



PREMIER MINISTRE

General Secretariat for Defence and National Security

French Network and Information Security Agency

## **Certification Report ANSSI-CC-2010/58**

**IAS ECC v1.0.1 card on ID-One Cosmo v7.0.1-n :  
applet, version 1121, masked on ID-One Cosmo  
V7.0.1-n (NXP chip) in configuration Standard  
dual, Standard or Basic dual**

*Paris, October 1<sup>st</sup> 2010*

**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 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](mailto:certification.anssi@ssi.gouv.fr)

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

<i>Certification report reference</i> <b>ANSSI-CC-2010/58</b>	
<i>Product name</i> <b>IAS ECC v1.0.1 card on ID-One Cosmo v7.0.1-n : applet, version 1121, masked on ID-One Cosmo V7.0.1-n (NXP chip) in configuration Standard dual, Standard or Basic dual</b>	
<i>Product reference</i> <b>Applet version : 1121</b>	
<i>Protection profile conformity</i> <b>[BSI-PP-0005-2002] : SSCD Type 2, version 1.04 [BSI-PP-0006-2002] : SSCD Type 3, version 1.05</b>	
<i>Evaluation criteria and version</i> <b>Common Criteria version 3.1</b>	
<i>Evaluation level</i> <b>EAL 4 augmented ALC_DVS.2, AVA_VAN.5</b>	
<i>Developer(s)</i> <b>Oberthur Technologies<sup>1</sup></b> 50 quai Michelet 92300 Levallois-Perret, France	<b>NXP Semiconductors GmbH<sup>1</sup></b> Stresemannallee 101 D-22502 Hamburg, Germany
<i>Sponsor</i> <b>Oberthur Technologies</b> 50 quai Michelet 92300 Levallois-Perret, France	
<i>Evaluation facility</i> <b>THALES - CEACI (T3S – CNES)</b> 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	
<i>Recognition arrangements</i>   <b>The product is recognised at EAL4 level.</b>	

<sup>1</sup> : these are main sites



## 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](http://www.ssi.gouv.fr).



# Contents

<b>1. THE PRODUCT .....</b>	<b>6</b>
1.1. PRESENTATION OF THE PRODUCT.....	6
1.2. EVALUATED PRODUCT DESCRIPTION .....	7
1.2.1. <i>Product identification</i> .....	7
1.2.2. <i>Security services</i> .....	7
1.2.3. <i>Architecture</i> .....	8
1.2.4. <i>Life cycle</i> .....	9
1.2.5. <i>Evaluated configuration</i> .....	11
<b>2. THE EVALUATION.....</b>	<b>12</b>
2.1. EVALUATION REFERENTIAL .....	12
2.2. EVALUATION WORK .....	12
2.3. CRYPTOGRAPHIC MECHANISMS ROBUSTNESS ANALYSIS.....	12
2.4. RANDOM NUMBER GENERATOR ANALYSIS .....	13
<b>3. CERTIFICATION.....</b>	<b>14</b>
3.1. CONCLUSION .....	14
3.2. RESTRICTIONS .....	14
3.3. RECOGNITION OF THE CERTIFICATE .....	15
3.3.1. <i>European recognition (SOG-IS)</i> .....	15
3.3.2. <i>International common criteria recognition (CCRA)</i> .....	15
<b>ANNEX 1. EVALUATION LEVEL OF THE PRODUCT.....</b>	<b>16</b>
<b>ANNEX 2. EVALUATED PRODUCT REFERENCES .....</b>	<b>17</b>
<b>ANNEX 3. CERTIFICATION REFERENCES .....</b>	<b>19</b>

# 1. The product

## 1.1. Presentation of the product

The evaluated product is the IAS ECC card v1.0.1 on ID-One Cosmo v7.0.1-n; applet, version 1121, masked on ID-One Cosmo V7.0.1-n (NXP component) in the Standard dual, Standard or Basic dual configuration. The applet and the platform are developed by Oberthur Technologies, the component by NXP.

