscription Duration, NASS User ID (optional), Event, Globally Unique IP Address (optional), and AD Identity (optional)
5	Event Registration Response between CLF and AF	e2	DIAMETER	Update Action, NASS User UD, Event, and Globally Unique Address
6	Notification Event Request between CLF and AF	e2	DIAMETER	Globally Unique Address, NASS User ID, and Event
7	Notification Event Response between AF and CLF	e2	DIAMETER	Globally Unique Address, NASS User ID, Event, and Result
8	Network Access Authentication between UE and NASS (via ARF)	e2	DIAMETER	NASS User Credentials (password, token, certificate, etc.)
9	IP Address Allocation and distribution of other network configuration parameters between UE and NASS (via ARF)	e2	DIAMETER	NASS User Credentials (password, token, certificate, etc.)
10	Implicit line authentication using ARF/AMF as proxies	e1	The protocol used for IP address allocation	Subscriber line ID, NASS-Port-ID, NASS-Port or Calling-Station-ID (line identification information)
11	Explicit authentication using ARF/AMF as proxies	e1	PPP/CHAP, EAP/CHAP, EAPoL, PANA, RADIUS	NASS user credentials (SIM, password, token, certificate, etc.), NAI
12	IP address allocation to UE using ARF/AMF as proxies	e1	RADIUS/Diameter	DHCP or PPP request (location, UE configurations)

NOTE 3: The analysis of e2 relevant scenarios also holds for e2' scenarios.

I.3 NASS security objectives

1) NASS should enable users to register securely to the NGN at the access level

2) NASS should provide registered users with secure access to the NGN and its services

3) NASS should securely allocate and manage IP addresses within the NGN access network

4) NASS should enable a user terminal to be moved securely from one access point to another even if the access points are in different networks

NOTE 1: NASS registration involves the identification, authentication, and authorization procedures between the UE and the NASS to control the access to the NASS.

NOTE 2: Two authentication types are defined for NASS: Implicit authentication and explicit authentication.

I.4 Functional security requirements

Table I.3 summarizes the functional security requirements and show how these relates to the security objectives defined in clause 4. The functional security requirements refers to ISO/IEC 15408-2 [i.31] components according to the guideline given in TR 187 011 [i.34]. Security requirements towards TS 187 001 [i.6] is given in clauses 9 and 10. Change requests to include additional NASS security requirements will be derived from clauses 9 and 10 in the present document.

Table I.3: Functional security requirements associated with confidentiality

Objective		Functional Security Requirements
ID	Text	
1	NASS should enable users to register securely to the NGN at the access level	FIA_ATD, FIA_SOS, FIA_USB, FIA_UID, FIA_UAU, FDP_UCT, FDP_UIT
2	NASS should provide registered users with secure access to the NGN and its services	FIA_UID, FIA_UAU, FDP_UCT, FDP_UIT, FCS_CKM, FCS_COP, FDP_ACC, FDP_ACF, FDP_DAU
3	NASS should securely allocate and manage IP addresses within the NGN access network	FIA_UID, FIA_UAU
4	NASS should enable a user terminal to be moved securely from one access point to another even if the access points are in different networks	FDP_UCT, FDP_UIT, FDP_UCT

I.5 NASS Assets

The NASS assets are the exposed interfaces and the information exchanged over these interfaces, as described in table I.2 in clause I.2.7.

I.6 NASS Vulnerabilities and Threats

Threats are potential events that can cause a system to respond in an unexpected or damaging way. It is useful to categorize threats to determine effective and deployable mitigation strategies. The identification and analysis of security threats to NASS have been carried out according to the STRIDE model, which includes the following categories:

- **Spoofing identity (masquerade).** An example of identity spoofing is illegally accessing following the exploitation of another user's authentication information, such as username and password.

- **Tampering with data (Manipulation).** Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two nodes over a network, such as the NGN.

- **Repudiation.** Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise - for example, a user performs an illegal operation in an NGN subsystem that lacks the ability to trace the prohibited operations.

- **Non-repudiation.** Non-repudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package.

- **Information disclosure.** Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it - for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.

- **Denial of service.** Denial of service (DoS) attacks denies service to valid users - for example, by making an NGN service temporarily unavailable or unusable. One must protect against certain types of DoS threats simply to improve system availability and reliability.
- **Elevation of privilege.** In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy certain NGN subsystems or services. Elevation of privilege threats include those situations in which an attacker has effectively penetrated related system defences and become part of the trusted system itself.

NOTE: The following clauses document the identification and analysis of vulnerabilities and threats for the scenario in table I.2.

I.6.1 Threat identification and risk analysis of scenarios 10-12 (e1)

Interface e1 is defined between the UE and NASS for access authentication and IP address allocation. The interface enables the UE to initiate authentication requests and to request IP address allocation, DNS allocation and other network configuration parameters.

The sources used for the analysis are:

- ES 282 004 [i.5];
- TS 183 019 [i.60];
- TS 133 210 [i.13];
- TS 133 310 [i.61];
- TS 133 320 [i.62];
- RFC 1661 [i.63];
- RFC 3741 [i.64];
- RFC 1994 [i.65];
- TS 181 005 [i.2].

I.6.1.1 Implicit line authentication and IP configuration using DHCP over e1

ES 282 004 [i.5] and TS 183 019 [i.60] specifies that prior to IP address allocation the UE must be authenticated to the NASS. Implicit line authentication does not support mutual authentication. Implicit line authentication and IP configuration using DHCP over e1 is done according to the following procedure (ES 282 004 [i.5]):

NOTE 1: The DHCP scenario is one of several implicit line authentication and IP configuration scenarios.

1) The UE initiates the IP address allocation and implicit authentication procedure by sending a DHCP Discover message.

2) ARF receives the message, adds additional information to the DHCP Discover (e.g. line identification), and forwards the message to AMF.

3) AMF receives the DHCP Discover and sends an access request to the UAAF to authorize the NASS User associated with the UE which sent the DHCP Discover. The association of NASS User profile and UE is facilitated by the line identification information.

4) UAAF responds with an access accept in case a NASS User profile could successfully be associated with the supplied line identification information.

NOTE 2: Information flow steps 3 and 4 perform the "implicit authentication" procedure-stage of the access network attachment process within this call flow.

5) AMF sends the DHCP Discover to NACF, which operates as a DHCP server.

NOTE 3: If NACF and UAAF are collocated, procedure-stage 1 may be initiated after step 5 above.

6) NACF responds with a DHCP Offer to the AMF.

7) AMF forwards the DHCP Offer to the UE.

8) The UE sends a DHCP Request to request an IP address and through DHCP option 120 the address of a TISPAN NGN Service/Applications Subsystem (e.g. P-CSCF). This request is relayed by the AMF to the NACF.

9) The NACF informs the CLF that an IP address is allocated to the UE.

NOTE 4: Step 8 is optional.

10) The CLF request the NASS User profile from UAAF.

11) The CLF retrieves the NASS User profile from UAAF and associates it with the IP address received.

12) The CLF pushes the NASS User profile along with the associated IP addressing and location information to RACS via the e4 reference point.

13) CLF acknowledges to NACF the successful binding of IP address to NASS User profile. This message may contain address information of the TISPAN NGN Service/Applications Subsystems contact point.

14) NACF provides the allocated IP address as well as the FQDN or IP address of the TISPAN NGN Service/Applications Subsystems contact point (e.g. P-CSCF), which is relayed by the AMF to the UE.

NOTE 5: The below analysis only relates to the information exchanged over the e1 interface.

I.6.1.1.1 Vulnerabilities and threats

Implicit line authentication assumes that the line identification information is known to the authenticating parties prior to the authentication. This implies that the line identification information has been distributed prior to the authentication request. This is the main weakness of this authentication schema, as there are no direct interface between UE and UAAF. ARF/AMF acts as the proxy between the UE and the NASS and can therefore be manipulated.

Implicit authentication is specified in TS 181 005 [i.2] and line identification information includes Universal Subscriber Identity Module (USIM), IMS Subscriber Identity Module (ISIM) and Subscriber Identity Module (SIM). The summary of the analysis is given in annex J.

I.6.1.2 Explicit authentication over e1

I.6.1.2.1 PPP-based Authentication

TS 183 019 [i.60] specifies the user-network interface protocol for NASS and TS 124 234 [i.66] specifies the PPP-based explicit authentication model.

Authentication and IP-address allocation using PPP/PPPoE can be summarized as following:

1) UE performs PPPoE discovery procedures to identify the appropriate AMF and establish a peer-to-peer relationship with the AMF, as required by PPP.

2) ARF implements a PPPoE intermediate agent function and inserts access line identification information into PPPoE messages.

3) Negotiation of data link parameters between UE and AMF, including the negotiation of the authentication procedure to be used.

4) UE initiates authentication and sends a corresponding information flow to AMF. The example assumes that NASS User identity and password information is supplied within the information flow.

5) AMF translates the PPP request into an access request to the UAAF which authenticates the NASS User associated to the UE.

6) UAAF responds with an access accept (assuming authentication success) to AMF.

7) AMF informs the UE about the successfully completed authentication.

NOTE: Steps 1 to 7 can be associated with the "PPPoE discovery" phase of PPPoE and "Link Control Protocol (LCP)" phase of PPP. The "authentication" procedure-stage of the access network attachment process is fulfilled as part of the LCP phase of PPP. Information flow steps 8 to 13 perform the "IP address allocation" procedure-stage within this call flow, typically associated with the "Network Control Protocols (NCPs)" phase of PPP, which is to configure the different network-layer protocols.

8) UE sends a request to ARM to obtain IP addressing information.

9) ARM forwards the request to NACF.

10) NACF and UAAF push IP address information and the NASS User profile to CLF.

11) The CLF pushes the NASS User profile along with the associated IP addressing and location information to RACS via the e4 reference point.

12) NACF supplies the IP addressing and network configuration information to the AMF.

13) AMF forwards the IP addressing and network configuration information to the UE.

I.6.1.2.1.1 Vulnerabilities and threats

The summary of the analysis is given in annex J.

I.6.1.2.2 EAPOL (EAP over Ethernet) Authentication

Authentication using EAP over Ethernet start with the UE sending an EAPOL-Start frame to ARP/AMF. If successfully received, the AMF/ARP sends back an EAP request containing an identifier. This identifier and the following response from UE contain a user name and the realm usually combined into a Network Access Identifier (NAI). The EAP request contains the NAI of AMF/ARM and the EAP-Response from UE contains the NAI of the UE. Note that this initial identity exchange is in clear text.

