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

Rapport de certification ANSSI-CC-2010/25

Applet ID One Classic v1.01.1 en configuration CNS, Classic ou CIE masquée sur Cosmo v7.0-a Large Dual, Large et Standard Dual sur composants Atmel

Paris, le 20 mai 2010

Le directeur général adjoint de l'agence nationale de la sécurité des systèmes d'information

Le vice-amiral Michel BENEDITTINI
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

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

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2010/25

Nom du produit

Applet ID One Classic v1.01.1 en configuration CNS, Classic ou CIE masquée sur Cosmo v7.0-a Large Dual, Large et Standard Dual sur composants Atmel

Référence/version du produit

Version 1.01.1

Conformité à un profil de protection

[BSI-PP-0005-2002] : SSCD Type 2, version 1.04
[BSI-PP-0006-2002] : SSCD Type 3, version 1.05

Critères d'évaluation et version

Critères Communs version 3.1

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

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

Commanditaire

Oberthur Technologies

50 quai Michelet
92300 Levallois-Perret, France

Centre d'évaluation

THALES - CEACI (T3S – CNES)

18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France
Tél : +33 (0)5 62 88 28 01 ou 18, mél : nathalie.feyt@thalesgroup.com

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

[1] : il s'agit des sites principaux.

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est l'applet, d'Oberthur Technologies, ID One Classic v1.01.1 en configuration CNS, Classic ou CIE masquée sur la plateforme, d'Oberthur Technologies, Cosmo v7.0-a Large Dual, Large et Standard Dual sur composants Atmel Secure Microcontroller Solutions.

La TOE (*Target Of Evaluation* – cible d'évaluation) est une carte à puce destinée à être utilisée dans le cadre de projets mettant en œuvre de la signature électronique, en particulier les projets [CNS] (*Carta Nazionale dei Servici* – carte nationale des services pour l'Italie) et [CIE] (*Carta di Identità Electronica* – carte d'identité électronique pour l'Italie).

Elle répond aux caractéristiques des dispositifs sécurisés de création de signature électronique (SSCD - *Secure Signature Creation Device* – dispositif de création de signature sécurisée), dont les fonctionnalités applicatives sont offertes par l'application ID One CIE qui s'exécute sur la plateforme JavaCard ouverte d'Oberthur Technologies ID-One Cosmo V7.0-a en configuration Large Dual, Large et Standard Dual sur composants Atmel Secure Microcontroller Solutions (plateforme certifiée par l'ANSSI, cf. [ANSSI-CC-2009_36]).

L'application ID One CIE couvre les domaines de l'identité, de la signature électronique et du stockage de données et est compatible avec les spécifications [CNS] et [CIE]. Elle offre les deux principales fonctions attendues des produits SSCD type 2 et type 3 :

- génération de SCD / SVD (*Signature Creation Data / Signature Verification Data* – données de création de signature (la clé secrète) / données de vérification de signature (la clé publique)) ;
- création de signature.

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité démontre sa conformité au profil de protection [BSI-PP-0005-2002] – SSCD type 2 - et [BSI-PP-0006-2002] - SSCD type 3. Cette conformité est choisie de type démontrable par la [ST] car les [CC] ont évolué entre le moment où les profils de protection ont été écrits - en CCv2.1 - et la [ST] - écrite en CCv3.1.

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par les éléments présents dans la réponse que donne le produit suite à la commande GET DATA (cf. [CONF]). En fait, le produit peut donner des éléments qui identifient la plateforme ID-One Cosmo V7.0-a ainsi que l'application ID One CIE. On ne donne ci-après que les éléments relatifs à l'application ID One CIE (pour les détails concernant la plateforme sous-jacente, voir [ANSSI-CC-2009_36]).

Ainsi, sur un produit utilisé lors de l'évaluation, la commande GET DATA pour le tag (étiquette) DF 65 a donné la réponse suivante :

- DF 65 04 **10 11 1D 00**.

