Open Smart Card Infrastructure for Europe

v2

Volume 8:	**Security and Protection Profiles**
Part 5:	**Guidance for smart card evaluation (Common Criteria Supporting Document)**
Authors:	**eESC TB3 Protection Profiles, Security Certification**

Common Criteria

Warning

This document is a Common Criteria supporting document. It is not officially endorsed by all the Common Criteria Recognition Arrangement participants, but is endorsed by some certificate-producing participants that use it in a particular field of technology. The use of this supporting document is not mandatory. It can be used by any certification/validation body, evaluation facility and vendors.

Any comments about this document can be sent to the sponsor of the document.

See the CCRA Procedure for Supporting Documents

Document name : Guidance for Smartcard Evaluation

Reference : Version 1.1, March 2002

Object : Smartcards

Sponsor : DCSSI

Supporters : BSI, CESG, DCSSI, NLNCSA

Last update : March 2002

By : DCSSI

Table of Contents

1.   General purpose

1   This document defines smart card evaluation terminology and describes appropriate advice. Evaluation sponsors and developers of smartcard products are the intended audience.

2.   Field of special use

2   Smartcard evaluations.

3.   Smartcard product presentation and definitions

3.1   Glossary

3   The following definitions are used throughout the document. It is important that each term be clearly understood in order that guidance documentation for the evaluation process be put in context:

Integrated Circuit (IC)

4   Electronic component(s) designed to perform processing and/or memory functions (i.e. the hardware component containing the micro-controller and IC dedicated software).

5   A typical IC comprises: a processing unit, security components, I/O ports and volatile and non-volatile memories. It also includes any IC designer/manufacturer proprietary IC dedicated software, required for testing purposes. This IC dedicated software may be either IC embedded software (also known as IC firmware) or security-relevant parts of tests programs outside the IC. The IC may include any IC pre-personalization data.

6   Figure 1 below describes a typical IC and smartcard product hardware architecture:
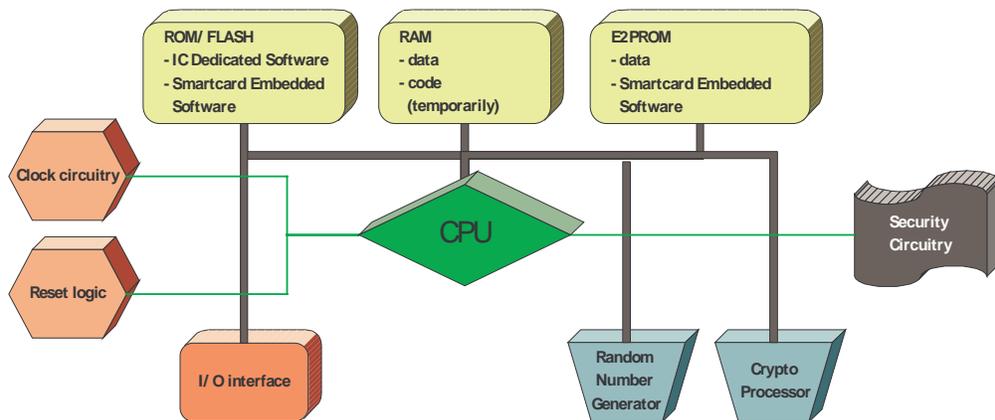

Figure 1 – Typical Smartcard IC

IC Dedicated Software

7   IC proprietary software embedded in a smartcard IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purposes (IC

Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated SW).

IC Dedicated Test Software

8   That part of the IC Dedicated Software (refer to above) which is used to test the device but which does not provide functionality during Phases 4 to 7. (Phases are described in figure 4)

IC Dedicated Support Software

9   That part of the IC Dedicated Software (refer to above) which provides functions in Phases 4 to 7. The usage of parts of the IC Dedicated Software might be restricted to certain phases.

Identification Data

10   Any data defined by the Integrated Circuit manufacturer and injected into the non-volatile memory by the Integrated Circuit manufacturer (Phase 3). These data are for instance used for traceability.

Basic Software (BS)

11   Smartcard embedded software in charge of generic functions of the Smartcard IC, such as an operating system, general routines and interpreters.

Application Software (AS)

12   Smartcard embedded software (may be in ROM or loaded onto a platform in EEPROM or Flash Memory) This is software dedicated to the applications.

Embedded Software (ES)

13   Software embedded in a smartcard IC but not developed by the IC Designer. This comprises embedded software in charge of generic functions of the Smartcard IC, such as an operating system, general routines and interpreters (Smartcard Basic Software -BS) and embedded software dedicated to applications (Smartcard Application Software - AS). The Smartcard Embedded Software is designed in Phase 1 and embedded into the Smartcard IC in Phase 3 or in later phases of the smartcard product life-cycle.

Smartcard Personalization

14   Final process under the responsibility of the card issuer, through which a smartcard is to be configured, security parameters loaded and secret keys set. At the end of the personalization process, the smartcard is irreversibly set into "user mode". Hence, it becomes fully operational and can be delivered to the end user.

IC Platform

15   Usually refers to a smartcard component which may undergo an evaluation process, as a complete Target of Evaluation (TOE) in itself, but which is not an end-user product (i.e. a smartcard component without any Application Software loaded).

IC Pre-personalization

16   Process performed at the IC manufacturer site, through which customer data can be loaded onto the IC, prior to the IC being irreversibly set into "issuer mode".