The Target Of Evaluation (TOE) is a secure software program running on a microcontroller, which may, for example, be put in a chip card or an inlay, and intended to be used in projects implementing electronic signatures. It has the characteristics of secure devices for the creation of electronic signatures (SSCD - Secure Signature Creation Device) as defined in European directive 1999/93/EC (Appendix III). Its applicative functionalities are provided by the ID-One IAS ECC v1.0.1 application, which run on the open JavaCard platform of Oberthur Technologies ID-One Cosmo V7.0.1-n in the Standard dual, Standard and Basic dual configuration on NXP component (platform certified by ANSSI, cf. [ANSSI-CC-2010\_40]).

As such, the TOE enables advanced electronic signatures, and electronic signatures known as qualified signatures, to be created (article 2 & article 5 of European directive 1999/93/EC).

The ID-One IAS-ECC v1.0.1 application covers the fields of identity, electronic signature, electronic services and data storage; it is compatible with the [IASECC] specifications.

It provides the two principal functions expected from the type 2 and type 3 SSCD products:

- generation and import of SCD/SVD (Signature Creation Data (the secret key)/Signature Verification Data (the public key));
- signature creation.

The other additional notable functions are:

- management of several SCD/SVD keys;
- regeneration and reimport of SCD/SVD;
- configuration of the application's operating mode (by an ad hoc administrator);
- authentication and establishment of trusted channels with remote entities;
- authentication of administrators;
- protection of anonymity and of data exchanged in contactless mode;
- provision of electronic services;
- data storage.

## 1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functions and its operating environment.

The security target demonstrates its compliance with the protection profile [BSI-PP-0005-2002] - SSCD type 2 - and [BSI-PP-0006-2002] - SSCD type 3. This compliance is chosen of demonstrable type by the [ST] since the [CCs] have been upgraded between the time when the protection profiles were written - according to CCv2.1 - and the [ST] - written according to CCv3.1.

### 1.2.1. Product identification

The elements making up the product are identified in the configuration list [CONF].

The certified version of the product is identifiable by the elements present in the answer provided by the product following the GET DATA command (cf. [CONF]). In fact, the product can give elements identifying the ID-One Cosmo V7.0.1-n platform, and the ID-One IAS-ECC v1.0.1 application. Only the elements relative to the ID-One IAS-ECC v1.0.1 application are given below (for the details concerning the underlying platform, see [ANSSI-CC-2010\_40]):

- GET DATA command for the tag DF 66: DF 66 02 **11 21**.

In this reply, **11 21** is the version of the ID-One IAS-ECC v1.0.1 application.

### 1.2.2. Security services

The main security services provided by the product, which are available in "contact" and "contactless" modes, consist of those provided by:

- the underlying platform part (cf. [ANSSI-CC-2010\_40]) including in particular:
  - o the interfaces to the service of APIs dedicated to the applets and access to these APIs;
  - o the firewall isolating the objects or applets;
  - o the standard "GlobalPlatform" services such as the logical channel and the secure channel protocol (SCP01, SCP02), together with the proprietary secure channel protocol (SCP03);
- the ID-One IAS-ECC v1.0.1 application (cf. [ST] for more details, notably § 2.1.4 and § 4.1.2);
  - o SF.PIN\_MGT: management of PIN in order to authenticate the signatory or the administrator;
  - o SF.SIG: provision of an electronic signature in accordance with the requirements of the protection profiles [BSI-PP-0005-2002] - SSCD type 2 - and [BSI-PP-0006-2002] - SSCD type 3;
  - o SF.DEV-AUTH: mutual authentication and opening of a trusted channel with the external entities (SCA, CGA, SSCD type 1); the cryptographic mechanisms used can then be symmetrical or asymmetrical;

- SF.ADM\_AUTH: external authentication of the administrators; the cryptographic mechanisms used can then be symmetrical or asymmetrical;
- SF.SM: management of the trusted channel with the external entities (SCA, CGA, SSCD type 1) guaranteeing integrity, origin, destination and confidentiality of the exchanges;
- SF.KEY\_MGT: management of the keys (SCD, SVD, authentication keys and dedicated keys for the electronic services);
- SF.CONF: TOE configuration management (choice of hashing location, of type of cryptography for authentication, of type of exchange protocol);
- SF.ESERVICE: provision of electronic services (client/server authentication, decryption of encrypted keys, verification of certificates);
- SF.EAVESDROPPING\_PROTECTION: protection against on-the-fly capture of sensitive data exchanged in contactless mode;
- SF.SAFESTATE-MGT: guarantee of safe internal states;
- SF.PHYS: protection against physical attacks.

