Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information

Paris, 28 March 2020
No. 1436/ANSSI/SDE/PSS/CCN

Référence :
ANSSI-CSPN-CER-P-02_v4.0

PROCEDURE

CRITERIA FOR EVALUATION IN VIEW OF A FIRST LEVEL SECURITY CERTIFICATION

Application : As soon as it is approved.

Circulation : Public.

COURTESY TRANSLATION

SÉCURITÉ CERTIFICATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP

Track changes

Editions	Date	Modifications
Experimental phase	28 August 2008	First draft for the experimental phase.
1.0	30 May 2011	End of the experimental phase. Change of name of the certification body (ANSSI), application of the "instruction" format and editorial improvements.
1.1	23 April 2014	Reorganisation of sub-chapters of chapters 3.2 and 4. In chapter 3.3, addition of the case where a generation of random numbers is used. Specification, in chapter 4, of the tasks of the evaluator regarding phase 3 (documentation review), phase 6 (resistance of mechanisms/functions) and phase 10 (evaluation of cryptography). Addition in chapter 4 of a new phase (phase 7 a) to cover the case of products requiring special implementation privileges.
2.0	6 September 2018	Updating of the rating table in chapter 4.6, in line with version 3.1 revision 3 of the document Common Methodology for Information Technology Security Evaluation : Evaluation Methodology. Modification of the type of document, initially corresponding to the ANSSI-NUMC-CER-I-02 instruction.
3.0	18 March 2019	§5.6 "Resistance of mechanisms/functions" - Correction of tables
4.0	28 March 2020	Clarifications related to the analysis of public vulnerabilities in third party components of the product under evaluation. Clarifications related to rating interpretation.

Pursuant to amended decree No. 2002-535 of 18 April 2002, this procedure has been submitted to the certification management committee, which gave a favourable opinion.

This procedure is available on-line on the ANSSI's institutional website (www.ssi.gouv.fr).

TABLE OF CONTENTS

1 Subject of the procedure

This procedure establishes the evaluation criteria for a first level security certification (CSPN).

2 References

[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, current version.
[RGS_B]	General security reference base, appendices B: [RGS_B1] : Rules and recommendations concerning the choice and the size of encryption mechanisms. [RGS_B2] : Rules and recommendations concerning the management of keys used in encryption mechanisms. [RGS_B3] : Rules and recommendations concerning authentication mechanisms.
[CSPN]	First level security certification for information technology products, reference: ANSSI-CSPN-CER-P-01, current version.
[CRY-P-01]	Methods for carrying out cryptographic analysis and random number evaluations, reference: ANSSI-CC-CRY-P-01, current version.
[CRYPTO]	Supplies needed to analyse cryptographic mechanisms, current version.
[CSPN NOTE 01]	Methods for evaluating with a view to issuing a first level Security Certification - Content and structure of the Evaluation technical report (ETR), reference: ANSSI-CSPN-NOTE-01, current version.
[JIL_HW]	Joint Interpretation Library - Application of Attack Potential to Smartcards and Similar Devices - Version 3.0 - April 2019
[JIL_HWD]	Joint Interpretation Library - Application of Attack Potential to Hardware Devices with Security Boxes - Version 2.0 (for trial use) - December 2015

3 Scope

3.1 Aim of these criteria

These criteria were defined by the Agence Nationale de la Sécurité des Systèmes d'Information (National Cybersecurity Agency of France - ANSSI) for time-constrained evaluation of security functionalities offered by hardware, software or both for a CSPN.

Two main objectives are sought in the evaluation:

- check that the product complies with its security specification;
- determine the effectiveness of security functionalities.

If the product requires special privileges to run on the host system, the evaluation should also cover the security impact of installing the product on its host system.

When essential security functions of the product are implemented by cryptographic mechanisms, two additional objectives are sought in the evaluation:

- checking compliance of the cryptographic mechanisms with the requirements described in the ANSSI General security reference base [RGS_B];
- checking compliance of the cryptographic mechanisms with the requirements described in the

ANSSI General security reference base.

These criteria may be supplemented by specific application notes, applicable to certain products or special cases.

3.2 Purpose of the evaluation

The objective of the evaluation process is to allow an evaluation facility to check whether the product conforms to its specification, determine the effectiveness of security functionalities and record the results in an evaluation technical report (ETR).

To do this, the evaluation facility relies on the information which it may access in particular on the product's security target and on the product itself.

