PREMIER MINISTRE

Secretariat General for National Defence

French Network and Information Security Agency

Certification Report ANSSI-CC-2009/46

ID-One Cosmo V7.0-a SmartCard in configuration Standard and Basic

Paris, 19 November 2009

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 ANSSI (French Network and Information Security Agency), 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
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP
France

certification.anssi@ssi.gouv.fr

Certification report reference

ANSSI-CC-2009/46

Product name

ID-One Cosmo V7.0-a SmartCard in configuration Standard and Basic

JavaCard platform embedded on Atmel Secure Microcontroller Solutions components AT90SC 28872RCU Rev G and Rev E, 28848RCU Rev G and Rev E and embedded with cryptographic library version 00.03.11.05 ToolBox from Atmel Secure Microcontroller Solutions

Product reference

JavaCard Platform version for any configuration: 7.0-a

Optional Code r1.0 High Secure version for each configuration: 071771, 071781

Optional Code CodopAuth r1.0 version for each configuration: 071631, 071641

ToolBox version for any configuration: 00.03.11.05

Protection profile conformity

[PP/0304]

Java Card System - Standard 2.1.1 Configuration Protection Profile – version 1.0b, August 2003 certified by ANSSI

Evaluation criteria and version

Common Criteria version 3.1

Evaluation level

EAL 5 augmented

ADV_IMP.2, ALC_DVS.2, AVA_VAN.5

Developer(s)

Oberthur Technologies[1] **50 quai Michelet** **92300 Levallois-Perret, France**	**ATMEL Secure Microcontroller Solutions**[1] **Maxwell Building - Scottish Enterprise technology Park** **East Kilbride, G75 0QR - Ecosse, Royaume-Uni**

Sponsor

Oberthur Technologies

50 quai Michelet, 92300 Levallois-Perret, France

Evaluation facility

THALES - CEACI (T3S – CNES)

18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

Phone: +33 (0)5 62 88 28 01 or 18, email : nathalie.feyt@thalesgroup.com

Recognition arrangements

CCRA

SOG-IS

The product is recognised at EAL4 level.

[1] : main site.

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 French Network and Information Security Agency 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 sponsors 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 ID-One Cosmo V7.0-a smartcard, a Java Card open platform, developed par Oberthur Technologies:

- compliant to Java Card 2.2.2 specifications and VISA GlobalPlatform 2.1.1 ;
- embedded on different (by memory size and interfaces) components of a same family developed by ATMEL ;
- embedded with cryptographic library version 00.03.11.05 toolbox from Atmel Secure Microcontroller Solutions;
- adjusted with two patches named Optional Code r1.0 High Secure and CodopAuth r1.0 Platform Identification, which version depends on the underlying component used, developed by Oberthur Technologies.

These different variants of the product are summarized in the following table:

Product version	Java Card platform version	Optional Code r1.0 High Secure patch version	CodopAuth r1.0 Platform Identification patch version	component version	ToolBox version
Standard	7.0-a	071771	071631	AT90SC 28872RCU révision G et E	00.03.11.05
Basic	7.0-a	071781	071641	AT90SC 28848RCU révision G et E	00.03.11.05

1.2. Evaluated product description

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

This security target claims conformance to [PP/0304] protection profile

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 elements included in the product answer to GET DATA command (cf. [GUIDES]).

So, on an evaluated product, the GET DATA command with tag DF 52 gave the following answer:

- DF 52 3E 01 01 **C3** 02 02 00 48 03 02 **08 01** 04 10 **07 16 31 01** CE D1 94 BB **07 17 71 01** 73 4C AE 83 05 01 01 06 17 83 00 01 3F 3F FF F9 00 00 00 00 01 C8 80 C0 00 00 96 FF 69 FF 00 FF 07 01 0F 08 00.

  Within this answer, we can read the following identifying data (in bold caracter):
  - The mask number is **0801 C3**, which corresponds to the ID-One Cosmo V7.0-a Standard;
  - The CodopAuth r1.0 Platform Identification patch number is **071631** in version **01**;
  - The Optional Code r1.0 High Secure patch number is **071771** in version **01**.

The GET DATA command with tag DF 50 gave the following answer:

- 50 09 **30 04 08 52 43 55 04 41 0A**.

  Within this answer, we can read the following identifying data (in bold caracter):
  - **30** identifies le component, i.e. AT90SC28872RCU ;
  - **04** identifies the component revision, i.e. revision E;
  - **08** identifies the production year;
  - **52** identifies factory and quarter of production;
  - **43 55** identifies the batch number;
  - **04** identifies the wafer number;
  - **41 0A** identifies the die number.

1.2.2. Security services

The product provides mainly the following security services:

- The card pre-personalization services;
- The personalization of applets with deletion, installation, loading under the GP Card Manager and associated security domain control with possibility of DAP (Data Authentication Pattern);
- The interfaces API service dedicated to applets and access to these API;
- Managing of GP and signature keys;
- The firewall for segregation of objects or applets;
- The standard GP services such as logical channel and the secure channel protocol (SCP01, SCP02) as well as the proprietary secure channel protocol (SCP03).

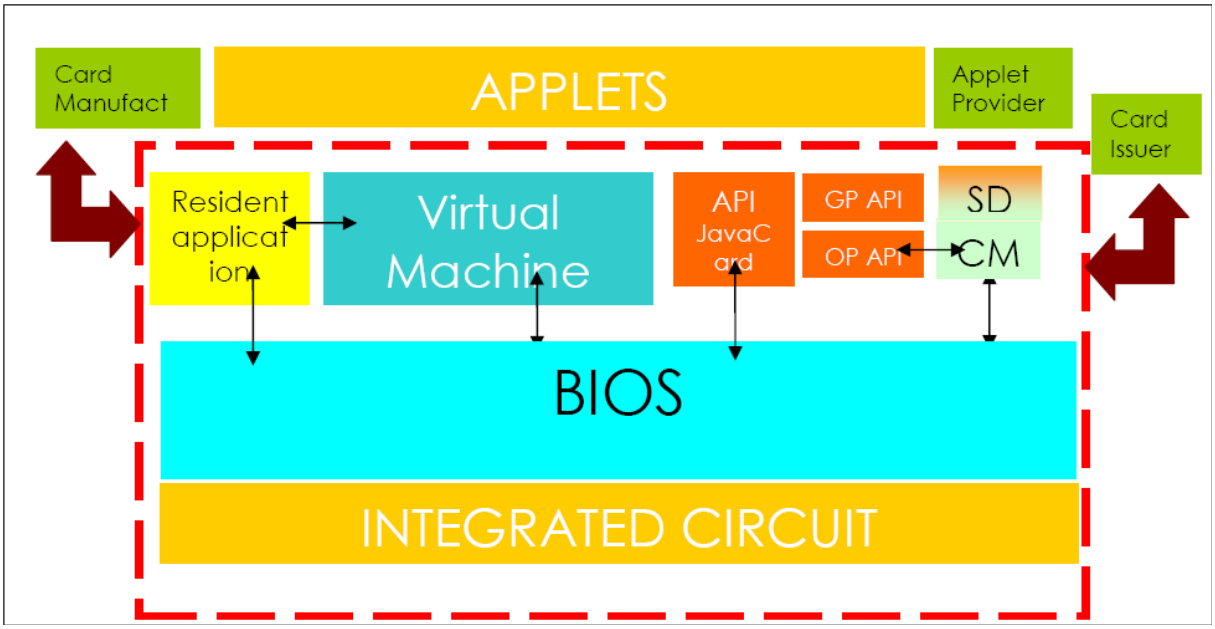
A more detailed list of security services is available in [ST].

1.2.3. Architecture

The product consists of:

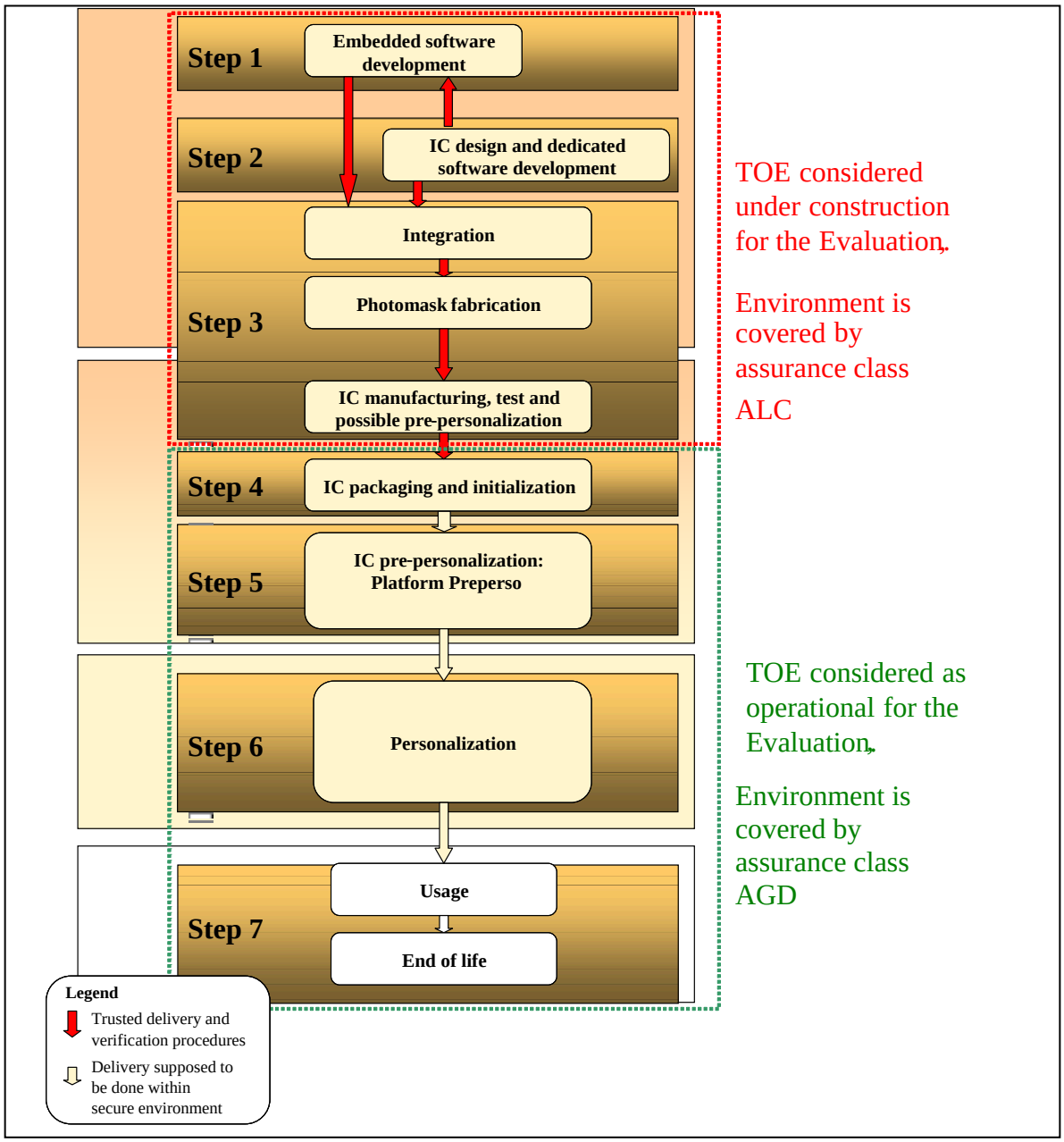
- a microcontroller, providing hardware features, and its cryptographic library ToolBox;
- a BIOS providing the interface between native applications, such as the virtual machine, and the hardware;
- a virtual machine which interprets the byte code of Java Card applets;
- APIs which offer interfaces to the applets such as key generation, key agreement, signature, message ciphering and other proprietary interfaces (OCS API);
- Common Open Platform with the Card Manager, OPSystem and GPSystems APIs; it is developed in native code and in Java (its byte code is in ROM);
- a resident application, in native code, with a basic main dispatcher, to receive the card commands.

This architecture is summarized in the following figure:



1.2.4. Life cycle

The product life cycle is compliant to the 7 steps life cycle of a smart card product and is summarized in the following figure:



The evaluation has covered the conception and the development of the platform which are done in step 1. Steps 2 and 3, until delivery, have been covered by component evaluation. The end of step 3 and steps 4, 5 and 6 are covered by guides. The evaluated product is the one delivered to the user in step 7.

The product has been developed by Oberthur Technologies on the following sites:

Oberthur Technologies - Nanterre
71-73, rue des Hautes Pâtures
92726 Nanterre
France

Oberthur Technologies - Levallois
50, quai Michelet
92 300 Levallois-Perret
France

Oberthur Technologies - Bordeaux
Parc Scientifique UNITEC 1
4, allée du Doyen Georges Brus - Porte 2
33 600 PESSAC
France

The microcontroller has been developed and manufactured by ATMEL Secure Microcontroller Solutions on its sites (cf. [BSI-DSZ-CC-0421-2008-MA-02]), whereof main site is:

ATMEL Secure Microcontroller Solutions

Maxwell Building - Scottish Enterprise technology Park
East Kilbride, G75 0QR – Ecosse
Royaume-Uni

In the evaluation context, the pre-personalization agent, personalization agent and card administrator have been considered as “product administrator” and the developers of applications to be loaded on the card have been considered as “product user”.

1.2.5. Evaluated configuration

The certificate applies to the Java Card platform only, as described above in chapter 1.2.3 Architecture, and configured according to personalization guide (cf. [GUIDES]).

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1** [CC], with the Common Evaluation Methodology [CEM].

For assurance components which are not covered by [CEM] manual, the evaluation facility own evaluation methods, validated by ANSSI, have been used.

In order to meet the specificities of smart cards, the [CC IC] and [CC AP] 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 comes from the integration of the software and the cryptographic library in the microcontroller. The library and the microcontroller have already been certified.

This evaluation has then taken into account the evaluation results for:

- the ATMEL secured microcontroller - ATMEL - AT90SC28872RCU / AT90SC28848RCU rev. G and E at EAL5 level augmented with ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, compliant to the protection profile [PP0002] ; this microcontroller has been certified then maintained by BSI (cf. [BSI-DSZ-CC-0421-2008-MA-02]) ;
- the ATMEL cryptographic library - Toolbox 00.03.11.05 at EAL 5 level augmented with ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4 ; this library has been certified by ANSSI (cf. [DCSSI-2009/11]).

The evaluation technical report [ETR], delivered to ANSSI on 4 September 2009, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis regarding to ANSSI's technical referentials

The robustness of cryptographic mechanisms has not been analysed by ANSSI.

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality of 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 ID-One Cosmo V7.0-a smartcard, as described above in chapter 1.1, 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 security objectives for the operational environment specified in the security target [ST] and shall respect the recommendations in the guidance [GUIDES].

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 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 EAL 4 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, Spain, Sweden 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 Republic of Korea, Malaysia, Netherlands, New-Zealand, Norway, Pakistan, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

Annex 1. Evaluation level of the product

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Intitulé du composant
ADV Development	ADV_ARC		**1**	1	1	**1**	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**2**	Complete mapping of the implementation representation of the TSF
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**4**	Semiformal modular design
AGD Guidance	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedure
ALC Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**5**	Development tools CM coverage
	ADO_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation standards
ASE Security Target Evaluation	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claim
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended component definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specifications
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	**2**	**3**	3	**4**	**3**	Testing: modular design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independant testing, sample
AVA Vulnerability assessment	AVA_VAN	**1**	**2**	**2**	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annex 2. Evaluated product references

[ST]	Security target : - ID-ONE COSMO V7.0 - CLIO SECURITY TARGET For AT90SC28872RCU / AT90SC28848RCU Référence FQR: 110 4626 - issue 1 - 22/06/2009 Oberthur Technologies Security Target for composition with components: - ID-ONE COSMO V7.0 - CLIO SECURITY TARGET COMPATIBILITY For ATMEL IC Référence FQR: 110 4622 - issue 1 - 22/06/2009 Oberthur Technologies For the needs of publication, the following security target has been provided and validated during the evaluation: - ID-ONE COSMO V7.0 - CLIO Security Target Lite For AT90SC28872RCU / AT90SC28848RCU Référence FQR: 110 4777 - issue 1 Oberthur Technologies
[RTE]	Evaluation Technical Report : - Evaluation technical report - Project: CLIO Référence CLIO_ETR_1 - révision 2.0 – 04/09/2009 THALES-CEACI For the needs of composite evaluation with this platform, an Evaluation Technical Report for composition has been evaluated: - Evaluation technical report lite - Project: CLIO ETR LITE for composition Référence CLIO_ETR Lite_1 – révision 2.0 – 04/09/2009 THALES-CEACI
[CONF]	Configuration List of the product - CLIO - CONFIGURATION LIST AT90SC288xxRCU Référence FQR : 110 4616 - issue: 3 – 09/02/2009 Oberthur Technologies
[GUIDES]	Installation Guides of the product : - COP REF V02.12 - PRODUCT GENERATION DESCRIPTION – PGD 069241 00 PGD – issue 1 AA, 10/06/2008 Oberthur Technologies - ID-One Cosmo V7.0-a Applets - PRODUCT GENERATION DESCRIPTION - PGD 069671 00 PGD – issue 1 AA, 23/10/2008 Oberthur Technologies - Optional Code r1.0 Authenticate on ID-One Cosmo V7.0-a Platform 72k - PRODUCT GENERATION DESCRIPTION - PGD 071631 00 PGD – issue 1 AA, 02/06/2009 Oberthur Technologies

	- Optional Code r1.0 Authenticate on ID-One Cosmo V7.0-a Platform 48k - PRODUCT GENERATION DESCRIPTION - PGD 071641 00 PGD – issue 1 AA, 15/05/2009 Oberthur Technologies - Optional Code r1.0 High Secure on ID-One Cosmo V7.0-A Platform 72k - PRODUCT GENERATION DESCRIPTION - PGD 071771 00 PGD – issue 1 AA, 15/06/2009 Oberthur Technologies - Optional Code r1.0 High Secure on ID-One Cosmo V7.0-A Platform 48k - PRODUCT GENERATION DESCRIPTION - PGD 071781 00 PGD – issue 1 AA, 15/06/2009 Oberthur Technologies Administration Guides of the product : - ID-One Cosmo V7.0 - Pre-Perso Guide FQR : 110 4379 – issue 6, 26/06/2009 Oberthur Technologies - ID-One Cosmo V7.0 - Security recommendations FQR 110 4730 – issue 1, 02/09/2009 Oberthur Technologies User Guide of the product : - ID-One Cosmo V7.0 - Reference Guide FQR 110 4483, issue 5 Oberthur Technologies
[PP/0304]	Protection profile certified on 30 September 2003 by ANSSI and named: Java Card System - Standard 2.1.1 Configuration Protection Profile – version 1.0b
[BSI-DSZ-CC-0421-2008-MA-02]	BSI maintenance report deliverd on 6 April 2009 for ATMEL secure microcontroller - AT90SC28872RCU / AT90SC28848RCU rev G.
[DCSSI-2009/11]	ANSSI certificate delivered on 30 June 2009 for ATMEL cryptographic library - Toolbox 00.03.11.05
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001.

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, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001, Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002, Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, revision 2, ref CCMB-2007-09-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2008-04-001 version 2.5 revision 1, April 2008.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[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.