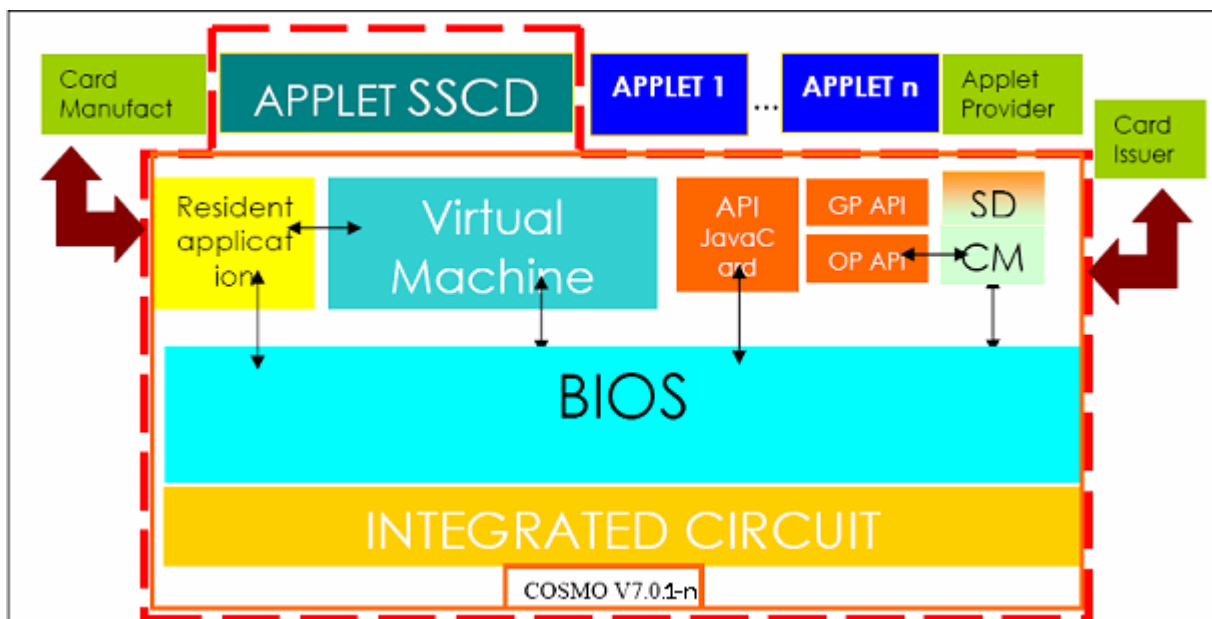
### 1.2.3. Architecture

The product consists of:

- the SSCD applet named ID-One IAS-ECC v1.0.1, version 1121;
- the underlying platform named ID-One Cosmo V7.0.1-n (the details of its blocks are given in [ANSSI-CC-2010\_40]);
- the underlying component corresponding to the platform, i.e. P5CD081, V1A, P5CC081 V1A, P5CD041 V1A.

The code of the applet, which is masked in the component, is interpreted by the virtual machine of the open JavaCard platform.

