PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2007/08

Card Usimera Protect: SLE88CFX4000P microcontroller embedding SIM, USIM and OTA applications on Java card open plate-form (version 2.1).

Paris, 30th of March 2007

Courtesy Translation

Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.
Certification does not, however, constitute a recommendation product from DCSSI (Central Directorate for Information Systems Security), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Any correspondence about this report has to be addressed to:

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Centre de certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP
France

certification.dcssi@sgdn.pm.gouv.fr

Certification report reference

DCSSI-2007/08

Product name

Card Usimera Protect: SLE88CFX4000P microcontroller embedding SIM, USIM and OTA applications on Java card open plate-form (version 2.1).

Product reference

Product reference: T1000230 Usimera Protect 128K crypto on Infineon
Code version: 2.1

Protection profile conformity

Java Card System Protection Profile Collection, V1.0b, Configuration Standard 2.2. Reference PP/0305

Evaluation criteria and version

Common Criteria version 2.2

Evaluation level

EAL 4 augmented

ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Developer(s)

Gemalto
6 rue de la verrerie,
92197 Meudon, France

Infineon Technologies AG
St.-Martin-Straße 76,
81609 München, Allemagne

Sponsor

Gemalto
6 rue de la verrerie, 92197 Meudon, France

Evaluation facility

Serma Technologies
30 avenue Gustave Eiffel, 33608 Pessac, France
Phone: +33 (0)5 57 26 08 75, email : e.francois@serma.com

Recognition arrangements

CCRA

SOG-IS

The product is recognised at EAL4 level.

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, and published in the "Journal Officiel de la République Française". This decree stipulates that:

- The central information system security department draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the principals desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures are available on the Internet site www.ssi.gouv.fr.

Content

1. The product

1.1. Presentation of the product

The evaluated product is the card "Usimera Protect", consisting of the SLE88CFX4000P / m8830 B17 microcontroller with its software library PSL v0.50.23, developed by Infineon Technologies AG, and embedding SIM, USIM and OTA applications on Java card open plate-form (version 2.1), developed by Gemalto.
The reference of the software embedded in flash memory is "T1000230 Usimera Protect 128K crypto on Infineon" in version 2.1.

Usimera Protect is a GSM 2G and UMTS 3G product, which is compliant with the Release 5 and Release 6 of ETSI Mobile Communication standards. Depending on the handset and network capabilities, it can be used as a USIM card, a SIM card, or both. This product can also support Java Card applets that need security like authentication based on DES/TDES mechanism.

1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operation environment.

This security target is compliant to "Java Card System Protection Profile Collection, V1.0b, Configuration Standard 2.2" protection profile (cf. [PP/JCS]).

1.2.1. Product identification

The configuration list [CONF] identifies the product's constituent elements.
The certified version of the product can be identified by the following elements:

- Product reference: T1000230 Usimera Protect 128K crypto on Infineon;
- Code version: v2.1;
- Microcontroller identifier: SLE88CFX4000P;
- Microcontroller design step: m8830 B17;
- Software library of the microcontroller: PSL v0.50.23.

These elements can be identified using the five last historical ATR (Answer To Reset) bytes: T9 to T11 (microcontroller identifier: D0 00 3E), and T12 to T13 (flash mask identifier: 01 7D).

1.2.2. Security services

The main security services of the product are described in its public security target (see [ST], chapter 6.1). They are provided by the operating system, the GSM and UMTS communication applications, and by the Java card platform.

1.2.3. Architecture

The product is a smartcard that consists of:

- The microcontroller "SLE88CFX4000P / m8830 B17" with its software cryptographic library;
- The GEOS operating system including UICC functionalities;
- The Card Manager and Open Platform functionalities;
- The Java Card platform including JCRE 2.2.1, JCVM 2.2.1 et JCAPI 2.2.1 ;
- The applications SIM, USIM and OTA.

The architecture of the product is summarised in the following picture:

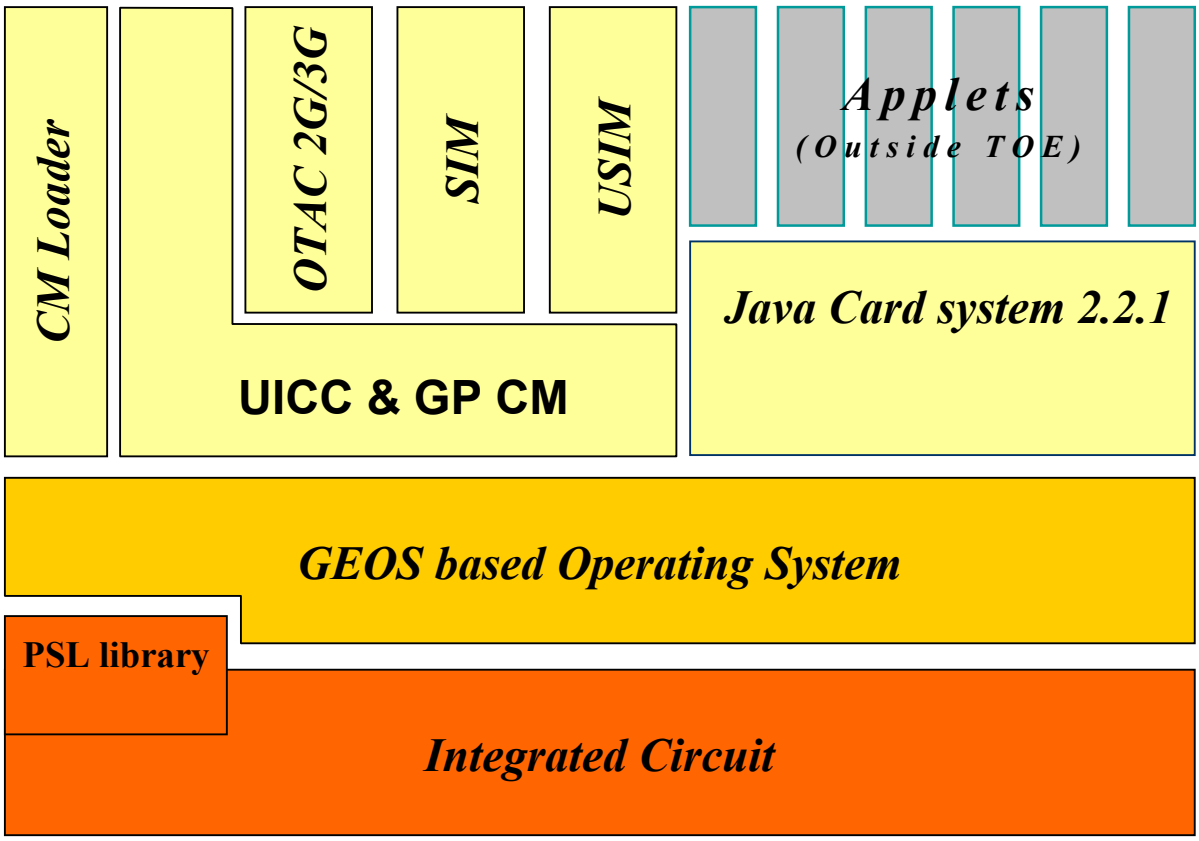

Figure 1 – Architecture of the product

1.2.4. Life cycle

The product's life cycle is organised as follow:

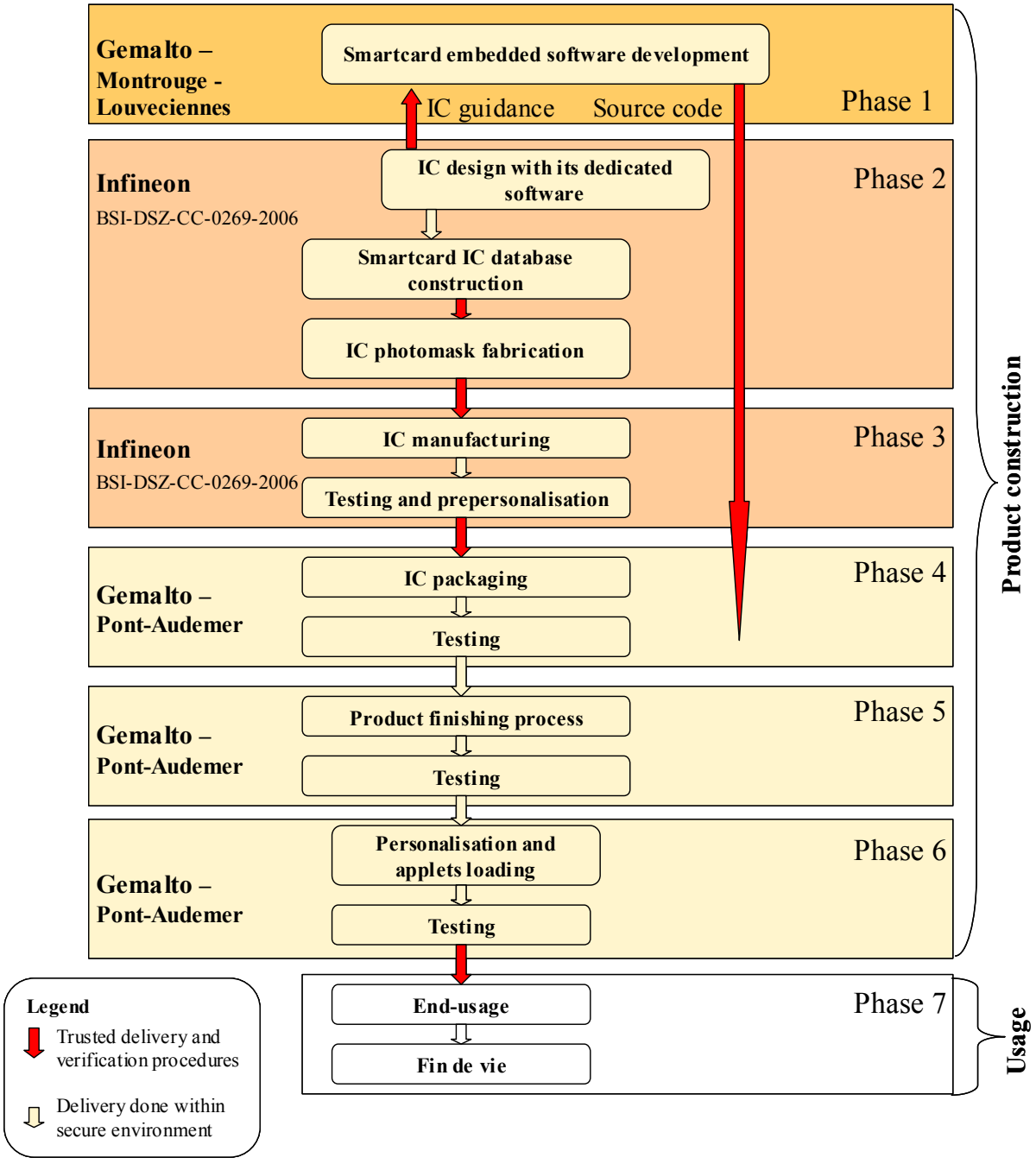

Figure 2 – Life cycle of the product

The embedded software was developed by Gemalto on both following sites:

Gemalto Montrouge

50 Av. Jean Jaurès,
92542 Montrouge Cedex,
France

Gemalto Louveciennes

36-38, rue de la princesse, BP 45
78431 Louveciennes Cedex
France

At the end of the project, Gemalto moved to the following development sites:

Gemalto Meudon

6 rue de la verrerie,
92197 Meudon,
France

The microcontroller and its cryptographic software library were developed by Infineon Technologies:

Infineon Technologies AG

CCM MTH, Postfach 80 09 49
D-81609 München,
Allemagne

The final smartcard is manufactured by Gemalto on the following site:

Gemalto Pont-Audemer

Rue George Clémenceau,
27500 Pont-Audemer,
France

1.2.5. Evaluated configuration

The certificate applies to the following functionalities:

- The microcontroller and the DES algorithm from its cryptographic software library;
- The GEOS Operating System;
- The authentication function for SIM and USIM applications;
- The Card Manager loader;
- The Java Card System.

