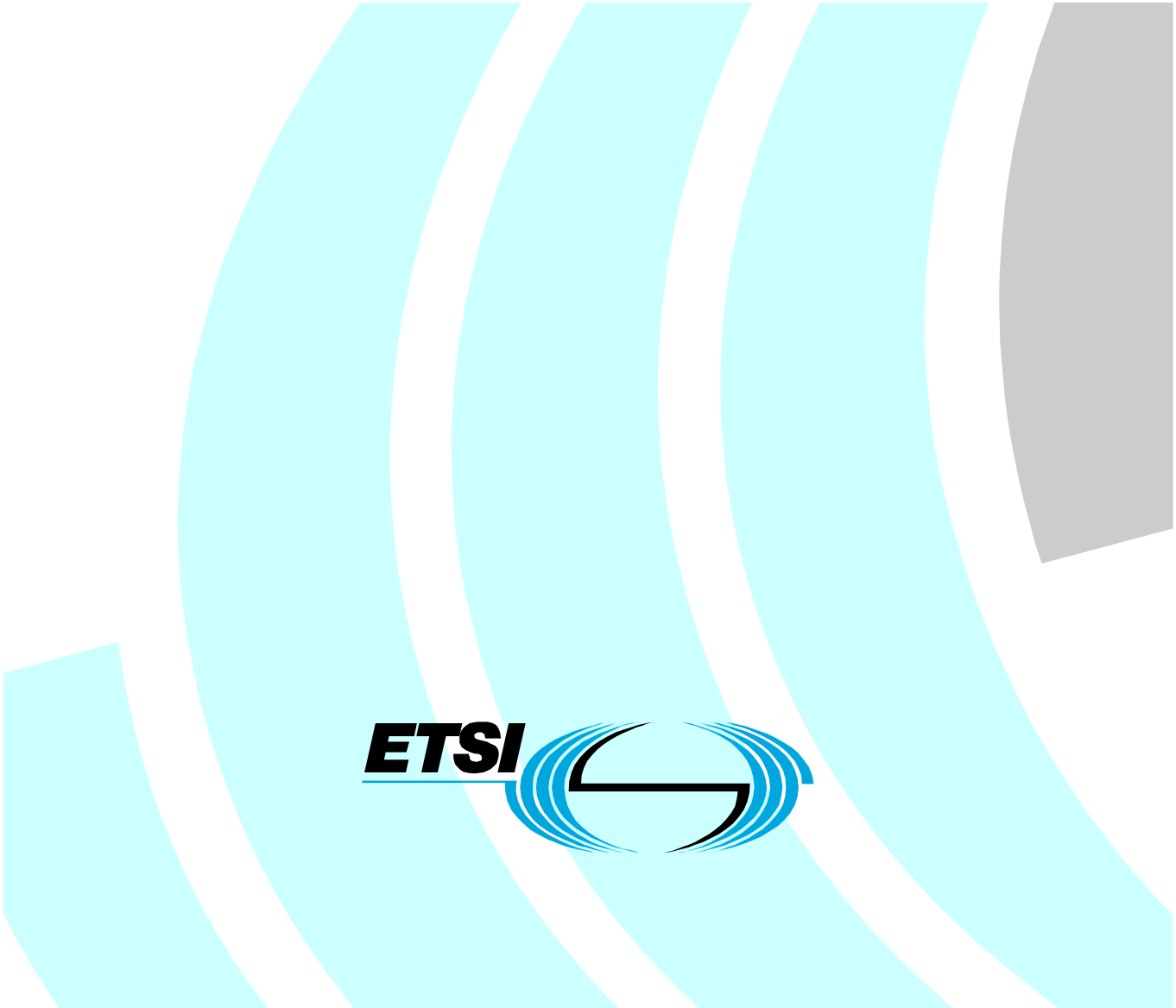
ETSI ES 202 383 V1.1.1 (2005-04)

ETSI Standard

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN);
Security Design Guide;
Method and proforma for defining Security Targets



Reference
DES/TISPAN-07010-Tech

Keywords
IP, methodology, 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

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

Introduction

The present document has been prepared with the sponsorship of the eEurope programme as part of the ETSI support to the eEurope action line for a secure information infrastructure (item 3: Society).

A major part of any security specification, and of a security product, is the measure of assurance it provides with respect to the security it offers.

Information security evaluation contributes to the users' trust and confidence in communications products and services. The use of common criteria for evaluation (as defined in ISO/IEC 15408 [6]) has facilitated mutual recognition of results in many European countries and these countries have also entered into an arrangement with the US and Canada for further mutual recognition of IT security certificates.

The present document is part of a set of standards and guidelines which show how the Common Criteria as identified in ISO/IEC 15408 [6] can be used effectively within the ETSI standardization process. The documents in this set are:

- EG 202 387 [1]: Method for application of Common Criteria to ETSI deliverables;
- ES 202 382 [2]: Method and proforma for defining Protection Profiles;
- ES 202 383: Method and proforma for defining Security Targets.

Between them, these documents identify how standards fit to the Common Criteria and how developers of standards should prepare their standards with a view to support submission for evaluation of product conforming to the standards.

Adoption of Common Criteria objectives in standardization of security countermeasures is also consistent with achieving the objectives and recommendations of the NIS report.

1 Scope

The present document provides guidance on the preparation of Security Targets (ST) based upon ETSI communication standards. The detailed contents of an ST are specified in ISO/IEC 15408-1 [4].

The present document endorses the requirements for STs expressed in ISO/IEC 15408-1 [4] annex C with some specified modifications and additional requirements.

A proforma for a Security Target is given in annex A in tabular form to align with the proforma structure defined for Protection Profiles in ES 202 382 [2].

The use and applicability of the Common Criteria (CC) to the ETSI standardization process is described in EG 202 387 [1].

Conformance to the present document is established by successful evaluation to the requirements of ISO/IEC 15408-3 [5].

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.

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

[3] ETSI TS 102 165-1: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis".

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

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

[6] 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.

3 Definitions and abbreviations

3.1 Definitions

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

3.2 Abbreviations

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

CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
ST	Security Target
TOE	Target Of Evaluation

4 Overview

The evaluation criteria for IT security, generally referred to as the "Common Criteria (CC)", are defined in the multipart standard, ISO/IEC 15408 [6] and are used as the basis for evaluation of security properties of IT products and systems.

CC evaluation involves the preparation of a Security Target (ST) that specifies the security requirements for an identified Target Of Evaluation (TOE) and describes the functional and assurance security measures offered by that TOE to meet the stated requirements. As an ST is directly related to the final TOE and is therefore prepared by the TOE developer there is no impact on the standardization process.

ISO/IEC 15408-3 [5] states that although an ST is not directly evaluated by itself it does describe the TOE that is evaluated.

5 ST development

5.1 Introduction

This clause endorses the content of ISO/IEC 15408-1 [4] annex C and identifies interpretations and guidelines to standards developers of specific clauses in the endorsed standard.

As stated in clause 4 "an ST specifies the security requirements for an identified Target Of Evaluation (TOE) and describes the functional and assurance security measures offered by that TOE to meet the stated requirements. Although an ST is likely to refer to one or more PPs, it is prepared by the TOE developer and has no impact on the standardization process". However whilst the present document acts as an endorsement of the annex C of ISO/IEC 15408-1 [4] this clause gives interpretations and guidance that may be applied when the supporting rationale and PP is derived from an ETSI standard.

As stated in clause 5.1 of ISO/IEC 15408-1 [4] evaluation of an ST gives an intermediate result in the path towards an evaluated TOE. This is in contrast to the outcome of a PP evaluation where the results are catalogued and made available for STs to be developed from. The ST expresses the security requirements that are evaluated in the TOE evaluation process.

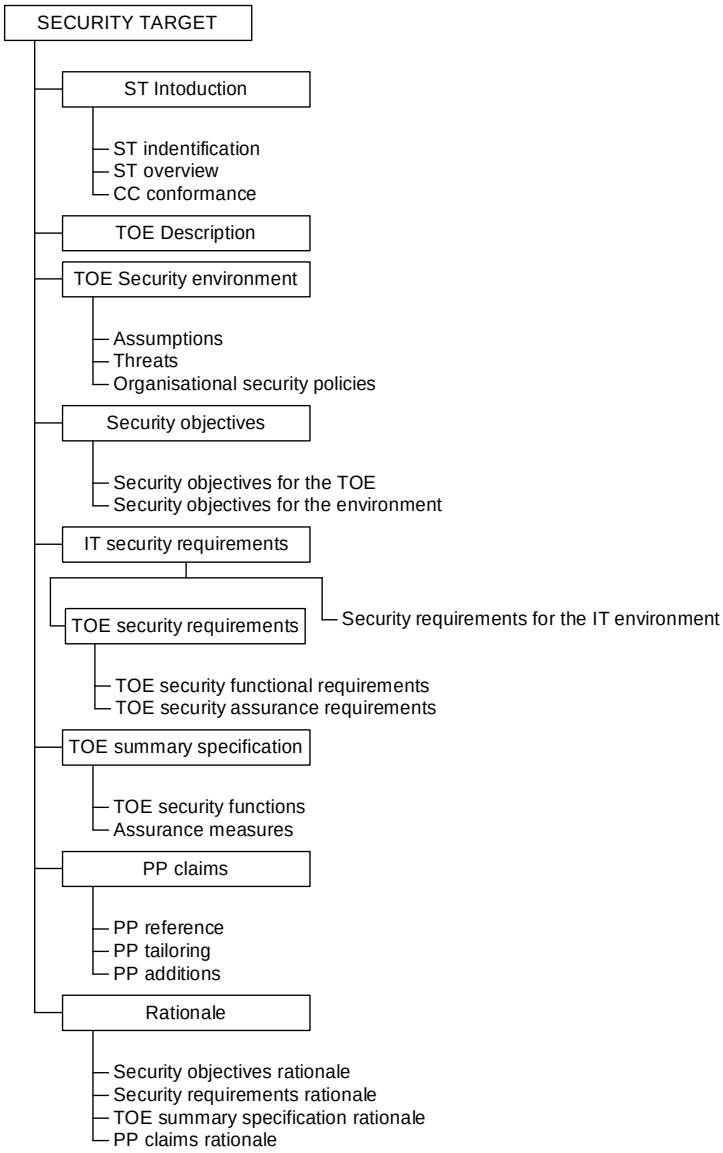


Figure 1: Security Target content

Figure 1 identifies the content of an ST and the notes that follow are given with respect to both the ST structure and to the content of annex C of ISO/IEC 15408-1 [4].

5.2 Endorsement Notice

The text of ISO/IEC 15408-1 [4] annex C is endorsed in full.

5.3 Guidance notes

5.3.1 Introduction

The following clauses offer additional guidance to that found in ISO/IEC 15408-1 [4]. The notes in the present document are intended to assist standards developers identify from existing standards development practices an approach to the development of STs. Not all parts of the required content of an ST are commented upon. Where no guidance notes are provided the existing text in ISO/IEC 15408-1 [4] should be taken as a whole.

5.3.2 ST Introduction (C.2.2)

5.3.2.1 ST identification (C.2.2 bullet item a)

The identification of an ST is not required for cataloguing so is not defined with the same rigour as that of a PP (see [2]). However by following the practice of identification identified for PP in [2] a consistent naming criteria for STs can be established. This is particularly true when the ST may need to be revisited over the life of the TOE.

5.3.2.2 CC conformance claim (C.2.2 bullet item b)

The conformance claim made for the ST has to use one of the terms identified in clause 5.4 of ISO/IEC 15408 -1 [4]. The claims are summarized in table 1.

Table 1: Conformance claim in STs and TOEs

	Claim	Summary	Condition
a	Part 2 conformant	The functional requirements are based only on functional components in part 2	Only one of a or b shall be chosen
b	Part 2 extended	The functional requirements include functional components not found in part 2	
c	Part 3 conformant	The assurance requirements are based only on assurance components in part 3	Only one of c or d or e shall be chosen
d	Part 3 augmented	The assurance requirements are based on an EAL plus other assurance components from part 3 (e.g. complies with all of the requirements of EAL4 and includes compliance with other assurance packages relevant only for higher EALs)	
e	Part 3 extended	The assurance requirements are based on assurance components either not in part 3, or in addition to those in part 3	
f	Conformant to PP	Conforms to all parts of a PP	None

Where conformance to a PP is claimed the PP has to be identified. A later section of the ST, "PP Claims", provides additional detail on the scope of the PP conformance.

Where PP conformance is declared the PP will have identified the assurance packages, normally this is done by reference to an EAL, sometimes by reference to an extension of an EAL (i.e. an EAL with additional evaluation components drawn from part 3). Similarly a PP will have stated the security requirements in terms of part 2 or may base its security functional requirements in a manner where "Part 2 extended" applies.

In large systems where an ST may define only a part of the scope of a PP the claim "Conformant to PP" should not be used.

5.3.3 Target Of Evaluation description (C.2.3)

This should describe both the hardware and software of the TOE. Where the system has been formally modelled in UML the deployment diagram may be used to illustrate this clause. The tone of the text should be not very technical as it is intended to give an understanding of the security requirements being fulfilled by the TOE.

Where UML or similar graphical tools are used in the development of the TOE the author should not assume that the evaluator is familiar with the language and therefore some explanation of the tool and language in use should be given.

5.3.4 TOE security environment (C.2.4)

5.3.4.1 Assumptions (C.2.4 bullet item a)

The purpose of this clause is to guide the evaluator towards an understanding of the application environment of the TOE. This should be used to identify, for example, the type of user who will use the TOE and for what purpose. If a formal modelling exercise has been used in the course of development this will be readily available. In SDL and in UML the top level context diagrams will highlight the assumptions.

5.3.4.2 Threats (C.2.4 bullet item b)

The text in this clause should come from the Vulnerability Analysis exercise. Where the ST claims conformance to a PP the developer shall indicate where the Vulnerability Analysis defined for the PP is extended for the ST and TOE.

5.3.4.3 Organizational security policies (C.2.4 bullet item c)

When identifying the countermeasures required to achieve the TOE's security objectives it is likely that one or more of those countermeasures will be realized by policy measures (see TS 102 165-1 [3] for an example). This clause therefore has to describe how those policy countermeasures are implemented.

5.3.5 Security objectives (C.2.5)

5.3.5.1 Security objectives for the TOE (C.2.5 bullet item b)

The requirement in this clause is to illustrate that there is a clear correlation between threat and countermeasure (noting that the countermeasure may take the form of a security policy). Formal modelling throughout the design process should provide this material as a matter of course. In addition validation and simulation of the model should clearly indicate where clear correlations do not exist and therefore allow for their correction.

5.3.6 IT security requirements (C.2.6)

5.3.6.1 TOE security requirements (C.2.6, bullet item a)

5.3.6.1.1 TOE security assurance requirements (C.2.6, bullet item a.2)

The text of ISO/IEC15408-1 [4] states that the TOE security assurance requirements should be stated by reference to one of the standardized EALs optionally augmented by other part 3 assurance components, or else by reference to one of the standardized EALs with additional assurance requirements not taken from part 3.

The ETSI guide [1] identifies, for a standards developer, how the assurance components from ISO/IEC 15408-3 [5] are addressed in a standard development environment.

5.3.7 PP claims (C.2.8)

5.3.7.1 PP reference (C.2.8 bullet item a)

This clause in an ST is only required where conformance to one or more PPs is claimed (see table 1). Reference should be made to only those PPs that have been evaluated and catalogued and therefore available for reference by the evaluator.

5.3.7.2 PP tailoring (C.2.8 bullet item b)

If the PP includes options then the selection of options shall be identified in the ST. Where the PP is written as defined in [2] and where the PP itself refers to standards where options are selected by means of a PICS document the PP and the PICS should be considered by the ST author as normative references.

5.3.7.3 PP additions (C.2.8 bullet item c)

In general as a PP is an an implementation-independent set of IT security requirements for a category of equipment there is often a requirement to add specific information in the ST that defines the particular methods of implementation. These extend the PP by making more specific the content of the PP to the current TOE. Within the ETSI standards development environment the PIXIT, a document that provides additional information over and above that contained in the PICS and ATS&TP documents required to perform a test, performs a similar role.

5.3.8 Rationale (C.2.9)

The presentation of the rationale is to a very large extent where the ST succeeds or fails. The rationale is a presentation of the evidence that a TOE that conforms to the ST provides an effective set of countermeasures to the threats posed. It is at this point that the method of development of the TOE has a large part to play. Where the methods of standards development recommended in EG 202 387 [1] are used and where, in particular, the development tools allow support of both abstract design and code generation (for example SDL, UML) then a large part of the rationale can be derived from the tools that support the design methods.

5.3.8.1 PP claims rationale (C.2.9 bullet item d)

This is only required if under C.2.2 bullet item b PP Conformance is claimed. If the PP security objectives and requirements are identical to the PP this can also be omitted. It is only is the ST differs in either security objectives or requirements that the rationale for the differences needs to be explained.

Annex A (normative): Security target definition proforma

Security Target					
Introduction					
Doc No.		Version		Date	
Full Title					
Overview					
CC conformance					
TOE Description					
a TOE Security Environment					
a.1 Assumptions					
a.1.1	<<Text>>				<<Reference>>
a.1.2					
…					
a.2 Threats					
a.2.1	<<Text>>				<<Reference>>
a.2.2					
…					
a.3 Organizational security policies					
a.3.1	<<Text>>				<<Reference>>
a.3.2					
…					
b Security Objectives					
b.1 Security objectives for the TOE					
b.1.1	<<Text>>				<<Reference>>
b.1.2	<<Text>>				<<Reference>>
b.2 Security objectives for the environment					
b.2.1	<<Text>>				<<Reference>>
b.2.2					
c IT Security Requirements					
c.1 Security requirements for the IT environment					
c.1.1					
c.1.2					
c.2 TOE security requirements					
c.2.1 TOE security functional requirements					
c.2.1.1	<<Text>>				<<Reference>>
c.2.1.2					
c.2.2 TOE security assurance requirements					
c.1.2.1	<<Text>>				<<Reference>>
c.1.2.2					
d TOE Security Requirements					
e TOE summary specification					
f PP claims					
f.1 PP reference					
f.2 PP tailoring					
f.3 PP additions					
g Rationale					

Annex B (informative): Bibliography

ETSI ETR 332 (1996): "Security Techniques Advisory Group (STAG); Security requirements capture".

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

History

Document history		
V1.1.1	February 2005	Membership Approval Procedure MV 20050401: 2005-02-01 to 2005-04-01
V1.1.1	April 2005	Publication