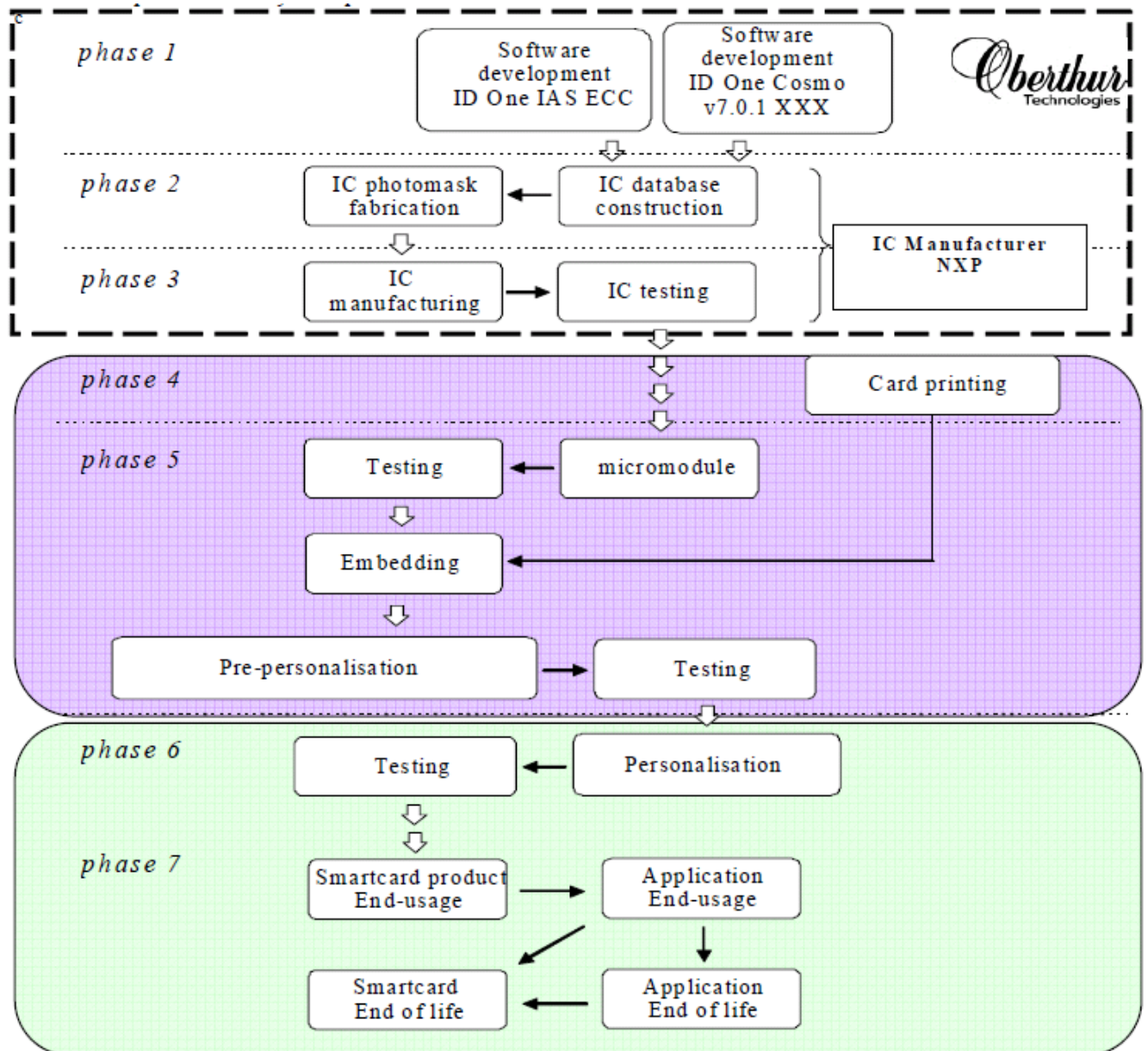
This architecture is summarised in the following figure:





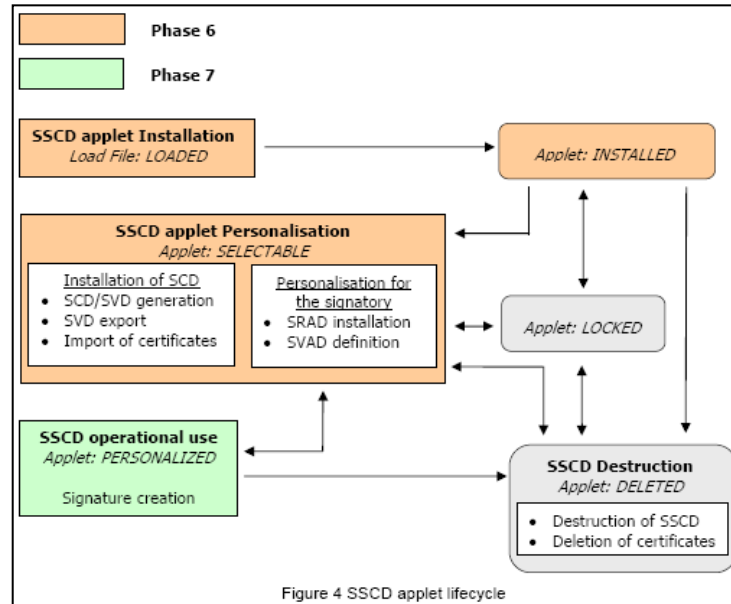
### 1.2.4. Life cycle

The life cycle of the product comprises seven stages and is summarised in the following figure:



The evaluation covered the design and development of the applet, which happen in phase 1. Phases 2 and 3, until delivery, were covered by the evaluation of the component. The end of phase 3 and phases 4 and 5 are covered by platform guides, and phase 6 is also covered by the platform guides completed by guides specific to the applet. The evaluated product is the one delivered to the user in phase 7.

It will be noted that, as indicated in the previous diagram, since composition is made on an ID-One Cosmo V7.0.1-n platform, the applet's code was masked in ROM at the same time as the code of the underlying platform (phase 2). Accordingly, there is no loading of the applet to be undertaken in phase 5. The applet is instantiated in phase 6. As a JavaCard applet managed using Global Platform, the detail of its life cycle is represented diagrammatically in the following figure:



The product was developed in the following sites:

#### **Oberthur Technologies - Levallois (phase 1)**

50 quai Michelet  
 92300 Levallois-Perret  
 France

#### **Oberthur Technologies - Nanterre (phase 1)**

71-73 rue des Hautes Pâtures  
 92726 Nanterre  
 France

#### **Oberthur Technologies - Pessac (phase 1)**

Parc Scientifique UNITEC 1  
 4 allée du Doyen Georges Brus - Porte 2  
 33600 Pessac  
 France

The underlying ID-One Cosmo V7.0.1-n platform was developed and manufactured by Oberthur Technologies and NXP in their respective sites (cf. [ANSSI-CC-2010\_40]).

For the evaluation, the evaluator considered three types of administrators of the product:

- the **application personalizer** involved in the personalization phase (phase 6) of the product; they are responsible for its personalization and for other administration functions such as:
  - o personalization of the RAD (Reference Authentication Data, i.e. the stored PIN);
  - o generation or import of the SCD;
  - o export of the SVD;
  - o generation, import or export of the authentication keys and electronic services;
  - o management of application locks (choice of hashing location, of type of cryptography for authentication, of type of exchange protocol);
  - o identification of the version of the ID-One IAS-ECC v1.0.1 application;
  - o passing the TOE to the usage phase;
- the **administrator** intervening in the usage phase (phase 7) of the product; they are responsible for its personalization and for other administration functions such as:
  - o personalization of the RAD;
  - o generation or import of the SCD;
  - o export of the SVD;
  - o generation, import or export of the authentication keys and electronic services;
- the **TOE administrator**, called "TOE\_Administrator" in [ST], intervening in the product usage phase (phase 7); they are responsible for management of applicative locks configuration and they have the rights to obtain the version of the ID-One IAS-ECC v1.0.1 application.

The evaluator considered as the user of the product its **end holder**, i.e. the person knowing secrets enabling them to undertake the signature operations with the card. They can, during the usage phase:

- o modify the RAD;
- o generate or import the SCD;
- o export the SVD;
- o provide electronic services;
- o generate, import and export the authentication keys and electronic services;

#### ***1.2.5. Evaluated configuration***

The certificate applies to the product as described above in section 1.2.3 Architecture and configured in accordance with the [GUIDES].

The results of tests are based on those acquired during tests undertaken on the samples:

- of the other variants of the product (cf. [ANSSI-CC-2010\_36], [ANSSI-CC-2010\_37], [ANSSI-CC-2010\_38]);
- of the platform underlying the variant of the product covered by the certificate [ANSSI-CC-2010\_39] (cf. [ANSSI-CC-2009\_48]);
- of the platform underlying the present product (cf. [ANSSI-CC-2010\_40]).