IC Pre-personalization data

17   Any data supplied by the software developer that is injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and/or to secure shipment between phases.

Smartcard product

18   A product corresponds to a fully operational smartcard, composed of both IC and complete ES, including application softwareas appropriate.

3.2   Architecture

19   The figures 2 and 3 below describe typical smartcard product architectures:

Closed architecture

20   All applications that are in the smartcard are known at the time of the evaluation.

ES including BS+AS	Application
	OS
	IC (Integrated Circuit)

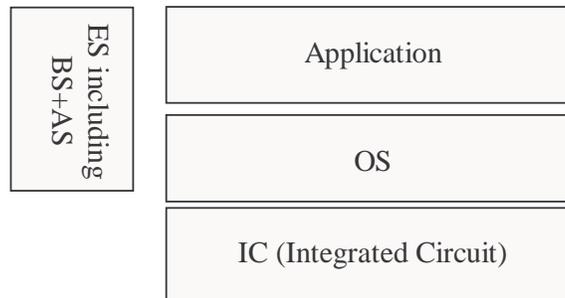**Figure 2 – Typical Smartcard architecture (Closed architecture)**

Open architecture

21   New applications could be accepted after the emission of the card.

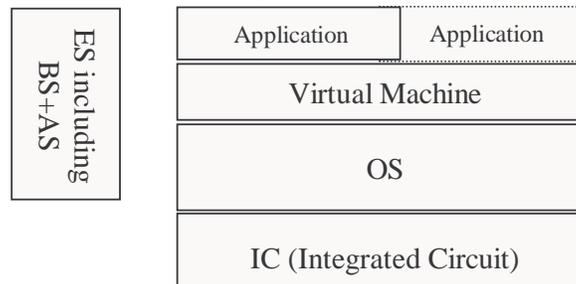| ES including BS+AS	Application	Application
	Virtual Machine	
	OS	
	IC (Integrated Circuit)	

Figure 3 – Typical Smartcard architecture (Open architecture)

3.3   Smartcard product life-cycle presentation

22   Figure 4 below describes the smartcard product life-cycle, which can be decomposed into 7 phases where the following authorities are involved:

Phase 1	Smartcard embedded software development	**the smartcard embedded software developer** is in charge of the smartcard embedded software development and the specification of IC pre-personalisation requirements,
Phase 2	IC development	**the IC designer** designs the IC, develops IC dedicated software, provides information, software or tools to the smartcard embedded software developer, and receives the smartcard embedded software from the developer, through trusted delivery and verification procedures. From the IC design, IC dedicated software and smartcard embedded software, he constructs the smartcard IC database, necessary for the IC photomask fabrication,
Phase 3	IC manufacturing and testing	**the IC manufacturer** is responsible for producing the IC through three main steps : IC manufacturing, IC testing, and IC pre-personalisation,
Phase 4	IC packaging and testing	**the IC packaging manufacturer** is responsible for the IC packaging and testing,
Phase 5	Smartcard product finishing process	**the smartcard product manufacturer** is responsible for the smartcard product finishing process and testing,
Phase 6	Smartcard personalisation	**the personaliser** is responsible for the smartcard personalisation and final tests. Other smartcard embedded software may be loaded onto the chip at the personalisation process,
Phase 7	Smartcard end-usage	**the smartcard issuer** is responsible for the smartcard product delivery to **the smartcard end-user**, and the end of life process.

Figure 4 – Smartcard product life-cycle and associated responsibilities

23   Note: Sometimes the IC manufacturer delivers modules ready for physical embedding into a plastic card. In this case, he is mostly in charge of Phase 4, i.e. IC packaging manufacturer's duty.

4.   Contributors roles in product evaluation

4.1   Roles clarification

24   Depending upon the exact TOE scope and targeted evaluation level, the following

entities may be involved in a smartcard evaluation process:

IC Manufacturer

25   Institution (or its agent) responsible for the IC manufacturing, testing, and pre-personalization.

ES Developer or AS Developer

26   Institution (or its agent) responsible for the smartcard Embedded Software . or Application Software development and the specification of IC pre-personalization requirements.

Card Manufacturer

27   The customer of the IC Manufacturer who receives the TOE during TOE Delivery. The Card Manufacturer includes all roles after TOE Delivery up to Phase 7. The Card Manufacturer has the following roles: (i) the Smartcard Product Manufacturer (Phase 5); (ii) the Personalizer (Phase 6). If the TOE is delivered after Phase 3 in the form of wafers or sawn wafers (dice) he also assumes the role of the IC Packaging Manufacturer (Phase 4). Usually, the Card Manufacturer is also the ES or AS developer.

Card Issuer

28   Customer for a product who is in charge of the issuance of the product to the smartcard holders (end users).

Sponsor (of the evaluation)

29   This is the body responsible for requesting and usually financing an evaluation: candidates might be the developer of the Target of Evaluation, the card issuer or even an independent customer of the product.

Evaluator

30   The evaluation laboratory that performs the evaluation work under a national scheme.

Certification body

31   An independent overseer that licenses national evaluation laboratories and issues the certificate based on the work of such laboratories.

4.2   Steps to be performed in order to get ready for an evaluation

32   The following steps need to be performed in order to prepare for an evaluation:

33   In order to provide the evaluator with the required deliverables, the sponsor and developer have to make sure:

- they have the appropriate skills and manpower,

- an adequate development methodology is used,

- an appropriate development environment has been set up.

34　Alternatively the developer could obtain training and/or assistance in the field of evaluation criteria. In this respect, evaluation consultancy might be elicited to assess a TOE's ability to meet its evaluation target (e.g. determine any evaluation deliverable shortfall or evaluation constraints).

35　The sponsor (possibly assisted by developer) has to make it clear that he knows precisely what he wants to be evaluated (IC, ES, platform, application software or any combination thereof).

36　The sponsor (possibly assisted by the developer) might choose to invoke an existing Protection Profile.

37　The sponsor (normally assisted by the developer) has to make available a Security Target which is precise and unambiguous, in order to ensure all relevant parties know exactly what is to be evaluated and against which requirements. Each party must approve the Security Target, thus reducing the risk of evaluation slippage.

38　The sponsor has to select an evaluation laboratory responsible for carrying out the evaluation. This is normally accomplished through an Invitation To Tender or direct contact with a specific evaluation laboratory. The price and evaluation time scales and any relevant non-disclosure agreements are factors to be negotiated. .

39　The sponsor has to make sure all parties are made aware of the role he plays in the evaluation process, particularly with regard to expected delivery date and content of evaluation deliverables.

40　With regard to the documentation needed for the evaluation, the objective is to reuse existing developmental documentation as much as possible. The shortfall between developer deliverables and CC requirements must be identified. Where a sponsor is new to evaluation, it is recommended that an evaluation laboratory be commissioned to perform a fit-for-purpose assessment of evaluation deliverables..

41　For an EAL3 evaluation, sponsor and developer have to be aware before the evaluation starts of site security requirements.

42　For a first of kind evaluation, it is recommended that a pre-evaluation review of sponsor deliverables and site security be performed.

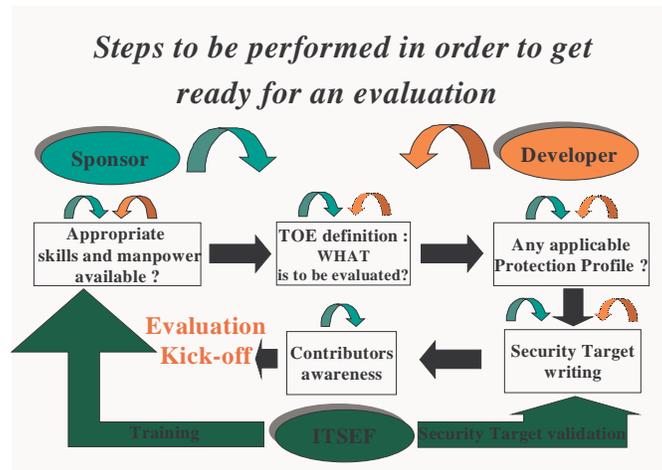43　Figure 5 below presents the above steps to be performed:

Figure 5 – Steps to be performed in order to get ready for an evaluation

4.3   Contributors involvement

44   The scope of evaluation concerns either an IC or an IC with embedded software.

45   The following contributions to the evaluation process are expected from each party:

IC manufacturer

46   The IC manufacturer is involved in the evaluation process in case the evaluation scope, includes the IC.

47   He provides the evaluation sponsor with the Security Target for the IC (for approval purposes), if requested to do so and provided it does not compromise IC proprietary content; otherwise, only part of the Security Target may be delivered to the evaluation sponsor (i.e. usually the first chapters of the Security Target without the Rationale).

48   In the event that an IC with ES evaluation be required, the global Security Target must be based on the IC Security Target, which is thus required to be delivered to the global Security Target writer (see concept of ST-lite).

49   He provides the evaluation laboratory with the entire Security Target for the IC (mandatory for an IC evaluation).

50   He provides the evaluation laboratory with every required evaluation deliverable according to the targeted evaluation level and evaluation scope, as defined in the Security Target (see the assurance requirements and assurance measures chapters of the Security Target).

ES developer or AS developer

51   The ES or AS developer is involved in the evaluation process, when the evaluation scope includes ES or AS.

52   He may be requested by the evaluation sponsor to write or assist him write the Security Target.

53   He provides the evaluation laboratory with every required evaluation deliverable according to the targeted evaluation level and evaluation scope, as defined in the Security Target (see the assurance requirements and assurance measures chapters of the Security Target),

54   He provides IC pre-personalization data.

Card Issuer

55   The card issuer is the customer for a product. He is in charge of the issuance of the product to the smartcard holders; as a minimum, he should be involved in the evaluation process and assumes responsibility for:

- Security Target approval,
- definition of the smartcard personalization data for the product,
- and authorship of the smartcard product guidance documentation.

Sponsor (of the evaluation)

56   The sponsor of the evaluation is involved in the evaluation process is responsible for: :

- writing and/or approving the Security Target (he can ask the developer to write the Security Target for him, but he has to approve its contents because it is the baseline for the whole evaluation process),

- mainly ensuring that every required evaluation deliverable be made available to the evaluator.

Evaluator

57   The evaluator analyses the evidence elements he is provided with throughout the evaluation process:

- He performs conformance and penetration testing on the TOE.

- He performs a site visit to the development premises.

- He performs a site visit to the production premises (for the evaluation including the IC).

- He writes and issues evaluation reports (including the final Evaluation Technical Report – ETR).

