Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2007/19

Java Card System of Usimera Protect V1.0 card on SLE88CFX4000P

Paris, 17th September 2007,

Courtesy Translation

SÉCURITÉ CERTIFICATION

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-2007/19

Product name

Java Card System of Usimera Protect V1.0 card on SLE88CFX4000P

Card reference

T1000230 Usimera Protect 128K crypto on Infineon

Code version: : 2.1

Protection profile conformity

None

Evaluation criteria and version

Common Criteria version 2.3

compliant with ISO 15408:2005

Evaluation level

EAL 4 augmented

ADV_FSP.4, ADV_HLD.5, ADV_IMP.3, ADV_INT.3, ADV_LLD.2, ADV_RCR.3, ADV_SPM.3, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Developer(s)

Gemalto

6 rue de la verrerie, 92197 Meudon, France

Sponsor

Gemalto

6 rue de la verrerie, 92197 Meudon, France

Evaluation facility

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France
Tél : +33 (0)5 57 26 08 75, mél : 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 JavaCard System of the Usimera Protect V1.0 card developed by Gemalto; this card was already certified at EAL 4 level augmented of ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4 components (see chapter 2.2).

Usimera Protect V1.0 card 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 card can also support Java Card applets that need security like authentication based on DES/TDES mechanism.

1.2. Description of the evaluated product

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operation environment.
The security target is based on “Java Card System Protection Profile Collection, V1.0b, Configuration Standard 2.2” protection profile (cf. [PP/JCS]).

1.2.1. Identification of the card

The configuration list [CONF] identifies the Usimera Protect V1.0 card’s constituent elements, including its Java Card System.
The version of the Usimera Protect V1.0 card 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 of the product

The product provides the following security services:

- Management of transactions in the JCVM;
- Management of the values of the following security attributes: resident applets, active applets and currently selected applet, and check of the consistency of applets' life cycle;
- Applet isolation enforced by the JCRE firewall;
- Protection of the CAP files loaded;
- Restriction of the creation of JCRE entry point to the JCRE;
- Management of the behaviour of each Java Card application.

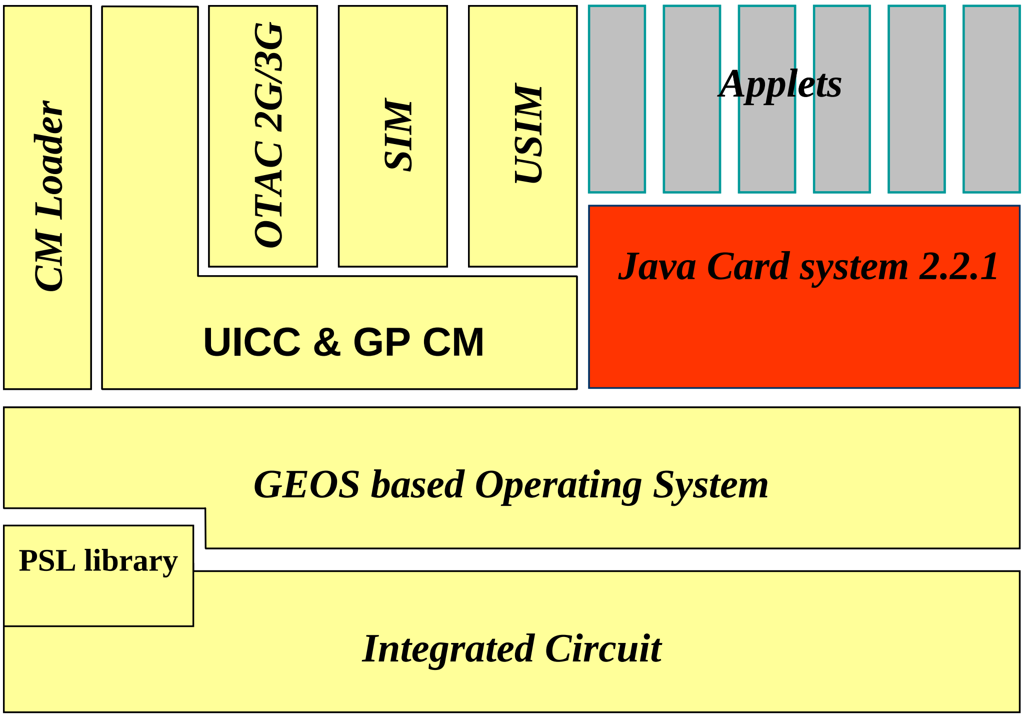
These services are detailed on chapter 6.1 of the public security target [ST].