Dans cette réponse, on lit les éléments d'identification suivants (caractères en gras) :

- **10 11** correspond à la version de l'application ID One CIE, soit 1.01.1 ici ;
- **1D** correspond à la configuration du produit, soit [CIE] ici[1] ;
- **00** indique que le *CHV manager* n'est pas utilisé.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit, accessibles en mode « à contact » et « sans contact », sont constitués de ceux fournis par :

- la partie plateforme sous-jacente (cf. [ANSSI-CC-2009_36]) ;
- l'application ID One CIE (cf. [ST] pour plus de détails, notamment les §2.2.2 et § 8.1) :
  - un produit hautement sécurisé et configurable pour stocker des données sensibles ainsi que les données utilisateur, basé sur ISO 7816-4 et 7816-9 ;
  - un canal sécurisé basé sur ISO 7816-4 (NB : la plateforme offre un autre mécanisme de canal sécurisé, cependant, il n'est pas utilisé par l'application ID One CIE) ;
  - gestion dynamique des règles de contrôle d'accès ;
  - gestion dynamique des paramètres confidentialité et intégrité intervenant dans le mécanisme canal sécurisé ;
  - génération dans la carte de la paire de clés RSA (jusqu'à 2048 bits), et conforme à l'ISO 7816-8 ;
  - authentification basée sur du triple DES, ainsi que le chiffrement et le déchiffrement, et conforme à l'ISO 7816-4 et l'ISO 7816-8 ;
  - signature électronique RSA conforme à l'ISO 7816-8 ;
  - gestion du PIN.

[1] Pour la configuration ID One Classic, la réponse serait 06 et 19 pour la configuration CNS.

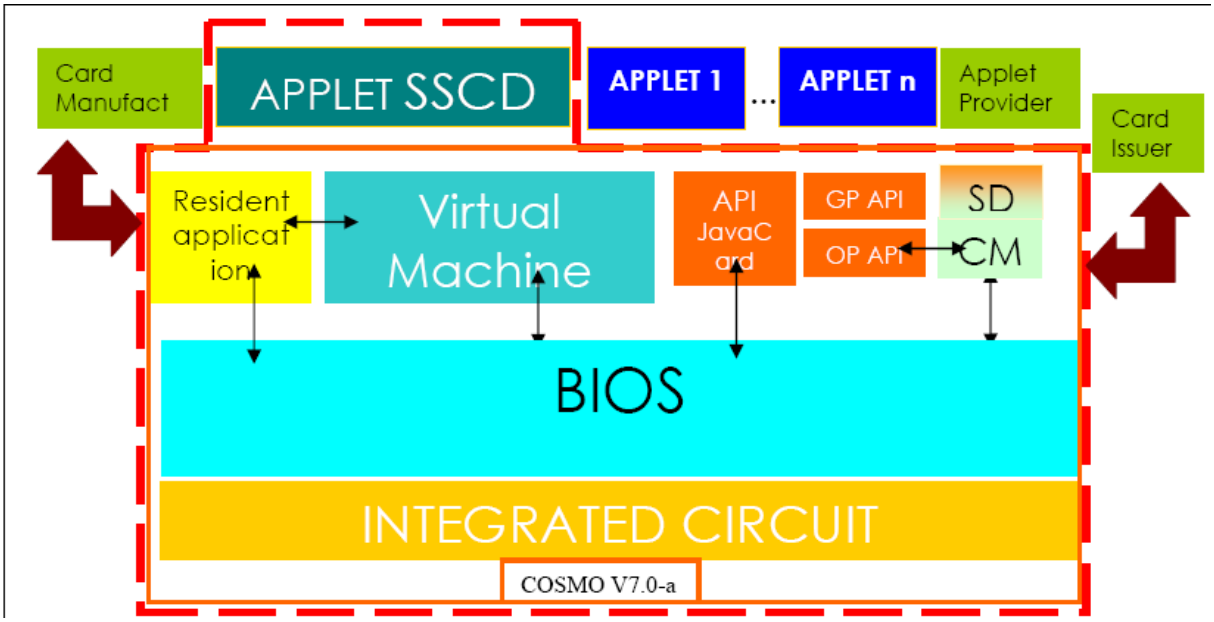
1.2.3. Architecture

Le produit est constitué de :

- l'applet SSCD nommée ID One CIE ;
- la plateforme nommée ID-One Cosmo V7.0-a sous-jacente (dont le détail des blocs est donné dans [ANSSI-CC-2009_36]) ;
- le composant sous-jacent correspondant à la plateforme, soit AT90SC256144RCFT rev F ou AT90SC256144RCFT rev F (antenne non montée) ou AT90SC25672RCFT rev F.

Le code de l'applet est interprété par la machine virtuelle de la plateforme JavaCard ouverte.