Certification body

58   The certification body (CB) is involved in any evaluation process running under its own scheme. It is responsible for:

- approving the evaluation scope as defined in the Security Target before the evaluation process is allowed to start,

- giving advice regarding the evaluation of cryptographic aspects,

- monitoring the evaluation work performed by the evaluation laboratory throughout the evaluation process (evaluation results and evaluation reports approval, attending evaluation meetings etc.),

- and finally, issuing a certificate and a certification report (assuming the evaluation process leads to an overall "Pass" verdict).

4.4 Detailed contributors inputs and evaluator tasks during the evaluation process

General evaluation inputs definition

59   With regard to the documentation needed for the evaluation, it is recommended to provide one "header" document for each task of a CC evaluation. For example, the "header" document could link internal documents with CC tasks. In some cases, more than one document is required like tasks ACM and ALC_DVS components where one set of documents per site is required.

60   For tutorial purposes, we need to illustrate the theory using evaluations from various operational contexts, these ones may not be endorsed by other issuers. According to different pilot and roll-out experiences in the field of bank services, some issuers have requested the following evaluation levels:

- EAL1+ (i.e. EAL1 augmented with AVA_VLA.2),

- EAL4+ (i.e. EAL4 augmented with ADV_IMP.2, ALC_DVS.2 and AVA_VLA.4).

61   The above mentioned evaluation levels EAL1+ and EAL4+ defined for smartcards are the result of a historical process and issuers risk analyses.

62   EAL1+ was defined in conjunction with the risk analysis of experiments and pilots in card-activated bank services, which can be terminated if anything goes wrong. The EAL1+ evaluation level is not strictly consistent with the Common Criteria but there is no assurance components for black-box testing in the version 2.1 of the CC. Therefore, AVA_VLA.2 without the normal dependencies is interpreted as black-box testing for smartcard evaluations.

63   EAL4+ was based on ITSEC level 3 high augmented with resistance to high attack potential.

EAL1+ evaluation : contributors input and evaluation tasks

Scope IC alone:

64   Usually, this security level is not used for an IC alone because on one hand the evaluation of the IC is done in *black box*.

65   Such certificates exist and an EAL1+ evaluation for an IC alone can be justified as follows:

- it allows the validation of the Security Target of the IC,

- it gives a first level of confidence in respect of IC security,

66   In such an evaluation, the IC manufacturer will provide the deliveries to the evaluation laboratory (for detailed deliveries see the list below).

Scope IC with ES:

ASE and EAL1+ Class	CC component	ES or AS Developer	Sponsor	Card Issuer	Evaluation lab	Certification Body
ASE	ASE_XXX.1		IC with ES Security Target		Task Report (TR)	TR approval
ACM : Configuration Management	ACM_CAP.1 Version numbers	ES identifier			Task Report (TR)	TR approval
ADO : Delivery and operation	ADO_IGS.1 Installation, generation, and start-up procedures	IC pre-personalization data and ATR description		Smartcard personalization data	Task Report (TR)	TR approval
ADV : Development	ADV_FSP.1 Informal functional specification	Informal functional specification			Task Report (TR)	TR approval
	ADV_RCR.1 Informal correspondence demonstration	Informal correspondence demonstration			Task Report (TR)	TR approval
AGD : Guidance documents	AGD_ADM.1 Administrator guidance			Administrator guidance	Task Report (TR)	TR approval
	AGD_USR.1 User guidance			User guidance (Card holder contract)	Task Report (TR)	TR approval
ATE : Tests	ATE_IND.1 Independent testing – conformance	IC with ES pieces + tools			Task Report (including conformance testing report)	TR approval

AVA : Vulnerability assessment	AVA_VLA.2 Independent vulnerability analysis	Vulnerability analysis + IC with ES pieces			Task Report (including penetration testing report) Final ETR	TR approval ETR approval

EAL4+ evaluation : Contributors inputs and evaluation tasks

<u>Scope IC alone:</u>

67 The only contributor involved in a hardware evaluation besides the evaluators and certification body, is the IC manufacturer.

68 As the IC certification purpose is to be reused in an IC with ES evaluation, some documents have to be produced for composite evaluation purposes (i.e. the ST-lite is issued from the full IC ST.).

<u>Scope IC with ES (IC being already certified):</u>

ASE and EAL4+ CC Class	CC component	IC manufacturer	ES or AS Developer	Sponsor	Card Issuer	Evaluation lab	Certification Body
ASE	ASE_XXX.1	IC Security Target Lite		IC with ES Security Target		Task Report (TR)	TR approval
ACM : Configuration Management	ACM_AUT.1 Partial CM automation		Configuration Management documentation			Task Report (TR)	TR approval
	ACM_CAP.4 Generation support and acceptance procedures	Masked IC Identifier	Configuration Management documentation			Task Report (TR)	TR approval
	ACM_SCP.2 Problem tracking CM coverage		Configuration Management documentation			Task Report (TR)	TR approval
ADO : Delivery and operation	ADO_DEL.2 Detection of modification		Delivery procedure description			Task Report (TR)	TR approval
	ADO_IGS.1 Installation, generation, and start-up procedures		IC pre-personalization data and ATR description		Smartcard personalization data	Task Report (TR)	TR approval
ADV : Development	ADV_FSP.2 Fully defined external interfaces		Functional specification			Task Report (TR)	TR approval
	ADV_HLD.2 Security enforcing high-level design		High-level design			Task Report (TR)	TR approval
	ADV_IMP.2 Implementation of the TSF	IC Security Guidance	Implementation of the TSF (source and object code)			Task Report (TR)	TR approval
	ADV_LLD.1 Descriptive low-level design		Descriptive low-level design			Task Report (TR)	TR approval
	ADV_RCR.1 Informal correspondence demonstration		Informal correspondence demonstration			Task Report (TR)	TR approval

	ADV_SPM.1 Informal TOE security policy model		Informal TOE security policy model			Task Report (TR)	TR approval
AGD : Guidance documents	AGD_ADM.1 Administrator guidance		Administrator guidance can be delegated to the developer		Administrator guidance	Task Report (TR)	TR approval
	AGD_USR.1 User guidance		User guidance can be delegated to the developer		User guidance (Card holder contract)	Task Report (TR)	TR approval
ALC Life cycle support	ALC_DVS.2 Sufficiency of security measures		Security measures description + justification analysis for their sufficiency	Security measures description + justification analysis for their sufficiency	Security measures description + justification analysis for their sufficiency	Task Report (TR)	TR approval
	ALC_LCD.1 Developer defined life-cycle model		Life-cycle model description			Task Report (TR)	TR approval
	ALC_TAT.1 Well-defined development tools		Development tools documentation			Task Report (TR)	TR approval
ATE : Tests	ATE_COV.2 Analysis of coverage		Analysis of coverage			Task Report (TR)	TR approval
	ATE_DPT.1 Testing : high-level design		Depth analysis			Task Report (TR))	TR approval
	ATE_FUN.1 Functional testing		Test plan, procedures and results.			Task Report (TR)	TR approval
	ATE_IND.2 Independent testing - sample		IC with ES pieces + Test resources			Task Report (including conformance testing report)	TR approval
AVA : Vulnerability assessment	AVA_MSU.2 Validation of analysis		Misuse analysis			Task Report (TR)	TR approval
	AVA_SOF.1 Strength of TOE security function evaluation		Strength of TOE security function analysis and cryptographic mechanisms implementation data, if appropriate			Task Report (TR)	TR approval
	AVA_VLA.4 Highly resistant	IC security mechanism description, deactivation & quotation	IC with ES vulnerability analysis + IC with ES pieces		Contribution to IC with ES vulnerability analysis (Operational Vulnerabilities)	Task Report (including penetration testing report) And final report (ETR)	TR approval ETR approval

69   For more details on the composition of an ES with an IC already certified, see the annex "Composite Smartcard Evaluation : recommended best-practice" of the "ETR-lite" document.

Annex A. Theoretical planning for an EAL4+ evaluation

A.1   Foreword

70   This annex gives a theoretical and optimal planning for an EAL4+ smartcard evaluation from the Evaluation laboratories point of view. For example, it could be an evaluation conformant to the Smartcard Integrated Circuit with Embedded Software Protection Profile. The duration presented here only represents the time spent by an evaluation laboratory to perform such an evaluation.

71   The time spent by the following tasks is not taken into account:

- The deliveries preparation by the developers;

- Meetings between evaluators, developers and certification body;

- The certification phases that occur if the evaluation is passed.

72   Nevertheless, despite the fact that the tasks above are not taken into account in the global duration of an evaluation, meetings can occur in parallel with evaluation tasks.

73   The evaluation tasks are sequenced as quickly as possible, according to the idealistic assumptions:

- The IC evaluation is not taken into account in this planning. The hypothesis is that the IC is certified and known by the evaluation laboratory.

- Parallelism is included:

    - this relies on the hypothesis that an infinite number of evaluators are available for the evaluation with a good knowledge of the product;

    - the developers provide deliveries on time without delay;

- Deliveries iterations are not taken into account. The hypothesis is that there is no critical issue that stops the progress of the evaluation. The consequence of an iteration in terms of duration is not easy to predict because it depends on the degree of errors and on the types of document. Moreover, the amount of work that has to be done by the developers for the corrections, the duration for a new delivery and the duration taken to re-evaluate these documents, has to be added to the global duration.

74   On a fact based experience, a **6 months evaluation** are **achievable** under the following conditions:

- Developers are trained to CC evaluation (reduced the number of iteration);

- The type of application is already known by the evaluators.

75   The following chapters give two figures to illustrate an example of planning. The first one shows a classical sequencing of tasks. Not just the CC dependencies are taken into account, but also the fact that the evaluator has to gain the knowledge of the product to go through evaluation. The second figure is a Gantt diagram.

76   In these figures, tasks in red are the critical tasks. A delay on this critical path results in a delay of the global evaluation.

A.2   Planning
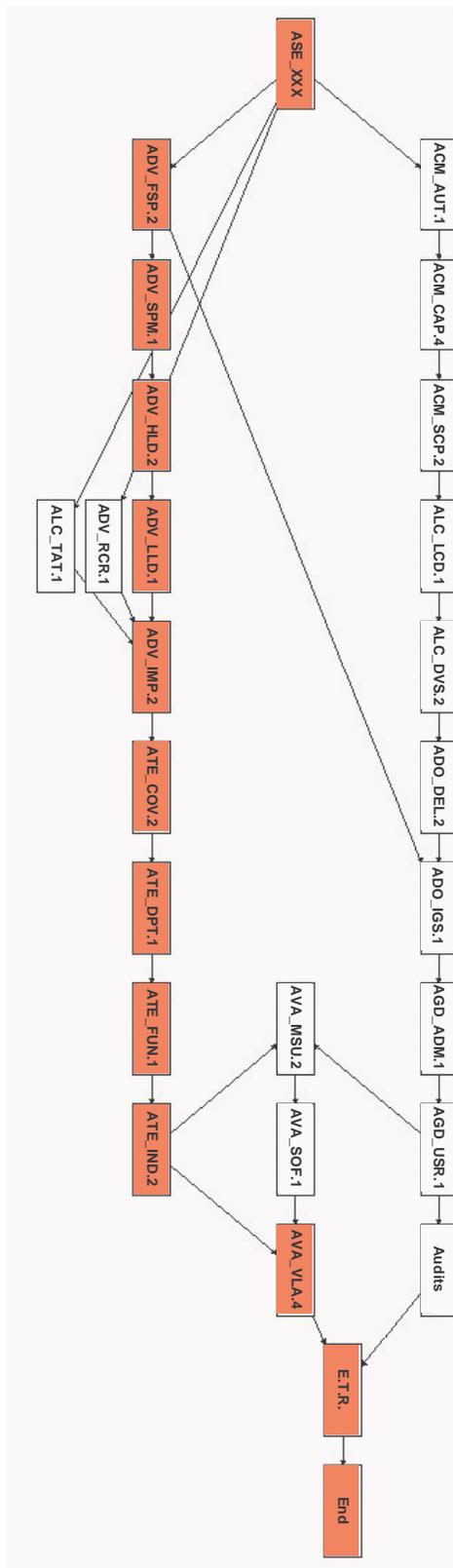
A.3 Gantt diagram
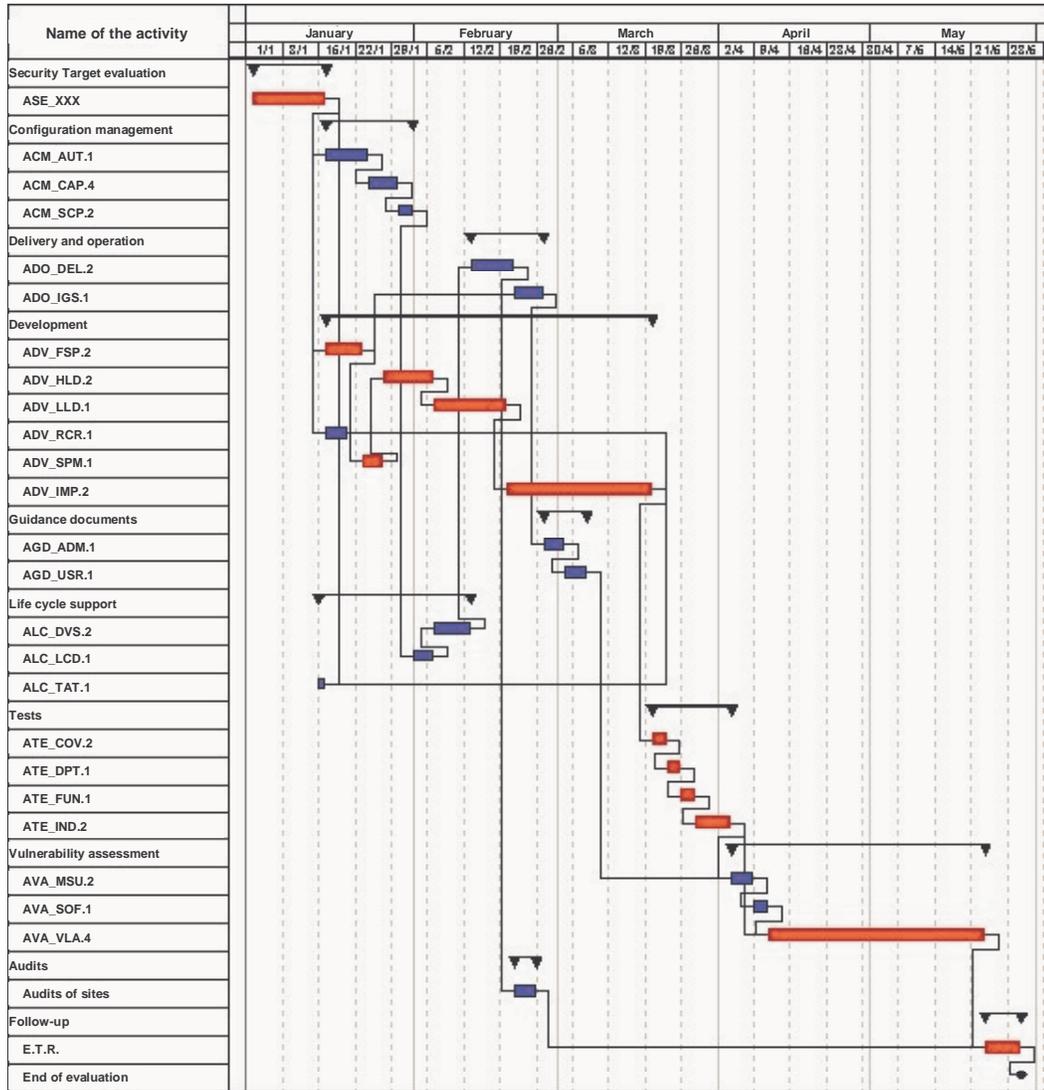
Annex B. Smartcard sub-processes

B.1 Introduction

77 The purpose of this annex is to identify the development sub-processes and to provide a CC oriented methodology for each sub-process in that evaluation may proceed as smoothly as possible.

78 In order to anticipate their development capability to comply to the requirements of CC product evaluations, the developers can set up and prepare the internal development methodology in order to achieve the best chance of success with little amount of work. This minimizes the duration of the product evaluation.

79 The TOEs taken into account to illustrate these definition are an Embedded or an Application Software.

80 The target evaluation level to illustrate this paper is EAL4 augmented with the components ALC_DVS.2, ADV_IMP.2, AVA_VLA.4.

B.2 Identification of sub-processes

81 Only the software development sub-processes for smartcard product developer and for application developer are detailed further. This could apply to "IC manufacturing process".

82 The identified sub-processes are the following:

- Development environment
- Security Target
- Guidance documentation
- Development/Test

83 The first sub-process can lead to an evaluation and certification that will be re-used in the smartcard product evaluation. For the three other sub-processes, the re-usability consists of preparing the development methodology through developers 'training and template documents' preparation.

B.3 Development environment sub-process

Sub-process definition

84 The following process relates to the generic methodology for the secure development of all products; a separate evaluation could be done in a maintenance mode. The following deliveries related to the assurance classes are described below:

Class	Component	Development environment Sub-process	Responsible
Configuration management ACM	Partial CM automation ACM_AUT.1	ACM_AUT.1	QA responsible
	Generation support and acceptance procedures ACM_CAP.4	ACM_CAP.4	QA responsible

	Problem tracking CM coverage ACM_SCP.2	ACM_SCP.2	QA responsible
Delivery and Operation ADO	Detection of modification ADO_DEL.2	ADO_DEL.2	Project responsible
	Installation, generation and start-up procedures ADO_IGS.1	(1)	
Life cycle support ALC	Sufficiency of security measures ALC_DVS.2	ALC_DVS.2	Security responsible
	Developer defined life-cycle model ALC_LCD.1	ALC_LCD. 1	QA responsible
	Well-defined development tools ALC_TAT.1	(1)	

(1) Those components cannot be described generically as the others because they are specific to the product type.

85 The roles of previous responsible are described in the following table:

Responsible	Role
Quality Assurance responsible	To define quality assurance procedures and verify the application of previous procedures.
Project responsible	To define delivery procedures and verify the application of previous procedures.
Security responsible	To define security procedures and verify the application of previous procedures.

86 In the development environment process, the product development follows a development life cycle model with the description of development/acceptance/maintenance general process and the mandatory documents as requirement specification, configuration management plan, functional requirement, high-level design, validation test plan, validation test specification, validation test result, anomaly list report.

87 In the development environment process, what is needed for the product development evaluation is used for all product development.

88 Note: development environment sub-process documentation could apply to card issuance, too.

Generic methodology

89 The generic methodology could be the following:

- Train the developer to the CC assurance components.

- Prepare a template document to ACM, ADO_DEL.2, ALC_DVS.2 and ALC_LCD.1 requirements and reference related documents as configuration management plan, configuration list, an acceptance plan, the delivery and security procedures.

- Complete each "reference" document according to the TOE specificities.

Development environment process evaluation

90   The possible target should be a system that could address the software development environment process for smartcard software.

91   The life cycle phase concerned is limited to software specification, implementation and testing with the delivery to IC manufacturer.

92   The possible objectives requested for a smartcard product development evaluation:

- To assure confidentiality, integrity and authorized access to the products, documentation and development tools (ALC_DVS.2, ALC_LCD.1),
- To assure only authorized modification of development procedures, tools and related documents (ALC_DVS.2, ALC_LCD.1, ACM),
- To track all the TOE representation evolutions (documentation, implementation, tests, tools) in a configuration management for the product development (ACM),
- To protect the deliveries against any modification or disclosure during the delivery process (ADO_DEL.2).

93   Note: the development environment process evaluation could replace the generic methodology steps 1 and 2.

Smartcard product evaluation based on development environment process evaluation

94   The smartcard product evaluation uses the development environment process evaluation results in order to answer to ACM, ADO_DEL.2, ALC_DVS.2 and ALC_LCD.1 security assurance requirements.

95   Some specific refinements of the components specific to the considered product will then have to be provided such as the configuration list.

96   The product evaluation could use, when available, the development environment process evaluation maintenance certificate in order to replace the audit.

B.4   Security target sub-process

Sub-process definition

97   The Security Target document is the basis of the evaluation. It is the representation of an identified TOE with set of security functions and assurance measures specifications to address an identified set of security requirements which themselves address an identified set of security objectives.

98   In order to apply the Security Target to the product range, the developer should produce a generic security target to optimize cost and time.

Class	Component	Security Target	Responsible

		Sub-process	
Security Target Evaluation ASE	TOE description ASE_DES.1	ASE_DES.1	Project responsible
	Security environment ASE_ENV.1	ASE_ENV.1	Project responsible
	ST introduction ASE_INT.1	ASE_INT.1	Project responsible
	Security objectives ASE_OBJ.1	ASE_OBJ.1	Project responsible
	PP claims ASE_PPC.1	ASE_PPC.1	Project responsible
	IT security requirements ASE_REQ.1		
	Explicitly stated IT security requirements ASE_SRE.1		
	TOE summary specification ASE_TSS.1		

99   The roles of previous responsible are described in the following table:

Responsible	**Role**
Project responsible	To define a set of security functions and assurance measures specifications to address an identified set of security requirements which themselves address an identified set of security objectives.

Generic methodology

100   The generic methodology could be the following:

- Train the developer to the CC introduction (CC Part 1), security functional requirements (CC Part 2), and the security assurance requirements (CC Part 3).
- Prepare a template document that answer to ASE_XXX.1 requirements.
- Complete each "reference" part according to the TOE specificity.

B.5   Guidance documentation sub-process

Sub-process definition

101   In order to ensure the development capability complies with the targeted evaluation assurance level, the developers should prepare, complete and maintain the related documents according to CC component requirements.

102   The reference document for all documents is the Security Target. Moreover, the

production of the TOE is necessary for the evaluation.

Class	Component	Guidance documentation Sub-process	Responsible
Delivery and Operation ADO	Detection of modification ADO_DEL.2		
	Installation, generation and start-up procedures ADO_IGS.1	ADO_IGS.1	Project responsible
Guidance documents AGD	Administrator guidance AGD_ADM.1	AGD_ADM.1	Documentation responsible or Card Issuer
	User guidance AGD_USR.1	AGD_USR.1	Documentation responsible or Card Issuer
Vulnerability assessment AVA	Validation of analysis AVA_MSU.2	AVA_MSU.2	Project responsible
	Strength of TOE security function evaluation AVA_SOF.1		
	Highly resistant AVA_VLA.4		

103   The roles of previous responsible are described in the following table:

Responsible	Role
Documentation responsible	To define documentation for administrator and user.
Project responsible	To analyze the misuse.

104   A generic methodology is necessary to prepare, complete and maintain the related documents. In order to reduce time and cost, it is very important to train developers in the generic methodology. Then, the reusable is applies to the product range.

105   Note: this guidance documentation sub-process could apply to card issuer, too.

Generic methodology

106   The generic methodology could be the following:

- Train the developer in the CC assurance components.
- Prepare a template document that answers AGD, and ADO_IGS.1 requirements and reference related documents as administrator/user guidance, and IGS processes. All these documents are dependent of ADV_FSP.2 requirements.

- Prepare the document that responds to AVA_MSU.2 requirements. All these documents are dependent on ADO_IGS, ADV_FSP, AGD, ATE_COV.2, and ATE_FUN.1 requirements.
- Complete each "reference" document according to the TOE specifics.

B.6   Development / Tests sub-process

Sub-process definition

107   In order to anticipate the development capability to comply with the targeting evaluation assurance level, the developers should prepare, complete and maintain the related documents according to CC component requirements.

108   The reference document for all documents is the Security Target. Moreover, the production of the TOE is necessary for the evaluation.

Class	Component	Development/Tests Sub-process	Responsible
Development ADV	Fully defined external interfaces : ADV_FSP.2	ADV_FSP.2	Developer
	Security enforcing high-level design : ADV_HLD.2	ADV_HLD.2	Developer
	Subset of the implementation of the TSF ADV_IMP.1	ADV_IMP.1	Developer
	Descriptive low-level design : ADV_LLD.1	ADV_LLD.1	Developer
	Informal correspondence demonstration ADV_RCR.1	ADV_RCR.1	Developer
	Informal TOE security policy model :ADV_SPM.1	ADV_SPM.1	Project responsible
Life cycle support ALC	Sufficiency of security measures : ALC_DVS.2		
	Developer defined life-cycle model : ALC_LCD.1		
	Well-defined development tools :ALC_TAT.1	ALC_TAT.1	Project responsible
Tests ATE	Analysis of coverage ATE_COV.2	ATE_COV.2	Qualifier
	Testing: High-level design ATE_DPT.1	ATE_DPT.1	Qualifier
	Functional testing ATE_FUN.1	ATE_FUN.1	Qualifier

	Independent testing – sample :ATE_IND.2		
Vulnerability assessment AVA	Validation of analysis AVA_MSU.2		
	Strength of TOE security function evaluation AVA_SOF.1	AVA_SOF.1	Security architect
	Highly resistant AVA_VLA.4	AVA_VLA.4	Security architect

109   The roles of previous responsible are described in the following table:

Responsible	Role
Developer	To develop the Embedded Software or the Application.
Project responsible	To define the security policy and development tools.
Qualifier	To test the Embedded Software or the Application.
Security architect	To analyze the strength of TOE security functions and the vulnerabilities.

110   A generic methodology is necessary to prepare, complete and maintain the related documents.

111   In order to reduce time and cost, it is very important to train developers to the generic methodology. Then, the re-usability can apply to the product range.

Generic methodology

112   The generic methodology could be the following:

- Train the developers to the CC assurance components.
- Prepare a template document that answer to ALC_TAT.1 requirements and reference related documents as development procedures, development tools etc.
- Prepare a template document that answer to ADV requirements and reference related documents as functional specification, high-level design etc.
- Prepare a template document that answer to ATE requirements and reference related documents as validation test plans, validation test specifications, validation test results. All these documents are dependent on ADV requirements.
- Prepare the document that responds to AVA_SOF.1 and AVA_VLA.4 requirements. All these documents are dependent on ADO, ADV, AGD, and ATE requirements.
- Complete each "reference" document according to the TOE specification.