The certification facility relies on the ETR to propose (or not) the product's first level security certification.

3.3 The stakeholders of the evaluation

The role of the different stakeholders is specified in the ANSSI-CSPN-CER-P-01 procedure (see [ANSSI-CSPN-CER-P-01]).

4 Minimum documentation to be provided

4.1 Introduction

A product that guarantees security (a combination of confidentiality, integrity, authentication and availability) must show appropriate security characteristics. It is necessary to determine the degree of trust that can be given to these characteristics.

For this, the characteristics themselves should be specified in a document, which is the security target of the product.

4.2 The security target

The security target is used both for specifying functions dedicated to security and describing the links between the product and the environment in which it will operate. The product developer and persons in charge of its evaluation, but also those responsible for its management, its purchase, installation, configuration, operation and use are therefore interested in the security target.

The required content of a security target is as follows::

a) an unambiguous identification of the product to be evaluated;
b) an identification of the product developer(s);
c) a product rationale describing the use of the product, and the context in which it is supposed to be used;
d) the technical environment in which the product works (computer model, operating system, etc.)
e) sensitive assets that the product must protect;
f) environment-specific measures;
g) the threats against which the product offers protection;
h) security functionalities implemented by the product to counter identified threats. These functionalities will be evaluated.

Each of these elements is described in detail below.

a) Unambiguous identification of the product

It must be possible to unambiguously identify the evaluated product and its version in particular.

b) Product developers

It must be possible to unambiguously identify the developer of the product. If some components are provided by third parties, or are open source, it must be possible to unambiguously identify the developer of each component.

c) Product rationale

The product rationale must identify how the product is intended to be used, the intended environment for its use and the assumed threats within that environment. It must also include a summary of the product's security characteristics. This should include the dependencies of the product relative to hardware, software and/or firmware that are not provided with the product..

The target must also describe the environment in which the product will be used. This environment is not always precisely known to its developer: indeed, the product can be incorporated into different systems and different environments. In this case, a rationale must be provided that gives the end user the necessary information to decide whether this product will help to meet the security objectives of their system, and to define what needs to be done to meet them completely.

c) Product's technical operating environment

The security target must specify the expected technical environment to enable use of the product. It can be a generic technical environment (e.g. PC compatible computer under a given operating system) or a dedicated environment (a specific computer model with such a specific configuration, etc.).

When the technical environment is described generically, the evaluator may consider testing the product on all possible platforms. A specific one is determined, possibly in agreement with the sponsor, to proceed with the evaluation. The specification of this platform must be clear in the ETR and indicated in the certification report.

d) Sensitive assets to be protected

The security target must describe sensitive assets that the security functions implemented in the product are intended to protect. It must specify the expected protection for these assets (confidentiality, integrity, availability, authentication). To protect sensitive assets, the product must sometimes handle information itself which also become a sensitive asset. For example, the confidentiality of user data can be protected through the encryption function, which normally uses an encryption key. This encryption key is also one of the product's sensitive assets.

e) Environment-specific measures

To meet its security requirements, it is possible that the product may be used in a particular environment with a particular organisation.

These environment-specific measures must be outlined in the security target. This should include logical, physical, organisational security measures, those related to personnel and information technology (IT) required to use the product.

They must be "realistic" with regard to the intended use of the product. For instance, a consumer desktop product may not claim an environment-specific measure requiring its use in a controlled access area under 24/24 surveillance, etc.

f) Description of threats

The security target must describe the threats covered by the security functions. A threat can be characterised by the following factors:

- a threat agent (authorised user, administrator, etc.);
- a type of threat (input error, computer abuse, etc.);
- an impacted asset.

For example, the fact that a user can make an input error modifying the behaviour of security function X constitutes a threat.

g) Specification of security-dedicated functions

The security target must include a specification of functions dedicated to security that the product must provide. These functions can be declared explicitly or refer to an accepted standard that defines a security functionality.

For functions that rely on a knowledge base[1] or on a code analysis engine, the evaluation does not look into the quality [2] of this knowledge base or analysis techniques implemented by the engine. Indeed, this type of analysis is beyond the scope of a CSPN evaluation in view of the load allocated to this evaluation process.

A security target may be based on one or more normative documents pertaining to security, either referring to them, or including them. When standards allow for options, the options chosen must be clearly identified. When a standard does not provide all the required information, the missing information must be explicitly provided in the security target.

In the case of a product, security-dedicated functions must be linked to expected modes of use of the product.

The specification of the security-dedicated functions must also show how those functions are designed to counter identified threats. This cross-referencing should include all dependencies on other security-dedicated functions and other measures not related to information technology (IT) security, supposedly provided by the environment.

From the evaluation standpoint, the specification of security-dedicated functions is the most important part of the security target. These functions must be specified at least in an informal way in natural language.

4.3 Specification of cryptographic mechanisms[3]

Information on algorithms should include:

- the description of the cryptographic functions provided by the product (encryption, signature, key management, etc.);
- the reference of algorithms to recognised, unambiguous standards, whose technical details are easily accessible and without conditions, with the settings and operating modes of their implementation.

Information on key management should include:

- the size of the keys;
- the key distribution method;
- the key generation method;
- the key storage format;
- the key transmission format.

[1] Signature, behaviour base, etc.

[2] In terms of completeness, relevance and accuracy.

[3] When the main security functions of the product are implemented by cryptographic mechanisms.

Information relating to data processing should include:

- the description of pre-processing experienced by plain text data before encryption (compression, formatting, adding a header, etc.);
- the description of post-processing of encrypted data, after its encryption (adding a header, formatting, packaging, etc.);
- reference product outputs, in electronic format, produced from a randomly chosen plain text and key.

When a random number generator is used for the implementation of cryptographic functions, the method and architecture used for this generator will be described. The reasons making it possible to show that the random number generator is effective will be explained.

This documentation must meet the requirements of [CRYPTO].

5 Evaluation criteria

This chapter sets out the evaluation criteria designed to verify compliance of the product with its specifications. The evaluation basis consists of a security target, which must contain the necessary information, as specified in this document.

5.1 Phase 1 - Analysis of the security target

Evaluator's tasks

Check that the security target contains the elements described in chapter 4.2 of this document.

Check that the target is not "misleading" and at least describes the main functionality for which the product is designed.

Check that the security functions are relevant with respect to generic threats described in the target.

Check that there are no security functions not connected to a threat described in the target.

Check that environment-specific measures are relevant with respect to threats and the intended purpose of the product.

In general, check that there are no inconsistencies in the security target.

5.2 Phase 2 – Installation of the product

Evaluator's tasks

Describe the platform actually used to perform tests on the product. This platform should be representative of the typical architecture of the information system in which the product is normally used, within the limits of possibilities allocated to the evaluation project.

For products that can be installed on several versions of the operating system, specify the operating system and version, as accurately as possible (patch, service pack, etc.).

If the product requires installation, proceed with the installation of the product in its typical configuration.

If installation documentation exists, check that it allows the installation of the product in different configurations covered by the evaluation.

Note any information deemed necessary to complete this installation. Indicate any non-compliances with the existing documentation.

Record any configuration specificities of the support system, if any.

5.3 Phase 3 – Compliance analysis – analysis of the documentation

Content and presentation requirements

The user documentation must allow users to safely implement the security functions described in the product's security target. It should also enable the user to ensure that the context of use meets the environment-specific measures demanded by the target. It must, as such, give recommendations or warnings necessary to the various categories of users. These documents, such as reference and user manuals, must be structured, internally consistent, and compatible with all other documents provided at this level.

The administration documentation must describe the functions applicable to an administrator and dedicated to security. There should be two types of functions: those allowing an administrator to modify security settings and those only providing information. If an administrator is required for the operations of the product, the documentation must describe all security settings under the administrator's responsibility. It must describe all events related to security covered by administration functions. It must describe the procedures related to security administration, in sufficient detail for their use. It should provide recommendations or warnings for the consistent and effective use of product security functions and how these characteristics interact. It should describe how the system or product should be installed and, if so, how it should be configured. Administration documentation, such as reference and administrator manuals, must be structured, internally consistent, and compatible with all other materials provided at this level. The administration documentation should describe how the product is securely administered.

If different configurations are possible, the impact of these security configurations must be described.

The delivery procedures should ensure the authenticity and integrity of the delivered product.

System generation procedures can be consulted within the context of the interview with the developers (Phase 9). These procedures must ensure the authenticity and integrity of the product generated. During the generation of the product, any option or change in the generation must be audited so that it is possible, subsequently, to reconstruct exactly how and when the product was generated.

