Common Criteria Security Evaluation

Pierre.Paradinas@cnam.fr

Introduction & definitions

- The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that:
  - Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfillment of particular security properties, to a certain extent or assurance;
  - Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;
  - The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation;
  - These certificates are recognized by all the signatories of the CCRA.
- The CC is the driving force for the widest available mutual recognition of **secure IT products.**

Common Criteria Recognition Arrangement

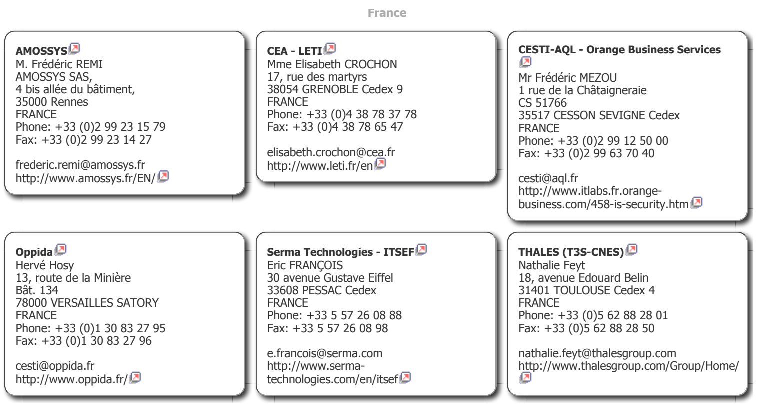
- The Participants in this Arrangement share the following objectives:
  - to ensure that evaluations of Information Technology (IT) products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles;
  - to improve the availability of evaluated, security-enhanced IT products and protection profiles;
  - to eliminate the burden of duplicating evaluations of IT products and protection profiles;
  - to continuously improve the efficiency and cost-effectiveness of the evaluation and certification/validation process for IT products and protection profiles.

Members

- Certificate Authorizing Members
  - Australia, Canada, France, Germany, Italy, Japan, Netherlands, Norway, NZ, Korean, Spain, Sweden, Turkey, UK, USA
- Certificate Consuming Members
  - Austria, Czech Republic, Denmark, Finland, Greece, Hungary, India, Israel, Malaysia, Pakistan, Singapore

Le schéma en France

- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
- Les laboratoires d'évaluation



France

AMOSSYS
M. Frédéric REMI
AMOSSYS SAS,
4 bis allée du bâtiment,
35000 Rennes
FRANCE
Phone: +33 (0)2 99 23 15 79
Fax: +33 (0)2 99 23 14 27

frederic.remi@amossys.fr
http://www.amossys.fr/EN/

CEA - LETI
Mme Elisabeth CROCHON
17, rue des martyrs
38054 GRENOBLE Cedex 9
FRANCE
Phone: +33 (0)4 38 78 37 78
Fax: +33 (0)4 38 78 65 47

elisabeth.crochon@cea.fr
http://www.leti.fr/en

CESTI-AQL - Orange Business Services
Mr Frédéric MEZOU
1 rue de la Châtaigneraie
CS 51766
35517 CESSON SEVIGNE Cedex
FRANCE
Phone: +33 (0)2 99 12 50 00
Fax: +33 (0)2 99 63 70 40

cesti@aql.fr
http://www.itlabs.fr.orange-business.com/458-is-security.htm

Oppida
Hervé Hosy
13, route de la Minière
Bât. 134
78000 VERSAILLES SATORY
FRANCE
Phone: +33 (0)1 30 83 27 95
Fax: +33 (0)1 30 83 27 96

cesti@oppida.fr
http://www.oppida.fr/

Serma Technologies - ITSEF
Eric FRANÇOIS
30 avenue Gustave Eiffel
33608 PESSAC Cedex
FRANCE
Phone: +33 5 57 26 08 88
Fax: +33 5 57 26 08 98

e.francois@serma.com
http://www.serma-technologies.com/en/itsef

THALES (T3S-CNES)
Nathalie Feyt
18, avenue Edouard Belin
31401 TOULOUSE Cedex 4
FRANCE
Phone: +33 (0)5 62 88 28 01
Fax: +33 (0)5 62 88 28 50

nathalie.feyt@thalesgroup.com
http://www.thalesgroup.com/Group/Home/

The documentation of CC

- This version of the Common Criteria for Information Technology Security Evaluation (CC v3.1) is the first major revision since being published as CC v2.3 in 2005.
- The content
  - CC version 3.1 consists of the following parts:
    - Part 1: Introduction and general model
    - Part 2: Security functional components
    - Part 3: Security assurance components

Introduction & Scope

- The CC permits comparability between the results of independent security evaluations. The CC does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software.
- The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfill their security needs.
- The CC is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.

CC introduction

- The CC is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products. Therefore users of the standard are cautioned to exercise care that this flexibility is not misused. For example, using the CC in conjunction with unsuitable evaluation methods, irrelevant security properties, or inappropriate IT products, may result in meaningless evaluation results.
- The CC addresses protection of assets from unauthorised disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. The CC may also be applicable to aspects of IT security outside of these three. The CC is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. Apart from IT security, the CC may be applied in other areas of IT, but makes no claim of applicability in these areas.

Out of the CC scope

- Certain topics, because they involve specialised techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of the CC. Some of these are identified below.
  - The CC does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality. However, it is recognised that significant security can often be achieved through or supported by administrative measures such as organisational, personnel, physical, and procedural controls.
  - The evaluation of some technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered, although many of the concepts addressed will be applicable to that area.
  - The CC does not address the evaluation methodology under which the properties of cryptography be required, the evaluation scheme under which the CC is applied must make provision for such assessments.

