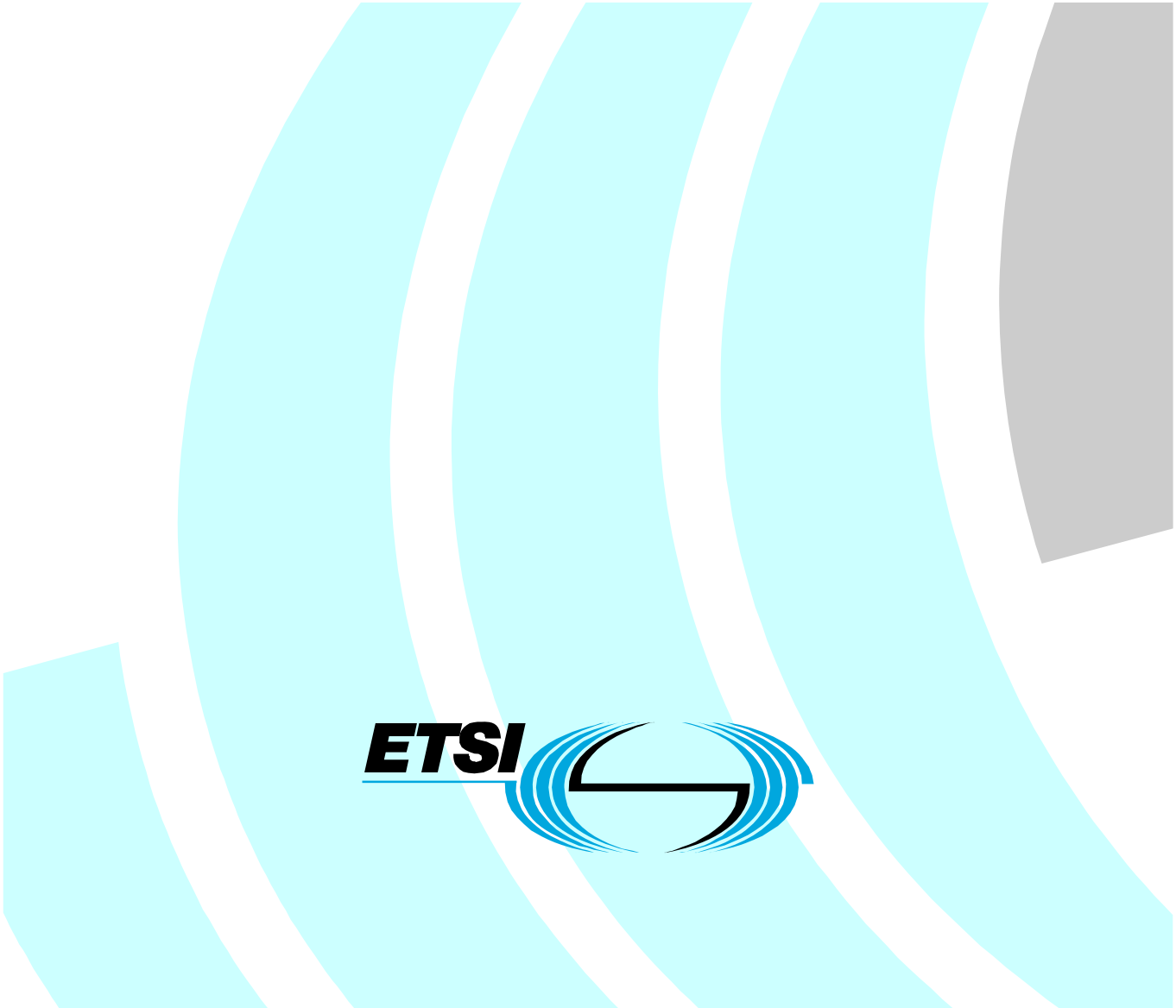
ETSI TR 187 002 V2.1.1 (2008-12)

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-07030-NGN-R2

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

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

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

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

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

2.1 Normative references

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

Not applicable.

2.2 Informative references

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

[i.1] ETSI 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); PSTN/ISDN Emulation Subsystem (PES); NGN Release 1 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); 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 Release 7)".

[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 Release 1".

[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.

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].

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
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
BGF	Border Gateway Function
BTF	Basic Transport Function
CC	Call Control
CD	Compact Disc
CHAP	Challenge Handshake Authentication Protocol
CLF	Connectivity session and repository Location Function
CPE	Customer Premises Equipment
C-RACF	Core-Resource and Admission Control Function
CSCF	Call Session Control Function
DNS	Domain Name System
DNSSEC	DNS SECurity
DoS	Denial-of-Service
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
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
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
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
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
UPSF	User Profile Server Function
VLAN	Virtual Local Area Network
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network

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).

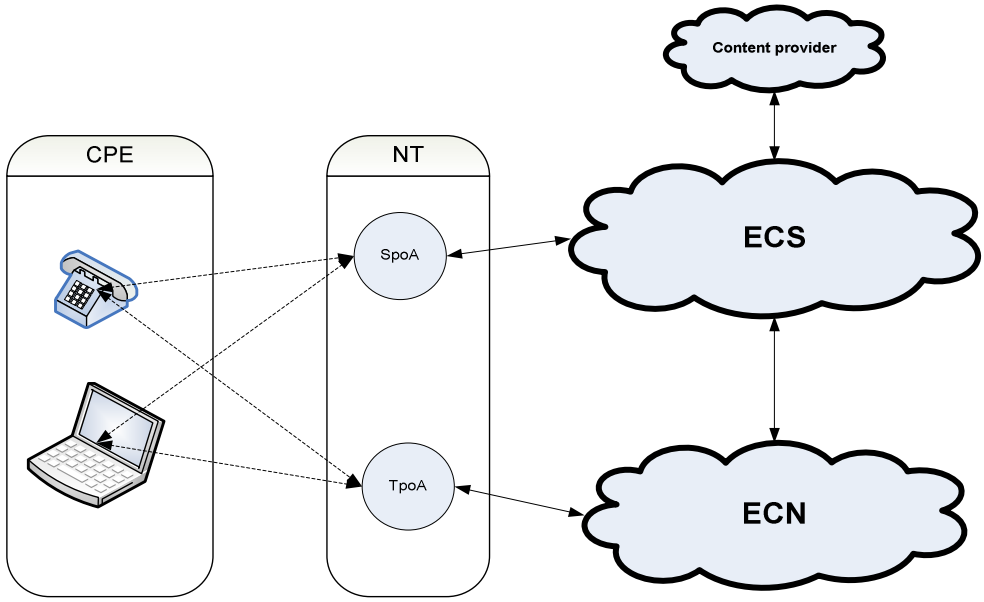


Figure 1: Basic ECN&S model for the NGN

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.