With regard to the life cycle, the evaluated product is the one at the end of its manufacturing phase, meaning personalised in its usage phase, and with the GlobalPlatform services for applet loading available (phase 7).

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.2** [CC], and with the Common Evaluation Methodology [CEM].
For assurance components above EAL4 level, the evaluation facility own evaluation methods consistent with [AIS34] and validated by DCSSI have been used.

In order to meet the specificities of smart cards, the [CCIC] and [CCAP] guides have been applied.

2.2. Evaluation work

The evaluation has been performed according to the composition scheme as defined in the guide [COMP] in order to assess that no weakness is introduced from the integration of the software in the microcontroller already certified.
Therefore, the results of the evaluation of the microcontroller "SLE88CFX4000P" at EAL5 level augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4, compliant with the [PP0002] protection profile. This microcontroller has been certified the 23rd of March 2006 under the reference BSI-DSZ-CC-0269-2006. A maintained version of the product has been validated through assurance continuity process on the 28th of March 2007, under the reference BSI-DSZ-CC-0269-2006-MA-02.

The evaluation technical report [ETR], delivered to DCSSI the 28th of March 2007, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis

The robustness of cryptographic mechanisms has been analysed by DCSSI. The results are stated in the cryptographic analysis report [ANA-CRY] and have been taken into account in the evaluator vulnerability analysis.
The cryptographic analysis showed that key sizes of some of the algorithms don't reach the "standard" DCSSI level (see. [REF-CRY]). These limitations are due to the GSM specification and are not under the developer control. The resulting vulnerabilities are system relevant and are not specific to the product itself. This is particularly the case for the authentication service to 2G networks. On the other hand, the authentication service to 3G-network reaches the DCSSI "standard" level.

2.4. Random number generator analysis

The platform provides two random number generators (a hardware one and software one) that can be used by the applets developers.

This hardware generator has been evaluated according to AIS31 method in the scope of the microcontroller certification (see BSI-DSZ-CC-0269-2006). The evaluator has also performed its own additional analysis. This analysis did not show any flawed statistic bias for a direct use of the generated numbers. This does not imply that the generated numbers are really random but ensures that the generator is exempt of major conception flaws. As stated in the document [REF-CRY], DCSSI reminds that for a cryptographic use, the hardware-generated numbers shall be reprocessed by a cryptographic algorithm, even if the analysed random number generator did not show any weakness.

The software random generator consists in a software post-treatment of the random numbers issued from the hardware generator. This post-treatment doesn't fulfill DCSSI requirements for the "standard" level (see [REF-CRY]). For a a cryptographic use, the software generator shall be reprocessed by a cryptographic algorithm in order to reach the "standard" level.

3. Certification

3.1. Conclusion

The evaluation identified in chapter 2 and described in the evaluation technical report [ETR], was carried out according to the current rules and standards, with the required competency and impartiality by a licensed evaluation facility. All the work performed permits the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the product "Card Usimera Protect: SLE88CFX4000P microcontroller embedding SIM, USIM and OTA applications on Java card open plate-form (version 2.1)." submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 4 augmented.

3.2. Restrictions

This certificate only applies on the product specified in chapter 1.2 of this certification report.

The user of the certified product shall respect the operational environmental security objectives summarized specified in the security target [ST] and shall respect the recommendations in the guidance [GUIDES], in particular:

- For the mobile services:
  - The GSM/UMTS system operator shall apply a high level of confidentiality to administrative and GSM/UMTS keys, so they can be used to authenticate the roles;
- For the Java card:
  - No applet loaded post-issuance contains native methods;
  - Any byte-code must be verified prior to being loaded, in order to ensure that each bytecode is valid at execution time.
  - The applets developers should take into account the recommendation identified §2.4 of this report, and related to the usage of the random number generators.