Cette architecture est résumée dans la figure suivante :



1.2.4. Cycle de vie

Le cycle de vie du produit est conforme au cycle de vie en sept étapes d'une carte à puce, il est résumé dans la figure suivante :

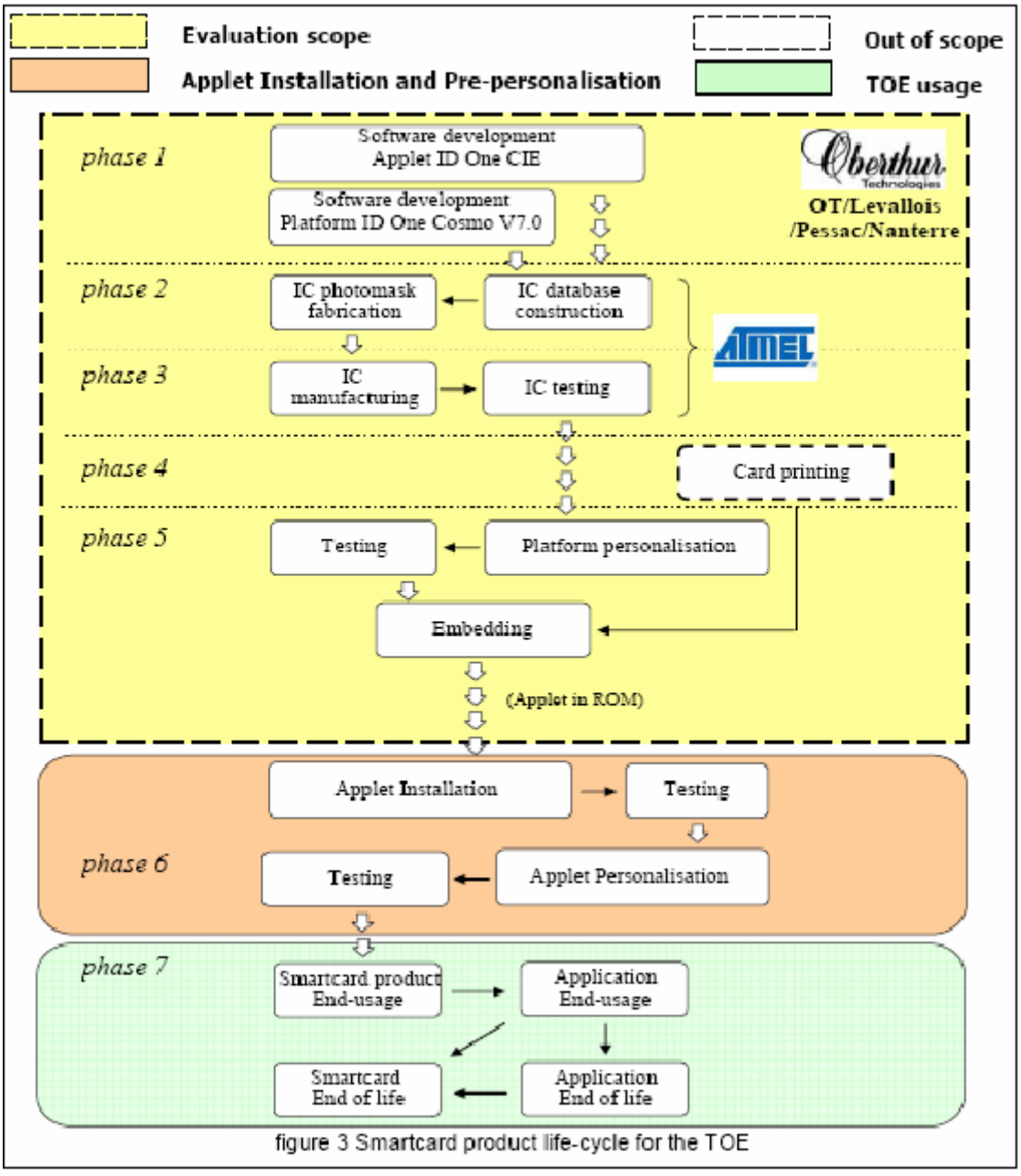


figure 3 Smartcard product life-cycle for the TOE

L'évaluation a couvert la conception et le développement de l'applet qui sont effectués en phase 1. Les phases 2 et 3, jusqu'à la livraison, ont été couvertes par l'évaluation du composant. La fin de la phase 3 et les phases 4, 5 sont couvertes par des guides de la plateforme, la phase 6 est également couverte par des guides de la plateforme complétés par des guides spécifiques à l'applet. Le produit évalué correspond à celui livré à l'utilisateur à la phase 7.

On notera que dans le cas présent, comme indiqué dans la figure ci-dessus, la composition étant faite sur une plateforme ID-One Cosmo V7.0-a, le code de l'applet a été masqué en ROM en même temps que le code de la plateforme sous-jacente (phase 2). En conséquence, il n'y a pas chargement de l'applet à effectuer en phase 5. L'instanciation de l'applet est effectuée en phase 6. En tant qu'applet JavaCard gérée selon Global Platform, le détail de son cycle de vie est schématisé dans la figure suivante :

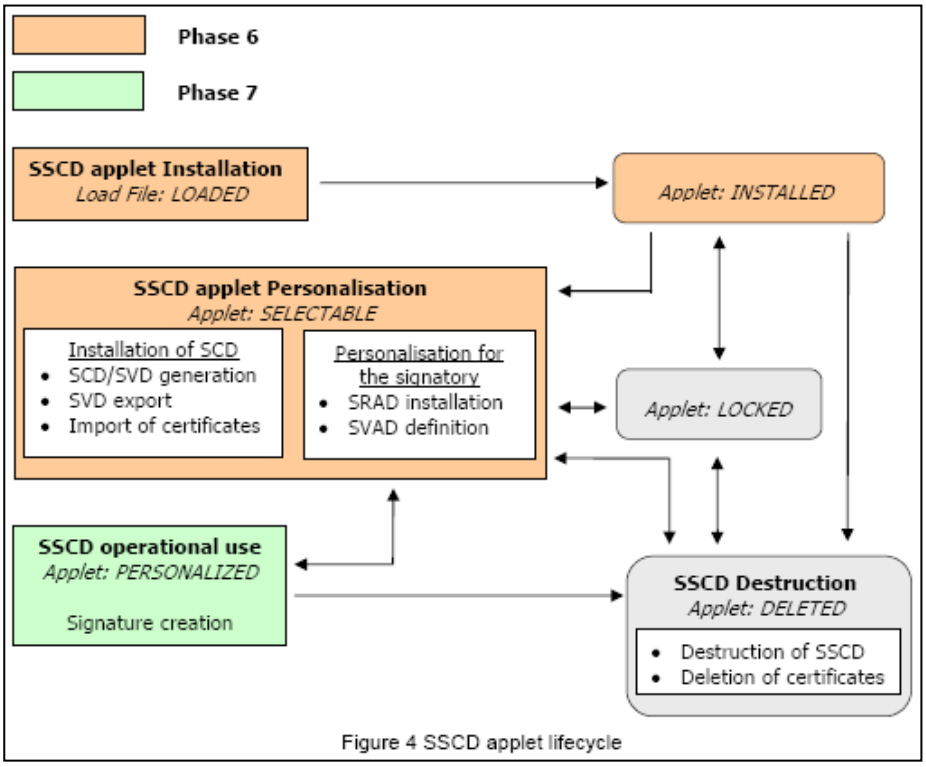


Figure 4 SSCD applet lifecycle

Le produit a été développé sur le site suivant :

Oberthur Technologies - Levallois

50 quai Michelet
92300 Levallois-Perret
France

Oberthur Technologies - Nanterre

71-73, rue des Hautes Pâtures
92726 Nanterre
France

Oberthur Technologies - Pessac

Parc Scientifique UNITEC 1
4 allée du Doyen Georges Brus - Porte 2
33 600 Pessac
France

La plateforme sous-jacente ID-One Cosmo V7.0-a a été développée et fabriquée par Oberthur Technologies et ATMEL Secure Microcontroller Solutions sur leurs sites respectifs (cf. [ANSSI-CC-2009_36]).

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit les rôles en charge de l'initialisation de la TOE, de sa personnalisation ainsi que des autres fonctions d'administration telles que :

- import de SCD (*Signature Creation Data* - données de création de signature (la clé secrète) si utilisé avec un SSCD type 1 ;
- génération SCD/SVD (SVD : *Signature Verification Data* – données de vérification de signature (la clé publique)), et export du SVD pour un CGA (*Certification Generation Application* – application de génération de certificats);
- import des clés pour l'authentification externe ainsi que pour le canal sécurisé ;
- mise à jour et déblocage du PIN.

De plus, l'évaluateur a considéré comme utilisateur du produit le détenteur final du produit, c'est-à-dire disposant des secrets lui permettant d'effectuer les opérations de signatures avec la carte.

1.2.5. Configuration évaluée

Le développeur a fourni à l'évaluateur la TOE décrite ci-après en configuration de test :

- Applet ID One CIE v1.01.1 masquée dans la plateforme JavaCard ouverte ID-One Cosmo v7.0-a Large Dual sur composants Atmel Secure Microcontroller Solutions (le composant était alors AT90SC256144RCFT).

La plateforme a été configurée conformément au guide de pré-personnalisation issu du projet CLIO (cf. [ANSSI-CC-2009_36]). L'applet a été configurée suivant [GUIDES].

Lors des tests, seules deux configurations, sur les trois présentes dans le produit, ont été étudiées :

- Classic ;
- [CIE].

En effet, l'évaluateur a considéré que la troisième configuration, nommée [CNS], est incluse dans celle [CIE], puisqu'elle se différencie seulement par l'ajout du bit 2 dans le troisième paramètre de l'installation, permettant ainsi au produit de chaîner des commandes et donc d'utiliser des clés RSA de 2048 bits.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués.

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans la plateforme sous-jacente déjà certifiée par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme sous-jacente intitulée « carte à puce ID-One Cosmo V7.0-a en configuration Large Dual, Large et Standard Dual » au niveau EAL5 augmenté des composants ADV_IMP.2, ALC_DVS.2, et AVA_VAN.5, conforme au profil de protection [PP/0304]. Cette plateforme a été certifiée par l'ANSSI (cf. [ANSSI-CC-2009_36]).

Par ailleurs, l'évaluation a également réutilisé les résultats de l'évaluation du produit intitulé « carte IDOneClassIC : composant P5CT072VOP masqué par ID-One Cosmo 64 RSA v5.4 et embarquant l'application IDOneClassIC v1.0 », qui a été certifié et maintenu par l'ANSSI (cf. [ANSSI-CC-2007_02-M02]), où l'applet était masquée sur une autre plateforme.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 16 avril 2010, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

L'ANSSI n'a pas réalisé la cotation des mécanismes cryptographiques selon ses référentiels techniques. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Le produit offre un générateur de pseudo-aléas. Ces pseudo-aléas sont obtenus à partir d'un retraitement algorithmique de nature cryptographique de la sortie du générateur d'aléas matériel du composant sous-jacent.

Ce générateur de pseudo-aléas n'a pas été analysé par l'ANSSI selon ses référentiels techniques. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN.5 visé.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que l'applet, d'Oberthur Technologies, ID One Classic v1.01.1 en configuration CNS, Classic ou CIE masquée sur la plateforme, d'Oberthur Technologies, Cosmo v7.0-a Large Dual, Large et Standard Dual sur composants Atmel Secure Microcontroller Solutions, soumise à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

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 4+	Intitulé du composant
ADV 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
AGD 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
ALC 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
	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	**1**	Well-defined development tools
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**	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
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	**2**	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - ID ONE CIE - SECURITY TARGET ; référence 1104711, version 3 ; Oberthur Technologies. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ID ONE CIE ON ID ONE COSMO V7.0-A LARGE, LARGE DUAL AND STANDARD DUAL CONFIGURATIONS - PUBLIC SECURITY TARGET; référence 110 5040, version 1; Oberthur Technologies.
[RTE]	Rapport technique d'évaluation : - Evaluation technical report - Project: ERATO; référence ERA_ETR, version 2; Thales-CEACI.
[CONF]	Liste de configuration du produit : - ERATO - CONFIGURATION LIST ; référence 110 4927, version 3 ; Oberthur Technologies.
[GUIDES]	Guide d'utilisation et d'administration du produit : - ID One CIE – GUIDANCE référence 110 4134, version 2 ; Oberthur Technologies.
[BSI-PP-0005-2002]	*Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001*. Certifié par le BSI sous la référence BSI-PP-0005-2002T.
[BSI-PP-0006-2002]	*Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001*. Certifié par le BSI sous la référence BSI-PP-0006-2002T.
[CNS]	*Carta Nazionale dei Servici – Functional Specification –1.1.2*
[CIE]	*Carta di Identità Electronica - Functional Specification - 2.0*
[ANSSI-CC-2009_36]	Certificat ANSSI délivré le 29 septembre 2009 pour le produit : carte à puce ID-One Cosmo V7.0-a en configuration Large Dual, Large et Standard Dual
[PP/0304]	Profil de protection ANSSI certifié le 30 septembre 2003 sous le titre : *Java Card System - Standard 2.1.1 Configuration Protection Profile – version 1.0b*

[ANSSI-CC-2007_02-M02]	Rapport de maintenance ANSSI délivré le 19 mai 2010 pour le produit intitulé : « Carte IDOneClassIC : ID-One Cosmo 64 RSA v5.4 embarquant l'application IDOneClassIC v1.0 masquée sur composant P5CT072VOP ».

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[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.