The procedures to ensure a secure start and secure operation must be described. If a security-dedicated function can be disabled or modified during start-up, normal operation or maintenance, it must be described. If the product includes security-dedicated hardware components, diagnostic functions must be implemented by the administrator or the end user, or automatically. These should be run by the product in its operating environment.

Evaluator's tasks

List the analysed documents.

Check that the information provided meets content and presentation requirements and advise on their clarity and comprehensiveness. The evaluator will conduct sampling if the documentation is important, focusing on:

- the security target provided by the sponsor;
- user documentation;
- installation, administration and operating documentation;
- technical documents on the security functions and mechanisms;
- if essential functions of the product use cryptographic mechanisms, the cryptography must be evaluated (see §4.11).

If all or part of the documentation is unavailable, indicate whether the product can still be installed, configured, administered and used in compliance with what is described in the security target, taking into account the skills this would require from the relevant users. The evaluator will be helped by the following definitions:

- general public user: no special computer skills;
- experienced user: knowledge of the main IT concepts;
- administrator: in-depth knowledge of the key concepts of computing and networking, ability to configure and administer a computer network;
- expert: expert in the product field (typically, the evaluator).

5.4 Phase 4 – Compliance analysis – review of the source code (if available)

Evaluator's tasks

Give an expert opinion on the clarity and structuring of the source code (examples of criteria: existence of comments, breakdown into modules, data typing, portability, etc.), specifying the modules that have been viewed. It is possible to proceed by sampling.

It should be noted that, in the case of a code developed in a cooperative environment by several developers, the analysis of a code sample may be insignificant.

5.5 Phase 5 – Compliance analysis – product testing

Evaluator's tasks

Review the security functionalities and cryptographic mechanisms [4] of the product individually and test them.

Indicate functional testing or mechanisms implemented, stating:

- the functionality or mechanism tested;
- conditions necessary to run tests (for example, size and type of the input file, size and type of the output file, possible analysis of the cryptogram etc.);
- the limits of the functionality where applicable;
- if the functionality or mechanism is compliant or not to the security target;
- assessment factors (expert opinion).

5.6 Phase 6 - Robustness of mechanisms/functions

Definition

Even it complies with its specification, a security function can be short-circuited, disabled, altered, bypassed or made ineffective by an attack. Such an attack usually takes advantage of shortcomings in the implementation of the product, its design or in its underlying security principles. The product's ability to contain such an attack must therefore be estimated. It is necessary for this analysis to consider the level of resources required by an attacker to succeed each attack in question.

[4] When the main security functions of the product are implemented by cryptographic mechanisms.

Content and presentation requirements

The mechanisms studied are those that implement the security functions offered by the product, and described in the security target. For the mechanisms implementing cryptographic algorithms, a detailed specification must be provided.

Evaluator's tasks

The evaluator's role is to:

- identify security mechanisms implementing security functions;
- analyse how each mechanism works to ensure that it is able to provide the required service;
- if vulnerabilities are discovered, propose a rating of the exploitation of each vulnerability, by using the following rating tables;
- give a rating of the product's general resistance in terms of security, by using the rating of vulnerabilities discovered;
- Depending on the rating obtained, give an expert opinion on the resistance of functions and general resistance of the product to attacks.

The following tables are the default model for rating calculation in CSPN. The evaluator will consult the [CEM] for more information on their use. Specific rating tables can however be redefined for certain product categories. In particular,

- smart cards and similar products will be evaluated according to the document's rating tables [JIL_HW];
- products such as "hardware with secure boxes" will be evaluated according to the document's rating tables [JIL_HWD].

In addition to these rating tables, the evaluator must take the document into account [CRY-P-01] to analyse mechanisms using cryptographic algorithms or random number generators.

If in doubt about the choice of the rating table, the evaluator is asked to contact the certification facility.

Factor	**Values**	
Time taken for the exploitation	<= 1 day	0
	<= 1 week	1
	<= 2 weeks	2
	<= 1 month	4
	<= 2 months	7
	<= 3 months	10
	<= 4 months	13
	<= 5 months	15
	<= 6 months	17
	> 6 months	19
Attacker skills	Layman	0
	Competent	3
	Expert	6

Factor	Values	
	Multiple experts	8
Knowledge required by the attacker	None [5]	0
	Restricted information	3
	Sensitive information	7
	Critical information	11
Access to the product by the attacker	Not necessary/unlimited	0
	Easy	1
	Moderate	4
	Difficult	10
	None	*[6]
Type of equipment needed [7]	None/ standard	0
	Specialised software	2

If the attack is scored by value	Then the attack is considered exploitable by an attacker by the following level	Does the resistance of the TOE fail?
0 to 9	Basic	Yes
10 to 13	Enhanced-Basic	Yes
14 to 19	Moderate	No
20 to 24	High	No
>= 25	Very high	No

5.7 Phase 7 – Analysis of the vulnerability (intrinsic, construction, exploitation, etc.)

Evaluator's tasks

The identification of known vulnerabilities is based on the competence of the evaluator and the exploitation of vulnerabilities databases. For the latter, the task is to extract the relevant vulnerabilities and to check if and how they can be exploited on the product.

There are two types of vulnerability to be processed:

- the specific vulnerabilities of the product, for which the analysis consists in describing the technical conditions and impact of vulnerability implementation, as well as clarifying the existence of patches or procedures to counteract, mitigate or compensate for the vulnerability;
- generic vulnerabilities applicable to the product. These are vulnerabilities discovered on similar products for which there is no information proving that the relevant product is

[5] Including the use of public documentation

[6] Indicates that the attack is not feasible due to counter-measures implemented in the operational environment of the TOE.

[7] These values factor in application note 18 (ANSSI-CC-NOTE-18), which differs from the [CEM]. If an attack requires physical intervention and the use of hardware, the whole attack must be scored using the [JIL_HW] or [JIL_HWD] scoring table (the ITSEF will choose whichever seems most appropriate for the evaluated product)

protected from them. The analysis task is completed during an attempt - within the limits of available resources - to exploit the vulnerability in order to test the target product.

This task consists in:

a) ensuring that vulnerability tracking exists for the product. If the product includes components developed by a third party (COTS or open source), the developer must be informed of vulnerabilities appearing on that component. If this information is not public, the developer must provide the evaluator with this information;

b) identifying the known vulnerabilities of the product. For each vulnerability, find a patch (whether official or not) or a workaround to limit the effects of the vulnerability. When the product includes components developed by third parties, especially when these components are old, there are likely to be several public vulnerabilities on the product. This can make it impossible to conduct the evaluation within a limited time frame. For this reason, the evaluator is allowed to demand from the developer:
   - the comprehensive list of the public vulnerabilities in third-party components included in the product, and
   - a demonstration showing that these vulnerabilities are not applicable, have no impact, are corrected or may be circumvented.

   This pre-analysis by the developer does not replace the evaluator's tasks, but aims to make them achievable within the time required for the evaluation.

c) identifying known vulnerabilities for products in the same category. These are known vulnerabilities across all products in the category, as well as potential theoretical vulnerabilities;

d) implementing, testing and validating certain vulnerabilities, based on criteria of choice such as feasibility, exploitability or lack of a patch.

5.8 Phase 7bis – Vulnerability analysis of the host system

Evaluator's tasks

If the product requires special privileges to run on its host system, the evaluation should also cover the security impact of installing the product on the host system. A host system can be an operating system or a network. Typically, if the product requires specific operating system implementation privileges, the evaluator will have to investigate whether the product facilitates a privilege escalation.

The evaluator's role is to:

- identify the privileges or isolation conditions required on the host system for the product to run properly;
- give an expert opinion on the impact the product has on the security of its host system.

5.9 Phase 8 – Analysis of ease of use

Evaluator's tasks

Identify cases where the product may give a false sense of security to an administrator or end user.

Identify potential inherently non-secure functionalities that should not be used if they lead to or contribute to an exploitable vulnerability, or if the complexity of their implementation is detrimental to confidence in the reliability of the configuration.

Provide realistic recommendations, where possible, to allow secure use of the product despite its potential vulnerabilities.

5.10 Phase 9 – Interview with developers

Evaluator's tasks

Obtain information from developers on all the criteria analysed. This task is optional. It implies that developers are available and accept this approach. It is recommended for the evaluator to conduct the interview at the start of the project and complete it throughout the project as and when new issues appear.

The evaluator gives expert advice on the developer's ability to master their product, the security of the product, etc. The evaluator will use the following list to support his/her opinion:

- security of the development environment: premises, personnel, development network, etc.;
- existence of a quality system;
- existence of design and product implementation documentation;
- existence of configuration management;
- ability of developers to answer the questions asked.