NOTE 1: TS 183 019 [i.60] specifies that the UE can use a generic user name in the NAI for the initial identity exchange phase.

NOTE 2: The ARP acts as a relay between UE and the AMF.

I.6.1.2.2.1 Vulnerabilities and threats

The summary of the analysis is given in annex J.

I.6.1.2.3 Explicit authentication over xDSL/FTTx

The xDSL/FTTx (wireline) access network will physically consist of at least one Access Node (DSLAM, MSAN, OLT for GPON, etc.) which provides the UE with access to aggregation network resources.

The UE acts as the 802.1X supplicant, the Access Node acts as the 802.1X authenticator, and the AAA server (which implements the UAAF functionality) acts as the authentication server.

When the UE comprises a customer network gateway (CNG) and associated customer network devices, the 802.1X Supplicant function must be located on the CNG. This is a direct consequence of 802.1x specifications which set a limitation of a single L2 hop between the supplicant and the 802.1x authenticator.

NOTE: As a consequence of the above limitation, specific users identified at the level of a terminal device connected to a CNG cannot be authenticated by the NASS.

A generic model for xDSL/FTTx 802.1x access to NGN networks is depicted in figure I.4.

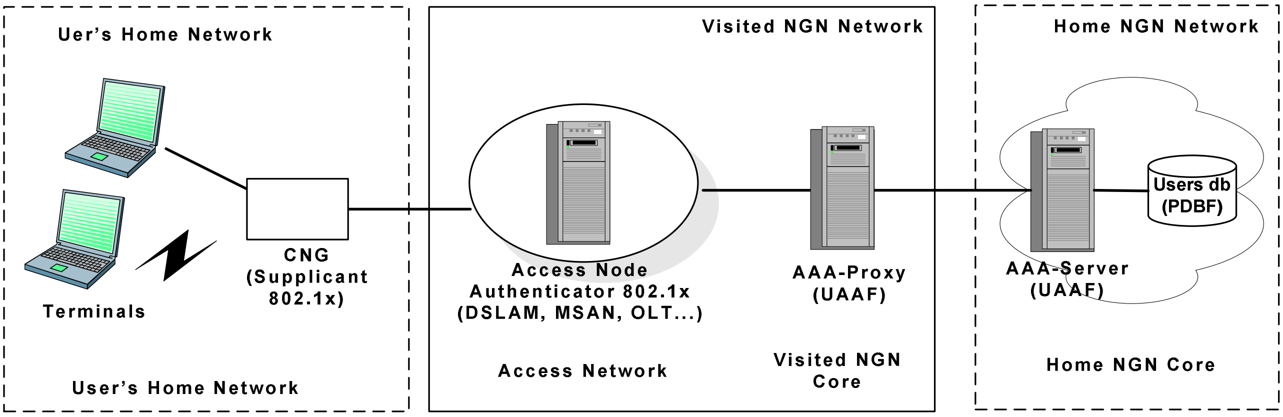


Figure I.4: Generic Model for wireline access (xDSL, FTTH, etc.)

I.6.1.2.3.1 Vulnerabilities and threats

The summary of the analysis is given in annex J.

I.6.1.2.4 WLAN-based authentication

The WLAN Access Network will physically consist of at least one Access Point (AP), which will provide the radio connectivity for the WLAN UE devices. The Access Network or the core network may also contain an Access Controller (AC) that may manage a number of APs.

For the WLAN scenario, the UE (mobile station) acts as the 802.1X supplicant, the AP acts as the 802.1X authenticator, and the AAA server (which implements the UAAF functionality) acts as the authentication server.

A generic model for access of WLAN to NGN networks is depicted in figure I.5.

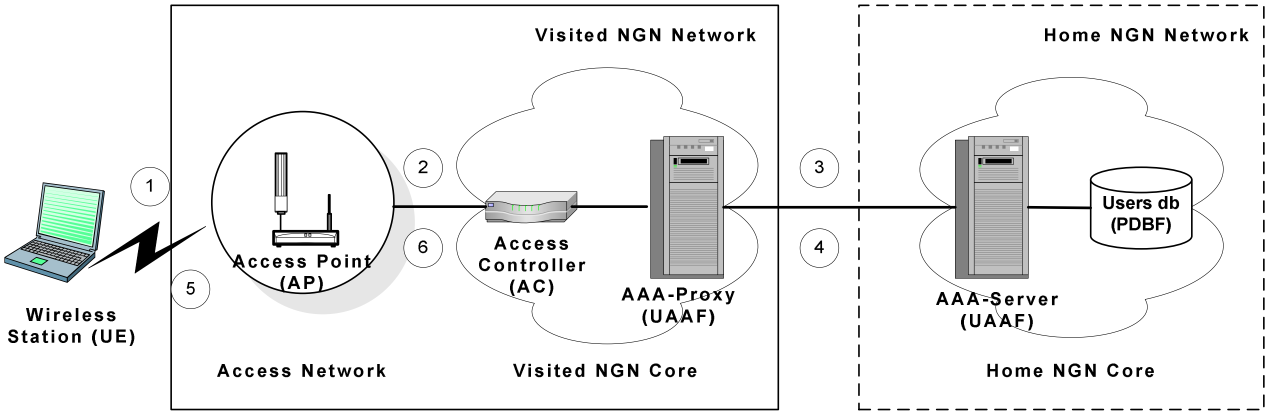


Figure I.5: Generic model for WLAN access to NGN

NOTE: Figure I.5 is from TS 183 019 [i.60]. For the purpose of the present document, AAA-proxy is referred to as V-UAAF, and AAA-server is referred to as H-UAAF.

The numbers shown in figure I.5 correspond to the following steps of a typical 802.1X-based authentication scenario:

1) The wireless station (UE) discovers an 802.11 Access Point (AP) and initiates a connection request. The AP (or a network authenticator) responds with a request for the UE identity.

2) The AP in the access network forwards the UE identity as an authentication request message to the local authentication server/proxy (AAA-Proxy) that implements the UAAF functionality. This may be forwarded via an Access Controller (AC). Either the AP, or the AC, or a combination of the two could implement the AMF functionality.

3) If the AAA-Proxy is able to authenticate the user credentials, it does so locally. If the AAA-Proxy examines the wireless station identity and decides that this is a roaming user, it forwards the authentication request on to the AAA server of the home provider of that user (AAA-Server) based on the realm name specified in the wireless station identity.

4) The AAA-Server (which also implements the UAAF functionality) authenticates the user via an EAP-based challenge-response method that runs end-to-end between the AAA-Server and the wireless station. A local user database (PDBF) is consulted by AAA-Server to verify the credentials provided by the wireless station. The result of the authentication and session key material are communicated back to the AAA-V and AP respectively.

5) The AP configures link-layer session keys and signals that the wireless station has been successfully authenticated. Prior to this time, the AP blocks any attempt by the wireless station to obtain an address or access the Internet.

6) The AP, through the AAA-Proxy, sends accounting messages to the AAA-Server. When the wireless station disconnects, an accounting stop message is sent as the last message for that session. The AAA-V and AAA-H generate charging records. The AAA-H sends these records to a billing centre.

I.6.1.2.4.1 Vulnerabilities and threats

The summary of the analysis is given in annex J.

I.6.1.2.5 NASS-IMS bundled authentication

I.6.1.2.5.1 Overview

IMS authentication is defined in TS 133 203 [i.19] in which there is strong authentication between IMS and UE using credentials resident on the ISIM.

For those deployments where ISIM is not available but where the network and IMS are within one trusted domain a variation on the early IMS authentication is proposed whereby the NASS authentication is made available to IMS.

NOTE: Early IMS authentication in 3GPP systems where the NASS is a GPRS network in the same trusted domain as the IMS uses the GPRS authentication to provide authentication access to IMS.

The coexistence between TISPAN and 3GPP authentication schemes is described in TR 33.803 and includes:

- IMS AKA with and without NAT traversal as specified in TS 133 203 [i.19] and TS 124 229 [i.67].

- Early IMS security mechanisms as specified in TR 133 978 [i.92].

- NASS-IMS-bundled authentication as specified in TS 187 003 [i.7] and ES 283 003 [i.49].

- HTTP Digest for non-3GPP defined NGN access networks as specified in RFC 2617 [i.68] and TS 187 003 [i.7].

Two modes of IMS authentication based on NASS authentication are defined as described in TS 181 005 [i.2]:

- Scenario A: IMS authentication is linked to access line authentication (no nomadism).

- Scenario B: IMS authentication is linked to access authentication for IP Connectivity (limited nomadism can be provided).

Both scenarios A and B allow UEs to perform access independent authentication to the IMS.

I.6.1.2.5.2 Stage 2 model of NASS-IMS bundled authentication

An outline model for authentication is given in figure I.6 in the form of an UML pattern.

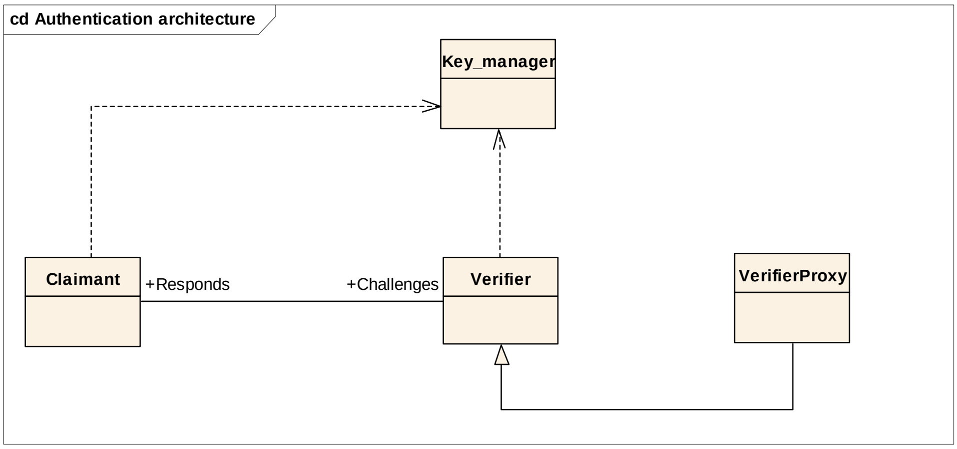


Figure I.6: Authentication pattern

In the IMS-NASS bundled authentication the verifier is in NASS and the result of the authentication communicated to IMS (i.e. there is no independence of NASS and IMS).

Figure I.7 shows the NASS authentication pattern.

