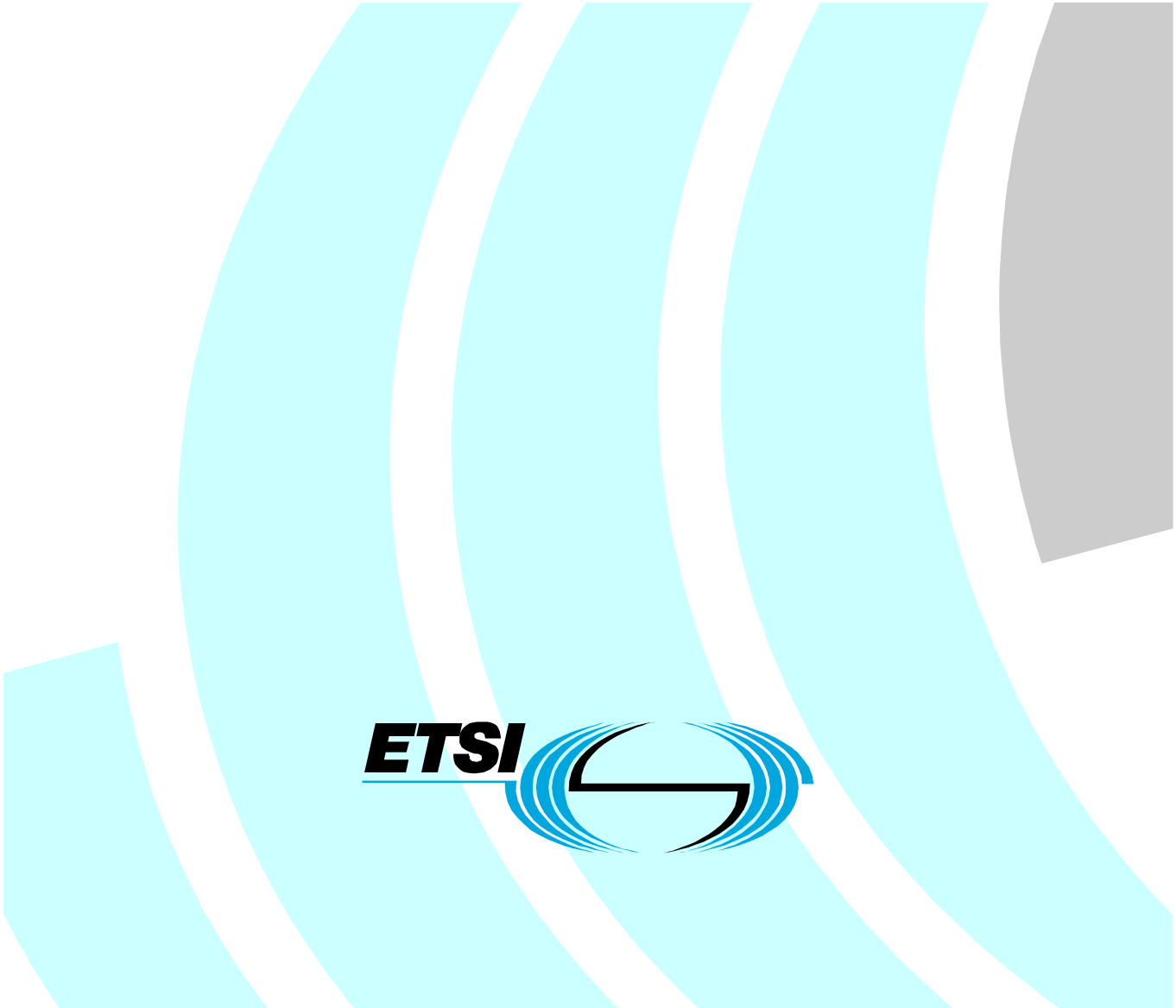
ETSI TR 187 002 V1.1.1 (2006-03)

Technical Report

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



Reference
DTR/TISPAN-07016-NGN-R1

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 two scenarios of release 1 of the NGN. Those two analyzed scenarios are PSTN/ISDN Emulation and NASS-IMS bundled authentication.

The document follows the method and proforma for carrying out a TVRA [5] 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 NGN R1. Note however, that depending on actual instantiation of NGN, some of the made assumptions may not fully hold; this may potentially impact the associated risks.

NOTE: Security threats and risks for issues NGN release 2 or later may also be captured in the present document.

2 References

For the purposes of this Technical Report (TR), the following references apply:

[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".

[2] ETSI TS 181 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Services and Capabilities Requirements for TISPAN NGN Release 1".

[3] IEEE 802.11i: "IEEE Standard For Information Technology Telecommunications and information Exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements".

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

[5] ETSI TS 102 165: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security".

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

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

[8] ETSI TS 187 003: "TISPAN; TISPAN NGN Security (NGN_SEC); Security Architecture - NGN Release 1".

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

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

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

[12] 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".

[13] 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]".

[14] 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)".

[15] ETSI TS 133 102: "Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture (3GPP TS 33.102 Release 7)".

[16] AS/NZS 4360: "Risk Management".

[17] 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).

[18] Directive 2002/22/EC of the European Parliament and of the council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).

[19] 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).

[20] IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".

[21] IETF RFC 2326: "Real Time Streaming Protocol (RTSP)".

[22] IETF RFC 2327: "SDP: Session Description Protocol".

[23] IETF RFC 3015: "Megaco Protocol Version 1.0".

[24] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1".

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

[26] ETSI ES 283 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Endorsement of "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 (Release 6)" for NGN Release 1".

[27] 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)".

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

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

3 Definitions and abbreviations

3.1 Definitions

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

attack: attempt to bypass security controls on a computer

T-*nnn*: numeric identifier for a threat

threat: potential cause of an unwanted incident which may result in harm to a system or organization (see ISO/IEC 13335 [4])

unwanted incident: incident such as loss of confidentiality, integrity and/or availability (see AS/NZS 4360 [16])

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
AGCF	Access Gateway Control Function
AGW	Access GateWay
A-MGF	Access Media Gateway Function
ARGW	Access Residential media GateWay
AS	Application Server
CC	Call Control
CD	Compact Disc
CHAP	Challenge Handshake Authentication Protocol
CLF	Connectivity session and repository Location Function
CPE	Customer Premises Equipment
CSCF	Call Session Control Function
DNS	Domain Name System
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
GPRS	GSM Packet Radio System
I-CSCF	Interrogating Call Session Control Function
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IMSI	IMS subscriber Identifier
IP	Internet Protocol
IPsec	Internet Protocol security
ISDN	Integrated Services Digital Network
ISIM	IMS subscriber Identity Module
ISO	International Standards Organization
ISUP	ISDN User Part
MGC	Media Gateway Controller
MGW	Media GateWay
MRFP	Media Resource Function Processor
NASS	Network Access SubSystem

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
PS	Packet-Switched
PSTN	Public Switched Telephone Network
RACS	Resource Admission Control Subsystem
RCEF	Resource Control Enforcement Function
RGW	Residential GateWay
R-MGF	Residential Media Gateway Function
ROM	Read-Only Memory
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
SpoA	Service point of Attachment
TDM	Time Division Multiplex
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
TOE	Target Of Evaluation
TpoA	Transport point of Attachment
TVRA	Threat Vulnerability Risk Assessment
UAAF	User Access Authorization Function
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 [17] 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).

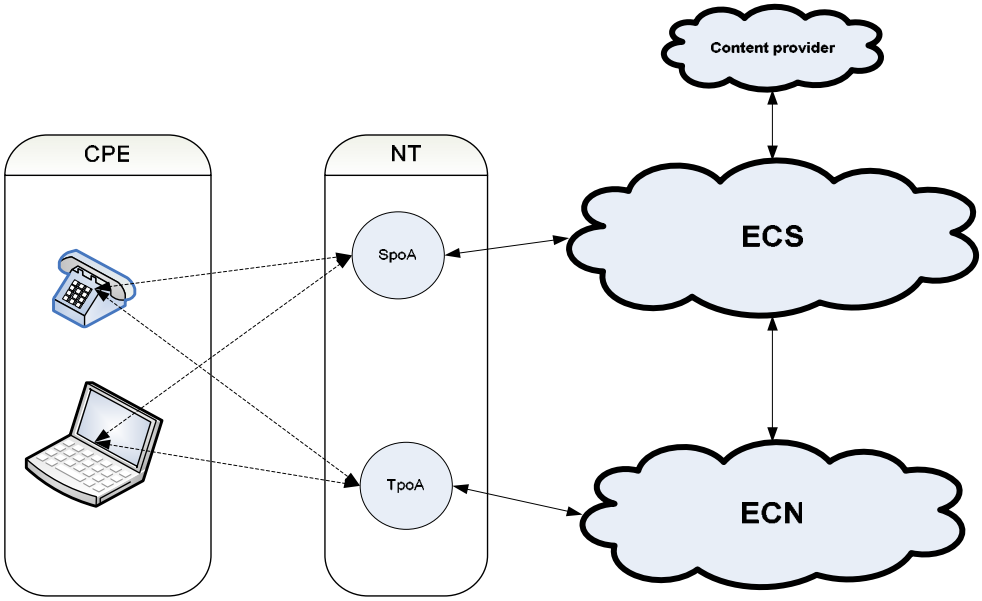


Figure 1: Basic ECN&S model for the NGN

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.

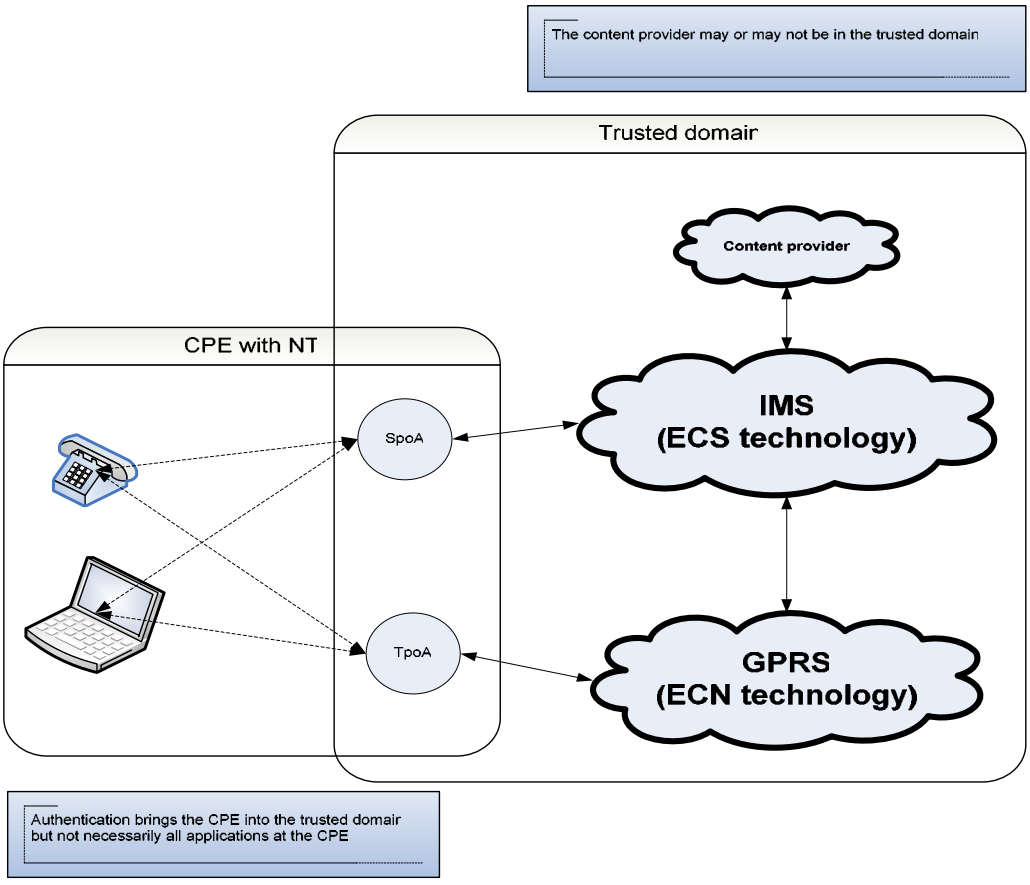


Figure 2: Simplified view of 3GPP IMS domains mapped to ECNS

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 authorisation and authentication on a per-service basis.

4.1.2.2 Generic or NGN IMS

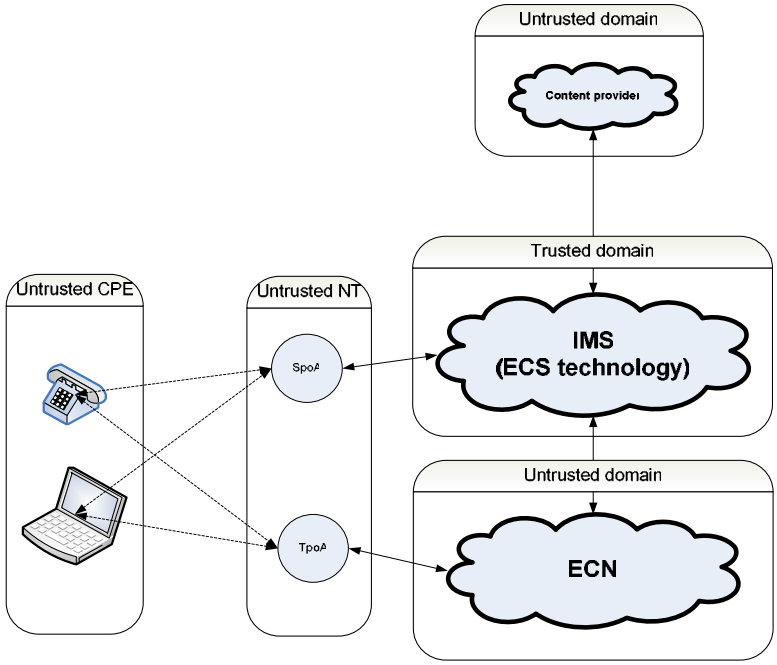


Figure 3: view of IMS where IMS is trusted

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

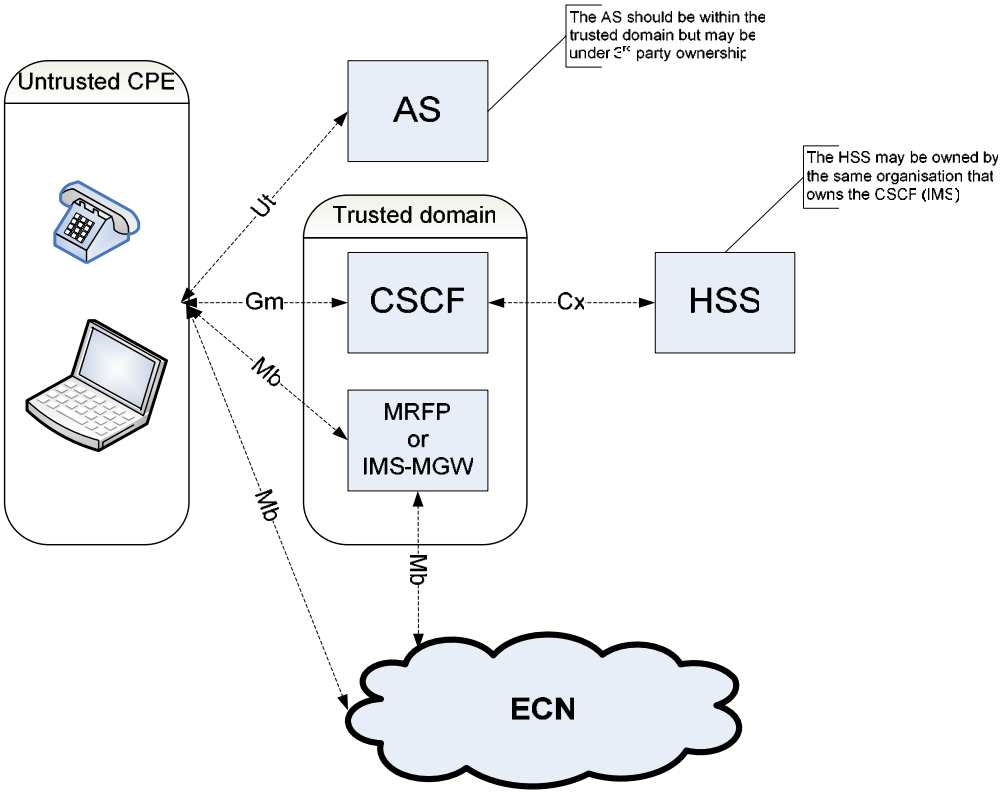


Figure 4: Open interfaces in the IMS model for NGN

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

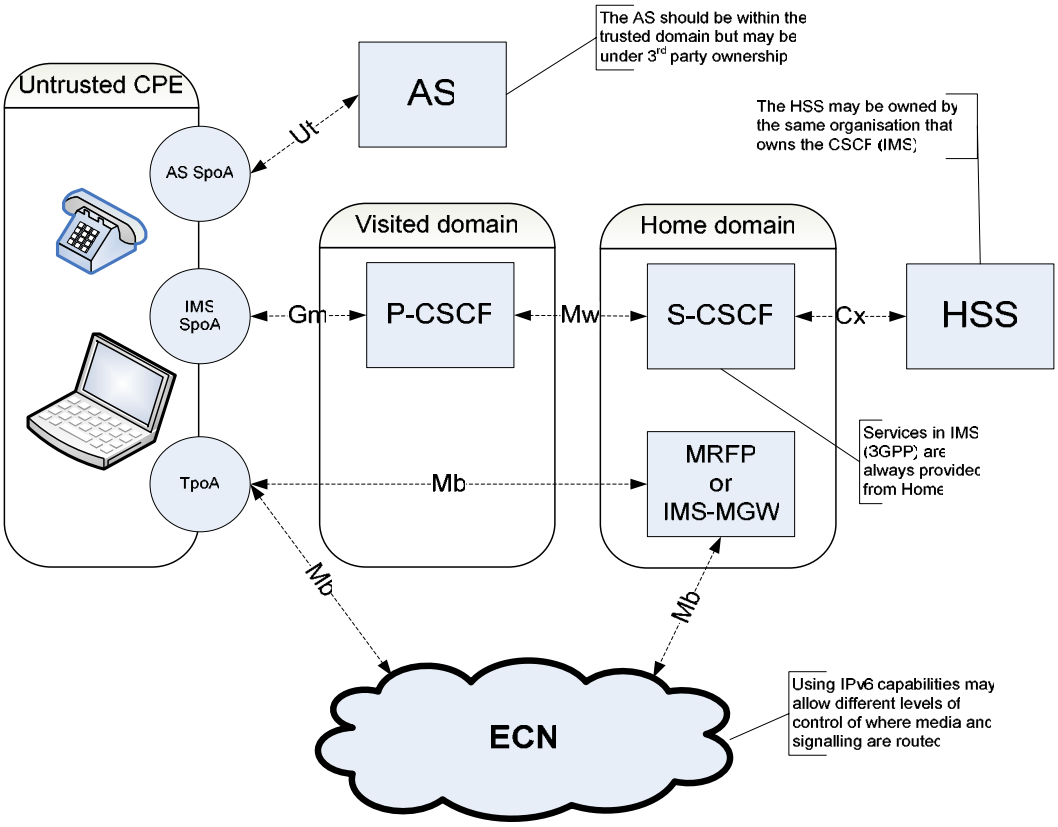


Figure 5: Roaming scenario

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.

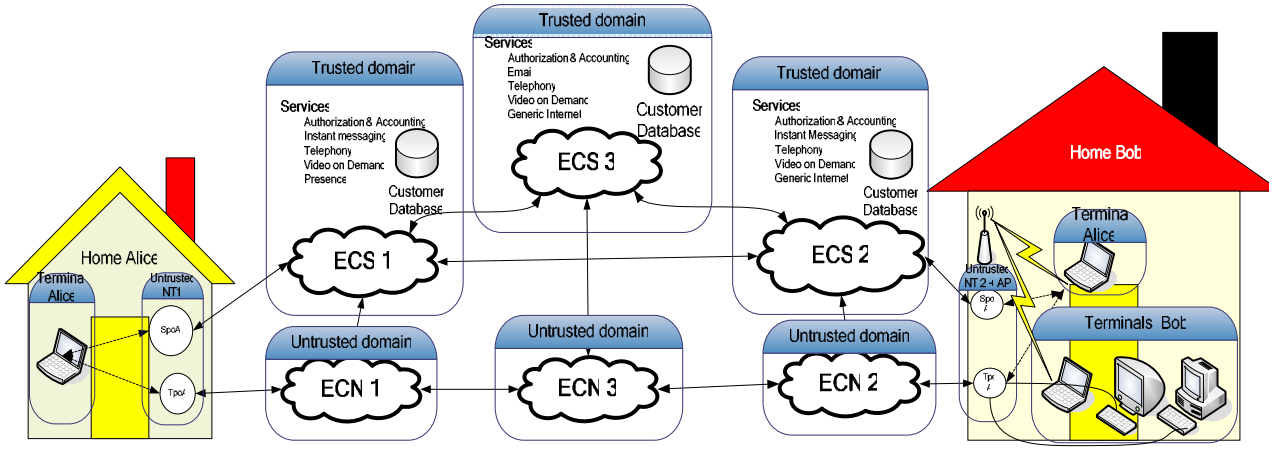


Figure 6: Nomadic user security scenario

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

This clause analyzes NGN in terms of threats and carries out an analysis of risks according to the methodology defined in TS 102 165 [5].

5.1 PES Analysis

5.1.1 PES objectives and security objectives

The current draft of ES 282 002 [10] 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 [17] and the Privacy Directive [19].

5.1.2 Stage 2 model of PES (UML)

The UML class diagram representing PES is given below.

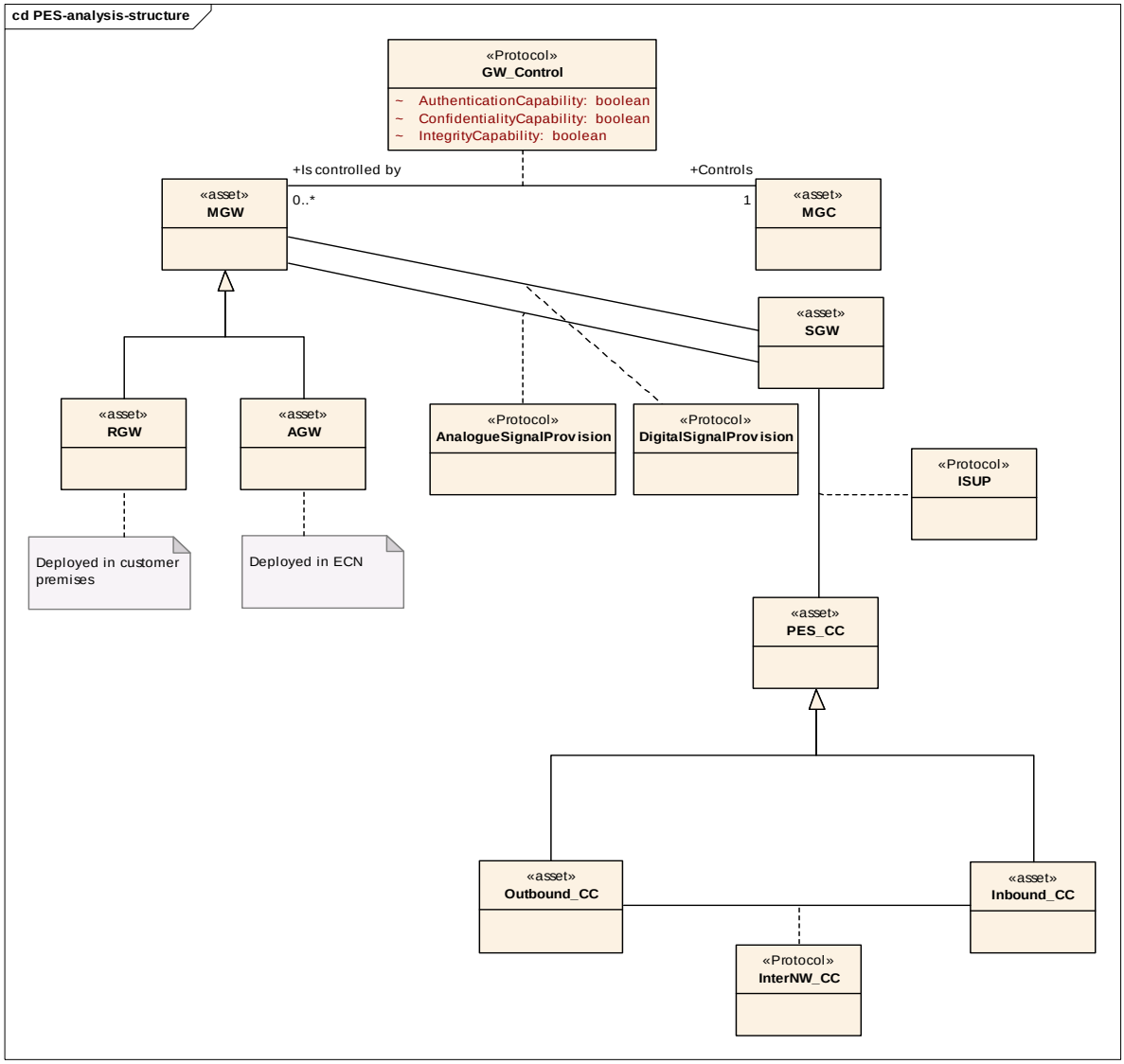


Figure 7: UML class diagram for PES

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 [12] for the Gateway control protocol and for the means of providing signalling from the analogue user line to the PES-CC, and SIP-I [13] for the Inter-network call control transfer protocol) in the available PES stage 3 definitions.

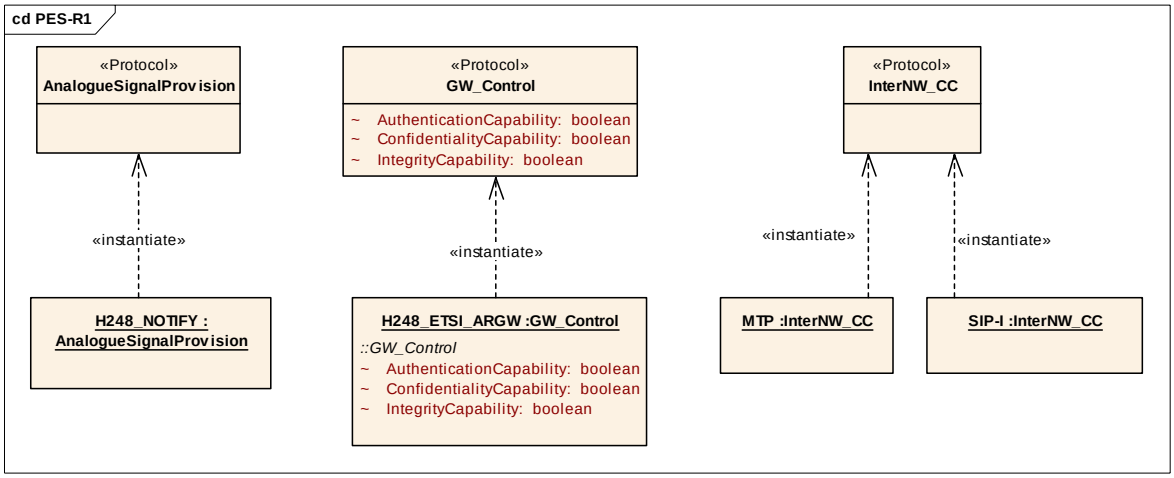


Figure 8: Instances of the PES protocols

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 [29] 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.

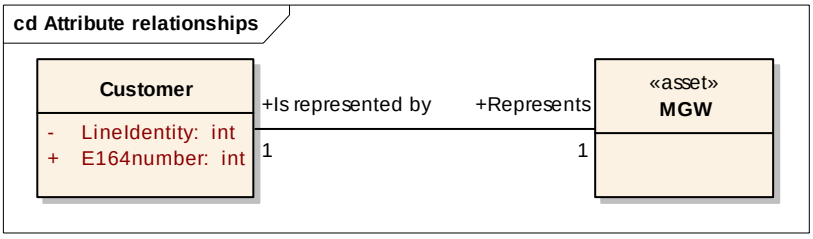


Figure 9: UML representation of customer to MGW relationship

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 [24] and the security provisions for use of H.248 [29] for that model are also described in ES 283 002 [12].

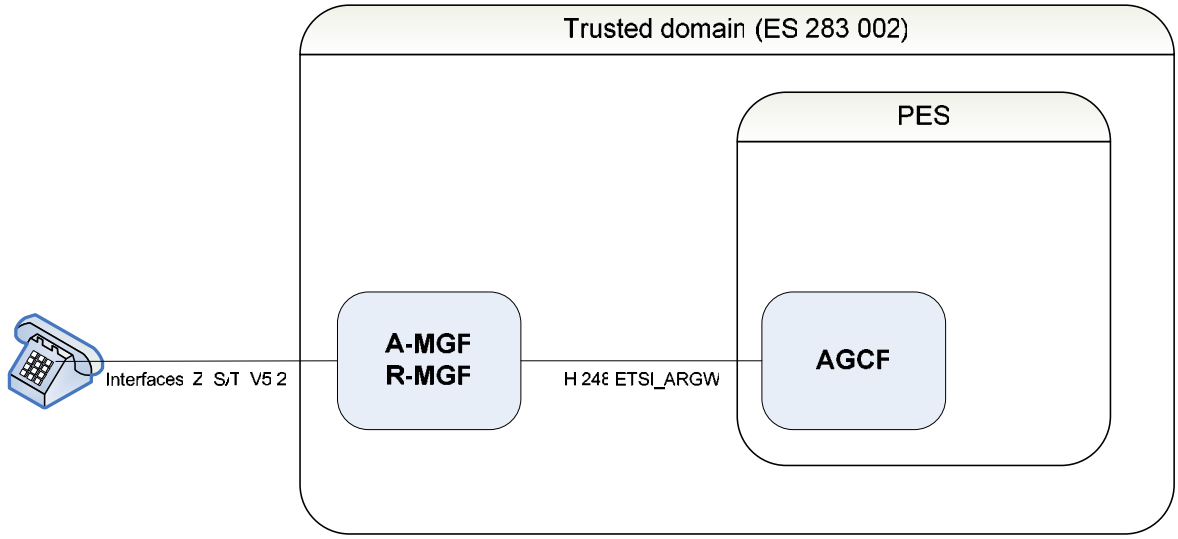


Figure 10: H.248 deployment model as specified in ES 282 002

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 [29] 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 [27] 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 [27] 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 133 203 [27] 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 [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 shall 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.

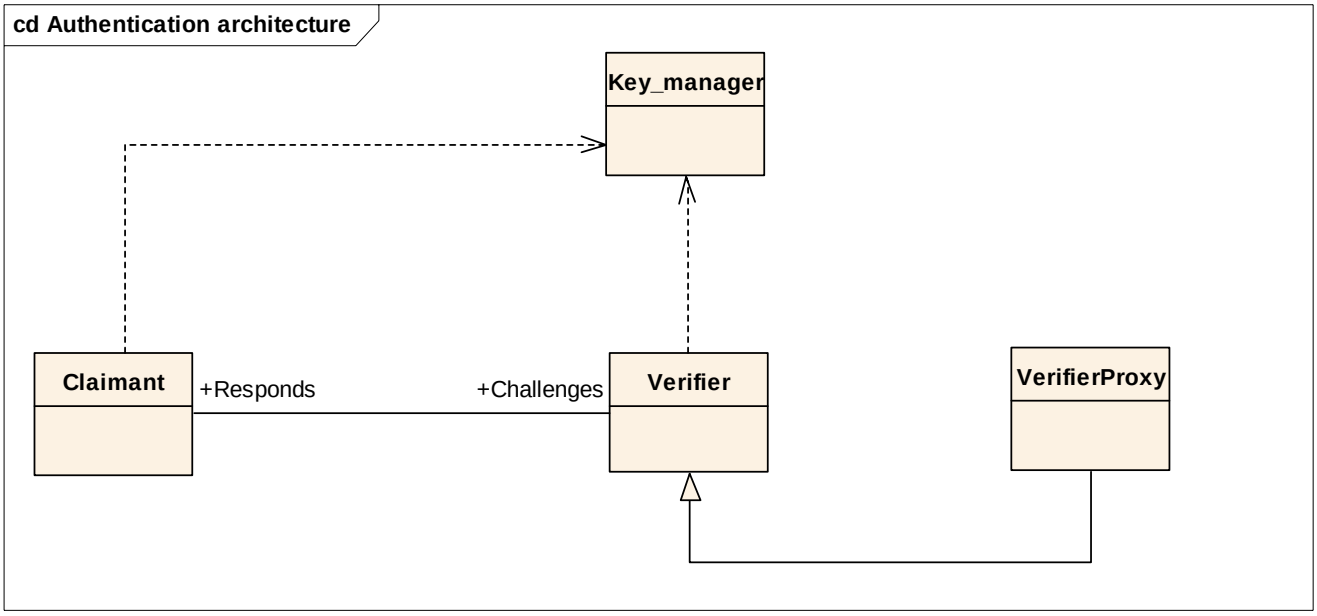


Figure 11: Authentication pattern

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).

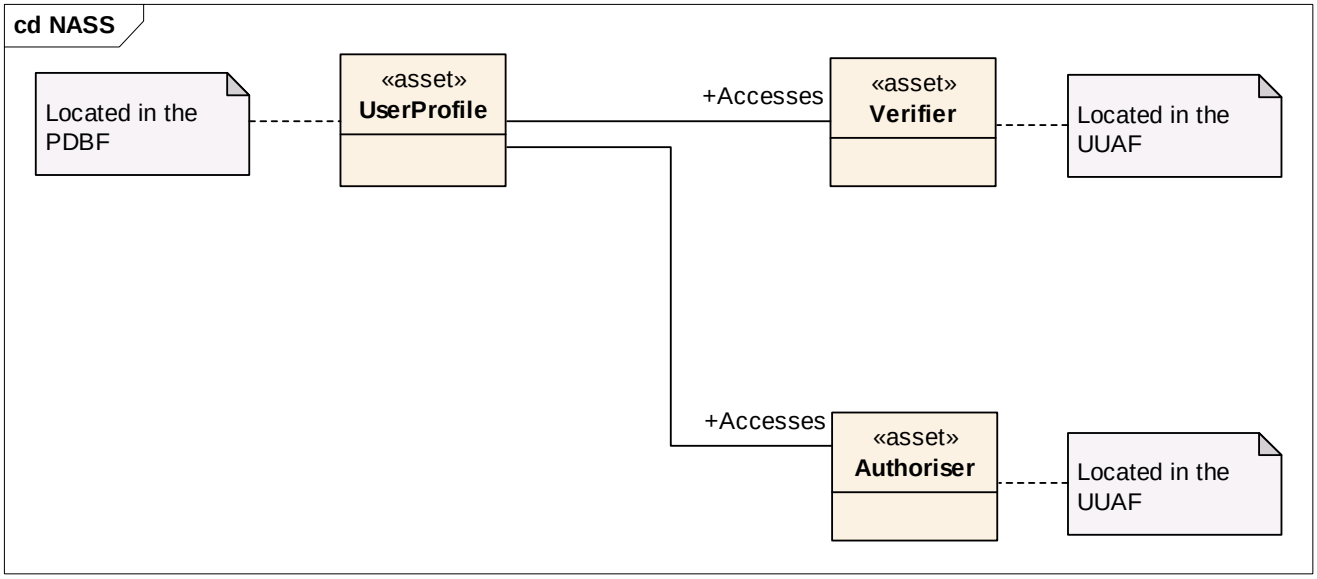


Figure 12: NASS matching to authentication pattern

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.

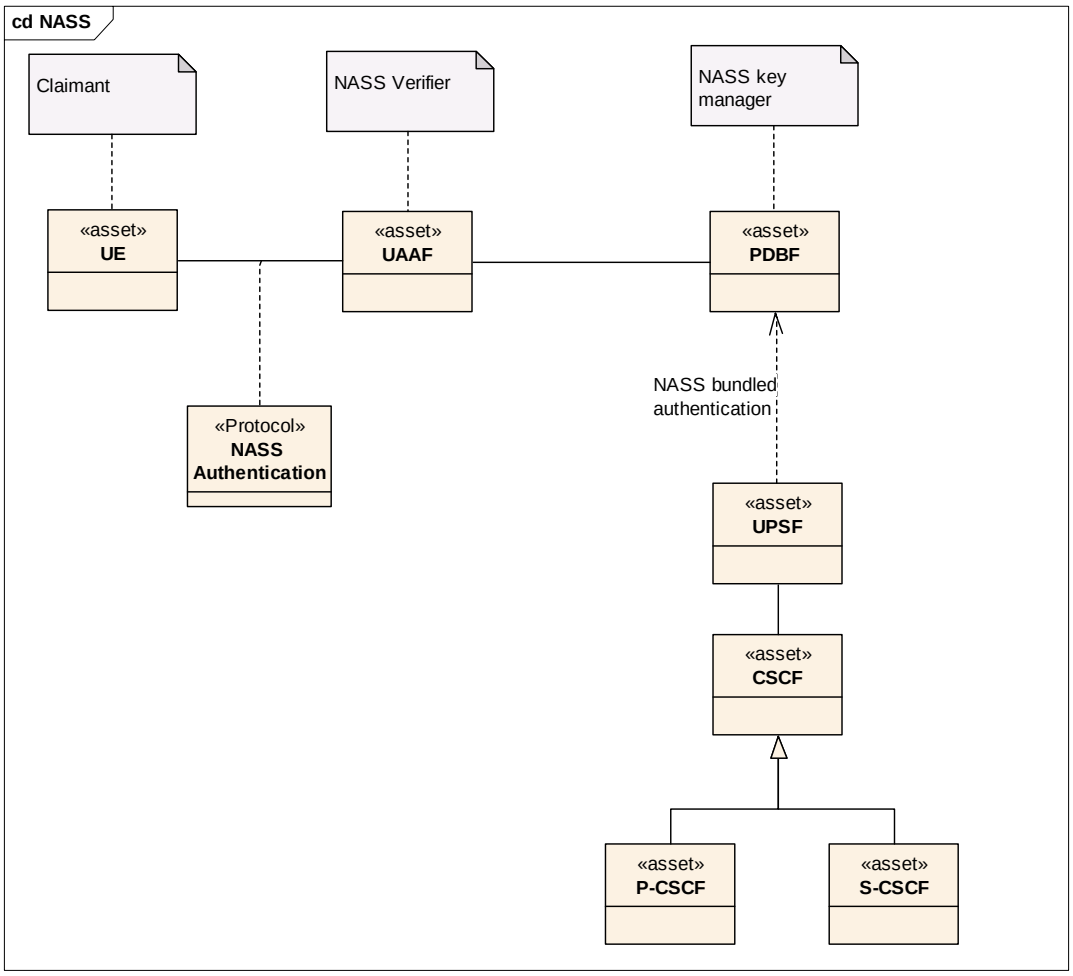


Figure 13: IMS-NASS bundled authentication class diagram model

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 [6] 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 98forms) 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.

5.2.1.3 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 1)
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 [28]).

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 [ES 282 001 [24]], specifically the RECF, shall 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 shall prevent "source IP spoofing". If IP address spoofing is detected the BGF shall 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 must lose IP connectivity without prior deregistration from IMS. Then the attacker must obtain the same IP address when he accesses the core network (or, given the assigned IP address, he must know the IMPU of the prior owner of this IP address, and this user must 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 must 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 must be performed by DoS prevention mechanisms within the target domains (e.g. IMS domain). These countermeasures must 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

5.2.1.5 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

Analysis of RACS in the access network and analysis of RACS in interdomain are FFS.

5.4 Analysis of NGN-IMS

FFS

5.5 Analysis of DNS and ENUM in NGN

FFS

5.6 Analysis of SIP in NGN

FFS

6 Conclusions

Table 22 below 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 22 identifies some example security requirements. Table 22 also identifies security countermeasures against the security vulnerabilities.

NOTE: The shown requirements in table 22 are not meant to be complete; TS 187 003 [8] may provide more security requirements.

Table 22: 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 [7]	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 [8].
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 [8].
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-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 [14].
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 [8].
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 [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 [8].
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 [8].
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 [14].

Threat Identifier	Security Threat (0 - 14) Subsystem/Feature: short description	Attack potential rating	Impact	Occurrence likelihood	Risk	Primary NGN Security Requirement [7]	Countermeasure as defined
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.

History

Document history		
V1.1.1	March 2006	Publication