5.11 Phase 10 – Evaluation of the cryptography (if the product implements cryptographic mechanisms)

Evaluator's tasks

The cryptography should be evaluated when the essential functionalities of the product are implemented by cryptographic mechanisms.

The evaluator must have a form of technical support available to interpret the supplies described in paragraph 4.3.

Compliance of cryptographic mechanisms with regard to the requirements of the ANSSI [RGS_B] general security reference base is verified by documentary analysis.

Compliance of the implementation of these mechanisms by the product is verified in different ways:

- by comparing the results of cryptographic processing performed by the product with respect to a reference implementation. This implies that several reference inputs/outputs (key, plain text, encrypted) are made available to the evaluator. These are means of bringing together a set of inputs/outputs and secrets which may then be injected into a software simulator to perform the same processing as the product, in order to make comparisons;
- by analysing the source code with unit tests of certain functions (for example, check that an AES function does in fact perform an AES;
- by checking that the product to be tested communicates in encrypted mode with a reference equipment, should it be a communicating system.

As there are several possible approaches, the evaluator will describe those adopted to ensure compliance of the implementation with respect to specifications.

Case of random number generators:

The evaluator will check that the random number generator architecture satisfies the requirements described in the ANSSI [RGS_B] technical reference base.

He/she will indicate any tests performed to ensure the random nature of the source.

6 Results of the evaluation

The evaluation of the product according to criteria presented in this document is designed to ensure that the product does in fact provide the security functions indicated in the security target, that no "enhanced-basic" vulnerability (as defined in chapter 5.6) was exploited during the evaluation. This last conclusion must be drawn with all the caution required in the information technology security field. Indeed, it is not possible to guarantee the absence of exploitable vulnerability in the product.

The evaluator must propose a rating for each security function and mechanism and describe it, if applicable, in the security target. If it is not possible to establish this rating for one or more functions, the evaluator should explicitly mention it in his/her report (ETR) and state the reasons why.

The ETR must provide the following information, at least :

- the reminder of the analysis context (context of use, length of the analysis, threats, etc.);
- a summary of the documentation to provide a functional description of security functions or security-related functions; what is functionally expected of the product (summary of the security characteristics in particular);
- the inventory of known vulnerabilities (CERT-FR, public databases, developer's information) and patches;
- the list of the main analysis tools used;
- a summary of the results of tests conducted on the product;
- an appraisal and rating of the different identified exploitable vulnerabilities;
- An appraisal of the product and of recommendations for use or configuring in the context of use to ensure, in particular, that no identified vulnerabilities are exploitable for a level equal to or lower than "enhanced-basic" (as defined in chapter 5.6).

The ETR follows a fixed table of contents. It is downloadable from the ANSSI website (www.ssi.gouv.fr), see [CSPN-NOTE-01].

The evaluation technical report drawn up by the evaluator, containing and justifying the results of the evaluation, must be presented in an acceptable form to be taken into consideration by the ANSSI certification facility.

If the ETR reveals that the product does not totally or partially satisfy its security target and it is not possible to identify realistic environmental counter-measures to improve that situation, the product will be considered not to satisfy its security target.

The same applies to tests that reveal malfunctions of the product not allowing normal or scheduled use, weakening of the host system or if some of the conclusions of the ETR are "inconclusive", for example due to lack of information.

Finally, a fail verdict could be declared if the product includes a third-party component whose vulnerabilities are not managed. This can be, for example:

- a beta version component;
- a component for which the developer has abandoned security maintenance;
- a COTS component for which security maintenance is chargeable and which the developer has not paid.

7 Glossary

This chapter contains definitions of technical terms used with meanings specific to this document. The technical terms used in this document and not defined in this section are used in a manner consistent with their ordinary meaning.

Acceptance procedure: procedure used to take the items produced in the development, production and maintenance process of a target of evaluation and deliberately put them under the control of a configuration management system.

Administration documentation: information on a target of evaluation provided by the developer for use by an administrator.

Administrator: person in contact with the product and responsible for keeping it in working order.

Assurance: trust in the security provided by a target of evaluation.

Availability: prevention of unauthorised denial of access to information or resources.

Binding of functionality: aspect of the estimation of the effectiveness of a target of evaluation which covers the capacity of its functions and mechanisms dedicated to security to cooperate in order to form an integrated and efficient whole.

Certification body: independent and impartial national body which issues certification.

Certification: issuing of a formal statement confirming the results of an evaluation and that the evaluation criteria have been properly applied.

Confidentiality: prevention of unauthorised disclosure of information.

Configuration: selection of one of the sets of possible combinations of characteristics of a target of evaluation.

Correctness: property of a representation of a target of evaluation which ensures that it accurately reflects the security target presented to the system or product.

COTS (Commercial Off-The-Shelf): product developed and marketed in series. A product subject to evaluation may include COTS components such as a processor or a proprietary library.

Covert channel: using an unscheduled communication mechanism for transferring information in a manner that violates security.

Customer: person or organisation purchasing a TOE.

Developer: person or organisation that produces a target of evaluation.

Documentation: written information (registered or otherwise) regarding a required target of evaluation demanded for an evaluation. This information can be assembled in one document constituted for this purpose, but this is not imperative.

Ease of use: aspect of estimating the effectiveness of a target of evaluation to ensure it cannot be configured or used in an insecure way, but which an administrator or end user could reasonably believe to be secure.

Effectiveness: property of a target of evaluation that represents the extent to which it provides security in the context of how it is actually or intended to be used.

End-user: person in contact with a target of evaluation who only uses its operational capabilities

Evaluation: assessment of a system or product with respect to defined evaluation criteria.

Evaluator actions: part of the evaluation criteria for a phase or aspect of the evaluation identifying what the evaluator must do to verify the information provided by the sponsor of the evaluation, and additional actions he/she must perform.

Evaluator: person or organisation performing an evaluation.

Implementation: phase of the development process in which the detailed specification of a target of evaluation is translated into actual hardware and software.

Integrity: prevention of unauthorised modification of information.

Operating procedure: set of rules defining the proper use of a target of evaluation.

Operation: process of use of a Target of Evaluation.

Operational documentation: information provided by the developer of a target of evaluation to specify and explain how it should be used by customers.

Operational environment: organisational measures, procedures and standards to be used during the operation of a target of evaluation.

Penetration testing: Tests by an evaluator on a target of evaluation to confirm whether or not the identified vulnerabilities are actually exploitable in practice.

Product rationale: description of a product's security capabilities, providing information needed by a potential buyer to decide if a product will help them satisfy their system's security objectives.

Product: information technology software and/or hardware package which provides a functionality designed for use or incorporated within multiple systems.

Programming languages and compilers: tools of the development environment used to build the software and/or firmware of a target of evaluation.

Requirements for content and presentation: part of the evaluation criteria for one phase or a specific aspect of the evaluation criteria, which explains what each item of documentation identified as being relevant to this phase or this aspect should contain, and how the information contained in it must be submitted.

Requirements for evidence: part of the evaluation criteria for a phase or specific aspect of the evaluation which defines the nature of the evidence intended to show that the criteria for this phase or this aspect are satisfied.

Requirements: phase of the development process in which the security target of a target of evaluation is produced.

Security mechanism: logic or algorithm that implements, through hardware or software, a function dedicated to security or contributing to security.

Security objectives: contribution to security which the target of evaluation is intended to provide.

Security target (ST): security specification that is required of a target of evaluation and is used as a basis for the evaluation. The security target must specify the functions of the target of evaluation dedicated to security. It will also specify the threats to sensitive assets and the special security mechanisms that will be employed.

Security: combination of confidentiality, integrity, availability, authentication and non-repudiation.

Sponsor: person or organisation requesting an evaluation.

Strength of mechanism: aspect of estimating the effectiveness of a target of evaluation that covers the capacity of its security mechanisms to withstand a direct attack against defects in algorithms, principles and underlying properties.

Suitability of functionality: aspect of estimating the effectiveness of a target of evaluation that covers the relevance of security functions and mechanisms of the target of evaluation to actually counter the threats to the security of the target of evaluation identified in its security target.

Target of evaluation (TOE): system or product that is subjected to a security evaluation.

Threat: action or event likely to affect security.

User documentation: information on a target evaluation provided by the developer for use by its end users.

Vulnerability assessment: aspect of the assessment of the efficacy of a target of evaluation that covers the extent to which known vulnerabilities in the target of evaluation could practically compromise its security as specified in the security target.

Vulnerability: security weakness of a target of evaluation (for example due to defects in analysis, design, implementation or operation).