



PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report 2006/28

**AXSEAL CC V2 72K e-Passport application
embedded on Philips P5CD072 V0Q
microcontroller**

Paris, 12 December 2006

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>	2006/28	
<i>Product name</i>	AXSEAL CC V2 72K e-Passport application embedded on Philips P5CD072 V0Q microcontroller	
<i>Product reference</i>	Reference of the application: Axseal V3, code revision 456 Reference of the microcontroller with embedded software: Philips P5CD072 V0Q - Part A1002922 (CHIP M576ICAOP3M P5CD072V3 MOB4)	
<i>Protection profile conformity</i>	PP BSI-PP-0017 Machine Readable Travel Document with ICAO Application, Basic Access Control	
<i>Evaluation criteria and version</i>	Common Criteria version 2.2	
<i>Evaluation level</i>	EAL 4 augmented ADV_IMP.2, ALC_DVS.2.	
<i>Developers</i>	Gemalto 6 rue de la Verrerie, 92197 Meudon Cedex, France	Philips Semiconductors Postfach 54 02 40, 22502 Hamburg, Allemagne
<i>Sponsor</i>	Gemalto 6 rue de la Verrerie, 92197 Meudon Cedex, France	
<i>Evaluation facility</i>	CEACI (Thales Security Systems – CNES) 18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France Phone: +33 (0)5 61 27 40 29, email : ceaci@cnes.fr	
<i>Recognition arrangements</i>	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>	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.....	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 the e-Passport application AXSEAL CC V2 72K (code revision 456) developed by Gemalto, embedded on Philips P5CD072 V0Q microcontroller (manufacturing identification: Part A1002922 - CHIP M576ICAOP3M P5CD072V3 MOB4) developed and manufactured by Philips Semiconductors.

The evaluated product is a contactless smartcard with its antenna. The smartcard implements the e-Passport features according to the specifications from the International Civil Aviation Organization (cf. [ICAO]). The product enables:

- To store passport holder's signed data (issuing state or organization, passport number, expire date, holder's name, nationality, birth date, sex, other optional data) a holder's biometric data (face portrait), optional authentication data and several other pieces of data for managing the document security;
- To check passport's authenticity and to identify its holder during a boarder control with the support of an inspection system.

The chip and its embedded software are intended to be inserted into the cover page of traditional passport booklets.

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 conformant to the Machine Readable Travel Document (MRTD) Protection Profile (cf. [MRTD]).

1.2.1. Product identification

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

In final user mode, the certified version of the product can be identified by the initial answer of the card (*Answer to select* – ATS). The following data shall be found in the ATS:

- "00 15" for the P5CD072 microcontroller;
- "D0 00 42" for Axseal V2 CC 72K (code revision 456);
- "00 00", meaning that no patch is loaded. The certified version of the product contains no patch.

Other commands for administrators allow identifying the product more precisely and are described in the guidance documents (cf. [GUIDES]).

The microcontroller can also be identified with the following element visible written on the top layer of the product, and visible with a microscope: "Philips T023Q".

1.2.2. Security services

The product provides mainly the following security services:

- Self_test of security functions,
- Life cycle management,
- Loading of the NVM embedded software,
- Check of sensitive data integrity,
- Identification and Authentication based on mutual authentication,
- Data exchange with secure messaging,
- Identification and Authentication based on external authentication,
- Authenticity of the MRTD chip,
- Access Control to stored data objects,
- Protection of sensitive data.

1.2.3. Architecture

A microcontroller circuit embedding the e-Passport application and the holder's identification data is connected to an antenna and mounted on a plastic film. This "Inlay" is then embedded in the coversheet of the passport booklet and provides a contactless interface for the passport holder identification. This is represented in the following figure:

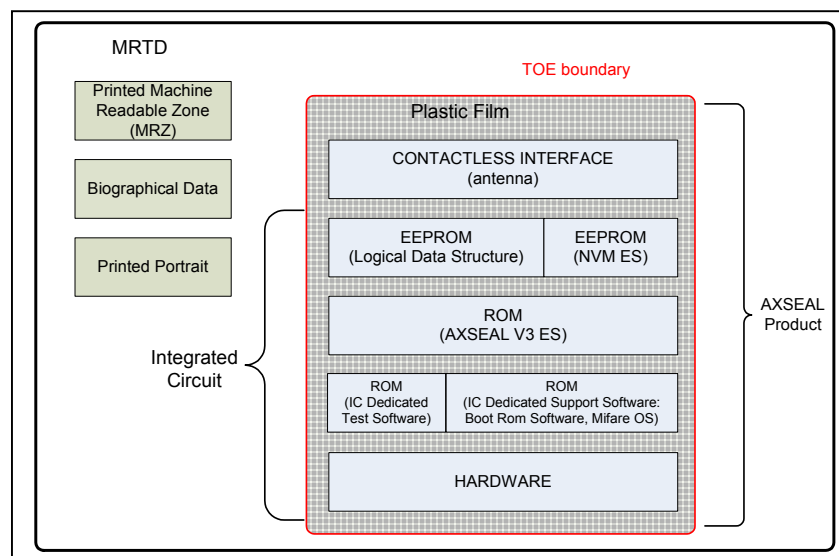


Figure 1 –Architecture of the product

The evaluated configuration of the product includes the logical data structure and the keys required to load the user data in personalisation phase. The product was delivered to the evaluation facility with an application for personalisation allowing to load user data and keys during the personalisation phase, in order to produce the final MRTD as required by the International Civil Aviation Organization (cf [ICAO]). This application was used and the final configuration of the MRTD was tested in order to check the conformity to the requirements defined in the MRTD PP (cf. [MRTD]).

1.2.4. Life cycle

The product's life cycle is organised as follow:

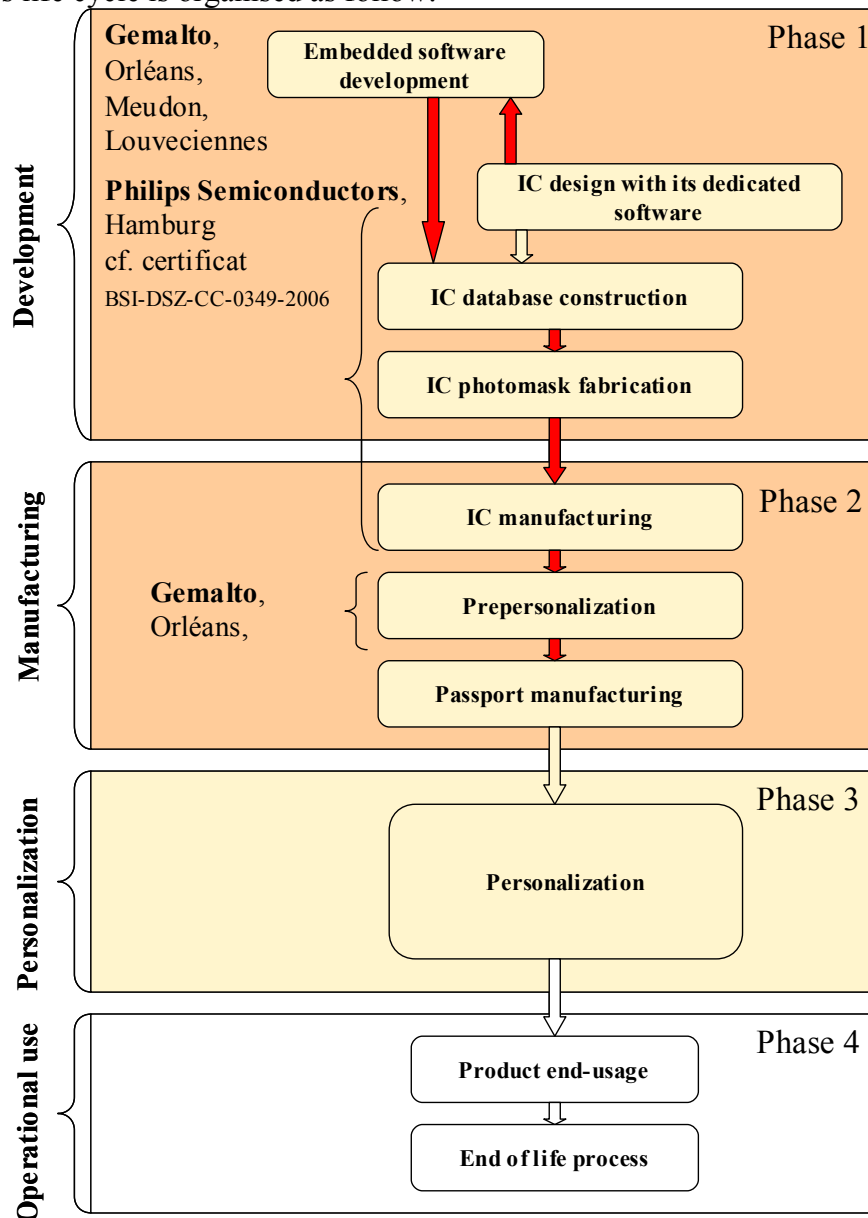


Figure 2 – Product life cycle

The product has been developed on the following sites:

Gemalto Meudon

6 rue de la Verrerie,
92197 Meudon Cedex,
France.

Gemalto Louveciennes

36-38 route de la Princesse, BP 45
78431 Louveciennes Cedex
France.

Gemalto Orléans

284 avenue de la Pomme de Pin, BP-6021 St Cyr en Val,
45060 Orléans Cedex 2,
France.

The microcontroller is developed and manufactured by Philips Semiconductors on the following site:

Philips Semiconductors

Postfach 54 02 40,
22502 Hamburg,
Allemagne.

The passport pre-personalization is performed by Gemalto in Orléans.

The phases regarding the Inlay manufacturing and the inclusion of the Inlay in the booklet are not in the scope of the evaluation, but these phases have no security impact on the product, which is already protected during these phases.

1.2.5. Evaluated configuration

The product under evaluation is the microcontroller with the embedded software, which are identified §1.1. The reference of the Inlay that identifies the antenna is « AWPFA 032/06-3 ». The product tested by the evaluation facility is typical to the final passport (product with Inlay packaging, in pre-personalized and personalized configurations).

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.2** [CC], with the Common Evaluation Methodology [CEM], and with the following interpretations: 86, 137, 146, 175, 180, 192, 220, 227, 228, 232, 243, 254.

For assurance components above EAL4 level, the evaluation facility own evaluation methods consistent with [AIS34] document, validated by DCSSI have been used.

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, this evaluation took into account the results of the microcontroller “**P5CD072 V0Q**” evaluation at EAL5 level augmented with ALC_DVS.2 and AVA_VLA.4, compliant with the [PP0002] protection profile. This microcontroller has been certified the 28 March 2006 under the reference BSI-DSZ-CC-0349-2006.

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

The evaluation also relies on the evaluation results of the “AXSEAL CC V2 36K e-Passport application embedded on Philips P5CD036V0Q microcontroller” product certified the 28 November 2006 under the reference 2006/23 (cf. [2006/23]).

2.2. Evaluation work

The evaluation technical report [RTE], delivered to DCSSI the 7th December 2006, 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 were stated in a cryptographic analysis report 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 “AXSEAL CC V2 72K e-Passport application embedded on Philips P5CD072 V0Q microcontroller” submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL4 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 specified in the security target [ST] and shall respect the recommendations in the guidance [GUIDES], in particular:

- The issuing State or Organization must ensure that the Personalization Agents acting on the behalf of the issuing State or Organization:
 - o Establish the correct identity of the holder and create biographic data for the MRTD;
 - o Enrol the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s);
 - o Personalize the MRTD for the holder together with the defined physical and logical security measures (including the digital signature in the Document Security Object). The Personalization Agents enable or disable the Basic Access Control function of the TOE according to the decision of the issuing State or Organization. If the Basic Access Control function is enabled the Personalization Agents generate the Document Basic Access Keys and store them in the MRTD’s chip;
- The Issuing State or Organization must:
 - o Generate a cryptographic secure Country Signing Key Pair;
 - o Ensure the secrecy of the Country Signing Private Key and sign Document Signer Certificates in a secure operational environment;
 - o Distribute the Certificate of the Country Signing Public Key to receiving States and organizations maintaining its authenticity and integrity;

The Issuing State or organization must:

- o Generate a cryptographic secure Document Signing Key Pair and ensure the secrecy of the Document Signer Private Keys;
- o Sign Document Security Objects of genuine MRTD in a secure operational environment only;
- o Distribute the Certificate of the Document Signing Public Key to receiving States and organizations. The digital signature in the Document Security

Object includes all data in the data groups DG1 to DG16 if stored in the LDS according to [ICAO];

- The issuing State or Organization has to establish the necessary public key infrastructure in order to:
 - o Generate the MRTD's Active Authentication Key Pair,
 - o Sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15,
 - o Support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Active Authentication Public Key by means of the Document Security Object;
- The issuing State or Organization must ensure that the MRTD administrator acting on the behalf of the issuing State or Organization establish the correct identity of the holder and update the MRTD with the defined physical and logical security measures. According to the decision of the issuing State or Organization the MRTD administrator can for example terminate the application or execute any administrative commands provided by the TOE;
- The inspection system of the Receiving State must examine the MRTD presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. Additionally the Extended Inspection System performs the Active Authentication mechanism to verify the Authenticity of the presented MRTD's chip;
- The border control officer of the Receiving State uses the inspection system to verify the traveller as MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and organizations must manage the Country Signing Public Key and the Document Signing Public Key maintaining their authenticity and availability in all inspection systems;
- The inspection system of the receiving State ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under Basic Access Control will use inspection systems, which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems). The receiving State examining the logical MRTD with Primary Inspection Systems will prevent eavesdropping to the communication between TOE and inspection system;
- The holder may prevent attempts to disclose the logical MRTD by following recommendations for the protection of the MRZ against unauthorized people. An attacker knowing the MRZ or a part of it have better chance to perform a successful skimming or eavesdropping attack.

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is released 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]. However, it is only recognised for EAL4 level.

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, 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	2	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	2	Independent vulnerability analysis

Annex 2. Evaluated product references

[ST]	<p>Reference security target for the evaluation:</p> <ul style="list-style-type: none"> - Axseal V2 CC 72K Security Target – HERMES, Reference: D1033361 Rev 1.4, Gemalto <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"> - e-Passport Axseal CC V2 72K Security Target Public Version, Reference: D1033361 Rev. 1.4, Gemalto
[RTE]	<p>Evaluation Technical Report, Project: HERMES 72K, Reference: HER72_ETR_V1.0 CEACI</p>
[CONF]	<p>Liste de Configuration Axseal V3, Reference: D1028643 Rev 1.1 Gemalto</p>
[GUIDES]	<p>Installation guidance:</p> <ul style="list-style-type: none"> - Pre-personalization Manual – Hermes ePassport Axseal V3, Reference: D1031012 Rev 1.3 Gemalto - Cards global personalization process for a new application, Reference: D1024364 Rev : B Gemalto <p>Administration guidance:</p> <ul style="list-style-type: none"> - Personalization Manual – Hermes ePassport Axseal V3, Reference: D1031013 Rev 1.3 Gemalto - AGD_ADM – Administrator manual Hermes ePassport Axseal V3 (V2 CC 36K and 72K), Reference: D1028647 Rev 1.2 Gemalto <p>User guidance:</p> <ul style="list-style-type: none"> - AGD_USR – User manual AXSEAL V3, Reference: D1028648 Rev : 1.1 Gemalto
[ICAO]	<ul style="list-style-type: none"> - PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 1st 2004 International Civil Aviation Organization, - Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7, May 18th 2004 International Civil Aviation Organization,



	- Machine Readable Travel Documents, supplement 9303, version 3.0, 12nd June 2005
[PP MRTD]	Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control, version 1.0, 18 August 2005. <i>Certified under the reference BSI-PP-0017</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>

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, 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.
[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 1.02 du 19 novembre 2004, réf: 2791/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