1.2.3. Architecture

The Usimera Protect V1.0 card consists of:

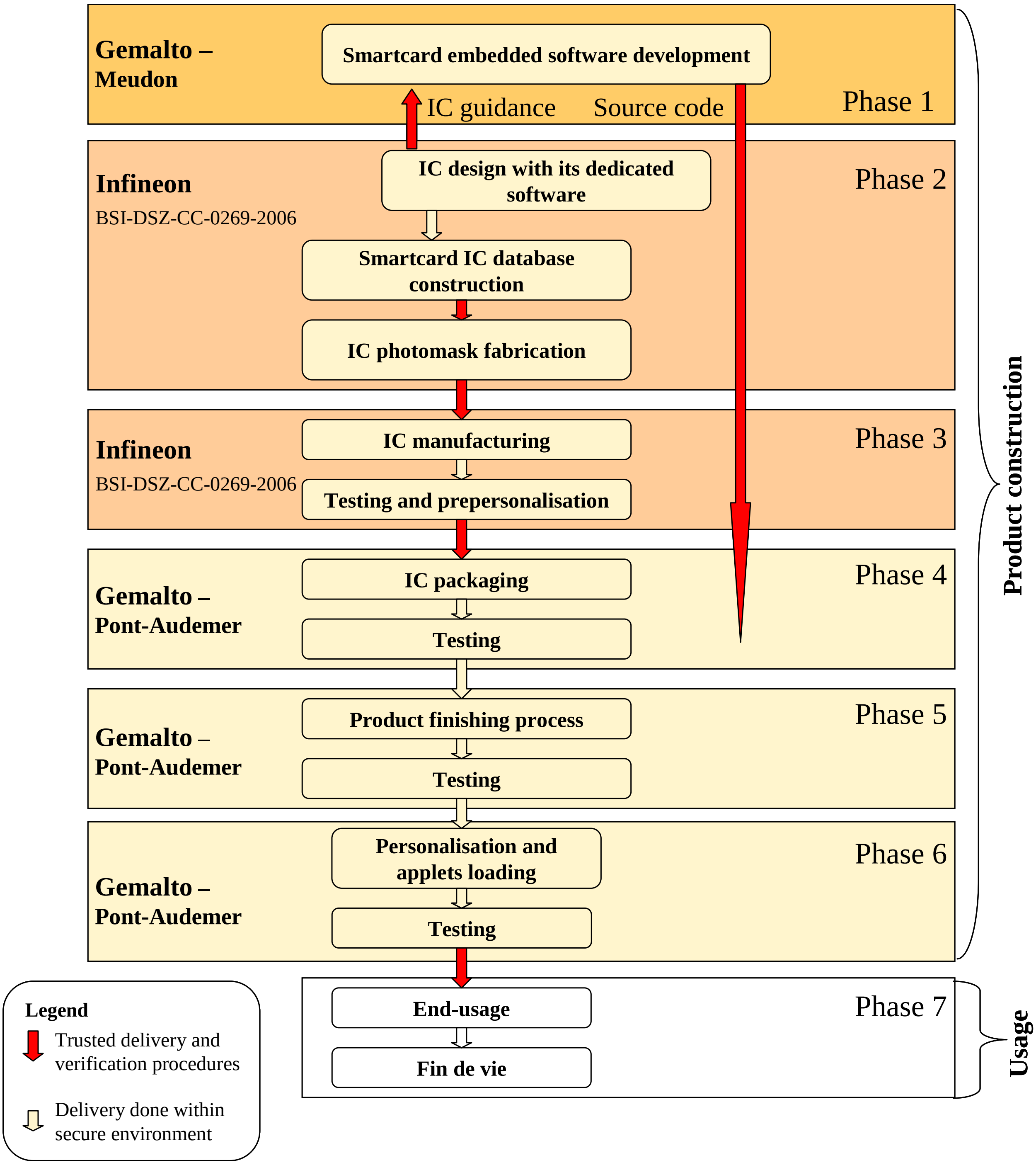
- The microcontroller “SLE88CFX4000P / m8830 B17” with its software cryptographic library;
- The GEOS operating system including UICC functionalities;
- The Card Manager and Open Platform functionalities;
- The Java Card platform including JCRE 2.2.1, JCVM 2.2.1 et JCAPI 2.2.1 ;
- The applications SIM,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

