

ETSI TS 102 165-1 V4.2.1 (2006-12)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis



Reference

RTS/TISPAN-07006-TECH

Keywords

IP, protocol, security, VoIP

ETSI

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

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

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

Important notice

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 2006.
All rights reserved.

DECTTM, **PLUGTESTS**TM and **UMTS**TM are Trade Marks of ETSI registered for the benefit of its Members.
TIPHONTM and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

Intellectual Property Rights	6
Foreword.....	6
Introduction	6
1 Scope	8
2 References	8
3 Definitions, symbols and abbreviations	10
3.1 Definitions	10
3.2 Symbols.....	11
3.3 Abbreviations	11
4 Introduction	12
4.1 Role of TVRA	12
4.2 Generic TVRA relationships	14
4.3 Countermeasure strategies.....	17
4.3.1 Asset redesign	17
4.3.2 Asset hardening	17
4.4 Relationship with Common Criteria evaluation	17
5 <i>e</i> TVRA method	18
5.1 Overview	18
5.1.1 Target Of Evaluation description	20
5.1.1.1 Security environment	20
5.1.1.2 Security objectives	21
5.1.1.3 Security requirements.....	22
5.1.1.3.1 The relationship between security objectives and security requirements	22
5.1.1.3.2 Security requirements	22
5.1.1.3.2.1 Interaction with ISO/IEC 15408 [13]	23
5.1.2 Threats and threat agents	24
5.2 Actors and roles.....	26
5.2.1 Rationale	26
6 Method process	27
6.1 Overview	27
6.2 Step 1: Identification of objectives.....	27
6.3 Step 2: Identification of requirements	28
6.4 Step 3: Systematic inventory of the assets.....	29
6.5 Step 4: Systematic identification of vulnerabilities	30
6.5.1 Step 4.1: Identification of vulnerability	31
6.5.2 Step 4.a: identification of weakness.....	31
6.5.2.1 Knowledge factor.....	31
6.5.3 Step 4.b: identification of attack method (threat agent).....	31
6.5.3.1 Assessment of the practicality	32
6.5.3.2 Time factor.....	32
6.5.3.3 Expertise factor	33
6.5.3.4 Opportunity factor.....	33
6.5.3.5 Equipment factor.....	34
6.5.3.6 Intensity factor	34
6.6 Step 5: Calculation of the likelihood of the attack and its impact	36
6.7 Step 6: Establishment of the risks	37
6.7.1 Impact of intensity	37
6.7.2 Classification of risk	38
6.7.2.1 Overview.....	38
6.8 Step 7: Security countermeasure identification	39
6.8.1 Countermeasures in the system.....	40
6.8.2 Composite countermeasures applied to the system.....	40

6.8.3	Impact of countermeasures applied to the system.....	40
Annex A (normative):	TVRA proforma.....	41
Annex B (informative):	The role of motivation	42
Annex C (informative):	Example TVRA for use of ENUM in NGN.....	43
C.1	Overview and introduction.....	43
C.1.1	Security critical ENUM operations	45
C.1.1.1	Registration of an E.164 number in the ENUM database	45
C.1.1.2	Processes for creation, modification and deletion of NAPTR Records in the Tier 2 database	46
C.1.1.3	Processes for removal of E.164 numbers from ENUM databases	47
C.1.1.4	Processes for changing Registrars	48
C.1.2	ENUM assets.....	49
C.1.2.1	NAPTR records	49
C.1.2.2	ENUM query	49
C.2	DNSSEC.....	50
C.3	Unwanted incidents in use of ENUM in NGN (eTVRA Step 1).....	50
C.4	Security requirements for ENUM in the NGN (eTVRA Step 2)	51
C.5	ENUM assets (eTVRA Step 3)	52
C.5.1	NNA provisioning scenario.....	52
C.5.2	Signalling scenario	53
C.5.3	Identification of assets.....	54
C.5.4	Logical Assets	55
C.5.5	Physical Assets	55
C.5.6	Summary of assets.....	56
C.5.7	Relationships between assets.....	57
C.6	Vulnerabilities in ENUM (eTVRA Step 4).....	58
C.6.1	Weakness in ENUM (eTVRA Step 4a).....	58
C.6.2	Threat agents in ENUM (eTVRA Step 4b)	59
C.6.3	Identification of vulnerabilities in ENUM (eTVRA Step 4.1)	59
C.7	Risk assessment for ENUM (eTVRA Step 5)	61
C.8	ENUM risk classification (eTVRA Step 6).....	61
C.9	ENUM countermeasure framework (eTVRA Step 7)	64
C.10	Completed eTVRA proforma for ENUM.....	66
Annex D (informative):	Denial of service attacks.....	69
D.1	DDoS Attacks viable on the NGN	69
D.1.1	Land.....	69
D.1.2	SYN Flood.....	69
D.1.3	Ping of Death.....	69
D.1.4	Process Table.....	70
D.1.5	Smurf Attack	70
D.1.6	SSH Process Table	70
D.1.7	TCP Reset.....	70
D.1.8	Teardrop	70
D.1.9	UDP Storm	70
D.2	DDoS characteristics	70
D.3	Defence against DDoS	71
D.3.1	Preventive Mechanisms.....	71
D.3.2	Reactive Mechanisms.....	71
D.3.2.1	Signature detection mechanisms.....	71
D.3.2.2	Anomaly detection mechanisms	72
D.3.3	Difficulties of defence	72

Annex E (informative):	TVRA database structure	73
E.1	Database structure	73
E.2	SQL code for TVRA database.....	75
E.2.1	Lookup tables	75
E.2.2	Core tables.....	76
E.2.3	Linking tables.....	78
E.2.4	Sample queries (used to complete input to eTVRA proforma)	79
Annex F (informative):	Use of ISO/IEC 15408-2 [11] security functional classes in security requirements statements	80
F.1	Overview	80
F.2	Review of functional capabilities	82
F.2.1	Authentication and identification	82
F.2.2	Communication class (non-repudiation)	83
F.2.3	User data protection class.....	84
F.2.4	Privacy class.....	88
F.2.5	Resource utilization class	90
F.2.6	Trusted path/channel class.....	90
F.2.7	Security management class.....	91
F.2.8	Protection of the TSF class.....	92
F.2.9	Cryptographic support class	94
F.2.10	Security audit class.....	96
F.2.11	TOE Access class	97
Annex G (informative):	Bibliography.....	99
G.1	UML.....	99
	History	100

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

The present document is part 1 of a multi-part deliverable covering methods and protocols for security standardization, as identified below:

Part1: "Method and proforma for Threat, Risk, Vulnerability Analysis";

Part 2: "Protocol Framework Definition; Security Counter Measures".

Introduction

The present document is one of a set of documents that addresses standardization of security protocols and mechanisms within the context of the eEurope 2005 programme. The suite of documents is composed as follows:

- ETSI EG 202 387 [1]: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".
- ETSI ES 202 383 [2]: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Security Targets".
- ETSI ES 202 382 [3]: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles".
- **ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Method and proforma for Threat, Risk, Vulnerability Analysis" (the present document).**
- ETSI TS 102 165-2 [6]: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protocol Framework Definition; Security Counter Measures".
- ETSI TS 102 556: "Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protection Profile".
- ETSI EG 202 549: "Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN); Design Guide; Application of security countermeasures to service capabilities".

These documents are developed based on the objectives of the eEurope programme and are also developed to ensure they comply with the overall objectives of the European regulatory framework as defined in the following documents:

- Directive 2002/19/EC [18] of the European Parliament and of the council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive).
- Directive 2002/20/EC [19] of the European Parliament and of the council of 7 March 2002 on the authorization of electronic communications networks and services (Authorization Directive).
- Directive 2002/21/EC [20] 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).
- Directive 2002/22/EC [21] 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).
- Directive 2002/58/EC [22] 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).

In particular the present document forms part of the standardization initiative for the Next Generation Network (NGN) platform to be used in eEurope and upon which the trust and viability of the e-enabled community will, to a very large part, depend on.

The eEurope 2005 action plan has been drawn up to focus on "*the widespread availability and use of broadband networks throughout the Union ... and the security of networks and information, eGovernment, eHealth and eBusiness*" requiring a supporting infrastructure, which is truly pan-European. To quote COM(2002)263: "*By 2005 Europe should have ... a secure information infrastructure*".

1 Scope

The present document defines a method for use by ETSI standards developers in undertaking an analysis of the threats, risks and vulnerabilities of a telecommunications system.

The method builds from the Common Criteria for security assurance and evaluation defined in ISO/IEC 15408 [13] and specifically targets the means to build a Threat Vulnerability and Risk Analysis (TVRA) to allow its reference by an ETSI specification developed using the guidelines given in EG 202 387 [1] and ES 202 382 [3]. The TVRA forms part of the documentation set for the Target Of Evaluation as specified in ES 202 382 [3] with its intended audience being a developer of standards based Protection Profiles.

The Unified Modelling Language (UML) is used to model relationships within systems for analysis within the TVRA as a semi-formal tool with verification and simulation capabilities deployed during development.

NOTE: This is in accordance with the goals of the *e*Europe project under objective Good practices (COM(2002) 263 page 18).

The present document provides a database definition for TVRA and provides, in annexes, the application of the TVRA method to a number of NGN subsystems or components. The database definition is appended to the present document as a text file containing Structured Query Language (SQL) database definition commands.

The TVRA method and its accompanying database described in the present document is referred to as *e*TVRA.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- 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.
- For a non-specific reference, the latest version applies.

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

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

- [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 ES 202 383: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Security Targets".
- [3] ETSI ES 202 382: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles".
- [4] ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Subsystem".
- [5] ETSI ETR 332 (1996): "Security Techniques Advisory Group (STAG); Security requirements capture".

- [6] ETSI TS 102 165-2 (2006) "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protocol Framework Definition; Methods and Protocols for Security".
- [7] ETSI TR 102 055: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); ENUM scenarios for user and infrastructure ENUM".
- [8] ETSI TR 102 420: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Review of activity on security".
- [9] ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECURITY (SEC); Requirements".
- [10] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".
- [11] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".
- [12] ISO/IEC 15408-3: "Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements".
- [13] 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.

- [14] Common Methodology for Information Technology Security Evaluation; Evaluation methodology; July 2005; Version 3.0 Revision 2 (CCMB-2005-07-004).
- [15] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model June 2005 Version 3.0 Revision 2 (CCMB-2005-07-001).
- [16] AS/NZS 4360: "Standards Australian, Risk Management".
- [17] ISO/IEC 13335: "Information technology - Security techniques - Guidelines for the management of IT security".

NOTE: ISO/IEC 13335 is a multipart publication and the reference above is used to refer to the series.

- [18] Directive 2002/19/EC of the European Parliament and of the council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive).
- [19] Directive 2002/20/EC of the European Parliament and of the council of 7 March 2002 on the authorization of electronic communications networks and services (Authorization Directive).
- [20] 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).
- [21] 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).
- [22] 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).
- [23] ISO/IEC 17799 2005: "Information technology - Security techniques - Code of practice for information security management".
- [24] ISO/IEC 27001 2005: "Information Technology - Security Techniques - Information Security Management Systems - Requirements".

- [25] Object Management Group. UML 2.0 Superstructure Specification, document: ptc/ 04-10-02 edition, 2004.
- [26] IETF RFC 2535: "Domain Name System Security Extensions".
- [27] IETF RFC 3761: "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".
- [28] IETF RFC 3403: "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database".
- [29] IETF RFC 2915: "The Naming Authority Pointer (NAPTR) DNS Resource Record".
- [30] Draft-ietf-dnsext-dnssec-protocol-06 (2004): "Protocol Modifications for the DNS Security Extensions".
- [31] Draft-ietf-dnsext-dnssec-records-08 (2004): "Resource Records for DNS Security Extensions".
- [32] Draft-ietf-dnsext-dnssec-intro-11 (2004): "DNS Security Introduction and Requirements".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EG 202 387 [1], ISO/IEC 17799 [23], ISO/IEC 13335-1 [17] and the following apply:

asset: anything that has value to the organization, its business operations and its continuity

authentication: ensuring that the identity of a subject or resource is the one claimed

availability: property of being accessible and usable on demand by an authorized entity ISO/IEC 13335-1 [17]

confidentiality: ensuring that information is accessible only to those authorized to have access

impact: the result of an information security incident, caused by a threat, which affects assets

integrity: safeguarding the accuracy and completeness of information and processing methods

mitigation: limitation of the negative consequences of a particular event

nonce: an arbitrary number that is generated for security purposes (such as an initialization vector) that is used only one time in any security session

NOTE: Although random and pseudo-random numbers theoretically produce unique numbers, there is the possibility that the same number can be generated more than once.

non-repudiation: ability to prove an action or event has taken place, so that this event or action cannot be repudiated later

residual Risk: risk remaining after risk treatment

risk: potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

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

NOTE 1: A threat consists of an asset, a threat agent and an adverse action of that threat agent on that asset (clause 6.2 of Common Criteria part 1, version 3 revision 2 [15]).

NOTE 2: A **Threat** is enacted by a **Threat Agent**, and may lead to an **Unwanted Incident** breaking certain pre-defined security objectives.

threat agent: an entity that can adversely act on an asset

unwanted Incident: incident such as loss of confidentiality, integrity and/or availability (reference [16])

user: person or process using the system in order to gain access to some system resident or system accessible service

vulnerability: weakness of an asset or group of assets that can be exploited by one or more threats

NOTE: A **Vulnerability**, consistent with the definition given in ISO/IEC 13335 [17], is modelled as the combination of a **Weakness** that can be exploited by one or more **Threats**.

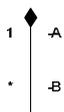
3.2 Symbols

For the purposes of the present document, the symbols given in OMG UML2 [25] and the following apply:



Generalization/Specialization: UML concept showing relationship between entities A and B where the two entities exhibit the property that A (top of arrow) is the general case whereas B is the specific case.

EXAMPLE: A countermeasure is a specialized asset.



Composition: UML concept showing relationship between entities A and B where A "is composed of" B.

EXAMPLE: Vulnerability "is composed of" a threat and a weakness.



Dependency: UML concept showing relationship between entities A and B where B is dependent upon A.

EXAMPLE: Security requirements "depend on" security objectives.



Aggregation: UML concept showing relationship between entities A and B where A "is an aggregate of" B.

EXAMPLE: System "is an aggregate of" assets.

3.3 Abbreviations

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

ANSI	American National Standards Institute
CC	Common Criteria
DDDS	Dynamic Delegation Discovery System
DDoS	Distributed Denial of Service
DNS	Domaine Name Service
DNSSEC	DNS SECurity
DoS	Denial of Service
EAL	Evaluation Assurance Level
ERD	Entity Relationship Diagram

ICMP	Internet Control Message Protocol
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network
IP	Internet Protocol
IPsec	IP security
IT	Information Technology
NAPTR	Naming Authority PoinTeR
NAT	Network Address Translation
NGN	Next Generation Network
PP	Protection Profile
RRSet	Resource Record Set
RRSIG	Resource Record SIGNature
RTP	Realtime Transport Protocol
SIP	Session Initiation Protocol
SQL	Structured Query Language
SSH	Secure SHell
ST	Security Targets
TCP	Transport Control Protocol
TIMSI	Temporary IMSI
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TOE	Target Of Evaluation
TVRA	Threat Vulnerability and Risk Analysis
UDP	User Datagram Protocol
UML	Unified Modelling Language
URI	Uniform Resource Identifiers

4 Introduction

4.1 Role of TVRA

It is recognized that without an understanding of the threats to the system that appropriate selection of countermeasures cannot be made. Within ETSI a Threat Vulnerability and Risk Analysis (TVRA) is used to identify risk to the system based upon the product of the likelihood of an attack, and the impact that such an attack will have on the system. The TVRA is primarily used within the standards domain to give justification for the development of standards based security solutions. In addition the TVRA may be used as the source of parts of a Protection Profile (PP), see ES 202 382 [3]. Large parts of the descriptive text of a PP will be derived from the TVRA: Security objectives; Security requirements; Rationale.

The method described in the present document provides a means of documenting the rationale for designing security countermeasures in a system by application of a systematic method, and by using part of the method to visualize the relationship of objectives, requirements, system design and system vulnerabilities.

The depth of the TVRA changes as the system design becomes more detailed. A TVRA working from the system objectives will identify at a very coarse level the required security functionality to ensure that the objectives can be met without damage to the system. The structure of activities in development of a TVRA is shown in figure 1. The process is shown as recursive wherein in any change to any aspect of the system or its environment requires the process to restarted.

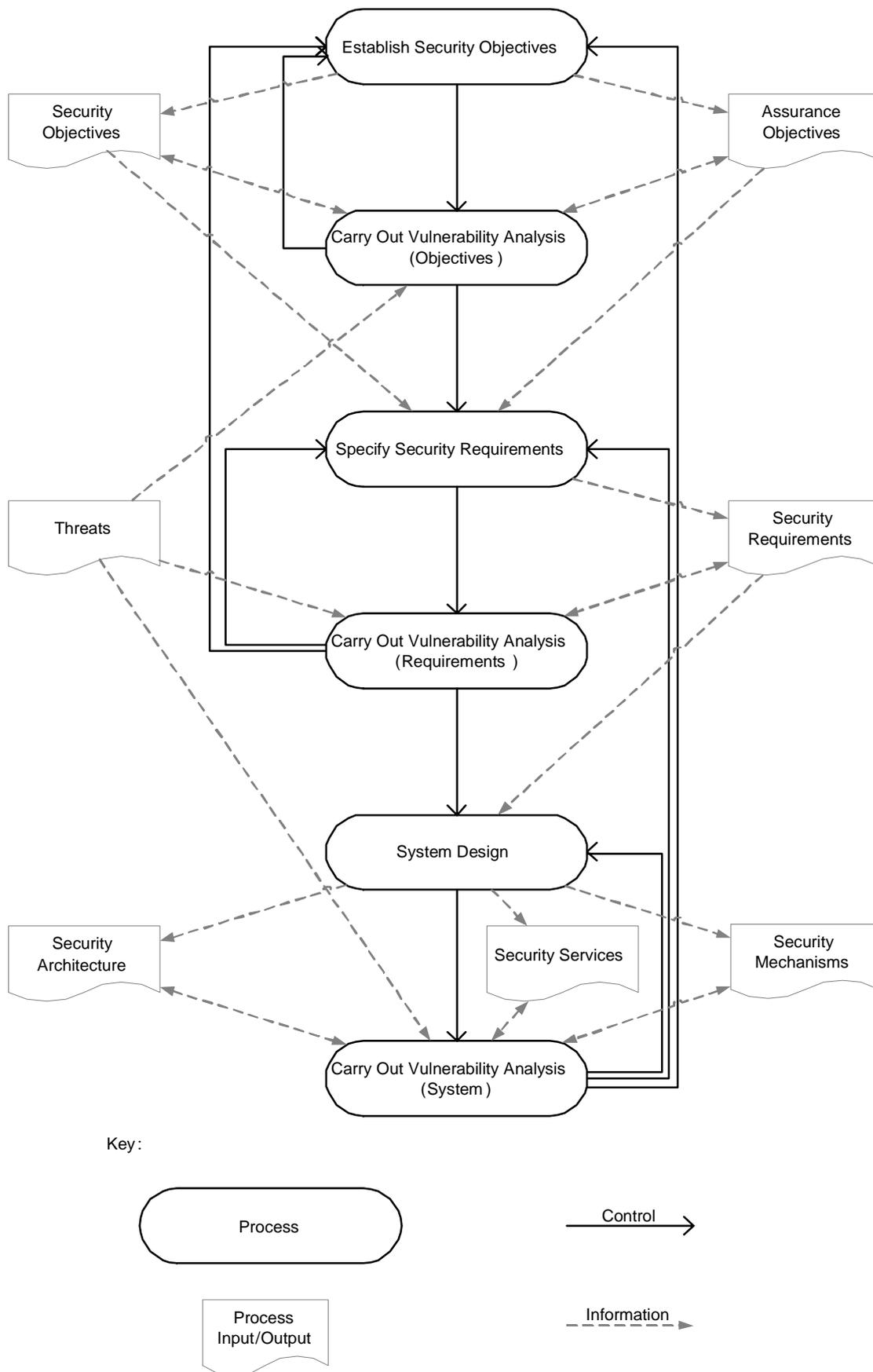


Figure 1: Structure of security analysis and development in standards documents

The purpose of the TVRA is to determine how open to attack the system, or components of the system are. A measure of openness of the system to attack is "attack potential" which combines factors of expertise, availability and resources to give a metric for attack evaluation and this is explored further in clause 6.6.

An alternative view of the nature of TVRA is given in figure 2 showing that any change either internal (say by application of countermeasures) or external to the system requires that the TVRA process is redone.