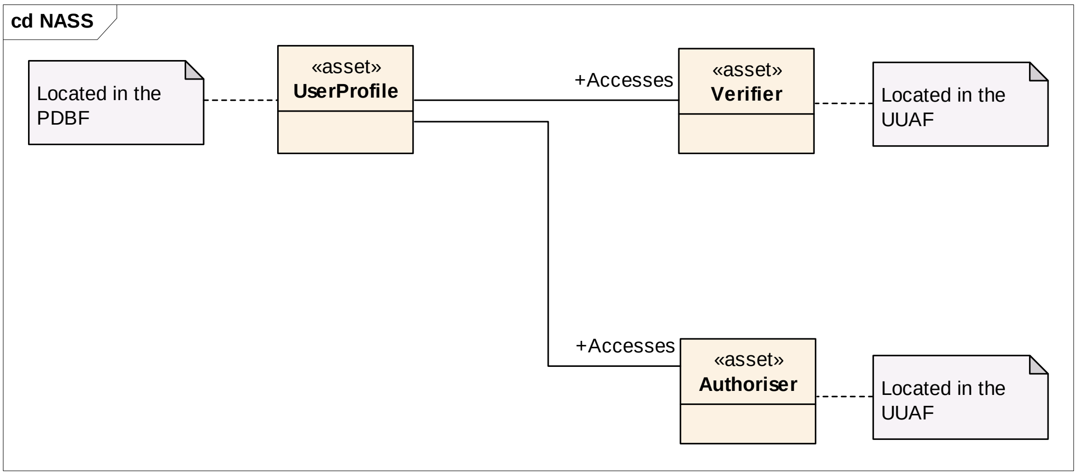


Figure I.7: NASS matching to authentication pattern

I.6.1.2.5.3 NASS-IMS-bundled authentication assets

The assets involved in the NASS-IMS bundled authentication (for stage 2 analysis) are:

- Connectivity Session Location and Repository Function (CLF).
- Call Session Control Function (CSCF):
  - Interrogating - Call Session Control Function (I-CSCF).
  - Proxy - Call Session Control Function (P-CSCF).
  - Serving - Call Session Control Function (S-CSCF).
- User Equipment (UE).
- User Profile Server Function (UPSF).
- Authentication Protocols:
  - NASS authentication - Between UE and CLF.
  - NASS-IMS bundled -Between UE, CLF, CSCF and UPSF.

For the purposes of analysis figure I.8 shows a class diagram of the IMS-NASS bundled authentication illustrating the dependency required between PDBF and UPSF which does not exist in conventional NASS or IMS.

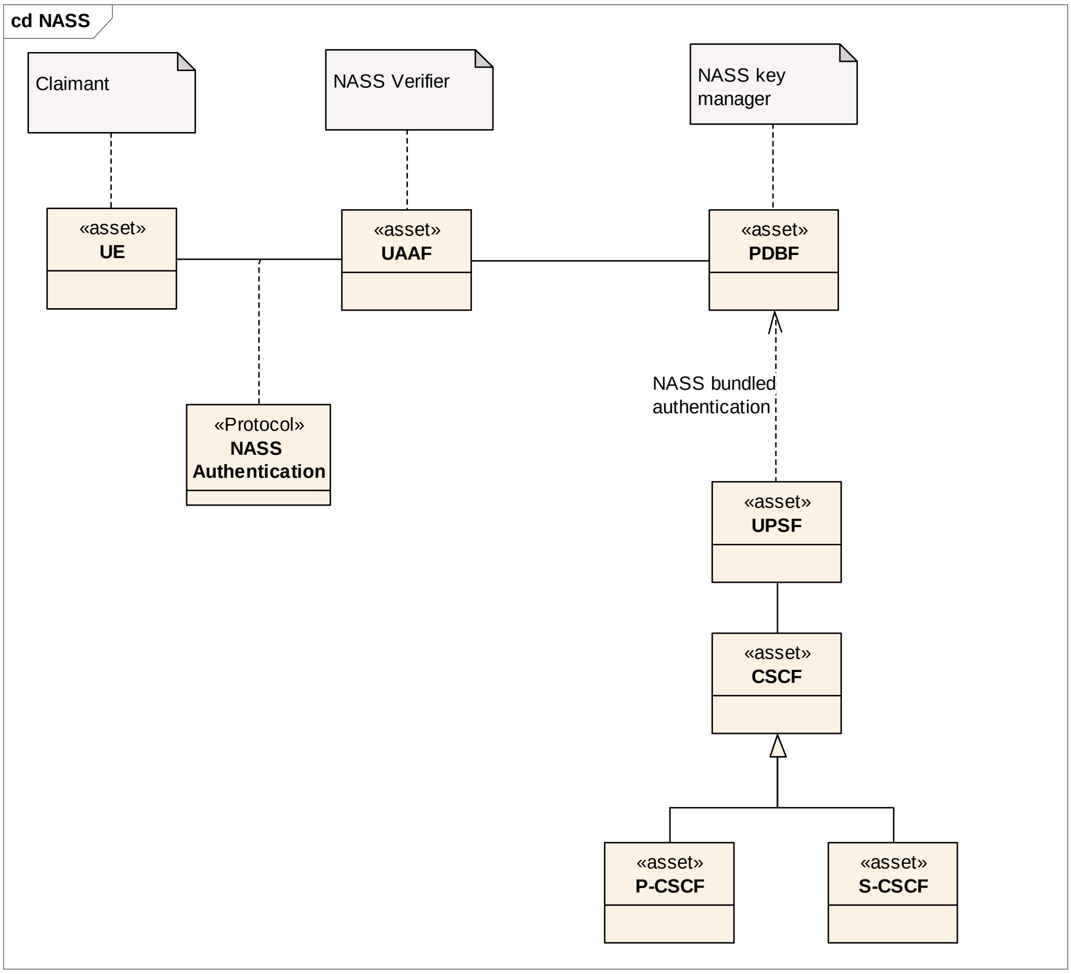


Figure I.8: IMS-NASS bundled authentication class diagram model

I.6.1.2.5.4 Uncertainty regarding functions in NASS

I.6.1.2.5.4.1 Authentication protocol

A number of authentication protocols are cited in ES 282 004 [i.5] but detail profiles of them are not given. The degree of protection offered by different protocols, and their mapping to the authentication pattern of figure I.8 is therefore not clear. It is known that some simple authentication protocols are susceptible to attack (e.g. dictionary attacks for username-password forms) whereas those with cryptographic parameters may be more resilient.

I.6.1.2.5.4.2 Cardinality of relationships

The cardinality of relationships between objects in NASS is not clear.

I.6.1.2.5.4.3 Trustworthiness of the location information

The location information carried in the network-provided P-Access-Network-Info is an essential input data for NASS-IMS bundled Authentication procedure. This information must be trustable in order to prevent authentication fraud. This trustworthiness must be considered and a mechanism must be specified to ensure it. Otherwise the NASS-IMS bundled authentication will be susceptible to the attack described in annex J.

I.6.1.2.5.5 Vulnerabilities and threats

The primary points of attack are the e1 interface where identity and authentication data is transmitted. The secondary point of attack is the authentication protocols. The summary of the analysis is given in annex J.

I.6.1.3 IP address allocation over e1

The Network Access Configuration Function (NACF) is responsible for the IP address allocation to the UE. It may also distribute other network configuration parameters such as address of DNS server(s) and address of signalling proxies for specific protocols. A NACF may be realized as a DHCP server.

The UE needs to be authenticated before it can request IP address allocation. The NACF receives from signalling via e1 the line identity (Line ID) and establishes the mapping between the allocated IP configuration information and the Line ID. This mapping information is forwarded to the CLF (via the a2 reference point), which correlates this with the NASS User identity and NASS User network profile and pushes this information to RACS via the e4 reference point. The RACS configures its functionality according to the NASS User network profile information it receives from CLF.

I.6.1.3.1 Vulnerabilities and threats

The summary of the analysis is given in annex J.

I.6.1.4 Risk analysis

Table I.4 summarizes the risk analysis of attacks for interface e1.

Table I.4: Risk level for attacks for interface e1

Threat no.	Description	Impact	Likelihood	Risk
e1-T1	Interception at e1, no air interface	High	Possible	Critical
e1-T2	Interception at e1, air interface present	High	Likely	Critical
e1-T3	Interception at e1 from within NASS	High	Unlikely	Major
e1-T4	Manipulation of information exchanged over e1, no air interface	High	Possible	Critical
e1-T5	Manipulation of information exchanged over e1, air interface present	High	Likely	Critical
e1-T6	Manipulation of information exchanged over e1 from within NASS	High	Unlikely	Major
e1-T7	IP Spoofing	High	Likely	Critical
e1-T8	Impersonation	Low	Unlikely	Minor
e1-T9	Denial of Service	Medium	Likely	Critical

I.6.1.5 Countermeasure framework as detailed requirements

The following requirements make up the countermeasure for interface e1:

- Signalling over the e1 interface shall not be revealed to unauthorized 3rd parties.

- Information exchanged over the e1 interface shall not be revealed to unauthorized 3rd parties.
- Signalling over the e1 interface shall be protected from change by unauthorized 3rd parties.
- Information exchanged over the e1 interface shall be protected from change by unauthorized 3rd parties.
- The Transport Functions, and specifically the BGF and RCEF, shall be able to detect IP packets from the UE where IP addresses differ from that assigned during network attachments.
- The Transport Functions, and specifically the BGF and RCEF, shall be able to deny IP packets from the UE where IP addresses differ from that assigned during network attachments.
- The Transport Functions shall have mechanisms to detect denial-of-service attacks.
- NGN services shall only be available to authorized users.

I.6.2 Threat identification and risk analysis of scenario 1 (e5)

I.6.2.1 Overview of interface e5

Interface e5 is a roaming interface and is independent of the access technology. The interface is used to provide a consistent method for the visited NGN network to communicate with the home NGN network. Interface e5 is defined between V-UAAF and H-UAAF, which may be in different security domains. The interface allows the V-UAAF to request the H-UAAF to perform user authentication and authorization on its behalf, based on user profiles. It also allows the V-UAAF to forward accounting data for the particular user session to the H-UAAF in case of roaming.

The V-UAAF will forward access and authorization requests, as well as accounting messages, received over interface a3 from the AMF, to the H-UAAF over interface e5. Responses received back in return from the H-UAAF over interface e5 will be forwarded to the AMF over interface a3. A bilateral trust relationship between the V-UAAF and the H-UAAF is required to facilitate this exchange. The nature of this relationship is not specified. The specification of interface e5 is similar to that of interface a3, between the AMF and the UAAF in the visited network.

RADIUS and Diameter are two possible options for carrier protocols on interface e5. The interface supports both authentication/authorization and accounting message exchange and the information exchanged are: NASS User ID, Privacy Indicator, Globally Unique Address, QoS Profile Information (optional), and Initial Gate Setting (list of allowed destinations, list of denied destinations and default bandwidth).

The following analysis is based on the below specifications and RFCs:

- ES 282 004 [i.5];
- TS 183 020 [i.70];
- TS 129 234 [i.71];
- RFC 3539 [i.72];
- RFC 4005 [i.73];
- RFC 4072 [i.74];
- RFC 2865 [i.75];
- RFC 3580 [i.76];
- RFC 3748 [i.77];
- RFC 2548 [i.78];
- RFC 2866 [i.79];
- RFC 4372 [i.80];
- IETF RFC 2486bis(6) [i.81].

I.6.2.2 Protocols and profiles for interface e5

I.6.2.2.1 802.1X-based Authentication

Figure I.9 depicts a typical protocol stack for 802.1X-based authentication. Further details may be found in Wi-Fi Alliance. The EAP messages are carried over EAPOL (EAP over LAN) frames between the UE and the AP and then re-encapsulated in RADIUS or Diameter messages when sent from the AP to the home AAA Server (via zero or more AAA proxies). In figure I.9, the UE (mobile station) acts as the 802.1X supplicant, the AP acts as the authenticator, and the RADIUS AAA server acts as the authentication server.

IPSec is used to provide secure communication of RADIUS messages (RFC 3162 [i.82] describes use of RADIUS over IPv6-IPsec, and RFC 3580 [i.76] recommends use of IPsec to protect RADIUS). IPSec is also used to provide security communication of Diameter messages.

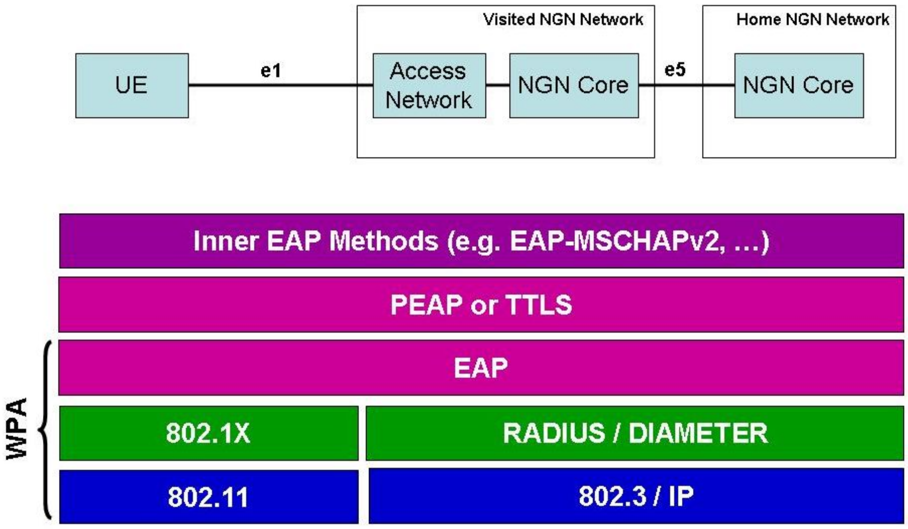


Figure I.9: 802.1X/EAP Authentication Protocol Stack

Figure I.10 depicts a typical 802.1X-based authentication scenario. The UE attempts to associate with an AP and is challenged to authenticate. At this point, the UE needs to indicate its user identity. There are usually two parts to this identity: the user name and the realm. Typically, these are combined into a Network Access Identifier (NAI) of the form user@realm. The realm part of the NAI is used to establish a connection with the appropriate AAA-H for that user. This presumes that the visited network recognizes that realm name. If this is not the case, then the visited network will signal an authentication failure back to the UE. The UE can then either try a different account (with a different realm) or can try to establish a new account on the visited network. If those alternatives also fail, the UE will be denied access or will be granted only limited guest access.

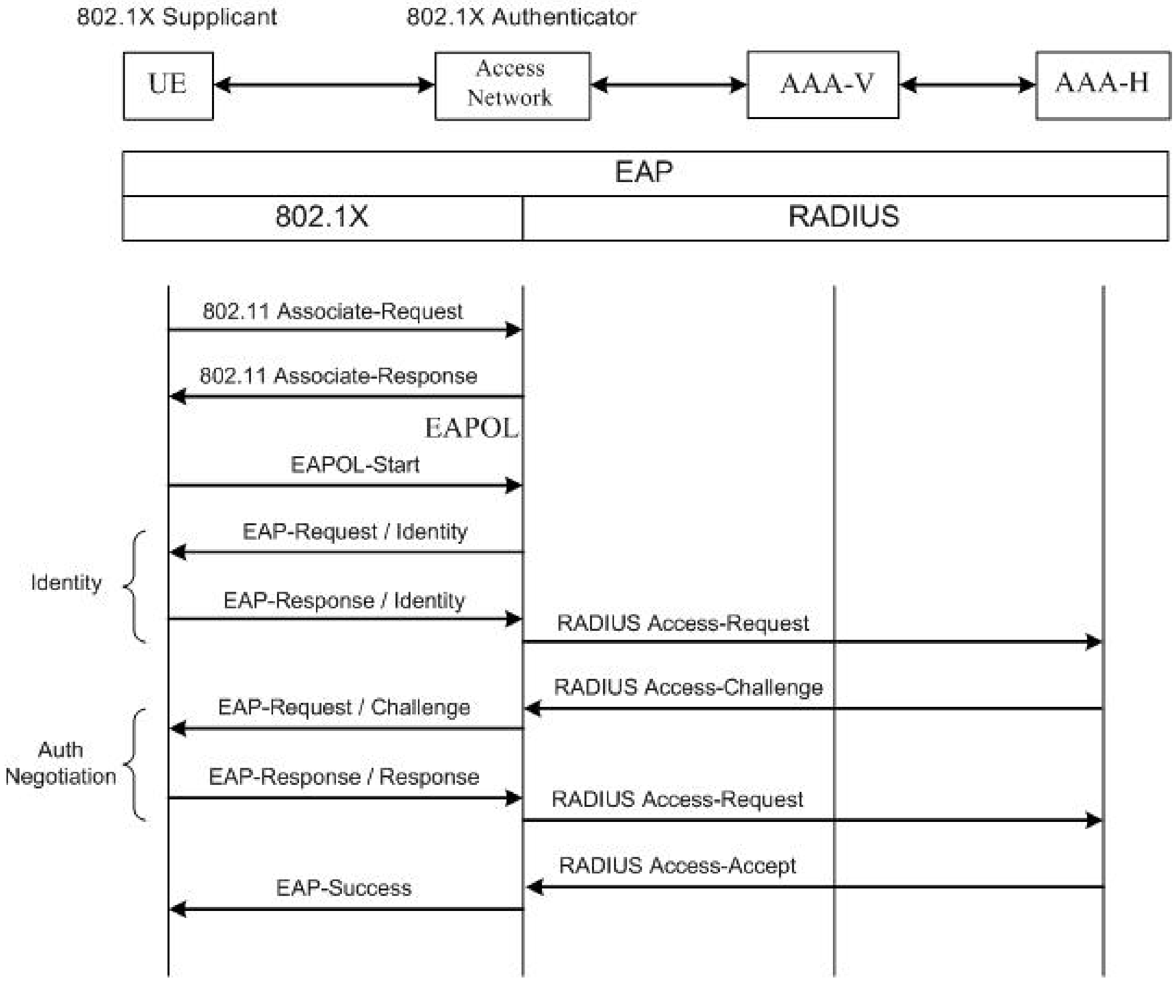


Figure I.10: 802.1X-based authentication with RADIUS as AAA protocol

I.6.2.2.2 Subscriber Profile Transfer

The protocol used on the e5 interface shall support the transport of subscriber profile information as defined in ES 282 004 [i.5]. Table I.5 provides the list of information elements to be carried over the interface for this purpose and indicates the list of Diameter attributes to achieve it. There is no standard solution defined for transferring subscriber profile data across networks where RADIUS is used instead of Diameter (TS 183 020 [i.70]).

Table I.5: Diameter attributes for Subscriber Profile Transfer

Information Element	Description	DIAMETER attribute	Defined in
SubscriberID	The identity of the subscriber requesting IP connectivity.	User-Name	RFC 3588 [i.83]
GloballyUniqueAddress	This information element contains: - The IP address of the user equipment used by the	Globally-Unique-Address	ES 283 034 [i.84]

Information Element	Description	DIAMETER attribute	Defined in
	subscriber for which profile information is being pushed. - The addressing domain in which the IP address is significant.		
InitialGateSetting	This information element contains: - The list of default destination IP addresses and ports to which traffic can be sent. - The maximum amount of bandwidth that can be used without explicit authorisation in the uplink direction. - The maximum amount of bandwidth that can be used without explicit authorisation in the downlink direction.	Initiate-Gate-Setting	ES 283 034 [i.84]
QoSProfile (NOTE 1)	For each subscribed transport service class and application class, this information element contains: - The maximum amount of bandwidth subscribed by the attached user in the uplink direction. - The maximum amount of bandwidth subscribed by the attached user in the downlink direction. - The maximum priority allowed for any reservation request.	QoS-Profile	ES 283 034 [i.84]
PrivacyIndicator (see note)	This information element provides policy rules for disclosure of subscriber profile elements to applications.	Privacy-Indicator	TS 183 020 [i.70]
NOTE: This information element may be repeated.			

I.6.2.3 Vulnerabilities and threats

Vulnerabilities of e5 are those of Diameter and Radius, depending on which protocol is deployed for the interface.

NOTE: There is no profile for e5 defined for Radius. Therefore, the analysis concentrates on the e5 Diameter profile.

Table I.6 summarizes the main vulnerabilities of the e5 Diameter Profile.

Table I.6: Vulnerabilities of e5 Diameter Profile

Vulnerability no.	Weakness	Attribute	Threats
e5-V1	The subscriber ID or NASS user identity is disclosed to visited NGN network	SubscriberID (User-Name)	The NASS identity will have the form of a NAI, which can be exploited for masquerade and IP spoofing attacks. The identity phase also carries information about the location and capabilities of an UE that an attacker can use to launch a DoS attack against the UE.
e5-V2	NGN visited and home network shall support WPA/802.1x. WPA has known weaknesses.	All information	WPA has known weaknesses and information protected by WPA should not be considered confidential. An attacker will, given the time and opportunity, gain knowledge of information protected by WPA.

