Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Certification Report ANSSI-CC-2010/40

ID-ONE Cosmo V7.0.1-n Smartcard masked on NXP P5CD081 V1A (Standard Dual), P5CC081 V1A (Standard) and P5CD041 V1A (Basic Dual) components

Paris, July, 6th 2010

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 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 et de la sécurité 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-2010/40

Product name

ID-ONE Cosmo V7.0.1-n Smartcard masked on NXP P5CD081 V1A (Standard Dual), P5CC081 V1A (Standard) and P5CD041 V1A (Basic Dual) components

Product reference

Java Card platform Version corresponding to all configurations : 7.0.1-n

Protection profile conformity

[PP/0304], version 1.0b

PP SUN Java Card™ System Protection Profile Collection, august 2003, certified by l'ANSSI

Evaluation criteria and version

Common Criteria version 3.1

Evaluation level

EAL 5 augmented

ALC_DVS.2, AVA_VAN5

Developer(s)

Oberthur Technologies
50 quai Michelet
92300 Levallois-Perret, France

NXP Semiconductors GmbH
Stresemannallee 101
D-22502 Hamburg, Germany

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
Tél : +33 (0)5 62 88 28 01, mail : nathalie.feyt@thalesgroup.com

Recognition arrangements

CCRA

The product is recognised at EAL4 level.

SOG-IS

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, modified. 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.

Contents

1. The product

1.1. Presentation of the product

The evaluated product is the ID-ONE Cosmo V7.0.1-n open Java Card platform Smartcard masked on NXP P5CD081 V1A (Standard Dual), P5CC081 V1A (Standard) et P5CD041 V1A (Basic Dual) components, developed by Oberthur Technologies :

- compatible with the Java Card 2.2.2 and VISA GlobalPlatform 2.1.1 specifications ;
- masked on some variations (in terms of memory size or interfaces) a family of NXP components.

These different product configurations are listed in the following table :

Name of the product	Java Card platform version	Reference of the component receiving the application	Mask reference identifying the component.
Standard Dual	V7.0.1-n	P5CD081 V1A	18 01 1F
Standard	V7.0.1-n	P5CC081 V1A	18 01 1A
Basic Dual	V7.0.1-n	P5CD041 V1A	18 01 1B

1.2. Evaluated product description

The security target [ST] defined the evaluated product, the evaluated security features and the security objectives for the environment.
This security target conforms to the [PP/034] protection profile.

1.2.1. Product identification

The constitutive elements of the product are identified in the configuration list [CONF].
The certified version of the product can be identified by the following:

- accessing to the « Device Coding Byte » DC2 value using the answer to the “GET DATA” command with tag DF 50 (see [GUIDES]) as indicated in the table

DC2 value	Component reference
44	P5CD081V1A
43	P5CC081V1A
42	P5CD041V1A

The DC2 value is in bold in this answer:

```
⇨  80 CA DF 50 17
<= DF 50 14 00 00 22 59 03 91 55 64 00 03 2C 00 20 41 21 07 44 31 34 31
90 00
```

- accessing to the Tag03 value using the answer to the “GET DATA” command with tag DF 52. The Tag03 value as specified in the following table:

Tag03 value	Operating system reference
18 01 1F	ID-One Cosmo V7.0.1-n Standard Dual
18 01 1A	ID-One Cosmo V7.0.1-n Standard
18 01 1B	ID-One Cosmo V7.0.1-n Basic Dual

```
⇨  80 CA DF 52 00
<= DF 52 44 01 01 1F 02 02 04 50 03 02 18 01 04 00 05 01 01 06 17 83 00 01 3F 3F FF
F9 00 05 00 00 01 00 00 00 00 00 FF FF FF FF FF FF 07 01 0F 08 0B 00 31 C0 64 1F 18
01 00 00 90 00 09 09 41 E8 01 F7 C0 03 CA E9 F2 90 00
```

The Tag 04 identifies the patches (here 00 for no patch).

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).

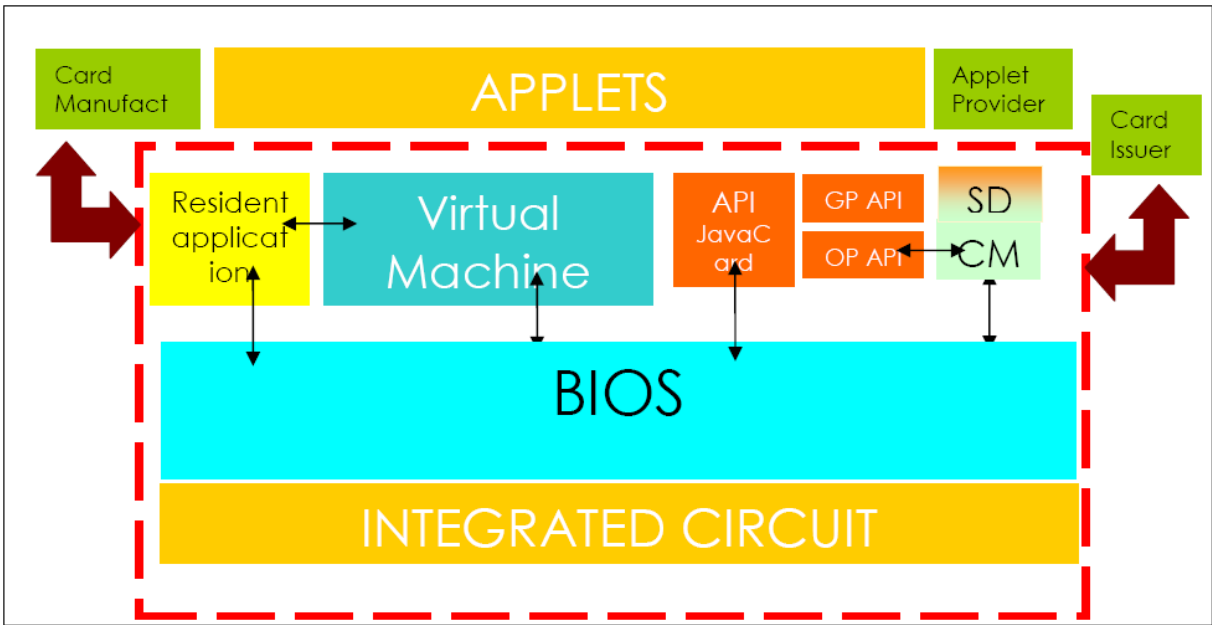
A more detailed list of security services is available in [ST].

1.2.3. Architecture

The product consists of:

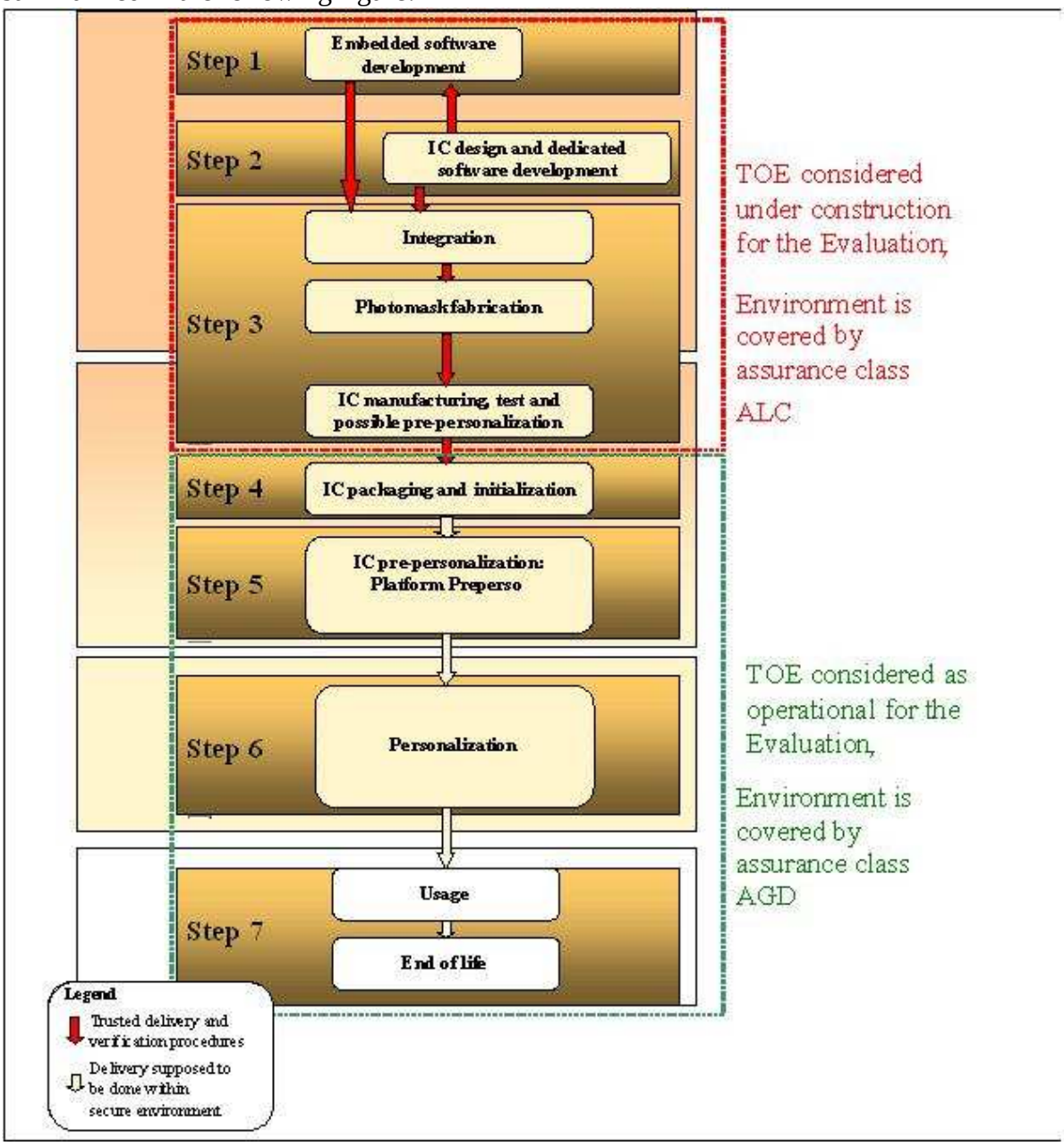
- a microcontroller, providing hardware features, and its cryptographic library ToolBox;
- a BIOS providing the interface between native applications, such as the virtual machine, and the hardware;
- a virtual machine which interprets the byte code of Java Card applets;
- APIs which offer interfaces 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:

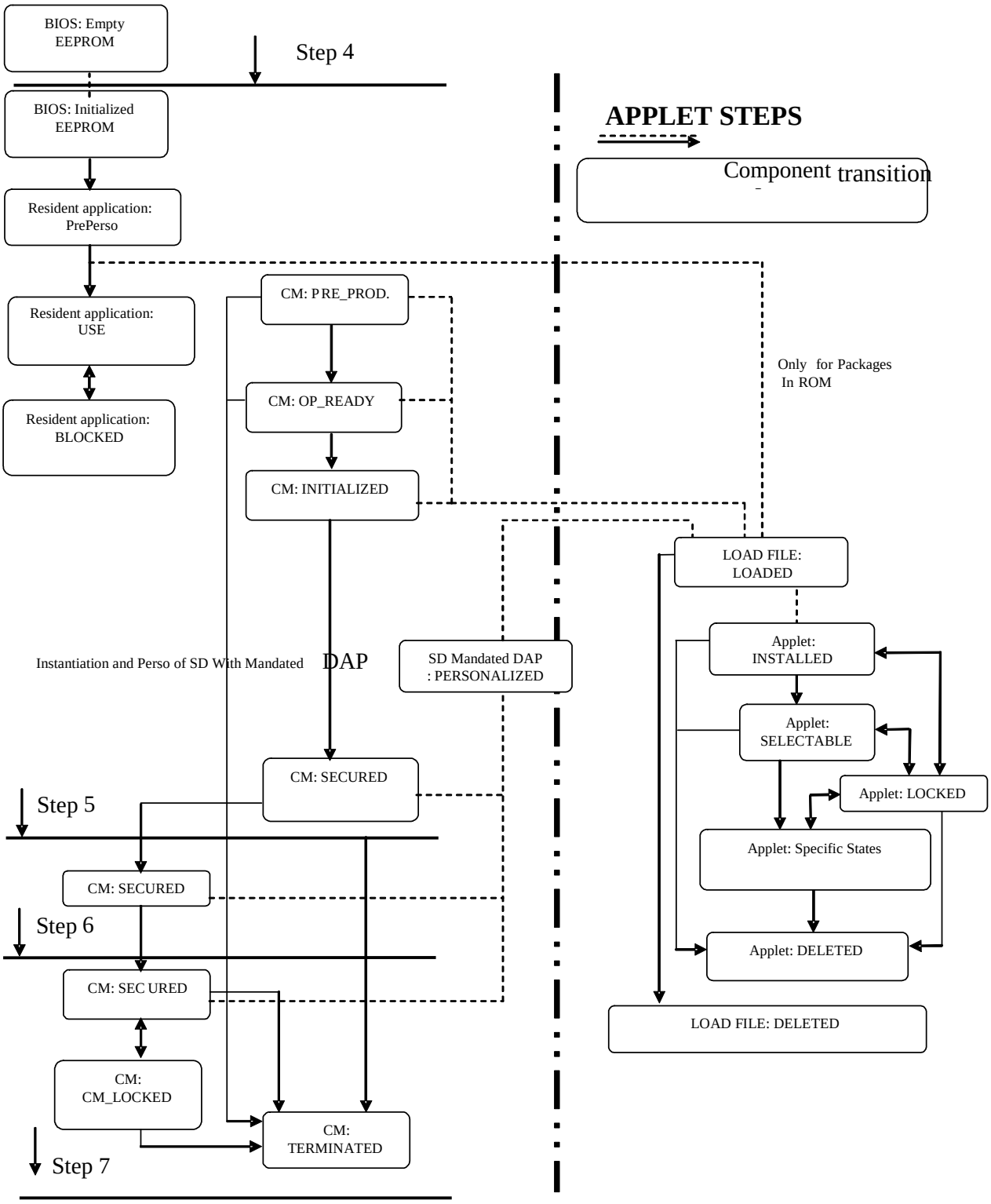


1.2.4. Life cycle

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



Product life cycle



States of the platform after phase 4

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 4.

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

Oberthur Technologies - Levallois

50 quai Michelet
92300 Levallois-Perret
France

Oberthur Technologies - Nanterre

71-73, rue des Hautes Pâtures
92726 Nanterre
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 NXP Semiconductors on its sites (cf. BSI-DSZ-CC-0555-2009), whereof main site is:

NXP Semiconductors GmbH1

Stresemannallee 101
D-22502 Hamburg
Allemagne

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]).

The tests have been performed on a ID-ONE Cosmo V7.0.1-n Standard Dual platform with IAS, on a P5CD081 component.
Some components were delivered in the “Secure” state of the “Card Manager’s” state machine. Other components were in the pre-personalization state « Resident Application : PrePerso ».

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 following microcontrollers P5CD081V1A, P5CC081V1A and P5CD041V1A (cf. [BSI-DSZ-CC-0555-2009]) at EAL5 level augmented with ALC_DVS.2 and AVA_VAN.5, compliant to the protection profile [PP0035].

The evaluation technical report [ETR], delivered to ANSSI the may 18th 2010, 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 ANSSI according to the [REF-CRY], [REF-KEY] et [REF-AUT] technical referentials.

The results are given in an analysis report [ANA-CRY] and conduct to the following conclusion:

- the analyzed mechanisms can be used to provide complaint applications to the ANSSI cryptographic referential ([REF-CRY]);
- the Global Platform specifications of the security target, to which the developer has to conform, lead to cryptographic weaknesses . These weaknesses are related to the 1024 bit RSA key size and the SHA-1 hash algorithm.

Anyway, these results have been taken in account in the evaluator vulnerability analysis and have not pointed any vulnerability the considered AVA_VAN level.

2.4. Random number generator analysis

The random generator has been analysed by the evaluator along with ANSSI, in conformance with the French standard for cryptography (cf. [ANA-CRY]).

The product is based on the P5CD081V1A, P5CC081V1A and P5CD041V1A components. Their random generators have been evaluated according to the [AIS31] methodology, as indicated in the BSI-DSZ-CC-0555-2009 certificate. The hardware generator reaches the class "P2 – *SOF-high*". This doesn't allow concluding that data are fully random but states that this random generator is free of major design flaw.
As required in [REF-CRY], the hardware random generator output is fended in a cryptographic post-treatment. The results are given in an analysis report [ANA-CRY] and conduct to the following conclusion:

- the key generation (RSA or elliptic curve) must be conduct under user control.

Anyway, these results have been taken in account in the evaluator vulnerability analysis and have not pointed any vulnerability the considered AVA_VAN level.

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 product “ID-ONE Cosmo V7.0.1-n open Java Card platform Smartcard masked on NXP P5CD081 V1A (Standard Dual), P5CC081 V1A (Standard) et P5CD041 V1A (Basic Dual) components submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 5 augmented.

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 V7.0.1-n open Java Card platform Smartcard masked on NXP P5CD081 V1A (Standard Dual), P5CC081 V1A (Standard) et P5CD041 V1A (Basic Dual) components, 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, as 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 2010 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable, for smart cards and similar devices, up to ITSEC E6 High 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 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, 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

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
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 semiformal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**2**	TSF internal description
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**4**	Semiformal modular design
AGD User guides	AGD_OPE	**1**	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	1	Preparative procedures
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
	ALC_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 claims
	ASE_ECD	**1**	1	1	1	1	1	1	1	Extended components 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 specification
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	Independent 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]	Reference security target for the evaluation: • TERPSICHORE Security Target ID-ONE COSMO V7.0.1-n for P5CD041V1A, P5CC081V1A and P5CD081V1A reference : FQR : 110 4933, version : 2 dated April 30th, 2010, by Oberthur Technologies For the needs of publication, the following security target has been provided and validated in the evaluation: - TERPSICHORE Security Target Lite For NXP reference FQR 110 5145 version 1 dated June 7th, 2010 by Oberthur Technologies
[ETR]	Evaluation technical report : TERN_ETR version v3.0 dated June 11th 2010 by THALES-CEACI For the needs of composite evaluation with this microcontroller a technical report for composition has been validated: - TERN_ETR Lite_v2_0 dated June 11th 2010 by THALES-CEACI
[ANA-CRY]	Cotation de mécanismes cryptographiques : project TERPSICHORE Reference 1684/ANSSI/ACE dated June 25th 2010 by ANSSI.
[CONF]	TERPSICHORE CONFIGURATION LIST NXP Reference FQR 110 4964 Ed4 dated may 12th 2010 by Oberthur Technologies
[GUIDES]	Installation guidance: - COP Ref v02.21 –PRODUCT GENERATION DESCRIPTION – PGD reference 071841 00 PGD / 1 –AB dated February 19th 2010 - ID-One Cosmo V7.0.1-n Applets – PRODUCT GENERATION DESCRIPTION – PGD reference 074001 00 PGD / 1 –AA dated March 4th,2010 - ID-One Cosmo V7.0.1- n Export Files – PRODUCT GENERATION DESCRIPTION – PGD reference 074011 00 PGD / 1 – AA dated February 19th 2010 - ID-One Cosmo V7.0.1- n Platform – PRODUCT GENERATION DESCRIPTION – PGD reference 072361 00 PGD / 1 – AA dated February 19th 2010 Administration guidance: - ID-One Cosmo V7.0.1- Pre-Perso Guide 3 reference FQR 110 4910 / Issue : 3 dated May 10th, 2010 - ID-One Cosmo V7.0.1 – Security recommendations Ed3 reference FQR 110 4912 / Issue : 3 dated May 17th 2010

	User guidance: - ID-One Cosmo V7.0.1 – Reference Guide ed3 Reference FQR 110 4911 /Issue: 3 dated May 10th, 2010
BSI-DSZ-CC-0555-2009	Certified by BSI on 10/11/2009 for *NXP Secure Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A each with specific IC Dedicated Software*
ANSSI-CC-2009/48	Certified by BSI on November 19th 2009 for *Carte à puce ID-One Cosmo V7.0-n en configuration Large, Standard, Basic (modes dual ou contact) ou Entry (mode dual) masquée sur composant NXP*
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007.*

Annex 3. Certification references

Decree number 2002-535, 18th April 2002, modified 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-2009-03-002 version 3.0, revision 1, March 2009.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.
[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 3.0, 8 Janvier 2010, Management Committee.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 dated January 20th 2010, cf. www.ssi.gouv.fr
[REF-KEY]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 dated October 18th 2008, cf. www.ssi.gouv.fr

[REF-AUT]	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 dated January 13th 2010, cf. www.ssi.gouv.fr
[AIS 31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik)