

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

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI TR 187 002 V3.1.1 \(2011-04\)](https://standards.iteh.ai/catalog/standards/etsi/509c637f-1992-46ce-89a8-6939243ac676/etsi-tr-187-002-v3-1-1-2011-04)

<https://standards.iteh.ai/catalog/standards/etsi/509c637f-1992-46ce-89a8-6939243ac676/etsi-tr-187-002-v3-1-1-2011-04>



Reference

RTR/TISPAN-07037-NGN-R3

Keywords

analysis, security**ETSI**

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

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

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

(<https://standards.iteh.ai>)
Document Preview

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

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

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

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

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

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

Copyright Notification

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

© European Telecommunications Standards Institute 2011.
All rights reserved.

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

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

LTE™ is a Trade Mark of ETSI currently being registered

for the benefit of its Members and of the 3GPP Organizational Partners.

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

Contents

Intellectual Property Rights	9
Foreword.....	9
1 Scope	10
2 References	10
2.1 Normative references	10
2.2 Informative references.....	10
3 Definitions and abbreviations.....	15
3.1 Definitions.....	15
3.2 Abbreviations	15
4 NGN-relevant Security Interfaces and Scenarios.....	17
4.1 Security-relevant NGN Scenarios	17
4.1.1 Basic NGN scenario (ECN&S model).....	17
4.1.2 IMS scenarios	18
4.1.2.1 3GPP IMS	18
4.1.2.2 Generic or NGN IMS	19
4.1.3 Nomadic user security scenario	21
5 Threat and risk analysis	21
5.1 PES Analysis	21
5.1.1 PES objectives and security objectives.....	21
5.1.2 Stage 2 model of PES (UML)	22
5.1.2.1 Identification of assets.....	23
5.1.2.2 Missing considerations in PES.....	23
5.1.2.2.1 ECN technology	23
5.1.2.2.2 Protocol stack	24
5.1.2.2.3 Cardinality of relationships	24
5.1.2.2.4 Deployment	24
5.1.3 Points of attack in PES.....	24
5.1.3.1 Interfaces.....	24
5.1.3.2 Implicit relationships.....	24
5.1.4 Risk analysis	25
5.1.4.1 Overview	25
5.1.4.2 Interception	25
5.1.4.2.1 Interception at the customer to MGW interface	25
5.1.4.2.2 Interception within the fixed network.....	25
5.1.4.3 Manipulation.....	25
5.1.4.3.1 Manipulation at the customer interface	26
5.1.4.3.2 Manipulation in the fixed parts of the network.....	26
5.1.4.3.3 Manipulation in links between networks	27
5.1.4.4 Denial-of-Service	27
5.1.5 PES unwanted incidents.....	28
5.1.6 Existing PES security provisions	28
5.1.7 Security capabilities in PES	28
5.1.7.1 H.248 ETSI_ARGW	28
5.1.7.1.1 Authentication	28
5.1.7.1.2 Confidentiality of signalling.....	28
5.1.7.1.3 Confidentiality of traffic.....	28
5.1.7.1.4 Integrity of signalling	29
5.1.7.1.5 Integrity of traffic	29
5.1.8 Role of NGN subsystems in PES.....	29
5.1.8.1 Transport plane	29
5.1.8.1.1 NASS.....	29
5.1.8.1.2 RACS	29
5.1.8.1.3 Transport elements	29

5.1.8.2	Service plane	29
5.1.8.2.1	IMS	29
5.1.8.2.2	PSS	29
5.1.8.3	Recommendations	29
5.2	Analysis of NASS	29
5.3	Analysis of RACS	29
5.4	Analysis of NGN-IMS.....	30
5.5	Analysis of DNS and ENUM in NGN.....	30
5.6	Analysis of SIP in NGN	30
6	Conclusions for NGN-R1	30

Annex A: TVRA of RACS in NGN-R2.....33

A.1	Scope of the TVRA	33
A.2	Identification of the ToE	33
A.2.1	Overview	33
A.2.2	Scenarios for analysis and derivation of ToE.....	35
A.2.2.1	Summary.....	35
A.2.2.2	Single trust domain deployment scenario	35
A.2.2.3	Two separate trust domains deployment scenario	36
A.2.2.4	Two collaborating trust domains deployment scenario.....	37
A.2.2.5	Multi trust domain deployment scenarios	38
A.3	Analysis of ToE elements.....	39
A.3.1	Transport processing functions.....	39
A.3.2	SPDF	40
A.3.3	RACF	40
A.3.4	Reference points	40
A.3.5	Information flow analysis.....	41
A.4	Security objectives	45
A.5	Threats to RACS and threat agents to enable them.....	46
A.6	Countermeasures for risk mitigation in RACS.....	47
A.6.1	Functional requirements	47
A.6.2	Detail requirements	48

Annex B: TVRA of Media transport NGN-R2.....49

B.1	Description of ToE	49
B.2	Identification of objectives	51
B.3	Step 2: Identification of requirements	51

Annex C: Example TVRA for use of ENUM in NGN.....54

C.1	Overview and introduction	54
C.1.1	Security critical ENUM operations	56
C.1.1.1	Registration of an E.164 number in the ENUM database	56
C.1.1.2	Processes for creation, modification and deletion of NAPTR Records in the Tier 2 database	57
C.1.1.3	Processes for removal of E.164 numbers from ENUM databases	58
C.1.1.4	Processes for changing Registrars	59
C.1.2	ENUM assets.....	60
C.1.2.1	NAPTR records	60
C.1.2.2	ENUM query	60
C.2	DNSSEC.....	60
C.3	Unwanted incidents in use of ENUM in NGN (eTVRA Step 1).....	61
C.4	Security requirements for ENUM in the NGN (eTVRA Step 2)	61
C.5	ENUM assets (eTVRA Step 3)	63
C.5.1	NNA provisioning scenario	63

C.5.2	Signalling scenario	64
C.5.3	Identification of assets	65
C.5.4	Logical Assets	66
C.5.5	Physical Assets	66
C.5.6	Summary of assets	67
C.5.7	Relationships between assets	68
C.6	Vulnerabilities in ENUM (eTVRA Step 4)	69
C.6.1	Weakness in ENUM (eTVRA Step 4a)	69
C.6.2	Threat agents in ENUM (eTVRA Step 4b)	70
C.6.3	Identification of vulnerabilities in ENUM (eTVRA Step 4.1)	71
C.7	Risk assessment for ENUM (eTVRA Step 5)	72
C.8	ENUM risk classification (eTVRA Step 6)	73
C.9	ENUM countermeasure framework (eTVRA Step 7)	75
C.10	Completed eTVRA proforma for ENUM	77

Annex D: TVRA of IPTV in NGN-R280

D.1	Step 0: Description of ToE (IPTV)	80
D.1.1	IPTV stakeholders	80
D.2	Step 1: Identification of objectives	82
D.2.1	Void	82
D.2.2	(System) Security Objectives	82
D.2.2.1	Security objective category authentication	82
D.2.2.2	Security objective category accountability	83
D.2.2.3	Security objective category confidentiality	83
D.2.2.4	Security objective category integrity	83
D.2.2.5	Security objective category availability	83
D.3	Step 2: Identification of requirements	83
D.3.1	Security requirements category authentication	83
D.3.2	Security requirement category accountability	84
D.3.3	Security requirement category confidentiality	85
D.3.4	Security requirement category integrity	86
D.3.5	Security requirement category availability	86
D.4	Step 3: Inventory of the assets	87

Annex E: TVRA of NAT and NAT-T in NGN-R288

E.1	Step 0: Description of NAT and NAT-T in NGN-R2	88
E.2	Step 1: Identification of objectives	90
E.2.1	(System) Security Objectives	90
E.3	Step 2: Identification of requirements	91
E.4	Step 3: Inventory of the assets	94
E.5	Vulnerabilities in R2 NAT traversal (eTVRA Step 4)	95
E.5.1	Weakness in R2 NAT traversal (eTVRA Step 4a)	95
E.5.2	Threat agents in R2 NAT traversal (eTVRA Step 4b)	95
E.6	Threats to NAT-T and threat agents to enable them (TVRA steps 4 and 5)	96
E.6.1	Identification of threats and threat agents in STUN	96
E.6.1.1	Manipulation threats and threat agents	96
E.6.1.1.1	Attacker in NAT-T path	96
E.6.1.1.1.1	Interception of STUN messages	96
E.6.1.1.1.2	Manipulation of STUN messages	96
E.6.1.1.1.3	Construction of integrity check value	97
E.6.1.1.1.4	Manipulation of STUN protocol	97
E.6.1.1.2	Attacker in NAT-T endpoint	98
E.6.1.2	STUN usage attacks	98

E.6.1.2.1	DDoS Against a Target	98
E.6.1.2.2	Silencing a Client	98
E.6.1.2.3	Masquerade as a known Client	98
E.6.1.2.4	Eavesdropping	98
E.6.1.2.5	Risk analysis for use of ICE	99
E.6.1.2.6	Risk analysis for use of Outbound	99
E.6.2	Risk analysis for use of IMS-ALG	99

Annex F: TVRA of UC in NGN-R2.....100

Annex G: TVRA of CPN in NGN-R3101

G.1 Customer Premises Network (CPN) Threat Vulnerability and Risk Analysis (TVRA)101

G.2 Identification of CPN for TVRA analysis101

G.2.1 Overall description of the CPN101

G.2.2 The security analysis process101

G.2.2.1 Initial security analysis102

G.2.2.2 Assumptions102

G.2.2.3 Security Objectives103

G.2.2.4 Security functional requirements derived from the security objectives104

G.2.2.5 Mapping from objectives to functional requirements105

G.2.3 Identification of the ToE107

G.2.3.1 Inherent weakness in the ToE108

G.2.3.2 Assets inside the ToE.....108

G.2.3.2.1 Decomposition of the CNG functional entities110

G.2.4 Mapping of functional requirements to assets in the ToE114

G.2.5 Weaknesses of assets in the ToE115

G.2.5.1 Wireless access devices115

G.2.5.1.1 Wireless Ethernet (IEEE 802.11 series)115

G.2.5.1.1.1 Wired Equivalent Privacy (WEP).....115

G.2.5.1.1.2 WiFi Protected Access (WPA).....116

G.2.5.1.1.3 WPA-2 or Robust Security Network (RSN).....116

G.2.5.1.2 DECT devices116

G.2.5.1.3 Bluetooth devices.....116

G.2.5.2 SIP signalling.....117

G.2.5.3 Lack of DoS Protection117

G.2.5.4 Summary of ToE weaknesses117

G.2.6 Threats to the weaknesses of assets in the ToE119

G.2.6.1 Denial of service (DoS)120

G.2.6.2 Eavesdropping120

G.2.6.2.1 Eavesdropping of content of communication.....120

G.2.6.2.2 Eavesdropping of network element IDs121

G.2.6.3 Masquerade.....121

G.2.6.4 Unauthorized access122

G.2.6.5 Loss of information.....122

G.2.6.6 Corruption of information.....122

G.2.6.7 Repudiation.....123

G.2.6.8 Threat list123

G.2.7 Risk factor calculation.....129

G.3 Countermeasures in the form of detailed requirements.....131

G.3.1 General countermeasures131

G.3.1.1 Wireless connection measures (CND to CNG).....131

G.3.1.2 Connection measures (CNG to NGN)131

G.3.1.3 Anti-masquerade countermeasures131

G.3.2 Detailed security requirements135

G.3.2.1 Confidentiality requirements135

G.3.2.2 Identification, authentication and authorization requirements.....135

G.3.2.3 Integrity requirements.....135

G.3.2.4 Availability and DoS protection requirements.....136

Annex H: Identity and privacy protection TVRA for NGN-R3.....137

Annex I:	TVRA of NASS in NGN-R3	138
I.1	Scope of NASS TVRA.....	138
I.2	NASS TVRA Target of Evaluation (ToE)	138
I.2.1	Definitions	138
I.2.2	ToE Description	139
I.2.3	Analysis of Interfaces.....	140
I.2.4	Assumptions on the ToE	142
I.2.5	Assumptions of the ToE Environment	142
I.2.6	Revised NASS architecture	142
I.2.7	Analysis of exposed interfaces	143
I.3	NASS security objectives.....	144
I.4	Functional security requirements	145
I.5	NASS Assets	145
I.6	NASS Vulnerabilities and Threats	145
I.6.1	Threat identification and risk analysis of scenarios 10-12 (e1).....	146
I.6.1.1	Implicit line authentication and IP configuration using DHCP over e1.....	146
I.6.1.1.1	Vulnerabilities and threats.....	147
I.6.1.2	Explicit authentication over e1	147
I.6.1.2.1	PPP-based Authentication.....	147
I.6.1.2.1.1	Vulnerabilities and threats.....	148
I.6.1.2.2	EAPOL (EAP over Ethernet) Authentication.....	148
I.6.1.2.2.1	Vulnerabilities and threats.....	148
I.6.1.2.3	Explicit authentication over xDSL/FTTx.....	148
I.6.1.2.3.1	Vulnerabilities and threats.....	149
I.6.1.2.4	WLAN-based authentication.....	149
I.6.1.2.4.1	Vulnerabilities and threats.....	150
I.6.1.2.5	NASS-IMS bundled authentication.....	150
I.6.1.2.5.1	Overview	150
I.6.1.2.5.2	Stage 2 model of NASS-IMS bundled authentication.....	150
I.6.1.2.5.3	NASS-IMS-bundled authentication assets	151
I.6.1.2.5.4	Uncertainty regarding functions in NASS.....	152
I.6.1.2.5.5	Vulnerabilities and threats.....	153
I.6.1.3	IP address allocation over e1	153
I.6.1.3.1	Vulnerabilities and threats.....	153
I.6.1.4	Risk analysis	153
I.6.1.5	Countermeasure framework as detailed requirements	153
I.6.2	Threat identification and risk analysis of scenario 1 (e5).....	154
I.6.2.1	Overview of interface e5.....	154
I.6.2.2	Protocols and profiles for interface e5.....	155
I.6.2.2.1	802.1X-based Authentication.....	155
I.6.2.2.2	Subscriber Profile Transfer	156
I.6.2.3	Vulnerabilities and threats	157
I.6.2.4	Risk analysis	158
I.6.2.5	Countermeasure framework as requirements.....	158
I.6.3	Threat identification and risk analysis of scenarios 5-11 (e2)	159
I.6.3.1	Overview of interface e2.....	159
I.6.3.2	Vulnerabilities and threats	160
I.6.3.3	Risk analysis	161
I.6.3.4	Countermeasure framework as requirements.....	162
I.7	Risk Analysis.....	162
I.8	Countermeasure framework as detailed requirements	163
I.9	Mapping NASS Countermeasure Framework to TS 187 001	163
I.10	TS 187 001 requirements aligned with NASS countermeasure framework.....	164
I.10.1	WLAN requirements	164
I.10.2	AAAA requirements.....	164