## 2. The evaluation

### 2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1 R2** [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 in the microcontroller already certified.

Therefore, the results of the evaluation of the underlying javacard platform “carte à puce ID-ONE Cosmo V7.0.1-n masquée sur composants NXP P5CD081 V1A (Standard Dual), P5CC081 V1A (Standard) et P5CD041 V1A (Basic Dual)” at EAL5 level augmented with ALC\_DVS.2, and AVA\_VAN.5, compliant with the [PP/0304] protection profile, have been used. This javacard platform has been certified by the ANSSI under the reference [ANSSI-CC-2010\_40].

The evaluation technical report [ETR], delivered to ANSSI the 13<sup>th</sup> September 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 its technical referential [RGS] during the certification of previous variants of the product (cf. [ANSSI-CC-2010\_36], [ANSSI-CC-2010\_37], [ANSSI-CC-2010\_38], [ANSSI-CC-2010\_39]) and of the underlying javacard platform ([ANSSI-CC-2010\_40]).

As the cryptographic mechanisms have not changed in this product, conclusions of previous quotations remain identical:

- for the previous variants of the product, see §2.3 of the certification reports [ANSSI-CC-2010\_36], [ANSSI-CC-2010\_37], [ANSSI-CC-2010\_38], [ANSSI-CC-2010\_39] and the corresponding quotation report [ANA-CRY\_EUTERPE] ;
- for the underlying javacard platform, see §2.3 of the certification report [ANSSI-CC-2010\_40] and the corresponding quotation report [ANA-CRY\_TERPSICHORE]).

The mechanisms analyzed are in accordance with the requirements of the ANSSI's technical referential [RGS], subject to the entire application of the guidance documentation (cf. [GUIDES] at §15 for AGD\_PRE and §11 for AGD\_OPE)

The results have been taken into consideration in the independent vulnerability analysis carried out by the evaluator and have not brought out any exploitable vulnerability for the targeted AVA\_VAN.5 level.

## **2.4. Random number generator analysis**

The product provides a pseudo-random generator. These pseudo-random numbers are obtained through a cryptographic post-treatment of the output of the hardware random generator of the underlying component.

This generator has been analysed by the ANSSI according to its technical referential [RGS] during the certification of the underlying javacard platform (cf. [ANSSI-CC-2010\_40]). As the composite product keeps the same generator, the conclusion of the previous analysis remains identical (cf. §2.4 of certification report [ANSSI-CC-2010\_40] and corresponding quotation report [ANA-CRY\_TERPSICHORE]) :

- key generation (RSA or elliptic curve keys) shall be done under the user's supervision.

The results have been taken into consideration in the independent vulnerability analysis carried out by the evaluator and have not brought out any exploitable vulnerability for the targeted AVA\_VAN.5 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 “IAS ECC v1.0.1 card on ID-One Cosmo v7.0.1-n : applet, version 1121, masked on ID-One Cosmo V7.0.1-n (NXP chip) in configuration Standard dual, Standard or Basic dual” 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 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<sup>1</sup>, 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<sup>2</sup>, 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 4+	Name of the component
<b>ADV</b> Développement	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_TDS		1	2	3	4	5	6	3	Basic modular design
<b>AGD</b> Guides d'utilisation	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
<b>ALC</b> Support au cycle de vie	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	4	Problem tracking 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	1	Well-defined development tools
<b>ASE</b> 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
<b>ATE</b> Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	1	Testing: basic 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
<b>AVA</b> Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	Advanced methodical vulnerability analysis



