D12.1

Technical Analysis of Available Assurance Techniques

Project number:	318353
Project acronym:	EURO-MILS
Project title:	EURO-MILS: Secure European Virtualisation for Trustworthy Applications in Critical Domains
Start date of the project:	1st October, 2012
Duration:	36 months
Programme:	FP7/2007-2013

Deliverable type:	Report
Deliverable reference number:	ICT-318353 / D12.1/ 1.0
Activity and Work package contributing to the deliverable:	Activity 1 / WP 12
Due date:	June 2013 – M09
Actual submission date:	31st July, 2013

Responsible organisation:	TCS
Editor:	TCS (Jean-Christophe Courrège)
Dissemination level:	Public
Revision:	1.0

Abstract:	Technical analysis of available assurance techniques proposed by the CC3.1 from EAL 5 to EAL 7 to examine their applicability to a feasible transnational CC certification. Review of known assurance requirements for resource management for existing separation kernels/hypervisors compiled from published protection profiles, security targets or relevant publications.
Keywords:	Evaluation Assurance Level, Common Criteria, differential.

Editor

Jean-Christophe Courrège, TCS

Contributors

Claire Barrat-Gély, TCS

Jean-Christophe Courrège, TCS

Jean-François Culat, TCS

Disclaimer

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 318353.

Executive Summary

This document presents a technical analysis of available assurance techniques proposed by the Common Criteria v3.1 (CC3.1) from Evaluation Assurance Level (EAL) 5 to EAL 7 to examine their applicability to a feasible transnational CC certification.

The conditions to international recognition of issued CC certificates are studied and several differentials are done showing what the prerequisites in terms of Security Assurance Requirements (SARs) are at EAL 5, 6 and 7 based on information available in CC3.1 and the Common Methodology for Information Technology Security Evaluation (CEM v3.1). EAL 5 evaluation is doable based on the CEM, EAL 6 evaluation requires the use of additional guidance and the gap to perform an EAL 7 evaluation is identified.

Finally a review of known evaluations at EAL 6 and 7 is done for resource management, for existing separation kernels/hypervisors compiled from published protection profiles, security targets or relevant publications.

Contents

List of Tables

Chapter 1 Presentation of high EAL issues

Two problems arise when EAL higher than 4 are concerned. First, the CEM does not specify every SAR needed to perform high level evaluations (this will be discussed in detail in chapter 2). Second, recognition agreements for CC evaluations state limits to the international recognition of certificates emitted by Certification Bodies.

This chapter describes what can be expected from the different high level EAL in terms of assurance then presents the international recognition agreements. Finally, the content of the supporting documents that help to complete the CEM is summarized.

1.1 EAL 4 to 7 overview

What does an EAL 5 (or higher) evaluation bring as additional assurance compared to lower EALs? The three paragraphs below come from CCv3.1 part 3 and describe the objectives of each evaluation level and what can be expected from EAL 5 to 7 in terms of assurance.

1.1.1 Evaluation assurance level 4 (EAL 4) – methodically designed, tested and reviewed

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity Targets of Evaluation (TOEs) and are prepared to incur additional security specific engineering costs.

1.1.2 Evaluation assurance level 5 (EAL 5) – semi-formally designed and tested

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialized techniques, will not be large.

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

1.1.3 Evaluation assurance level 6 (EAL 6) – semi-formally verified design and tested

EAL 6 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.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.

1.1.4 Evaluation assurance level 7 (EAL 7) - formally verified design and tested

EAL 7 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 EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.

1.2 Low vs. high EALs recognition

To this day, CC certifications are recognized by the different Certification Bodies (BSI, ANSSI, CESG, NLNCSA, etc.) up to EAL 4. A CC certification delivered by the BSI (German Certification Body) will be recognized and the certification confirmed by the ANSSI (FrenchCertification Body) as well as by the NIST or NSA if the certified product is commercialized in France or USA and if the certification is EAL 4 or lower. There are two official international arrangements between Certification Bodies.

1.2.1 CC Recognition Agreement (CCRA)

The first arrangement is based on the CCRA, written in 2000, that states that all countries that endorse this agreement recognize (accept) the certificates emitted by any other signatory countries up to EAL 4. Basically the limitation of the recognition is linked to the limitation of the common interpretation of the criteria and associated evaluation tasks as described in the CEM documentation. Since the CEM only covers EAL 4 components the recognition agreement are also limited to the EAL 4 level.

For higher levels (and mainly in term of AVA [1]activities) no formal consensus has been found by the different Certification Bodies. Last year the CC Management Board (CCMB) has presented a “vision statement”: http://www.commoncriteriaportal.org/vision.cfm. This document presents the new proposal for the future recognition arrangement between CCRA countries. Based on the status that the application of the CC is strongly dependent on the type of Target Of Evaluation (TOE), this new trend proposes a limitation of the recognition agreement to the EAL 2 level, the main reason being that for higher levels, interpretations of the CEM and CC are possible. The CCRA asks for the establishment of CC communities for each type of TOE to develop Collaborative Protection Profiles (cPP). Those cPP will be composed of PPs (as defined today) but also a set of supporting documents to refine the CEM for this particular type of product. The set of document under the cPP will be developed

[1] AVA is the CC assurance class regarding vulnerability assessment (cf CC v3.1 part 3).

by Technical Communities composed of Certification Bodies, developers and labs. Upon the establishment of this cPP an EAL 4 evaluation would be possibly still covered by the CCRA agreements.

1.2.2 SOG-IS Agreement

The second arrangement was written by the Senior Officials Group – Information Systems Security (SOG-IS). This agreement has been established in Europe to enlarge the CCRA. In its first version (1992) this agreement claims a mutual recognition of any IT evaluation certificate emitted by one of the SOG-IS certificate authorized scheme, including those higher than EAL 4. This agreement has been reviewed in 2010 to limit this recognition agreement for high EALs to specific domains. In 2010 the only domain was “Smart Card and similar devices”. In 2011 a new domain “Hardware Devices with Security Boxes” has been introduced.

Several working groups (JHAS, ISCI/WG1, JTEMS that together constitute the Joint International Working Group, JIWG) have been established to develop and maintain a set of supporting document that explains in detail the expected work to be done during the evaluation and ensure the homogeneity of the evaluation process.

1.3 SOG-IS and IT-Technical domains

The SOG-IS agreement defines two IT-Technical domains for which it is possible to realize evaluations for higher levels than EAL 4 and share the results between over the different countries that endorsed the agreement.

SOG-IS extract: scope article of the agreement

“It is mutually understood that, in respect of IT products […] and protection profiles, the Participants (e.g. the Certification Bodies) plan to recognize the conformant certificates […] which have been authorized by any other certificate authorizing Participant in accordance with the terms of this Agreement and in accordance with the applicable laws and regulations of each Participant. This Agreement covers claims of compliance against any of the Common Criteria Evaluation Assurance Level 1 through 4 […]. Recognition of higher assurance levels (including augmentations) can be defined for specific IT technical domains as agreed by the Management Committee and as defined in 1.3.1 and 1.3.2. This recognition requires additional proof of competencies as defined in 1.4.”

1.3.1 IT-Technical Domain “Smart cards and similar devices”

This section provides the scope and rationale for the IT-Technical Domain with Smart card and similar devices.

The IT-Technical Domain is related to smart cards and similar devices where significant proportions of the required security functionality depend upon hardware (for example smart card hardware, smart card composite products, TPMs used in Trusted Computing, digital tachographs, Host Security Modules, etc.).

Rationale

In the technologies covered by the scope above an attacker will often be able to obtain ready physical access to the device (or a set of devices), the device may well contain critical information such as security credentials/keys and part of the security functionality required of

the device will relate to self-protection either by active (tamper detection) or passive means (such as tamper resistant coatings). This contrasts with standard multipurpose hardware as used in general processing equipment such as a PC. The evaluation approach needs to consider all hardware specific aspects of vulnerability analysis including those that require significant additional equipment and resources. Such devices are frequently composed from elements produced by different developers (for example hardware, smart card operating system, and application) and may involve production across a range of development sites (e.g. IC design, mask production, fabrication, characterization, etc.). These factors must also be consistently taken into account during evaluation and certification.

1.3.2 IT-Technical Domain "Hardware Devices with Security Boxes"

This section provides the scope and rationale for the IT-Technical Domain "Hardware Devices with Security Boxes".

This IT-Technical Domain is related to products produced from a series of discrete parts on one or more printed circuit boards whereby significant proportions of the required security functionality depend upon a hardware physical envelope with counter-measures (a so-called "Security Box") against direct physical attacks (for example payment terminals, tachograph vehicle units, smart meters, taxi meters, access control terminals, Hardware Security Modules, etc.). More precisely, this domain covers products such as payment terminal or HSM on which part of the security relies on a "secure" package that protects internal from an attacker. Those secure envelops detect any physical attack and trigger security action (generally secret erasure) on detection.

Rationale

In the technologies covered by the above scope, an attacker will often be able to obtain ready physical access to the device (or a set of devices). The device may well contain critical information such as security credentials/keys, or could be used also for secure entry of credentials/keys and a significant part of the security functionality required of the device will relate to self-protection against physical attacks. These self-protection counter-measures or the "security box" of such devices is composed of physical protection counter-measures based on hardware and software active mechanisms. Usually these mechanisms involves also passive protections as an inherent part of the provided security functionality e.g. metallic shields or armored plating, wire meshing, chemical protections like epoxy resin, etc. in conjunction with sensors and electronic anti-tampering mechanisms like secure data erasing, alarm generation or component emergency destruction.

The evaluation approach needs to consider all software, firmware and hardware specific aspects of vulnerability analysis including those that may require significant additional equipment and resources. Such devices are also frequently composed from discrete parts produced by different developers. These factors must also be consistently taken into account during evaluation and certification.

1.4 CC and SOG-IS supporting documents

Regarding the evaluations for higher EALs (EAL 5 to 7), on the one hand, the CEM does not propose any guidance (except for some SARs, but this is not exhaustive and a complete EAL 5 evaluation cannot be based on what is written solely in the CEM). On the other hand, these high level missing SARs are clearly out of scope in the SOG-IS agreement.

A big open question is: how in these conditions a CC evaluation with a level equal or greater than 5 can be performed and recognized internationally? There are very few approaches on how to deal with this question. The SOG-IS approach is to create supporting documents specifically to cover the SOG-IS IT-Technical domains high EAL specificities. In the next section we present these documents.

1.4.1 Smart card and similar devices supporting documents

In the table below are listed the approved JIWG supporting documents for the IT-Technical Domain ”Smart card and similar devices”.

The JIWG supporting documents listed in the following are related to the IT-Technical Domain ”Smart card and similar devices” and are approved with the version indicated at the time when this agreement comes into force. The documents listed below support the evaluation up to EAL 7. They are monitored and updated by the JIWG.

Document title	Version	Type
Application of Attack Potential to Smartcards	2.9	Mandatory
Application of CC to Integrated Circuits	3.0	Mandatory
Composite product evaluation for Smart Cards and similar devices	1.2	Mandatory
ETR for composite evaluation template	1.0	Guidance
Guidance for Smartcard evaluation	2.0	Guidance
Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices	2.0	Mandatory
Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices - Appendix 1	2.0	Guidance
Certification of "open" smart card products	1.1	For test
Requirements to perform Integrated Circuit Evaluations	1.1	Mandatory
Minimum site security requirements	1.0	For test

Source: http://sogis.eu/fr/supporting_doc_fr.html

1.4.2 Hardware devices with security boxes CC supporting documents

In the table below are listed the approved JIWG supporting documents for the domain "Hardware devices with security boxes".

The JIWG supporting documents listed in the following table support the evaluation of products related to the IT-Technical Domain "Hardware Devices with Security Boxes" up to EAL 7. They are continuously monitored and updated by the JIWG.

Document title	Version	Type
Application of Attack Potential to Hardware Devices with Security Boxes	1.0	For trial use

1.4.2.1 Point of Interaction (POIs)

Document title	Version	Type
Application of Attack Potential to POIs	1.0	For trial use
CEM Refinements for POI Evaluation	1.0	For trial use

1.4.2.2 Digital Tachograph

Document title	Version	Type
Security Evaluation and Certification of Digital Tachographs	1.12	Mandatory

1.5 Feasibility of high EAL evaluations with AIS34 and ANSSI Note 12

In CC3.1 part 3, every action of the evaluator and every action of the developer are written. However, in the CEM, the work units corresponding to high level SAR, composing the high EALs are not formulated. For instance, in the CEM for ADV_FSP.6 (required for EAL 7), it is stated: "There is no general guidance; the scheme should be consulted for guidance on this sub-activity."

In order to perform high EAL evaluations, there exists generic guidance on CC evaluations, distinct from the IT-technical domains guidance:

- AIS34 provides supplementary methodology with respect to the CEM. This additional methodology addresses EAL 5 in CC2.3 on the one hand and EAL 5+ (with "traditional" augmentations like ALC_DVS.2) and EAL 6 in CC3.1 on the other hand.
- ANSSI Note 12 explains how the assurance component ADV_SPM (related to Security Policy Modeling) must be understood and addressed by the developers and the evaluators. ADV_SPM is required starting from EAL 6. ANSSI Note 12 is based on AIS 34 and CC3.1. It can be seen as an add-on to AIS 34. Its intended readership

is European ITSEFs and developers. It provides additional information on the interpretation of the task ADV_SPM with respect to AIS 34 and clarifies some technical notions such as characteristics, rules, features and properties and provides explanations on the differences between ADV_SPM.3 in CC2.3 and ADV_SPM.1 in CC3.1.

Regarding EAL 5, the CEM entirely defines the assurance components required.

Regarding EAL 6, the AIS34 and the ANSSI note 12 provide missing guidance to assurance components not included in the CEM.

However, regarding EAL 7, there are still missing assurance components that are not defined either in the CEM, in AIS34, or in Note 12.

The details on each assurance component sufficiency for EAL 5 to 7 are presented in chapter 2.

Chapter 2 Assurance components differential in EAL 5/6/7

In this version of the document, the inputs considered to elaborate the differential analysis are the CC3.1 part 3, the CEM, AIS34 and ANSSI Note 12.Please note that AIS 34 and ANSSI Note 12 are not international CC supporting documents but depends on national schemesHowever, they are largely used in European evaluations.

This chapter is organized as follows: first, a comparison between the different assurance packages for high EALs, then a synthesis of the differentials between the SARs required for EAL 5 to 7.

This synthesis summarizes the detailed analysis (§2.3 to 2.5) performed on each individual EAL (5 to 7). The analysis states sufficiency or not of the information contained in the CEM or the CC to perform an evaluation at EAL 5, 7 or 7.

2.1 Comparison between assurance packages

This comparison is based on CC3.1 part 3. Differences and/or additions are in bold characters.

EAL 5	EAL 6	EAL 7
EAL 5 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.	**EAL 6** 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.	**EAL 7** 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.
	Assurance is additionally gained through a formal model of select TOE security policies and a semiformal presentation of the functional specification and TOE design.	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 TSF design is also required. The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional	A modular, **layered and simple** TSF design is also required. The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional	A modular, layered and simple TSF design is also required. The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional

EAL 5	EAL 6	EAL 7
specification, TOE design, selective independent confirmation of the developer test results, and **an independent** vulnerability analysis demonstrating resistance to penetration attackers with **a moderate** attack potential. **EAL 5** also provides assurance through the use of **a** development environment controls, and **comprehensive** TOE configuration management including automation, and evidence of secure delivery procedures. This EAL represents a meaningful increase in assurance from **EAL 4** 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.	specification, TOE design, selective independent confirmation of the developer test results, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a **high** attack potential. **EAL 6** also provides assurance through the use of a **structured** development **process, development** environment controls, and comprehensive TOE configuration management including **complete** automation, and evidence of secure delivery procedures. This EAL represents a meaningful increase in assurance from **EAL 5** 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.**	specification, TOE design **and implementation representation, complete** independent confirmation of the developer test results, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a high attack potential. **EAL 7** also provides assurance through the use of a structured development process, development environment controls, and comprehensive TOE configuration management including complete automation, and evidence of secure delivery procedures. This EAL represents a meaningful increase in assurance from **EAL 6** by requiring more comprehensive analysis **using formal representations** and **formal correspondence,** and **comprehensive testing.**

Table 1: Assurance packages comparison

2.2 EALs differential synthesis based on EAL 5+ as defined in PikeOS-ST

Pike-OS ST states that the TOE shall be evaluated at EAL 5 augmented with ASE_TSS.2 and AVA_VAN.5.

