ETSI TR 187 011 V2.1.1 (2008-07)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples

Reference
DTR/TISPAN-07028-NGN-R2

Keywords
security, protocol, methodology

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/chaircor/ETSI_support.asp

Contents

Intellectual Property Rights

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

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

Foreword

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

1 Scope

The present document defines a method, based on the application of ISO/IEC 15408-2 [i.10], for concisely and unambiguously declaring security requirements expressed in ETSI standards. The purpose of the present document is to provide support to developers of ETSI standards in using the security functional components of ISO/IEC 15408-2 [i.10]. In particular it explains the elements in the ISO/IEC 15408-2 [i.10] functional capabilities and describes how they fit within a structured security requirements engineering method. Required elements are defined with respect to the NGN and, where appropriate, are illustrated with examples from the NGN Security programme.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

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

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

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

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

2.1 Normative references

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

Not applicable.

2.2 Informative references

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

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

[i.2] ETSI ES 202 382: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles".

[i.3] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.4] ETSI TR 102 420: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Review of activity on security".

[i.5] ETSI EG 201 383: "Methods for Testing and Specification (MTS);Use of SDL in ETSI deliverables; Guidelines for facilitating validation and the development of conformance tests".

[i.6] ETSI EG 201 872: "Methods for Testing and Specification (MTS); Methodological approach to the use of object-orientation in the standards making process".

[i.7] ETSI EG 202 106: "Methods for Testing and Specification (MTS); Guidelines for the use of formal SDL as a descriptive tool".

[i.8] ITU-T Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[i.9] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.10] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.11] ISO/IEC 15408-3: "Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements".

[i.12] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".

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

[i.13] Directive 2002/58/EC: "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 commu-nications sector (Directive on privacy and electronic communications).

[i.14] IETF RFC 4306: "Internet Key Exchange (IKEv2) Protocol".

[i.15] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[i.16] IETF RFC 4305: "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

access service provider: entity that provides the underlying IP transport connectivity between the consumer and the NGN entities

asset: information or resource to be protected by countermeasures

attack interface: point of attack presented by a functional entity that is reachable from outside a trust domain and which exposes the trust domain to one or more forms of malicious action

NOTE: Malicious action may include but not be restricted to denial of service attack, traffic analysis, masquerade, replay attack, penetration and sabotage.

consumer: domain where the IPTV services are consumed

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

content provider: entity that owns or is licensed to sell content or content assets

NOTE: Although the IPTV Service Provider is the primary source for the Consumer, a direct logical information flow may be set up between Content Provider and Consumer, e.g. for rights management and content protection.

IPTV service provider: entity that prepares the content bundle provided by the content provider for delivery to the consumer by providing metadata, content encryption and physical binaries

NGN service provider: entity offering IP based services, which shares a consistent set of policies and common technologies

NOTE: It handles user authentication/identification, Service Control and security, Charging, IPTV common functions, etc. Several IPTV Service Providers could use the same NGN Service Provider to delivery contents to the consumer. The NGN Service Provider may also provide IPTV service.

secure connection: connection between two functional entities that provides properties of confidentiality, authenticity and integrity proof for any transmission across the connection

secure ICT system: physical implementation of a security standard or set of associated security standards

security standard: communications standard that includes provisions for protecting users and networks from threats to the confidentiality and integrity of both identity and data

trust domain: grouping and/or collection of functional entities (implemented in one or more physical devices) whose operation or ownership arrangements mitigate any risk of exploit to the grouping and/or collection within the trust domain boundary

NOTE 1: In the simplest case, a Trust Domain is a set of physical or functional entities with a single owner/operator who can accurately know the behaviour of those physical or functional entities. Such simple Trust Domains may be joined into larger Trust Domains by bi-lateral agreements between the owners/operators of the physical or functional entities.

NOTE 2: A node is "trusted" (with respect to a given Trust Domain) if and only if it is a member of that domain.

NOTE 3: A node, A, in the Trust Domain is "trusted by" a node, B, (or "B trusts A") if and only if there is a secure connection between the nodes, AND B has configuration information indicating that A is a member of the Trust Domain. Further it is noted that B may or may not be a member of the Trust Domain, e.g. B may be a UE which trusts a given network intermediary, A (e.g. its home proxy).