## Annex 2. Evaluated product references

[ST]	<p>Reference security target for the evaluation:</p> <ul style="list-style-type: none"> <li>- Euterpe on Terpsichore (NXP) - Security target référence 110 5165, version 3 ; Oberthur Technologies.</li> </ul> <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"> <li>- Euterpe on Terpsichore - IAS ECC v1.0.1 on ID-One Cosmo V7.0.1-n - Public Security target référence 110 5185, version 2; Oberthur Technologies.</li> </ul>
[ETR]	<p>Evaluation technical report :</p> <ul style="list-style-type: none"> <li>- Evaluation technical report - Project: EUTERPEonTERPSICHORE; référence EUTT_ETR, version 2; Thales-CEACI.</li> </ul>
[ANA-CRY_EUTERPE]	<p>ANSSI's cryptographic analysis report :          Cotation de mécanismes cryptographiques - Qualification EUTERPE, N° 722/ANSSI/ACE/LCC, 25 mars 2010</p>
[ANA-CRY_TERPSICHORE]	<p>ANSSI's cryptographic analysis report :          Cotation de mécanismes cryptographiques : projet TERSICHORE          Référence 1684/ANSSI/ACE du 25 juin 2010 édité par ANSSI.</p>
[CONF]	<p>Configuration list of the product:</p> <ul style="list-style-type: none"> <li>- Euterpe on Terpsichore - Configuration List référence 110 5169, version 3 ; Oberthur Technologies.</li> </ul>
[GUIDES]	<p>Administration guidance:</p> <ul style="list-style-type: none"> <li>- Euterpe on Terpsichore – AGD_PRE</li> <li>- référence 110 5171, version 3 ; Oberthur Technologies.</li> </ul> <p>User guidance:</p> <ul style="list-style-type: none"> <li>- Euterpe on Terpsichore– AGD_OPE</li> <li>- référence 110 5170, version 2 ; Oberthur Technologies.</li> </ul>
[IASECC]	<p>IAS ECC v1.0.1 specifications :</p> <ul style="list-style-type: none"> <li>- EUROPEAN CARD FOR e-SERVICES AND NATIONAL e-ID APPLICATIONS - IAS ECC v1.0.1 – GIXEL – 21/03/2008;</li> </ul> <p><a href="http://www.gixel.fr/includes/cms/_contenus/bibliotheque/file/CAP%20IAS%20ECC%20v1_0_1UK.pdf">http://www.gixel.fr/includes/cms/_contenus/bibliotheque/file/CAP%20IAS%20ECC%20v1_0_1UK.pdf</a></p>

[BSI-PP-0005-2002]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. <i>Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0005-2002T.</i>
[BSI-PP-0006-2002]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. <i>Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0006-2002T.</i>
[ANSSI-CC-2010_40]	ANSSI's certificate delivered the 6 july 2010 for the product : carte à puce ID-ONE Cosmo V7.0.1-n masquée sur composants NXP P5CD081 V1A (Standard Dual), P5CC081 V1A (Standard) et P5CD041 V1A (Basic Dual)
[ANSSI-CC-2010_36]	ANSSI's certificate delivered the 29 june 2010 for the product : carte ID-One IAS-ECC v1.0.1 R1 : applet (version 1121) chargée sur Cosmo v7.0-a (composant Atmel) en configuration Large Dual, Large et Standard Dual
[ANSSI-CC-2010_37]	ANSSI's certificate delivered the 29 june 2010 for the product : carte ID-One IAS-ECC v1.0.1 R1 : applet (version 1121) chargée sur Cosmo v7.0-a (composant Atmel) en configuration Standard
[ANSSI-CC-2010_38]	ANSSI's certificate delivered the 29 june 2010 for the product : carte ID-One IAS-ECC v1.0.1 R1 : applet (version 1121) chargée sur Cosmo v7.0-a (composant Atmel) en configuration USB
[ANSSI-CC-2010_39]	ANSSI's certificate delivered the 29 june 2010 for the product : carte ID-One IAS-ECC v1.0.1 R1 : applet (version 1121) chargée sur Cosmo v7.0-n (composant NXP) en configuration Large et Standard (modes dual ou contact)
[ANSSI-CC-2009_48]	ANSSI's certificate delivered the 19 november 2010 for the product : 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
[PP/0304]	Protection Profile certified by the ANSSI the 30 september 2003: Java Card System - Standard 2.1.1 Configuration Protection Profile – version 1.0b



## Annex 3. Certification references

Decree number 2002-535 dated 18 <sup>th</sup> 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-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 <sup>th</sup> January 2010, Management Committee.
[RGS]	Référentiel Général de Sécurité (RGS), version 1.0 – Documents related to the usage of cryptographic mechanisms in security functions. see <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .