



PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report 2007/02

**IDOneClassIC Card : ID-One Cosmo 64 RSA
v5.4 and applet IDOneClassIC v1.0 embedded
on P5CT072VOP**

Paris, 29 January 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

Reproduction of this document without any change or cut is authorised.

<i>Certification report reference</i>
2007/02
<i>Product name</i>
IDOneClassIC Card : ID-One Cosmo 64 RSA v5.4 and applet IDOneClassIC v1.0 embedded on P5CT072VOP
<i>Product reference</i>
Embedded applet reference : IDOneClassIC, Version 1.0 Microcontroller references : P5CT072VOP, ROM mask P5CT072EWE1/T0PB6311
<i>Protection profile conformity</i>
PP SSCD type 2 [PP0005] and PP SSCD type 3 [PP0006]
<i>Evaluation criteria and version</i>
Common Criteria version 2.3 (compliant with ISO 15408:2005)
<i>Evaluation level</i>
EAL 4 augmented ADV_IMP.2, AVA_MSU.3, AVA_VLA.4
<i>Developers</i>
Oberthur Card Systems Philips Semiconductors GmbH 71-73 rue des Hautes Pâtures, Business Line Identification 92726 Nanterre Cedex, France PP Box 54 02 40 D-22502 Hamburg, Germany
<i>Sponsor</i>
Oberthur Card Systems 71-73 rue des Hautes Pâtures, 92726 Nanterre Cedex, France
<i>Evaluation facility</i>
Serma Technologies 30 avenue Gustave Eiffel, 33608 Pessac, France Phone: +33 (0)5 57 26 08 64, email : m.dus@serma.com
<i>Recognition arrangements</i>
  The product is recognised at EAL4 level. Recognition does not apply to the ADV_IMP.2, AVA_MSU.3 and AVA_VLA.4 components.

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	6
1.1. PRESENTATION OF THE PRODUCT.....	6
1.2. EVALUATED PRODUCT DESCRIPTION	6
1.2.1. <i>Product identification</i>	6
1.2.2. <i>Security services</i>	6
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Life cycle</i>	8
1.2.5. <i>Evaluated configuration</i>	9
2. THE EVALUATION.....	10
2.1. EVALUATION REFERENTIAL	10
2.2. EVALUATION WORK	10
2.3. CRYPTOGRAPHIC MECHANISMS ROBUSTNESS ANALYSIS.....	10
3. CERTIFICATION.....	11
3.1. CONCLUSION	11
3.2. RESTRICTIONS	11
3.3. RECOGNITION OF THE CERTIFICATE	11
3.3.1. <i>European recognition (SOG-IS)</i>	11
3.3.2. <i>International common criteria recognition (CCRA)</i>	12
ANNEX 1. EVALUATION LEVEL OF THE PRODUCT.....	13
ANNEX 2. EVALUATED PRODUCT REFERENCES	14
ANNEX 3. CERTIFICATION REFERENCES	15

1. The product

1.1. Presentation of the product

The evaluated product is « IDOneClassIC Card : ID-One Cosmo 64 RSA v5.4 and applet IDOneClassIC v1.0 embedded on P5CT072VOP », developed by Oberthur Card Systems and Philips Semiconductors GmbH.

This product is a Secure Signature Creation Device (SSCD) defined by:

- the underlying Integrated Circuit ;
- the Operating System embedding the Java Virtual Machine (JVM) ;
- the SSCD Application.

1.2. Evaluated product description

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

The security target is compliant with [PP005] and [PP006] (SSCD type 2 and type 3).

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:

- microcontroller identifier, « Philips T023P », written on the top layer of the product and visible with a microscope ;
- ROM code identifier, « 0B6 », written on the top layer of the product and visible with a microscope ;
- applet identifier (AID), « A0 00 00 00 77 01 00 00 07 10 00 01 00 00 04 », entered for the applet loading.