The table below must be read as follows: in white cells is written what is expected from aSAR level to the next, if the EAL augmentation triggers an SAR augmentation. If there is no difference between SARs from one EAL to the next, the cell is grey.

SAR titles reminder:

- ADV_ARC: security architecture
- ADV_FSP: functional specification
- ADV_IMP: implementation representation
- ADV_INT: TSF internals
- ADV_SPM: security policy modeling
- ADV_TDS: TOE design
- AGD_OPE: operational user guidance
- AGD_PRE: preparative procedures
- ALC_CMC: CM capabilities
- ALC_CMS: CM scope
- ALC_DEL: delivery
- ALC_DVS: development security
- ALC_LCD: life cycle definition
- ALC_TAT: tools and techniques
- ATE_COV: coverage
- ATE_DPT: depth
- ATE_FUN: functional tests
- ATE_IND: independent testing
- AVA_VAN: vulnerability analysis

EAL4 to EAL 5+		**EAL 5+ to EAL 6**		**EAL 6 to EAL 7**	
SARs augmentations	Differences	SARs augmentations	Differences	SARs augmentations	Differences
ADV_ARC.1		ADV_ARC.1		ADV_ARC.1	
ADV_FSP.4 to 5	Changes from EAL 4 (ADV_FSP.4) are the semiformal style of the FSP plus a rationale for each error message, even those that do not result from an invocation of a TOE Security Functionality Interface (TSFI). Only rationales for error messages resulting from the TSFI invocation were required in ADV_FSP.4	ADV_FSP.5		ADV_FSP.5 to 6	SAR title: *complete semi-formal functional specification with additional formal specification.* **No guidance** in the CEM or in AIS34 for ADV_FSP.6
ADV_IMP.1		ADV_IMP.1 to 2	Changes from EAL 5 (ADV_IMP.1) are the complete mapping of design description, instead of a sample mapping, to the implementation representation.	ADV_IMP.2	

EAL4 to EAL 5+		EAL 5+ to EAL 6		EAL 6 to EAL 7	
SARs augmentations	Differences	SARs augmentations	Differences	SARs augmentations	Differences
none to ADV_INT.2	SAR title: *well-structured internals.* The whole TOE Security Functionality (TSF) has to be well structured and the developer shall provide characteristics, definitions and rationales to demonstrate it.	ADV_INT.2 to 3	SAR title: *minimally complex internals.* **No guidance** in the CEM. AIS34: details are provided on the fact that the TSF shall have well-structured internals but not overly complex. The developer is supposed to discuss both aspects (i.e. every well-structured internal is not too complex) simultaneously.	ADV_INT.3	
None		none to ADV_SPM.1	SAR title: *formal TOE security policy model.* The developer has to provide a formal security policy model, a formal proof of correspondence between the model and any formal specification and a demonstration of correspondence between the model and the functional specification.	ADV_SPM.1	

EAL4 to EAL 5+		EAL 5+ to EAL 6		EAL 6 to EAL 7	
SARs augmentations	Differences	SARs augmentations	Differences	SARs augmentations	Differences
ADV_TDS.3 to 4	Changes from EAL4 are that modular design has to be in a semiformal representation and the Security Functional Requirement (SFR) characterization of modules details. In ADV_TDS.4, SFR-enforcing AND SFR-supporting modules have to be described in terms of SFR-related interfaces (+ return values, interactions, etc.) to other modules whereas in ADV_TDS.3, only SFR-enforcing modules' interfaces were required.	ADV_TDS.4 to 5	Changes from EAL5 are that the semiformal modular design has to be complete and justifications on purposes, interfaces, interactions, etc. of **all** type of SFR characterized modules (including SFR-non-interfering ones) have to be provided.	ADV_TDS.5 to 6	SAR title: *Complete semiformal modular design.* **No guidance** in the CEM or in AIS34.
AGD_OPE.1		AGD_OPE.1		AGD_OPE.1	
AGD_PRE.1		AGD_PRE.1		AGD_PRE.1	

EAL4 to EAL 5+		EAL 5+ to EAL 6		EAL 6 to EAL 7	
SARs augmentations	Differences	SARs augmentations	Differences	SARs augmentations	Differences
ALC_CMC.4		ALC_CMC.4 to 5	Quality: parts of adequate quality are included into the TOE if acceptance procedures followed. Roles segregation: the developer of a conf. item cannot accept it into the CM/TOE. TSF items of the CM clearly identified. Audit trails of all changes (min: originator, date and time). Dependencies: systematically describe how the changes made to one item impact other items. Identification of the CM version from which the TOE is generated. Reapplying by the evaluator of the production procedures (if possible).	ALC_CMC.5	
ALC_CMS.4 to 5	Configuration List must include all tools involved in the development and production of the TOE.	ALC_CMS.5		ALC_CMS.5	

EAL4 to EAL 5+		EAL 5+ to EAL 6		EAL 6 to EAL 7	
SARs augmentations	Differences	SARs augmentations	Differences	SARs augmentations	Differences
ALC_DEL.1		ALC_DEL.1		ALC_DEL.1	
ALC_DVS.1		ALC_DVS.1 to 2	Strongly linked to AVA_VAN (see below): presentation of security measures of the development/production sites and rationale on why/how these measures contribute to protect the TOE confidentiality and integrity. To be coupled with the vulnerability analysis by the developer.	ALC_DVS.2	
ALC_LCD.1		ALC_LCD.1		ALC_LCD.1 to 2	Measurable life-cycle model: metrics and parameters must be provided to measure the quality of the TOE and its development.

EAL4 to EAL 5+		EAL 5+ to EAL 6		EAL 6 to EAL 7	
SARs augmentations	Differences	SARs augmentations	Differences	SARs augmentations	Differences
ALC_TAT.1 to 2	2 new evidences in this task: - implementation standards description - TSF implementation representation Use of implementation standards or not. If some are used, Developer must provide a description of their implementation that the evaluator verifies based on the implementation representation of the TSF.	ALC_TAT.2 to 3	Documentation of development tools used by third party contributors to the TOE has to be included and reviewed in each work unit along the rest of the documentation for this task.	ALC_TAT.3	
ASE_TSS.1 to 2	Provide description of how the TOE protects itself against interference, logical tampering and bypass. Composed TOE: how the components combine to provide protection.	ASE_TSS.2		ASE_TSS.2	
ATE_COV.2		ATE_COV.2 to 3	Complete testing of all the TSFIs. In ATE_COV.2, only testing of all the TSFIs is required.	ATE_COV.3	

EAL4 to EAL 5+		EAL 5+ to EAL 6		EAL 6 to EAL 7	
SARs augmentations	Differences	SARs augmentations	Differences	SARs augmentations	Differences
ATE_DPT.1 to 3	Testing modular design: all modules in the TOE design must be tested whereas in ATE_DPT.1, only subsystems have to be tested.	ATE_DPT.3		ATE_DPT.3 to 4	SAR title: *testing implementation representation.* **No guidance** in the CEM or in AIS34.
ATE_FUN.1		ATE_FUN.1 to 2	SAR title: *ordered functional testing.* **No guidance** in the CEM. AIS34: this task is strongly linked to the vulnerability analysis. The ordering of tests chosen by the developer must be justified in order to show that the ordering aims to counter known vulnerabilities and does not, on the contrary, hide potential vulnerabilities by avoiding tests that would highlight them.	ATE_FUN.2	
ATE_IND.2		ATE_IND.2		ATE_IND.2 to 3	SAR title: *independent testing - complete.* **No guidance** in the CEM or in AIS34.

EAL4 to EAL 5+		EAL 5+ to EAL 6		EAL 6 to EAL 7	
SARs augmentations	Differences	SARs augmentations	Differences	SARs augmentations	Differences
AVA_VAN.3 to 5	The only difference between the two tasks is the attacker potential: high in AVA_VAN.5, enhanced-basic in AVA_VAN.3. However, the guides and approach to follow by the developer and the evaluator for the vulnerability analysis are not at all the same depending on the attacker potential on the one hand, on the type of device on the other hand. For a smart card-like device, particular care has to be taken for hardware penetration testing since the attacker can have total access to the whole device.	AVA_VAN.5		AVA_VAN.5	

Table 2: EALs differential

2.3 EAL 5

2.3.1 ADV (Development)

2.3.1.1 ADV_FSP.5 (Functional Specification)

2.3.1.1.1 Dependencies

ADV_IMP.1, ADV_TDS.1

2.3.1.1.2 Objectives

The objective is to determine whether the developer has completely described all the interfaces to the TSF (the TSFI) and if the TSFI implement the security functional requirements (SFR) of the Security Target.

2.3.1.1.3 Developer

The developer activities are the same as EAL 4 level.

2.3.1.1.4 Evaluator

Changes for the evaluator are the TSFI description using a semi-formal [2]style and the providing of a rationale for each error message contained in the TSF implementation yet does not result from an invocation of a TSFI.

2.3.1.1.5 Conclusion

The CEM contains sufficient information to guide the evaluator activities.

2.3.1.2 ADV_INT.2 (TSF Internals)

2.3.1.2.1 Dependencies

ADV_IMP.1, ADV_TDS.3

2.3.1.2.2 Objectives

The objective is to determine whether the TSF is designed and structured such that the likelihood of flaws is reduced and that maintenance can be more readily performed without the introduction of flaws.

2.3.1.2.3 Developer

The developer has to demonstrate that the entire TSF is designed and implemented with well-structured internals, providing description and justification.

2.3.1.2.4 Evaluator

The evaluator determines that a justification is provided describing the characteristics used to judge the meaning of “well-structured” and that the TSF internals description demonstrates that the entire TSF is well-structured.

[2] A semi-formal presentation is characterised by a standardised format with a well-defined syntax that reduces ambiguity that may occur in informal presentations. Since the intent of the semi-formal format is to enhance the reader's ability to understand the presentation, use of certain structured presentation methods (pseudo-code, flow charts, block diagrams) are appropriate, though not required.

2.3.1.2.5 Conclusion

It should be noted that ADV_INT.1 is never required for an existing EAL. ADV_INT.1 asks for a demonstration of well-structured internals subset of the TSF.

EAL 5 introduces directly ADV_INT.2, where the whole TSF has to be well structured and the developer shall provide characteristics, definitions and rationales to demonstrate it.

The CEM contains sufficient information to guide the evaluator activities.

2.3.1.3 ADV_TDS.4 (TOE Design)

2.3.1.3.1 Dependencies

ADV_FSP.5

2.3.1.3.2 Objectives

The objective is to determine whether the TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary, and provides a description of the TSF internals in terms of modules (and optionally higher-level abstractions). It provides a detailed description of the SFR-enforcing and SFR-supporting modules and enough information about the SFR-non-interfering modules for the evaluator to determine that the SFRs are completely and accurately implemented; as such, the TOE design provides an explanation of the implementation representation.

2.3.1.3.3 Developer

The developer activities are the same as EAL 4 level but its description must classify each module as SFR-enforcing, SFR-supporting, or SFR-non-interfering and use semiformal description.

2.3.1.3.4 Evaluator

Changes for the evaluator are the checking of the following elements:

- The description of the whole TSF in terms of modules, designating each of them as SFR-enforcing, SFR-supporting, or SFR-non-interfering,
- A semiformal description of each subsystem of the TSF, supported by informal, explanatory text where appropriate,
- The description of each SFR-enforcing and SFR-supporting module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing or SFR-supporting modules.

2.3.1.3.5 Conclusion

Changes from EAL 4 are that subsystem design has to be in a semiformal representation as well as SFR characterization of modules details. In ADV_TDS.4, SFR-enforcing AND SFR-supporting modules have to be described in terms of SFR-related interfaces (and return values, interactions, etc.) to other modules whereas in ADV_TDS.3, only SFR-enforcing modules' interfaces are required.

The CEM contains sufficient information to guide the evaluator activities.

2.3.2 AGD (Guidance Documents)

There is no difference between EAL 4 and 5 for the AGD assurance class.

2.3.3 ALC (Life-Cycle Support)

2.3.3.1 ALC_CMS.5 (CM scope)

2.3.3.1.1 Dependencies

No dependencies.

2.3.3.1.2 Objectives

The objective is to determine whether the configuration list includes the TOE, the parts that comprise the TOE, the TOE implementation representation, security flaws, development tools and related information, and the evaluation evidence. These configuration items are controlled in accordance with CM capabilities (ALC_CMC).

2.3.3.1.3 Developer

The developer activities are similar to EAL 4 one but the configuration list must be covers additional items .

2.3.3.1.4 Evaluator

There is one new item to check for the evaluator with respect to ALC_CMS.4: the configuration list must include **development tools and related information.**

2.3.3.1.5 Conclusion

The configuration list must include **all** tools involved in the TOE development, including third party tools or components.

The CEM contains sufficient information to guide the evaluator activities.

2.3.3.2 ALC_TAT.2 (Tools and techniques)

2.3.3.2.1 Dependencies

ADV_IMP.1

2.3.3.2.2 Objectives

There is one new item in the objectives for ALC_TAT.2 with respect to the objectives for ALC_TAT.1.

The objective is to determine whether the developer has used well-defined development tools (e.g. programming languages or computer-aided design (CAD) systems) that yield consistent and predictable results, **and whether implementation standards have been applied.**

2.3.3.2.3 Developer

Change for the developer is that he must describe and provide the implementation standards that are being applied.

2.3.3.2.4 Evaluator

Change for the evaluator is that he has to examine the implementation process to determine that documented implementation standards have been applied, by using the TSF implementation representation provided in this task.

2.3.3.2.5 Conclusion

Two new evidences are required for this task:

- The implementation standards description,
- TSF implementation representation.

The evaluator has to determine if implementation standards are used or not. If some are used, the developer must provide a description of their implementation that the evaluator verifies based on the implementation representation of the TSF.

The CEM contains sufficient information to guide the evaluator activities.

2.3.4 ASE (Security Target Evaluation)

2.3.4.1 ASE_TSS.2 (TOE summary specification)

2.3.4.1.1 Dependencies

ADV_ARC.1, ASE_INT.1, ASE_REQ.1

2.3.4.1.2 Objectives

The objective is to determine whether the TOE summary specification addresses all SFRs, whether the TOE summary specification addresses interference, logical tampering and bypass, and whether the TOE summary specification is consistent with other narrative descriptions of the TOE.

2.3.4.1.3 Developer

The developer activities are the same as EAL 4 level.

2.3.4.1.4 Evaluator

A description has to be provided of how the TOE protects itself against interference, logical tampering and bypass. In the case of a composed TOE, the description must address the way the different components combine to provide protection.

2.3.4.1.5 Conclusion

The CEM contains sufficient information to guide the evaluator activities.

2.3.5 ATE (Tests)

2.3.5.1 ATE_DPT.3 (Depth)

2.3.5.1.1 Dependencies

ADV_ARC.1, ADV_TDS.4, ATE_FUN.1

2.3.5.1.2 Objectives

The objective is to determine whether the developer has tested all the TSF subsystems and modules against the TOE design and the security architecture description.

2.3.5.1.3 Developer

The developer must provide test and provides tests evidence for all modules.

2.3.5.1.4 Evaluator

The main difference is that all TSF modules have to be tested whereas in ATE_DPT.1, only TSF subsystems level has to be.

2.3.5.1.5 Conclusion

The CEM contains sufficient information to guide the evaluator activities.

2.3.6 AVA (Vulnerability Assessment)

2.3.6.1 AVA_VAN.4 (Vulnerability analysis)

2.3.6.1.1 Dependencies

ADV_ARC.1, ADV_FSP.2, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

2.3.6.1.2 Objectives

The objective is to determine whether the TOE, in its operational environment, has vulnerabilities exploitable by attackers possessing **Moderate** attack potential (AIS34)

2.3.6.1.3 Developer

The developer activities are the same as EAL 4.

2.3.6.1.4 Evaluator

The evaluator activities are the same as EAL 4 (if we refer to AIS34 only and since there is no guidance in the CEM for this task).

The criteria also introduce the concept of methodical vulnerability analysis. The CEM gives all necessary explanation in annex B2.2.2.3.

2.3.6.1.5 Conclusion

The only difference between the two tasks is the attacker potential: **moderate** in AVA_VAN.4, **enhanced-basic** in AVA_VAN.3. However, the guides and approach to follow by the developer and the evaluator for the vulnerability analysis are not at all the same depending on the attacker potential on the one hand, on the type of device on the other hand.
For a smart card-like device, particular care has to be taken for hardware penetration testing since the attacker can have total access to the whole device.

For a MILS product special guidance must be developed to refine which specific potential vulnerabilities have to be used for the analysis. This guidance may be initiated with deliverables from EURO-MILS WPs 3.2 (evaluation) and 3.3 (attack methods). The physical limits of the TOE must also be stated.

2.4 EAL 6

2.4.1 ADV (Development)

2.4.1.1 ADV_IMP.2 (Implementation representation)

2.4.1.1.1 Dependencies

ADV_TDS.3, ALC_TAT.1, ALC_CMC.5

2.4.1.1.2 Objectives

The objective is to determine that the implementation representation made available by the developer is suitable for use in other analysis activities; suitability is judged by its conformance to the requirements for this component.

2.4.1.1.3 Developer

The difference with the EAL 5 level is that the developer shall provide a **complete** mapping between TOE design and implementation representation.

2.4.1.1.4 Evaluator

Completeness has to be in both directions: TOE Design must be covered by the implementation representation and implementation representation must be mapped to a part of the TOE Design. So the evaluator shall check the completeness in the both directions. There is no more information in the CEM.

2.4.1.1.5 Conclusion

The EAL 6 has not an important impact on the evaluation method, as the verification is already done in EAL 5, but here the mapping has to be complete. The CEM contains sufficient information to guide the evaluator activities.

2.4.1.2 ADV_INT.3 (TSF Internals)

2.4.1.2.1 Dependencies

ADV_IMP.1, ADV_TDS.3, ALC_TAT.1

2.4.1.2.2 Objectives

Based on AIS34, the objective of this component is to provide a mean for requiring the TSF to be well-structured and of minimal complexity. The intent is that the entire TSF has to be designed and implemented using sound engineering principles.

The activities on this component depend on the technologies used in the TOE, for example the complexity notion is not the same between software and hardware products.

2.4.1.2.3 Developer

The developer activities are the same as EAL 5 level, but the meaning of "complex" has to be described and the TSF internals description should not be too complex.

2.4.1.2.4 Evaluator

The evaluator activities are the same as EAL 5 level, but with a focus on complexity of the TSF and the evaluator shall perform an analysis on the entire TSF.

2.4.1.2.5 Conclusion

There is no information in the CEM regarding this task.

A guidance to define the complexity notion should be done. Indeed, complexity is a subjective notion and depends on the technologies used (programming language, software, hardware…). An option could be to define some generic metrics on main technologies used.

2.4.1.3 ADV_SPM.1 (Security policy modelling)

2.4.1.3.1 Dependencies

ADV_FSP.4

2.4.1.3.2 Objectives

It is the objective of this family to provide additional assurance from the development of a formal security policy model of the TSF, and establishing correspondence between the functional specification and this security policy model. Preserving internal consistency the security policy model is expected to formally establish the security principles from its characteristics by means of a mathematical proof.

The activities on this component are not strongly dependent on technologies used in the TOE as the formal specification can be an abstraction of the TOE.

2.4.1.3.3 Developer

The developer shall provide a formal security policy model, a formal proof of correspondence between the model and any formal specification and a demonstration of correspondence between the model and the functional specification. According to CC3.1 definition, formal means expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

According to ANSSI Note 12, the documentation of the model must contain at least:

- A justification of the methods and tools chosen,
- An explication of the model,
- An argument of the links between the models and the security target (formal/informal),
- A presentation and justification of hypothesis,
- Links between the TOE and model.

2.4.1.3.4 Evaluator

The evaluator shall verify the relevance, sufficiency and correctness of the element provided by the developer.

The ANSSI Note 12 specifies in details the different steps of evaluation (http://www.ssi.gouv.fr/IMG/pdf/NOTE-12-modelisation-formelle.pdf) and so does AIS34.

2.4.1.3.5 Conclusion

There is no information in the CEM regarding this task.

AIS34 and Note 12 (see 1.5) are sufficient to guide the evaluator on SPM Evaluation. The Note 12 specifies the link with FSP.5 and FSP.6, AIS34 specifies only with FSP.5. A guide about weakness and typical error with formal methods could be done to share the same point of view between developer and evaluator.

2.4.1.4 ADV_TDS.5 (TOE Design)

2.4.1.4.1 Dependencies

ADV_FSP.5

2.4.1.4.2 Objectives

Based on AIS34, the design description of a TOE provides both context for a description of the TSF, and a thorough description of the TSF. As assurance needs increase, the level of detail provided in the description also increases. As the size and complexity of the TSF increase, multiple levels of decomposition are appropriate. The design requirements are

intended to provide information (commensurate with the given assurance level) so that a determination can be made that the security functional requirements are realized.

The activities on this component depend on the technologies used in the TOE.

2.4.1.4.3 Developer

The main difference with the EAL 5 level is that the developer shall provide a complete semiformal modular design instead of a semiformal subsystem design. This description must give the purpose of each module.

2.4.1.4.4 Evaluator

The evaluator shall check that the design provides a semiformal description of each module in terms of its purpose, interaction, interfaces, return values from those interfaces, and called interfaces to other modules, supported by informal, explanatory text where appropriate.

He shall also check that each module is described in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing, SFR-supporting or SFR-non-interfering modules.

2.4.1.4.5 Conclusion

There is no information in the CEM regarding this task.

As the semi-formal notion is already defined in EAL 5, EAL 6 impacts are on the completeness of the modular design and the addition of SFR-non-interfering interfaces modules description. The guidance that will be defined for EAL 5 should be the same for EAL 6.

2.4.2 AGD (Guidance documents)

There is no difference between EAL 5 and 6 for the AGD assurance class.

2.4.3 ALC (Life-Cycle support)

2.4.3.1 ALC_CMC.5 (CM capabilities)

2.4.3.1.1 Dependencies

ALC_CMS.1, ALC_DVS.2, ALC_LCD.1

2.4.3.1.2 Objectives

A unique reference is required to ensure that there is no ambiguity in terms on which instance of the TOE is being evaluated. Labeling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

2.4.3.1.3 Developer

The differences with the EAL 5 are:

- The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.
- The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.
- The CM system shall identify the configuration items that comprise the TSF.

- The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.
- The CM system shall provide automated means to identify all other configuration items that are affected by the change of a given configuration item.
- The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.

2.4.3.1.4 Evaluator

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. The verification shall be done on a sample of CI (Configuration Item).

CEM specifies with more details the evaluator activities:

- Examine the CM documentation to determine that the acceptance procedures are sufficiently to review all changes to all CI.
- Examine from acceptance procedure that there is independence between acceptance and development.
- Examine from the CM Documentation and a sample of CI containing TSF and non-TSF item that items are correctly classified by the CM system.
- Examine a sample of audits trails and check that the originator, date and time are included.
- Select a sample of configuration items, covering all types of items, and exercise the automated means to determine that it identifies all items that are affected by the change of the selected item.

The CEM provides guidance on sampling.

The evaluator shall examine the production support procedures to determine that by following these procedures a TOE would be produced like that one provided by the developer for testing activities.

If the TOE is a small software TOE and production consists of compiling and linking, the evaluator might confirm the adequacy of the production support procedures by reapplying them himself.

If the production process of the TOE is more complicated (as for example in the case of a smart card), but has already started, the evaluator should inspect the application of the production support procedures during a visit of the development site. He might compare a copy of the TOE produced in his presence with the samples used for his testing activities.

The CEM provides a guidance on site visits.

Otherwise the evaluator's determination should be based on the documentary evidence provided by the developer.

2.4.3.1.5 Conclusion

The CEM contains sufficient information to guide the evaluator activities.

2.4.3.2 ALC_DVS.2 (Development security)

2.4.3.2.1 Dependencies

No dependencies.

2.4.3.2.2 Objectives

The objective of this sub-activity is to determine whether the developer's security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised. Additionally, sufficiency of the measures as applied is intended to be justified.

2.4.3.2.3 Developer

The main difference with EAL 5 level is that development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

The idea here is to make the developer elaborate its vulnerability analysis, for AVA_VAN task, in parallel with the site presentation documentation.

2.4.3.2.4 Evaluator

The evaluator shall examine the development security documentation to determine that an appropriate justification is given as to why the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

2.4.3.2.5 Conclusion

The CEM contains sufficient information to guide the evaluator activities.

2.4.3.3 ALC_TAT.3 (Tools and techniques)

2.4.3.3.1 Dependencies

ADV_IMP.1

2.4.3.3.2 Objectives

The objective of this sub-activity is to determine whether the developer and his subcontractors have used well-defined development tools (e.g. programming languages or computer-aided design (CAD) systems) that yield consistent and predictable results, and whether implementation standards have been applied.

2.4.3.3.3 Developer

The main difference with EAL 5 is that the developer shall describe and provide the implementation standards applied by any third-party providers for all parts of the TOE.

2.4.3.3.4 Evaluator

The evaluator shall confirm that the documentation associated to third-party providers tools, including implementation standards, has been provided and that all the implementation standards have been applied.

2.4.3.3.5 Conclusion

The scope of evaluation is larger, because the evaluator has to consider the third-party providers for all parts of the TOE. The CEM contains sufficient information to guide the evaluator activities.

2.4.4 ASE (Security Target Evaluation)

There is no difference between EAL 5 and 6 for the ASE assurance class.

2.4.5 ATE (Tests)

2.4.5.1 ATE_COV.3 (Coverage)

2.4.5.1.1 Dependencies

ADV_FSP.2, ATE_FUN.1

2.4.5.1.2 Objectives

Based on AIS34, in this component, the objective is to confirm that the developer performed exhaustive tests of all interfaces in the functional specification.

The objective of this component is to confirm that all parameters of all of the TSFIs have been tested. The activities on this component depend on the technologies used in the TOE, indeed coverage testing are not the same between hardware and software.

2.4.5.1.3 Developer

The main difference with EAL 5 is that the test coverage shall demonstrate that all TSFIs in the functional specification have been **completely** tested.

2.4.5.1.4 Evaluator

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. There is no real difference with EAL 5, except that the coverage has to be complete. AIS34 specifies with more details the evaluator activities.

2.4.5.1.5 Conclusion

There is no guidance in the CEM for ATE_COV.3. AIS34 elements can be used to complete this task.

2.4.5.2 ATE_FUN.2 (Functional tests)

2.4.5.2.1 Dependencies

ATE_COV.1

2.4.5.2.2 Objectives

The objective is to determine whether the developer correctly performed and documented the tests in the test documentation and to ensure that testing is structured such as to avoid circular arguments about the correctness of the interfaces being tested.

2.4.5.2.3 Developer

The developer activities are the same as EAL 5.

2.4.5.2.4 Evaluator

AIS34 proposes a new action element for the evaluator:

ATE_FUN.2.5C The test documentation shall include an analysis of the test procedure ordering dependencies.

2.4.5.2.5 Conclusion

There is no guidance in the CEM for EAL 6. AIS34 elements can be used to complete this task. This task is strongly linked to the vulnerability analysis. The ordering of tests chosen by the developer must be justified in order to show that the ordering aims to counter known vulnerabilities and does not, on the contrary, hide potential vulnerabilities by avoiding tests that would highlight them.

2.4.6 AVA (Vulnerability Assessment)

2.4.6.1 AVA_VAN.5 (Vulnerability analysis)

2.4.6.1.1 Dependencies

ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

2.4.6.1.2 Objectives

The objective is to determine whether the TOE, in its operational environment, has vulnerabilities exploitable by attackers possessing **high** attack potential (AIS34)

2.4.6.1.3 Developer

The developer activities are the same as EAL 4.

2.4.6.1.4 Evaluator

The evaluator activities are the same as EAL 4 (if we refer to AIS34 only and since there is no guidance in the CEM for this task).

The criteria also introduce the concept of methodical vulnerability analysis. The CEM gives all necessary explanation in annex B2.2.2.3.

2.4.6.1.5 Conclusion

The only difference between the two tasks is the attacker potential: **high** in AVA_VAN.5, **moderate** in AVA_VAN.4. However, the guides and approach to follow by the developer and the evaluator for the vulnerability analysis are not at all the same depending on the attacker potential on the one hand, on the type of device on the other hand.

For a MILS product special guidance must be developed to refine which specific potential vulnerabilities have to be used for the analysis. The description of an attacker with high attack potential has to be refined in the case of MILS.

2.5 EAL 7

2.5.1 ADV (Development)

2.5.1.1 ADV_FSP.6 (Functional specification)

2.5.1.1.1 Dependencies

ADV_TDS.1, ADV_IMP.1

2.5.1.1.2 Objectives

The objective of this sub-activity is to determine whether the developer has provided a high-level description of at least the SFR-enforcing and SFR-supporting TSFIs.

2.5.1.1.3 Developer

The main differences with EAL 6 are:

- The functional specification of the TSF shall have a formal presentation.

- All error messages contained in TSF implementation representation shall describe or justify why it is not associated with a TSFI.
- Formal model describing the TSFI with informal explanatory text.

2.5.1.1.4 Evaluator

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

2.5.1.1.5 Conclusion

There is no information in the CEM or in AIS34.

A guide with information about FSP.6 evaluation should be done. This guide should contain some precisions about formal modeling of the TSFI, linkage with the other component (ADV_SPM.1 and ADV_TDS.6) and how to choose what has to be formal and semi-formal.

The ANSSI Note 12 specifies that the correspondence with ADV_SPM.1 model should be in a formal style for formal part of FSP. It should also provide some good practices on formal modeling.

2.5.1.2 ADV_TDS.6 (TOE Design)

2.5.1.2.1 Dependencies

ADV_FSP.6

2.5.1.2.2 Objectives

The objective of this sub-activity is to determine that the design description of the TOE provides both context for a description of the TSF, and a thorough description of the TSF.

2.5.1.2.3 Developer

The main differences with EAL 6 are:

- A formal specification of the TSF subsystems shall be done.
- A proof of correspondence between formal specifications of the TSF and of the functional specification (linkage between FSP and TDS). The proof shall demonstrate that all behavior in the TOE design is a correct and complete refinement of the TSFI that invoked it.

2.5.1.2.4 Evaluator

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

There is no information in the CEM or in AIS34.

2.5.1.2.5 Conclusion

A guide with information about TDS.6 evaluation should be done. This guide should contain some precisions about formal modeling of the TSF, linkage with the other component (ADV_TDS.6) and how to choose what has to be formal and semi-formal. It should also provide some good practices on formal modeling. It can also precise in the MILS context what are the main expected subsystems that can be described using formal models.

2.5.2 AGD (Guidance documents)

There is no difference between EAL 6 and 7 for the AGD assurance class.

2.5.3 ALC (Life-Cycle support)

2.5.3.1 ALC_LCD.2 (Life-Cycle definition)

2.5.3.1.1 Dependencies

No dependencies.

2.5.3.1.2 Objectives

The objective of this sub-activity is to determine whether the developer has used a documented **and measurable** model of the TOE life-cycle.

2.5.3.1.3 Developer

The developer has to establish a life-cycle model that is measurable and use it to measure the TOE development.

2.5.3.1.4 Evaluator

The evaluator has to examine the documentation and check that it includes results of the measurements of the TOE development and the details of the model arithmetic parameters and/or metrics used to measure the quality of the TOE and/or its development.

2.5.3.1.5 Conclusion

What is new in ALC_LCD.2 with respect to ALC_LCD.1 is the measurability of the life-cycle model: metrics and parameters must be provided to measure the quality of the TOE and its development. These metrics and parameters must be justified.

There is sufficient information in the CEM regarding this task.

2.5.4 ASE (Security Target Evaluation)

There is no difference between EAL 6 and 7 for the ASE assurance class.

2.5.5 ATE (Tests)

2.5.5.1 ATE_DPT.4 (Depth)

2.5.5.1.1 Dependencies

ADV_ARC.1, ADV_IMP.1, ADV_TDS.4, ATE_FUN.1

2.5.5.1.2 Objectives

The subsystem and module descriptions of the TSF provide a high-level description of the internal workings, and a description of the interfaces of the modules, of the TSF. Testing at this level of TOE description provides assurance that the TSF subsystems and modules behave and interact as described in the TOE design and the security architecture description, and in accordance with the implementation representation.

2.5.5.1.3 Developer

The developer activities are the same as EAL 6 level.

2.5.5.1.4 Evaluator

The evaluator must assess using the depth of testing that the TSF operates in accordance with its implementation representation.

There is no guidance in the CEM or in AIS34.

2.5.5.1.5 Conclusion

Guides have to be written on how this evaluation task is meant to be performed.

2.5.5.2 ATE_IND.3 (Independent testing)

2.5.5.2.1 Dependencies

ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1

2.5.5.2.2 Objectives

The objective is to demonstrate that the TOE operates in accordance with its design representations and guidance documents.

Evaluator testing includes repeating all of the developer tests.

The title of this evaluation task is: Testing implementation representation.

2.5.5.2.3 Developer

The developer activities are the same as EAL 6 level.

2.5.5.2.4 Evaluator

In this component the evaluator must repeat all of the developer's tests as part of the programme of testing. As in the previous component the evaluator will also conduct tests that aim to exercise the TSF in a different manner from that achieved by the developer. In cases where developer testing has been exhaustive, there may remain little scope for this.

There is no guidance in the CEM or in AIS34.

2.5.5.2.5 Conclusion

However, the only difference between ATE_IND.2 and_ATE_IND.3 is completeness concerning:

- The repetition of developer tests and
- The own testing of the entire TSF (i.e. all the SFRs with all their single properties).

Hence, the CEM guidance on ATE_IND.2 may be considered as sufficient also for performing ATE_IND.3..

2.5.6 AVA (Vulnerability Assessment)

There is no difference between EAL 6 and 7 for the AVA assurance class.

Chapter 3 Known EAL 6/7 evaluations and associated assurance components

In this part we propose a non-exhaustive list of the most known hypervisor and a survey about the EAL 6 and EAL 7 evaluation in the world.

3.1 Hypervisor

A hypervisor is a piece of computer software, firmware or hardware that creates and runs virtual machine.

Below, we propose a non-exhaustive list of the most known hypervisor with comments about evaluation

- Bertin Technologies: Polyxene. It was evaluated EAL 5 (CC v2.3) in 2009 based on DCSSI-PP 2009/01
- Green Hills: INTEGRITY-Multivisor. No evaluation was found, but INTEGRITY-178B Separation Kernel from Green Hills was evaluated EAL 6+ (CC v2.3) based on SKPP,
- Wind River: Wind River VxWorks MILS Platform was to be evaluated at EAL6+/NSA high robustness. Evaluation effort has been stopped in 2011.
- Micrium: µC/TimeSpaceOS, (http://micrium.com/rtos/uctimespaceos/overview/)
- SYSGO: PikeOS,
- LynuxWorks: LynxSecure[3]., (http://www.lynuxworks.com/virtualization/lynxsecure-hypervisor.pdf)

3.2 EAL 6/7 Evaluations

To this day, there are 32 CC evaluations EAL 6 or EAL 7 according to the Common Criteria Portal. Most of them concern SmartCard with SECURITY_IC_V1.0 Protection Profile.

Only one evaluation concerns operating systems with Green Hills Software INTEGRITY-178B Separation Kernel EAL 6+ evaluation. This evaluation is based on the SKPP Protection Profile with CC 2.3. However, SKPP does not claim an EAL level because of severe modifications on SARs. SKPP has also been sunset by the NSA (http://www.niap-ccevs.org/announcements/SKPP%20Sunset%20Q&A.pdf).

There is no evaluation EAL 6+ with formal augmentation on FSP or TDS.

[3] Certifiable according claims on the official website to EAL 7. No real certification efforts are known.

Five evaluations EAL 7 were conducted among which three in France on smart card and one in Australia on network device (Tenix ST).

There is one evaluation EAL 7+ (ALC_FLR.3, ASE_TSS.2) for a device (data diode) in Netherlands. According to the security target (Fox ST), the TOE contains physical hardware and does not contain any logic, firmware or software.

3.3 Protection Profiles available

Only four protection profiles have been found on operating system, among which one from US Government (IAD: Information Assurance Directorate), one from BSI, one US/German, and one English (Hewlett Packard). The PP used in PolyXene evaluation was not found on ANSSI website.

The SKPP is the only PP in the following paragraphs addressing Operating Systems for embedded systems: SKPP. The others address more general purpose Operating Systems.

3.3.1 SKPP

The IAD protection profile is called *SKPP for U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness*. It was used on INTEGRITY-178B Separation Kernel EAL 6+ evaluation (CC V2.1), but is no longer available for new Security Target compliance claims since 2011-09-01 (source: http://www.niap-ccevs.org/pp/archived)

3.3.2 OSPP

The OSPP, a BSI protection profile is called BSI-CC-PP-0067 Operating System Protection Profile. It defines the security functionality expected to be provided by a general-purpose operating system capable of operating in a networked environment. It's suitable for evaluation up to EAL 4+ (ALC_FLR.3). It was used on many evaluations in Germany

3.3.3 GPOSPP

The US/German protection profile is called GPOSPP V3.9 for General-Purpose Operating System Protection Profile. According to the protection profile it's a joint effort by NIAP (National Information Assurance Partnership) and BSI. It's an evolution from the GPSOPP v1.0 by NIAP. The previous PP was used one many evaluation in USA. No evaluation with the new version of PP was found.

3.3.4 CCOPP-OS

The English PP is called CCOPP-OS for Compartmentalized Operations Protection Profile – Operating Systems. It was proposed by Hewlett-Packard and is suitable for evaluation up to EAL 4.

Appendix A. Chosen Assurance Levels in Relevant Related Work

Assurance class	Assurance Family (V3.1)	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7		ST for PR/SM for IBM zEC12	Assurance Family (V2.3)	EAL6 (V2.3)	SKPP = ST Green Hills
Source		CC	CC	CC	CC	CC	CC	CC		0846b_pdf.pdf			skpp.pdf/st_vid10362-st.pdf
											ACM_AUT	2	2
											ACM_CAP	5	5
											ACM_SCP	3	3
											ADO_DEL_EXP	2	2
											ADO_IGS	1	1
Development	ADV_ARC		1	1	1	1	1	1	ADV_ARC	1	ADV_ARC_EXP		1
											ADV_CTD_EXP		1
	ADV_FSP	1	2	3	4	5	5	6	ADV_FSP	5	ADV_FSP_EXP	3	4
											ADV_HLD_EXP	4	4
	ADV_IMP				1	1	2	2	ADV_IMP	1	ADV_IMP_EXP	3	3
											ADV_INI_EXP		1
	ADV_INT					2	3	3	ADV_INT	2	ADV_INT_EXP	2	3
											ADV_LLD_EXP	2	2
											ADV_LTD_EXP		1
											ADV_RCR_EXP	2	3
	ADV_SPM						1	1			ADV_SPM_EXP	3	3
											AGD_ADM_EXP	1	1
	ADV_TDS		1	2	3	4	5	6	ADV_TDS	4			

Assurance class	Assurance Family (V3.1)	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7		ST for PR/SM for IBM zEC12	Assurance Family (V2.3)	EAL6 (V2.3)	SKPP = ST Green Hills
Guidance documents	AGD_OPE	1	1	1	1	1	1	1	AGD_OPE	1			
	AGD_PRE	1	1	1	1	1	1	1	AGD_PRE	1			
											AGD_USR	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5	ALC_CMC	4			
	ALC_CMS	1	2	3	4	5	5	5	ALC_CMS	5			
	ALC_DEL		1	1	1	1	1	1	ALC_DEL	1			
	ALC_DVS			1	1	1	2	2	ALC_DVS	1	ALC_DVS	2	2
	ALC_FLR								ALC_FLR	3	ALC_FLR		3
	ALC_LCD			1	1	1	1	2	ALC_LCD	1	ALC_LCD	2	2
	ALC_TAT				1	2	3	3	ALC_TAT	3	ALC_TAT	3	3
											AMA_AMP_EXP		1
											APT_PDF_EXP		1
											APT_PSP_EXP		1
											APT_PCT_EXP		1
											APT_PST_EXP		1
											APT_PVA_EXP		1
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					

Assurance class	Assurance Family (V3.1)	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7		ST for PR/SM for IBM zEC12	Assurance Family (V2.3)	EAL6 (V2.3)	SKPP = ST Green Hills
Tests	ATE_COV		1	2	2	2	3	3	ATE_COV	2	ATE_COV	3	3
	ATE_DPT			1	1	3	3	4	ATE_DPT	3	ATE_DPT	2	3
	ATE_FUN		1	1	1	1	2	2	ATE_FUN	2	ATE_FUN	2	2
	ATE_IND	1	2	2	2	2	2	3	ATE_IND	2	ATE_IND	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5	AVA_VAN	5			
											AVA_CCA_EXP	2	2
											AVA_MSU	3	3
											AVA_SOF	1	1
											AVA_VLA_EXP	4	4

Table 3: Chosen assurance levels in relevant related work

Appendix B. CC Developer Action Elements by EAL Level

Here is the list of CC developer action elements according to CC3.1 part 3, starting at EAL 5.

B.1. EAL 5

B.1.1. ALC_CMS.5: Development tools CM coverage

```
The developer shall provide a configuration list for the TOE.
```

B.1.2. ADV_FSP.5: Complete semi-formal functional specification with additional error information

```
The developer shall provide a functional specification.
The developer shall provide a tracing from the functional specification
to the SFRs.
```

B.1.3. ADV_INT.2: Well-structured internals

```
The developer shall design and implement the entire TSF such that it
has well-structured internals.
The developer shall provide an internals description and justification.
```

B.1.4. ADV_TDS..4: Semiformal modular design

```
The developer shall provide the design of the TOE.
The developer shall provide a mapping from the TSFI of the functional
specification to the lowest level of decomposition available in the TOE
design.
```

B.1.5. ALC_TAT.2: Compliance with implementation standards

```
The developer shall provide the documentation identifying each
development tool being used for the TOE.
The developer shall document and provide the selected implementation-
dependent options of each development tool.
The developer shall describe and provide the implementation standards
that are being applied by the developer.
```

B.1.6. ATE_DPT.3: Testing: modular design

```
The developer shall provide the analysis of the depth of testing.
```

B.1.7. AVA_VAN.4: Methodical vulnerability analysis

```
The developer shall provide the TOE for testing.
```

B.2. EAL 6

B.2.1. ALC_CMC.5: Advanced support

```
The developer shall provide the TOE and a reference for the TOE.
The developer shall provide the CM documentation.
The developer shall use a CM system.
```

B.2.2. ADV_IMP.2: Complete mapping of the implementation representation of the TSF

```
The developer shall make available the implementation representation
for the entire TSF.
The developer shall provide a mapping between the TOE design
description and the entire implementation representation.
```

B.2.3. ADV_INT.3: Minimally complex internals

```
The developer shall design and implement the entire TSF such that it
has well-structured internals.
The developer shall provide an internals description and justification.
```

B.2.4. ADV_SPM.1: Formal TOE security policy model

```
The developer shall provide a formal security policy model for
[assignment: the list of policies that are formally modeled].
For each policy covered by the formal security policy model, the model
shall identify the relevant portions of the statement ofv SFRs that
make up that policy.
The developer shall provide a formal proof of correspondence between
the model and any formal functional specification.
The developer shall provide a demonstration of correspondence between
the model and the functional specification.
```

B.2.5. ADV_TDS.5: Complete semiformal modular design

```
The developer shall provide the design of the TOE.
The developer shall provide a mapping from the TSFI of the functional
specification to the lowest level of decomposition available in the TOE
design.
```

B.2.6. ALC_DVS.2: Sufficiency of security measures

```
The developer shall produce and provide development security
documentation.
```

B.2.7. ALC_TAT.3: Compliance with implementation standards - all parts

The developer shall provide the documentation identifying each development tool being used for the TOE.
The developer shall document and provide the selected implementation-dependent options of each development tool.
The developer shall describe and provide the implementation standards that are being applied by the developer and by any third-party providers for all parts of the TOE.

B.2.8. ATE_COV.3: Rigorous analysis of coverage

The developer shall provide an analysis of the test coverage.

B.2.9. ATE_FUN.2: Ordered functional testing

The developer shall test the TSF and document the results.
The developer shall provide test documentation.

B.2.10. AVA_VAN.5: Advanced methodical vulnerability analysis

The developer shall provide the TOE for testing.

B.3. EAL 7

B.3.1. ADV_FSP.6: Complete semi-formal functional specification with additional formal specification

The developer shall provide a functional specification.
The developer shall provide a formal presentation of the functional specification of the TSF.
The developer shall provide a tracing from the functional specification to the SFRs.

B.3.2. ADV_TDS.6: Complete semiformal modular design with formal high-level design presentation

The developer shall provide the design of the TOE.
The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.
The developer shall provide a formal specification of the TSF subsystems.
The developer shall provide a proof of correspondence between the formal specifications of the TSF subsystems and of the functional specification.

B.3.3. ALC_LCD.2: Measurable life-cycle model

The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE, that is based on a measurable life-cycle model.
The developer shall provide life-cycle definition documentation.
The developer shall measure the TOE development using the measurable life-cycle model.
The developer shall provide life-cycle output documentation.

B.3.4. ATE_DPT.4: Testing: implementation representation

The developer shall provide the analysis of the depth of testing.

B.3.5. ATE_IND.3: Independent testing - complete

The developer shall provide the TOE for testing.

Appendix C. List of Abbreviations

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
CCMB	Common Criteria Management Board
CCRA	Common Criteria Recognition Agreement
SOG-IS	Senior Officials Group – Information Systems Security
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CI	Configuration Item
EAL	Evaluation Assurance Level
NLNCSA	Netherlands National ComSec Agency
JIWG	Joint International Working Group
SAR	Security Assurance Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
SFR	Security Functional Requirement
ST	Security Target

Appendix D. Bibliography

[AIS34] Application Notes and Interpretation of the Scheme (AIS), AIS34, v3, September 2009

[CC3.1] Common Criteria for Information Technology Security Evaluation. Version 3.1, revision 4, vol. 1--3, September, 2012, http://www.commoncriteriaportal.org/cc/.

[CCOPP-OS] COTS Compartmentalized Operations Protection Profile Operating Systems, v2.0, 2008

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012, Version 3.1, revision 4

[Fox ST] Fox Crypto, Fort Fox Hardware Data Diode: Security Target Common Criteria FFHDD - EAL7+, 2010, http://www.commoncriteriaportal.org/files/epfiles/Fox%2520DataDiode%2520Security%2520Target%2520EAL7%2520(v2.04).pdf.

[GH SW ST] Green Hills Software INTEGRITY-178B Separation Kernel Security Target, v1.0, Ref. IN-ICR750-0100-GH01ST, 2008

[GPOSPP] General-Purpose Operating System Protection Profile, v3.9, September 2012 draft

[PikeOS ST] Security Target for PikeOS, v0.24, June 2013

[OSPP] Operating System Protection Profile, 2010, v2.0, BSI-CC-PP-0067

[SKPP] U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness. No. Version 1.03, National Security Agency, June 2007.

[SOG-IS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, v3.0, January 2010 [Note 12] Note d'application, réf. 12.1, Modélisation formelle des politiques de sécurité d'une cible d'évaluation, March 2008

[Tenix ST] Tenix Datagate Inc, Interactive link data diode device: Common Criteria security target, no. 9126P01000001, August, 2005, http://www.commoncriteriaportal.org/files/epfiles/st_vid9512-st.pdf.

[WR MILS] Wind River VxWork MILS Platform, PO_VE_MILS_Platform.pdf, Rev 08/2010, www.windriver.com