3.2 Abbreviations

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

CSP	Communications Service Provider
EAL	Evaluation Assurance Level
ICT	Information and Communications Technology
IKE	Internet Key Exchange Version 2
IPTV	Internet Protocol TeleVision
MSC	Message Sequence Chart
NAT	Network Address Translation
NGN	Next Generation Network
PATS	Publicly Available Telecommunications Service
RACS	Resource Admission Control Subsystem
SDL	Specification and Description Language
SDPF	Service Policy Decision Function
TOE	Target Of Evaluation
TOE	Target Of Evaluation

TSF	TOE Security Functions
TVRA	Threat, Vulnerability and Risk Analysis
UDP	User Datagram Protocol
UML	Unified Modelling Language

4 Standards, assets and systems

Communications standards specify detailed requirements that must be met by implementations of the standard in order to be compliant. Depending on the range and complexity of the specified requirements, such standards might be implemented by whole systems or by individual component parts of the systems. In those cases where implementations are likely to either provide or exist within a secure environment, the standard will specify addition, security-related requirements derived from a thorough Threat, Vulnerability and Risk Analysis (TVRA) as defined in TS 102 165-1 [i.3]. In TVRA terminology, a system component that implements a communications standard is referred to as an "asset" and this term is used with the same meaning throughout the present document.

In summary:

- Standards specify requirements for both communication and security aspects;
- Assets are implementations of one or more security-related standards; and
- Systems comprise one or more assets.

5 Objectives and requirements in security standards

5.1 Overview

One of the keys to successful system design is the ability to show the relationships which exist between objectives, requirements and the system design. Furthermore, when all the assets of the system can be shown to be necessary by directly mapping to the requirements they implement, it may be said that the design is complete.

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. Objectives may be considered to be desires rather than mandates. Security requirements are derived from the security objectives and, in order to make this process simpler, requirements can be further subdivided into functional requirements and detailed requirements.

Functional security requirements identify the major functions to be used to realize the security objectives. They are specified at a level which gives an indication of the broad behaviour expected of the asset, generally from the user's perspective. Detailed security requirements, as their name implies, specify a much lower-level of behaviour which would, for example, be measurable at a communications interface. Figure 1 shows how functional requirements can be extracted from existing specifications and from other input and that they are combined to achieve the security objectives of the target system. Each functional requirement is realized by a number of implementation requirements.

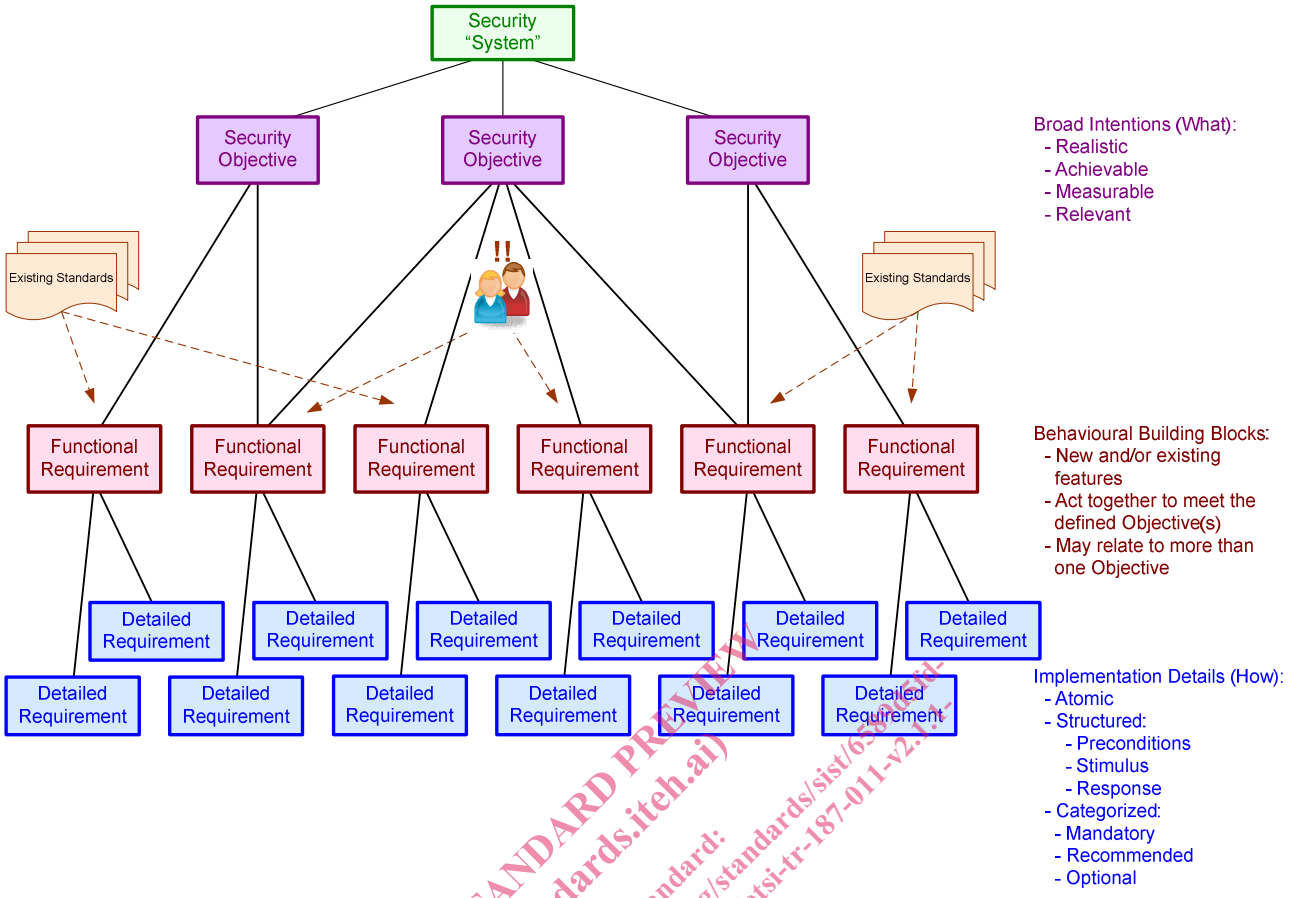

Figure 1: Security objectives and requirements

The following is a simple example of a security objective with a small selection of associated functional requirements and detailed requirements:

- Objective:
  - An NGN should be able to ***restrict access*** to its services so that they are only available to ***validated known users***.
- Functional requirements:
  - An NGN shall allow the establishment of emergency calls on behalf of the user to be performed before the user is identified (from ISO/IEC 15408-2 [i.10] FIA_UID.1.1).
    - This functional requirement arises from asking the question: Is there anything an NGN should allow an unidentified user to do? The answer comes in part from a review of the EU Framework Directive and in particular the Universal Service Directive where some services should be available on a PATS at all times. In addition in some radio networks (e.g. TETRA, GSM) initial camping on a cell is allowed prior to registration and it is registration that involves the exchange of identity.
  - An NGN shall require each user to be successfully identified before allowing any other NGN-mediated actions on behalf of that user (from ISO/IEC 15408-2 [i.10] FIA_UID.1.2).
  - An NGN shall require each user to identify itself before allowing any other NGN-mediated actions on behalf of that user (from ISO/IEC 15408-2 [i.10] FIA_UID.1.1).
- Detailed requirements:
  - An NGN user shall be identified by their NGN CSP assigned identifier in E.164 format.

There are also consequential requirements that need to be taken into account. Whilst in the example a detail requirement is identified this itself requires that the NGN CSP has a means to assign identifiers and to audit the assignment, it will also be necessary to protect the distribution of the identity such that there will be strong assurance that it is given to the correct party.

5.2 Security objectives

The specification of any security system should contain a definition of the security objectives of both the system (including its component assets) and its environment. These objectives are expected to be based upon the assumptions, threats and policies described in the asset security environment. 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:

  A clear definition of which aspects of the identified threats and policies are addressed by each objective;

NOTE 1: 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:

  A clear definition of 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;

NOTE 2: 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.

When developing the security objectives related to a standard it is essential to ensure that each objective is:

- realistic;
- achievable;
- measurable;
- relevant.

NOTE 3: These criteria are a refinement of the commonly used SMART criteria used in some system analysis environments.

Clause 7 provides further details on the meaning of these characteristics.

5.3 Security requirements

5.3.1 Functional security requirements

Security functional requirements should be defined using the model specified in ISO/IEC 15408-2 [i.10] and should be specified for both the asset and, where applicable, its environment. The asset security functional requirements should be classified into the following groups:

- asset security functional requirements:

  - an identification the security functional requirements as specified by reference to the functional components defined in ISO/IEC 15408-2 [i.10] where the assignments and/or selections required have been made for the system under evaluation;