Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRIME MINISTER

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, 16 July 2010

N° 1897/ANSSI/SR

Reference: ANSSI-CC-NOTE/07.1

APPLICATION NOTE

INTERPRETATION OF COMMON CRITERIA FOR THE EVALUATION OF SYSTEMS

Application : From its approval.

Distribution : Public.

COURTESY TRANSLATION

SÉCURITÉ CERTIFICATION

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

Modification history

Edition	Date	Modifications
1	16/07/2010	First official edition.

In application of decree n° 2002-535 dated 18 April 2002, the present note was submitted to the Certification Management Board, which gave a favourable opinion.

TABLE OF CONTENTS

1. Purpose of the note

The purpose of the present note is to supply an approach to the concept of "system" evaluation in order to obtain a "Common Criteria" certificate, certifying that an EAL level has been reached.

This is because the Common Criteria, designed for evaluating information-technology products, unlike ITSEC, do not clearly show what is a "system" and how, in practice, it may be evaluated.

It should be made clear that systems are evaluated under the same procedural framework as product evaluations (see the ANSSI-CC-CER/P/01 procedure, available on www.ssi.gouv.fr).

2. References

- [CC v3.1rx]:
  The different revisions of CC v3.1, namely, on the date of publication of the present note:
  - Common Criteria parts 1-2-3 and CEM; Version 3.1, Revision 1; June 2006; Ref. : CCMB-2006-06-001 to 004
  - Common Criteria parts 1-2-3 and CEM; Version 3.1, Revision 2; June 2006 and September 2007; Ref. : CCMB-2006-06-001 and CCMB-2007-09-002 to 004
  - Common Criteria parts 1-2-3 and CEM; Version 3.1, Revision 3; July 2009; Ref. : CCMB-2009-07-001 to 004
- [CC v2.x]:
  - Common Criteria parts 1-2-3 and CEM; Version 2.1; August 1999; Ref. : CCIMB-99-031, CCIMB-99-032, CCIMB-99-033 and CEM-99/045
  - Common Criteria parts 1-2-3 and CEM; Version 2.2; January 2004 (Revision 256); Ref. : CCIMB-2004-01-001 to 004
  - Common Criteria parts 1-2-3 and CEM; Version 2.3; August 2005; Ref. : CCMB-2005-08-001 to 004
- [ITSEC]: Criteria for the evaluation of the security of information technologies, version 1.2, June 1991, Office for Official Publications of the European Communities.

3. Definition of a system

A system is a specific installation of information technology (IT) products in a known operating context.

A system is built from a certain number of hardware and software components (IT products). Some components are created specially, others are standard products. The specific installation of IT products corresponds to their technical configuration.

The operating context corresponds to the physical, human and organisational security measures that apply to the system, such as:

- physical security measures: the use of badge readers, infrared barriers, video surveillance, etc.;
- human security measures: training the final users of the system, training system administrators, etc.;

- organisational security measures: assignment of system access permissions, etc.

The concept of the operating context corresponds to that of the operational environment, which is defined in the [CC v3.1rx].

In the rest of the document, we differentiate the technical part of a system (i.e. the IT part) from its non-technical part (i.e. its operating context).

4. Special characteristics of system evaluation compared to product evaluation.

From the security point of view, the main difference between "system" and "product" is that, in the case of a system, the operating context, within the area identified in the security target, is clearly defined and perfectly controlled, and it is designed to satisfy the requirements of a specific group of final users. A product, on the other hand, is always considered in relation to an assumed deployment environment (operational environment that will be described in the "usage restrictions" chapter in the certification report).

Furthermore, the operating environment for a product is entirely under the responsibility of the final user, while in the case of a system, the developer[1] (in the capacity of a supplier of the service) may be partly responsible.

It is therefore assumed in this note that the client and the developer have reached prior agreement on the security target and the operating context, and that the developer supplies the appropriate evidence during the evaluation (see section 6.1).

From the point of view of evaluation, the main difference lies in the evaluation of the additional guidance documents, which establish the protection measures for the operating context.

Also, it should be noted that the evaluation of an IT system at a high level of confidence is an operation that is difficult to perform for several reasons:

- Supposing that all the expected documentation is available, it is difficult for any individual to understand the whole of an IT system from a security point of view.
- In general, the expected documentation for evaluating the whole of an IT system is not available. If the IT system is made up of IT products that have not been evaluated or for which the design documentation is not available, we then find ourselves in a situation where we can go no further (it should be noted that just the fact that the IT products are evaluated is not sufficient: we must make sure that the security functions of the product that were evaluated correspond to those identified in the system evaluation, and that the product is deployed in accordance with the restrictions identified in its certification report).

This is why, usually, IT system evaluation is only envisaged at limited levels of confidence corresponding to what it is realistic to expect in terms of deliverables.

5. Scope of certification

The certification of an IT system covers the system that is evaluated and tested, considered in its planned usage environment.

The IT system tested may be only a significant representation of the real IT system.

[1] In the rest of this document, by "developer", we mean the developer of the system, whether he/she designs new software or hardware, or only integrates off-the-shelf hardware and software.

By "client", we mean all the groups of final users of the system. A system may have several separate clients.

Developments to the system may also be certified, providing that they are carried out in accordance with evaluated procedures (note: all of the evaluated procedures will be identified in the system certification report).

If guidance documents relative to changes to the dimensioning of the system have been evaluated, the certification report will also specify the changes that were made in accordance with these guidance documents (the version sheet still remains valid for these changes).

6. Evaluation tasks

This chapter specifies what the certification body expects for a system evaluation, both from the developer and the evaluator, according to the different assurance families defined by the [CC v3.1rx] (the correspondence of the concepts presented in relation to [CC v2.x] is supplied in Annexe A).

This paragraph first describes the specific concepts used in a system evaluation, then describes the tasks to be carried out as part of a system evaluation at a lower level of confidence (levels EAL1 and EAL2). For evaluations of the highest level, the certification body must be contacted.

6.1. Specific evidence to be supplied as part of a system evaluation

As mentioned above, a system is defined as a specific IT[2] installation and a particular (non-IT) operating context.

The following figure gives a summary identification of the specific components that must be supplied for a system evaluation, as compared to a product evaluation. These components are those shown in the light boxes in the figure. They correspond to the system's operating context.

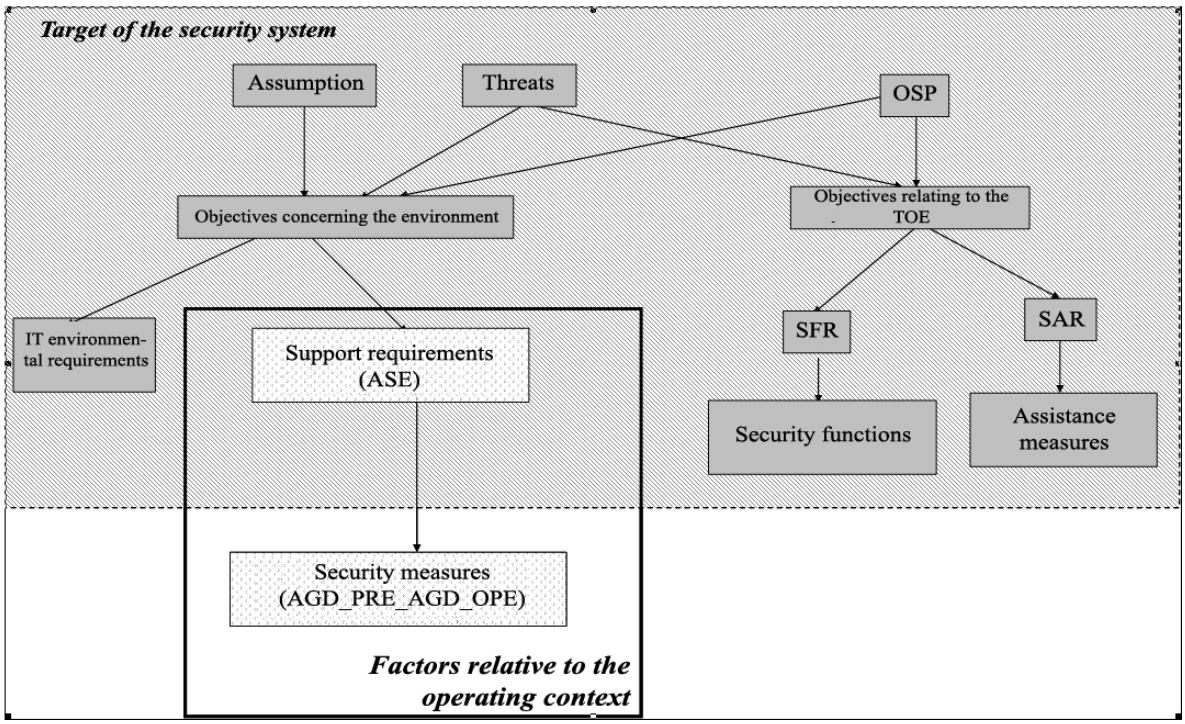

Figure 1 Specifics of evidence for a system evaluation

[2] That corresponds to a particular fixed configuration of IT products making up the system.

At the level of the security target, the operating context is represented by "support requirements". These requirements are applied in the guidance documents for the system by "site security measures".

The operating context is formalised in the security target by assumptions and Organisation Security Policies (OSP), which are themselves refined as support requirements. (Note: The term "requirement" employed here does not designate the requirements stemming from part 2 of the CC; no specific formalism is imposed here to express these requirements). If the support requirements concern specific roles or phases, this must be presented in the security target.

The security requirement and its coverage (factors for ensuring that the security issue is correctly covered) must remain understandable in the security target. The complexity of the security target must not make it difficult to understand

We distinguish "developer support requirements" from "client support requirements". This distinction allows responsibility for implementing these security measures to be established. The breakdown of these responsibilities depends on the contract which is negotiated between these two parties.

The support requirements are then applied as security measures, also under the responsibility of one of the two parties. These security measures are applicable to the sites where the system is deployed. Among these sites, some are under the responsibility of the developer and others under the responsibility of the client. The ITSEF does not have to worry about this division. It must just make sure, in relation to the AGD component, that all necessary measures for the protection of the system have been defined.

6.2. Low level evaluation

The following paragraphs identify the specifics of the application of the CC assurance classes in the context of a low-level system evaluation.

The evaluation tasks identified in the CEM are all applied. This note only specifies the additional evaluation tasks.

a) Security target (ASE)

The main difference between a system security target and a more conventional target is that this document must, in the case of a system, describe the system's deployment characteristics.

The evaluator must check that the operating context and the technical security requirements cover the security requirements defined by the security objectives of the security target. The ASE report must identify the security objectives relating to the system overall. To facilitate the conduct of the evaluation, the report must specify how the IT part of the system and its operating context contribute to the coverage of the objectives. The evaluator must also check that all assumptions and OSP not relating to IT measures concerning the environment are correctly applied as support requirements. However, it is not the responsibility of the evaluator to decide on the breakdown of these support requirements between the developer and the client. The evaluator must give an opinion as to the adequacy and appropriateness of the support requirements for covering the security requirements of the IT system operating context.

Identification of the TOE is covered in section 6.2.d, by ALC_CMC and ALC_CMS.

Although the description of the requirements for the environment is no longer needed by [CC v3.1rx], the description of the security measures, and the associated evaluation tasks, are required for the application of a coherent system process.

b) Development (ADV)

This class only applies to the technical part of the evaluated system. No specific interpretation of a system evaluation is therefore required here.

ADV_ARC

The deliverables must describe the security mechanisms implemented by the system.

ADV_FSP

The deliverables must present the security specifications of the system for the objectives of the system's technical part (description of "what").

ADV_TDS

The deliverables must present the breakdown of the technical part of the IT system into sub-systems, in accordance with the chosen level, and the interfaces between these sub-systems (description of "how").

The sub-systems may correspond to different products integrated in the system.

c) Guidance documents (AGD: AGD_OPE, AGD_PRE)

The breakdown of the AGD_OPE and AGD_PRE components of the guidance documents identified below must be performed case-by-case according to the specifics of the system.

Also, the evaluator must apply the AGD criteria to all the guidance documents specific to a system evaluation identified by the present note (see Annexe B).

Guidance documents intended for clients of the system

In relation to the technical part of the system, these guidance documents must describe the actions of clients of the system that is being evaluated, which are necessary for activating the system and/or integrating this client's sites into the system (for example, guidance to the installation and configuration of hardware under the client's responsibility).

For the non-technical part of the system, these guidance documents must specify the security measures with which clients must comply (for example, in the form of physical security procedures for client sites).

Guidance documents intended for developers of the system

These guidance documents must describe the administration procedures (initiation and maintenance) for the evaluated system, together with the evaluated configurations of each item of hardware making up the TOE.

These guidance documents may also describe the procedures to be applied to allow changes to be made to the dimensioning of the system. The degree of freedom for these changes must be specified and will be evaluated. The changes considered here only concern those related to dimensioning, for example adding new items of hardware compliant with those identified in the sheet showing the system's versions (see ALC_CMS and ALC_CMC). These developments must not modify the architecture of the system described by ADV_ARC (for example, hardware redundancy required for the security and dependability of functioning of the system forms part of the system architecture).

For the non-technical part of the system, these guidance documents must specify the security measures with which the deployment sites for the system managed by the developer must comply (for example, in the form of physical security procedures for developer sites).

The evaluator must check that the security measures for the sites described in the guidance documents correctly meet the support requirements described in the security target.

All of the guidance documents describing the operating context will be identified in the certification report to allow verification, both by the final user and by the developer of the system, of the implementation of the overall security context as defined in the security target. This verification may be performed by a compliance audit of type ISO 27001/ISO17799/BS7799.

d) Life cycle (ALC)

ALC_CMC, ALC_CMS

Some of these tasks are carried out on the configuration list, as for a product evaluation. However, as the system may change, a version sheet must also be supplied by the developer. This version sheet must identify all the different types of equipment that are integrated (hardware) associated with all the different versions of the software installed in the system (versions of software products). It is not a requirement for this version sheet to count the items of equipment and software programs installed (i.e., the certificate will remain valid even if the size of the system develops). The labelling of the target of evaluation is interpreted as being this version sheet (which allows identification of the evaluated version of the system) associated with the guidance documents defining the authorised changes to the system. This is why this sheet is always required whatever the assurance components chosen by the sponsor of the evaluation.

It should be noted that a coherent correspondence between the configuration list, the ADV representation levels and the versions sheet is essential for the evaluation.

ALC_DEL

The procedures for delivery of the system to a client (delivery of access to the system) must describe the process of delivering the documents identified by AGD_OPE and the procedures for application of the AGD_PRE guidance documents. The procedures for delivery of equipment must also be described if they are under the responsibility of the client.

ALC_FLR

The procedures for the operational maintenance of the system must describe the procedures for the deployment of patches identified concerning the technical components of the system, and the procedures for changes to the physical security measures of the various sites.

The developer must also describe the process by which these clients notify him/her in case security anomalies are identified, together with the process for handling these anomalies.

e) Tests (ATE)

This class only applies to the technical part of the evaluated system.

ATE_COV, ATE_FUN

These tests are carried out under ADV_FSP (the various integrated products are tested together so as to analyse their cooperation). The developer's deliverables must describe the test environment that is used and the ITSEF must determine whether this platform is representative (the versions sheet and the configuration list for the system will therefore need to have been delivered previously). Tests carried out on a platform considered non-representative may be rejected by the ITSEF.

ATE_IND

These tests are also carried out under ADV_FSP. A test platform must be made available to ITSEF by the developer so that it can perform its own tests. If this platform has not been previously analysed, ITSEF must determine whether it is representative. A platform considered

non-representative may be rejected by ITSEF. It is therefore in the developer's interest to supply a description of this platform well in advance of this task.

f) Vulnerabilities (AVA_VAN)

The tests performed for this evaluation task only apply to the technical part of the system, but the ability to exploit any identified technical vulnerabilities will be determined in relation to the security measures as evaluated in AGD, particularly those covering the support requirements outlined in the security target.

A test platform must be made available to ITSEF by the developer so that it can perform these tests. If this platform has not been previously analysed, ITSEF must determine whether it is representative. A platform considered non-representative may be rejected by ITSEF.

Annexe A

Correspondence with CC v2.x

The present note is also applicable to previous versions of the CC. Only references to version 3.1 of the CC [CC v3.1rx] were mentioned previously to avoid needlessly burdening this document.

The following table explains how to apply this note (essentially its chapter 4.3) in the context of evaluation according to [CC v2.x].

Paragraphs of the note	**Components CC v3.1**	**Components CC v2.x**
6.2.a	ASE_*	ASE_*
6.2.b	ADV_ARC	AVA_VLA
	ADV_FSP	ADV_FSP
	ADV_TDS	ADV_HLD
6.2.c	AGD_OPE	AGD_USR, AGD_ADM, AVA_MSU
	AGD_PRE	ADO_IGS, ADO_DEL AVA_MSU
6.2.d	ALC_CMC	ACM_CAP, ADO_IGS
	ALC_CMS	ACM_CAP
	ALC_DEL	ADO_DEL
	ALC_FLR	ALC_FLR
6.2.e	ATE_COV	ATE_COV
	ATE_FUN	ATE_FUN
	ATE_IND	ATE_IND
6.2.f	AVA_VAN	AVA_VLA

Annexe B

Some examples of supplies specific to a system evaluation

As has been previously mentioned, specific deliverables may be produced for a system evaluation.

These deliverables usually correspond to guidance documents. Whether it is necessary to deliver these guidance documents essentially depends upon the sponsor of the system (i.e. the client) and the scope that they have defined in their specifications. These specifications must also define the responsibilities of each party. The security target will reflect this sharing of responsibilities by breaking down the non-IT requirements for the environment into developer support requirements and client support requirements.

This step prior to the evaluation will always be assumed to have been done when the evaluation process is initiated. Indeed, the security target represents the compromise that has been established between sponsor and developer after contracting.

The following table gives a few examples of guidance documents, relative to a system evaluation, not explicitly identified in the common criteria. All of these guidance documents are evaluated in relation to the AGD class. The evaluator must, in particular, make sure that:

- these guidance documents are adequate (that they appropriately cover all aspects of the support requirements identified in the security target);
- these guidance documents are mutually coherent (they do not contain contradictory recommendations).

	IT part	**Non-IT part**
AGD_OPE	• System initialisation guide (if the initialisation – or part of the initialisation – is the responsibility of the client) • New hardware integration guide (if the client is authorised for this) • …	• Physical security measures for client sites (if the protection of these sites is the client's responsibility) • Organisational security measures for client sites • Training material for users • …
AGD_PRE	• System deployment guide • Guide to changes to the dimensioning of the system (if such changes are planned) • Procedures for the administration of hardware (it is obligatory to supply these procedures and they must describe the configuration of each type of hardware if this configuration is not automated) • …	• Physical security measures for developer sites • Organisational security measures for developer sites • Training material for administrators • …