The vulnerabilities identified for the e5 Diameter profile also hold for e5 when Radius is used, as the information used in the attacks is not directly related to interface e5.

NOTE: For the purpose of the analysis it is assumed that IPSec are employed according to TS 133 210 [i.13].

I.6.2.4 Risk analysis

Table I.7 lists the threats to information exchange between V-UAAF (also referred to as UAAF-proxy) and H-UAAF (also referred to as UAAF-server)

Table I.7: Risk level for e5 Diameter profile

Threat no.	Description	Impact	Likelihood	Risk
e5-T1	Masquerade as valid UE	High	Unlikely	Major
e5-T2	IP spoofing	Medium	Possible	Major
e5-T3	Denial of Service	Medium	Likely	Critical
e5-T4	Disclosure of sensitive information	High	Possible	Critical
e5-T5	Disclosure of privacy-related information	High	Possible	Critical

I.6.2.5 Countermeasure framework as requirements

The countermeasure proposed in ES 282 004 [i.5] and TS 183 020 [i.70] for protecting subscriber identity (user name, NAI) are the following:

- "To avoid revealing the true user identity to an entity other than the home service provider, especially across the WLAN radio link, the UE can use a generic user name like "anonymous" or "user" in the NAI given in the initial identity exchange. The realm part of the NAI is the only information the visited network needs to know at this point. If PEAP or TTLS are used to establish a secure tunnel between the STA and the AAA-H, then the protected identity exchange will not be visible to the visited network or to any eavesdroppers. The visited network will eventually need to obtain some identity value for charging and billing purposes if the authentication is successful. The home network can provide the identity that identifies the account for charging. This account is used between the visited network and the home network. This account need not be the same as that used by the home network to bill the subscriber. Furthermore, this identity can be an alias specified by the home provider rather than information that might compromise the true identity of the UE user. The identity used for charging can be shared only with the AAA infrastructure and never needs to be sent unprotected across the WLAN radio link."

The problem with this countermeasure is that the UE needs to be identifiable to the home NGN network. This means that the alias must be a pseudonym known only to the home network. This leads to the following requirements:

- The user identity visible to the visited NGN network should be pseudonymous.
- The pseudonymous user identity should only be resolvable by the home NGN network.
- There should be means to enable confidentiality protection on all communication over interface e5.

TS 183 020 [i.70] specifies that WPA/802.1x is mandatory to support for the home NGN network and that WPA2 is optional. This is an identified weakness of NASS (see table I.6). To remove this weakness, the following requirements should be added to 187 001:

- The visited NGN network should support WPA2.
- The home NGN network should support WPA2.

I.6.3 Threat identification and risk analysis of scenarios 5-11 (e2)

I.6.3.1 Overview of interface e2

This reference point enables Application Functions (AF) to retrieve information about the characteristics of the IP-connectivity session used to access NGN services and applications (e.g. network location information) from the CLF.

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

The following information flows are exchanged between the CLF and AF over interface e2:

- Information Query Request.
- Information Query Response.
- Event Registration Request.
- Event Registration Response.
- Notification Event Request.
- Notification Event Response.

The threat analysis of information exchanged over interface e2 is based on the following documents:

- ES 283 035 [i.85];
- TS 129 329 [i.86];
- TS 133 210 [i.13];
- RFC 3588 [i.83];
- RFC 3554 [i.87];
- RFC 2960 [i.88];
- RFC 3309 [i.89];
- ES 283 034 [i.84];
- RFC 4005 [i.73];
- RFC 4201 [i.90] and RFC 4301 [i.91].

I.6.3.2 Vulnerabilities and threats

ES 283 035 [i.85] specifies the Diameter profile for the e2 interface, and TS 133 210 [i.13] specifies the secure transport of Diameter messages. The following analysis covers both the e2 Diameter profile and the secure transport of Diameter messages.

Table I.8 summarizes the main vulnerabilities related to the e2 interface.

Secure communication of Diameter messages over e2 is protected by IPSec, as described in TS 133 210 [i.13]. IPSec is an IP layer protocol and can operate in two modes: transport mode and tunnel mode. Transport mode is a mode of operation that primarily protects the payload of the IP packet, in effect giving protection to higher level layers. Tunnel mode is a mode of operation that protects the whole IP packet by tunnelling it so that the whole packet is protected. The IPSec transport mode may be used to protect information exchanges within one security domain. Across security domains, the IPSec tunnel mode is mandatory and established between security gateways. TS 133 210 [i.13] specifies that security gateways shall be physically secured. The security gateway offers secure storage of the keys used for authentication and for confidentiality and integrity protection.

The security services offered over interface e2 are:

- data integrity;
- data origin authentication;
- anti-replay protection;
- confidentiality (optional);
- limited protection against traffic flow analysis when confidentiality is applied.

In cases where the application layer has been compromised, IPSec does not protect the higher layers in the protocol stack (application) from fabrication, masquerade and replay attacks. Information originating in the service layer will not be easily intercepted during transmission, but provided that the application itself is comprised, the information is presented in clear text on the receiver side on the service layer (or whatever layer is the target of the communication).

Table I.8: Vulnerabilities of e2 Diameter Profile

Vulnerability no.	Weakness	Attribute	Threats
e2-V1	Diameter over IPSec does not protect against compromised applications	Physical and logical address of UE, user identity, terminal type, type of access network, identity of sending application, the information requested, capabilities of UE, and QoS information.	Malicious application gains knowledge of sensitive and privacy-related information. Such information may be used to fabricate messages, to masquerade as an authorized application towards the UE and masquerade as the UE. The information can also be used to launch targeted DoS attacks.

Vulnerability no.	Weakness	Attribute	Threats
e2-V2	Confidentiality protection is not mandatory	All information	Disclosure of sensitive information. This information may also be used in combination with masquerade and IP spoofing attacks.
e2-V3	Lack of authorization of permanent failure messages	DIAMETER_ERROR_USER_UNKNOWN, DIAMETER_ERROR_IDENTITIES_DONT_MATCH, DIAMETER_ERROR_IDENTITIES_NOT_REGISTERED, DIAMETER_ERROR_IDENITY_ALREADY_REGISTERED, DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED	DoS attack against NASS, UE or specific applications if exploited in combination with e2-V1 and e1-V2
e2-V3	Diameter session handling. Diameter sessions are implicitly terminated, which means that the server does not maintain state information and that the client does not need to send any re-authorization or session termination request to the server.	NO_STATE_MAINTAINED (RFC 3588 [i.83])	Session hijacking

I.6.3.3 Risk analysis

Table I.9 summarizes the risk analysis of the e2 Diameter profile.

Table I.9: Risk level for e2 Diameter profile

Threat no.	Description	Impact	Likelihood	Risk
e2-T1	Disclosure of sensitive information	High	Possible	Critical
e2-T2	Masquerade	Medium	Unlikely	Minor
e2-T3	IP spoofing	Medium	Unlikely	Minor
e2-T4	DoS	Medium	Possible	Major
e2-T5	Session Hijacking	Medium	Unlikely	Minor

NOTE: The impact depends on the length of the session timeout.

I.6.3.4 Countermeasure framework as requirements

Confidentiality protection is optional (TS 133 210 [i.13]) between security domains, and even when confidentiality protection according to TS 133 210 [i.13] is employed, there is limited protection against traffic flow analysis. TS 133 210 [i.13] do not cover accountability, but provides measures for data origin authentication.

To protect e2 against disclosure, masquerade and DoS attacks the following requirements should be added to TS 187 001 [i.6]:

- There should be means to enable confidentiality protection of all information exchanged over interface e2.
- The CLF shall be able to validate the authenticity of Application Functions (AF).
- The CLF shall be able to detect multiple similar information requests/response messages from the same origin within the service control subsystems.

I.7 Risk Analysis

Table I.10 summarizes the risk analysis of attacks relevant for NASS.

Table I.10: Risk level for attacks for NASS

Threat no.	Description	Impact	Likelihood	Risk
e1-T1	Interception at e1, no air interface	High	Possible	Critical
e1-T2	Interception at e1, air interface present	High	Likely	Critical
e1-T3	Interception at e1 from within NASS	High	Unlikely	Major
e1-T4	Manipulation of information exchanged over e1, no air interface	High	Possible	Critical
e1-T5	Manipulation of information exchanged over e1, air interface present	High	Likely	Critical
e1-T6	Manipulation of information exchanged over e1 from within NASS	High	Unlikely	Major
e1-T7	IP Spoofing	High	Likely	Critical
e1-T8	Impersonation	Low	Unlikely	Minor
e1-T9	Denial of Service	Medium	Likely	Critical
e1-T1	"Line-id poisoning" attack	Medium	Likely	Critical (N/A)
e5-T2	Masquerade as valid UE	High	Unlikely	Major
e5-T3	IP spoofing	Medium	Possible	Major
e5-T4	Denial of Service	Medium	Likely	Critical
e5-T5	Disclosure of sensitive information	High	Possible	Critical
e5-T6	Disclosure of privacy-related information	High	Possible	Critical
e2-T1	Disclosure of sensitive information	High	Possible	Critical
e2-T2	Masquerade	Medium	Unlikely	Minor
e2-T3	IP spoofing	Medium	Unlikely	Minor
e2-T4	DoS	Medium	Possible	Major
e2-T5	Session Hijacking	Medium	Unlikely	Minor

I.8 Countermeasure framework as detailed requirements

The following requirements make up the countermeasure framework for NASS:

1) Signalling over the e1 interface shall not be revealed to unauthorized 3rd parties.

2) Information exchanged over the e1 interface shall not be revealed to unauthorized 3rd parties.

3) Signalling over the e1 interface shall be protected from change by unauthorized 3rd parties.

4) Information exchanged over the e1 interface shall be protected from change by unauthorized 3rd parties.

5) The Transport Functions, and specifically the BGF and RCEF, shall be able to detect IP packets from the UE where IP addresses differ from that assigned during network attachments.

6) The Transport Functions, and specifically the BGF and RCEF, shall be able to deny IP packets from the UE where IP addresses differ from that assigned during network attachments.

7) The Transport Functions shall have mechanisms to detect denial-of-service attacks.

8) NGN services shall only be available to authorized users.

9) <deleted>

10) The user identity visible to the visited NGN network should be pseudonymous.

11) The pseudonymous user identity should only be resolvable by the home NGN network.

12) There shall be means to enable confidentiality protection on all communication over interface e5.

13) The visited NGN network should support WPA2.

14) The home NGN network should support WPA2.

15) There shall be means to enable confidentiality protection of all information exchanged over interface e2

16) The CLF shall be able to validate the authenticity of Application Functions (AF)

17) The CLF shall be able to detect multiple similar information requests/response messages from the same origin within the service control subsystems

I.9 Mapping NASS Countermeasure Framework to TS 187 001

The below list summarizes the mapping of the NASS countermeasure framework as described in clause 9 to the NGN security requirements as specified in TS 187 001 [i.6].

- Requirements 1, 2, 12, 13 and 14 relate TS 187 001 [i.6] requirement number R-CD-2.
- Requirements 1, 2 and 12 relate TS 187 001 [i.6] requirement number R-CD-21.
- Requirements 3, 4 relate to TS 187 001 [i.6] requirement number R-CD-13, R-CD-14, R-CD-18 and R-CD-19.
- Requirements 9, 10 and 11 relate to TS 187 001 [i.6] requirement number R-CD-22, R-P-4, R-P-7, R-P-8, R-P-12, R-P-13, R-IR-2 and R-IR-3.
- Requirements 7, 8 and 17 relate to TS 187 001 [i.6] requirement number R-AD-1.
- Requirements 13 and 14 relate to TS 187 001 [i.6] requirement number R-CPN-CR-1.
- Requirements 9, 12 and 15 relate to TS 187 001 [i.6] requirement number R-AA-12.
- Requirement 8 relates to TS 187 001 [i.6] requirements number R-AA-7, R-AA-29, R-AD-2 and R-AD-3.

- Requirements 1, 2, 12 and 15 relate to TS 187 001 [i.6] requirements number R-CD-2, R-CD-3, R-CD-18, R-CD-19, R-P-1, R-P-2 and R-P-5.
- Requirements 3 and 4 relate to TS 187 001 [i.6] requirement number R-CD-13.
- Requirements 5 and 6 relate to TS 187 001 [i.6] requirement number R-AA-14.
- Requirements 1, 2, 9, 10, 11, 12 and 15 relate to TS 187 001 [i.6] requirement number R-P-3.
- Requirements 5, 6, 8 and 17 relate to TS 187 001 [i.6] requirement number R-NF-2.

Requirement 16 is not addressed by any of the TS 187 001 [i.6] requirements.

I.10 TS 187 001 requirements aligned with NASS countermeasure framework

I.10.1 WLAN 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.

13 - The visited NGN network should support WPA2.

14 - The home NGN network should support WPA2.

I.10.2 AAAA requirements

(R-AA- 7) It shall be possible to prevent the use of a particular ISIM to access NGN networks and services and it should be possible to revoke a specific ISIM.

(R-AA- 1) Access to NGN networks, services, and applications shall be provided for authorized users only.

8 - NGN services shall only be available to authorized users.

(R-AA- 12) Transmitted passwords shall be sufficiently protected; e.g. by encryption or other techniques.

12 - There shall be means to enable confidentiality protection on all communication over interface e5.

15 - There shall be means to enable confidentiality protection of all information exchanged over interface e2

(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.

8 - NGN services shall only be available to authorized users.

I.10.3 Identity and secure registration requirements

(R-IR- 1) An access identity shall be used for access authentication. This identity may or may not be used for other purposes.

10 - The user identity visible to the visited NGN network should be pseudonymous.

11 - The pseudonymous user identity should only be resolvable by the home NGN network.

(R-IR- 2) The line ID shall be possible to use for line authentication.

10 - The user identity visible to the visited NGN network should be pseudonymous.

11 - The pseudonymous user identity should only be resolvable by the home NGN network.

I.10.4 Privacy requirements

(R-P- 16) 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.

1 - Signalling over the e1 interface shall not be revealed to unauthorized 3rd parties.

2 - Information exchanged over the e1 interface shall not be revealed to unauthorized 3rd parties.

12 - There shall be means to enable confidentiality protection on all communication over interface e5.

15 - There shall be means to enable confidentiality protection of all information exchanged over interface e2

(R-P- 17) User location and usage patterns shall be kept from unwanted disclosure.

1 - Signalling over the e1 interface shall not be revealed to unauthorized 3rd parties.

2 - Information exchanged over the e1 interface shall not be revealed to unauthorized 3rd parties.

12 - There shall be means to enable confidentiality protection on all communication over interface e5.

15 - There shall be means to enable confidentiality protection of all information exchanged over interface e2

(R-P- 18) It shall be possible to protect the confidentiality of user identity data.

1 - Signalling over the e1 interface shall not be revealed to unauthorized 3rd parties.

2 - Information exchanged over the e1 interface shall not be revealed to unauthorized 3rd parties.

9 - The NASS user identity shall not be disclosed to unauthorized 3rd parties.

10 - The user identity visible to the visited NGN network should be pseudonymous.

11 - The pseudonymous user identity should only be resolvable by the home NGN network.

12 - There shall be means to enable confidentiality protection on all communication over interface e5.

15 - There shall be means to enable confidentiality protection of all information exchanged over interface e2

(R-P- 19) 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.

9 - The NASS user identity not be disclosed to unauthorized 3rd parties.

10 - The user identity visible to the visited NGN network should be pseudonymous.

11 - The pseudonymous user identity should only be resolvable by the home NGN network.

(R-P- 20) 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.

1 - Signalling over the e1 interface shall not be revealed to unauthorized 3rd parties.

2 - Information exchanged over the e1 interface shall not be revealed to unauthorized 3rd parties.

12 - There shall be means to enable confidentiality protection on all communication over interface e5.

15 - There shall be means to enable confidentiality protection of all information exchanged over interface e2

(R-P- 21) 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).

9 - The NASS user identity shall not be disclosed to unauthorized 3rd parties.

10 - The user identity visible to the visited NGN network should be pseudonymous.

11 - The pseudonymous user identity should only be resolvable by the home NGN network.

(R-P- 22) The NGN shall provide mechanisms that allow to present the identity of the session originator, if this is not restricted by the session originator.

9 - The NASS user identity shall not be disclosed to unauthorized 3rd parties.

10 - The user identity visible to the visited NGN network should be pseudonymous.

11 - The pseudonymous user identity should only be resolvable by the home NGN network.

(R-P- 23) It shall be possible for the sender of the message to request to hide its public ID from the recipient.

9 - The NASS user identity shall not be disclosed to unauthorized 3rd parties.

10 - The user identity visible to the visited NGN network should be pseudonymous.

11 - The pseudonymous user identity should only be resolvable by the home NGN network.

(R-P- 24) 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.

9 - The NASS user identity shall not be disclosed to unauthorized 3rd parties.

10 - The user identity visible to the visited NGN network should be pseudonymous.

11 - The pseudonymous user identity should only be resolvable by the home NGN network.

I.10.5 Communication, data security and confidentiality requirements

(R-CD- 2) Network Domain Security (NDS) shall be provided at the network layer and comply to TS 133 210 [i.13].

1 - Signalling over the e1 interface shall not be revealed to unauthorized 3rd parties.

2 - Information exchanged over the e1 interface shall not be revealed to unauthorized 3rd parties.

12 - There shall be means to enable confidentiality protection on all communication over interface e5.

15 - There shall be means to enable confidentiality protection of all information exchanged over interface e2

(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

1 - Signalling over the e1 interface shall not be revealed to unauthorized 3rd parties.

2 - Information exchanged over the e1 interface shall not be revealed to unauthorized 3rd parties.

12 - There shall be means to enable confidentiality protection on all communication over interface e5.

15 - There shall be means to enable confidentiality protection of all information exchanged over interface e2

(R-CD- 7) 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.

1 - Signalling over the e1 interface shall not be revealed to unauthorized 3rd parties.

2 - Information exchanged over the e1 interface shall not be revealed to unauthorized 3rd parties.

12 - There shall be means to enable confidentiality protection on all communication over interface e5.

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

3 - Signalling over the e1 interface shall be protected from change by unauthorized 3rd parties.

4 - Information exchanged over the e1 interface shall be protected from change by unauthorized 3rd parties.

(R-CD- 18) Confidentiality of communications should be achieved by cryptographic encryption. Confidentiality of stored data shall be achieved by cryptographic encryption or by access controls.

1 - Signalling over the e1 interface shall not be revealed to unauthorized 3rd parties.

2 - Information exchanged over the e1 interface shall not be revealed to unauthorized 3rd parties.

12 - There shall be means to enable confidentiality protection on all communication over interface e5.

15 - There shall be means to enable confidentiality protection of all information exchanged over interface e2

(R-CD- 19) Confidentiality of signalling and control messages shall be enforced if required by the application or in environments where the security policy demands confidentiality. The mechanism should allow a choice in the algorithm to be used.

1 - Signalling over the e1 interface shall not be revealed to unauthorized 3rd parties.

2 - Information exchanged over the e1 interface shall not be revealed to unauthorized 3rd parties.

12 - There shall be means to enable confidentiality protection on all communication over interface e5.

15 - There shall be means to enable confidentiality protection of all information exchanged over interface e2

(R-CD- 21) Confidentiality protection between Network Functions (e.g. between CSCFs, or between CSCFs and the HSS) shall rely on mechanisms specified by Network Domain Security in TS 133 210 [i.13].

1 - Signalling over the e1 interface shall not be revealed to unauthorized 3rd parties.

2 - Information exchanged over the e1 interface shall not be revealed to unauthorized 3rd parties.

12 - There shall be means to enable confidentiality protection on all communication over interface e5.

(R-CD- 22) It shall be possible to protect the confidentiality of user-related data which is stored or processed by a provider.

1 - Signalling over the e1 interface shall not be revealed to unauthorized 3rd parties.

2- Information exchanged over the e1 interface shall not be revealed to unauthorized 3rd parties.

9 - The NASS user identity shall not be disclosed to unauthorized 3rd parties.

10 - The user identity visible to the visited NGN network should be pseudonymous.

11 - The pseudonymous user identity should only be resolvable by the home NGN network.

12 - There shall be means to enable confidentiality protection on all communication over interface e5.

15 - There shall be means to enable confidentiality protection of all information exchanged over interface e2

I.10.6 Availability and DoS Protection requirements

(R-NF- 2) Filters to screen the IP packets to restrict/grant access to specific bearer streams shall be supported.

5 - The Transport Functions, and specifically the BGF and RCEF, shall be able to detect IP packets from the UE where IP addresses differ from that assigned during network attachments.

6 - The Transport Functions, and specifically the BGF and RCEF, shall be able to deny IP packets from the UE where IP addresses differ from that assigned during network attachments.

8 - NGN services shall only be available to authorized users.

17 - The CLF shall be able to detect multiple similar information requests/response messages from the same origin within the service control subsystems

(R-AD- 1) Mechanisms shall be provided to mitigate denial-of-service attacks.

7 - The Transport Functions shall have mechanisms to detect denial-of-service attacks.

8 - NGN services shall only be available to authorized users.

17 - The CLF shall be able to detect multiple similar information requests/response messages from the same origin within the service control subsystems

(R-AD- 2) Provide access control mechanisms to ensure that authorized users only can access the service.

8 - NGN services shall only be available to authorized users.

(R-AD- 3) It shall be possible to prevent intruders from restricting the availability of services by logical means.

8 - NGN services shall only be available to authorized users.

I.11 Residual Risk

This clause documents the residual risk from the NASS TVRA. The numbering of the requirements in the below list aligns with that in clause I.9, which gives the complete NASS countermeasure framework.

NOTE: The below requirements have not been addressed in TS 187 001 [i.6] and TS 187 003 [i.7] and is for further study.

1 - Signalling over the e1 interface shall not be revealed to unauthorized 3rd parties.

2 - Information exchanged over the e1 interface shall not be revealed to unauthorized 3rd parties.

3 - Signalling over the e1 interface shall be protected from change by unauthorized 3rd parties.

4 - Information exchanged over the e1 interface shall be protected from change by unauthorized 3rd parties.

5 - The Transport Functions, and specifically the BGF and RCEF, shall be able to detect IP packets from the UE where IP addresses differ from that assigned during network attachments.

6 - The Transport Functions, and specifically the BGF and RCEF, shall be able to deny IP packets from the UE where IP addresses differ from that assigned during network attachments.

13 - The visited NGN network should support WPA2.

14 - The home NGN network should support WPA2.

18) 16 - The CLF shall be able to validate the authenticity of Application Functions (AF)

19) 17 - The CLF shall be able to detect multiple similar information requests/response messages from the same origin within the service control subsystems

I.12 Open issues and topics for further study

The NASS TVRA has identified the following open issues:

- What EAP "deployments" are supported in NGN (EAP-SIM and EAP-AKA)?
  - The various EAP deployments have distinctive problems. Some are vulnerable to dictionary attacks, plaintext attacks, MiM attacks and Ciphertext attacks.

- Secure communication for Diameter messages are IPSec as specified in TS 133 210 [i.13]:
    - Confidentiality services should be made mandatory.
    - IPSec does not secure the Diameter message as such, it only provides secure communication of Diameter messages over interfaces.
- There is a need for a security profile for Diameter messages in NGN.
- Radius is supported as the protocol for several interfaces, but there is no Radius profile for e5, e4 and e2.
- SIP has know weaknesses that has yet not been addressed.
- Lack of protection of interface e1.
- No direct security association between UE and UAAF in NASS for authentication.

Annex J: Vulnerabilities, Threats and Risks to interface e1

NOTE: Whilst the present document is a technical report it identifies requirements for future work as a direct consequence of the analysis and should not be interpreted as mandates in the scope of the present document. In all cases these requirements are considered indicative pending their ratification in formal ETSI Technical Specifications within the TISPAN Work Programme.

J.1 Risk analysis

The following clauses summarize the threat identification and risk analysis for information exchanged over interface e1.

J.1.1 Information Disclosure

Information disclosure means that an unauthorized party may learn information transferred or stored. According to the penetration points the following threats can be distinguished.

J.1.1.1 Interception at the customer interface (e1)

There are essentially two scenarios to consider:

- Scenario A: Access authentication based on implicit line authentication.
- Scenario B: Access authentication based on explicit authentication mechanism such as CHAP or EAP.

If an air interface is present in scenario B then confidentiality of signalling messages has to be provided on that air link. Otherwise, for scenarios A and B, confidentiality of the signalling messages is generally not required as the operator can rely on its security countermeasures in both its access and IMS domains, e.g. intrusion protection and countermeasures to protect administrative operations in the access and IMS domains.

Table J.1: Attack potential for interception at e1, no air interface

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 week	1
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Moderate	4
Equipment	Standard	0
Total	Moderate - possible	7

Table J.2: Attack potential for interception at e1, air interface present

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 week	1
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Easy	1
Equipment	Standard	0
Total	Basic - Likely	4

J.1.1.2 Interception within the access network providers network

For the purposes of this analysis it is assumed that the access network is physically difficult to penetrate and will manage to identify break-ins. It is assumed that the protocols and signalling are defined with respect to publicly available specifications.

Table J.3: Attack potential for interception e1 from within NASS

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 month	4
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Difficult	12
Equipment	Standard	0
Total	High - unlikely	18

Table J.4 summarizes the risk analysis of interception attacks at interface e1.

Table J.4: Risk level for interception attacks at interface e1

Threat no.	Description	Impact	Likelihood	Risk
e1-T1	Interception at e1, no air interface	High	Possible	Critical
e1-T2	Interception at e1, air interface present	High	Likely	Critical
e1-T3	Interception at e1 from within NASS	High	Unlikely	Major

J.1.1.3 Countermeasure framework as detailed requirements

Detailed requirements to protect the e1 interface against interception attacks are given below.

- Signalling over the e1 interface shall not be revealed to unauthorized 3rd parties.
- Information exchanged over the e1 interface shall not be revealed to unauthorized 3rd parties.

J.1.2 Manipulation

J.1.2.1 Manipulation at the customer interface (e1)

There are essentially two scenarios to consider:

- Scenario A: Access authentication based on implicit line authentication.
- Scenario B: Access authentication based on explicit authentication mechanism such as CHAP or EAP.

In scenario A, the IMS domain can rely on existing protection against message modification since the IMS domain can rely on the access domain providing this protection by means of VPNs, message separation using VLANs, and other security methods, as both IMS and access domain are one and the same operator.

Table J.5: Attack potential for manipulation of information exchanged over e1, no air interface present

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 week	1
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Moderate	4
Equipment	Standard	0
Total	Moderate - possible	7

In scenario B, when the access is provided using WLANs or other wireless technologies then radio-link protection is to be provided. Table J.6 documents the attack potential if insufficient radio-link protection is provided.

Table J.6: Attack potential for manipulation information exchanged over e1, air interface present

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 week	1
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Easy	1
Equipment	Standard	0
Total	Basic - Likely	4

In scenario B, when the access is provided using WLANs or other wireless technologies then air-link protection is provided using keys derived from the authentication process (e.g. key derivation procedures as described by TS 133 234 [i.20]).

If sufficient protection of signalling messages is provided then the risks associated with message modification is greatly reduced for scenario B.

J.1.2.2 Manipulation within the access network providers network

For the purposes of this analysis it is assumed that the access network is physically difficult to penetrate and is able to identify a compromise. It is assumed that the protocols and signalling are defined with respect to publicly available specifications.

Table J.7: Attack potential for manipulation at the customer interface (e1)

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 month	4
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Difficult	12
Equipment	Standard	0
Total	High - unlikely	18

Table J.8 summarizes the risk analysis of manipulation attacks towards interface e1.

Table J.8: Risk level for manipulation on information exchanged over interface e1

Threat no.	Description	Impact	Likelihood	Risk
e1-T4	Manipulation of information exchanged over e1, no air interface	High	Possible	Critical
e1-T5	Manipulation of information exchanged over e1, air interface present	High	Likely	Critical
e1-T6	Manipulation of information exchanged over e1 from within NASS	High	Unlikely	Major

J.1.2.3 Countermeasure framework as requirements

Detailed requirements to protect the e1 interface against manipulation attacks are given below.

- Signalling over the e1 interface shall be protected from change by unauthorized 3rd parties.
- Information exchanged over the e1 interface shall be protected from change by unauthorized 3rd parties.

J.1.3 IP Address and Identity spoofing

Identity spoofing is a technique used to gain unauthorized access to networks and services, whereby the attacker sends messages to a computer with a forged identity indicating that the message is coming from a trusted host. Consider the following scenario where User B attaches to NASS and gets IP address IP_B. Now the User B registers with the IMS using his IMS identity ID_B with the P-CSCF using the NBA. The following three kinds of attacks are possible by spoofing the identities:

- Attacker A sends SIP messages using his own IMS identity (ID_A) but with the source IP address of B (IP_B):
    - If the binding between the IP address (allocated by NASS during attachment) and the source IP address in subsequent packets is not checked, then the attacker will succeed. The consequence is that A pays for IMS service but IP connectivity is fraudulently charged to B. Note that this attack only makes sense for IMS services with outgoing traffic because the attacker will not receive any incoming packets addressed to the IMS identity that the attacker is impersonating.
- Attacker A sends SIP invite using his own source IP address (IP_A) but with the IMS identity of B (ID_B):
    - If the binding between the IP address on the NASS level, and the public and private user identities is not checked then the attacker will succeed. The consequence will be that A pays for IP connectivity but IMS service is fraudulently charged to B.
- Attacker A sends SIP messages using IMS identity (ID_B) and source IP address (IP_B):
    - If the bindings mentioned in the above attacks are not checked then the attacker will succeed, i.e. A fraudulently charges both IP connectivity and the IMS service to B. Note this attack only makes sense for IMS services with outgoing traffic because the attacker will not receive any incoming packets addressed to the IMS identity that he is impersonating.
- Denial of Service attacks aims at preventing authorized access or to reduce service levels. A DoS attack can be carried out by attacker A sending SIP BYE using the IP address IP_B and the IMS identity (ID_B) as described in the previous section. This attack assumes a successful IP address and identity spoofing.

J.1.3.1 Risk assessment

Table J.9 summarizes the attack potential of IP spoofing, and table J.10 summarizes the risk analysis of IP Spoofing attacks.

Table J.9: Attack potential for IP Spoofing

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 day	0
Expertise	Layman	0
Knowledge of TOE	Public	0
Access to mount attack	Easy	1
Equipment	Standard	0
Total	No rating - likely	1

Table J.10: Risk level for IP Spoofing attacks at interface e1

Threat no.	Description	Impact	Likelihood	Risk
e1-T7	IP Spoofing	High	Likely	Critical

J.1.3.2 Countermeasure framework as requirements

The risk of IP spoofing attacks is highest for the Transport Functions. One mechanism that can be used to protect against such attacks are to make the BGF, specifically the RCEF, able to detect and deny the UE to successfully transmit an IP packet with a source IP address that is different to the one assigned during the network attachment. When such a mismatch is detected the BGF should drop the packet.

NOTE: The RCEF function is the function that should enforce the anti IP spoofing but the ARF manages the association between the layer-2 and layer-3 identities. As no interface exists between the two components they need to be collocated.

This gives the following requirements:

- The Transport Functions, and specifically the BGF and RCEF, shall be able to detect IP packets from the UE where IP addresses differ from that assigned during network attachments.
- The Transport Functions, and specifically the BGF and RCEF, shall be able to deny IP packets from the UE where IP addresses differ from that assigned during network attachments.

J.1.4 Invalidation of IP address not signalled

In case an IP address becomes invalid (e.g. the user ends or loses the connection to the core network without deregistering from IMS), this information is not signalled to the IMS. Hence, another user who obtains the same IP address as the other user before him may impersonate that user on the IMS level. This impersonation will be detected during the next network-initiated re-registration procedure. The interval between two (re-)registrations is not specified, but would most probably be around one minute. The consequence is that the IMS may be under attack between to registrations. As long as the impersonation lasts, the attacker has the same authorizations as that of the impersonated user.

J.1.4.1 Risk assessment

Table J.11 summarizes the attack potential of impersonation attacks, and table J.12 summarizes the risk analysis of impersonation attacks.

Table J.11: Attack potential for impersonation attacks

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 month	4
Expertise	Layman	0
Knowledge of TOE	Public	0
Access to mount attack	Difficult	12
Equipment	Standard	0
Total	High - unlikely	16

Table J.12: Risk level for impersonation attacks at interface e1

Threat no.	Description	Impact	Likelihood	Risk
e1-T8	Impersonation	Low	Unlikely	Minor

J.1.4.2 Countermeasure framework as requirements

The following requirements define the countermeasure framework for impersonation threats:

- The IP address invalidation shall be signalled to the IMS.
- The access network shall guarantee that an IP address that has become invalid cannot be re-assigned for a certain amount of time.

NOTE: As the risk level is minor there is no need to add countermeasures to protect against impersonation attacks.

J.1.5 Denial-of-Service

This threat means that an unauthorized party may deny system availability to authorized parties.

There are essentially two scenarios to consider:

- Scenario A: Access authentication based on implicit line authentication.
- Scenario B: Access authentication based on explicit authentication mechanism such as CHAP or EAP.

J.1.5.1 Risk assessment

Table J.13 summarizes the attack potential of DoS attacks, and table J.14 summarizes the risk analysis of DoS attacks.

Table J.13: Attack potential for DoS attacks

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1 week	1
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Easy	1
Equipment	Standard	0
Total	Basic - Likely	4

Table J.14: Risk level for DoS attacks at interface e1

Threat no.	Description	Impact	Likelihood	Risk
e1-T9	Denial of Service	Medium	Likely	Critical

J.1.5.2 Countermeasure framework as requirements

The countermeasure framework to protect the e1 interface against DoS attacks are defined as the following requirements:

- The Transport Functions shall have mechanisms to detect denial-of-service attacks.
- NGN services shall only be available to authorized users.

J.1.6 "line-id poisoning" attack with malicious P-Access-Network-Info

Figure J.1 illustrates line-id poisoning attacks and shows the steps involved in the attack.

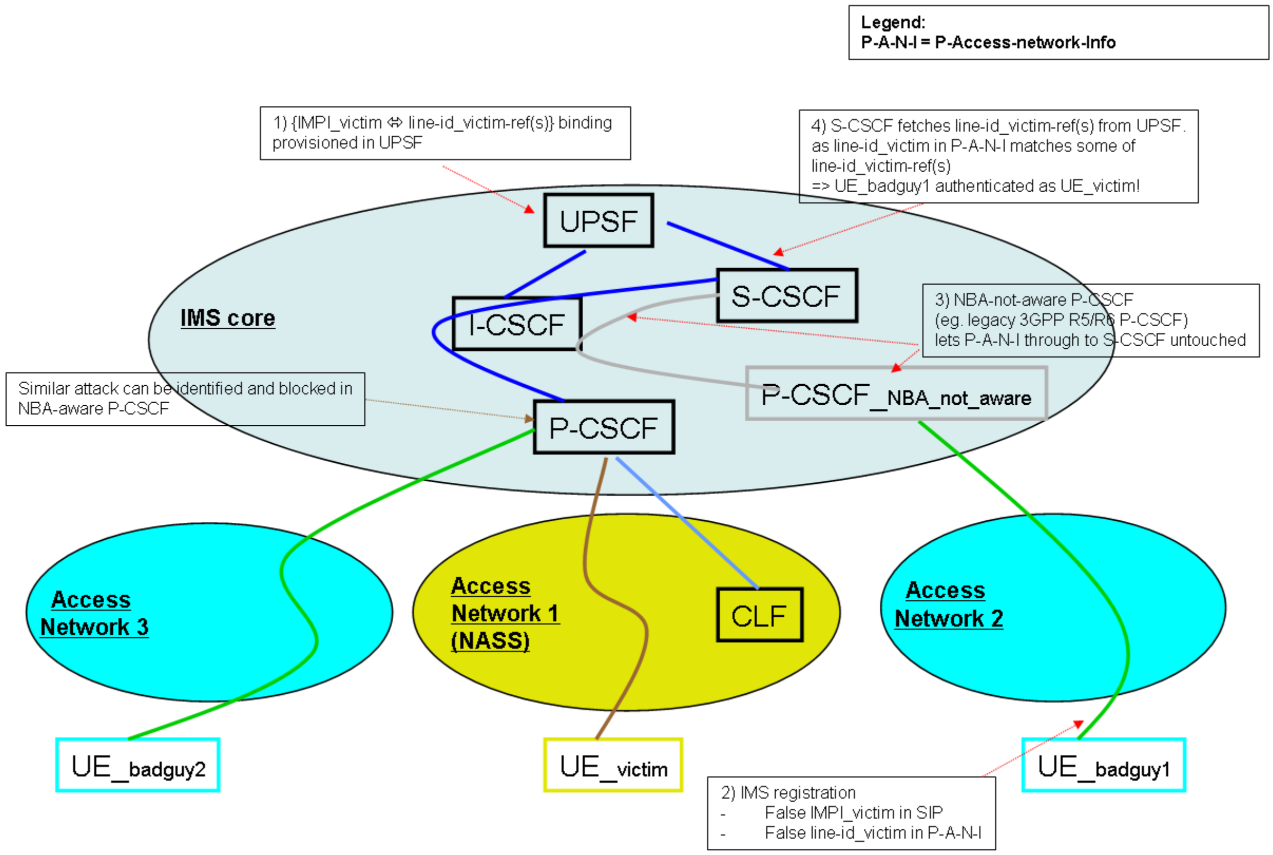

Legend:
P-A-N-I = P-Access-network-Info
1) {IMPI_victim ⇔ line-id_victim-ref(s)} binding provisioned in UPSF
4) S-CSCF fetches line-id_victim-ref(s) from UPSF. as line-id_victim in P-A-N-I matches some of line-id_victim-ref(s)
=> UE_badguy1 authenticated as UE_victim!
UPSF
S-CSCF
I-CSCF
IMS core
3) NBA-not-aware P-CSCF (eg. legacy 3GPP R5/R6 P-CSCF) lets P-A-N-I through to S-CSCF untouched
P-CSCF_NBA_not_aware
Similar attack can be identified and blocked in NBA-aware P-CSCF
P-CSCF
Access Network 3
Access Network 1 (NASS)
CLF
Access Network 2
UE_badguy2
UE_victim
UE_badguy1
2) IMS registration
- False IMPI_victim in SIP
- False line-id_victim in P-A-N-I

Figure J.1: "line-id poisoning" attack scenario

The target of the attack are those networks where both deployed P-CSCFs are "NBA-aware", that is, implementing the NASS-IMS bundled Authentication procedure, and those "NBA non-aware" P-CSCFs that are not aware of network-provided P-Access-Network-Info.

Attack Steps:

1) The victim (UE_victim) is an IMS subscriber provisioned with NASS-IMS bundled authentication so the mapping between IMPI and reference line-id set exists in UPSF.

2) Attacker (UE_badguy1) launches the attack by sending REGISTER that contains IMPI of the victim and a malicious "network-provided" P-Access-Network-Info that contains "line-id" corresponding to that IMPI. The REGISTER is purposely sent to an "NBA-non-aware" P-CSCF.

3) "NBA-non-aware" P-CSCF will not check the P-Access-Network-Info; so P-CSCF passes the header untouched toward S-SCCF via I-CSCF.

4) S-CSCF performs normal NASS-IMS bundled authentication procedure, fetching reference line-id set from UPSF based on the IMPI and comparing that with the one provided in P-Access-Network-Info. The comparison will be successful so the attacker can masquerade to the victim.

J.1.6.1 Risk assessment

Table J.15 summarizes the attack potential of line-id poisoning attacks, and table J.16 summarizes the risk analysis of line-id poisoning attacks.

Table J.15: Attack potential for "line-id poisoning" attack

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	≤ 1	1
Expertise	Layman	0
Knowledge of TOE	Public	0
Access to mount attack	Easy	1
Equipment	Standard	0
Total	Basic - Likely	2

Table J.16: Risk level for "line-id poisoning" attack

Threat no.	Description	Impact	Likelihood	Risk
e1-T10	"Line-id poisoning" attack	Medium	Likely	Critical

J.1.6.2 Countermeasure framework as requirements

NOTE: This does not apply to e1 communication, but to NASS-IMS bundled authentication.

Annex K:
Change history

Date mm-yy	WG Doc.	CR	Rev	CAT	Title / Comment	Current Version	New Version
11-07	WG7TD011r1	001	1		NAT-T input from STF329	2.0.2	2.0.3
05-08	17bTD057r1	002	1		TVRA for RACS	2.0.2	2.0.3
07-08	18WTD021	003	1		Drafting notes from minutes of WG7 session	2.0.2	2.0.3
End of R2 CRs, numbering restarted for R3 CRs							
09-09	22WTD088r1	001	1	B	Addition of CPN TVRA	2.2.1	3.0.1
01-10	23WTD088	002	1	B	Changes arising from 7035 work on identity and privacy protection	3.0.1	3.0.2
12-10	TISPAN07(10)196	003	-	B	Addition of NASS TVRA	3.0.2	3.0.3
					publication	3.0.3	3.1.1

Annex L: Bibliography

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

History

Document history		
V1.1.1	March 2006	Publication
V1.2.2	March 2008	Publication
V2.1.1	December 2008	Publication
V3.1.1	April 2011	Publication