Out of the CC scope (cont'd)

- The CC does not address the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that the CC will be used for evaluation purposes in the context of such a framework.
- The procedures for use of evaluation results in accreditation are outside the scope of the CC. Accreditation is the administrative process whereby authority is granted for the operation of an IT product (or collection thereof) in its full operational environment including all of its non-IT parts. The results of the evaluation process are an input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related properties and their relationship to the IT security parts, accreditors should make separate provisions for those aspects.
- The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the CC. Should independent assessment of mathematical properties of cryptography be required, the evaluation scheme under which the CC is applied must make provision for such assessments.

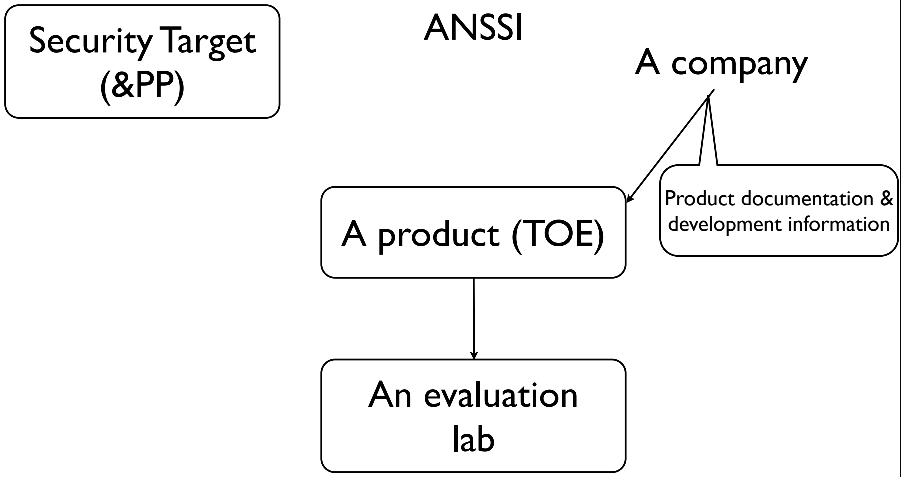
Definitions & Scope

- Part one provides an overview of all parts of the CC standard. It describes the various parts of the standard; defines the terms and abbreviations to be used in all parts of the standard; establishes the core concept of a Target of Evaluation (TOE); the evaluation context and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.
- It defines the various operations by which the functional and assurance components given in CC Part 2 and CC Part 3 may be tailored through the use of permitted operations.
- The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation, evaluation results are described. This part of the CC gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model. General information about the evaluation methodology are given in the CEM and the scope of evaluation schemes is provided.

The TOE

- A TOE is defined as a set of software, firmware and/or hardware possibly accompanied by guidance.
- A TOE may be a part of an IT product. The evaluation is only on TOE not on all the IT (or not) product.
- Examples
  - A software application;
  - An operating system;
  - A software application in combination with an operating system;
  - A software application in combination with an operating system and a workstation;
  - An operating system in combination with a workstation;
  - A smart card integrated circuit;
  - The cryptographic co-processor of a smart card integrated circuit;
  - A Local Area Network including all terminals, servers, network equipment and software;
  - A database application excluding the remote client software normally associated with that database application.

General presentation



Security Target (&PP)

ANSSI

A company

Product documentation & development information

A product (TOE)

An evaluation lab

The CC Audience

- There are three groups with a general interest in evaluation of the security properties of TOEs: consumers, developers and evaluators.
- Consumers
  - The CC is written to ensure that evaluation fulfils the needs of the consumers as this is the fundamental purpose and justification for the evaluation process.
  - Consumers can use the results of evaluations to help decide whether a TOE fulfils their security needs. These security needs are typically identified as a result of both risk analysis and policy direction. Consumers can also use the evaluation results to compare different TOEs.
  - The CC gives consumers, especially in consumer groups and communities of interest, an implementation-independent structure, termed the Protection Profile (PP), in which to express their security requirements in an unambiguous manner.

The CC Audience

- Developers
  - The CC is intended to support developers in preparing for and assisting in the evaluation of their TOEs and in identifying security requirements to be satisfied by those TOEs. These requirements are contained in an implementation-dependent construct termed the Security Target (ST). This ST may be based on one or more PPs to show that the ST conforms to the security requirements from consumers as laid down in those PPs.
  - The CC can then be used to determine the responsibilities and actions to provide evidence that is necessary to support the evaluation of the TOE against these requirements. It also defines the content and presentation of that evidence.

The CC Audience

- Evaluators
  - The CC contains criteria to be used by evaluators when forming judgements about the conformance of TOEs to their security requirements. The CC describes the set of general actions the evaluator is to carry out. Note that the CC does not specify procedures to be followed in carrying out those actions.

The different parts of the CC

- The different parts of the CC
  - Part 1, Introduction and general model is the introduction to the CC. It defines the general concepts and principles of IT security evaluation and presents a general model of evaluation.
  - Part 2, Security functional components establishes a set of functional components that serve as standard templates upon which to base functional requirements for TOEs. CC Part 2 catalogues the set of functional components and organizes them in families and classes.
  - Part 3, Security assurance components establishes a set of assurance components that serve as standard templates upon which to base assurance requirements for TOEs. CC Part 3 catalogues the set of assurance components and organizes them into families and classes. CC Part 3 also defines evaluation criteria for PPs and STs and presents seven pre-defined assurance packages which are called the Evaluation Assurance Levels (EALs).

