



PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report 2007/16

**COSMOS V1.1 card: ID One IAS applet v1.01
(SSCD configuration) loaded on COSMO 64
RSA D v5.4 embedded on P5CT072VOP**

Paris, 29th august 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.

Certification report reference

2007/16

Product name

COSMOS V1.1 card: ID One IAS applet v1.01 (SSCD configuration) loaded on COSMO 64 RSA D v5.4 embedded on P5CT072VOP

Product reference

**Embedded applet reference : ID One IAS (ID One V3), Version 1.01
Microcontroller references : ROM mask P5CT072EWE1/T0PB6311**

Protection profile conformity

PP SSCD type 2 [PP0005] and PP SSCD type 3 [PP0006]

Evaluation criteria and version

**Common Criteria version 2.3
compliant with ISO 15408:2005**

Evaluation level

**EAL 5 augmented
ALC_DVS.2, AVA_MSU.3, AVA_VLA.4**

Developer(s)

Oberthur Card Systems

**71-73 rue des Hautes Pâtures,
92726 Nanterre Cedex, France**

NXP

**Stresemannallee 101
22505 Hamburg, Germany**

Sponsor

Oberthur Card Systems

**71-73 rue des Hautes Pâtures,
92726 Nanterre Cedex, France**

Evaluation facility

Serma Technologies

**30 avenue Gustave Eiffel, 33608 Pessac, France
Phone: +33 (0)5 57 26 08 64, 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	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>	7
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Life cycle</i>	9
1.2.5. <i>Evaluated configuration</i>	10
2. THE EVALUATION.....	11
2.1. EVALUATION REFERENTIAL	11
2.2. EVALUATION WORK	11
2.3. CRYPTOGRAPHIC MECHANISMS ROBUSTNESS ANALYSIS.....	11
3. CERTIFICATION.....	12
3.1. CONCLUSION	12
3.2. RESTRICTIONS	12
3.3. RECOGNITION OF THE CERTIFICATE	12
3.3.1. <i>European recognition (SOG-IS)</i>	12
3.3.2. <i>International common criteria recognition (CCRA)</i>	13
ANNEX 1. EVALUATION LEVEL OF THE PRODUCT.....	14
ANNEX 2. EVALUATED PRODUCT REFERENCES	15
ANNEX 3. CERTIFICATION REFERENCES	17

1. The product

1.1. Presentation of the product

The evaluated product is « COSMOS V1.1 card: ID One IAS applet v1.01 (SSCD configuration) loaded on COSMO 64 RSA D v5.4 embedded on P5CT072VOP » developed by Oberthur Card Systems and NXP.

The ID One IAS applet is also called ID One V3.

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.

This security target is compliant to [PP0005] and [PP0006] protection profile (SSCD type 2 and type 3).

1.2.1. Product identification

The configuration list [CONF] identifies the product's constituent elements.

Each software component version of the certified version of the product can be checked in usage phase through *Get Data* command (see [AGD_JCP] and [SRS]).

This command provides the following data:

- For the platform, Tag 'DF52':
 - o 00 02 **e9 10** 01 06 41 07 11 30 42 36 02 05 **00 00 f9 00 ff** 03 06 **06 58 81** 01 23
e9 04 01 77 05 01 0f 90 00
 - Mask Identification : **E910** ;
 - Card identification : **00 00 f9 00 ff** ;
 - Optional Code Identification : **065881** ;
- For the applet and APIs, Tag '61':
 - o 61 20 53 02 **d0 14** 53 02 **a0 04** 53 02 **a0 08** 53 02 **a0 0d** 53 02 **a0 09** 53 02 36
40 53 02 02 19 53 02 02 19 90 00
 - ID One V3 Applet : **D014** ;
 - Utilities : **A004** ;
 - File System : **A008** ;
 - Secure Messaging : **A00D** ;
 - Security : **A009**.

1.2.2. Security services

The product mainly includes the following components:

- The JavaCard Platform which provides mainly the following security services :
 - o interface between the Integrated Circuit and the ID One V3 applet ;
 - o basic services to provide to ID One V3 applet access to memories and all needed cryptographic operations ;
 - o global management of the card (loading, installation and deletion of applets) and monitor the security of the card (data integrity and physical attacks counter-measures) ;
 - o blocking of the loading mechanism after the ID One V3 loading (therefore no loading can be initiated after JCP status is SECURED).

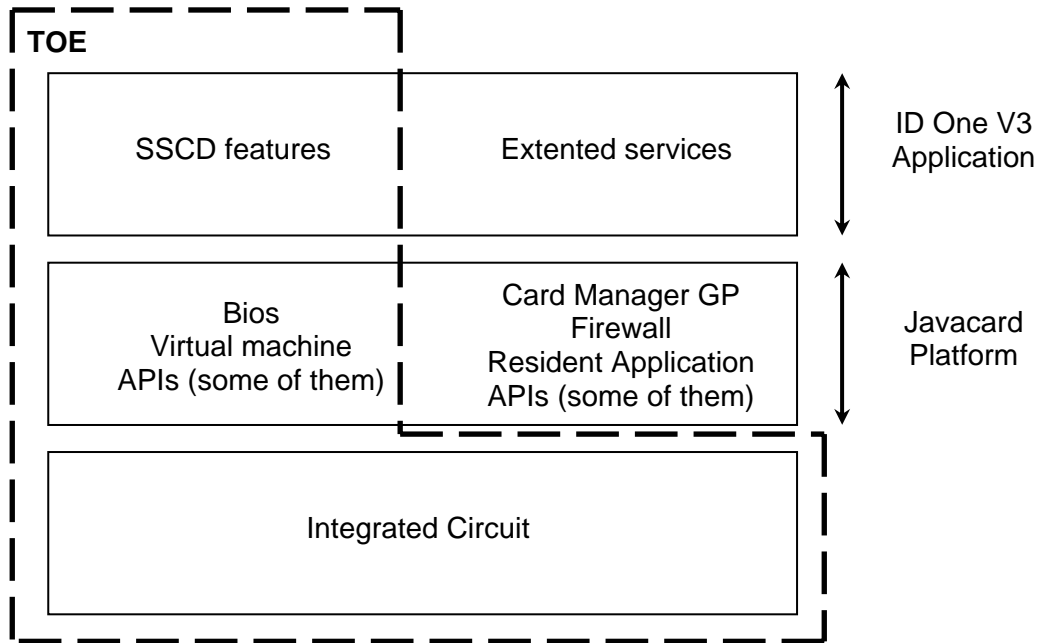
- The ID One V3 Applet (which commercial name is ID One IAS Applet) which mainly provides the following security services:
 - o generation of private and public signing keys (SCD: signature creation data and SVD: signature verification data ;
 - o secrecy of the signature creation data ;
 - o import of signature creation data and signature verification data ;
 - o export of signature verification data ;
 - o signature creation ;
 - o PIN administration ;
 - o PIN authentication of the Signatory ;
 - o External authentication of an administrator ;
 - o Implementation of a trusted path to a human interface device.

This applet also provides IAS functionalities that are out of the scope of this evaluation.

1.2.3. Architecture

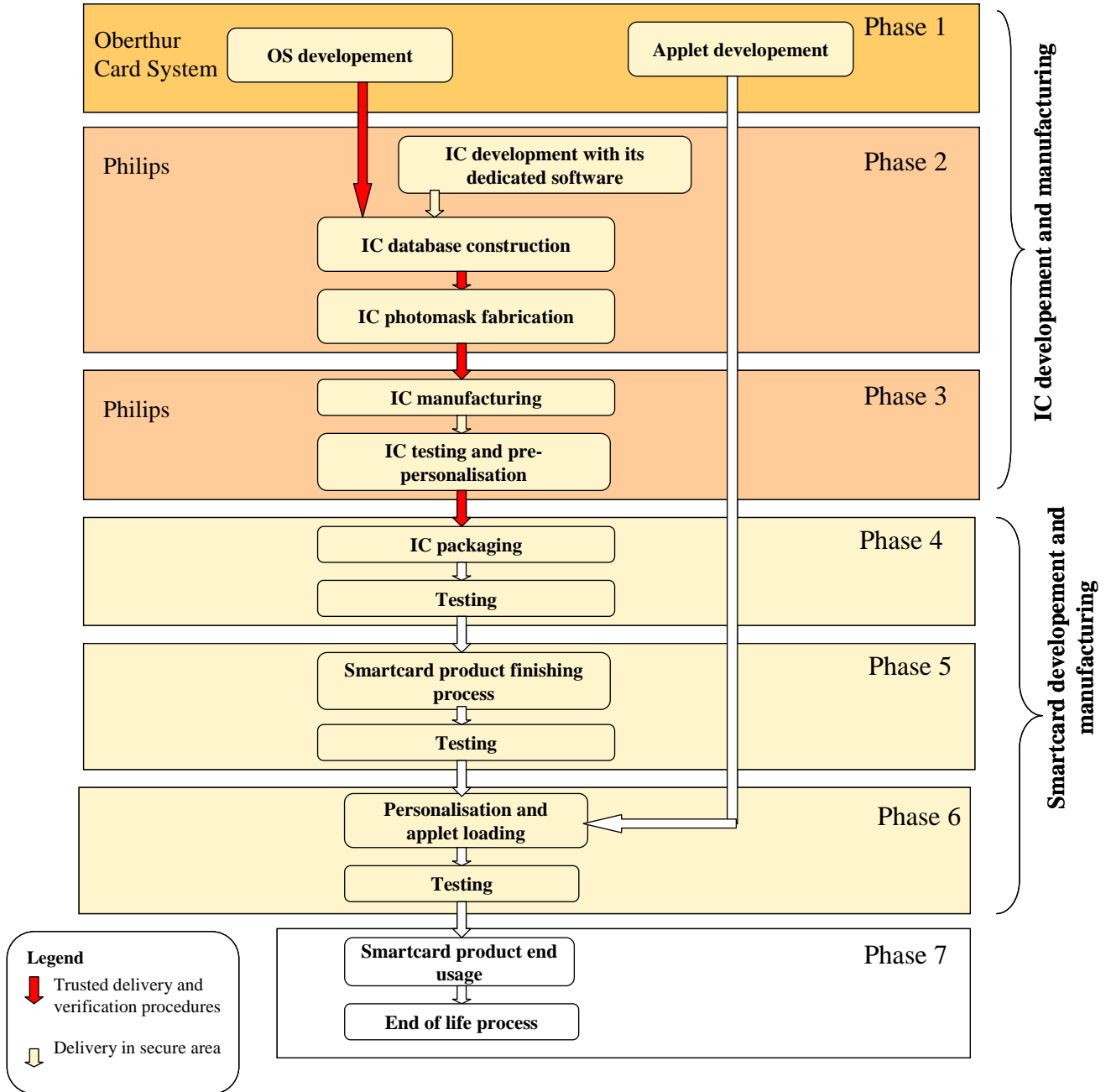
The product is composed of:

- the microcontroller P5CT072VOP developed and produced by NXP ;
- the JavaCard Operating System, developed by Oberthur Card Systems, which is composed of :
 - o the platform 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 ID One V3 developed by Oberthur Card Systems which is loaded on the personalisation phase (v1.01).



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 NXP (previously known as Philips Semiconductors GmbH).

In the evaluation context, the product personaliser has 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 certificate only applies to the SSCD configuration of the product: IAS functionalities are not available in the configuration in which the product is set (e.g. objects dealing with IAS functionalities are not created during the ID One V3 pre-personalisation phase). All the personalisation operations are described in [PEP].

The certificate applies to the “closed” configurations of the product (blocking of the applet loading mechanism after the ID One V3 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], 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 “P5CT072VOP” 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 microcontroller robustness level has been confirmed by the German scheme the 6th august 2007 in a surveillance process.

The evaluation relies on the evaluation results of the CNS Card and IDOneClassIC Card products, certified by DCSSI, respectively, the 15th September 2006 and the 29th January 2007 under the references 2006/13 [2006_13] and 2007/02 [2007_02].

The evaluation technical report [ETR], delivered to DCSSI the 8th June 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 analysed mechanisms reach, until 2008, the “standard” level as defined in DCSSI cryptographic referential [REF-CRY]. 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 product “COSMOS V1.1 card: ID One IAS applet v1.01 (SSCD configuration) loaded on COSMO 64 RSA D v5.4 embedded on P5CT072VOP,” submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 5 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 :

- the correspondence between public signing key –SVD- and private signing key –SCD- (OE.SCD_SVD_Corresp) ;
- the secure transfer of private signing key –SCD- between SSCD (OE.SCD_Transfer) ;
- the uniqueness of the signature-creation data (OE.SCD_Unique) ;
- the generation of qualified certificates (OE.CGA_Qcert) ;
- the authenticity check of the SVD by the CGA (OE.SVD_Auth_CGA) ;
- the protection of the verification authentication data –VAD- (OE.HI_VAD) ;
- the data 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 5+	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	3	Development tools 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	3	Semiformal functional specification
	ADV_HLD		1	2	2	3	4	5	3	Semiformal high-level design
	ADV_IMP				1	2	3	3	2	Implementation of the TSF
	ADV_INT					1	2	3	1	Modularity
	ADV_LLD				1	1	2	2	1	Descriptive low-level design
	ADV_RCR	1	1	1	1	2	2	3	2	Semiformal 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	2	Standardised life-cycle model
	ALC_TAT				1	2	3	3	2	Compliance with implementation standards
ATE Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	2	2	3	2	Testing: low-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	1	Covert channel analysis
	AVA_MSU			1	2	2	3	3	3	Analysis and testing of insecure states
	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]	<p>Reference security target for the evaluation:</p> <ul style="list-style-type: none"> - ID ONE V3 Security Target, ref. FQR: 110 2963, edition 6, 16/05/07 <p>For the needs of publication, the following security target has been provided and validated in the evaluation:</p> <ul style="list-style-type: none"> - Oberthur Card System - Cosmos Security Target Lite, ref UDD 064471 02, edition 1-AA
[ETR]	<p>Evaluation technical reports :</p> <ul style="list-style-type: none"> - COSMOS project: Evaluation Technical Report, ref. COSMOS_ETR_V1.1.fm, version 1.1, 08/06/07 - Addendum to Evaluation Technical Report, ref. Add_COSMOS_ETR_v1.1_V1.0.fm, version 1.0, 28/08/07
[ANA-CRY]	<p>Cotation de mécanismes cryptographiques - Projet COSMOS, ref. N° 1479/SGDN/DCSSI/SDS/Crypto du 06 Juillet 2006</p>
[CONF]	<p>COSMOS Configuration List, ref. FQR : 110 3217, edition 2, 30/01/07</p>
[GUIDES]	<p>Installation guidance:</p> <ul style="list-style-type: none"> - [PEP]: ID One IAS PERSONNALISATION ref. 065421 00 PEP, edition 1-AB, 01/12/06 <p>Administration and user guidance:</p> <ul style="list-style-type: none"> - [AGD_JCP] : ID One Cosmo 64 RSA D v5.4, ref. 064471 01 UDD AA - [SRS]: ID One V3 Applet SRS, ref. 063253 00 SRS, edition 3-AA, 30/01/07 - COSMOS AGD_USR/AGD_ADM, ref. FQR : 110 3597, edition 1, 01/12/06
[PP0005]	<p>Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. <i>Certified by BSI under the reference BSI-PP-0005-2002T.</i></p>
[PP0006]	<p>Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. <i>Certified by BSI under the reference BSI-PP-0006-2002T.</i></p>
[PP0002]	<p>Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. <i>Certified by BSI under the reference BSI-PP-0002-2001.</i></p>
[2006_13]	<p>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</p>



[2007_02]	Certification report 2007/02 - IDOneClassIC Card : ID-One Cosmo 64 RSA v5.4 and applet IDOneClassIC v1.0 embedded on P5CT072VOP, 29 january 2007, 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 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
----------	--