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is issued in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:

3.3.2. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[2], of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:

1 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.
2 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, The Netherlands, New-Zealand, Norway, Singapore, Spain, Sweden, Turkey, United Kingdom and United States.

Annex 1. Evaluation level of the product

Class	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Name of the component
ACM Configuration management	ACM_AUT				1	1	2	2	1	Partial CM automation
	ACM_CAP	1	2	3	4	4	5	5	4	Configuration support and acceptance procedures
	ACM_SCP			1	2	3	3	3	2	Problem tracking CM coverage
ADO Delivery and operation	ADO_DEL		1	1	2	2	2	3	2	Detection of modification
	ADO_IGS	1	1	1	1	1	1	1	1	Installation, generation and start-up procedures
ADV Development	ADV_FSP	1	1	1	2	3	3	4	2	Fully defined external interfaces
	ADV_HLD		1	2	2	3	4	5	2	Security enforcing high-level design
	ADV_IMP				1	2	3	3	2	Implementation of the TSF
	ADV_INT					1	2	3		
	ADV_LLD				1	1	2	2	1	Descriptive low-level design
	ADV_RCR	1	1	1	1	2	2	3	1	Informal correspondence demonstration
	ADV_SPM				1	3	3	3	1	Informal TOE security policy model
AGD Guidance	AGD_ADM	1	1	1	1	1	1	1	1	Administrator guidance
	AGD_USR	1	1	1	1	1	1	1	1	User guidance
ALC Life-cycle support	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				1	2	2	3	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	Well-defined development tools
ATE Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	2	2	3	1	Testing: high-level design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing – sample
AVA Vulnerability assessment	AVA_CCA					1	2	2		
	AVA_MSU			1	2	2	3	3	3	Validation of analysis
	AVA_SOF		1	1	1	1	1	1	1	Strength of TOE security function evaluation
	AVA_VLA		1	1	2	3	4	4	4	Highly resistant

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation: - Usimera Protect - Security Target, Référence : D1019540 rev. 5.0, Gemalto For the needs of publication, the following security target has been provided and validated in the evaluation: - Usimera Protect Security Target – Public version, Référence : D1019540 rev. 5.0 Gemalto
[ETR]	Evaluation Technical Report - SIMEOS platform (EAL4+ evaluation), Référence : SIMEOS_ETR_V1.1 Serma Technologies
[ANA-CRY]	Cotation de mécanismes cryptographiques, Projet SIMEOS, Référence : N° 294/SGDN/DCSSI/SDS/Crypto du 12 février 2007
[CONF]	Simeos Configuration List, Référence : D1021043 v2.3 Gemalto
[GUIDES]	- Installation, Generation and Start-up - Pre-personalization Procedure, Référence : IGS_D1021046 v1.0, Gemalto - USimera Protect Volume 1 - User Guide, Référence : D1019543 revision 2.0, Gemalto - USimera Protect Volume 2 - Administrator Guide, Référence : D1019545 revision 2.0, gemalto - JCVM 2.2: User Manual Applets Development Guide, Référence : AGD_D1016741 revision 0.5, Gemalto
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certified by BSI under the reference BSI-PP-0002-2001.*
[PP/JCS]	Java Card System Protection Profile Collection, V1.0b, Configuration Standard 2.2. *Certified by DCSSI under the reference PP/0305.*

Annex 3. Certification references

Decree number 2002-535 dated 18th April 2002 related to the security evaluations and certifications for information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 - Certification of the security provided by IT products and systems, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[CCSUP]	Common Criteria Supporting Document – Rationale for Smart cards and similar devices, version 1.1, June 2006.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, version 2.0, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, version 2.1, April 2006.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - ETR-lite for composition, Version 1.3, April 2006.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[REF-CRY]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, version 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto.

[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004 Bundesamt für Sicherheit in der Informationstechnik
[AIS31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, Bundesamt für Sicherheit in der Informationstechnik