1.2.2. Security services

The product mainly includes the following components :

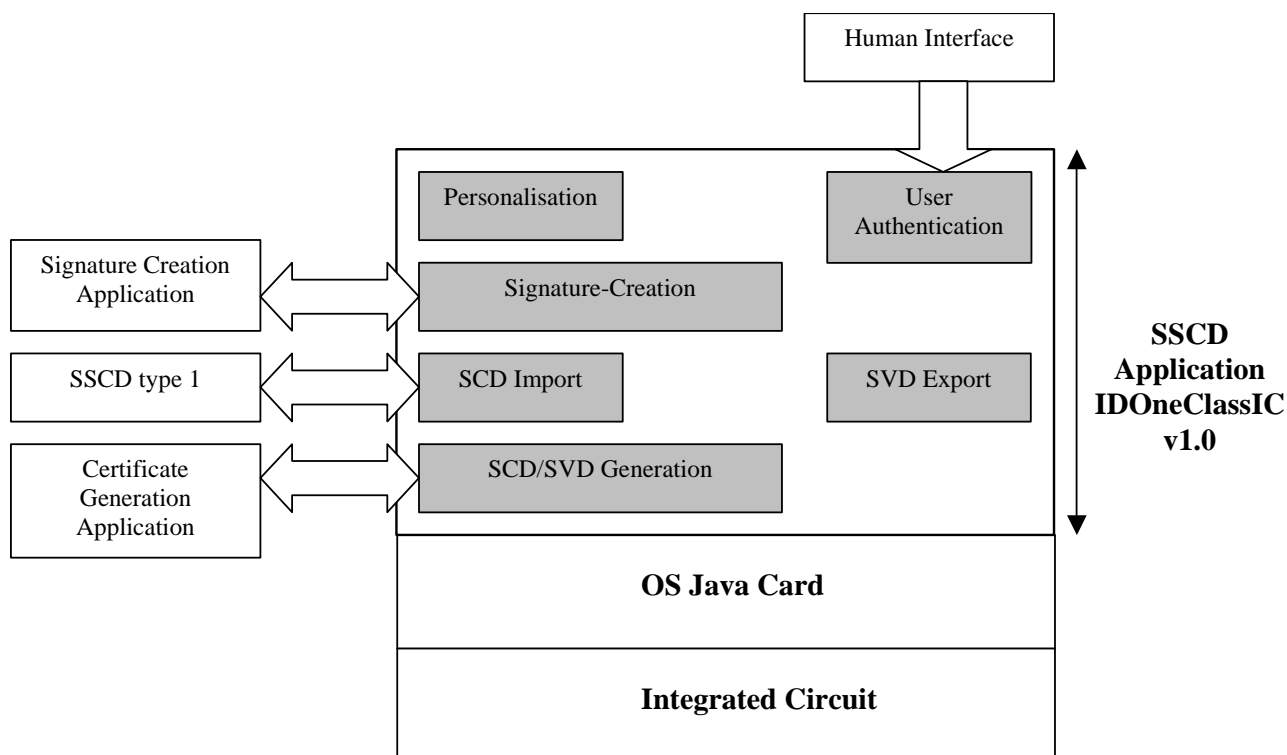
- the Platform, based on JavaCard and GlobalPlatform technologies, which provides mainly the following security services :
 - o interface between the Integrated Circuit and the IDOneClassIC applet ;
 - o basic services to provide to IDOneClassIC applet access to memories and all needed cryptographic operations ;
 - o global management of the card (loading, installation and deletion of applets) and monitoring of the security of the card (data integrity and physical attacks counter-measures) ;
 - o blocking of the loading mechanism after the IDOneClassIC loading (therefore no loading can be initiated after IDOneClassIC loading).

- the IDOneClassIC Applet which mainly provides the following security services:
 - o generation of private and public RSA signing keys (SCD: signature creation data and SVD: signature verification data) ;
 - o import of private RSA signing key (SCD) ;
 - o export of public RSA signing key (SVD) ;
 - o signature creation ;
 - o pin authentication of the signatory.

1.2.3. Architecture

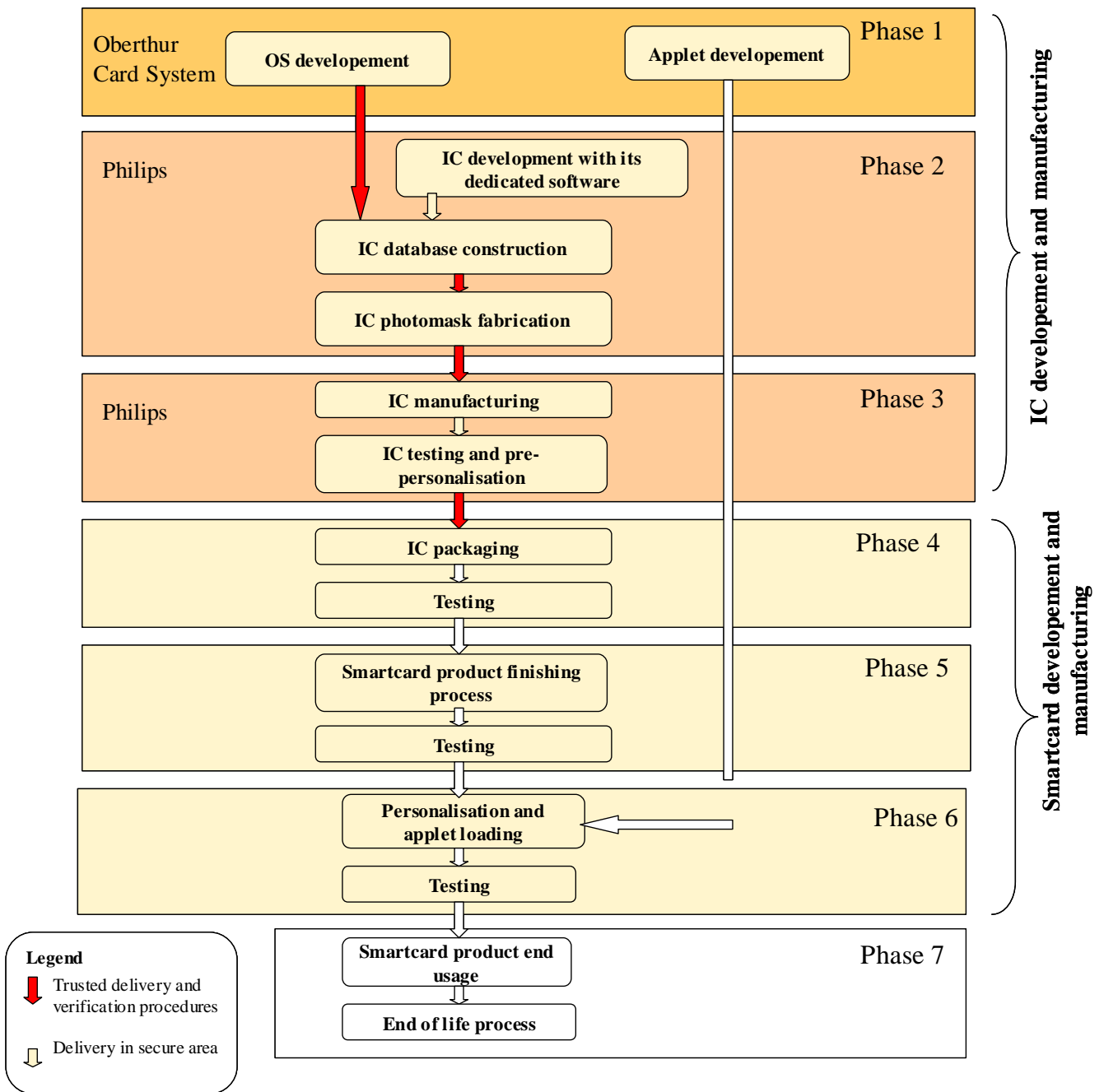
The product is composed of :

- the microcontroller P5CT072VOP developed and produced by Philips Semiconductors GmbH ;
- the JavaCard Operating System, developed by Oberthur Card Systems, which is composed of :
 - o the platform ID-One Cosmo 64 RSA v5.4 (GOP ID MX 64), embedded on the ROM's microcontroller (BIOS/VM label : build33, Platform label : Platform RefV87, Resident application label : GOP64_20051014) ;
 - o the optional code RSA SFM embedded on the EEPROM's microcontroller (version r1.0, label Liv20060310) ;
- the SSCD Application IDOneClassIC developed by Oberthur Card Systems which is loaded on the personalisation phase (IDOneClassIC v1.0).



1.2.4. Life cycle

The product's life cycle is organised as follow :



The product has been developed on the following site :

Oberthur Card Systems
 71-73, rue des Hautes Pâtures,
 92726 Nanterre Cedex,
 France

The microcontroller, certified by BSI, is developed and manufactured by Philips Semiconductors GmbH.

In the evaluation context, the product personaliser have been considered as “product administrator” and the terminal on which the signatory uses the card have been considered as “product user”.

1.2.5. Evaluated configuration

The product evaluated is the microcontroller with the embedded software identified §1.1.

The certificate applies to the “closed” configurations of the product (blocking of the applet loading mechanism after the IDOneClassIC loading).

The product tested by the evaluation facility is typical to final product.

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 consistent with [AIS34], 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 P5CTT072VOP 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 28th March 2006 under the reference BSI-DSZ-CC-0348-2006.

The evaluation relies on the evaluation results of the CNS Card product, certified the 15th September 2006 under the reference 2006/13 [2006_13].

The evaluation technical report [ETR], delivered to DCSSI the 24th January 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 not been analysed by DCSSI.

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 “IDOneClassIC Card : ID-One Cosmo 64 RSA v5.4 and applet IDOneClassIC v1.0 embedded on P5CT072VOP” 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:

- correspondence between public signing key –SVD- and private signing key –SCD- (OE.SCD_SVD_Corresp) ;
- secure transfer of private signing key –SCD- between SSCD (OE.SCD_Transfer) ;
- uniqueness of the signature-creation data (OE.SCD_Unique) ;
- generation of qualified certificates (OE.CGA_Qcert) ;
- CGA verifies the authenticity of the SVD (OE.SVD_Auth_CGA) ;
- protection of the verification authentication data –VAD- (OE.HI_VAD) ;
- data intended to be signed (OE.SCA_Data_Intend).

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 agreement¹, 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 countries², 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 2+	Name of the component
ACM Gestion de configuration	ACM_AUT				1	1	2	2		
	ACM_CAP	1	2	3	4	4	5	5	2	Configuration items
	ACM_SCP			1	2	3	3	3		
ADO Livraison et opération	ADO_DEL		1	1	2	2	2	3	1	Delivery procedures
	ADO_IGS	1	1	1	1	1	1	1	1	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	1	1	1	2	3	3	4	1	Informal functional specification
	ADV_HLD		1	2	2	3	4	5	2	Security enforcing high-level design
	ADV_IMP				1	2	3	3	1*	Subset of the 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		
AGD Guides d'utilisation	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 Support au cycle de vie	ALC_DVS			1	1	1	2	2	1	Identification of security measures
	ALC_FLR								3	Systematic Flow remediation
	ALC_LCD				1	2	2	3		
	ALC_TAT				1	2	3	3	1*	Well-defined development tools
ATE Tests	ATE_COV		1	2	2	2	3	3	1	Evidence coverage
	ATE_DPT			1	1	2	2	3		
	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 Estimation des vulnérabilités	AVA_CCA					1	2	2		
	AVA_MSU			1	2	2	3	3	1	Examination of guidance
	AVA_SOF		1	1	1	1	1	1	1	Strength of TOE security function evaluation
	AVA_VLA		1	1	2	3	4	4	2	Independent vulnerability analysis

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation: <ul style="list-style-type: none">- IDOneClassIC CARD Security Target, ref. FQR: 110 3517, edition 4, 16/01/07 For the needs of publication, the following security target has been provided and validated in the evaluation: <ul style="list-style-type: none">- IDOneClassIC CARD Public Security Target, ref. 110 36 45, version 1.0, 16/01/07
[ETR]	ANTERAK project: Evaluation Technical Report, ref. ANTERAK_ETR_V1.2, version 1.2, 24/01/07
[CONF]	ANTERAK Configuration List, ref. FQR : 110 3580, édition 2, 16/01/07
[GUIDES]	Installation, administration and user guidance: <ul style="list-style-type: none">- IDOneClassIC Guidance, ref. FQR : 110 3558, édition: 1 du 20/11/06- Software Requirement Specification, ref. 066771 00 SRS, édition 1-AB du 23/11/06
[PP0005]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. <i>Certified under the reference BSI-PP-0005-2002T.</i>
[PP0006]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. <i>Certified under the reference BSI-PP-0006-2002T.</i>
[PP0002]	Protection Profile — Smart card IC Platform Protection Profile, Version: 1.0, July 2001. <i>Certified under the reference BSI-PP-0002-2001.</i>
[2006_13]	Certification report 2006/13 - Carte CNS : composant P5CT072VOP masqué par la plate-forme JavaCard GOP ID MX 64 et embarquant l'application CNS 1.0.7, 15 September 2006 SGDN/DCSSI

Annex 3. Certification references

Decree number 2002-535 dated 18 th 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 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 1.0, March 2002.
[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.
[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004