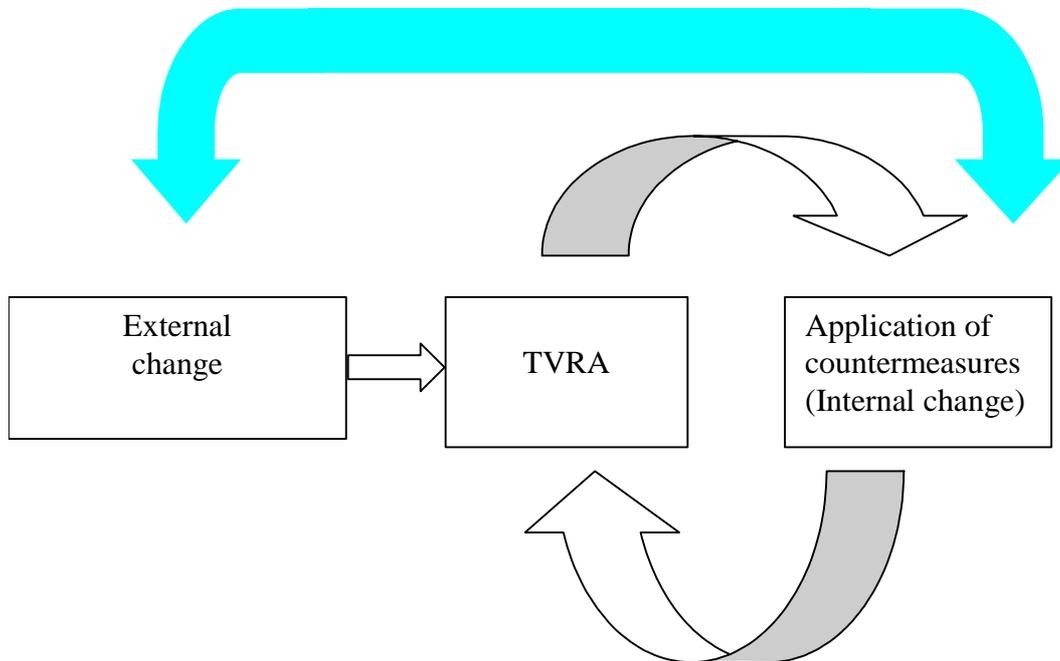


Figure 2: Cyclical nature of TVRA

4.2 Generic TVRA relationships

One of the keys to a successful TVRA, and also of a successful system design, is the ability to show the relationship of objectives and requirements to the system design. Figure 3 shows the dependencies between system objectives, system requirements and system design highlighting the interplay of security objectives and requirements.

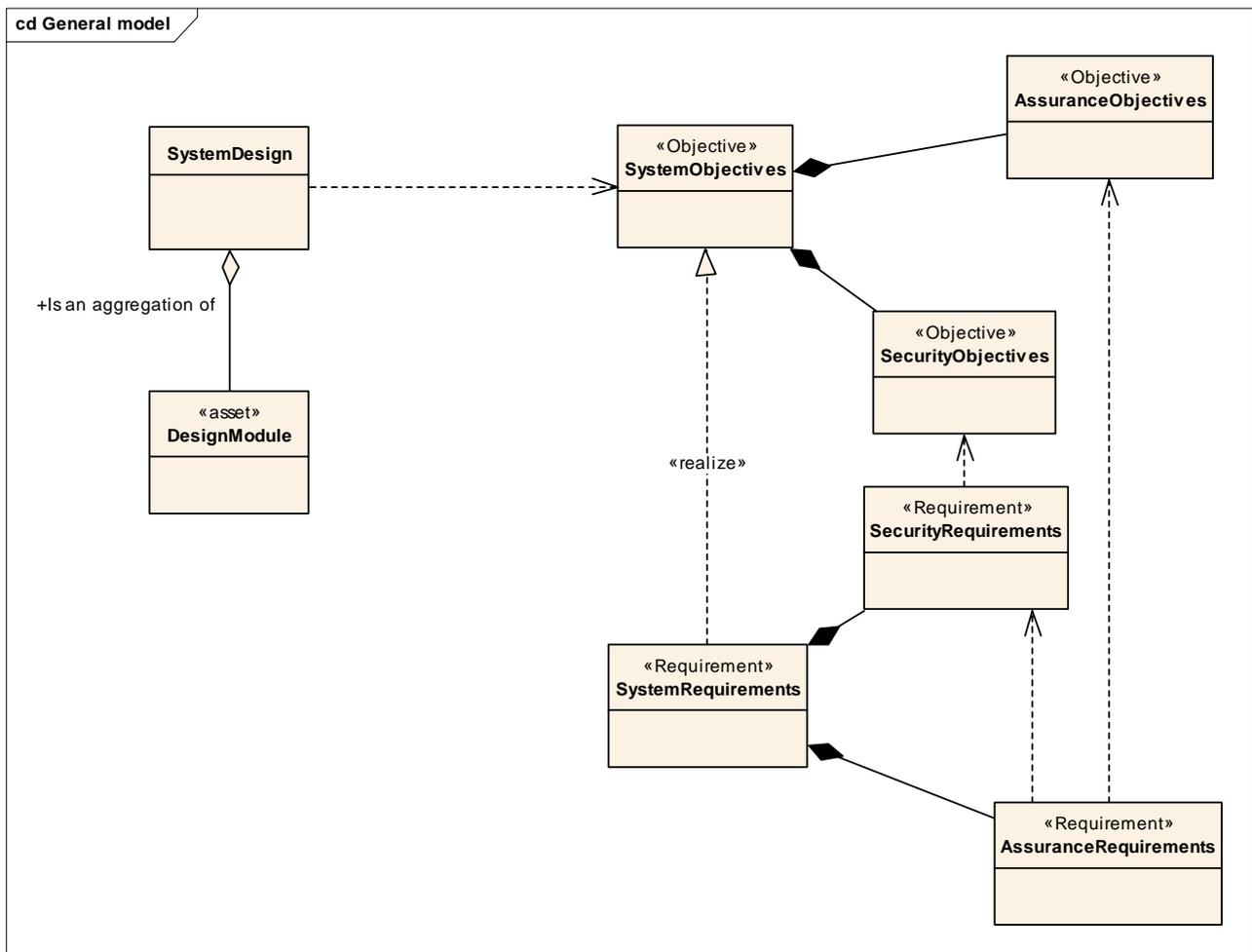


Figure 3: Relationship between system design, objectives and requirements

For most systems and in particular for the Next Generation Network (NGN) the development of system requirements goes far beyond just security and one concern for TVRA is to ensure that the system design is itself robust and therefore has fully documented requirements across all its aspects.

A TVRA requires that both the system being examined (with its catalogued objectives and requirements) and the assets of the system and how it fits to its environment are clearly identified. In the context of TVRA the key relationship is that between a vulnerability and an asset and this is a weighted relationship with the weighting being defined as the risk to the asset due to the associated vulnerability. A pictorial view of the asset-threat-weakness-vulnerability-countermeasure relationship to system design is given in figure 4.

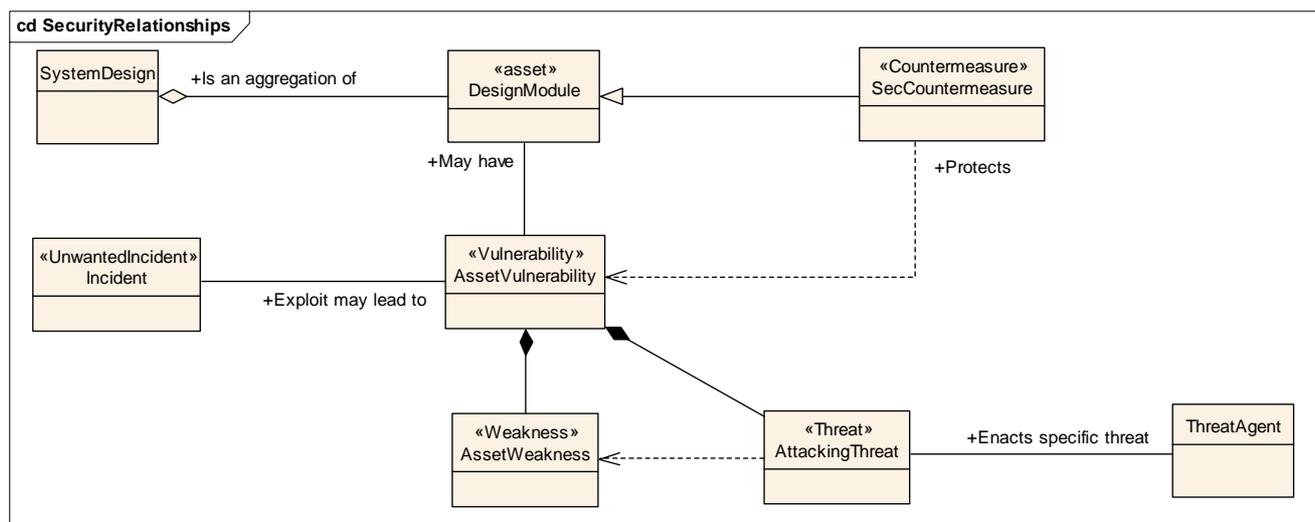


Figure 4: Generic security TVRA model

One of the purposes of security design is to minimize the probability of any instance of the class "unwanted incident" being instantiated. It should be noted that whilst some countermeasures may themselves become system assets, and as such have their own vulnerabilities, many instances of vulnerabilities will be considered as policies, system guidelines and, if captured early enough, system redesign.

The data types pertaining to the model in figure 4 are given in figure 5. Essentially threats can be classified as one of 4 types:

- Interception.
- Manipulation.
- Repudiation of sending.
- Repudiation of receiving.

Similarly the security objectives can be classified as one of 4 types:

- Confidentiality.
- Integrity.
- Accountability.
- Availability.

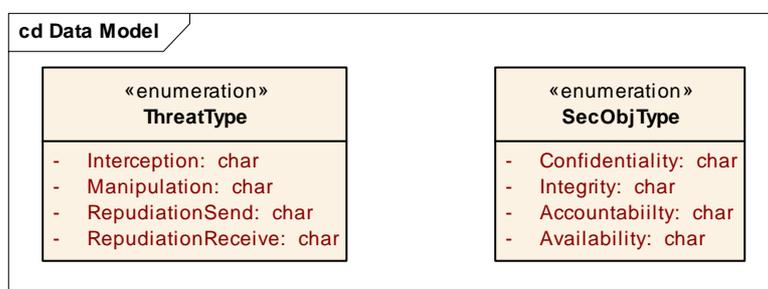


Figure 5: Data types pertaining to security relationship model

4.3 Countermeasure strategies

The goal of security design is to ensure a low likelihood of an unwanted incident arising. As the likelihood of an unwanted incident is dependent upon the presence of weakness in an asset and also the presence of both threats and threat agents that exploit the weakness it is the purpose of security systems to remove, or mask, the weaknesses of an asset. An essential non-technical component of security strategies is the management of the system and its human components. The non-technical measures are outlined in ISO/IEC 27001 [24] and in ISO/IEC 17799 [23].

The following strategies are considered within the present document:

- Asset redesign.
- Asset hardening.

4.3.1 Asset redesign

The assumption made prior to analysis is that all assets have weaknesses and the job of the analyst is to identify those weaknesses. Where weaknesses are found and have a large number of associated threats and threat agents there may be a possibility to redesign the asset in such a way as to remove the inherent weaknesses. The viability of this strategy will depend on a number of factors including the maturity of the asset design and the relative cost of redesign versus the cost of weakness masking through asset hardening.

4.3.2 Asset hardening

An asset may have some weaknesses that cannot be removed but which may be masked or made inaccessible by the addition of assets to the vulnerable asset such that the combination of assets presents a lower likelihood of attack and this presents a lower risk to the system.

4.4 Relationship with Common Criteria evaluation

The primary purpose of an ETSI TVRA is to support and rationalize security standardization, and to support and rationalize system design decisions, where the overall objective of the standard is to minimize risk of exploitation and attack of a compliant system when deployed. In order to consider this fully the TVRA method described in the present document addresses the impact of an attack on the system whereas ISO-15408 [13] primarily addresses the resistance to attack of the system. In this view the eTVRA method compliments ISO-15408 [13]. A particular objective of the TVRA method is to prepare the justifications for security decisions and that may as a result be referenced in a PP for the security feature.

The structure of the assurance class for vulnerability analysis described in ISO-15408 [13] is slightly different from the structure recommended for a TVRA in the present document, however the two approaches are considered complimentary.

Within a final common criteria evaluation [13] the vulnerability analysis assurance family assumes that the system design is complete whereas the purpose of the vulnerability analysis exercise in ETSI is to be able to identify vulnerabilities that require the provision of countermeasures, and then to assess the vulnerabilities that exist in the system with the countermeasures applied. The final documented TVRA may be used in the context of common criteria evaluation [13] to satisfy those aspects of evaluation found in sections (a), (b) and (c) of a protection profile (see ES 202 382 [3], clauses 5.1.2 through to 5.1.7).

Figure 6 (taken from EG 202 387 [1]) shows a simplified view of the relationships between the components of Common Criteria Protection Profiles (PP), Security Targets (ST) and Targets Of Evaluation (TOE)). The standardization process fits primarily in the "Consumer side" of the figure.

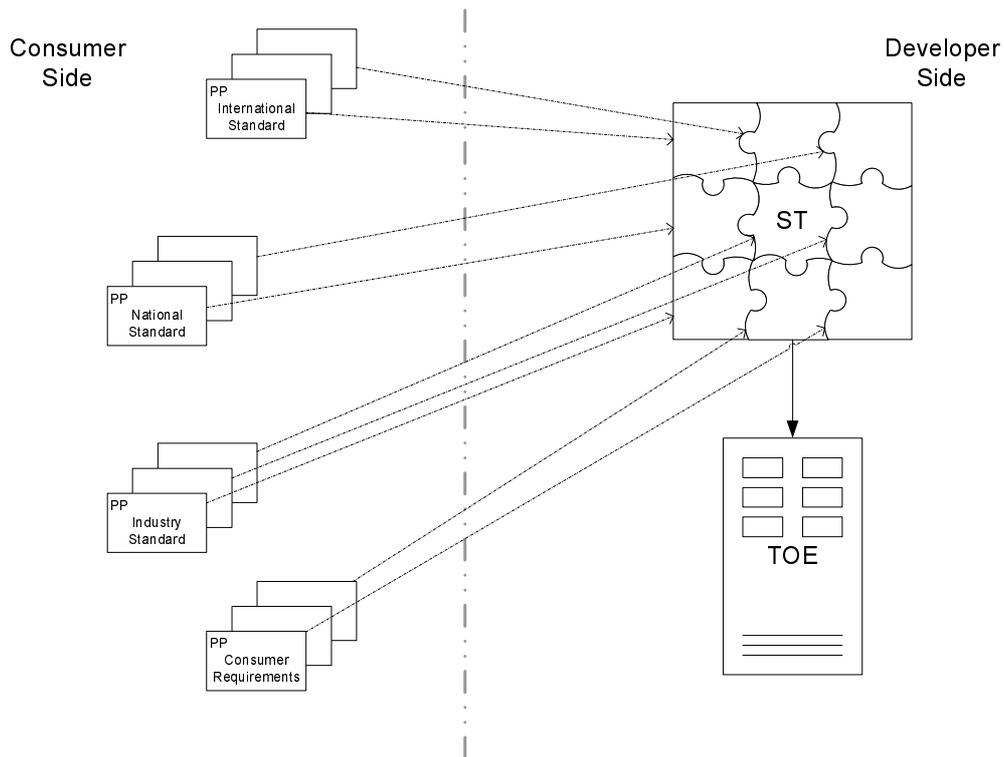


Figure 6: Relationship between PPs, STs and TOEs

5 eTVRA method

5.1 Overview

The eTVRA method involves a systematic identification of the unwanted incidents to be prevented in the system, and for the system itself, identifying the assets it is composed of and their associated weaknesses, the threats and the threat agents that will attack the system, before determining the risk to the system by modelling the likelihood and impact of attacks on the system's vulnerabilities.

The eTVRA method derives from the model shown in figure 4. The eTVRA models a system consisting of assets. An asset may be physical, human or logical. **Assets** in the model may have **Weaknesses** that may be attacked by **Threats**. A **Threat** is enacted by a **Threat Agent**, and may lead to an **Unwanted Incident** breaking certain pre-defined security objectives. A **Vulnerability**, consistent with the definition given in ISO/IEC 13335 [17], is modelled as the combination of a **Weakness** that can be exploited by one or more **Threats**. When applied, **Countermeasures** protect against **Threats** to **Vulnerabilities** and reduce the **Risk**.

The eTVRA method process consists of the following steps:

- 1) Identification of the objectives resulting in a high level statement of the security aims and issues to be resolved.
- 2) Identification of the requirements, derived from the objectives from step 1.
- 3) Inventory of the assets.
- 4) Identification and classification of the vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result.
- 5) Quantifying the occurrence likelihood and impact of the threats.
- 6) Establishment of the risks.
- 7) Identification of countermeasures framework (architecture).

Each step in the method has guidance attached to lead the analyst. In particular for step 5, which involves detailed calculations of the likelihood and impact values, the use of repeatable metrics is essential to the repeatability of the analysis over time. The metrics used in step 5 are developed from the guidance given in ETR 332 [5] and ISO/IEC 15408 [13]. One characteristic of the method is to include an evaluation of whether an attack exploiting a vulnerability can be automated thereby offering an additional metric to be used in assessing risk. The product of occurrence likelihood and impact values from step 5 gives a measure of the risk to the asset. A countermeasure will reduce the likelihood of the threat being successful and/or reduces its impact. This step results in a set of countermeasures to protect the vulnerabilities against threats. The application of countermeasures adds assets to the system and may create new vulnerabilities, indicating that the eTVRA will need to be executed again, and the method should be repeated until all the risks have been reduced to an acceptable level. Furthermore, by allowing the analysis to be rerun when attack likelihood changes, the risk to the system may be re-evaluated as knowledge of new or revised attacks becomes available.

It is recommended to use a database to store the system elements (assets), and to record threats, threat agents, weaknesses and vulnerabilities such that the analysis, and revisions of the analysis, can be recovered and redone regularly.

NOTE 1: The database is to be compiled by the analyst/designer. A sample database structure is provided in annex E.

The method systematically addresses those aspects of telecommunications systems covered by standardization and quantifies their assets, vulnerabilities and threats. The primary focus of the eTVRA is on the assets of a system and is required to ensure that they can perform their primary function when subjected to malicious attack. The output of the eTVRA is a quantified measure of the risks to the assets and a set of requirements that will minimize that risk.

For the purposes of analysis all assets are considered to have weaknesses.

In the eTVRA assets are identified and threats and weaknesses against them are identified. As a weakness may be present in a system for years before it is actually discovered it is clear that the eTVRA activity has to be considered over the long term. When weaknesses are discovered and published the risk to the system is increased, particularly where exploits for the weakness are also published.

NOTE 2: The term threat agent is used in the present document to refer to a specific means to enact a threat in order to exploit a weakness.

It should be noted that in some cases the existence of a countermeasure to a particular vulnerability will not automatically lead to its deployment. Some countermeasures have significant cost (in complexity, or in process) that may not be justified by the pre-deployed risk to the system or the resultant residual risk after deployment.

5.1.1 Target Of Evaluation description

In the context of ISO/IEC 15408-1 [10] there is a requirement to give a brief but clear description of the Target Of Evaluation (TOE). The purpose is to make the security aspects of the TOE clear. A similar approach has to be taken for a TVRA and the scope of the TVRA should be considered in the same way that a TOE is considered in ISO/IEC 15408-1 [10] and in the PP proforma defined in ES 202 382 [3]. However in the present document TOEs are not explicitly addressed, instead the analysis considers individual assets (or groups of assets) and how those assets are vulnerable and what unwanted incidents flow from attacking those assets. It is recognized that an attack on any asset may affect not only the asset but also the system in which the asset exists (the environment).

The TVRA target is described by its environment and whilst this is referred to by a PP needs to be made complete in the TVRA documentation itself.

5.1.1.1 Security environment

The security environment describes the security aspects of the environment in which the asset is intended to be used. It shall include:

- security assumptions:
 - the intended use of the implementation;
 - the physical, user and connection aspects of the environment in which an implementation will operate;
- assets:
 - the assets with which the asset under analysis will interact with;
 - the nature of the asset's interaction with other assets;
- threats and threat agents:
 - all threats against which specific protection is required within either the implementation of a standard or its expected environment;
 - the threat agents that will be used to enact the identified threats;
- organizational security policies:
 - any security policies or rules with which an implementation of a standard must comply.

The description of the security environment shall be tabulated following the format illustrated in the example.

NOTE: Where the eTVRA database is used the data is entered in a form similar to the example table and can be reported back in the tabular form given in the example.

EXAMPLE:

A Security Environment		
a.1 Assumptions		
TVRA-id	Summary text	Citation
a.1.1	ENUM is used to resolve a given telephone number (E.164 identity) to a known IP address	RFC TS 102 051 TR 102 055 [7]
a.1.2	ENUM runs over DNS	
..
a.2 Assets		
a.2.1	DNS records in Leaf server	
a.2.2	NAPTR record in Leaf server	
..
a.3 Threats		
a.3.1	Confidentiality	
a.3.2		
..
a.4 Threat agents		
a.4.2	overload of communication	
a.4.3		
..
a.5 Security policies (OPTIONAL)		
a.5.1		
a.5.2		

5.1.1.2 Security objectives

The eTVRA shall contain a definition of the security objectives of both the asset and its environment [10]. These objectives are expected to cover the assumptions, threats and policies described in the asset security environment (see clause 5.1.1.1). They should be expressed in broad terms rather than in detail and should be segregated into two distinct groups, thus:

- security objectives for the asset:
 - it should be clear which aspects of the identified threats and policies are addressed by each objective;
 - if the base security standard specifies a protocol, it is likely that the asset security objectives will be specified in the Stage 1 (or equivalent) specification;
- security objectives for the environment:
 - it should be clear which aspects of the identified threats and policies are expected to be addressed by the environment because they are not covered (either wholly or in part) by the asset security objectives;
 - communications standards rarely specify requirements for the environment so it is unlikely that the security objectives for the environment will be stated explicitly in the base security standard or any associated document.

EXAMPLE:

B Security Objectives		
b.1 Security objectives for the asset		
TVRA-id	Summary text	Citation
b.1.1	The asset must identify and authenticate all users before granting access to the system	
b.1.2		
..
b.2 Security objectives for the environment		

5.1.1.3 Security requirements

5.1.1.3.1 The relationship between security objectives and security requirements

The distinction between security objectives and security requirements is an important one to make. An objective is the expression of what a security system should be able to do in very broad terms whereas a requirement is a more detailed specification of how an objective is achieved. As an example, the following statement is a security objective for an asset.

EXAMPLE 1: The asset must identify and authenticate all users before granting access to the system.

One of the security requirements associated with this objective could be:

EXAMPLE 2: A user shall be successfully identified and authenticated to the asset by means of a user name and password before all other interactions between the asset and that user.

NOTE: It would not be unusual for a single objective to be realized by the implementation of more than one requirement nor for a single requirement to partially implement more than one objective.

5.1.1.3.2 Security requirements

Security requirements should be identified for both the asset and, where applicable, its environment [10]. The asset security requirements should be classified into the following groups:

- asset security functional requirements:
 - an identification of each of the security-related functional requirements specified in the base security standard and an indication of where in the standard the detailed requirement can be found;
 - where possible, in indication of which of the functional components defined in ISO/IEC 15408-2 [11] the requirement represents;
- asset security assurance requirements:
 - an indication of the Evaluation Assurance Level (EAL) [12] that an implementation of the base security standard could be expected to meet. As there are likely to be many implementations in a number of different application areas, the EAL requirement could be expressed as a range (e.g., EAL3 - EAL5);
 - where possible, an identification of any specific assurance components from ISO/IEC 15408-3 [12] which will apply to an implementation;
 - where necessary, a specification of any essential assurance requirements which are not included in ISO/IEC 15408-3 [12].

The specification of security requirements for the environment is optional and should only be included in the analysis if security objectives for the environment are identified earlier in the analysis (see clause 5.1.1.2). If requirements for the environment are included, they should be presented in the same way as functional requirements for the asset.

EXAMPLE:

C Security Requirements			
c.1 asset security requirements			
c.1.1 asset security functional requirements			
c.1.1.1	NGN R1 IMS authentication shall support early deployment scenarios (with support for legacy equipments).	FIA_UAU.3	TS 187 001 [9] clause 4.2, ISO/IEC 15408-2 [11] clause 11.4.2
c.1.1.1	In non-early deployment scenarios, IMS authentication shall be independent from access authentication.	FIA_UAU.3	TS 187 001 [9] clause 4.2, ISO/IEC 15408-2 [11] clause 11.4.2
..
c.1.2 asset security assurance requirements			
c.1.2.1			
..
c.2 Environment security requirements (OPTIONAL)			
c.2.1			

5.1.1.3.2.1 Interaction with ISO/IEC 15408 [13]

In the preceding clause it is recommended that where possible assurance and functional components from ISO/IEC 15408-2 [11] and ISO/IEC 15408-3 [12] should be identified. The guidance to the application of Common Criteria in ETSI deliverables, EG 202 387 [1], should be used as source material in this case. A summary of the relevant content of EG 202 387 [1] follows.

ISO/IEC 15408-2 [11] identifies a set of functional components which cover the major elements of any security product or process and these are defined in the following classes (ISO/IEC 15408-2 [11] component name in brackets):

- Security audit (FAU).
- Communication (FCO).
- Cryptographic support (FCS).
- User data protection (FDP).
- Identification and authentication (FIA).
- Security management (FMT).
- Privacy (FPR).
- Protection of the Target of Evaluation Security Functions (FPT).
- Resource utilization (FRU).
- Target of Evaluation access (FTA).
- Trusted path/channels (FTP).

The components can be used in the development of requirements at both an abstract level and at the detail development level.

The developer needs to be aware of the functional components and to report their use.

EXAMPLE: A countermeasure to prevent masquerade may require that the identity is presented and validated, then authenticated, prior to system access. To implement this countermeasure will require a design that includes components "User identification before action" and "User authentication before action" (FIA_UID.2 and FIA_UAU.2 respectively in ISO/IEC-15408-2 [11]).

When choosing which evaluation level components to add to the system design the guidance given in table 1 should be used as a starting point where additional analysis is to be found in EG 202 387 [1].

Table 1: Evaluation service level summary as specified in ISO/IEC 15408-3 [12]

Assurance class	Assurance family	Assurance components by EAL						
		1	2	3	4	5	6	7
Configuration management	CM automation (ACM_AUT)				1	1	2	2
	CM capabilities (ACM_CAP)	1	2	3	4	4	5	5
	CM scope (ACM_SCP)			1	2	3	3	3
Delivery and operation (see note)	Delivery (ADO_DEL)		1	1	2	2	2	3
	Installation, generation and startup (ADO_IGS)	1	1	1	1	1	1	1
Development	Functional specification (ADV_FSP)	1	1	1	2	3	3	4
	High level design (ADV_HLD)		1	2	2	3	4	5
	Implementation representation (ADV_IMP)				1	2	3	3
	TSF internals (ADV_INT)					1	2	3
	Low level design (ADV_LLD)				1	1	2	2
	Representation correspondence (ADV_RCR)	1	1	1	1	2	2	3
	Security policy modelling (ADV_SPM)				1	3	3	3
Guidance documents (see note)	Administrator guidance (AGD_ADM)	1	1	1	1	1	1	1
	User guidance (AGD_USR)	1	1	1	1	1	1	1
Life cycle support (see note)	Development security (ALC_DVS)			1	1	1	2	2
	Flaw remediation (ALC_FLR)							
	Life cycle definition (ALC_LCD)				1	2	2	3
	Tools and techniques (ALC_TAT)				1	2	3	3
Tests	Coverage (ATE_COV)		1	2	2	2	3	3
	Depth (ATE_DEP)			1	1	2	2	3
	Functional tests (ATE_FUN)		1	1	1	1	2	2
	Independent testing (ATE_IND)	1	2	2	2	2	2	3
Vulnerability assessment	Covert channel analysis (AVA_CCA)					1	2	2
	Misuse (AVA_MSU)			1	2	2	3	3
	Strength of TOE security functions (AVA_SOF)		1	1	1	1	1	1
	Vulnerability analysis (AVA_VLA)		1	1	2	3	4	4
NOTE: No output from ETSI standardization process.								

Annex F of the present document gives more information on the use of security requirements statements from ISO/IEC 15408-2 [11].

5.1.2 Threats and threat agents

Threats to a telecommunications system are fairly restricted and fall into a small set of easily identified operations. The means to enact these threats are conversely many and varied and it is the "agent of threat" that will take most time to identify and that is the source of the risk to the system.

Threats in telecommunications belong to one of the following groups (showing subclasses of each threat) as outlined in clause 4.2 and shown in a tree in figure 7:

- Interception
 - Eavesdropping:
 - A breach of confidentiality by unauthorized monitoring of communication.
- Manipulation
 - Masquerade ("spoofing"):
 - The pretence of an entity to be a different entity. This may be a basis for other threats like unauthorized access or forgery.
 - Loss or corruption of information:
 - The integrity of data (transferred) is compromised by unauthorized deletion, insertion, modification, reordering, replay or delay.

- Unauthorized access:
 - An entity accesses data in violation to the security policy in force.
- Forgery:
 - An entity fabricates information and claims that such information was received from another entity or sent to another entity.
- Repudiation
 - An entity involved in a communication exchange subsequently denies the fact.
- Denial of service
 - An entity fails to perform its function or prevents other entities from performing their functions.

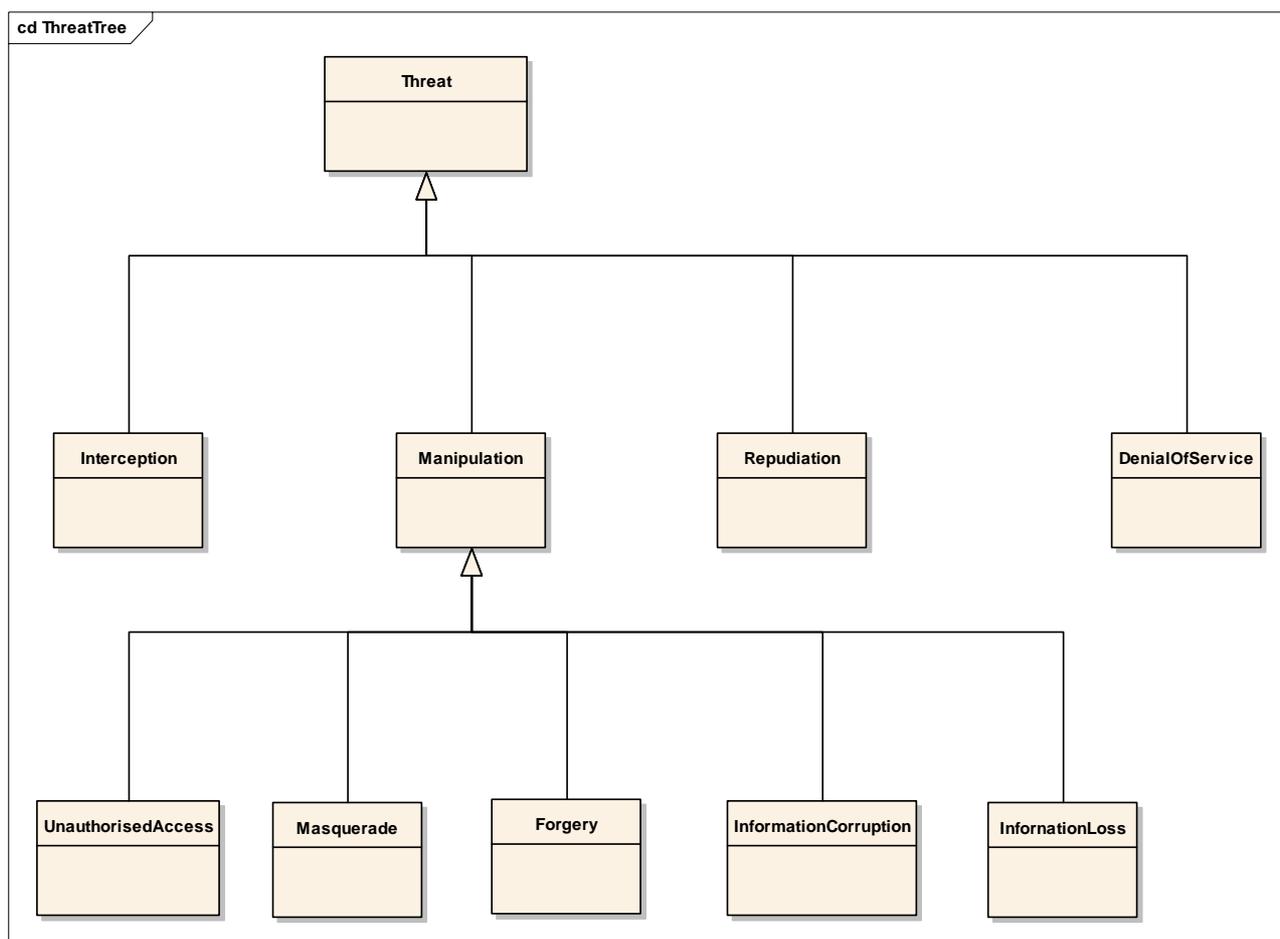


Figure 7: Threat tree

These threats counteract the identified main objectives as shown in table 1A.

Table 1A: Threats to security objectives

Threat	Objective			
	Confidentiality	Integrity	Accountability	Availability
Masquerade	X	X	X	X
Unauthorized access	X (within a system)	X (within a system)	X	X
Eavesdropping	X (on the line)			
Loss or corruption of information		X (on the line)	X	X
Repudiation			X	
Forgery		X	X	
Denial of service				X

5.2 Actors and roles

For the purpose of security standardization, only technical security countermeasures are considered, which means that relevant actors to consider are *users*. A user is defined as a person or process using the system in order to gain access to some system resident or system accessible service. Users can further be categorized dependent on whether they belong to the organization running the services (internal users) or whether they access the services as external users.

Each time a user accesses a service, the user will take on a role. In some cases there will be a one-to-one relationship between a user and a role, i.e. the user will always stay in the same role. In other cases there will be a one-to-many relationship between a specific user and the possible roles the user can play. This latter case is the normal telecommunications and ICT case in which the same user may act as a call initiator, call receiver, registrant, etc.

The following gives a high level classification of the most common roles:

- network operators (*private or public*);
- service providers (Bearer Service Providers or Value Added Service Providers);
- service subscribers/service customers;
- service end users;
- equipment/software vendors.

Some security measures may require actors to enforce the role of a Trusted Third Party (TTP). An important security issue is how these actors should be allowed to interact with each other in the context of the NGN.

5.2.1 Rationale

ISO/IEC 15408-1 [10] requires that a PP provides a rationale, subdivided into security objectives rationale and security requirements rationale to explain in detail how the security objectives and the security requirements, respectively, address the threats identified in the asset security environment. Providing this rationale is the purpose of the eTVRA and therefore the TVRA may be referred to in the PP as the source of the rationale. For the TVRA itself the tying together of objectives, requirement, threats and assets has the effect of acting as the rationale for the selection of the security architecture and the countermeasures.

EXAMPLE:

e Rationale

6 Method process

6.1 Overview

The method systematically identifies the assets and then for each asset establishes the weaknesses this asset may have, assesses how practical it is to attack this weakness and assesses the resulting risk.

For each step in this method a number of metrics are defined to assist the user of the method.

6.2 Step 1: Identification of objectives

The objectives for security are the essential starting point of the design. Should these objectives be unclear or *unconsciously* changing during the design process the system become more difficult (and hence expensive) to secure. Alternatively, if the objectives are not clear from the outset of the design important security aspects may be left unaddressed that may lead to costly incidents and/or repair operations.

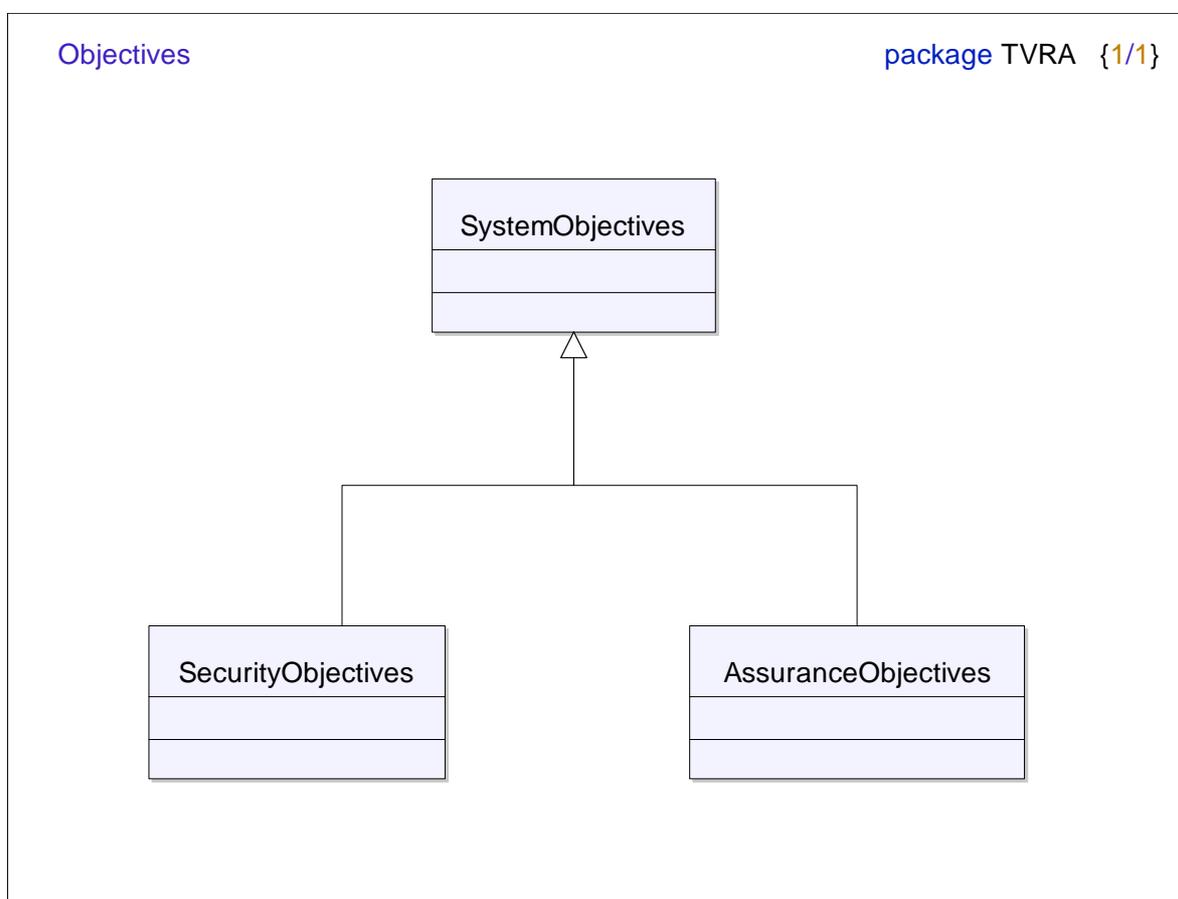


Figure 8: Hierarchy of objectives in a system design

As shown in figure 8 assurance objectives and security objectives are specializations of system objectives. Those characteristics of an objective that mark it out as a security objective are those that refer to one or more of the following system attributes:

- Authenticity.
- Confidentiality.
- Availability.
- Integrity.

Within the context of standardization there are a number of objectives for security that are intended to ensure availability of the network and customer confidence. These objectives break down to the following technical security issues for most telecommunications services:

- charging fraud;
- protection of privacy; and
- ensuring availability of the offered services.

The goals for telecommunications services should therefore aim to reduce these risks by reducing the ability to mount attacks that prevent the achievement of these objectives.

The following technical objectives for telecommunications services security hold:

- Prevention of masquerade
 - being able to determine that a user claiming to be Alice is always Alice, Bob is always Bob, and Bob cannot pretend to be Alice;
 - applies to both masquerade of the user and of the system or service.
- Ensure availability of the telecommunications services
 - the service must be accessible and usable on demand by an authorized entity.

NOTE: In general, a user expects to be able to place a call, and complete the call without being cut off in the middle.

- Maintain privacy of communication
 - where the parties to a call communicate across public networks mechanisms should exist to prevent eavesdropping;
 - the only delivery points for communication have to be the legitimate parties to the call.

6.3 Step 2: Identification of requirements

The system requirements are dependent on the system objectives identified in step 1 and have two specialisms shown in figure 9 identifying security and assurance requirement specialisms.

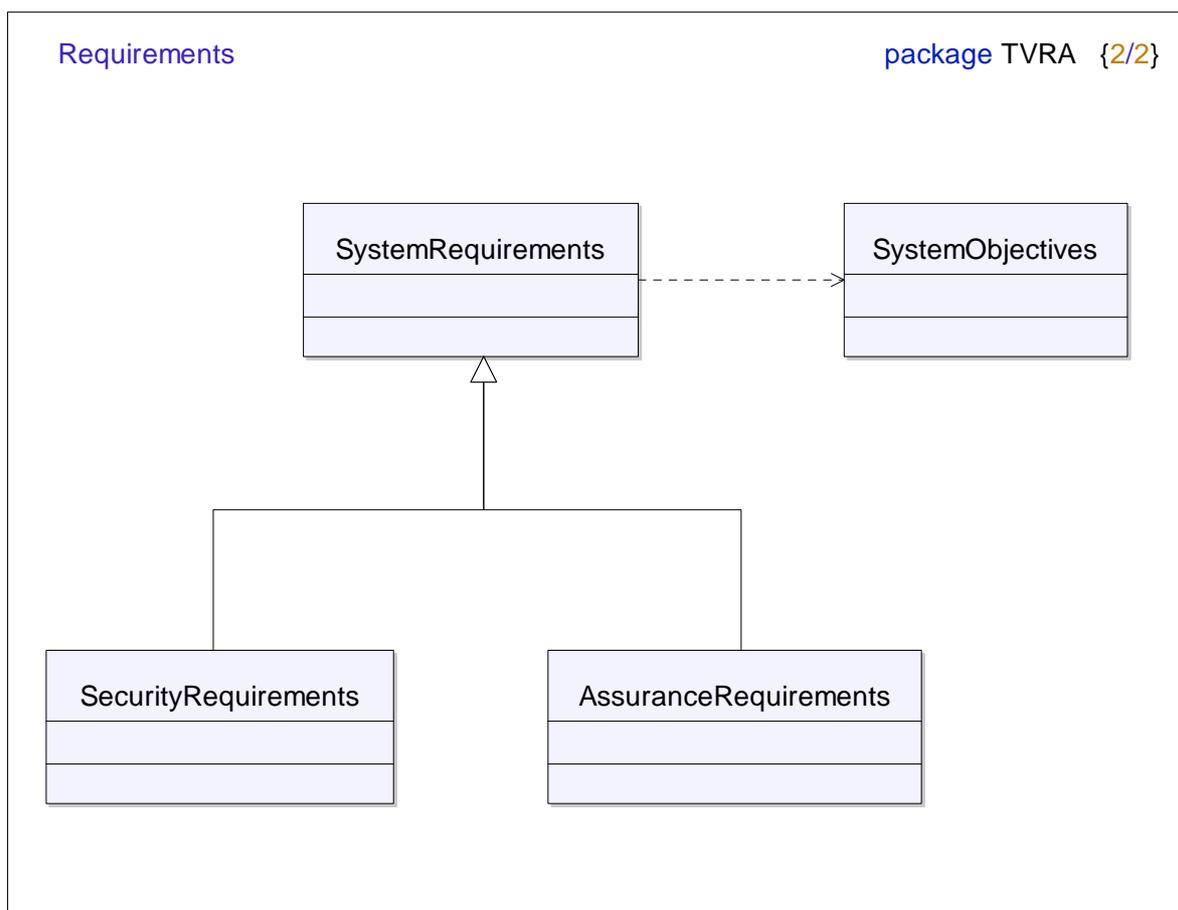


Figure 9: Dependency relationship between requirements and objectives

When building systems the use of ISO/IEC 15408-2 [11] functional capabilities offer a means to unambiguously state requirements. Annex G of the present document reviews the functional capabilities and how they fit to use in telecommunications.

6.4 Step 3: Systematic inventory of the assets

It is important to document the nature of any asset of the system and the complexity of the technology used in the construction of the asset and any information relating to the technology used in the asset that is available in the public domain. Between them these three aspects determine in large part the level of understanding of the asset.

The life expectancy of the asset is used in consideration of the time taken to develop and run an attack (develop a threat agent for a specific attack type). This may be affected by aspects such as the frequency with which a key or password is updated, and the duration in which the asset is expected to be in operational use.

NOTE: If an asset is protected by a key or password and the attack is based on key or password guessing then the frequency of key or password update may be a countermeasure.

Three kinds of **assets** are defined:

- physical assets
 - equipment;
- human assets; and
- logical assets
 - the information stored in and handled by the physical assets.

An asset is at **risk** when a weakness exists and a **viable threat** is present. The seriousness of the **vulnerability** depends on the **value** of the **asset** and the **likelihood** of the **weakness** to be exploited by the threat.

Systematic inventory of the assets requires a thorough evaluation of the system at hand. A first round of this evaluation should be performed by addressing typical scenarios appropriate to the system under discussion.

- Take a typical scenario.
- Analyze the physical assets by following the scenario.
- Analyze the human assets involved in the scenario.
- Analyze which logical assets exist in each of the physical assets.
- Analyze which logical assets are handled by the human assets.
- Consider other scenarios which may highlight different assets and repeat the process until no further assets are found.

When the system under discussion has multiple aspects, repeat this process for all aspects of the system until no more assets are found.

The use of UML use case diagrams, class diagrams and object diagrams may assist in the analysis of the system to identify the assets. If such methods are used the diagrams should be used in the analysis documentation.

The eTVRA database may be used to store the assets and the database definition (see annex E) contains a number of tables to store the definition of the asset and its relationship to other assets and to the system it is a member of.

In order to catalogue an asset the following attributes and relationships have to be identified:

- The system in which the asset resides.

NOTE 1: An asset may exist in more than one system and a system may contain many assets (a many to many relationship).

- The asset parent-child-sibling relationships if any exist.

NOTE 2: An asset may be a parent to one or more other assets and such relationships have to be captured. Similarly an asset may be a peer (sibling) to another asset and such relationships have to be captured.

An asset has a certain importance in the ToE. Each asset has to be rated by the impact when on the system when the asset is compromised by an attack is described. A metric for applying impact is defined in table 2.

Table 2: Impact

Value	Impact	Explanation
1	Low	The concerned party is not harmed very strongly; the possible damage is low.
2	Medium	The threat addresses the interests of providers/subscribers and cannot be neglected.
3	High	A basis of business is threatened and severe damage might occur in this context.

6.5 Step 4: Systematic identification of vulnerabilities

The systematic identification of vulnerabilities results in classification of all known vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result. For an attacker to exploit weaknesses in the asset an attack against the weakness has to be identified and developed. The presence of both the weakness and a plausible threat are modelled as vulnerabilities to a particular asset, or set of assets (see also the generic model given in figure 4).

For an attacker to exploit a vulnerability in the asset, the potential vulnerability must first be identified, the attack method then developed and finally the potential vulnerability exploited using the attack method. Each of these stages of determining whether there is a vulnerability in the asset must be considered when quantifying the factors comprising the attack potential.

6.5.1 Step 4.1: Identification of vulnerability

As part of the eTVRA possible Attack Interfaces need to be identified and all possible attacks need to be enumerated.

6.5.2 Step 4.a: identification of weakness

The weakness provides the attack interface (e.g. a low-powered server). A weakness leads to an unwanted incident as derived in step 2 and requires a certain system knowledge as described below.

6.5.2.1 Knowledge factor

The metric defined here is derived from those defined in clause B.4 of the Common Criteria Evaluation methodology [14] using the **weighted summation method** to calculate the overall attack potential.

Knowledge of the asset refers to specific expertise in relation to the asset. This is distinct from generic expertise, but not unrelated to it. Identified levels are as follows:

- **Public** information concerning the ASSET (e.g. as gained from the Internet).
- **Restricted** information concerning the ASSET (e.g. knowledge that is controlled within the developer organization and shared with other organizations under a non-disclosure agreement).
- **Sensitive** information about the asset (e.g. knowledge that is shared between discreet teams within the developer organization, access to which is constrained only to members of the specified teams).
- **Critical** information about the asset (e.g. knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need to know basis and individual undertaking).

The knowledge of the asset may graduate according to design abstraction, although this can only be done on a asset by asset basis. Some asset designs may be public source (or heavily based on public source) and therefore even the design representation would be classified as public or at most restricted, while the implementation representation for other assets is very closely controlled as it would give an attacker information that would aid an attack and is therefore considered to be sensitive or even critical.

Care should be taken here to ensure the highest level of knowledge of the asset required during identification, development and running of the potential vulnerability is identified.

6.5.3 Step 4.b: identification of attack method (threat agent)

A *threat agent* is an entity that can adversely act on assets [10]. In the eTVRA model, the *threat agent* is a model element that models the behaviour of the attacker. A *threat agent* exploits a vulnerability through e.g. a vulnerability port and/or an attack interface.

The threat agent provides the attack vector. A threat is part of a certain threat family which threaten one of the security objectives identified from step 1.

- **Confidentiality**, information is leaked that should have remained private.
- **Integrity**, information is altered that should have remained unaltered.
- **Availability**, the asset is less available than required.

The likelihood that a threat becomes a successful attack is determined by a number of factors that are defined and described in detail in the remainder of this clause.

6.5.3.1 Assessment of the practicality

To illustrate this, consider a potential vulnerability that is uncovered following months of analysis by an expert, but requires use of a simple attack method published on the Internet to exploit. Compare this with a potential vulnerability that is well known, but requires enormous time and resource to exploit.

When a vulnerability is identified by an evaluator, the evaluator must determine the attack potential associated with the vulnerability. The evaluator may have performed considerable analysis to identify the vulnerability. However, the evaluator must consider the effect of the vulnerability becoming publicly known. That is, an attacker would not have to repeat the analysis to identify the vulnerability, but would only have to perform the exploitation. In some instances knowledge of the vulnerability would not immediately facilitate exploitation because considerable further analysis would be required to permit the development of an attack method. For each of the assets identify potential and known weaknesses.

In direct attacks against probabilistic or permutational mechanisms, the issue of exploitation will normally be the most important, since potential vulnerabilities in these mechanisms will often be self evident, however this may not always be the case. With cryptographic mechanisms, for example, knowledge of subtle potential vulnerabilities may considerably affect the effectiveness of a brute force attack. Knowledge that users of a system tend to choose first names as passwords will have a similar effect. For vulnerability testing above AVA_VAN.1 (see ISO/IEC 15408-3 [12] and EG 202 387 [1] for further consideration of the Common Criteria Vulnerability Analysis Assurance class), the initial identification of potential vulnerabilities will become a much more important consideration, since the existence of difficult to uncover potential vulnerabilities may be promulgated, often rendering exploitation trivial.

The metrics defined here are derived from those defined in clause B.4 of the Common Criteria Evaluation methodology [14] using the **weighted summation method** to calculate the overall attack potential.

The following factors shall be evaluated during analysis to determine the weight of the attack potential required to exploit a vulnerability:

- Time.
- Expertise.
- Opportunity.
- Equipment.

6.5.3.2 Time factor

The role of time in evaluating the likelihood of an attack requires evaluation of the total amount of time taken by an attacker to identify that a particular, potential, weakness may exist, then to develop an attack method (threat agent) and to sustain effort required to mount the attack. When considering this factor, the worst case scenario should be used to estimate the amount of time required.

EXAMPLE: The time taken to identify a potential vulnerability may be the time taken to locate the potential vulnerability from information that is publicly available or may be the time required to analyse the design information to identify a potential vulnerability.

In addition to this time taken for identification, consideration of the time required to develop an attack method (which may also be publicly available) and successfully run the attack method on the asset to exploit the vulnerability must be included in this factor.

The following definitions apply (values escalate):

- within minutes means an attack can be identified or exploited in less than an hour;
- within hours means an attack can succeed in less than a day;
- within days means an attack can succeed in less than a week;
- within weeks means an attack can succeed in less than a month;
- in months means a successful attack requires in excess of a month.

6.5.3.3 Expertise factor

Specialist expertise refers to the level of generic knowledge of the underlying principles, product type or attack methods (e.g. Internet protocols, Unix operating systems, buffer overflows). The levels of expertise to be applied within this factor are defined as below:

- **Laymen** are not knowledgeable compared to experts or proficient persons, with no particular expertise.
- **Proficient** persons are knowledgeable in that they are familiar with the security behaviour of the product or system type.
- **Experts** are familiar with the underlying algorithms, protocols, hardware, structures, security behaviour, principles and concepts of security employed, techniques and tools for the definition of new attacks, cryptography, classical attacks for the product type, attack methods, etc. implemented in the product or system type.

When describing the expertise required, the total number of experts required must be included; the number of people for each type of expertise required and access to the expertise (dissemination) must be considered when describing the expertise required. Therefore, if expertise in both techniques for types of attack applicable to the asset and underlying algorithms and protocols is required, then the highest level of Specialist Expertise characterization should be assumed.

6.5.3.4 Opportunity factor

Opportunity is also an important consideration, and has a relationship to the Elapsed Time factor. Identification or exploitation of a vulnerability may require considerable amounts of access to an asset that may increase the likelihood of detection. Some attack methods may require considerable effort off-line, and only brief access to the asset to exploit. Access may also need to be continuous, or over a number of sessions.

For some assets the Window of opportunity may equate to the number of samples of the asset that the attacker can obtain. This is particularly relevant where attempts to penetrate the asset and undermine the TSP may result in the destruction of the asset preventing use of that asset sample for further testing, e.g. hardware devices. Often in these cases distribution of the asset is controlled and so the attacker must apply effort to obtain further samples of the asset.

For the purposes of this discussion unnecessary/unlimited access means that the attack does not need any kind of opportunity to be realized; easy means that access is required for less than a day or that the number of asset samples required to perform the attack is less than ten; moderate means that access is required for less than a month or that the number of asset samples required to perform the attack is less than fifty; difficult means that access is required for at least a month or that the number of asset samples required to perform the attack is less than one hundred; none means that the opportunity window is not sufficient to perform the attack (the length for which the asset to be exploited is available or is sensitive is less than the opportunity length needed to perform the attack -for example, if the asset key is changed each week and the attack needs two weeks).

Consideration of this factor may result in a determining that it is not possible to complete the exploit, due to requirements for time availability that are greater than the opportunity time.

6.5.3.5 Equipment factor

IT hardware/software or other equipment refers to the equipment required to identify or exploit a vulnerability.

- **Standard** equipment is readily available to the attacker, either for the identification of a vulnerability or for an attack. This equipment may be a part of the asset itself (e.g. a debugger in an operating system), or can be readily obtained (e.g. Internet downloads, protocol analyser or simple attack scripts).
- **Specialized** equipment is not readily available to the attacker, but could be acquired without undue effort. This could include purchase of moderate amounts of equipment (e.g. power analysis tools, use of hundreds of PCs linked across the Internet would fall into this category), or development of more extensive attack scripts or programs.
- **Bespoke** equipment is not readily available to the public as it may need to be specially produced (e.g. very sophisticated software), or because the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be very expensive.

Specialist expertise and knowledge of the asset are concerned with the information required for persons to be able to attack an asset. There is an implicit relationship between an attacker's expertise (where the attacker may be one or more persons with complementary areas of knowledge) and the ability to effectively make use of equipment in an attack. The weaker the attacker's expertise, the lower the potential to use equipment (IT hardware/software or other equipment). Likewise, the greater the expertise, the greater the potential for equipment to be used in the attack. Although implicit, this relationship between expertise and the use of equipment does not always apply, for instance, when environmental measures prevent an expert attacker's use of equipment, or when, through the efforts of others, attack tools requiring little expertise to be effectively used are created and freely distributed (e.g. via the Internet).

6.5.3.6 Intensity factor

The intensity of an attack may of itself be a factor in determining risk to the system or asset under attack. A metric for attack intensity is defined in table 3.

Table 3: Attack intensity metric

Intensity	
Metric value	Description
0	single
1	moderate
2	heavy

The intensity of an attack may be modified by use of: distributed threat agents (many sources of attack); reducing the time interval between attacks; or by combining these two.

In the simplest case for analysis a threat agent is assumed to operate at one place for one instance of an attack in any one time period (where even if the attack is repeated the interval between attacks is greater than the asset recovery time such that the attacks can be considered as discrete). For many attacks where manual processes need to be executed at a particular location (such as intercepting a physical line) this is an adequate point of view. In many practical implementations or deployments, including those considered in standards development, consideration only of the discrete attack may be insufficient for risk analysis. Assets are often automated and accessible via networks, and as threat agents are also assets, then so may the attacks be automated and network accessible.

In addition to automating an attack instances of discrete attacks may be published on the internet for downloading by those who are less skilled (and possibly less inhibited) to launch the attack (so called *script kiddies*). The scripted attack may be downloaded into other devices on the network (willing or unwilling agents of the attack) forming a robot network (BotNet).

Analysis for an attack where many thousands of attacks of this time happen concurrently from different locations on the network needs to be considered. The metric acknowledges 4 kinds of threat agents:

- 1) Manual Threat agents.
- 2) Scripted automated threat agents.
- 3) Controlled automated threat agents.
- 4) Autonomous automated threat agents.

The automated agents are discussed in more detail below and the relationships shown in figure 10.

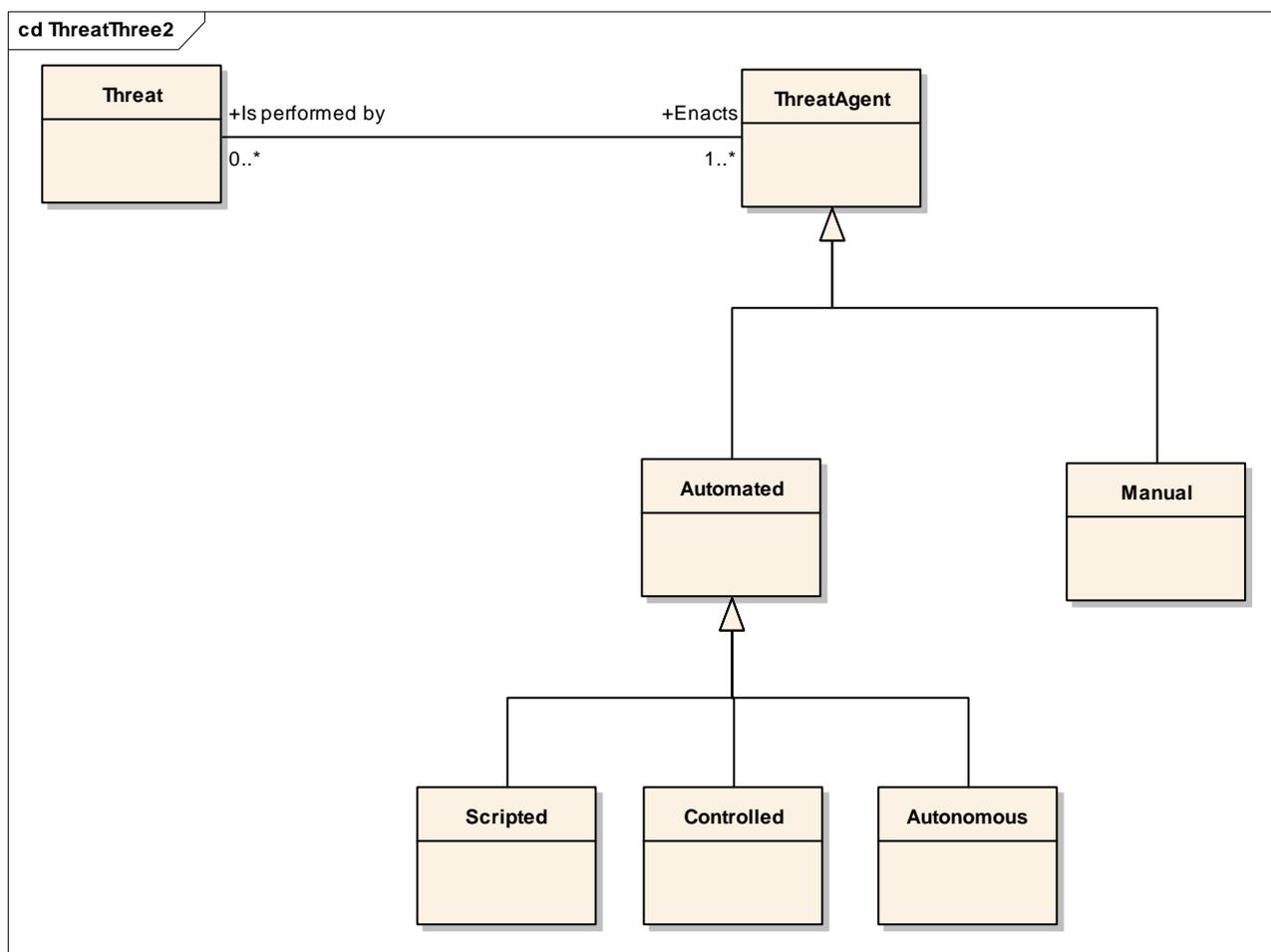


Figure 10: Specializations of threat agent

- Scripted attacks
 - An attack that is automated and then distributed over the Internet will allow people with a lower expertise (*script kiddies*) and generic PC hardware to mount the attack.
 - The impact of such automated threat is that people with lower expertise but not the lowest will be able to launch this attack. So an attack that may be automated will lower the Expertise Level, System Knowledge, Time and Equipment ratings to that of executing the scripted attack.

NOTE: This explicitly removes the time it may take to develop the attack from the evaluation of the likelihood metric.

- Controlled threat agents (BotNet)
 - If an attack is automatable and requires no interaction from the user *after starting* the impact of the attack (and thus its risk) may be further raised by a coordinated issuing of multiple instances of the attack. For example an attack may be uploaded to a so-called BotNet (Robot network) comprising 10 000-25 000 nodes. These networks are usually used for Distributed Denial of Service (DDoS) attacks but other uses for such concentrated attacks may also be conceived.
 - An attack that may be automated so that it may run without user intervention will lower the Expertise Level, System Knowledge and Equipment ratings to that of executing the distributed scripted attack. (So when it becomes easier to run a botnet, this will impact all threats that fall in this category). Furthermore the Impact will be raised to that of all nodes executing the attack in the worst possible way (either concurrently or sequentially).
- Autonomous automated threat agents (Worm/Virus)
 - If an attack is automatable and requires no interaction from the user *to start* one may include the attack into a worm or a virus. One may not have direct control over the execution of the attack but it may be released based on clock time or time after infection or even an external event such as certain key-word on the main page of a publicly available website.
 - By itself this type of attack would have all the risk ratings associated with the botnet attack but its rating takes the larger number of attack agents into account.
 - This type of automated attack may be issued from most of the Internet but also may penetrate supposedly closed networks.
- Automated attacks on protected networks
 - Automated attacks that may be put into a worm or virus may work their way into protected/closed networks. They may lay dormant until they are on a machine with a certain IP range or domain name and may then execute their attack. Infected bearers (for example computers or memory keys) may be carried into the secure facility and may thus bring the attack into the protected network.
 - In this case the fact that the attack may be automatable also has an impact on supposedly closed networks. This type of attack will therefore have all the impact of a distributed automated attack and will impact the access description to Moderate.

When a threat is deemed to be automatable the likelihood parameters are updated to the *minimum* of the value of the base vulnerability and the appropriate values of the automated threat indicated.

Table 4: Worst-case values for automated threats

Name	Expertise Description	Access Description	System Knowledge	Equipment Description	Impact
Manual	Expert	Not exploitable	Critical	Bespoke	Single
Script	Proficient	Not exploitable	Public	Standard	Single
ControlBot	Proficient	Not exploitable	Public	Standard	Moderate
AutoWormVirus	Proficient	Moderate	Public	Standard	Heavy

6.6 Step 5: Calculation of the likelihood of the attack and its impact

Each of the attack factors are summed (i.e. Time + Expertise + Knowledge + Opportunity + Equipment) to give an overall attack potential rating as shown in table 5. The attack potential rating is then mapped to the Occurrence likelihood as shown in table 7.

Table 5: Attack potential

Factor	Range	Value
Time (1 point per week)	≤1 day	0
	≤ 1 week	1
	≤ 1 month	4
	≤ 3 months	13
	≤ 6 months	26
	> 6 months	See note 1
Expertise	Layman	0
	Proficient	2
	Expert	5
Knowledge	Public	0
	Restricted	1
	Sensitive	4
	Critical	10
Opportunity	Unnecessary / unlimited access	0
	Easy	1
	Moderate	4
	Difficult	12
	None	See note 2
Equipment	Standard	0
	Specialized	3
	Bespoke	7
NOTE 1: Attack potential is beyond high.		
NOTE 2: Attack path is not exploitable.		

Table 6: Vulnerability rating

Range of values	Resistant to attacker with attack potential of:
0 to 2	No rating
3 to 6	Basic
7 to 14	Moderate
15 to 26	High
> 26	Beyond high

The method for threat analysis defined in ETR 332 [5] combines the likelihood with the impact of the attack in determining if a countermeasure should be applied. The form of countermeasures can include redesign of the at risk element in the system to remove the vulnerability that is to be attacked, and application of a defensive system component that masks the vulnerability.

Table 7: Mapping of vulnerability rating to likelihood of attack

Vulnerability rating	Likelihood
Beyond high	Unlikely
High	
Moderate	Possible
Basic	Likely
No rating	
NOTE: Motivation is not considered explicitly in the vulnerability rating.	

6.7 Step 6: Establishment of the risks

For each of the assets in the system under study one can identify their vulnerabilities and corresponding threats and weaknesses. For each vulnerability the likelihood should be computed as described in the clause above. For each asset the risk associated with each vulnerability should be computed.

6.7.1 Impact of intensity

The intensity factor defined above applies to the Asset Impact-value as defined in clause 6.4.

Table 8: Impact of attack intensity

Intensity Impact		
Asset Impact	Threat Intensity	Resulting Impact
1	0	1
1	1	2
1	2	3
2	0	2
2	1	3
2	2	3
3	0	3
3	1	3
3	2	3

6.7.2 Classification of risk

6.7.2.1 Overview

Risk is defined in ETSI standards as the product of the likelihood of an attack and the impact of the attack on the system.

The likelihood of a threat occurring may be estimated with values from 1 to 3 as explained in table 9 (Occurrence likelihood).

Table 9: Occurrence likelihood

Value	Likelihood of occurrence	Explanation
1	Unlikely	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to state the threat or the motivation for an attacker is very low.
2	Possible	The technical requirements necessary to state this threat are not high and could be solved without significant effort; furthermore, there is a reasonable motivation for an attacker to perform the threat.
3	Likely	There are no sufficient mechanisms installed to counteract this threat and the motivation for an attacker is quite high.

The impact of a threat is also estimated with values from 1 to 3 as explained in table 2.

The product of occurrence likelihood and impact value as defined in clause 6.6 gives the risk which serves as a measurement for the risk that the concerned asset is compromised. The result is classified into three categories as shown in table 10.

Table 10: Risk

Value	Risk	Explanation
1, 2, 3	Minor	No essential assets are concerned, or the attack is unlikely. Threats causing minor risks have no primary need for counter measures.
4	Major	Threats on relevant assets are likely to occur although their impact is unlikely to be fatal. Major risks should be handled seriously and should be minimized by the appropriate use of countermeasures.
6, 9	Critical	The primary interests of the providers and/or subscribers are threatened and the effort required from a potential attacker's to implement the threat(s) is not high. Critical risks should be minimized with highest priority.

NOTE: Because risk is calculated as the product of likelihood and impact the values 5, 7 and 8 cannot occur.

A summary of the data types used in this analysis is given in figure 11.

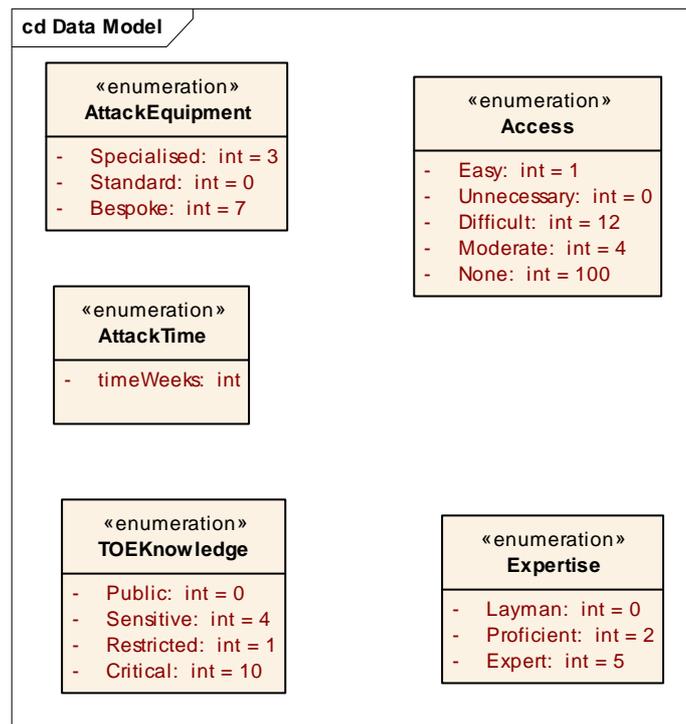


Figure 11: Data types in attack potential calculation

6.8 Step 7: Security countermeasure identification

Security Countermeasures are assets that are added to the system to reduce the weighted risk to the system. The purpose of countermeasures is to reduce either the likelihood of an attack or to the impact attack. Security countermeasures are modelled in the eTVRA as instances of assets and whilst primarily logical may also be human or physical.

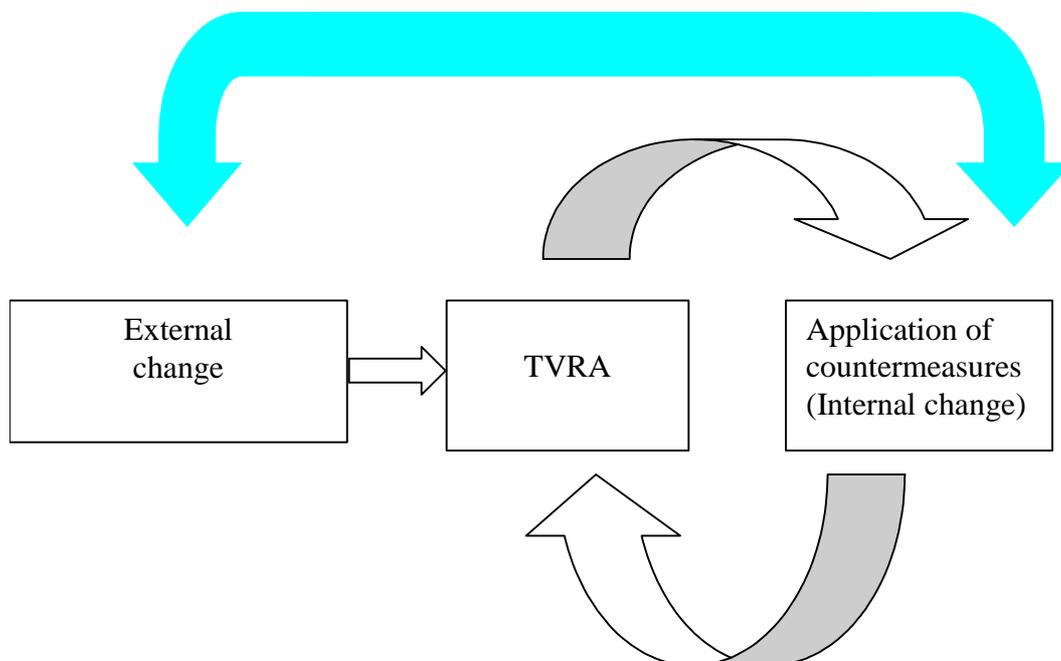


Figure 12: Cyclical nature of TVRA

Figure 12 shows that countermeasures are added as internal changes to the system and require that the TVRA process is repeated. This should continue either until no further countermeasures are applied (indicating stability in the system).

NOTE 1: The eTVRA method does not provide an automated means of identifying countermeasures.

NOTE 2: Some countermeasures may be inferred by inspection of the security requirements.

6.8.1 Countermeasures in the system

Where a countermeasure has been defined as is implemented as a logical asset it will require to be deployed in a corresponding physical assets (e.g. a firewall rule requires a firewall). The countermeasures and their supporting physical assets will bring their own vulnerabilities.

NOTE: When using the eTVRA database as defined in annex E it is possible to replicate systems and to add countermeasures only to the new replicate thus allowing comparison of systems with and without countermeasures, or with different countermeasure configurations.

6.8.2 Composite countermeasures applied to the system

More than one countermeasures may be applied against a single threat agent, or to protect a single asset. In such case the residual risk is only identified by re-performing the eTVRA.

6.8.3 Impact of countermeasures applied to the system

The impact of countermeasures on the overall risks analysis takes a similar approach as the automated threat agents. In this case the least likely of the two values is taken for each of the likelihood parameters. The impact of the countermeasures on the impact is similarly calculated by taking the least impact. This calculation is applied after the impact of automated threat agents.

Annex A (normative): TVRA proforma

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the TVRA definition proforma in this annex so that it can be used for its intended purposes and may further publish the completed TVRA definition.

A Security Environment			
a.1 Assumptions			
a.1.1	<i>Text of assumption</i>		<i>Citation for full text</i>
a.1.2			
a.2 Assets			
a.2.1	<i>Short text describing asset</i>		<i>Citation for full text</i>
a.2.2			
a.3 Threat agents			
a.3.1	<i>Short text describing threat agent</i>		<i>Citation for full text</i>
a.3.2			
a.4 Threats			
a.4.1	<i>Short text describing threat</i>		<i>Citation for full text</i>
a.4.2			
a.5 Security policies (OPTIONAL)			
a.5.1	<i>Short text describing security policy</i>		<i>Citation for full text</i>
a.5.2			
B Security Objectives			
b.1 Security objectives for the asset			
b.1.1	<i>Short text describing objective for the asset</i>		<i>Citation for full text</i>
b.1.2			
b.2 Security objectives for the environment			
b.2.1	<i>Short text describing objective for the requirement</i>		<i>Citation for full text</i>
b.2.2			
C IT Security Requirements			
c.1 asset security requirements			
c.1.1 asset security functional requirements			
c.1.1.1	<i>Short text describing security functional requirement</i>	<i>ISO15408 [16] class</i>	<i>Citation for full text</i>
c.1.1.2			
c.1.2 asset security assurance requirements			
c.1.2.1	<i>Short text describing security assurance requirement</i>	<i>ISO15408[16] class</i>	<i>Citation for full text</i>
c.1.2.2			
c.2 Environment security requirements (OPTIONAL)			
c.2.1	<i>Short text describing security environment requirement</i>	<i>ISO15408[16] class</i>	<i>Citation for full text</i>
c.2.2			
D Application notes (OPTIONAL)			
E Rationale			
<i>The eTVRA should define the full rationale, if this is true only a citation (reference) to the full text is required</i>			

Annex B (informative): The role of motivation

A full critique of the role of motivation in attacking a system when viewed in the context of Common Criteria evaluation can be found in clause B.4.1.1 of the Common Criteria Evaluation methodology [14]. In the present document motivation is addressed in broadly similar terms as a factor in determining attack potential.

Motivation can be used to describe aspects both of the attacker, and of the system (assets) he is attacking. The following key criteria may be considered when evaluating motivation:

- The likelihood of an attack
 - If a threat is highly motivated an attack can be considered imminent, with a corollary of.
 - If a threat is unmotivated no attack can be anticipated.
- The value of the asset, monetarily or otherwise, to either the attacker or the asset holder
 - An asset of very high value is likely to motivate an attack, with a corollary of.
 - An asset of little value is unlikely to motivate an attack.
- The expertise and resources with which an attacker is willing to effect an attack
 - A highly motivated attacker is likely to acquire sufficient expertise and resources to defeat the measures protecting an asset, with a corollary of.
 - An attacker with significant expertise and resources is not willing to effect an attack using them if the attacker's motivation is low.

In each case there is no probabilistic means of determining the role of motivation in mounting an attack. However in assessing threat potential it is essential to consider motivation in order to minimize the effect of motivation on the attacker.

Annex C (informative): Example TVRA for use of ENUM in NGN

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 [7]. 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 [8] 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 [27] and RFC 3403 [28] 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.

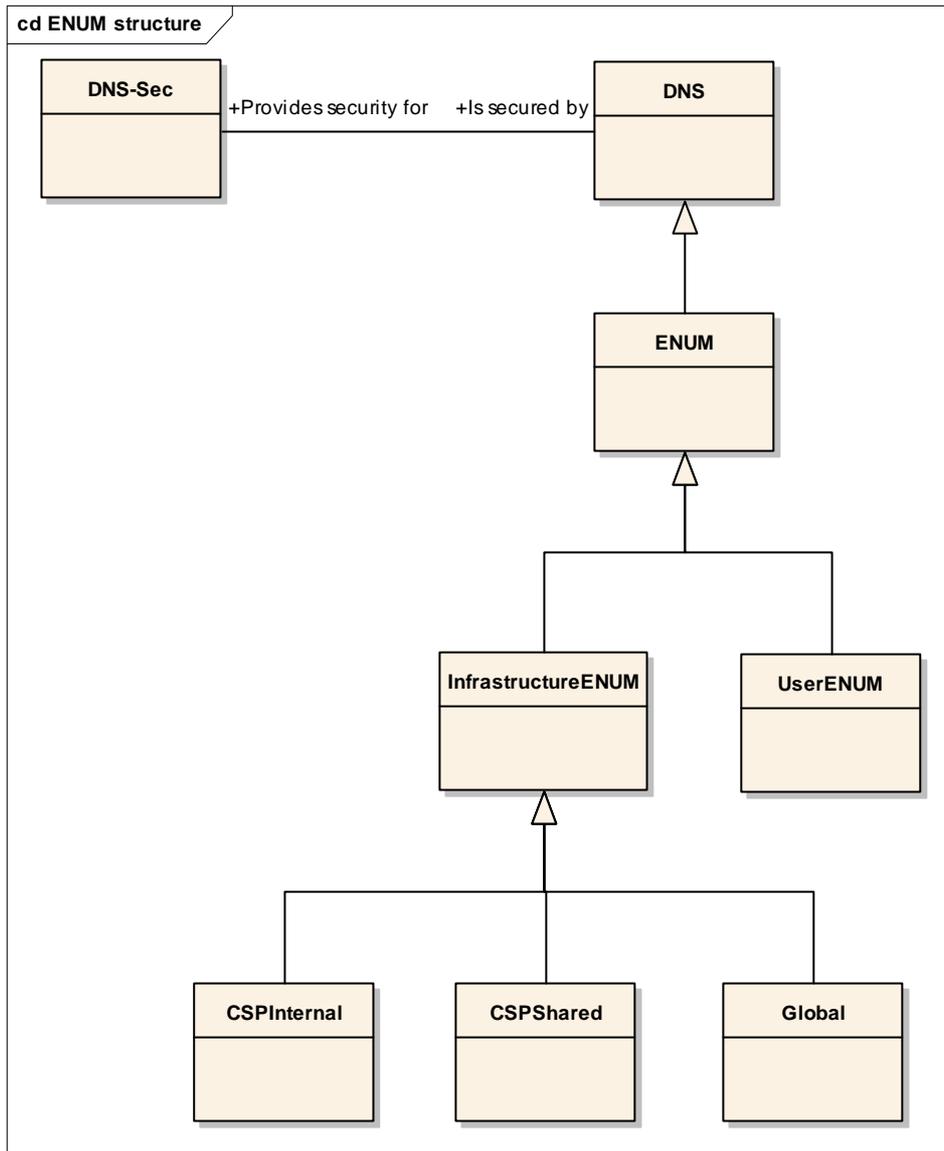


Figure C.1: Hierarchical structure of ENUM showing increasing generalization at top

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.

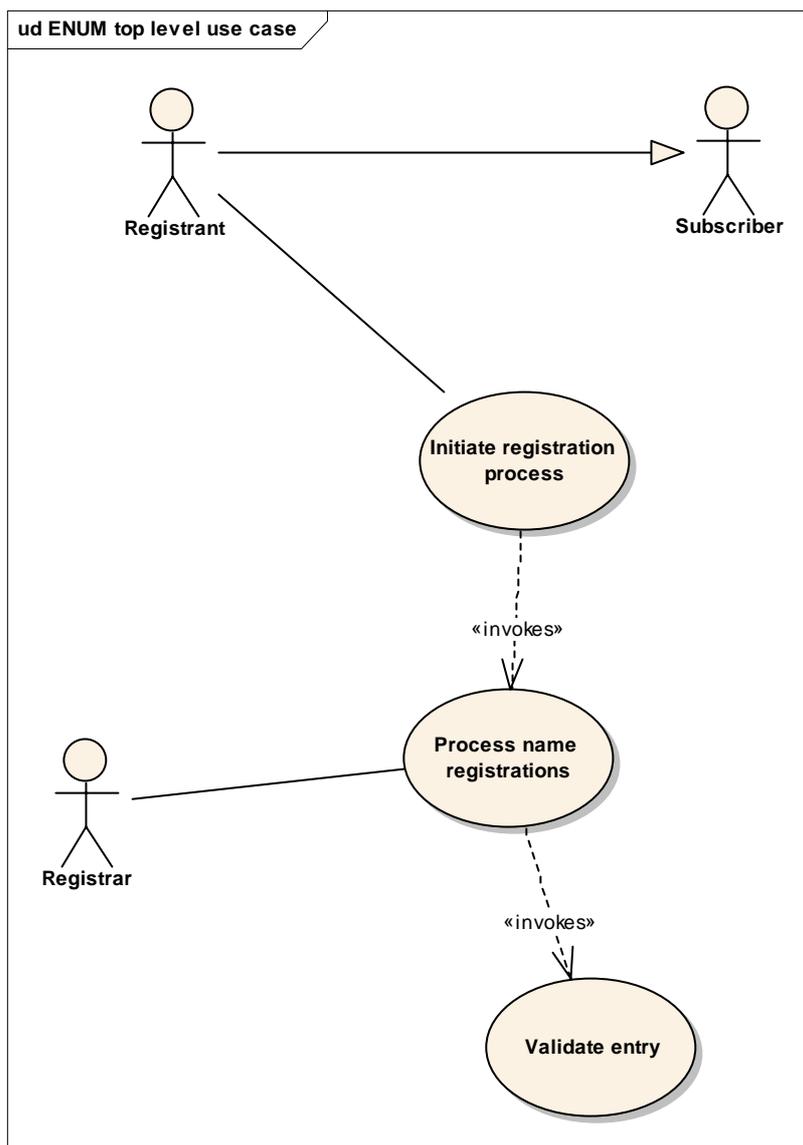


Figure C.2: Main actors and use cases in ENUM

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.

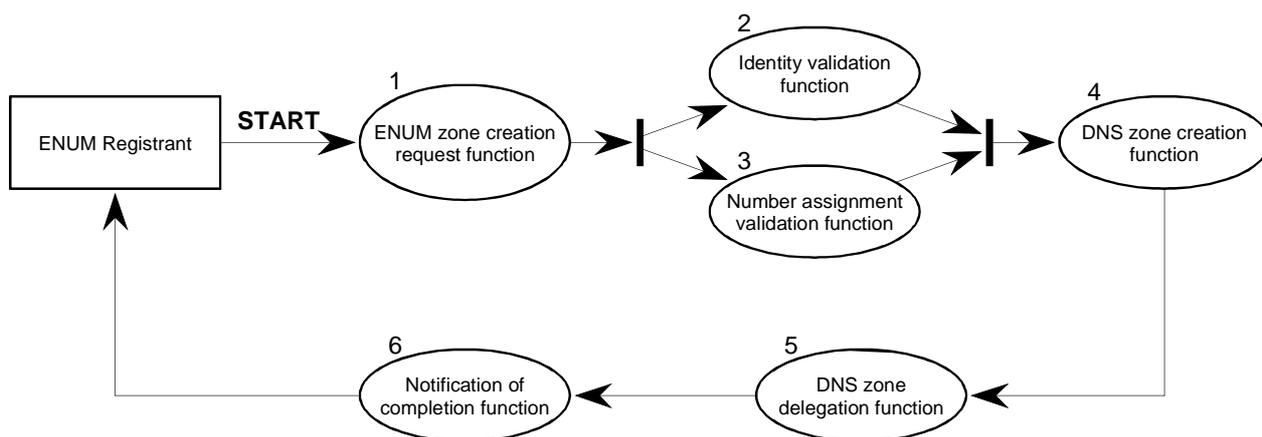


Figure C.3: Functional model for Registration

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).

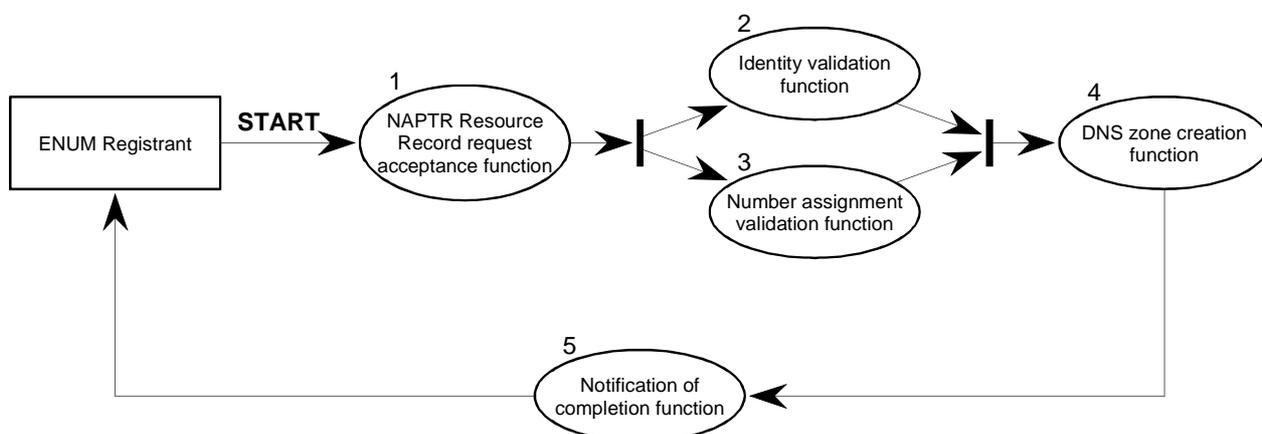


Figure C.4: Functional model for amendment of NAPTR Resource Records in Tier 2 database

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.

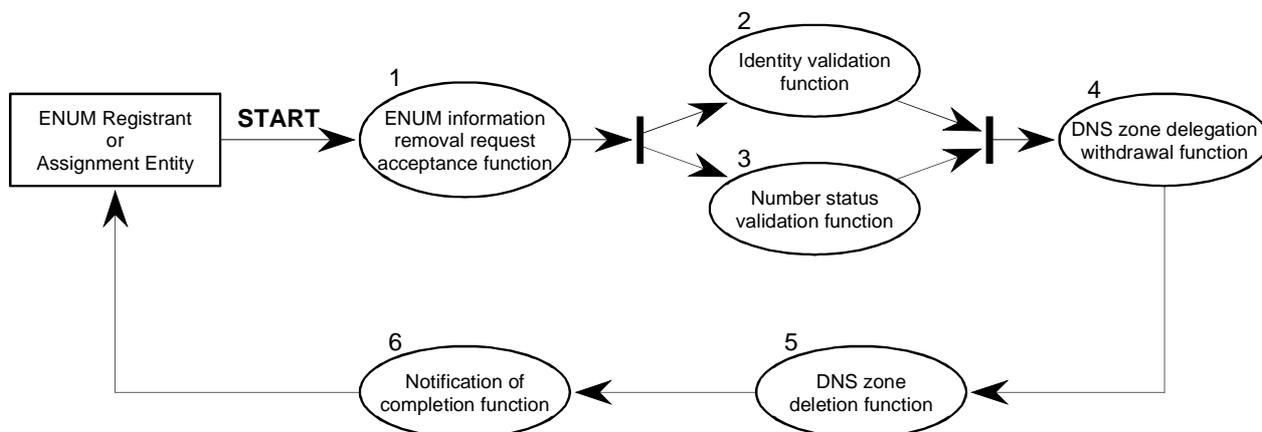


Figure C.5: Functional model for removal of E.164 numbers from ENUM databases

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 [29] 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 [26] 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 [30], [32], [31] 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 [9]) does not explicitly identify security requirements for ENUM or for the use of DNS. Detail security requirements referred to ISO/IEC 15408 [13] functional capabilities are defined in TR 102 420 [8] and summarized below.

Table C.2: Security concern classification from RFC 3761 [27]

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.
Integrity and Availability	Authenticated denial of Domain Names	The placing of a malicious entry into the database to ensure that calls cannot be completed for the user.
	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.

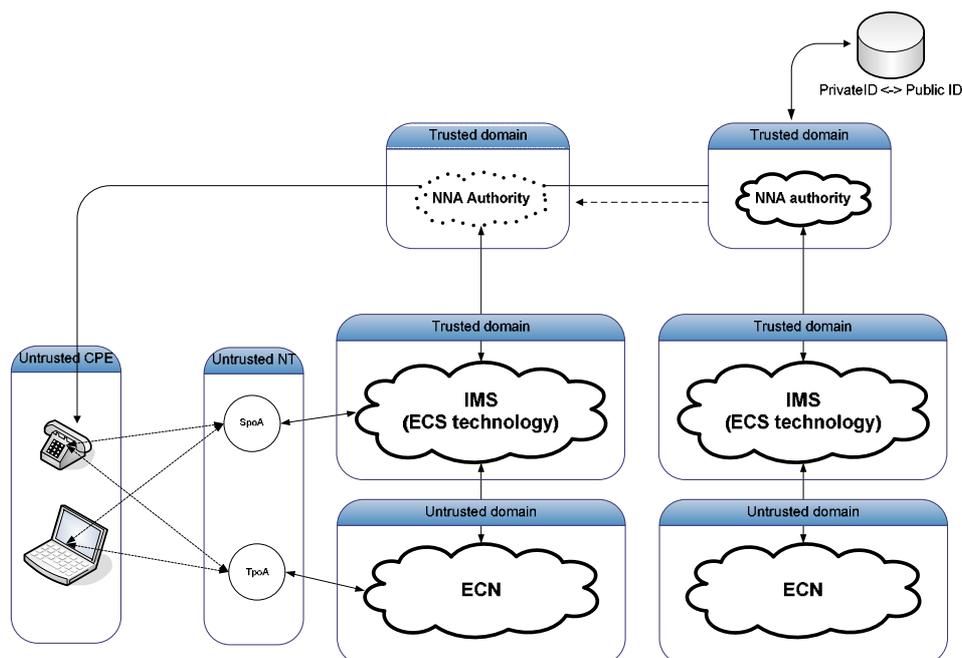


Figure C.6: NNA provisioning scenario

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.

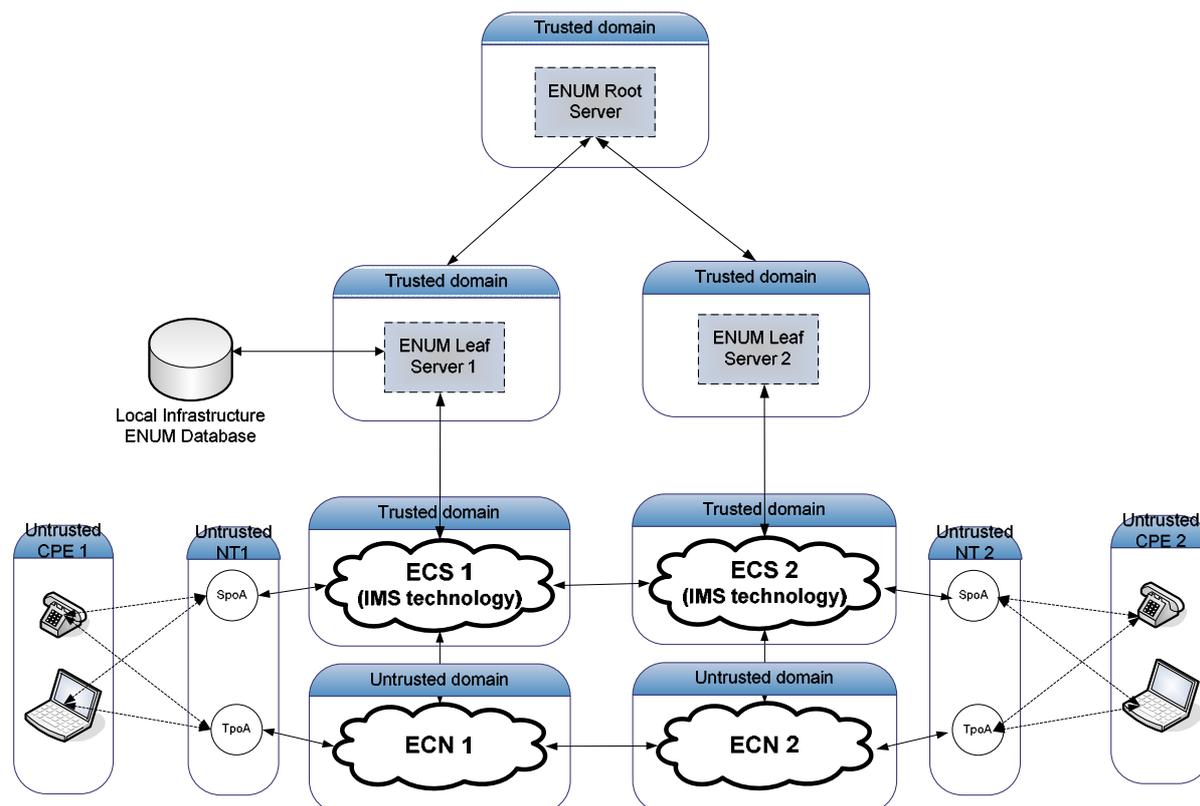


Figure C.7: Signalling scenario

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, eg 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 (R 102 055 [7]), 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 and RFC 3403 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 SIP
25	SIP message	RFC 3261 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, eg smartphone)	(NONE)
62	TCP/IP packet	(NONE)
63	UDP/IP packet	(NONE)
64	RTP packet	(NONE)
A.3 Threat agents		
1	DNS cache poisoning	<i>Citation for full text</i>
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 (rogue 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 (rogue 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	<i>Short text describing threat</i>	<i>Citation for full text</i>
a.4.2		
a.5 Security policies (OPTIONAL)		
a.5.1	<i>Short text describing security policy</i>	<i>Citation for full text</i>
a.5.2		
B Security Objectives		
b.1 Security objectives for the asset		
b.1.1	<i>Short text describing objective for the asset</i>	<i>Citation for full text</i>
b.1.2		
b.2 Security objectives for the environment		
b.2.1	<i>Short text describing objective for the requirement</i>	<i>Citation for full text</i>
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 <i>Citation for full text</i>

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	<i>Short text describing security assurance requirement</i>	<i>ISO15408 [16] class</i>	<i>Citation for full text</i>
c.1.2.2			
c.2 Environment security requirements (OPTIONAL)			
c.2.1	<i>Short text describing security environment requirement</i>	<i>ISO15408 [16] class</i>	<i>Citation for full text</i>
c.2.2			
D Application notes (OPTIONAL)			
E Rationale			
<i>The eTVRA should define the full rationale, if this is true only a citation (reference) to the full text is required</i>			

Annex D (informative): Denial of service attacks

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include:

- attempts to "flood" a network, thereby preventing legitimate network traffic;
- attempts to disrupt connections between two machines, thereby preventing access to a service;
- attempts to prevent a particular individual from accessing a service;
- attempts to disrupt service to a specific system or person.

Not all service outages, even those that result from malicious activity, are necessarily denial-of-service attacks. Other types of attack may include a denial of service as a component, but the denial of service may be part of a larger attack.

Illegitimate use of resources may also result in denial of service.

Denial-of-service attacks come in a variety of forms and aim at a variety of services. There are three basic aims of the attacker:

- To cause consumption of scarce, limited, or non-renewable resources.
- To lead to destruction or alteration of configuration information.
- To cause physical destruction or alteration of network components.

D.1 DDoS Attacks viable on the NGN

D.1.1 Land

In Land attacks, the attacker sends the victim a TCP SYN packet that contains the same IP address as the source and destination addresses. Such a packet completely locks the victim's system.

D.1.2 SYN Flood

A SYN flood attack occurs during the three-way handshake that marks the onset of a TCP connection. In the three-way handshake, a client requests a new connection by sending a TCP SYN packet to a server. After that, the server sends a SYN/ACK packet back to the client and places the connection request in a queue. Finally, the client acknowledges the SYN/ACK packet. If an attack occurs, however, the attacker sends an abundance of TCP SYN packets to the victim, obliging it both to open a lot of TCP connections and to respond to them. Then the attacker does not execute the third step of the three-way handshake that follows, rendering the victim unable to accept any new incoming connections, because its queue is full of half-open TCP connections.

D.1.3 Ping of Death

In Ping of Death attacks, the attacker creates a packet that contains more than 65 536 bytes, which is the limit that the IP protocol defines. This packet can cause different kinds of damage to the machine that receives it, such as crashing and rebooting.

D.1.4 Process Table

This attack exploits the feature of some network services to generate a new process each time a new TCP/IP connection is set up. The attacker tries to make as many uncompleted connections to the victim as possible in order to force the victim's system to generate an abundance of processes. Hence, because the number of processes that are running on the system cannot be boundlessly large, the attack renders the victim unable to serve any other request.

D.1.5 Smurf Attack

In a "smurf" attack, the victim is flooded with *Internet Control Message Protocol* (ICMP) "echo-reply" packets. The attacker sends numerous ICMP "echo-request" packets to the broadcast address of many subnets. These packets contain the victim's address as the source IP address. Every machine that belongs to any of these subnets responds by sending ICMP "echo-reply" packets to the victim. Smurf attacks are very dangerous, because they are strongly distributed attacks.

D.1.6 SSH Process Table

Like the Process Table attack, this attack makes hundreds of connections to the victim with the *Secure Shell* (SSH) Protocol without completing the login process. In this way, the daemon contacted by the SSH on the victim's system is obliged to start so many SSH processes that it is exhausted.

D.1.7 TCP Reset

In TCP Reset attacks, the network is monitored for "tcpconnection" requests to the victim. As soon as such a request is found, the malevolent attacker sends a spoofed TCP RESET packet to the victim and obliges it to terminate the TCP connection.

D.1.8 Teardrop

While a packet is travelling from the source machine to the destination machine, it may be broken up into smaller fragments, through the process of fragmentation. A Teardrop attack creates a stream of IP fragments with their offset field overloaded. The destination host that tries to reassemble these malformed fragments eventually crashes or reboots.

D.1.9 UDP Storm

In a *User Datagram Protocol* (UDP) connection, a character generation ("chargen") service generates a series of characters each time it receives a UDP packet, while an echo service echoes any character it receives. Exploiting these two services, the attacker sends a packet with the source spoofed to be that of the victim to another machine. Then, the echo service of the former machine echoes the data of that packet back to the victim's machine and the victim's machine, in turn, responds in the same way. Hence, a constant stream of useless load is created that burdens the network.

D.2 DDoS characteristics

Distributed Denial of Service (DDoS) attacks extend conventional Denial of Service (DoS) attacks by the additional characteristic of being distributed attacks (i.e. the attack is from many points at once). For a DDoS attack the multiplicity of the attack relationship in figure D.1 is 1 too many (1 victim, many attackers), whereas in most conventional attacks the multiplicity is 1 to 1.

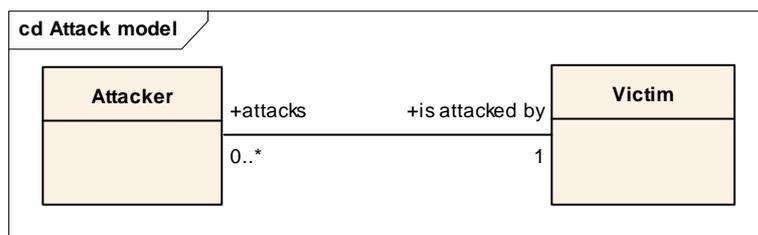


Figure D.1: Attack model (static state)

There are two primary assets of a system that are victimised in DDoS attacks:

- Bandwidth.
- Processing resources (CPU cycles).

Bandwidth is consumed by flooding the network with useless packets. Attacks against processing resource may be achieved by generating several thousands of useless processes on the victim's system sufficient to fully occupy memory and process tables.

D.3 Defence against DDoS

From the beginning, all legitimate users have tried to respond against these threats. University communities and software corporations have proposed several methods against the DDoS threat. Despite the efforts, the solution remains a dream. The attackers manage to discover other weaknesses of the protocols and, what is worse, they exploit the defence mechanisms in order to develop attacks. They discover methods to overcome these mechanisms or they exploit them to generate false alarms and to cause catastrophic consequences.

Many experts have tried to classify the DDoS defence mechanisms in order to clarify them. This classification gives users an overall view of the situation and helps defence-mechanism developers cooperate against the threat. The basic discrimination is between preventive and reactive defence mechanisms.

D.3.1 Preventive Mechanisms

The preventive mechanisms try to eliminate the possibility of DDoS attacks altogether or to enable potential victims to endure the attack without denying services to legitimate clients. With regard to attack prevention, countermeasures can be taken on either victims or on zombies. In both cases the system configuration is modified to eliminate the possibility of accepting a DDoS attack or participating in a DDoS attack.

Filtering of input and output traffic may be possible and may offer simple rules, for example, the source IP address of output traffic should belong to the sub-network, whereas the source IP address of input traffic should not.

D.3.2 Reactive Mechanisms

Reactive mechanisms try to detect the attack and respond to it immediately and by doing so restrict the impact of the attack on the victim.

RISK: Characterizing a legitimate connection as an attack.

D.3.2.1 Signature detection mechanisms

Signature-based methods search for patterns (signatures) in observed network traffic that match known attack signatures from a database. The advantage of these methods is that they can easily and reliably detect known attacks, but they cannot recognize new attacks. Moreover, the signature database must always be kept up-to-date in order to retain the reliability of the system.

D.3.2.2 Anomaly detection mechanisms

Anomaly-based methods compare the parameters of the observed network traffic with normal traffic. Hence it is possible for new attacks to be detected. However, in order to prevent a false alarm, the model of "normal traffic" must always be kept updated and the threshold of categorizing an anomaly must be properly adjusted.

D.3.3 Difficulties of defence

Development of detection and defending tools is unlikely to every prove 100% effective and some of the more common problems include:

- DDoS attacks flood victims with packets. The rate of change of network activity that leads to an attack may be greater than the speed at which countermeasures can be brought into play.
- Any attempt of filtering the incoming flow may mean that legitimate traffic will be rejected.
- Filtering may rob processor time and more advanced filtering rules take more of the resource.
- Attack packets usually have spoofed IP addresses so tracing the real attacker rather than a masqueraded victim may be difficult.

Annex E (informative): TVRA database structure

E.1 Database structure

The database Entity Relationship Diagram (ERD) shown in figure E.1 has been extracted from the database used in development. For readability the lookup tables have been omitted.

E.2 SQL code for TVRA database

The following SQL code is offered without claims for completeness but to allow readers of the present document to incorporate them into an existing database environment. The code follows the ANSI-SQL language syntax wherever possible and has been tested using the open source MySQL database without optimization.

NOTE: For use in MySQL databases the database engine has to be set to InnoDB in order to allow foreign key relationships to work.

E.2.1 Lookup tables

Lookup tables are used throughout the database to store data that is either intransient, or which may be referenced in more than one of the core tables. This covers the criteria for weighting a risk as defined in clauses 5 and 6 of the present document, the use of Common Criteria Functional and Assurance classes as defined in ISO/IEC 15408 [13] and referred to in clause 5 of the present document, and citations used to record the source material used in analysis.

NOTE: Lookup tables are used to resolve many-to-one relationships identified in the UML models in the core of the present document.

```
CREATE TABLE Citation_LU (
  CitationId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (CitationId),
  Publisher Text(50) NOT NULL,
  DocumentName Text(255),
  Notes Text(255)
) ENGINE = InnoDB
;
```

```
CREATE TABLE RequirementType_LU (
  RequirementTypeId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (RequirementTypeId),
  RequirementType Text(25) NOT NULL,
  RequirementTypeDescription Text(127)
)
;
```

```
CREATE TABLE CC_Components_LU (
  ComponentId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (ComponentId),
  Citation INT,
  INDEX (Citation),
  FOREIGN KEY (Citation) REFERENCES Citation_LU (CitationId),
  CC_ComponentShortName Text(7) NOT NULL,
  CC_ComponentLevel INT NOT NULL,
  CC_ComponentLongName Text(80) NOT NULL
)
;
```

```
CREATE TABLE Likelihood_LU (
  LikelihoodId INT NOT NULL,
  PRIMARY KEY (LikelihoodId),
  Likelihood Text(50),
  Description Text(1024)
) ENGINE = InnoDB
;
```

```
CREATE TABLE AssetValue_LU (
  AssetImpact INT NOT NULL,
  PRIMARY KEY (AssetImpact),
  AssetImpactShortText Text(50) NOT NULL,
  AssetImpactLongDescription Text(1024)
) ENGINE = InnoDB
;
```

```
CREATE TABLE AttackEquipment_LU (
  AttackEquipment INT NOT NULL,
  PRIMARY KEY (AttackEquipment),
  Equipment Text(50) NOT NULL,
  AttackEquipmentLongDescription Text(1024)
) ENGINE = InnoDB
;
```

```
CREATE TABLE AttackExpertise_LU (
  AttackExpertise INT NOT NULL,
  PRIMARY KEY (AttackExpertise),
  Expertise Text(50) NOT NULL,
  AttackExpertiseLongDescription Text(1024)
) ENGINE = InnoDB
;
```

```
CREATE TABLE AttackKnowledge_LU (
  AttackKnowledge INT NOT NULL,
  PRIMARY KEY (AttackKnowledge),
  Knowledge Text(50) NOT NULL,
  AttackKnowledgeLongDescription Text(1024)
) ENGINE = InnoDB
;
```

```
CREATE TABLE AttackOpportunity_LU (
  AttackOpportunity INT NOT NULL,
  PRIMARY KEY (AttackOpportunity),
  OpportunityText Text(50) NOT NULL,
  OpportunityLongDescription Text(1024)
) ENGINE = InnoDB
;
```

E.2.2 Core tables

Core tables are those that contain the main body of the analysis. This covers the assets, threats, threat agents, weaknesses, vulnerabilities and unwanted-incidents. The tables make use of many foreign key relationships that ensure that terms stored in the database are restricted to those values found in the lookup tables using only the index of the lookup tables. As such a *SELECT * FROM <<table-name>>* query may return non-user readable output.

```
CREATE TABLE Asset_T (
  AssetId INT NOT NULL AUTO_INCREMENT,
  AssetName Text(50) NOT NULL,
  AssetDescription Text(1024),
  CitationId INT,
  AssetImpactWeight INT,
  PRIMARY KEY (AssetId),
  INDEX (AssetImpactWeight),
  FOREIGN KEY (AssetImpactWeight) REFERENCES AssetValue_LU (AssetImpact),
  INDEX (CitationId),
  FOREIGN KEY (CitationId) REFERENCES Citation_LU (CitationId)
) ENGINE = InnoDB
;
```

```
CREATE TABLE System_T (
  SystemId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (SystemId),
  SystemName Text(50) NOT NULL,
  SystemDescription Text(1024),
  CitationId INT,
  INDEX (CitationId),
  FOREIGN KEY (CitationId) REFERENCES Citation_LU (CitationId)
) ENGINE = InnoDB
;
```

```

CREATE TABLE ThreatAgent_T (
  ThreatAgentId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (ThreatAgentId),
  TA_name Text(50) NOT NULL,
  TA_description Text(1024) NOT NULL,
  AttackTimeValue INT,
  AttackExpertise INT,
  AttackKnowledge INT,
  AttackOpportunity INT,
  AttackEquipment INT,
  INDEX (AttackExpertise),
  FOREIGN KEY (AttackExpertise) REFERENCES AttackExpertise_LU (AttackExpertise),
  INDEX (AttackKnowledge),
  FOREIGN KEY (AttackKnowledge) REFERENCES AttackKnowledge_LU (AttackKnowledge),
  INDEX (AttackOpportunity),
  FOREIGN KEY (AttackOpportunity) REFERENCES AttackOpportunity_LU (AttackOpportunity),
  INDEX (AttackEquipment),
  FOREIGN KEY (AttackEquipment) REFERENCES AttackEquipment_LU (AttackEquipment)
) ENGINE = InnoDB
;

```

```

CREATE TABLE Threat_T (
  ThreatId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (ThreatId),
  ThreatName Text(50),
  ThreatDescription Text(1024)
) ENGINE = InnoDB
;

```

```

CREATE TABLE UnwantedIncident_T (
  UnwantedIncidentId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (UnwantedIncidentId),
  Name Text(50),
  Description Text(1024)
) ENGINE = InnoDB
;

```

```

CREATE TABLE Weakness_T (
  WeaknessId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (WeaknessId),
  WeaknessName Text(50),
  WeaknessDescription Text(1024)
) ENGINE = InnoDB
;

```

```

CREATE TABLE Objective_T (
  ObjectiveId INT NOT NULL AUTO_INCREMENT,
  Objective Text(255) NOT NULL,
  Citation INT,
  INDEX (Citation),
  FOREIGN KEY (Citation) REFERENCES Citation_LU (CitationId),
  PRIMARY KEY (ObjectiveId)
)
;

```

```

CREATE TABLE Requirement_T (
  RequirementId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (RequirementId),
  Requirement Text(255) NOT NULL,
  Citation INT,
  RequirementType INT NOT NULL,
  CCReference INT,
  INDEX (CCReference),
  FOREIGN KEY (CCReference) REFERENCES CC_Components_LU (ComponentID),
  INDEX (RequirementType),
  FOREIGN KEY (RequirementType) REFERENCES RequirementType_LU (RequirementTypeId),
  INDEX (Citation),
  FOREIGN KEY (Citation) REFERENCES Citation_LU (CitationId)
)
;

```

E.2.3 Linking tables

Linking tables are used throughout the database to store data that combines two or more tables. For example an asset may appear in many systems, an objective may be tied to an asset.

NOTE: Linking tables are used to resolve many-to-many relationships identified in the UML models in the core of the present document.

```
CREATE TABLE AssetObjective_LT (
  ObjectiveId INT,
  AssetId INT,
  INDEX (ObjectiveId),
  INDEX (AssetId),
  FOREIGN KEY (ObjectiveId) REFERENCES Objective_T (ObjectiveId),
  FOREIGN KEY (AssetId) REFERENCES Asset_T (AssetId)
)
;
```

```
CREATE TABLE SystemObjective_LT (
  ObjectiveId INT,
  SystemId INT,
  INDEX (ObjectiveId),
  INDEX (SystemId),
  FOREIGN KEY (ObjectiveId) REFERENCES Objective_T (ObjectiveId),
  FOREIGN KEY (SystemId) REFERENCES System_T (SystemId)
)
;
```

```
CREATE TABLE ProblemsToAvoid_LT (
  UnwantedIncidentId INT,
  SystemId INT,
  ObjectiveId INT,
  INDEX (UnwantedIncidentId),
  INDEX (SystemId),
  INDEX (ObjectiveId),
  FOREIGN KEY (ObjectiveId) REFERENCES Objective_T (ObjectiveId),
  FOREIGN KEY (SystemId) REFERENCES System_T (SystemId),
  FOREIGN KEY (UnwantedIncidentId) REFERENCES UnwantedIncident_T (UnwantedIncidentId)
) ENGINE = InnoDB
;
```

```
CREATE TABLE RiskAssesment_LT (
  VulnerabilityId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (VulnerabilityId),
  AssetId INT,
  WeaknessId INT,
  ThreatAgentId INT,
  Likelihood INT,
  RiskAssesmentDate DateTime,
  INDEX (AssetId),
  INDEX (WeaknessId),
  INDEX (ThreatAgentId),
  INDEX (Likelihood),
  FOREIGN KEY (AssetId) REFERENCES Asset_T (AssetId),
  FOREIGN KEY (WeaknessId) REFERENCES Weakness_T (WeaknessId),
  FOREIGN KEY (ThreatAgentId) REFERENCES ThreatAgent_T (ThreatAgentId),
  FOREIGN KEY (Likelihood) REFERENCES Likelihood_LU (LikelihoodId)
)
ENGINE = InnoDB
;
```

```
CREATE TABLE SystemComponents_LT (
  SystemId INT,
  AssetId INT,
  INDEX (SystemId),
  FOREIGN KEY (SystemId) REFERENCES System_T (SystemId),
  INDEX (AssetId),
  FOREIGN KEY (AssetId) REFERENCES Asset_T (AssetId)
) ENGINE = InnoDB
;
```

```
CREATE TABLE ThreatEnabler_LT (  
    ThreatAgentId INT,  
    ThreatId INT,  
    INDEX (ThreatAgentId),  
    INDEX (ThreatId),  
    FOREIGN KEY (ThreatAgentId) REFERENCES ThreatAgent_T (ThreatAgentId),  
    FOREIGN KEY (ThreatId) REFERENCES Threat_T (ThreatId)  
) ENGINE = InnoDB  
;
```

E.2.4 Sample queries (used to complete input to eTVRA proforma)

Not yet tested.

Annex F (informative): Use of ISO/IEC 15408-2 [11] security functional classes in security requirements statements

F.1 Overview

When preparing the security requirements the model given in ISO/IEC 15408-2 [11] is highly recommended as it provides a clear statement of the requirement and uses a common language that can be applied to any ICT security scenario.

Each class of functions in ISO/IEC 15408-2 [11] is defined such that they can be combined to provide complex composite requirements.

Table F.1 summarizes the classes and their class members.

Table F.1: ISO/IEC 15408-2 [11] classes and families

Class	Class members	
FAU Security audit	FAU_ARP FAU_GEN FAU_SAA FAU_SAR FAU_SEL FAU_STG	Security audit automatic response Security audit data generation Security audit analysis Security audit review Security audit event selection Security audit event storage
FCO Communication	FCO_NRO FCO_NRR	Non-repudiation of origin Non-repudiation of receipt
FCS Cryptographic support	FCS_CKM FCS_COP	Cryptographic key management Cryptographic operation
FDP User Data Protection	FDP_ACC FDP_ACF FDP_DAU FDP_ETC FDP_IFC FDP_IFF FDP_ITC FDP_ITT FDP_RIP FDP_ROL FDP_SDI FDP_UCT FDP_UIT	Access control policy Access control functions Data authentication Export to outside TSF control Information flow control policy Information flow control functions Import from outside TSF control Internal TOE transfer Residual information protection Rollback Stored data integrity Inter-TSF user data confidentiality transfer protection Inter-TSF user data integrity transfer protection
FIA Identification and authentication	FIA_AFL FIA_ATD FIA_SOS FIA_UAU FIA_UID FIA_USB	Authentication failures User attribute definition Specification of secrets User authentication User identification User-subject binding
FMT Security management	FMT_MOF FMT_MSA FMT_MTD FMT_REV FMT_SAE FMT_SMR	Management of functions in TSF Management of security attributes Management of TSF data Revocation Security attribute expiration Security management roles
FPR Privacy	FPR_ANO FPR_PSE FPR_UNL FPR_UNO	Anonymity Pseudonymity Unlinkability Unobservability
FPT Protection of the TSF	FPT_AMT FPT_FLS FPT_ITA FPT_ITC FPT_ITI FPT_ITT FPT_PHP FPT_RCV FPT_RPL FPT_RVM FPT_SEP FPT_SSP FPT_STM FPT_TDC FPT_TRC FPT_TST	Underlying abstract machine test Fail secure Availability of exported TSF data Confidentiality of exported TSF data Integrity of exported TSF data Internal TOE TSF data transfer TSF physical protection Trusted recovery Protection of the TSF Replay detection Reference mediation Domain separation State synchrony protocol Time stamps Inter-TSF TSF data consistency Internal TOE TSF data replication consistency TSF self test
FRU Resource Utilization	FRU_FLT FRU_PRS FRU_RSA	Fault tolerance Priority of service Resource allocation

Class	Class members	
FTA TOE Access	FTA_LSA	Limitation on scope of selectable attributes
	FTA_MCS	Limitation on multiple concurrent sessions
	FTA_SSL	Session locking
	FTA_TAB	TOE access banners
	FTA_TAH	TOE access history
	FTA_TSE	TOE session establishment
FTP Trusted path/channels	FTP_ITC	Inter-TSF trusted channel
	FTP_TRP	Trusted path

The use and application of the security requirements class members in defining deployable security capabilities is considered in greater depth in TS 102 165-2 [6].

F.2 Review of functional capabilities

NOTE: When writing requirements using the statements in the tables that follow the designer has to explicitly identify the "assignment" and "selection" criteria for each chosen statement. This may lead to many variants of a single functional requirement.

F.2.1 Authentication and identification

The functional capabilities in the authentication and identification class address the requirements to establish and verify a claimed user identity.

Table F.2: ISO/IEC 15408-2 [11] Functional capabilities (Authentication and Identification class)

Shortname	Definition	Form of assignment in NGN
FIA_AFL.1.1	The TSF shall detect when [assignment: number] unsuccessful authentication attempts occur related to [assignment: list of authentication events].	Integer number of allowed failures
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: list of actions].	Barring further attempts (e.g. barring a SIM after 3 failed PIN entry attempts)
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes].	Application dependent
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [assignment: a defined quality metric].	Not normally done
FIA_SOS.2.1	The TSF shall provide a mechanism to generate secrets that meet [assignment: a defined quality metric].	Not normally done
FIA_SOS.2.2	The TSF shall be able to enforce the use of TSF generated secrets for [assignment: list of TSF functions].	Not normally done
FIA_UAU.1.1	The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.	Making emergency calls; Location update processing
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.	Any actions not restricted by FIA_UAU.1.1 and within the access allowance of the NGN user
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.	As per FIA_UAU.1.2
FIA_UAU.3.1	The TSF shall [selection: detect, prevent] use of authentication data that has been forged by any user of the TSF.	Detect and prevent
FIA_UAU.3.2	The TSF shall [selection: detect, prevent] use of authentication data that has been copied from any other user of the TSF.	Detect and prevent
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to [assignment: identified authentication mechanism(s)].	This has to be applied to specific NGN mechanisms
FIA_UAU.5.1	The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.	
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication].	Needs an identity management method
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions [assignment: list of conditions under which re-authentication is required].	Time; Change of location
FIA_UAU.7.1	The TSF shall provide only [assignment: list of feedback] to the user while the authentication is in progress.	Information messages relating to the authentication
FIA_UID.1.1	The TSF shall allow [assignment: list of TSF-mediated actions] on behalf of the user to be performed before the user is identified.	Making of emergency calls
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.	Any NGN service not excluded by FIA_UID.1.1
FIA_UID.2.1	The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.	As per FIA_UID.2.1
FIA_USB.1.1	The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.	Applies to user-agents in the NGN

F.2.2 Communication class (non-repudiation)

The functional capabilities in the communication class address those requirements dealing with repudiation (and non-repudiation) of a communication).

Table F.3: ISO/IEC 15408-2 [11] Functional capabilities (Communication class (non-repudiation))

Shortname	Definition	Form of assignment in NGN
FCO_NRO.1.1	The TSF shall be able to generate evidence of origin for transmitted [assignment: list of information types] at the request of the [selection: originator, recipient, [assignment: list of third parties]].	Billable events and messages
FCO_NRO.1.2	The TSF shall be able to relate the [assignment: list of attributes] of the originator of the information, and the [assignment: list of information fields] of the information to which the evidence applies.	FFS
FCO_NRO.1.3	The TSF shall provide a capability to verify the evidence of origin of information to [selection: originator, recipient, [assignment: list of third parties]] given [assignment: limitations on the evidence of origin].	Originator and recipient
FCO_NRO.2.1	The TSF shall enforce the generation of evidence of origin for transmitted [assignment: list of information types] at all times.	Not generally done in communications scenarios but may apply for e-commerce scenarios
FCO_NRO.2.2	The TSF shall be able to relate the [assignment: list of attributes] of the originator of the information, and the [assignment: list of information fields] of the information to which the evidence applies.	FFS
FCO_NRO.2.3	The TSF shall provide a capability to verify the evidence of origin of information to [selection: originator, recipient, [assignment: list of third parties]] given [assignment: limitations on the evidence of origin].	FFS
FCO_NRR.1.1	The TSF shall be able to generate evidence of receipt for received [assignment: list of information types] at the request of the [selection: originator, recipient, [assignment: list of third parties]].	FFS
FCO_NRR.1.2	The TSF shall be able to relate the [assignment: list of attributes] of the recipient of the information, and the [assignment: list of information fields] of the information to which the evidence applies.	Not generally done in communications scenarios but may apply for e-commerce scenarios
FCO_NRR.1.3	The TSF shall provide a capability to verify the evidence of receipt of information to [selection: originator, recipient, [assignment: list of third parties]] given [assignment: limitations on the evidence of receipt].	Not generally done in communications scenarios but may apply for e-commerce scenarios
FCO_NRR.2.1	The TSF shall enforce the generation of evidence of receipt for received [assignment: list of information types].	Not generally done in communications scenarios but may apply for e-commerce scenarios
FCO_NRR.2.2	The TSF shall be able to relate the [assignment: list of attributes] of the recipient of the information, and the [assignment: list of information fields] of the information to which the evidence applies.	FFS
FCO_NRR.2.3	The TSF shall provide a capability to verify the evidence of receipt of information to [selection: originator, recipient, [assignment: list of third parties]] given [assignment: limitations on the evidence of receipt].	Not generally done in communications scenarios but may apply for e-commerce scenarios

F.2.3 User data protection class

The functional capabilities in the user data protection class address those requirements dealing protection of data and cover information policy, and transfer as well as the actual mechanics of protection.

Table F.4: ISO/IEC 15408-2 [11] Functional capabilities (User data protection class)

Shortname	Definition	Form of assignment in NGN
FDP_ACC.1.1	The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].	At gateways using policy or firewall rules
FDP_ACC.2.1	The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.	At gateways using policy or firewall rules
FDP_ACC.2.2	The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.	Management policy
FDP_ACF.1.1	The TSF shall enforce the [assignment: access control SFP] to objects based on [assignment: security attributes, named groups of security attributes].	At gateways using policy or firewall rules
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].	At gateways using policy or firewall rules
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].	
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].	
FDP_DAU.1.1	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: list of objects or information types].	
FDP_DAU.1.2	The TSF shall provide [assignment: list of subjects] with the ability to verify evidence of the validity of the indicated information.	
FDP_DAU.2.1	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: list of objects or information types].	
FDP_DAU.2.2	The TSF shall provide [assignment: list of subjects] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.	
FDP_ETC.1.1	The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] when exporting user data, controlled under the SFP(s), outside of the TSC.	
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes.	
FDP_ETC.2.1	The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] when exporting user data, controlled under the SFP(s), outside of the TSC.	
FDP_ETC.2.2	The TSF shall export the user data with the user data's associated security attributes.	
FDP_ETC.2.3	The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.	
FDP_ETC.2.4	The TSF shall enforce the following rules when user data is exported from the TSC: [assignment: additional exportation control rules].	
FDP_IFC.1.1	The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].	
FDP_IFC.2.1	The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP.	
FDP_IFC.2.2	The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.	
FDP_IFF.1.1	The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes].	

Shortname	Definition	Form of assignment in NGN
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].	
FDP_IFF.1.3	The TSF shall enforce the [assignment: additional information flow control SFP rules].	
FDP_IFF.1.4	The TSF shall provide the following [assignment: list of additional SFP capabilities].	
FDP_IFF.1.5	The TSF shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows].	
FDP_IFF.1.6	The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].	
FDP_IFF.2.1	The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes].	
FDP_IFF.2.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].	
FDP_IFF.2.3	The TSF shall enforce the [assignment: additional information flow control SFP rules].	
FDP_IFF.2.4	The TSF shall provide the following [assignment: list of additional SFP capabilities]	
FDP_IFF.2.5	The TSF shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows].	
FDP_IFF.2.6	The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].	
FDP_IFF.2.7	The TSF shall enforce the following relationships for any two valid information flow control security attributes: a) There exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable; and b) There exists a 'least upper bound' in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and c) There exists a 'greatest lower bound' in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes.	
FDP_IFF.3.1	The TSF shall enforce the [assignment: information flow control SFP] to limit the capacity of [assignment: types of illicit information flows] to a [assignment: maximum capacity].	
FDP_IFF.4.1	The TSF shall enforce the [assignment: information flow control SFP] to limit the capacity of [assignment: types of illicit information flows] to a [assignment: maximum capacity].	
FDP_IFF.4.2	The TSF shall prevent [assignment: types of illicit information flows].	
FDP_IFF.5.1	The TSF shall ensure that no illicit information flows exist to circumvent [assignment: name of information flow control SFP].	
FDP_IFF.6.1	The TSF shall enforce the [assignment: information flow control SFP] to monitor [assignment: types of illicit information flows] when it exceeds the [assignment: maximum capacity].	
FDP_ITC.1.1	The TSF shall enforce the [assignment: access control SFP and/or information flow control SFP] when importing user data, controlled under the SFP, from outside of the TSC.	
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.	
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: additional	

Shortname	Definition	Form of assignment in NGN
	importation control rules].	
FDP_ITC.2.1	The TSF shall enforce the [assignment: access control SFP and/or information flow control SFP] when importing user data, controlled under the SFP, from outside of the TSC.	
FDP_ITC.2.2	The TSF shall use the security attributes associated with the imported user data.	
FDP_ITC.2.3	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.	
FDP_ITC.2.4	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.	
FDP_ITC.2.5	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: additional importation control rules].	
FDP_ITT.1.1	The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to prevent the [selection: disclosure, modification, loss of use] of user data when it is transmitted between physically-separated parts of the TOE.	
FDP_ITT.2.1	The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to prevent the [selection: disclosure, modification, loss of use] of user data when it is transmitted between physically-separated parts of the TOE.	
FDP_ITT.2.2	The TSF shall separate data controlled by the SFP(s) when transmitted between physically-separated parts of the TOE, based on the values of the following: [assignment: security attributes that require separation].	
FDP_ITT.3.1	The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [assignment: integrity errors].	
FDP_ITT.3.2	Upon detection of a data integrity error, the TSF shall [assignment: specify the action to be taken upon integrity error].	
FDP_ITT.4.1	The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [assignment: integrity errors], based on the following attributes: [assignment: security attributes that require separate transmission channels].	
FDP_ITT.4.2	Upon detection of a data integrity error, the TSF shall [assignment: specify the action to be taken upon integrity error].	
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, deallocation of the resource from] the following objects: [assignment: list of objects].	
FDP_RIP.2.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, deallocation of the resource from] all objects.	
FDP_ROL.1.1	The TSF shall enforce [assignment: access control SFP(s) and/or information flow control SFP(s)] to permit the rollback of the [assignment: list of operations] on the [assignment: list of objects].	
FDP_ROL.1.2	The TSF shall permit operations to be rolled back within the [assignment: boundary limit to which rollback may be performed].	
FDP_ROL.2.1	The TSF shall enforce [assignment: access control SFP(s) and/or information flow control SFP(s)] to permit the rollback of all the operations on the [assignment: list of objects].	
FDP_ROL.2.2	The TSF shall permit operations to be rolled back within the [assignment: boundary limit to which rollback may be performed].	
FDP_SDI.1.1	The TSF shall monitor user data stored within the TSC for [assignment: integrity errors] on all objects, based on the following attributes: [assignment: user data attributes].	
FDP_SDI.2.1	The TSF shall monitor user data stored within the TSC for [assignment: integrity errors] on all objects, based on the following attributes: [assignment: user data attributes].	
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall [assignment: action to be taken].	
FDP_UCT.1.1	The TSF shall enforce the [assignment: access control SFP(s) and/or	

Shortname	Definition	Form of assignment in NGN
	information flow control SFP(s)] to be able to [selection : transmit, receive] objects in a manner protected from unauthorized disclosure.	
FDP_UIT.1.1	The TSF shall enforce the [assignment : access control SFP(s) and/or information flow control SFP(s)] to be able to [selection : transmit, receive] user data in a manner protected from [selection : modification, deletion, insertion, replay] errors.	
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether [selection : modification, deletion, insertion, replay] has occurred.	
FDP_UIT.2.1	The TSF shall enforce the [assignment : access control SFP(s) and/or information flow control SFP(s)] to be able to recover from [assignment : list of recoverable errors] with the help of the source trusted IT product.	
FDP_UIT.3.1	The TSF shall enforce the [assignment : access control SFP(s) and/or information flow control SFP(s)] to be able to recover from [assignment : list of recoverable errors] without any help from the source trusted IT product.	

F.2.4 Privacy class

The functional capabilities in the privacy class address those requirements dealing with provision of privacy including those required to suppress user identity, provision of anonymity (including linking and unlinking to a real identity).

Table F.5: ISO/IEC 15408-2 [11] Functional capabilities (Privacy class)

Shortname	Definition	Form of assignment in NGN
FPR_ANO.1.1	The TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects].	
FPR_ANO.2.1	The TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects].	
FPR_ANO.2.2	The TSF shall provide [assignment: list of services] to [assignment: list of subjects] without soliciting any reference to the real user name.	
FPR_PSE.1.1	The TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects].	
FPR_PSE.1.2	The TSF shall be able to provide [assignment: number of aliases] aliases of the real user name to [assignment: list of subjects].	
FPR_PSE.1.3	The TSF shall [selection, choose one of: determine an alias for a user, accept the alias from the user] and verify that it conforms to the [assignment: alias metric].	
FPR_PSE.2.1	The TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects].	
FPR_PSE.2.2	The TSF shall be able to provide [assignment: number of aliases] aliases of the real user name to [assignment: list of subjects].	
FPR_PSE.2.3	The TSF shall [selection, choose one of: determine an alias for a user, accept the alias from the user] and verify that it conforms to the [assignment: alias metric].	
FPR_PSE.2.4	The TSF shall provide [selection: an authorized user, [assignment: list of trusted subjects]] a capability to determine the user identity based on the provided alias only under the following [assignment: list of conditions].	
FPR_PSE.3.1	The TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects].	
FPR_PSE.3.2	The TSF shall be able to provide [assignment: number of aliases] aliases of the real user name to [assignment: list of subjects].	
FPR_PSE.3.3	The TSF shall [selection, choose one of: determine an alias for a user, accept the alias from the user] and verify that it conforms to the [assignment: alias metric].	
FPR_PSE.3.4	The TSF shall provide an alias to the real user name which shall be identical to an alias provided previously under the following [assignment: list of conditions] otherwise the alias provided shall be unrelated to previously provided aliases.	
FPR_UNL.1.1	The TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine whether [assignment: list of operations][selection: were caused by the same user, are related as follows[assignment: list of relations]].	
FPR_UNO.1.1	The TSF shall ensure that [assignment: list of users and/or subjects] are unable to observe the operation [assignment: list of operations] on [assignment: list of objects] by [assignment: list of protected users and/or subjects].	
FPR_UNO.2.1	The TSF shall ensure that [assignment: list of users and/or subjects] are unable to observe the operation [assignment: list of operations] on [assignment: list of objects] by [assignment: list of protected users and/or subjects].	
FPR_UNO.2.2	The TSF shall allocate the [assignment: unobservability related information] among different parts of the TOE such that the following conditions hold during the lifetime of the information: [assignment: list of conditions].	
FPR_UNO.3.1	The TSF shall provide [assignment: list of services] to [assignment: list of subjects] without soliciting any reference to [assignment: privacy related information].	
FPR_UNO.4.1	The TSF shall provide [assignment: set of authorized users] with the capability to observe the usage of [assignment: list of resources and/or services].	May apply for lawful interception and management roles.

F.2.5 Resource utilization class

The functional capabilities in the resource utilization class address those requirements dealing with system reliability and availability.

Table F.6: ISO/IEC 15408-2 [11] Functional capabilities (Resource utilization class)

Shortname	Definition	Form of assignment in NGN
FRU_FLT.1.1	The TSF shall ensure the operation of [assignment: list of TOE capabilities] when the following failures occur: [assignment: list of type of failures].	
FRU_FLT.2.1	The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: [assignment: list of type of failures]	
FRU_PRS.1.1	The TSF shall assign a priority to each subject in the TSF.	
FRU_PRS.1.2	The TSF shall ensure that each access to [assignment: controlled resources] shall be mediated on the basis of the subjects assigned priority.	
FRU_PRS.2.1	The TSF shall assign a priority to each subject in the TSF.	
FRU_PRS.2.2	The TSF shall ensure that each access to all shareable resources shall be mediated on the basis of the subjects assigned priority.	
FRU_RSA.1.1	The TSF shall enforce maximum quotas of the following resources: [assignment: controlled resources] that [selection: individual user, defined group of users, subjects] can use [selection: simultaneously, over a specified period of time].	
FRU_RSA.2.1	The TSF shall enforce maximum quotas of the following resources [assignment: controlled resources] that [selection: individual user, defined group of users] can use [selection: simultaneously, over a specified period of time].	
FRU_RSA.2.2	The TSF shall ensure the provision of minimum quantity of each [assignment: controlled resource] that is available for [selection: an individual user, defined group of users, subjects] to use [selection: simultaneously, over a specified period of time].	

F.2.6 Trusted path/channel class

The functional capabilities in the trusted path/channel class address those requirements dealing with the communication path between users and the TSF, and for a trusted communication channel between the TSF and other trusted IT products. Trusted paths and channels have the following general characteristics:

- The communications path is constructed using internal and external communications channels that isolate an identified subset of TSF data and commands from the remainder of the TSF and user data.
- Use of the communications path may be initiated by the user and/or the TSF.
- The communications path is capable of providing assurance that the user is communicating with the correct TSF, and that the TSF is communicating with the correct user.

Table F.7: ISO/IEC 15408-2 [11] Functional capabilities (Trusted path/channel class)

Shortname	Definition	Form of assignment in NGN
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.	
FTP_ITC.1.2	The TSF shall permit [selection : the TSF, the remote trusted IT product] to initiate communication via the trusted channel.	
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [assignment : list of functions for which a trusted channel is required].	
FTP_TRP.1.1	The TSF shall provide a communication path between itself and [selection : remote, local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.	
FTP_TRP.1.2	The TSF shall permit [selection : the TSF, local users, remote users] to initiate communication via the trusted path.	
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [selection : initial user authentication],[assignment : other services for which trusted path is required]].	

F.2.7 Security management class

The functional capabilities in the security management class address those requirements dealing with the establishment, maintenance and deletion of security functions and data.

Table F.8: ISO/IEC 15408-2 [11] Functional capabilities (Security management class)

Shortname	Definition	Form of assignment in NGN
FMT_MOF.1.1	The TSF shall restrict the ability to [selection : determine the behaviour of, disable, enable, modify the behaviour of] the functions [assignment : list of functions] to [assignment : the authorized identified roles].	
FMT_MSA.1.1	The TSF shall enforce the [assignment : access control SFP, information flow control SFP] to restrict the ability to [selection : change_default, query, modify, delete, [assignment : other operations]] the security attributes [assignment : list of security attributes] to [assignment : the authorized identified roles].	
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for security attributes.	
FMT_MSA.3.1	The TSF shall enforce the [assignment : access control SFP, information flow control SFP] to provide [selection , choose one of: restrictive, permissive, [assignment : other property]] default values for security attributes that are used to enforce the SFP.	
FMT_MSA.3.2	The TSF shall allow the [assignment : the authorized identified roles] to specify alternative initial values to override the default values when an object or information is created.	
FMT_MTD.1.1	The TSF shall restrict the ability to [selection : change_default, query, modify, delete, clear, [assignment : other operations]] the [assignment : list of TSF data] to [assignment : the authorized identified roles].	
FMT_MTD.2.1	The TSF shall restrict the specification of the limits for [assignment : list of TSF data] to [assignment : the authorized identified roles].	
FMT_MTD.2.2	The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [assignment : actions to be taken].	
FMT_MTD.3.1	The TSF shall ensure that only secure values are accepted for TSF data.	
FMT_REV.1.1	The TSF shall restrict the ability to revoke security attributes associated with the [selection : users, subjects, objects, [assignment : other additional resources]] within the TSC to [assignment : the authorized identified roles].	
FMT_REV.1.2	The TSF shall enforce the rules [assignment : specification of revocation rules].	
FMT_SAE.1.1	The TSF shall restrict the capability to specify an expiration time for [assignment : list of security attributes for which expiration is to be supported] to [assignment : the authorized identified roles].	
FMT_SAE.1.2	For each of these security attributes, the TSF shall be able to [assignment : list of actions to be taken for each security attribute] after the expiration time for the indicated security attribute has passed.	
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: [assignment : list of security management functions to be provided by the TSF].	
FMT_SMR.1.1	The TSF shall maintain the roles [assignment : the authorized identified roles].	
FMT_SMR.1.2	The TSF shall be able to associate users with roles.	
FMT_SMR.2.1	The TSF shall maintain the roles: [assignment : authorized identified roles].	
FMT_SMR.2.2	The TSF shall be able to associate users with roles.	
FMT_SMR.2.3	The TSF shall ensure that the conditions [assignment : conditions for the different roles] are satisfied.	
FMT_SMR.3.1	The TSF shall require an explicit request to assume the following roles: [assignment : the roles].	

F.2.8 Protection of the TSF class

The functional capabilities in the TSF protection class address those requirements dealing with the integrity and management of the mechanisms that provide the TSF

Table F.9: ISO/IEC 15408-2 [11] Functional capabilities (Protection of the TSF class)

Shortname	Definition	Form of assignment in NGN
FPT_AMT.1.1	The TSF shall run a suite of tests [selection : during initial start-up, periodically during normal operation, at the request of an authorized user, [assignment : other conditions]] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.	
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: [assignment : list of types of failures in the TSF].	
FPT_ITA.1.1	The TSF shall ensure the availability of [assignment : list of types of TSF data] provided to a remote trusted IT product within [assignment : a defined availability metric] given the following conditions [assignment : conditions to ensure availability].	
FPT_ITC.1.1	The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.	
FPT_ITI.1.1	The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [assignment : a defined modification metric].	
FPT_ITI.1.2	The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [assignment : action to be taken] if modifications are detected.	
FPT_ITI.2.1	The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [assignment : a defined modification metric].	
FPT_ITI.2.2	The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [assignment : action to be taken] if modifications are detected.	
FPT_ITI.2.3	The TSF shall provide the capability to correct [assignment : type of modification] of all TSF data transmitted between the TSF and a remote trusted IT product.	
FPT_ITT.1.1	The TSF shall protect TSF data from [selection : disclosure, modification] when it is transmitted between separate parts of the TOE.	
FPT_ITT.2.1	The TSF shall protect TSF data from [selection : disclosure, modification] when it is transmitted between separate parts of the TOE.	
FPT_ITT.2.2	The TSF shall separate user data from TSF data when such data is transmitted between separate parts of the TOE.	
FPT_ITT.3.1	The TSF shall be able to detect [selection : modification of data, substitution of data, re-ordering of data, deletion of data, [assignment : other integrity errors]] for TSF data transmitted between separate parts of the TOE.	
FPT_ITT.3.2	Upon detection of a data integrity error, the TSF shall take the following actions: [assignment : specify the action to be taken].	
FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.	
FPT_PHP.1.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.	
FPT_PHP.2.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.	
FPT_PHP.2.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.	
FPT_PHP.3.1	The TSF shall resist [assignment : physical tampering scenarios] to the [assignment : list of TSF devices/elements] by responding automatically such that the TSP is not violated.	
FPT_RCV.1.1	After [assignment : list of failures/service discontinuities] the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.	
FPT_RCV.2.1	When automated recovery from [assignment : list of failures/service discontinuities] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.	
FPT_RCV.2.2	For [assignment : list of failures/service discontinuities], the TSF shall ensure the return of the TOE to a secure state using automated procedures.	
FPT_RCV.3.1	When automated recovery from [assignment : list of failures/service discontinuities] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.	
FPT_RCV.3.2	For [assignment : list of failures/service discontinuities], the TSF shall ensure the return of the TOE to a secure state using automated procedures.	
FPT_RCV.3.3	The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [assignment : quantification] for loss of TSF data or objects within the TSC.	

Shortname	Definition	Form of assignment in NGN
FPT_RCV.3.4	The TSF shall provide the capability to determine the objects that were or were not capable of being recovered.	
FPT_RCV.4.1	The TSF shall ensure that [assignment: list of SFs and failure scenarios] have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.	
FPT_RPL.1.1	The TSF shall detect replay for the following entities: [assignment: list of identified entities].	
FPT_RPL.1.2	The TSF shall perform [assignment: list of specific actions] when replay is detected.	
FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.	
FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.	
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.	
FPT_SEP.2.1	The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.	
FPT_SEP.2.2	The TSF shall enforce separation between the security domains of subjects in the TSC.	
FPT_SEP.2.3	The TSF shall maintain the part of the TSF related to [assignment: list of access control and/or information flow control SFPs] in a security domain for their own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to those SFPs.	
FPT_SEP.3.1	The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.	
FPT_SEP.3.2	The TSF shall enforce separation between the security domains of subjects in the TSC.	
FPT_SEP.3.3	The TSF shall maintain the part of the TSF that enforces the access control and/or information flow control SFPs in a security domain for its own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to the TSP,	
FPT_SSP.2.1	The TSF shall acknowledge, when requested by another part of the TSF, the receipt of an unmodified TSF data transmission.	
FPT_SSP.2.2	The TSF shall ensure that the relevant parts of the TSF know the correct status of transmitted data among its different parts, using acknowledgements.	
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps for its own use.	
FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret [assignment: list of TSF data types] when shared between the TSF and another trusted IT product.	
FPT_TDC.1.2	The TSF shall use [assignment: list of interpretation rules to be applied by the TSF] when interpreting the TSF data from another trusted IT product.	
FPT_TRC.1.1	The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.	
FPT_TRC.1.2	When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [assignment: list of SFs dependent on TSF data replication consistency].	
FPT_TST.1.1	The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions] [assignment: conditions under which self test should occur] to demonstrate the correct operation of the TSF. operation of [selection: [assignment: parts of TSF], the TSF].	
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of [selection: [assignment: parts of TSF], TSF data].	
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.	

F.2.9 Cryptographic support class

The functional capabilities in the cryptographic support class address those requirements dealing with the use of cryptographic material

NOTE: ETSI standards will, in general, not make specific requirements in this class.

Table F.10: ISO/IEC 15408-2 [11] Functional capabilities (cryptographic support class)

Shortname	Definition	Form of assignment in NGN
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment : cryptographic key generation algorithm] and specified cryptographic key sizes [assignment : cryptographic key sizes] that meet the following: [assignment : list of standards].	
FCS_CKM.2.1	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment : cryptographic key distribution method] that meets the following: [assignment : list of standards].	
FCS_CKM.3.1	The TSF shall perform [assignment : type of cryptographic key access] in accordance with a specified cryptographic key access method [assignment : cryptographic key access method] that meets the following: [assignment : list of standards].	
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment : cryptographic key destruction method] that meets the following: [assignment : list of standards].	
FCS_COP.1.1	The TSF shall perform [assignment : list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment : cryptographic algorithm] and cryptographic key sizes [assignment : cryptographic key sizes] that meet the following: [assignment : list of standards].	

F.2.10 Security audit class

The functional capabilities in the security audit class address those requirements dealing with recognizing, recording, storing, and analysing information related to security relevant activities.

Table F.11: ISO/IEC 15408-2 [11] Functional capabilities (security audit class)

Shortname	Definition	Form of assignment in NGN
FAU_ARP.1.1	The TSF shall take [assignment: list of the least disruptive actions] upon detection of a potential security violation.	
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and c) [assignment: other specifically defined auditable events] .	
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information] .	
FAU_GEN.2.1	The TSF shall be able to associate each auditable event with the identity of the user that caused the event.	
FAU_SAA.1.1	The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.	
FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of [assignment: subset of defined auditable events] known to indicate a potential security violation; b) [assignment: any other rules] .	
FAU_SAA.2.1	The TSF shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [assignment: the profile target group] .	
FAU_SAA.2.2	The TSF shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.	
FAU_SAA.2.3	The TSF shall be able to indicate an imminent violation of the TSP when a user's suspicion rating exceeds the following threshold conditions [assignment: conditions under which anomalous activity is reported by the TSF] .	
FAU_SAA.3.1	The TSF shall be able to maintain an internal representation of the following signature events [assignment: a subset of system events] that may indicate a violation of the TSP.	
FAU_SAA.3.2	The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [assignment: the information to be used to determine system activity] .	
FAU_SAA.3.3	The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.	
FAU_SAA.4.1	The TSF shall be able to maintain an internal representation of the following event sequences of known intrusion scenarios [assignment: list of sequences of system events whose occurrence are representative of known penetration scenarios] and the following signature events [assignment: a subset of system events] that may indicate a potential violation of the TSP.	
FAU_SAA.4.2	The TSF shall be able to compare the signature events and event sequences against the record of system activity discernible from an examination of [assignment: the information to be used to determine system activity] .	
FAU_SAA.4.3	The TSF shall be able to indicate an imminent violation of the TSP when system activity is found to match a signature event or event sequence that indicates a potential violation of the TSP.	
FAU_SAR.1.1	The TSF shall provide [assignment: authorized users] with the capability to read [assignment: list of audit information] from the audit records.	
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.	
FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.	
FAU_SAR.3.1	The TSF shall provide the ability to perform [selection: searches, sorting, ordering] of audit data based on [assignment: criteria with logical relations] .	

Shortname	Definition	Form of assignment in NGN
FAU_SEL.1.1	The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: a) [selection : object identity, user identity, subject identity, host identity, event type] b) [assignment : list of additional attributes that audit selectivity is based upon]	
FAU_STG.1.1	The TSF shall protect the stored audit records from unauthorized deletion.	
FAU_STG.1.2	The TSF shall be able to [selection , choose one of: prevent, detect] unauthorized modifications to the stored audit records in the audit trail.	
FAU_STG.2.1	The TSF shall protect the stored audit records from unauthorized deletion.	
FAU_STG.2.2	The TSF shall be able to [selection , choose one of: prevent, detect] unauthorized modifications to the stored audit records in the audit trail.	
FAU_STG.2.3	The TSF shall ensure that [assignment : metric for saving audit records] audit records will be maintained when the following conditions occur: [selection : audit storage exhaustion, failure, attack]	
FAU_STG.3.1	The TSF shall [assignment : actions to be taken in case of possible audit storage failure] if the audit trail exceeds [assignment : pre-defined limit].	
FAU_STG.4.1	The TSF shall [selection , choose one of: 'ignore auditable events', 'prevent auditable events, except those taken by the authorized user with special rights', 'overwrite the oldest stored audit records'] and [assignment : other actions to be taken in case of audit storage failure] if the audit trail is full.	

F.2.11 TOE Access class

The functional capabilities in the TOE Access class address those requirements dealing with the establishment of a user session.

NOTE: In ETSI network standards it is unusual to specify requirements as mandates on the user interface.

Table F.12: ISO/IEC 15408-2 [11] Functional capabilities (TOE Access class)

Shortname	Definition	Form of assignment in NGN
FTA_LSA.1.1	The TSF shall restrict the scope of the session security attributes [assignment : session security attributes], based on [assignment : attributes].	
FTA_MCS.1.1	The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.	
FTA_MCS.1.2	The TSF shall enforce, by default, a limit of [assignment : default number] sessions per user.	
FTA_MCS.2.1	The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [assignment : rules for the number of maximum concurrent sessions].	
FTA_MCS.2.2	The TSF shall enforce, by default, a limit of [assignment : default number] sessions per user.	
FTA_SSL.1.1	The TSF shall lock an interactive session after [assignment : time interval of user inactivity] by: a) clearing or overwriting display devices, making the current contents unreadable; b) disabling any activity of the user's data access/display devices other than unlocking the session.	
FTA_SSL.1.2	The TSF shall require the following events to occur prior to unlocking the session: [assignment : events to occur].	
FTA_SSL.2.1	The TSF shall allow user-initiated locking of the user's own interactive session, by: a) clearing or overwriting display devices, making the current contents unreadable; b) disabling any activity of the user's data access/display devices other than unlocking the session.	
FTA_SSL.2.2	The TSF shall require the following events to occur prior to unlocking the session: [assignment : events to occur].	
FTA_SSL.3.1	The TSF shall terminate an interactive session after a [assignment : time interval of user inactivity].	
FTA_TAB.1.1	Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.	
FTA_TAH.1.1	Upon successful session establishment, the TSF shall display the [selection : date, time, method, location] of the last successful session establishment to the user.	
FTA_TAH.1.2	Upon successful session establishment, the TSF shall display the [selection : date, time, method, location] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.	
FTA_TAH.1.3	The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.	
FTA_TSE.1.1	The TSF shall be able to deny session establishment based on [assignment : attributes].	

Annex G (informative): Bibliography

G.1 UML

The following sources may give the reader a deeper understanding of the use and application of UML and of UML2 in particular.

[UML2-Style] "The elements of UML™ 2.0 style", Scott W. Ambler, Cambridge University Press, 2005. ISBN 0-521-61678-6.

[UML2-Doldi] "UML 2 illustrated: Developing real-time & communications systems", Laurent Doldi, TMSO 2003. ISBN 2-9516600-1-4.

[UML2-OReilly] "UML 2.0 in a nutshell", Dan Pilone with Neil Pitman, O'Reilly. ISBN 0-596-00795-7.

History

Document history		
V4.1.1	February 2003	Publication
V4.2.1	December 2006	Publication