The different use of CC parts

	Consumers	Developers	Evaluators
Part 1	Use for background information and are obliged to use for reference purposes. Guidance structure for PPs.	Use for background information and reference purposes. Are obliged to use for the development of security specifications for TOEs.	Are obliged to use for reference purposes and for guidance in the structure for PPs and STs.
Part 2	Use for guidance and reference when formulating statements of requirements for a TOE.	Are obliged to use for reference when interpreting statements of functional requirements and formulating functional specifications for TOEs.	Are obliged to use for reference when interpreting statements of functional requirements.
Part 3	Use for guidance when determining required levels of assurance.	Use for reference when interpreting statements of assurance requirements and determining assurance approaches of TOEs.	Use for reference when interpreting statements of assurance requirements.

Table 1 - Road map to the Common Criteria

Evaluation context

- In order to achieve greater comparability between evaluation results, evaluations should be performed within the framework of an authoritative evaluation scheme that sets the standards, monitors the quality of the evaluations and administers the regulations to which the evaluation facilities and evaluators must conform.
- The CC does not state requirements for the regulatory framework. However, consistency between the regulatory frameworks of different evaluation authorities will be necessary to achieve the goal of mutual recognition of the results of such evaluations.
- A second way of achieving greater comparability between evaluation results is using a common methodology to achieve these results. For the CC, this methodology is given in the CEM.

Evaluation context

- Use of a common evaluation methodology contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgement and background knowledge for which consistency is more difficult to achieve. In order to enhance the consistency of the evaluation findings, the final evaluation results may be submitted to a certification process.
- The certification process is the independent inspection of the results of the evaluation leading to the production of the final certificate or approval, which is normally publicly available. The certification process is a means of gaining greater consistency in the application of IT security criteria.
- The evaluation schemes and certification processes are the responsibility of the evaluation authorities that run such schemes and processes and are outside the scope of the CC.

General Model (Assets and countermeasures)

- Security is concerned with the protection of assets. Assets are entities that someone places value upon. Examples of assets include:
  - contents of a file or a server;
  - ...
- but given that value is highly subjective, almost anything can be an asset.
  - The environment(s) in which these assets are located is called the operational environment. Examples of (aspects of) operational environments are:
    - the computer room of a bank;
    - ...
- Many assets are in the form of information that is stored, processed and transmitted by IT products to meet requirements laid down by owners of the information. Information owners may require that availability, dissemination and modification of any such information are strictly controlled and that the assets are protected from threats by countermeasures.

Schema & Relationship

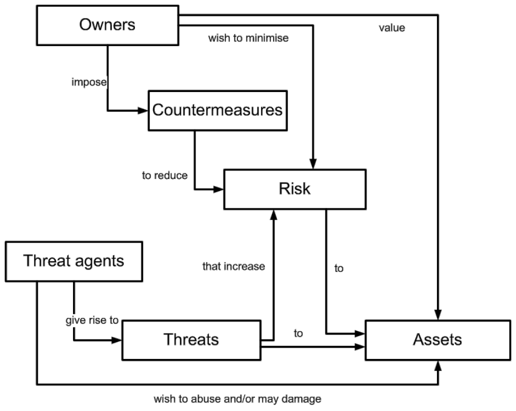


Figure 2 - Security concepts and relationships

Owners/Assets

- The owners is responsible for the assets.
- The owner needs to answer :
  - the countermeasures are **sufficient**: if the countermeasures do what they claim to do, the threats to the assets are countered;
  - the countermeasures are **correct**: the countermeasures do what they claim to do.

The evaluation

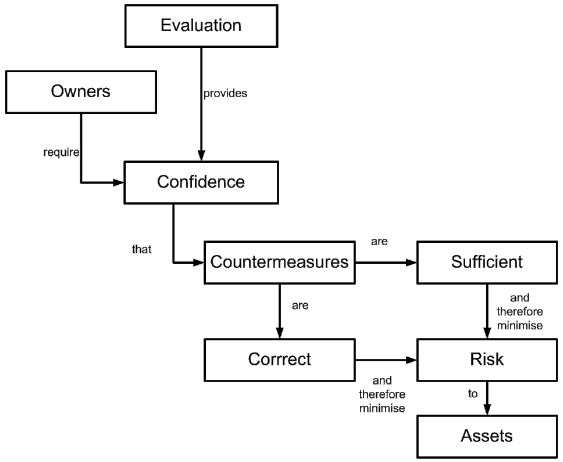


Figure 3 - Evaluation concepts and relationships

The sufficiency of the countermeasure

- In an evaluation, sufficiency of the countermeasures is analysed through a construct called the Security Target.
  - The Security Target begins with describing the assets and the threats to those assets. The Security Target then describes the countermeasures (in the form of Security Objectives) and demonstrates that these countermeasures are sufficient to counter these threats: if the countermeasures do what they claim to do, the threats are countered.
  - The Security Target then divides these countermeasures in two groups:
    - the security objectives for the TOE: these describe the countermeasure(s) for which correctness will be determined in the evaluation;
    - the security objectives for the Operational Environment: these describe the countermeasures for which correctness will not be determined in the evaluation.

The sufficiency of the countermeasure

- The reasons for this division are:
  - The CC is only suitable for assessing the correctness of IT countermeasures. Therefore the non-IT countermeasures (e.g. human security guards, procedures) are always in the Operational Environment.
  - Assessing correctness of countermeasures costs time and money, possibly making it infeasible to assess the correctness of all IT countermeasures.
  - The correctness of some IT countermeasures may already have been assessed in another evaluation. It is therefore not cost-effective to assess this correctness again.

The sufficiency of the countermeasure

- For the TOE (the IT countermeasures whose correctness will be assessed during the evaluation), the Security Target requires a further detailing of the security objectives for the TOE in Security Functional Requirements (SFRs). These SFRs are formulated in a standardised language (described in CC Part 2) to ensure exactness and facilitate comparability.
  - In summary, the Security Target demonstrates that:
    - The SFRs meet the security objectives for the TOE;
    - The security objectives for the TOE and the security objectives for the operational environment counter the threats;
    - And therefore, the SFRs and the security objectives for the operational environment counter the threats.
- From this it follows that a correct TOE (meeting the SFRs) in combination with a correct operational environment (meeting the security objectives for the operational environment) will counter the threats. In the next two sections correctness of the TOE and correctness of the operational environment are discussed separately.

Correctness of the TOE

- Correctness of the TOE
  - A TOE may be incorrectly designed and implemented, and may therefore contain errors that lead to vulnerabilities. By exploiting these vulnerabilities, attackers may still damage and/or abuse the assets.
    - These vulnerabilities may arise from accidental errors made during development, poor design, intentional addition of malicious code, poor testing etc.
    - To determine correctness of the TOE, various activities can be performed such as:
      - testing the TOE;
      - examining various design representations of the TOE;
      - examining the physical security of the development environment of the TOE.

Evaluation

- The CC recognises two types of evaluation: an ST/TOE evaluation, which is described below, and an evaluation of PPs, which is defined in CC Part 3. In many places, the CC uses the term evaluation (without qualifiers) to refer to an ST/TOE evaluation.
  In the CC an ST/TOE evaluation proceeds in two steps:
  - a) An ST evaluation: where the sufficiency of the TOE and the operational environment are determined;
  - b) A TOE evaluation: where the correctness of the TOE is determined. As said earlier, the TOE evaluation does not assess correctness of the operational environment.

Protection Profiles and Packages

- To allow consumer groups and communities of interest to express their security needs, and to facilitate writing STs, this part of the CC provides two special constructs: packages and Protection Profiles (PPs). In the following two sections these constructs are described in more detail, followed by a section on how these constructs can be used.
  - A package is a named set of security requirements. A package is either
    - a functional package, containing only SFRs, or
    - an assurance package, containing only SARs.

Protection Profiles and Packages

- Protection Profiles
  Whereas an ST always describes a specific TOE (e.g. the MinuteGap v18.5 Firewall), a PP is intended to describe a TOE type (e.g. firewalls). The same PP may therefore be used as a template for many different STs to be used in different evaluations. A detailed description of PPs is given in Annex B.
  In general an ST describes requirements for a TOE and is written by the developer of that TOE, while a PP describes the general requirements for a TOE type, and is therefore typically written by:
  - A user community seeking to come to a consensus on the requirements for a given TOE type;
  - A developer of a TOE, or a group of developers of similar TOEs wishing to establish a minimum baseline for that type of TOE;
  - A government or large corporation specifying its requirements as part of its acquisition process.

PP, ST & TOE

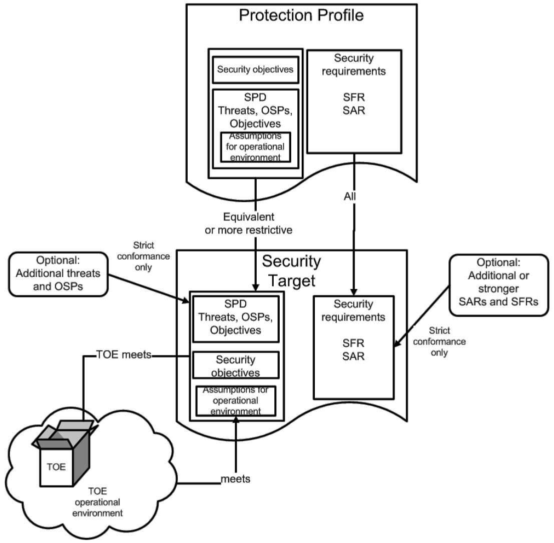


Figure 4 - Relationships between PP, ST and TOE contents

Using PPs and packages

- If an ST claims to be conformant to one or more packages and/or Protection Profiles, the evaluation of that ST will (among other properties of that ST) demonstrate that the ST actually conforms to these packages and/or PPs that they claim conformance to. Details of this determination of conformance can be found in Annex A.
  - This allows the following process:
    - An organisation seeking to acquire a particular type of IT security product develops their security needs into a PP, then has this evaluated and publishes it;
    - A developer takes this PP, writes an ST that claims conformance to the PP and has this ST evaluated;
    - The developer then builds a TOE (or uses an existing one) and has this evaluated against the ST.

Using Multiple Protection Profiles

- The CC also allows PPs to conform to other PPs, allowing chains of PPs to be constructed, each based on the previous one(s).
- For instance, one could take a PP for an Integrated Circuit and a PP for a Smart Card OS, and use these to construct a Smart Card PP (IC and OS) that claims conformance to the other two. One could then write a PP on Smart Cards for Public Transport based on the Smart Card PP and a PP on Applet Loading. Finally, a developer could then construct an ST based on this Smart Cards for Public Transport PP.

Evaluation results

- This chapter presents the expected results from PP and ST/TOE evaluations performed according to the CEM.

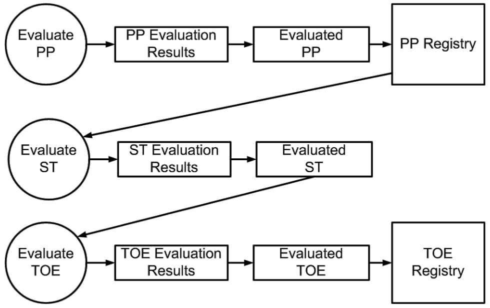


Figure 5 - Evaluation results

- STs may be based on packages, evaluated PPs or non-evaluated PPs - however this is not mandatory, as STs do not have to be based on anything at all.

Results of an ST/TOE evaluation

- CC Part 3 contains the evaluation criteria that an evaluator is obliged to consult in order to determine whether sufficient assurance exists that the TOE satisfies the SFRs in the ST. Evaluation of the TOE shall therefore result in a pass/fail statement for the ST. If both the ST and the TOE evaluation have resulted in a pass statement, the underlying product is eligible for inclusion in a registry. The results of evaluation shall also include a "Conformance Claim" as defined in the next section.

Conformance claim

- The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation.
- Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:
  - Package name Conformant - A PP or ST is conformant to a pre- defined package (e.g. EAL) if:
    - the SFRs of that PP or ST are identical to the SFRs in the package, or
    - the SARs of that PP or ST are identical to the SARs in the package.
  - Package name Augmented - A PP or ST is an augmentation of a predefined package if:
    - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
    - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Use of ST/TOE evaluation results

- Once an ST and a TOE have been evaluated, asset owners can have the assurance (as defined in the ST) that the TOE, together with the operational environment, counters the threats. The evaluation results may be used by the asset owner in deciding whether to accept the risk of exposing the assets to the threats.
  - However, the asset owner should carefully check whether:
    - the Security Problem Definition in the ST matches the security problem of the asset owner;
    - the Operational Environment of the asset owner conforms (or can be made to conform) to the security objectives for the Operational Environment described in the ST.
- If either of these is not the case, the TOE may not be suitable for the purposes of the asset owner.

Evolution/Correction

- Additionally, once an evaluated TOE is in operation, it is still possible that previously unknown errors or vulnerabilities in the TOE may surface. In that case, the developer may correct the TOE (to repair the vulnerabilities) or change the ST to exclude the vulnerabilities from the scope of the evaluation. In either case, the old evaluation results may no longer be valid.
- If it is deemed necessary that confidence is regained, re-evaluation is needed. The CC may be used for this re-evaluation, but detailed procedures for re-evaluation are outside the scope of this part of the CC.

ST content

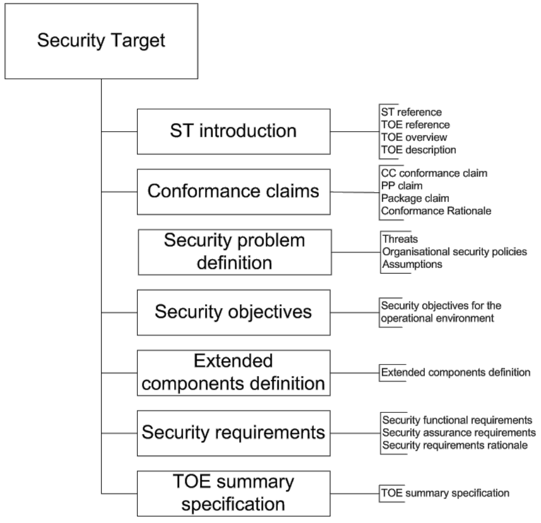
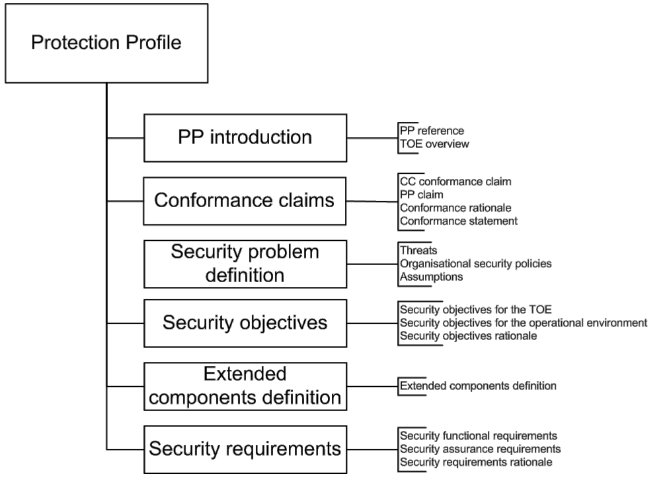

Security Target
ST introduction
ST reference
TOE reference
TOE overview
TOE description
Conformance claims
CC conformance claim
PP claim
Package claim
Conformance Rationale
Security problem definition
Threats
Organisational security policies
Assumptions
Security objectives
Security objectives for the operational environment
Extended components definition
Extended components definition
Security requirements
Security functional requirements
Security assurance requirements
Security requirements rationale
TOE summary specification
TOE summary specification

Figure 6 - Security Target contents

PP content



Protection Profile

PP introduction: PP reference; TOE overview

Conformance claims: CC conformance claim; PP claim; Conformance rationale; Conformance statement

Security problem definition: Threats; Organisational security policies; Assumptions

Security objectives: Security objectives for the TOE; Security objectives for the operational environment; Security objectives rationale

Extended components definition: Extended components definition

Security requirements: Security functional requirements; Security assurance requirements; Security requirements rationale

Figure 10 - Protection Profile contents

The other part of the standard

- Part 2: Security functional components
- Document of 321 pages...
- Scope
  - This part of the CC defines the required structure and content of security **functional components** for the purpose of security evaluation. It includes a **catalogue of functional components** that will meet the common security functionality requirements of many IT products.

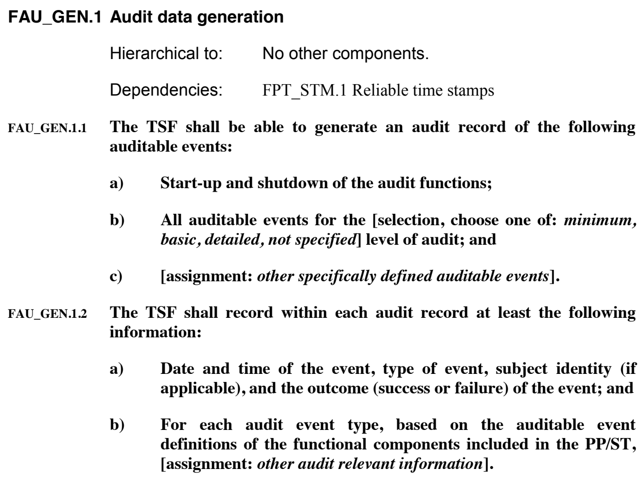
The users of part 2

- Security functional components express security requirements intended to counter threats in the assumed operating environment of the TOE and/or cover any identified organisational security policies and assumptions.
- The users of part 2 are :
  - Consumers, who use this CC Part 2 when selecting components to express functional requirements to satisfy the security objectives expressed in a PP or ST.
  - Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, may find a standardised method to understand those requirements in this part of the CC.
  - Evaluators, who use the functional requirements defined in this part of the CC in verifying that the TOE functional requirements expressed in the PP or ST satisfy the IT security objectives and that all dependencies are accounted for and shown to be satisfied. Evaluators also should use this part of the CC to assist in determining whether a given TOE satisfies stated requirements.

Functional requirement paradigm

- This part of the CC is a catalogue of security functional components that can be specified for a Target of Evaluation (TOE)
- TOE evaluation is concerned primarily with ensuring that a defined set of security functional requirements (SFRs) is enforced over the TOE resources.
- The SFRs may define multiple Security Function Policies (SFPs) to represent the rules that the TOE must enforce.

Example of SFR



FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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 (if applicable), 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*].

The Security Assurance Components

- Part 3 is only 232 pages !
- The scope is :
  - This CC Part 3 defines the assurance requirements of the CC. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance for component TOEs,...
  - ...
  - and the criteria for evaluation of PPs and STs.

Assurance paradigm

- Assurance approach
  - The CC philosophy is to provide assurance based upon an evaluation (active investigation) of the IT product that is to be trusted
  - The CC proposes measuring the validity of the documentation and of the resulting IT product by expert evaluators with increasing emphasis on scope, depth, and rigour.
- It is assumed that there are threat agents that will actively seek to exploit opportunities to violate security policies...
  - vulnerabilities should be:
    - eliminated -- that is, active steps should be taken to expose, and remove or neutralise, all exercisable vulnerabilities;
    - minimised -- that is, active steps should be taken to reduce, to an acceptable residual level, the potential impact of any exercise of a vulnerability;
    - monitored -- that is, active steps should be taken to ensure that any attempt to exercise a residual vulnerability will be detected so that steps can be taken to limit the damage.

Cause of vulnerability

- Vulnerabilities can arise through failures in
  - requirements -- that is, an IT product may possess all the functions and features required of it and still contain vulnerabilities that render it unsuitable or ineffective with respect to security;
  - development -- that is, an IT product does not meet its specifications and/or vulnerabilities have been introduced as a result of poor development standards or incorrect design choices;
  - operation -- that is, an IT product has been constructed correctly to a correct specification but vulnerabilities have been introduced as a result of inadequate controls upon the operation.

Assurance paradigm

- Evaluation has been the traditional means of gaining assurance, and is the basis of the CC approach. Evaluation techniques can include, but are not limited to:
  - analysis and checking of process(es) and procedure(s);
  - checking that process(es) and procedure(s) are being applied;
  - analysis of the correspondence between TOE design representations;
  - analysis of the TOE design representation against the requirements;
  - verification of proofs;
  - analysis of guidance documents;
  - analysis of functional tests developed and the results provided;
  - independent functional testing;
  - analysis for vulnerabilities (including flaw hypothesis);
  - penetration testing.

EALs

- Evaluation Assurance Level
  - 7 levels of Evaluation Assurance
  - But is also possible to
    - While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of "**augmentation**" allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL.

Overview of EALs

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC	▨	**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP	▨	▨	▨	**1**	1	**2**	2
	ADV_INT	▨	▨	▨	▨	**2**	**3**	3
	ADV_SPM	▨	▨	▨	▨	▨	**1**	1
	ADV_TDS	▨	**1**	**2**	**3**	**4**	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL	▨	**1**	1	1	1	1	1
	ALC_DVS	▨	▨	**1**	1	1	**2**	2
	ALC_FLR	▨	▨	▨	▨	▨	▨	▨
	ALC_LCD	▨	▨	**1**	1	1	1	**2**
	ALC_TAT	▨	▨	▨	**1**	**2**	**3**	3
Security Target evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD	▨	**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV	▨	**1**	**2**	2	2	**3**	3
	ATE_DPT	▨	▨	**1**	1	**3**	3	**4**
	ATE_FUN	▨	**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

Table 1 - Evaluation assurance level summary

EAL 1

- Evaluation assurance level 1 (EAL1) - functionally tested
  - EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious.
  - EAL1 provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behavior.

EAL 2

- Evaluation assurance level 2 (EAL2) - structurally tested
- EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise.
- This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.

EAL 3

- Evaluation assurance level 3 (EAL3) - methodically tested and checked
- EAL3 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation, and an architectural description of the design of the TOE, to understand the security behaviour.
- This EAL represents a meaningful increase in assurance from EAL2 by requiring more complete testing coverage of the security functionality and mechanisms and/or procedures that provide some confidence that the TOE will not be tampered with during development.

EAL 4

- Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed
- EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.
- EAL4 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation, to understand the security behaviour.
- This EAL represents a meaningful increase in assurance from EAL3 by requiring more design description, the implementation representation for the entire TSF, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development.

EAL 5

- Evaluation assurance level 5 (EAL5) - semiformally designed and tested
- EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.
  - EAL5 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the design of the TOE, and the implementation, to understand the security behaviour. A modular TSF design is also required.
- This EAL represents a meaningful increase in assurance from EAL4 by requiring semiformal design descriptions, a more structured (and hence analysable) architecture, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development.

EAL 6

- Evaluation assurance level 6 (EAL6) - semiformally verified design and tested
- EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.
  - EAL6 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, the design of the TOE, and the implementation to understand the security behaviour. Assurance is additionally gained through a formal model of select TOE security policies and a semiformal presentation of the functional specification and TOE design. A modular, layered and simple TSF design is also required.
- This EAL represents a meaningful increase in assurance from EAL5 by requiring more comprehensive analysis, a structured representation of the implementation, more architectural structure (e.g. layering), more comprehensive independent vulnerability analysis, and improved configuration management and development environment controls.

EAL 7

- Evaluation assurance level 7 (EAL7) - formally verified design and tested
- EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.
  - EAL7 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, the design of the TOE, and a structured presentation of the implementation to understand the security behaviour.
- This EAL represents a meaningful increase in assurance from EAL6 by requiring more comprehensive analysis using formal representations and formal correspondence, and comprehensive testing.

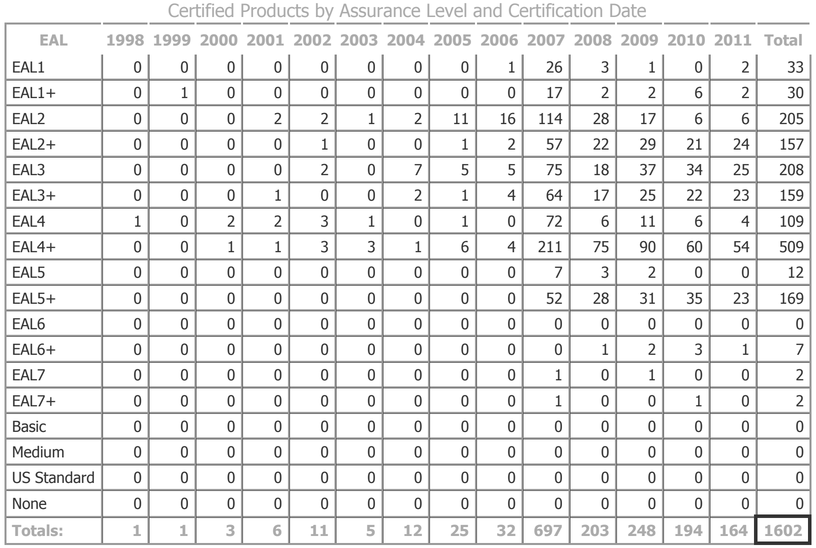
About CEM document

- Scope :
  - The Common Methodology for Information Technology Security Evaluation (CEM) is a companion document to the Common Criteria for Information Technology Security Evaluation (CC). The CEM defines the minimum actions to be performed by an evaluator in order to conduct a CC evaluation, using the criteria and evaluation evidence defined in the CC.
- Pages : 424

1602 Products ! (figures are on the Oct. 2011)

Product Family	**Nb of Certified Products**
Access Control Devices and Systems	75
Biometric Systems and Devices	2
Boundary Protection Devices and Systems	131
Data Protection	71
Databases	59
Detection Devices and Systems	41
ICs, Smart Cards and Smart Card-Related Devices and Systems	459
Key Management Systems	35
Multi-Function Devices	171
Network and Network-Related Devices and Systems	132
Operating System	115
Other Devices and Systems	248
Products for Digital Signatures	62
Trusted Computing	1

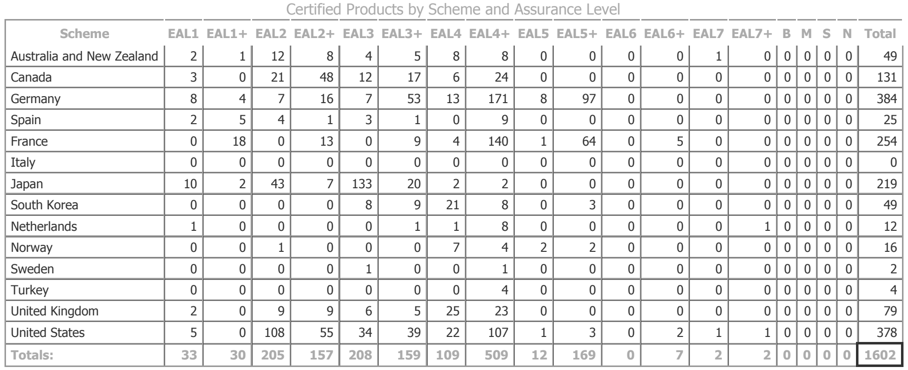
Level/Per years



Certified Products by Assurance Level and Certification Date

EAL	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	Total
EAL1	0	0	0	0	0	0	0	0	1	26	3	1	0	2	33
EAL1+	0	1	0	0	0	0	0	0	0	17	2	2	6	2	30
EAL2	0	0	0	2	2	1	2	11	16	114	28	17	6	6	205
EAL2+	0	0	0	0	1	0	0	1	2	57	22	29	21	24	157
EAL3	0	0	0	0	2	0	7	5	5	75	18	37	34	25	208
EAL3+	0	0	0	1	0	0	2	1	4	64	17	25	22	23	159
EAL4	1	0	2	2	3	1	0	1	0	72	6	11	6	4	109
EAL4+	0	0	1	1	3	3	1	6	4	211	75	90	60	54	509
EAL5	0	0	0	0	0	0	0	0	0	7	3	2	0	0	12
EAL5+	0	0	0	0	0	0	0	0	0	52	28	31	35	23	169
EAL6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAL6+	0	0	0	0	0	0	0	0	0	0	1	2	3	1	7
EAL7	0	0	0	0	0	0	0	0	0	1	0	1	0	0	2
EAL7+	0	0	0	0	0	0	0	0	0	1	0	0	1	0	2
Basic	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Medium	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
US Standard	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
None	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Totals:	1	1	3	6	11	5	12	25	32	697	203	248	194	164	1602

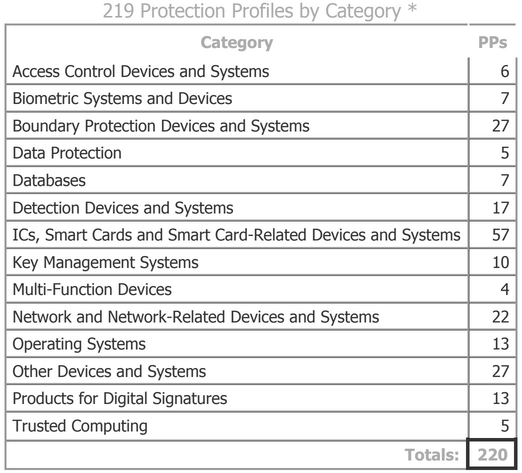
Level/Per countries



Certified Products by Scheme and Assurance Level

Scheme	EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6	EAL6+	EAL7	EAL7+	B	M	S	N	Total
Australia and New Zealand	2	1	12	8	4	5	8	8	0	0	0	0	1	0	0	0	0	0	49
Canada	3	0	21	48	12	17	6	24	0	0	0	0	0	0	0	0	0	0	131
Germany	8	4	7	16	7	53	13	171	8	97	0	0	0	0	0	0	0	0	384
Spain	2	5	4	1	3	1	0	9	0	0	0	0	0	0	0	0	0	0	25
France	0	18	0	13	0	9	4	140	1	64	0	5	0	0	0	0	0	0	254
Italy	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Japan	10	2	43	7	133	20	2	2	0	0	0	0	0	0	0	0	0	0	219
South Korea	0	0	0	0	8	9	21	8	0	3	0	0	0	0	0	0	0	0	49
Netherlands	1	0	0	0	0	1	1	8	0	0	0	0	0	1	0	0	0	0	12
Norway	0	0	1	0	0	0	7	4	2	2	0	0	0	0	0	0	0	0	16
Sweden	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	2
Turkey	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	4
United Kingdom	2	0	9	9	6	5	25	23	0	0	0	0	0	0	0	0	0	0	79
United States	5	0	108	55	34	39	22	107	1	3	0	2	1	1	0	0	0	0	378
Totals:	33	30	205	157	208	159	109	509	12	169	0	7	2	2	0	0	0	0	1602

Protection Profile

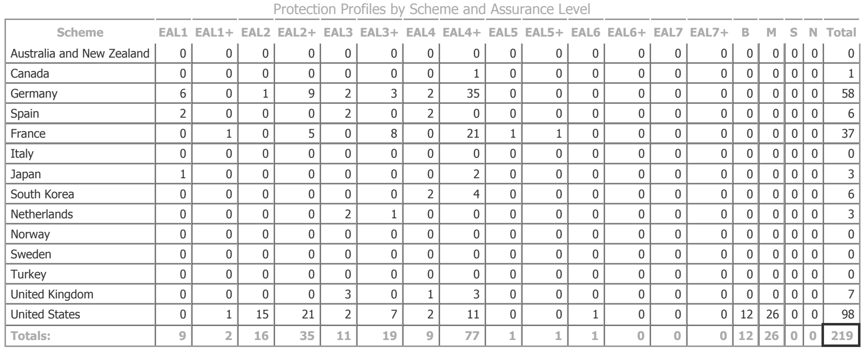


219 Protection Profiles by Category *

Category	PPs
Access Control Devices and Systems	6
Biometric Systems and Devices	7
Boundary Protection Devices and Systems	27
Data Protection	5
Databases	7
Detection Devices and Systems	17
ICs, Smart Cards and Smart Card-Related Devices and Systems	57
Key Management Systems	10
Multi-Function Devices	4
Network and Network-Related Devices and Systems	22
Operating Systems	13
Other Devices and Systems	27
Products for Digital Signatures	13
Trusted Computing	5
Totals:	220

** Totals include archived Protection Profiles.*
A Protection Profile may have multiple Categories associated with it.

PP by country



Protection Profiles by Scheme and Assurance Level

Scheme	EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6	EAL6+	EAL7	EAL7+	B	M	S	N	Total
Australia and New Zealand	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Canada	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1
Germany	6	0	1	9	2	3	2	35	0	0	0	0	0	0	0	0	0	0	58
Spain	2	0	0	0	2	0	2	0	0	0	0	0	0	0	0	0	0	0	6
France	0	1	0	5	0	8	0	21	1	1	0	0	0	0	0	0	0	0	37
Italy	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Japan	1	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	3
South Korea	0	0	0	0	0	0	2	4	0	0	0	0	0	0	0	0	0	0	6
Netherlands	0	0	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	3
Norway	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sweden	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Turkey	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
United Kingdom	0	0	0	0	3	0	1	3	0	0	0	0	0	0	0	0	0	0	7
United States	0	1	15	21	2	7	2	11	0	0	1	0	0	0	12	26	0	0	98
Totals:	9	2	16	35	11	19	9	77	1	1	1	0	0	0	12	26	0	0	219

Au niveau français

- Pour alléger le process l'Agnce Nationale pour la Sécurité des Systèmes d'information (ANSSI) a mis en place :
  - En application des décisions prises lors du CISI du 11 juillet 2006, l'ANSSI est chargée de proposer et d'expérimenter un processus de délivrance d'un label de premier niveau pour les produits de sécurité des systèmes d'information permettant notamment de labelliser des logiciels libres.
- Mais il y a aussi :
  - la qualification
    - Qualification d'un produit de sécurité
    - Qualification d'un prestataire de service de confiance