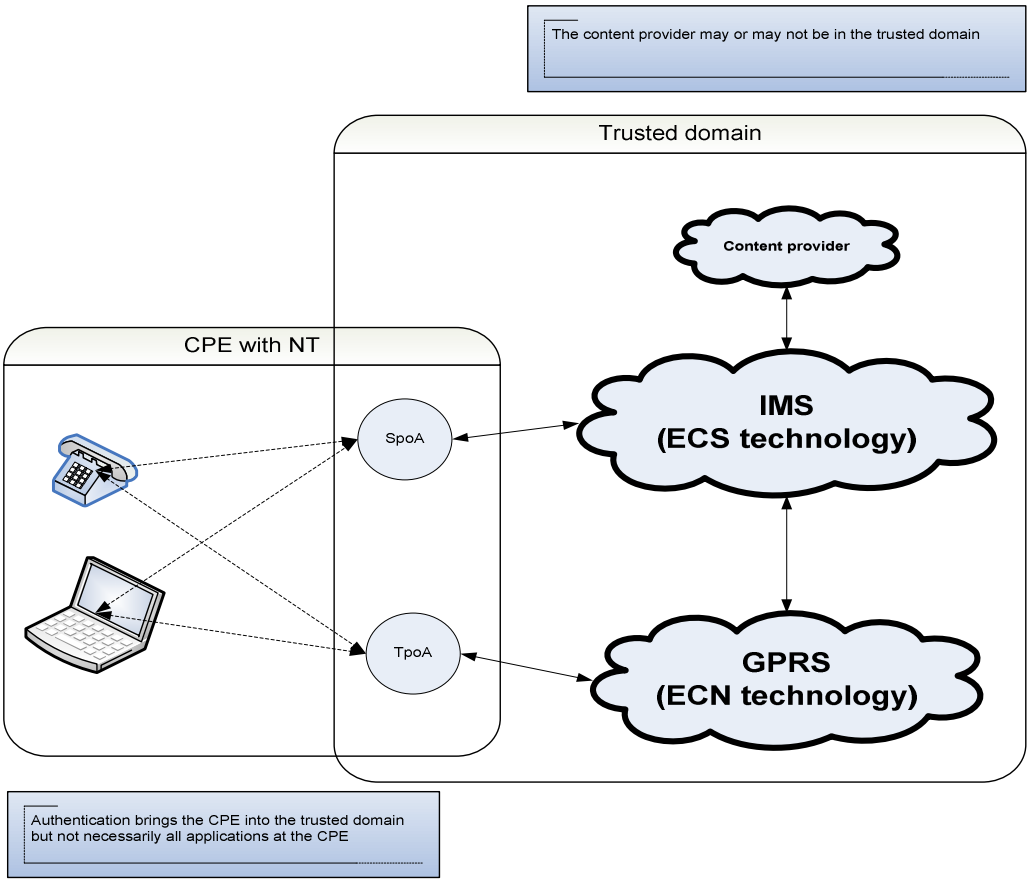


Figure 2: Simplified view of 3GPP IMS domains mapped to ECNS

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

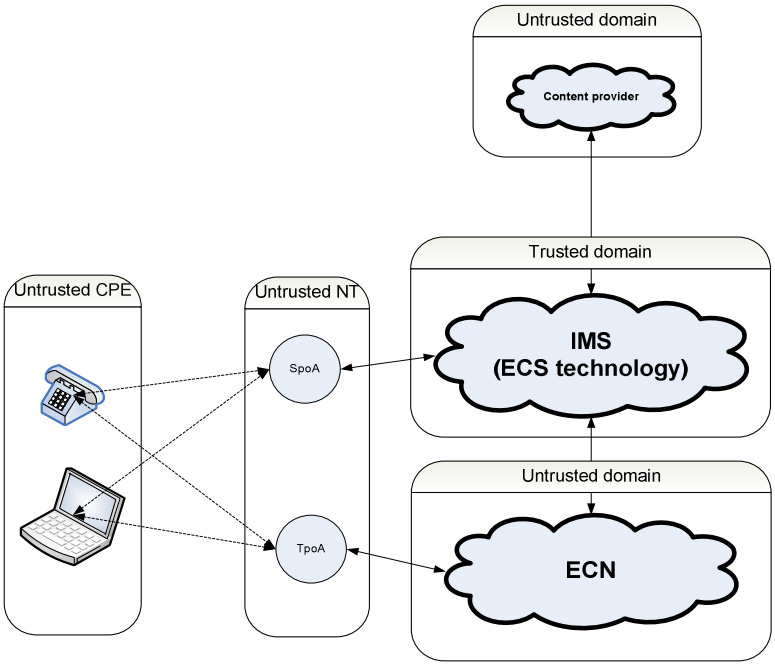


Figure 3: view of IMS where IMS is trusted

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

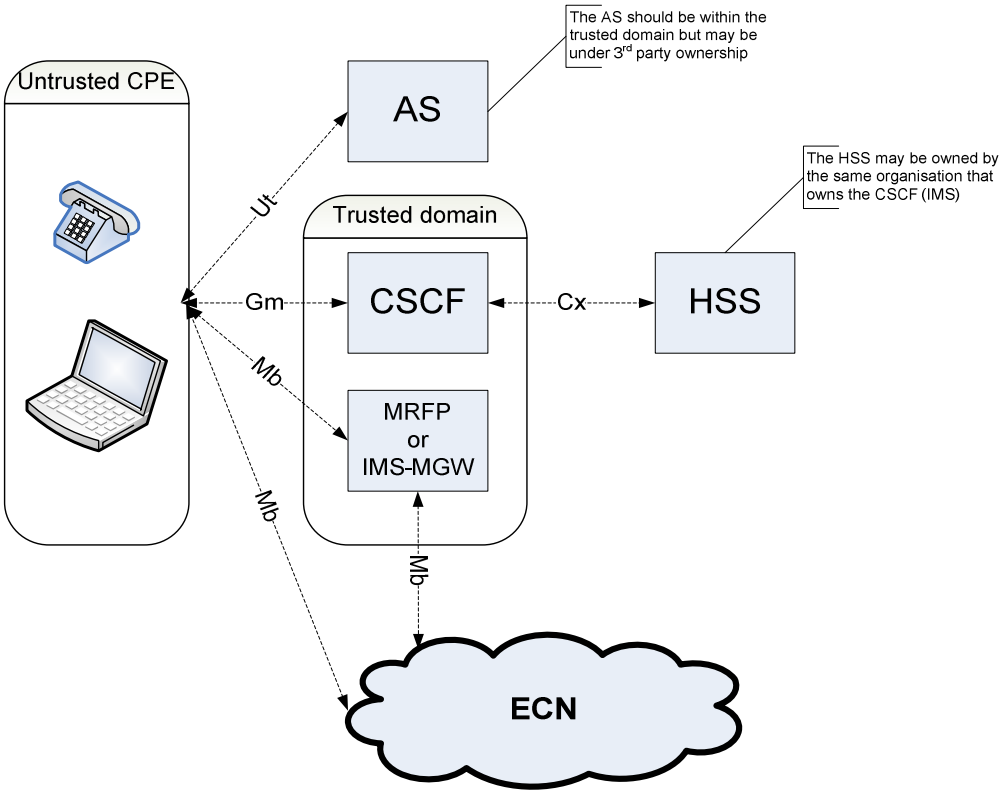


Figure 4: Open interfaces in the IMS model for NGN

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

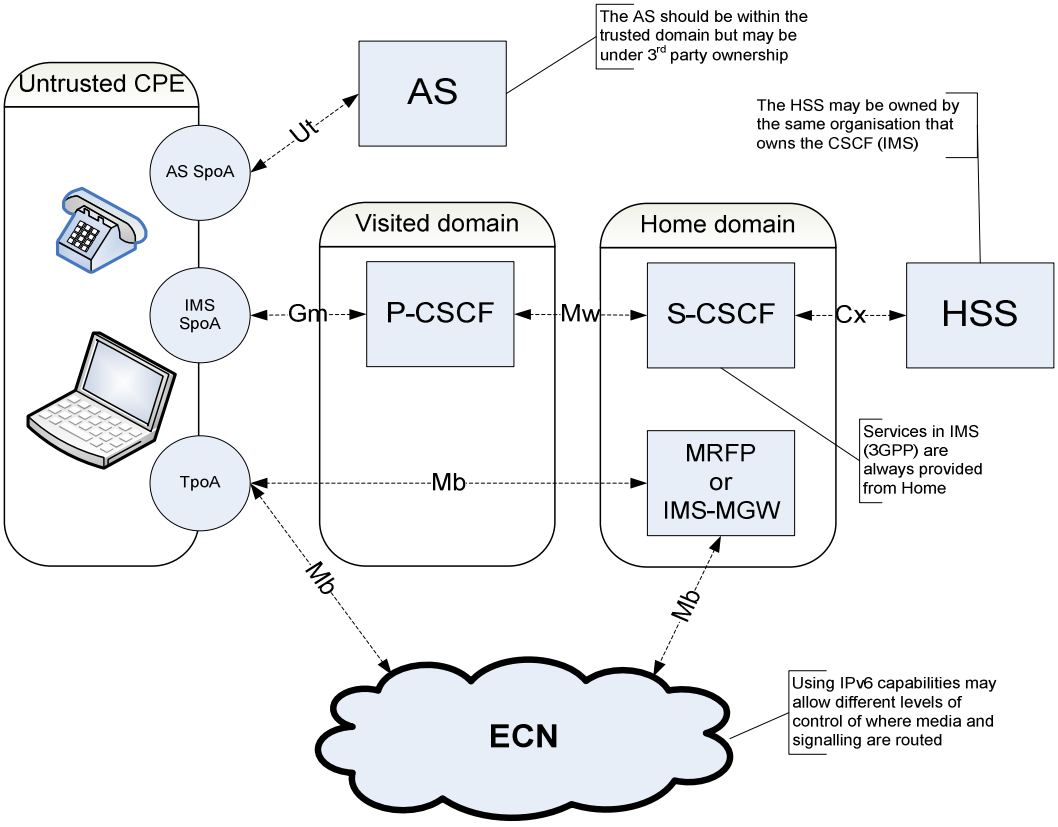


Figure 5: Roaming scenario

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.

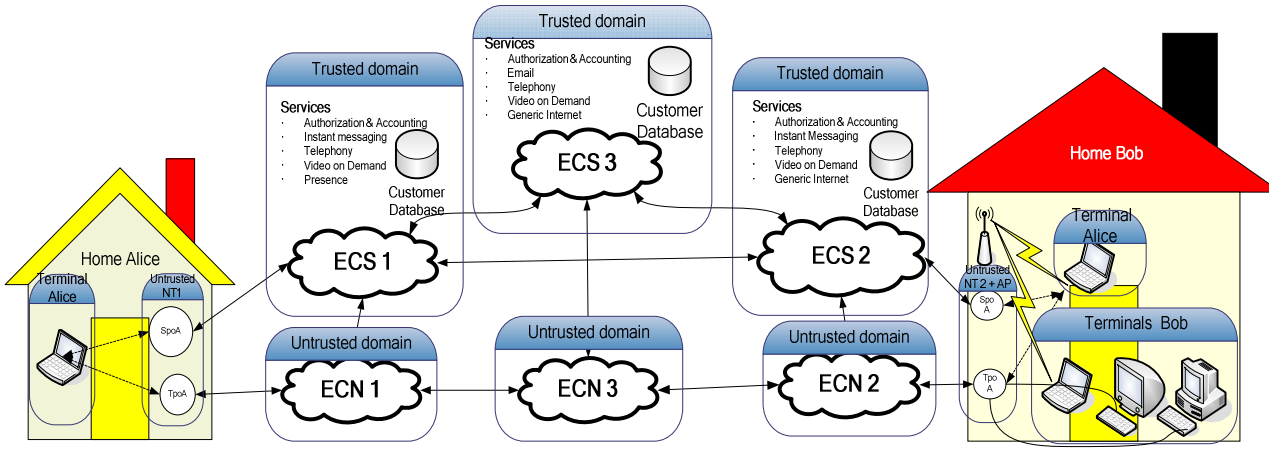


Figure 6: Nomadic user security scenario

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 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 [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.

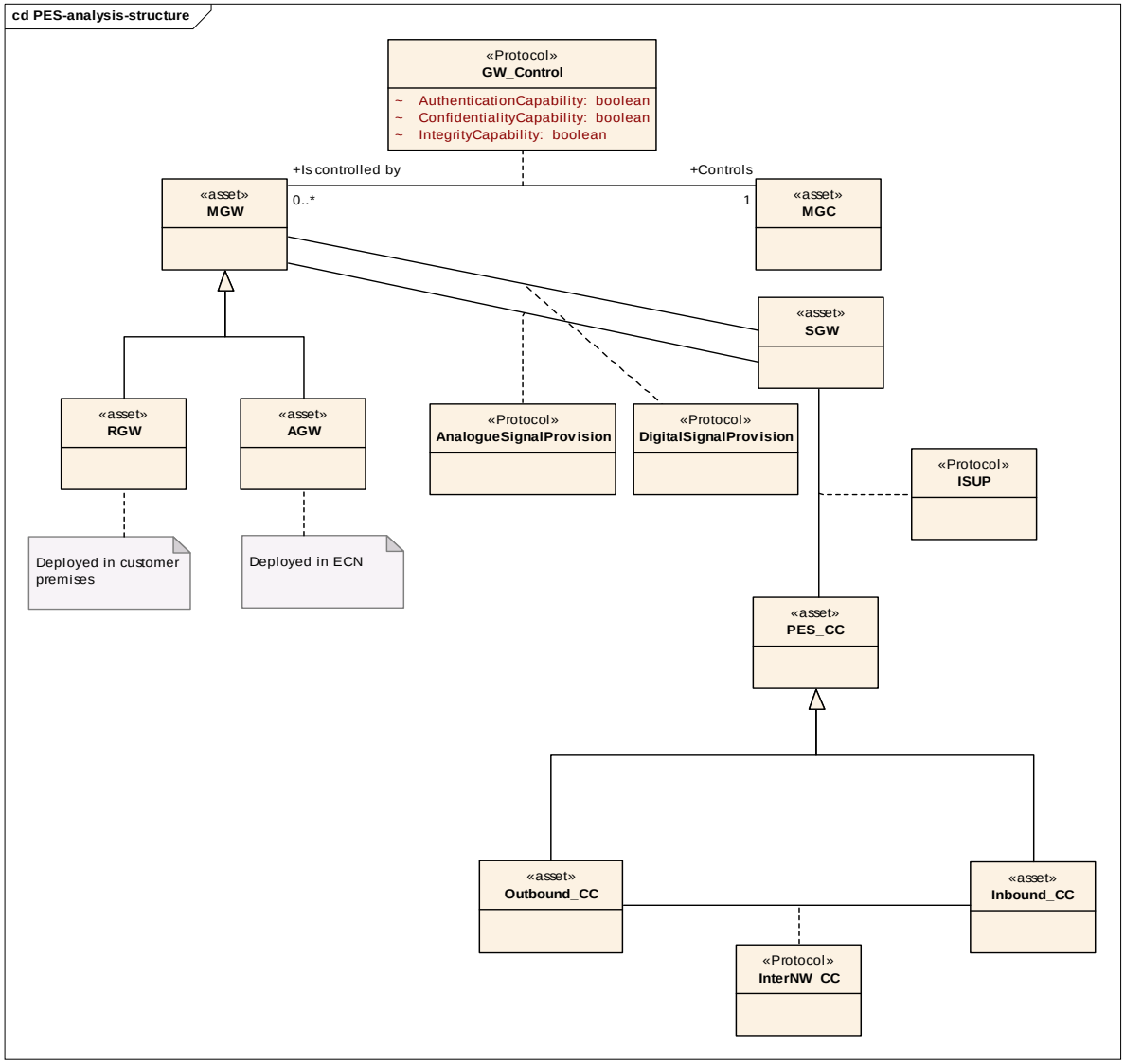


Figure 7: UML class diagram for PES

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 11 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.

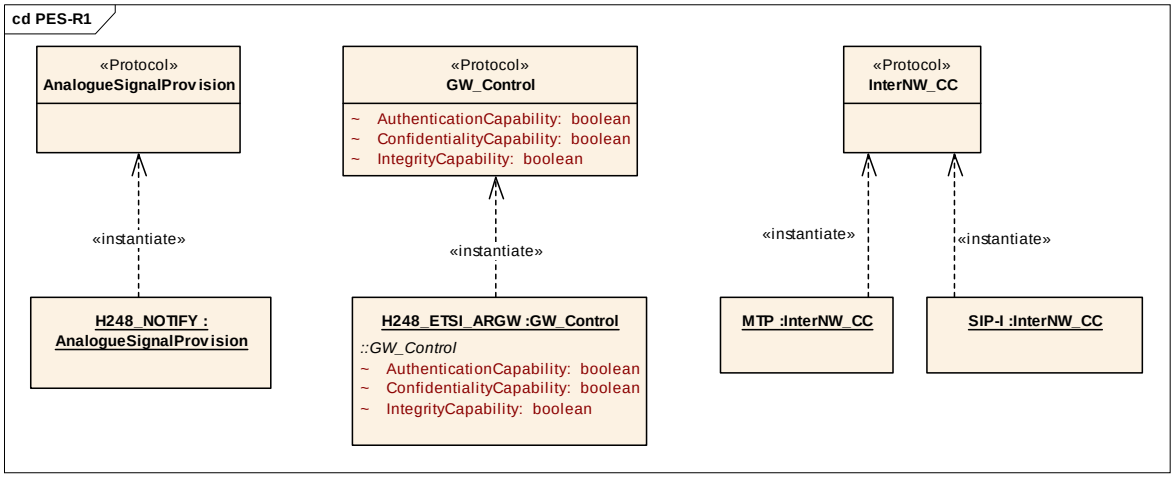


Figure 8: Instances of the PES protocols

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.

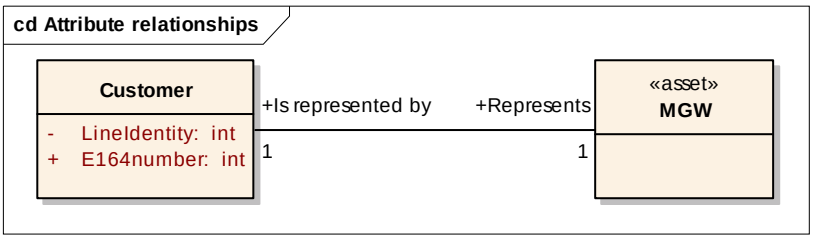


Figure 9: UML representation of customer to MGW relationship

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].

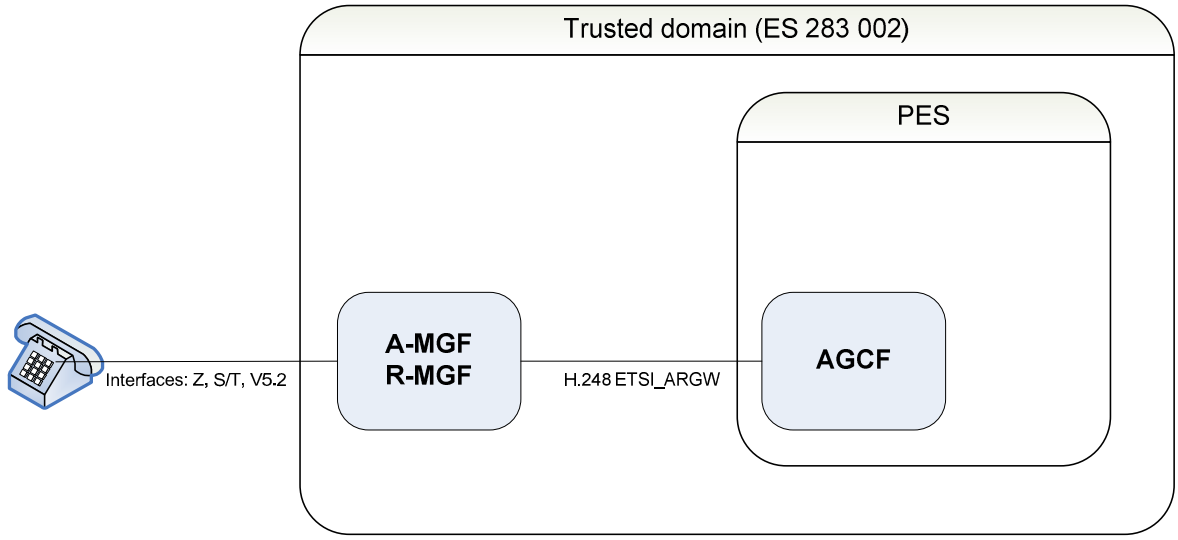


Figure 10: H.248 deployment model as specified in ES 282 002

As shown in figure 13, 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

This clause is for FFS. Currently, only the specific NASS-IMS bundled authentication scenario has been analysed.

5.2.1 NASS-IMS bundled authentication analysis

5.2.1.1 NASS-IMS bundled Authentication objectives and security objectives

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 defined in [3GSecArch] to provide authentication access to IMS.

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.

Table 11: NASS-IMS bundled authentication objectives

Actor (note 1)	Objective
Access Network and IMS services provider (note 2)	To offer access to IMS-based services, including connectivity to a user entitled to use the resources of the NGN and the IMS subsystem
NOTE 1: The end customer is not considered as an actor although he may be considered a stakeholder. NOTE 2: This is a special case of an ECS and ECN under the same ownership.	

5.2.1.2 Stage 2 model of NASS-IMS bundled authentication

An outline model for authentication is given in figure 11 in the form of an UML pattern.

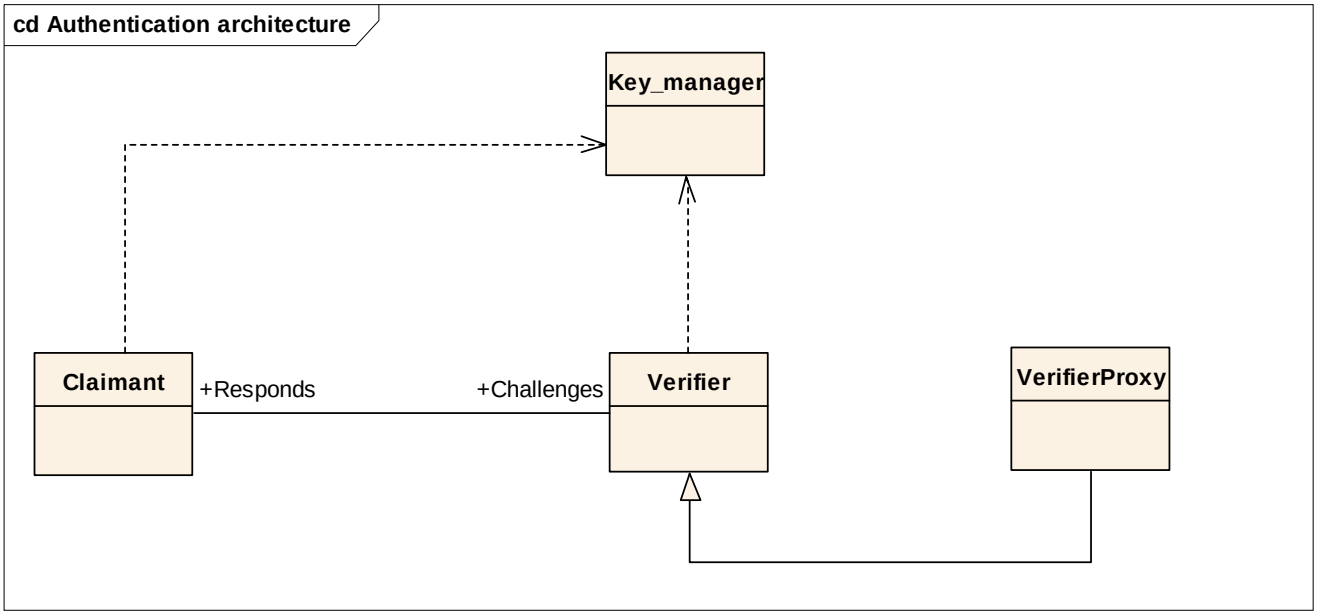


Figure 11: Authentication pattern

In the IMS-NASS bundled authentication the verifier is in NASS and the result of authentication accessed by IMS (i.e. there is no independence of NASS and IMS).

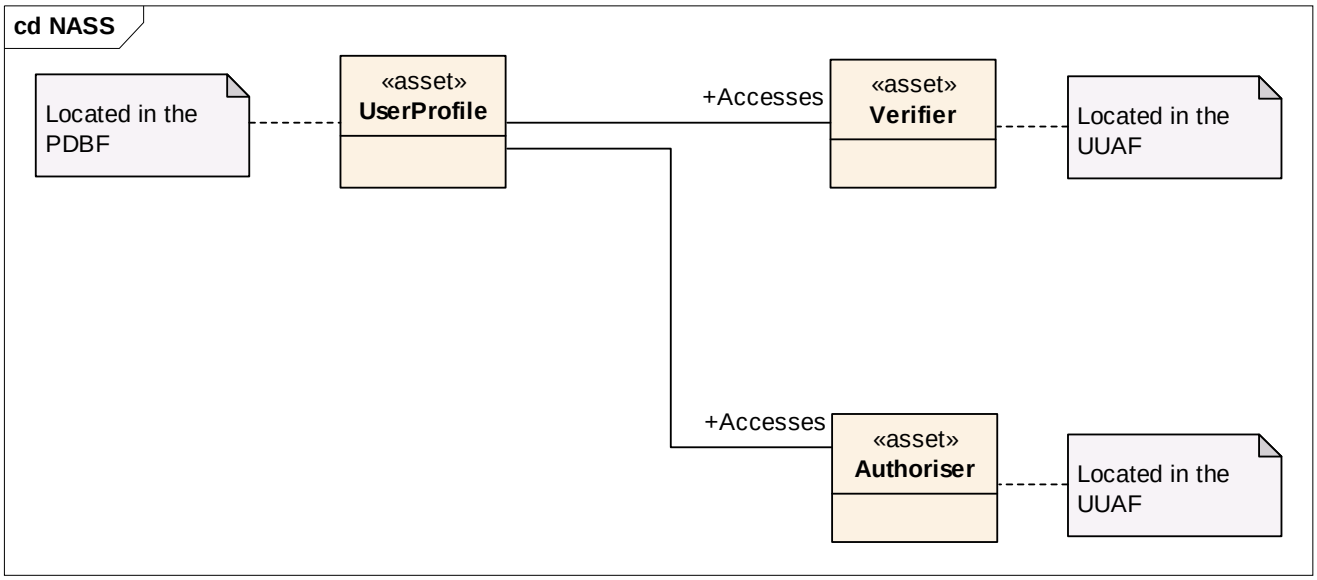


Figure 12: NASS matching to authentication pattern

5.2.1.2.1 Identification of 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 13 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.

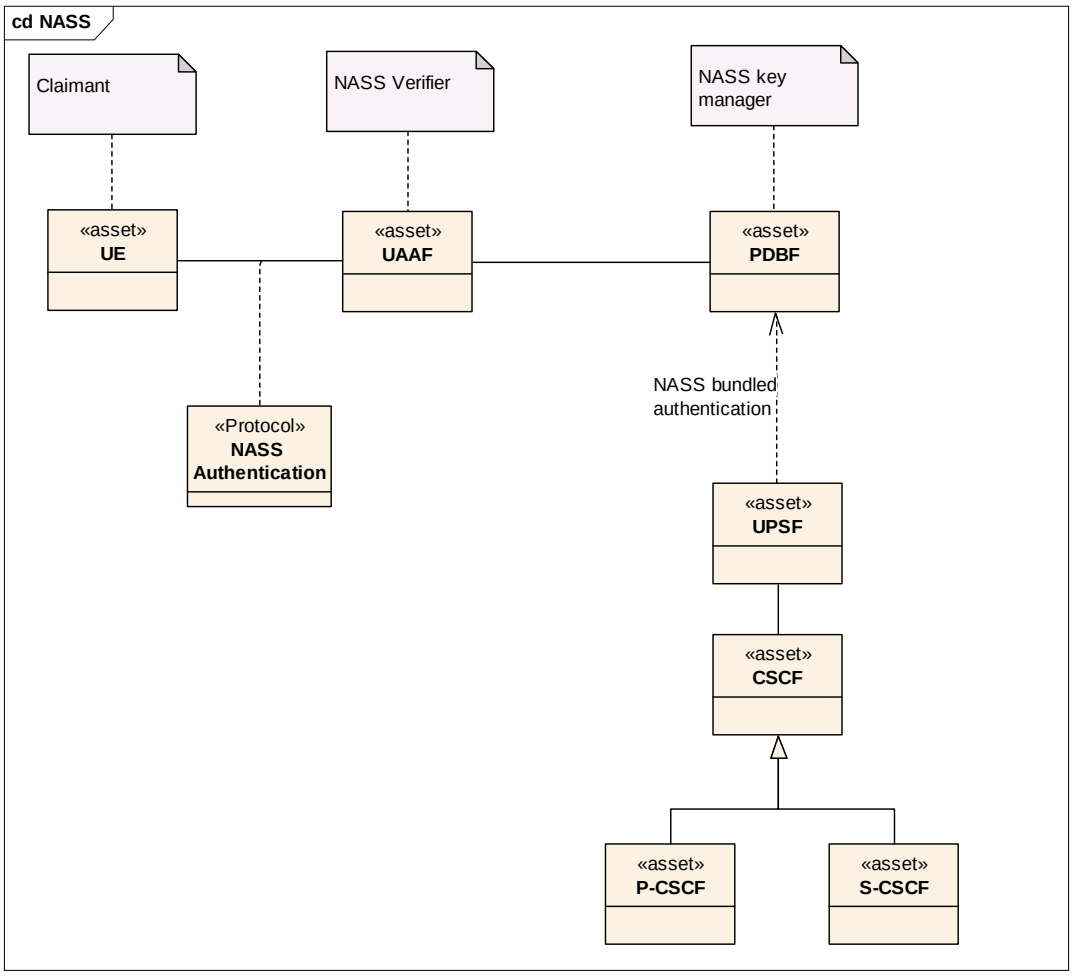


Figure 13: IMS-NASS bundled authentication class diagram model

5.2.1.2.2 Missing considerations in NASS

5.2.1.2.2.1 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 11 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.

5.2.1.2.2.2 Cardinality of relationships

The cardinality of relationships between objects in NASS is not clear.

5.2.1.2.2.3 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 clause 5.2.1.4.7.

NOTE: This vulnerability can be mitigated either with configuration-based or protocol-based support. The work for counter measure is being jointly developed by TISPAN and 3GPP and is documented in 3GPP TR 33.803 [i.33].

5.2.1.3 Points of attack on the NASS-IMS bundled authentication

5.2.1.3.1 Interfaces

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

NOTE: The secondary point of attack is the authentication protocols.

Table 12: Interfaces and their characteristics

Communication paths	Characteristics	Attributes transferred
UE to CLF		EAP/CHAP signalling messages (note)
UE to P-CSCF	IP transfer	REGISTER message Source IP address (UE) 200 OK
P-CSCF to CLF (Internal Interface)	IP transfer	Location Info: Source IP address (in LIQ) Access subscriber (in response)
P-CSCF to I-CSCF (Internal Interface)		REGISTER message 200 OK
I-CSCF to S-CSCF (Internal Interface)		REGISTER message 200 OK
S-CSCF to UPSF (Internal Interface)		MAR MAA
NOTE: Scenario B.		

5.2.1.4 Risk analysis

5.2.1.4.1 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.

5.2.1.4.2 Interception

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

5.2.1.4.2.1 Interception at the customer to ECN/ECS (CLF/ P-CSCF) interface

There are essentially two scenarios to consider:

- Scenario A: Access authentication based on the implicit line authentication.
- Scenario B: Access authentication based on the 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&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 13: T-10: Attack potential for interception at the customer interface, 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 14: T-11: Attack potential for interception at the customer interface, 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

5.2.1.4.2.2 Interception within the access network providers network

For the purposes of attack it is assumed that the access 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 15: T-12: Attack potential for interception at the customer interface (e1 IF)

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

5.2.1.4.3 Manipulation

5.2.1.4.3.1 Manipulation at the customer interface

There are essentially two scenarios to consider:

- Scenario A: Access authentication based on the implicit line authentication.
- Scenario B: Access authentication based on the 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 16: T-13: Attack potential for manipulation at the customer interface, 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 17 documents the attack potential if insufficient radio-link protection is provided.

Table 17: T-14: Attack potential for manipulation at the customer interface, 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 to be 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.

5.2.1.4.3.2 Manipulation within the access network providers network

For the purposes of attack it is assumed that the access 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 18: T-15: Attack potential for manipulation at the customer interface (e1 IF)

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

5.2.1.4.4 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. Now, 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, i.e. 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 only because the attacker will not receive any incoming packets addressed to the IMS identity that he 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, i.e. 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 only because the attacker will not receive any incoming packets addressed to the IMS identity that he is impersonating.

Denial of service: Attacker A can send SIP BYE using the IP address IP_B and the IMS identity (ID_B).

5.2.1.4.4.1 Risk assessment

Table 19 can be used as basis for risk assessment.

Table 19: T-16: Risk assessment for IP Spoofing

1	Likelihood of occurrence	Likely (2)
2	Impact	High (2)
3	Risk	Critical (4)
4	Time to mount the attack	≤1 day (0)
5	Expertise	Layman (0)
6	Knowledge of TOE	Public (0)
7	Access to launch the attack	Easy (1)
8	Equipment	Standard (0)
	Total risk value =	No rating (1) (Likely)

5.2.1.4.4.2 Recommended countermeasure

The attacks using forged IP address are relevant to the Transfer Functions. To prevent IP spoofing, the BGF [i.17], specifically the RECF, not allow a UE to successfully transmit an IP packet with a source IP address that is different to the one assigned during the network attachment. In other words, the BGF prevent "source IP spoofing". If IP address spoofing is detected the BGF 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 (at least in Release 1), they need to be collocated.

5.2.1.4.5 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; a reasonable assumption would be one minute. As long as the impersonation lasts, the attacker can do everything the true user is entitled to in IMS.

In order to mount such an attack, the legitimate user lose IP connectivity without prior deregistration from IMS. Then the attacker obtain the same IP address when he accesses the core network (or, given the assigned IP address, he know the IMPU of the prior owner of this IP address, and this user still be registered for IMS). In all, this threat scenario is not very likely.

5.2.1.4.5.1 Risk assessment

Table 20 can be used as basis for risk assessment.

Table 20: T-17: Risk assessment for Invalidation of IP address not signalled

1	Likelihood of occurrence	Unlikely (1)
2	Impact	Low (1)
3	Risk	Minor (1)
4	Time to mount the attack	≤1 month (4)
5	Expertise	Layman (0)
6	Knowledge of TOE	Public (0)
7	Access to launch the attack	Difficult (12)
8	Equipment	Standard (0)
	Total risk value =	High (16) (Unlikely)

5.2.1.4.5.2 Recommended countermeasure

1) The IP address invalidation should be signalled to the IMS.

2) The access network should guarantee that an IP address that has become invalid will not be re-assigned for a certain amount of time.

5.2.1.4.6 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 the implicit line authentication.
- Scenario B: Access authentication based on the explicit authentication mechanism such as CHAP or EAP.

Attacks can be distinguished between those that combine a DoS attack with the spoofing of source IP addresses to confuse the target, and those attacks that do not modify the source IP address of the attack packets. In the first case, the source IP address filtering countermeasures in the access network allow to discard the spoofed packets. In the case the source IP address of the attack packets is not modified, the user equipment has most probably been compromised by being connected to a compromised domain, having downloaded compromised software, or having installed compromised software passed along on physical means (CD/DVD-ROM). The compromised user equipment can be an isolated case or be part of a larger scheme (synchronized attack in large numbers).

In this scenario, even if the compromised terminal contains an ISIM on a UICC, the user could be unaware of the problem, type in his PIN code, and consequently the ISIM/UICC validly authenticating with the network.

This example scenario is simply to illustrate the fact that the protection against DoS attacks (e.g. against the IMS domain), cannot be prevented by authentication procedures but be performed by DoS prevention mechanisms within the target domains (e.g. IMS domain). These countermeasures be applied to any flow, irrespective of whether they have been validly authenticated or not.

In that respect, the scenarios A and B do not increase the risk of DoS attack as compared to scenario C.

Table 21: T-18: Attack potential for manipulation at the customer interface (Denial-of-service)

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

5.2.1.4.7 "line-id poisoning" attack with malicious P-Access-Network-Info

The deployment scenario and steps performed in the attack is described below:

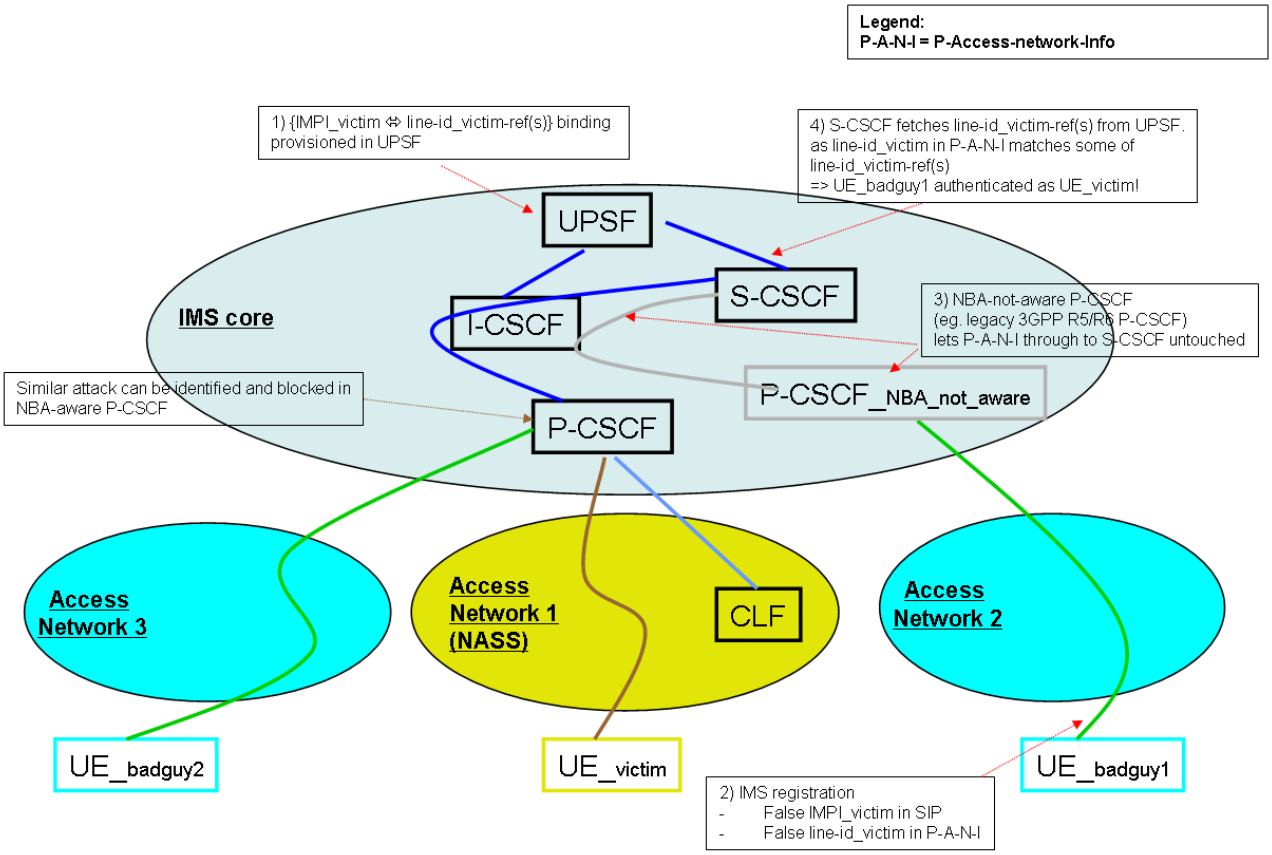


Figure 14: "line-id poisoning" attack scenario

The target of the attack are those networks where both deployed P-CSCFs those are "NBA-aware", i.e. 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.

Steps:

1) The victim (UE_victim) is a 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.

Table 22: T-18: 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

5.2.1.5 NASS-IMS bundled authentication related unwanted incidents

For the NASS-IMS bundled authentication mechanism with the assumptions as stated in clause 5.2.1.1, the threat of a denial of service attack can lead to unwanted incidents of loss of availability of e.g. IMS-based services.

Further threats of interception at the customer to ECN/ECS (CLF/ P-CSCF) interface, and/or interception within the access network providers network can lead to the unwanted incident of loss of confidentiality of signalling messages, in particular authentication data. These threats may also lead to fraudulent access to IMS, e.g. via the air interface.

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 23 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 23 identifies some example security requirements. Table 23 also identifies security countermeasures against the security vulnerabilities.

NOTE: The shown requirements in table 23 are not meant to be complete; TS 187 003 [i.7] may provide more security requirements.

Table 23: 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.

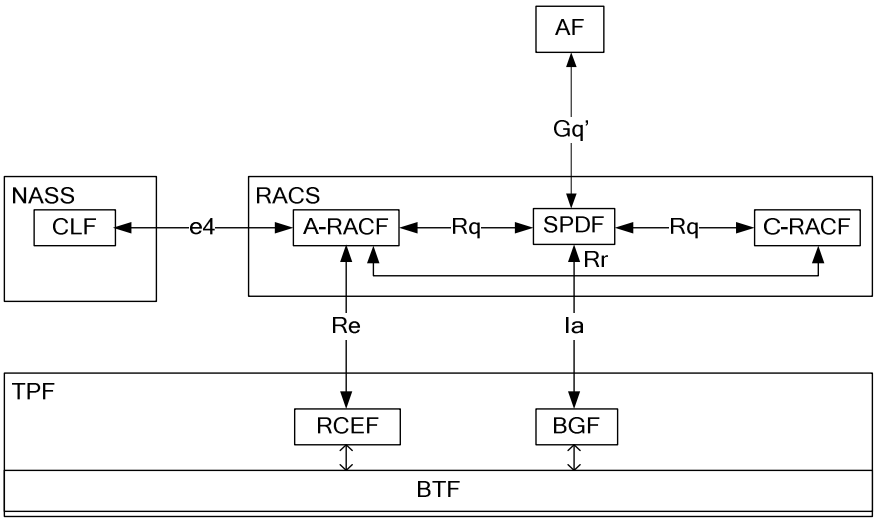
RACS in the NGN offers a suite of procedures and mechanisms to allow:

- 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.

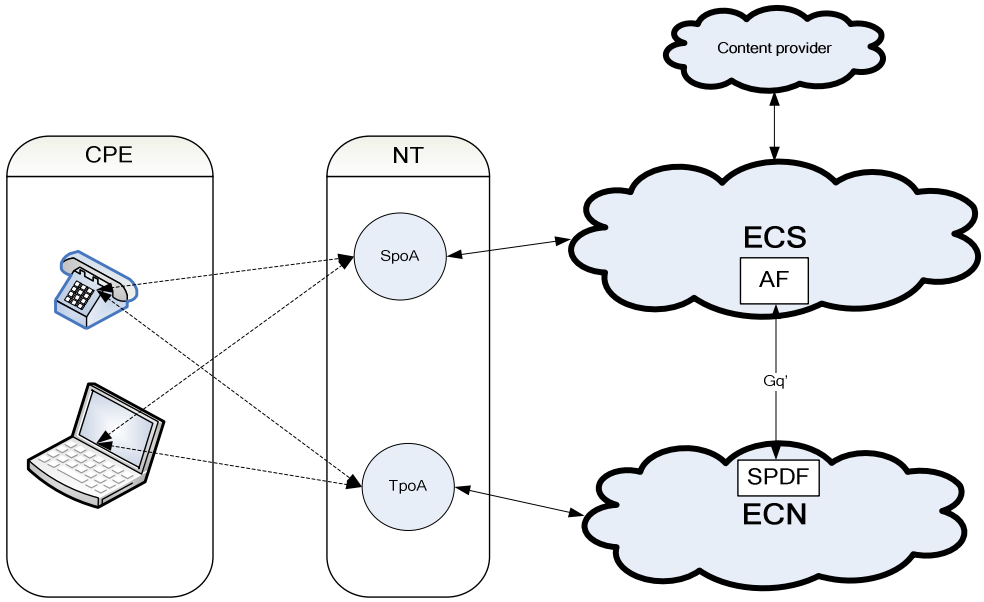
The ToE of RACS are the functional entities Access-Resource and Admission Control Function (A-RACF), Core-Resource and Admission Control Function (C-RACF) and Service Policy Decision Function (SPDF), and the reference points e4, Rr, Re, Rq, Rd', Ri', Gq' and Ia which interconnect them to the ToE environment. 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.

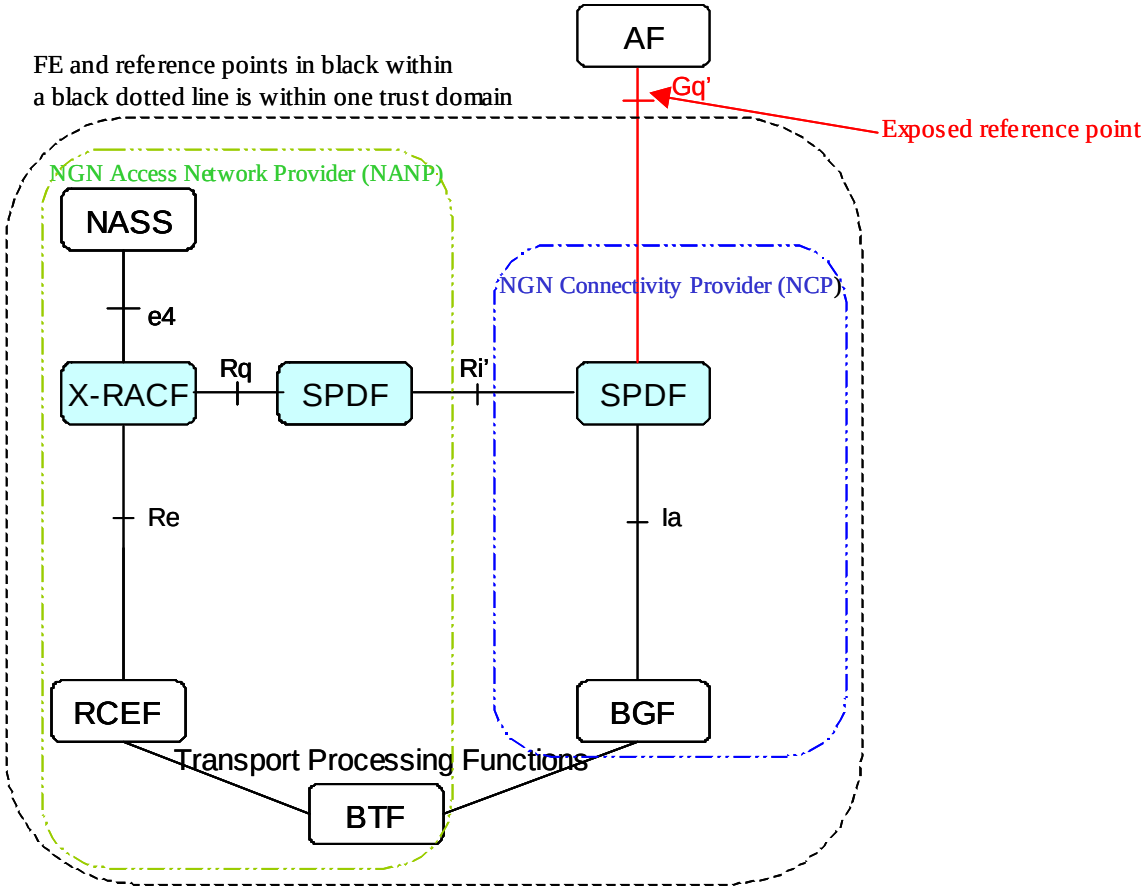


Figure A.3: RACS ToE deployment scenario 1

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'.

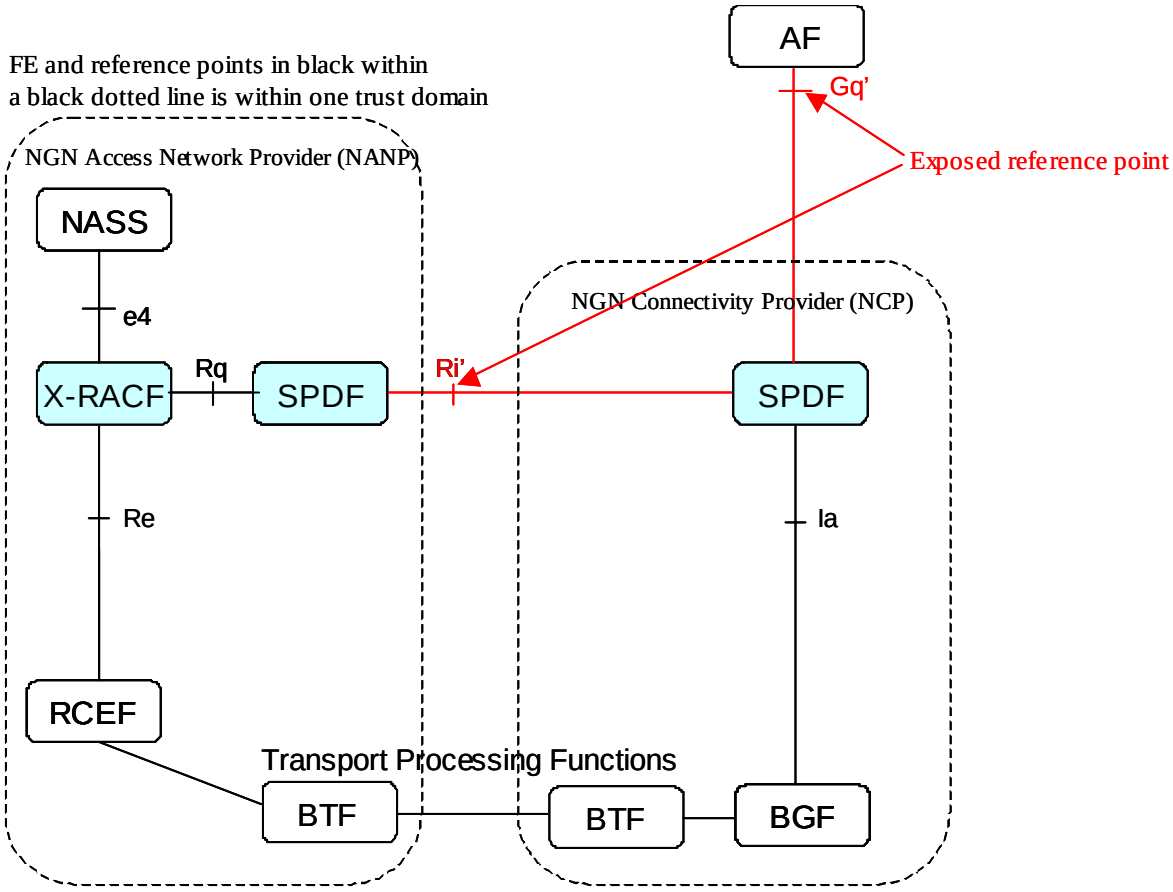


Figure A.4: RACS ToE deployment scenario 2

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'.

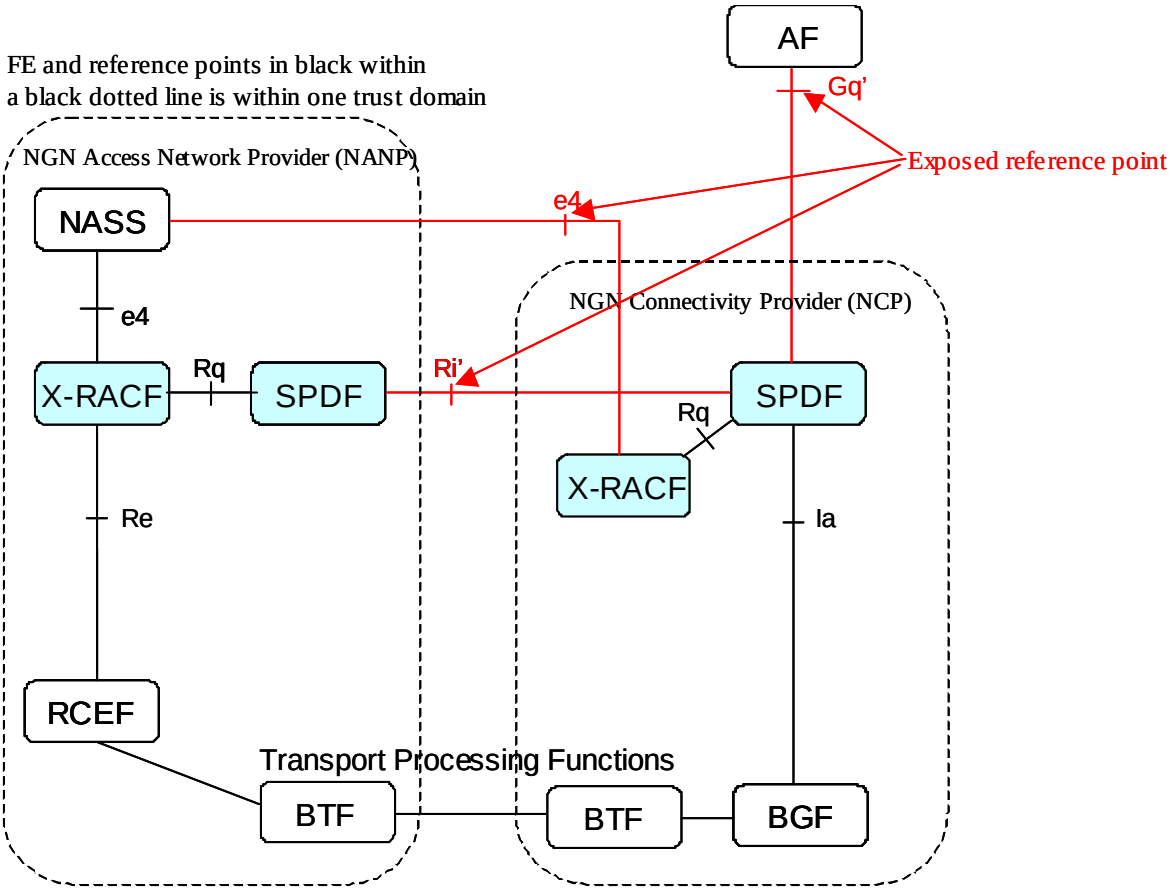
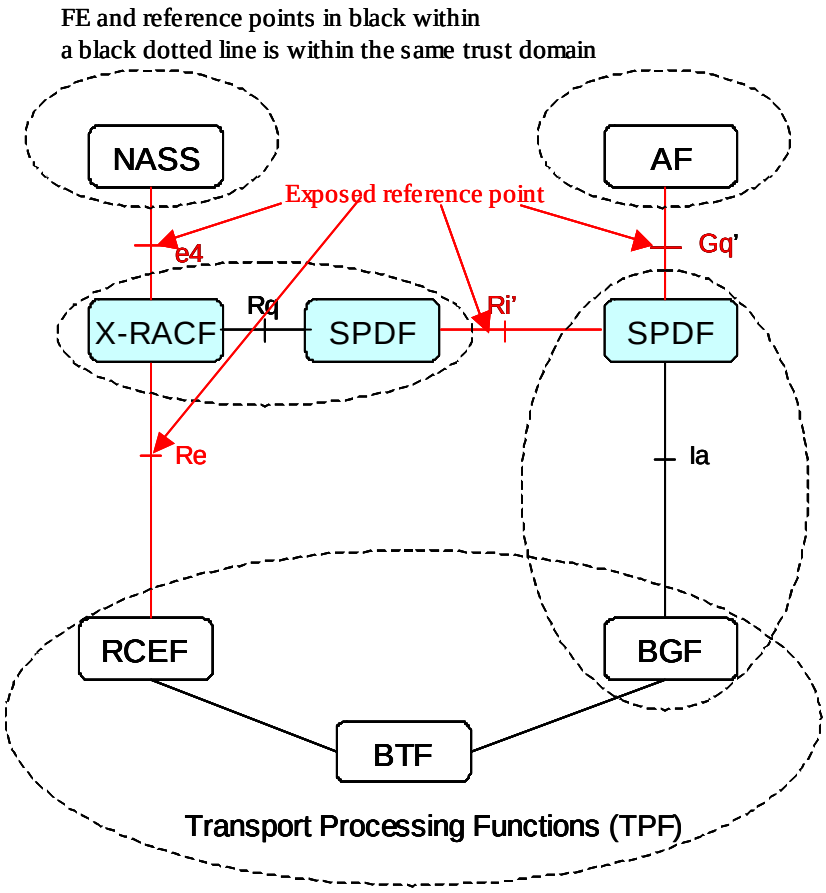


Figure A.5: RACS ToE deployment scenario 3

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.



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

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).

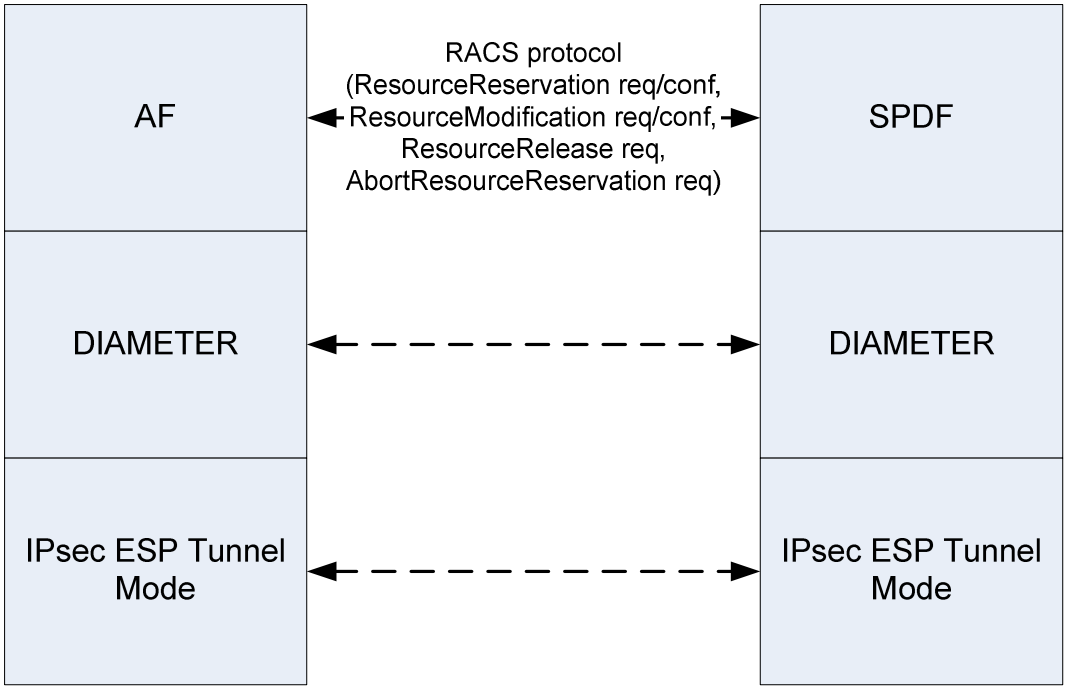


Figure A.7: Protocol stack between AF and SPDF

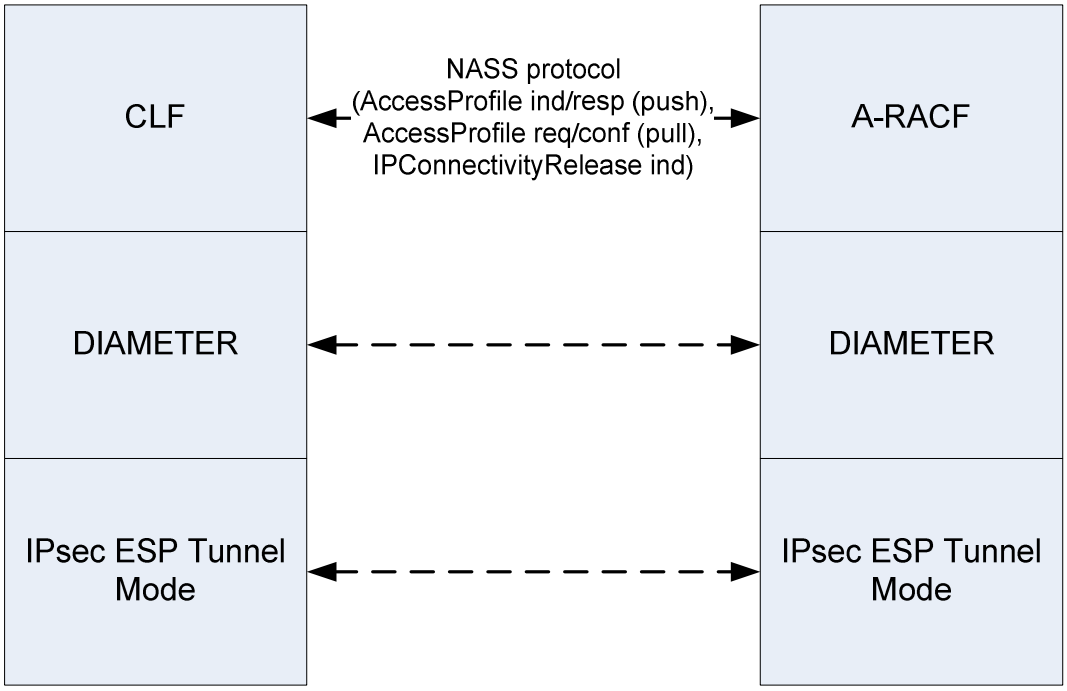


Figure A.8: Protocol stack between CLF and A-RACF

The functional architecture of RACS used in the analysis is that found in draft 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 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.

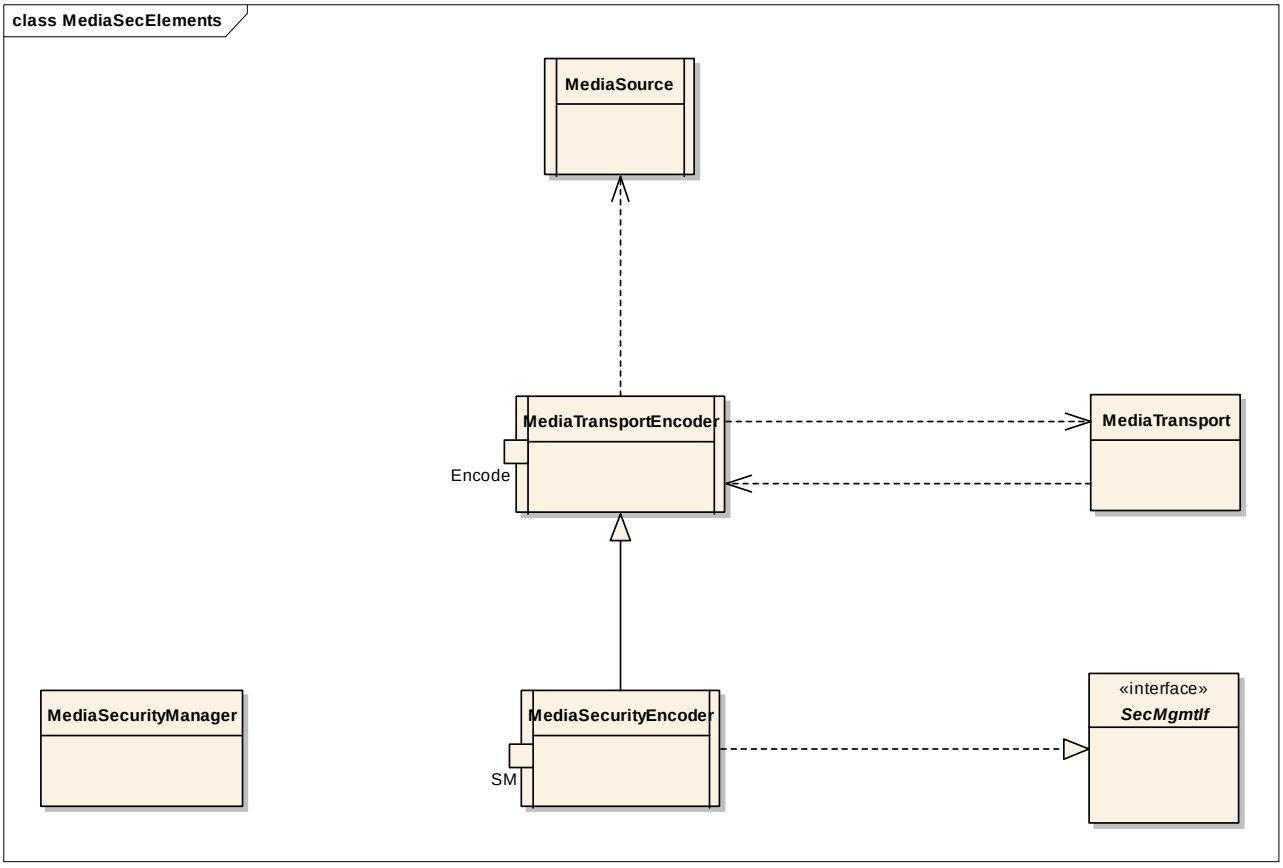


Figure B.1: Abstract model of media security elements (shown as UML classes)

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.

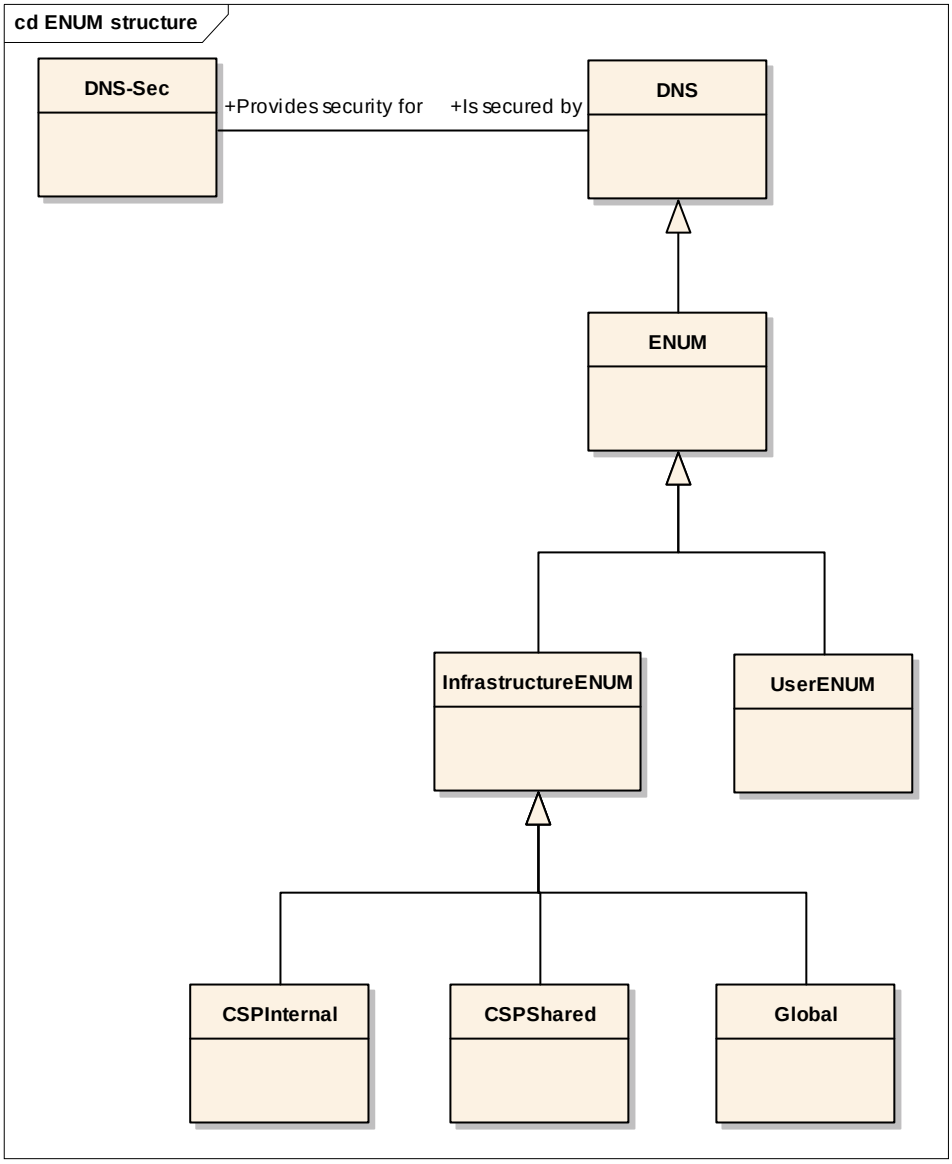


Figure C.1: Hierarchical structure of ENUM showing increasing generalization at top

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.

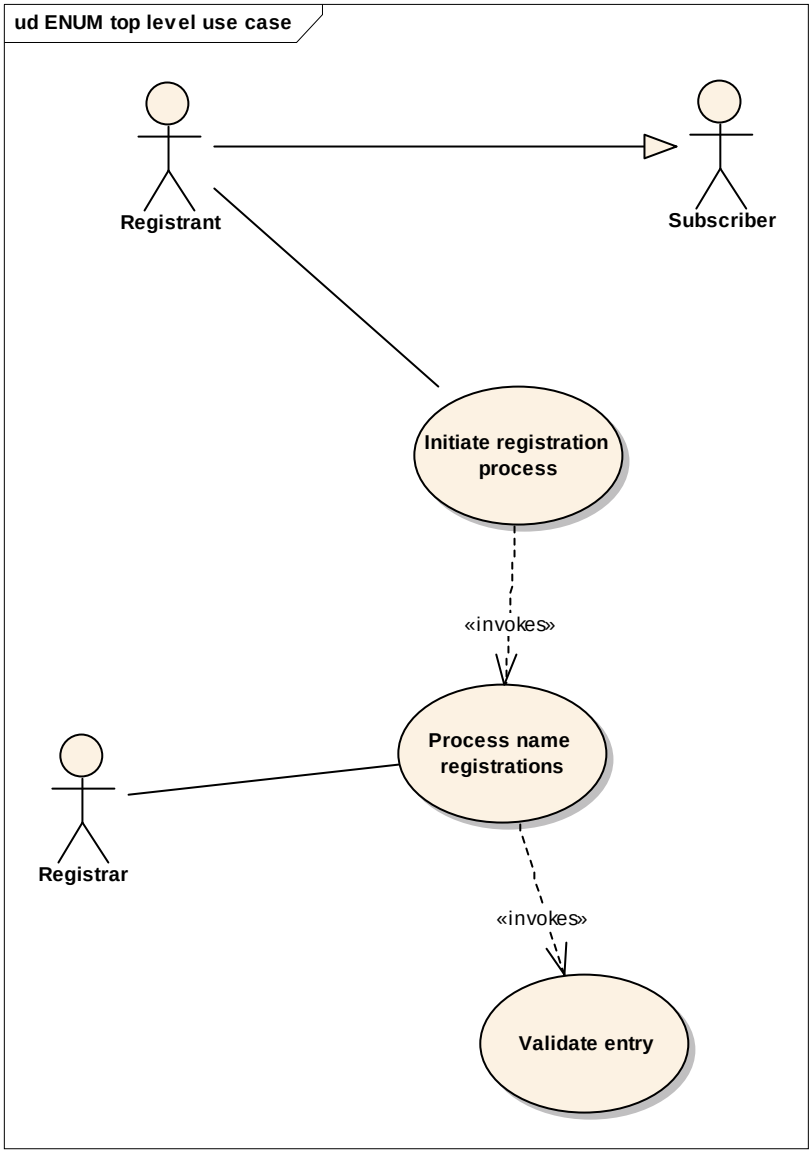


Figure C.2: Main actors and use cases in ENUM

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.

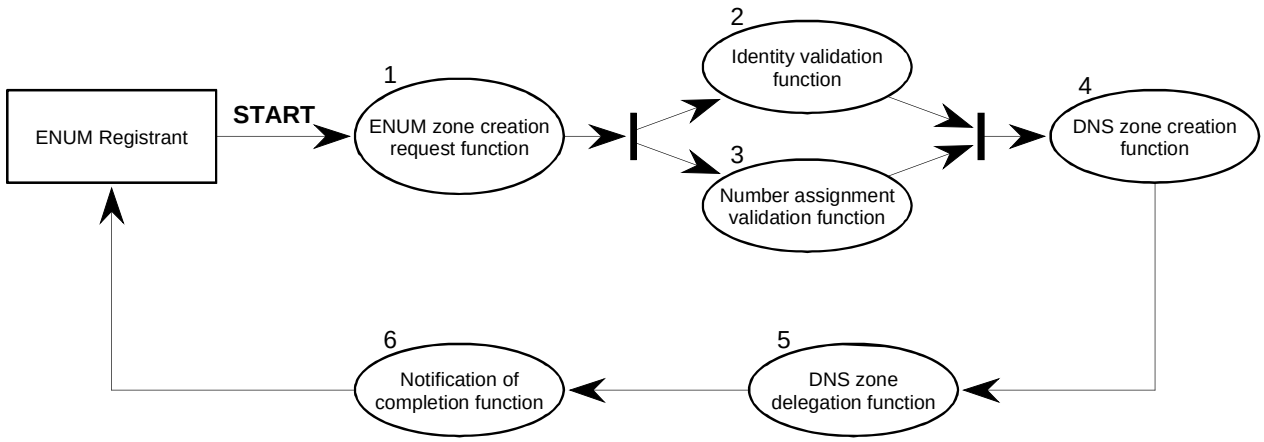


Figure C.3: Functional model for Registration

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).

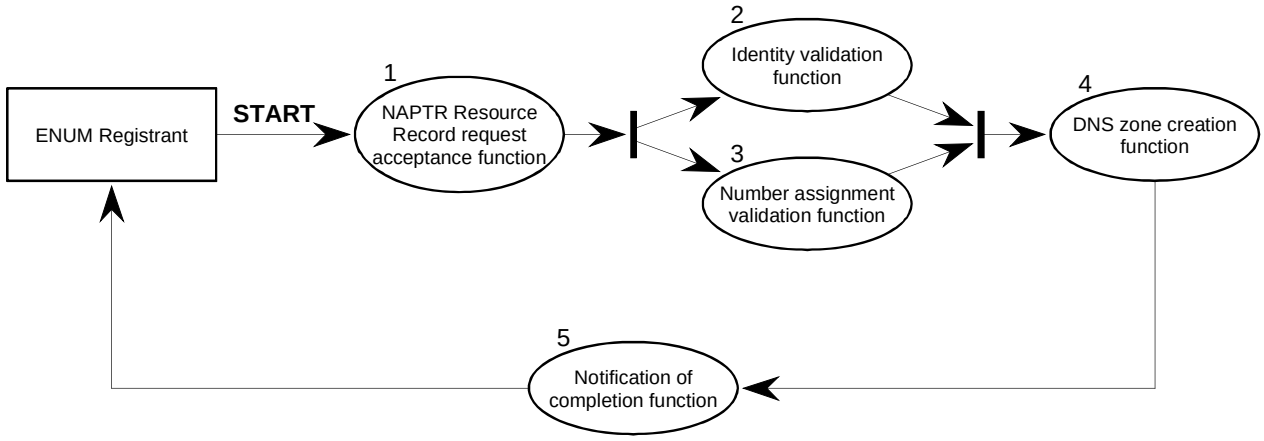


Figure C.4: Functional model for amendment of NAPTR Resource Records in Tier 2 database

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.

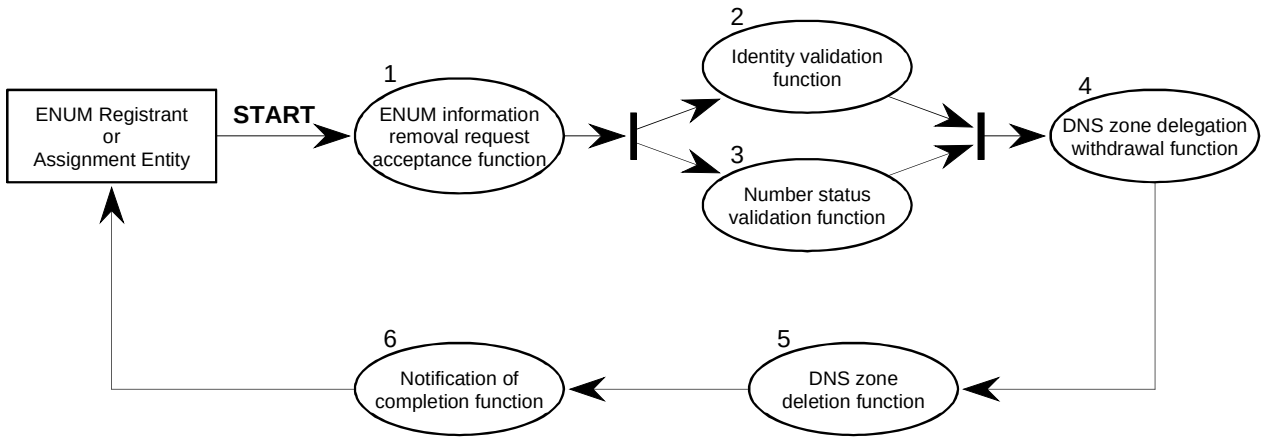


Figure C.5: Functional model for removal of E.164 numbers from ENUM databases

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], [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.

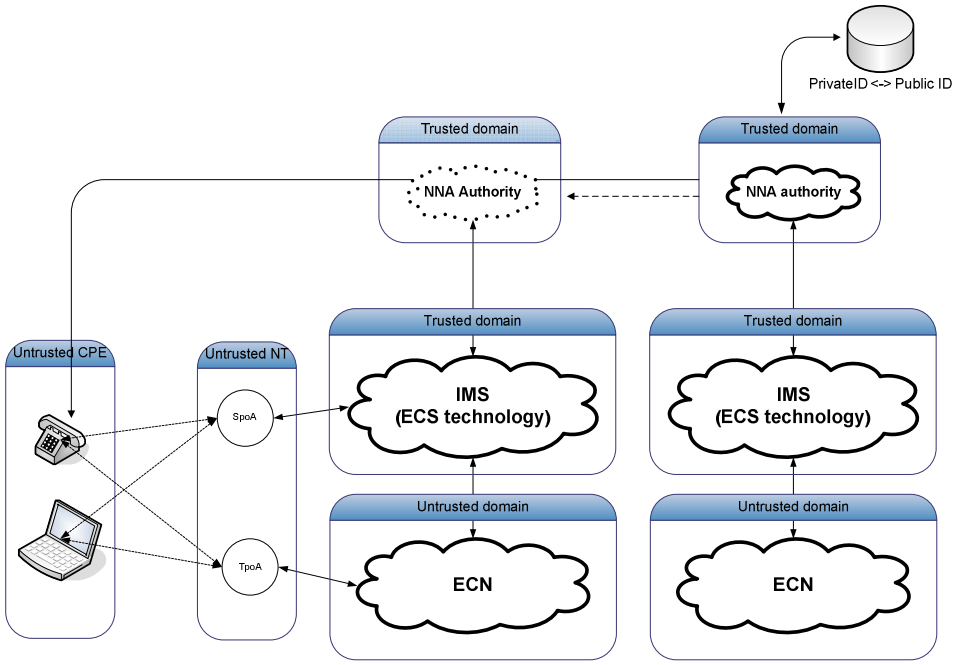


Figure C.6: NNA provisioning scenario

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.

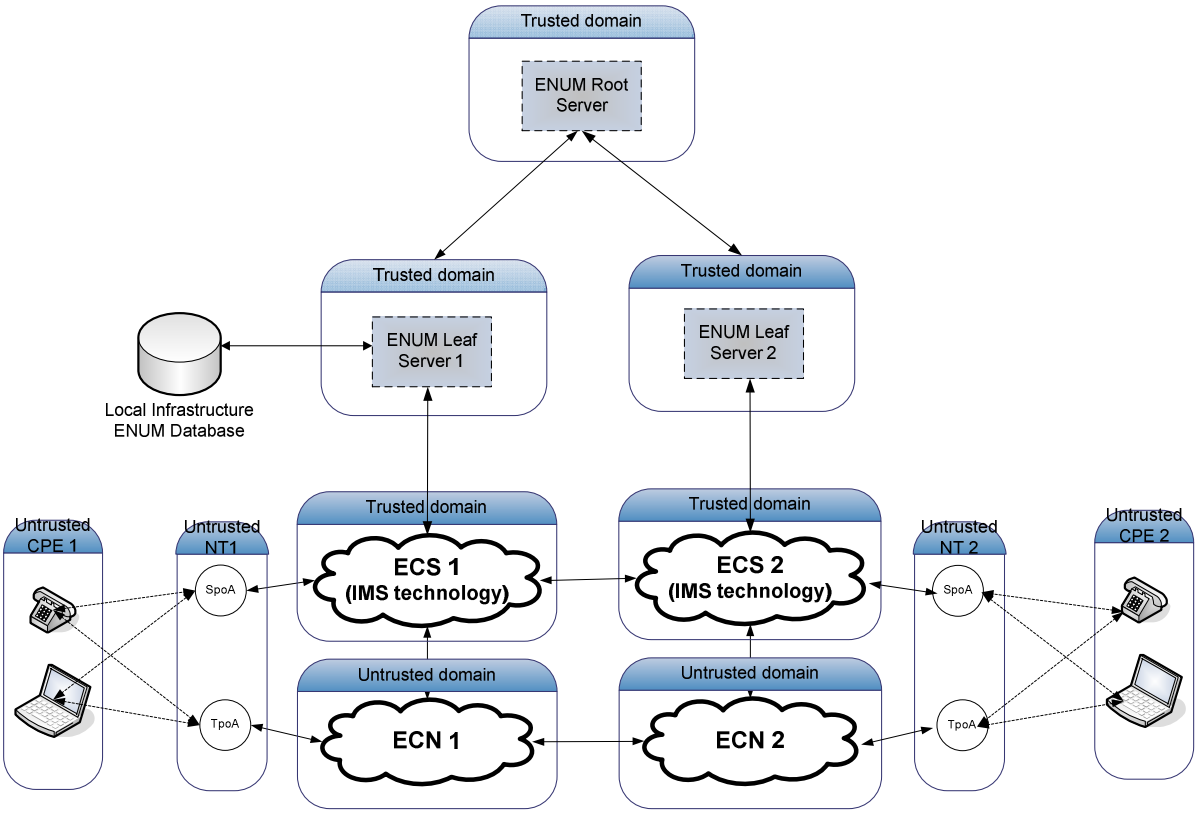


Figure C.7: Signalling scenario

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 [16] 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 [16] 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.

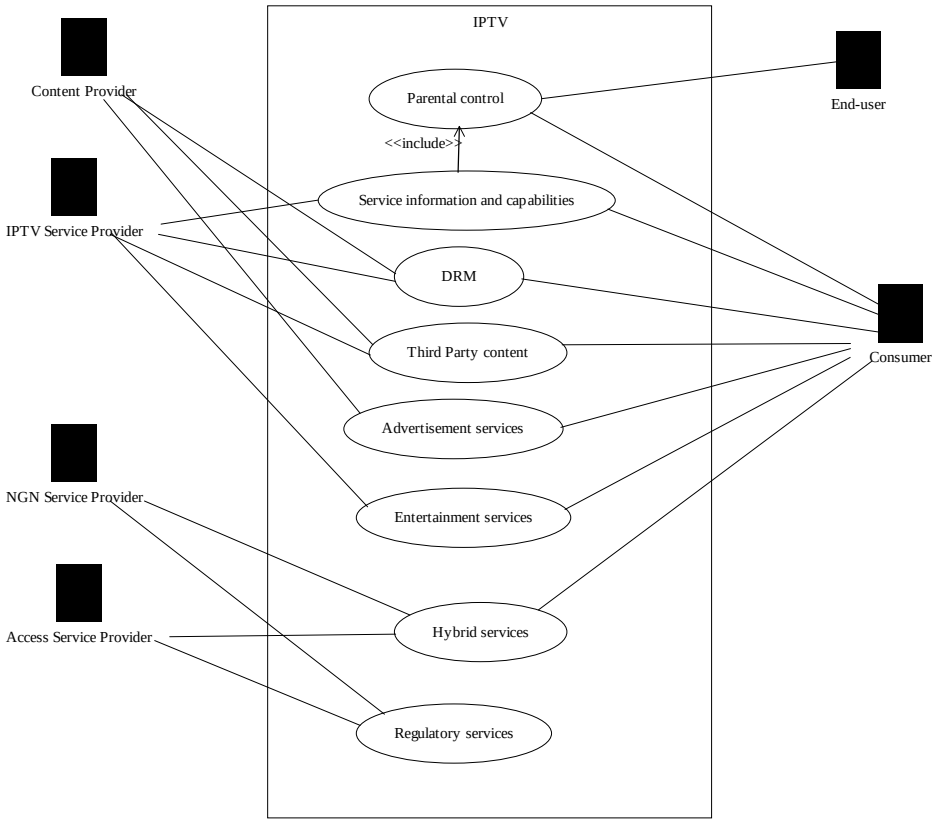


Figure D.1: IPTV stakeholders and main service categories

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.

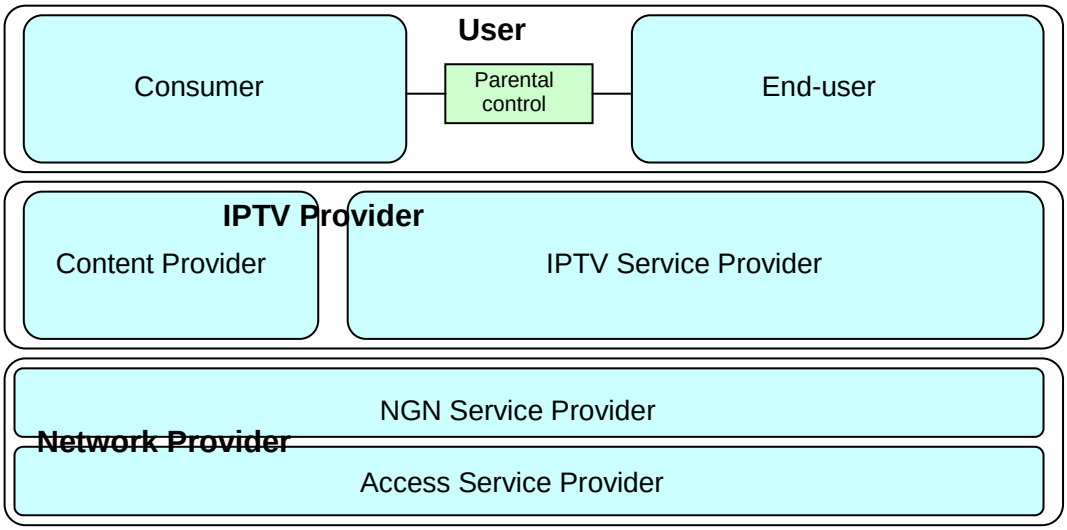


Figure D.2: General IPTV architecture

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.2.2 (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.

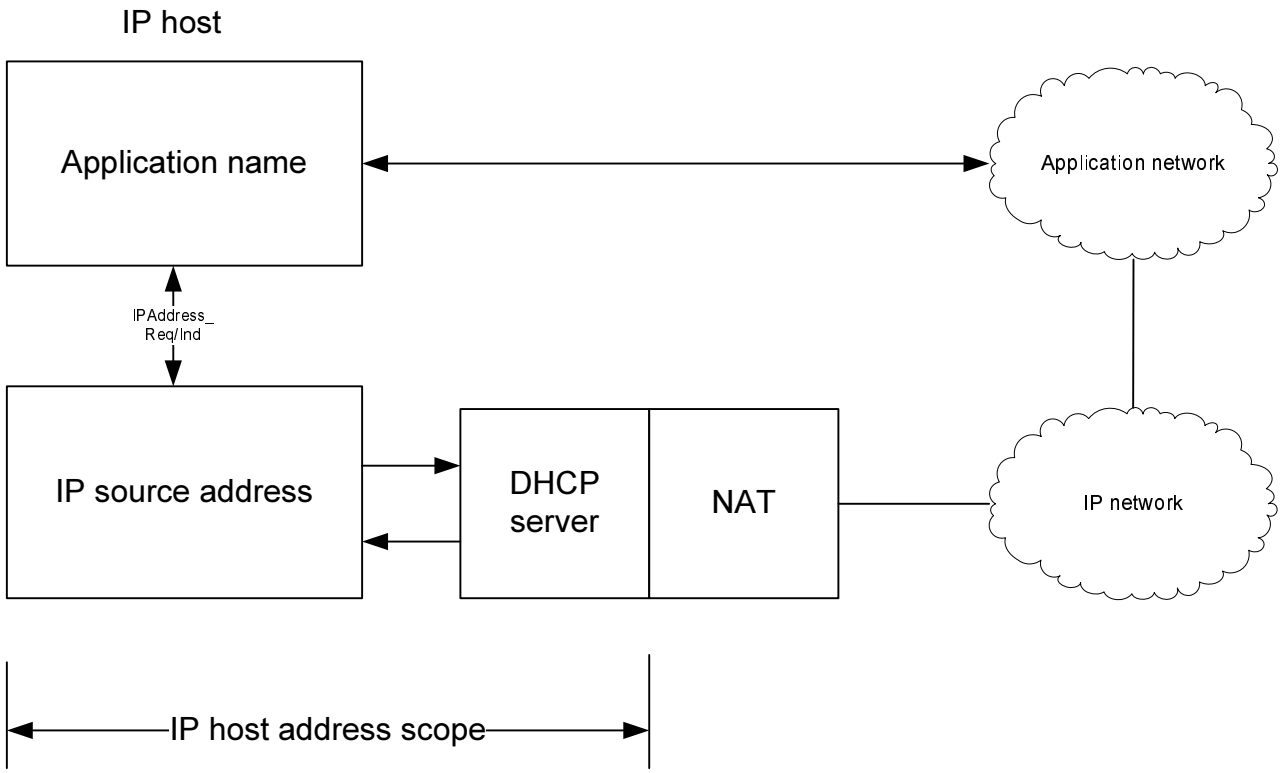


Figure E.1: NAT Traversal problem

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.

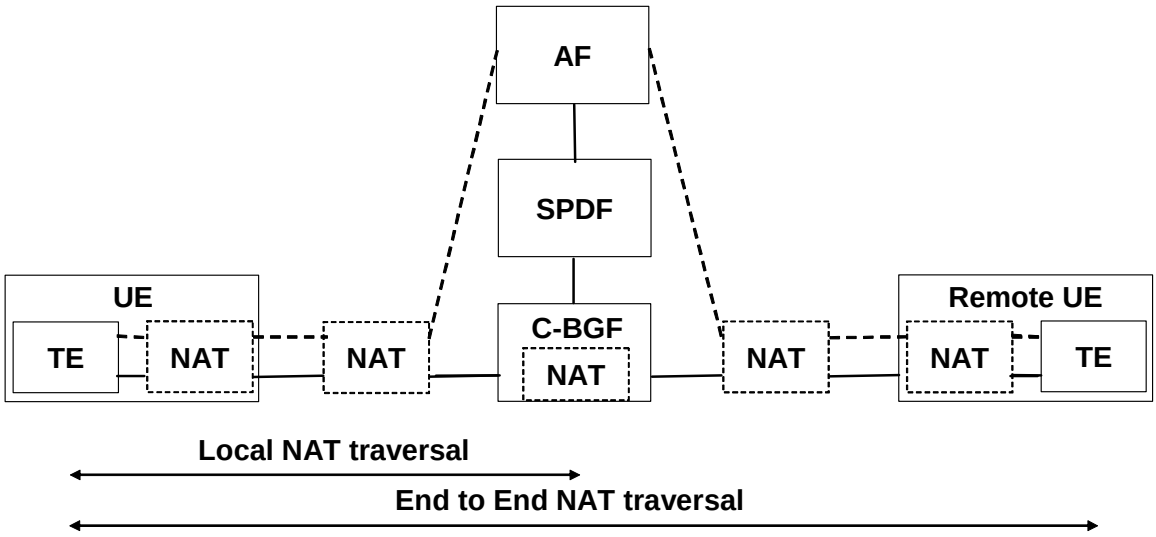


Figure E.2: Reference architecture for NGN R2 NAT

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 WI-07028 is given in the "analysis" column of the table. WI-07028 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.2: 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.3: 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:
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

History

Document history		
V2.1.1	December2008	Publication