The architecture of this card is summarised in the following picture (evaluated product in red):



1.2.4. Life cycle

The Usimera Protect V1.0 card's life cycle is organised as follow:



The software embedded on the Usimera Protect V1.0 card was developed by Gemalto on the following site:

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 only applies to the Java Card System functionalities of Usimera Protect V1.0 card.

With regard to the life cycle, the evaluated product is included in the card at the end of its manufacturing phase, meaning personalised in its usage phase, and with the 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 2.3** [CC], with the Common Evaluation Methodology [CEM].
For assurance components above EAL4 level, the evaluation facility own evaluation methods, validated by DCSSI, have been used.

2.2. Evaluation work

The evaluation relies on the evaluation results of the “Usimera Protect Card: SLE88CFX4000P microcontroller embedding SIM, USIM and OTA applications on Java card open plateform (version 2.1)” product certified the 30th march 2007 under the reference 2007/08 [2007_08].

This evaluation was a new evaluation of the already certified product against the higher CC requirements of the ADV class: the ADV components used here are those of the EAL7 level, which require formal methods. Most of the former evaluation results of the others assurance requirements had been reused. It is the case for the vulnerability analysis, which was thus realised on the complete Usimera Protect V1.0 card.

The evaluation technical report [ETR], delivered to DCSSI the 6th September 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 during the former evaluation (see [2007_08]). The results are stated in the cryptographic analysis report [ANA-CRY] and have been taken into account in the evaluator vulnerability analysis.

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 Java Card System, included in the Usimera Protect V1.0 card on SLE88CFX4000P, 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:

- During phases 1 to 6, procedures shall be used suitably to maintain the integrity and confidentiality of the assets of the TOE (OE.DEVELOPMENT),
- No applet loaded post-issuance contains native methods (OE.APPLET),
- Any byte-code must be verified prior to being loaded and installed before the execution in order to ensure that each bytecode is valid at execution time (OE.VERIFICATION),
- Any pre-issuance native application on the card shall be conformant with the TOE so as to ensure that security policies and objectives described in [ST] are not violated (OE.NATIVE.2),
- If there is a loss of power, or if the smart card is withdrawn from the card reader while an operation is in progress, the platform (SCP) must allow the TOE to eventually complete the interrupted operation successfully, or recover to a consistent and secure state (OE.SCP.RECOVERY),
- The SCP shall provide functionalities that support the well-functioning of the TSFs of the TOE (avoiding they are bypassed or altered) and by controlling the access to information proper of the TSFs. In addition, the smart card platform should also provide basic services, which are required by the runtime environment to implement security mechanisms such as atomic transactions, management of persistent and transient objects and cryptographic functions (OE.SCP.SUPPORT),
- The SCP shall possess IC security features (OE.SCP.IC),
- The card manager shall control the access to card-management functions such as the installation (except the linking), update or deletion of applets. It shall also implement the card issuer's policy on the card (OE.CARD-MANAGEMENT),
- The IT environment must ensure continued correct operation of its security functions (OE.OPERATE),
- The IT environment (Card Manager) controls the availability of resources for the applications (OE.RESOURCES),

- The IT environment (Card Manager) shall ensure that the re-allocation of a memory block for the runtime areas of the JCVM does not disclose any information that was previously stored in that block (OE.REALLOCATION),
- The only means that the IT environment shall provide for an application to execute native code is the invocation of a method of the standards or proprietary Java Card API (OE.NATIVE),
- The Card Manager shall ensure that any data container that is shared by all applications (like the input/output buffer or a public global variable of the API) is always cleaned after the execution of an application (OE.SHRD_VAR_CONFID),
- The SCP (the Crypto APIs) shall provide means to cipher sensitive data for applications in a secure way (OE.CIPHER),
- The SCP (the Crypto APIs) shall provide means to securely manage cryptographic keys (OE.KEY-MNGT),
- The IT environment shall provide means to securely manage PIN objects (OE.PIN-MNGT),
- The IT environment shall provide means to restrict remote access from the CAD to the services implemented by the applets on the card (OE.REMOTE),
- The card manager shall ensure that the loading of a package into the card is safe (OE.LOAD),
- The Deletion Manager shall ensure that both applet and package deletion are safe (OE.DELETION),
- The IT environment (Deletion Manager) TOE shall ensure the object deletion shall not break references to objects (OE.OBJ-DELETION).

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:

[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.

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[1], 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 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	4	Formal functional specification
	ADV_HLD		1	2	2	3	4	5	5	Formal high-level design
	ADV_IMP				1	2	3	3	3	Structured implementation of the TSF
	ADV_INT					1	2	3	3	Minimisation of complexity
	ADV_LLD				1	1	2	2	2	Semiformal low-level design
	ADV_RCR	1	1	1	1	2	2	3	3	Formal correspondence demonstration
	ADV_SPM				1	3	3	3	3	Formal 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: - Formal Assurance on the JavaCard Virtual Machine embedded in Usimera Protect - Security Target, ref. D1031392, rev. 1.3, September 2007 For the needs of publication, the following security target has been provided and validated in the evaluation: - Formal Assurance on the JavaCard Virtual Machine embedded in Usimera Protect - Security Target – Public Version, ref. D1031392, rev. 1.3, September 2007
[ETR]	Evaluation technical report : - SIMEOS EXTENDED project Evaluation Technical Report, reference SIMEOSEXT_ETR_V1.1.fm, version 1.1, 21/08/07 (delivered the 06/09/07)
[CONF]	Simeos Configuration List, ref. D1021043, version 3.3, July 2007
[GUIDES]	- Installation, Generation and Start-up - Pre-personalization Procedure, ref. IGS_D1021046, revision 1.0 - USimera Protect Volume 1 - User Guide, ref. D1019543, rev. 2.0 - USimera Protect Volume 2 - Administrator Guide, ref. D1019545, rev. 2.0 - JCVM 2.2: User Manual Applets Development Guide, ref.: AGD_D1016741, rev. 0.5
[PP/JCS]	Java Card System Protection Profile Collection, V1.0b, Configuration Standard 2.2. *Certified by DCSSI under the reference PP/0305.*
[2007_08]	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), 30th march 2007, SGDN/DCSSI
[ANA-CRY]	Cotation de mécanismes cryptographiques, Projet SIMEOS, Référence : N° 294/SGDN/DCSSI/SDS/Crypto du 12 février 2007

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, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. The content of Common Criteria version 2.3 is identical to the international ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. The content of CEM version 2.3 is identical to the international ISO/IEC 18045:2005.
[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.