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-2012/10

Carte IAS ECC v1.0.1 sur ID-One Cosmo v7.0.1-a : applet (version 3124) masquée sur ID-One Cosmo V7.0.1-a (composant Inside Secure) en configuration Standard et Basic avec correctif 075243

Paris, le 12 juin 2012

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

Patrick Pailloux
[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-2012/10

Nom du produit

Carte IAS ECC v1.0.1 sur ID-One Cosmo v7.0.1-a : applet (version 3124) masquée sur ID-One Cosmo V7.0.1-a (composant Inside Secure) en configuration Standard et Basic avec correctif 075243

Référence/version du produit

Version applet 3124

Version correctif 075243

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 révision 3

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, ATE_DPT.2, AVA_VAN.5

Développeurs

Oberthur Technologies
50 quai Michelet
92300 Levallois-Perret, France

Inside Secure
Maxwell Building – Scottish Enterprise Technology Park - East Kilbride – Glasgow G75 0QF - Ecosse

Commanditaire

Oberthur Technologies
50 quai Michelet
92300 Levallois-Perret, France

Centre d'évaluation

THALES (TCS – CNES)
18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

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 modifié. 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 la « Carte IAS ECC v1.0.1 sur ID-One Cosmo v7.0.1-a : applet (version 3124) masquée sur ID-One Cosmo V7.0.1-a (composant Inside Secure) en configuration Standard et Basic avec correctif 075243 ». L'applet, la plateforme et le correctif sont développés par Oberthur Technologies, le composant est développé par Inside Secure.

La cible d'évaluation (TOE : *Target Of Evaluation* – cible d'évaluation) est un logiciel sécurisé s'exécutant sur un microcontrôleur pouvant être mis, par exemple, dans une carte à puce ou un *inlay*, et destinée à être utilisée dans le cadre de projets mettant en œuvre de la signature électronique. Elle répond aux caractéristiques des dispositifs sécurisés de création de signature électronique (SSCD - *Secure Signature Creation Device*) comme défini dans la directive Européenne 1999/93/CE (Annexe III). Ses fonctionnalités applicatives sont offertes par l'application ID-One IAS-ECC v1.0.1 qui s'exécute sur la plateforme JavaCard fermée d'Oberthur Technologies ID-One Cosmo V7.0.1-a en configuration Standard et Basic avec correctif 075243 sur composant Inside Secure (plateforme certifiée par l'ANSSI, voir [ANSSI-CC-2011_01]).

A ce titre, la TOE est destinée à la réalisation de signatures électroniques avancées, et de signatures électroniques dites « qualifiées » (article 2 & article 5 de la directive Européenne 1999/93/CE).

L'application ID-One IAS-ECC v1.0.1 couvre les domaines de l'identité, de la signature électronique, des services électroniques et du stockage de données ; elle est compatible avec les spécifications [IASECC].

Elle offre les deux principales fonctions attendues des produits SSCD type 2 et type 3 :
- la génération et l'import 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) ;
- la création de signature.

Les fonctionnalités complémentaires notables sont :
- la gestion de plusieurs paires de SCD/SVD ;
- la re-génération et le re-import de SCD/SVD ;
- la configuration du mode de fonctionnement de l'application (par un administrateur ad hoc) ;
- l'authentification et l'établissement de canaux de confiance avec des entités distantes ;
- l'authentification des administrateurs ;
- la protection de l'anonymat et des données échangées ;
- la réalisation de services électroniques ;
- le stockage de données.

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 est conforme aux profils de protection [BSI-PP-0005-2002] – SSCD type 2 - et [BSI-PP-0006-2002] - SSCD type 3. Cette conformité est 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 où la [ST] a été 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 (voir [CONF]).

Le produit permet l'identification de ses constituants. Les éléments identifiant la plateforme sous-jacente sont détaillés dans [ANSSI-CC-2011_01]. Ceux identifiant l'applet et le correctif sont :

- la version de l'applet, qui est obtenue par la commande GET DATA pour le tag (étiquette) DF 66 : DF 66 02 **31 24** ;
- la version du correctif, qui est obtenue par la commande GET DATA pour le tag (étiquette) DF 52 : 04 08 **07 52 43** 00 42 FE 00 F7

1.2.2. Services de sécurité

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

- la partie plateforme sous-jacente (voir [ANSSI-CC-2011_01]) incluant en particulier :
  - les interfaces au service des API dédiées aux applets et l'accès à ces API ;
  - le pare-feu isolant les objets et les applets ;
  - les services standards « GlobalPlatform » comme le canal logique et le protocole de canal sécurisé (SCP01, SCP02), ainsi que le protocole de canal sécurisé propriétaire (SCP03) ;
- l'application ID-One IAS-ECC v1.0.1 (voir [ST] pour plus de détails, notamment les chapitres 2.1.4 et 4.1.2) :
  - SF.PIN_MGT : gestion du PIN permettant d'authentifier le signataire ou l'administrateur ;
  - SF.SIG : fourniture d'une signature électronique conformément aux exigences des profils de protection [BSI-PP-0005-2002] – SSCD type 2 - et [BSI-PP-0006-2002] - SSCD type 3 ;
  - SF.DEV_AUTH : authentification mutuelle et ouverture d'un canal de confiance avec les entités externes (SCA, CGA, SSCD type 1) ; les mécanismes cryptographiques utilisés peuvent alors être de type symétrique ou asymétrique ;
  - SF.ADM_AUTH : authentification externe des administrateurs ; les mécanismes cryptographiques utilisés peuvent alors être de type symétrique ou asymétrique ;

- SF.SM : gestion du canal de confiance avec les entités externes (SCA, CGA, SSCD type 1) assurant l'intégrité, la provenance, la destination et la confidentialité des échanges ;
- SF.KEY_MGT : gestion des clés (SCD, SVD, clés d'authentification et clés dédiées pour les services électroniques) ;
- SF.CONF : gestion de la configuration de la TOE (choix du lieu de hachage, du type de cryptographie pour l'authentification, du type de protocole d'échange) ;
- SF.ESERVICE : réalisation de services électroniques (authentification client/serveur, déchiffrement de clés de chiffrement, vérification de certificats) ;
- SF.SAFESTATE_MGT : garantie d'états internes sûrs ;
- SF.PHYS : protection contre les attaques physiques.

1.2.3. Architecture

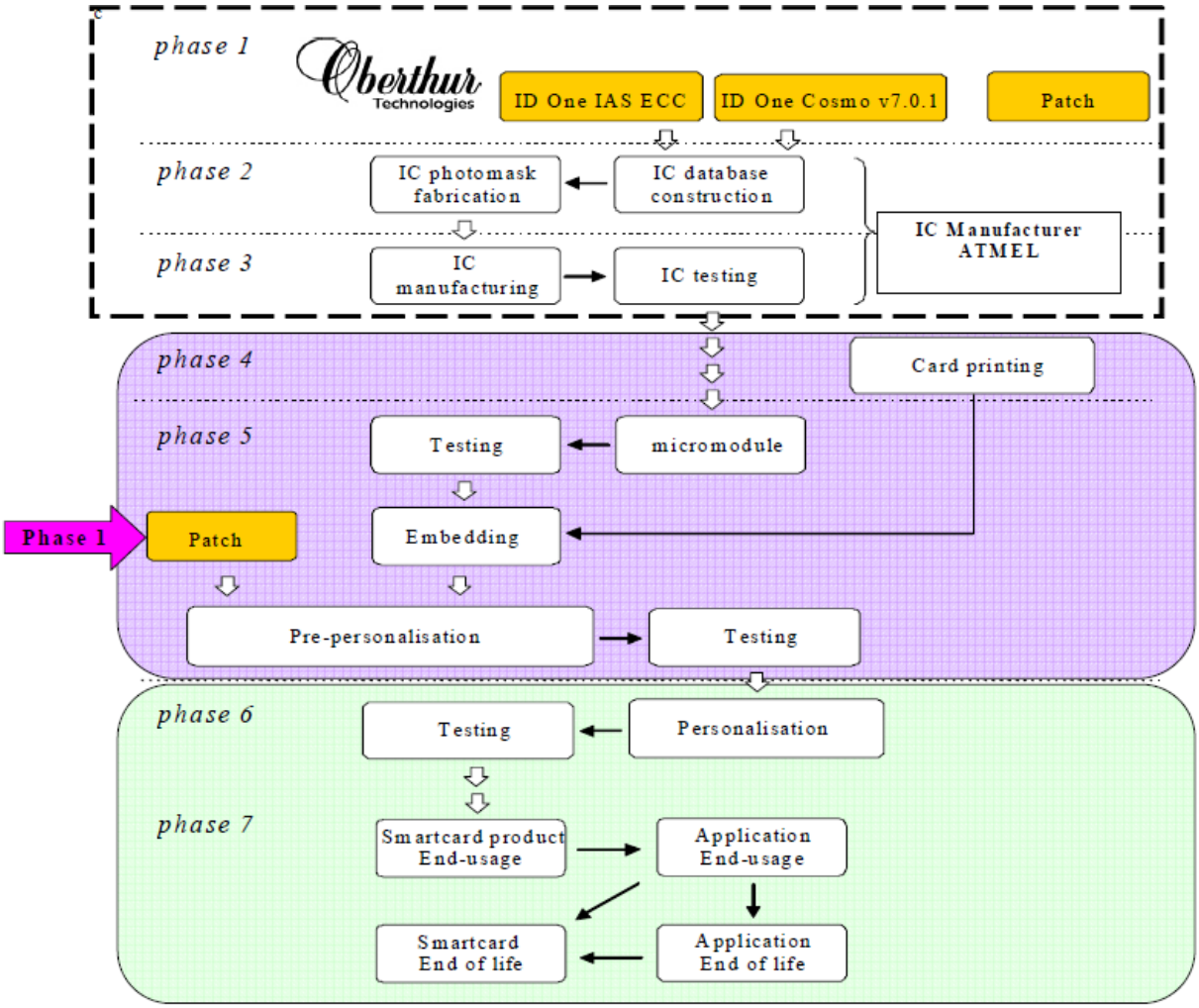
Le produit comprend :

- en mémoire ROM, l'applet SSCD nommée ID-One IAS-ECC v1.0.1, version 3124 ;
- en mémoire ROM, la plateforme nommée ID-One Cosmo V7.0.1-a sous-jacente (dont le détail des blocs est donné dans [ANSSI-CC-2011_01]) ;
- en mémoire EEPROM, le correctif 075243 ;
- le composant sous-jacent correspondant à la plateforme : AT90SC 28872RCU Rev G (configuration Standard) et AT90SC 28848RCU Rev G (configuration Basic).

Le code de l'applet, masqué dans le composant, est interprété par la machine virtuelle de la plateforme JavaCard fermée.

1.2.4. Cycle de vie

Le cycle de vie du produit comporte sept étapes et est résumé dans la figure suivante :



Le point de livraison est situé en phase 3.

Toutes les étapes qui précèdent ce point de livraison ont été couvertes (au titre d'ALC) :

- par la présente évaluation : cela concerne la phase 1 où s'effectuent la conception et le développement de l'applet, de la plateforme et du correctif ;
- par l'évaluation du composant sous-jacent : cela concerne les phases 2 et 3 où le composant est fabriqué et où le masquage de la plateforme et de l'applet est réalisé.

Les phases 4 à 6 ont été prises en compte durant l'évaluation au travers des guides de la plateforme et de l'applet (au titre d'AGD).

En particulier, ces guides détaillent la procédure de transfert sécurisé du correctif depuis la phase 1, où il est développé, vers la phase 5, où il est chargé. Le correctif doit être :

- protégé en confidentialité et en intégrité sur le site de développement, en utilisant des mécanismes techniques connus du produit ;
- chargé ainsi protégé dans le produit.

Le produit offre par ailleurs un mécanisme d'autoprotection depuis sa sortie de la phase 3.

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 :

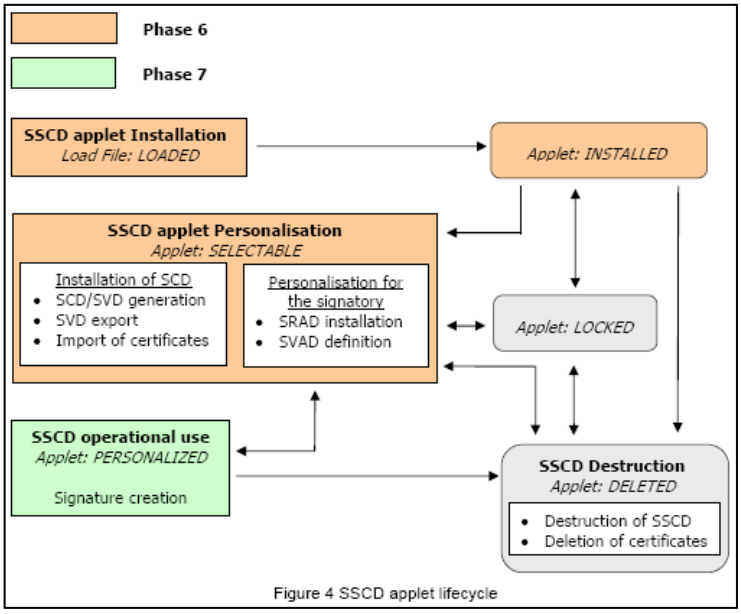


Figure 4 SSCD applet lifecycle

Les tests ont porté sur les fonctionnalités du produit disponibles en phase opérationnelle (au titre d'ATE et d'AVA).

Le produit a été développé sur les sites suivants :

Oberthur Technologies – Levallois (pour la phase 1)

50 quai Michelet
92300 Levallois-Perret
France

Oberthur Technologies – Nanterre (pour la phase 1)

71-73, rue des Hautes Pâtures
92726 Nanterre
France

Oberthur Technologies – Pessac (pour la phase 1)

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

La plateforme sous-jacente ID-One Cosmo V7.0.1-a a été développée et fabriquée par Oberthur Technologies et Inside Secure sur leurs sites respectifs (voir [ANSSI-CC-2011_01]).

Pour l'évaluation, l'évaluateur a considéré quatre types d'administrateurs du produit :

- le **pré-personnalisateur de l'application** intervenant en phase de pré-personnalisation (phase 5) du produit ; il est en particulier en charge du chargement du correctif sur le produit ;
- le **personnalisateur de l'application** intervenant en phase de personnalisation (phase 6) du produit ; il est en charge de sa personnalisation ainsi que des autres fonctions d'administration telles que :
  - personnalisation du RAD (*Reference Authentication Data*, soit le PIN stocké) ;
  - génération ou import du SCD ;
  - export du SVD ;
  - génération, import ou export des clés d'authentification et de services électroniques ;
  - gestion des verrous applicatifs (choix du lieu de hashage, du type de cryptographie pour l'authentification, du type de protocole d'échange) ;
  - identification de la version de l'application ID-One IAS-ECC v1.0.1 ;
  - passage de la TOE en phase d'utilisation ;
- l'**administrateur** intervenant en phase d'utilisation (phase 7) du produit ; il est en charge de sa personnalisation ainsi que des autres fonctions d'administration telles que :
  - personnalisation du RAD ;
  - génération ou import du SCD ;
  - export du SVD ;
  - génération, import ou export des clés d'authentification et de services électroniques ;
- l'**administrateur de la TOE**, appelé « *TOE_Administrator* » dans [ST], intervenant en phase d'utilisation du produit (phase 7) ; il est en charge en charge de la gestion de la configuration des verrous applicatifs et il possède les droits pour obtenir la version de l'application ID-One IAS-ECC v1.0.1.

L'évaluateur a considéré comme utilisateur du produit son **détenteur final**, c'est-à-dire celui disposant des secrets lui permettant d'effectuer les opérations de signatures avec la carte. Il peut, en phase d'utilisation :

- modifier le RAD ;
- générer ou importer le SCD ;
- exporter le SVD ;
- réaliser des services électroniques ;
- générer, importer et exporter les clés d'authentification et de services électroniques.

1.2.5. Configuration évaluée

Le certificat porte sur le produit tel que décrit plus haut au chapitre « *1.2.3 Architecture* » et configuré conformément aux [GUIDES], la plateforme JavaCard sous-jacente étant configurée en mode « fermée » au sens de JavaCard (aucune autre applet, autre que celle SSCD et dont la version est 3124, n'est donc présente dans la configuration évaluée).

Les conclusions sur les tests sont basées :

- sur celles acquises lors des précédentes évaluations :
  - des autres variantes du produit (voir [ANSSI-CC-2010_36], [ANSSI-CC-2010_37], [ANSSI-CC-2010_38], [ANSSI-CC-2010_39], [ANSSI-CC-2010_58]) ;
  - des plateformes sous-jacentes à ces autres variantes du produit (voir [ANSSI-CC-2009_36], [ANSSI-CC-2009_46], [ANSSI-CC-2009_47], [ANSSI-CC-2009_48], [ANSSI-CC-2010_40]) ;
  - de la plateforme sous-jacente au présent produit (voir [ANSSI-CC-2011_01]).
- sur celles acquises lors de cette évaluation où des tests spécifiques ont été effectués sur la variante « Standard » du produit. Les échantillons fournis à l'évaluateur ont alors été fabriqués « en mode test » par le développeur. L'évaluateur a vérifié qu'ils correspondaient à la configuration fournie à l'utilisateur final en phase 7 (environnement d'exploitation du produit).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [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. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [CC AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

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 déjà certifiée par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme intitulée « Carte à puce ID-ONE Cosmo V7.0.1-a masquée sur composants standard et basic AT90SC 28872RCU Rev G et AT90SC 28848RCU Rev G » 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 le 3 février 2011 (voir [ANSSI-CC-2011_01]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 2 mars 2012 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

La cotation des mécanismes cryptographiques a été réalisée conformément aux référentiels techniques de l'ANSSI [REF-CRY], [REF-KEY] et [REF-AUT].

L'évaluateur a analysé les résultats des cotations des variantes précédentes du produit (voir [ANSSI-CC-2010_36], [ANSSI-CC-2010_37], [ANSSI-CC-2010_38], [ANSSI-CC-2010_39], [ANSSI-CC-2010_58]) et de la plateforme sous jacente ([ANSSI-CC-2011_01]). Lorsqu'il l'a jugé utile, il a effectué des tests, c'est le cas en particulier pour le générateur d'aléas.

Les résultats ont fait l'objet d'un rapport d'analyse inclus dans le [RTE] (au chapitre « *8 CRYPTOGRAPHIC EXPERTISE* ») et donnent lieu aux conclusions suivantes :

- les mécanismes cryptographiques n'ayant pas changé dans le présent produit, les conclusions des cotations précédentes demeurent identiques (voir chapitre 2.3 des rapports de certification mentionnés plus haut) ;
- les mécanismes analysés sont conformes aux exigences des référentiels techniques de l'ANSSI sous réserve du complet respect des guides (voir [GUIDES] au chapitre 15 pour AGD_PRE et chapitre 11 pour AGD_OPE).

Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable 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 a été analysé en suivant la même méthodologie que celle exposée dans le chapitre précédent relative à la cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI.

Les résultats ont fait l'objet d'un rapport d'analyse incluse dans [RTE] (au « *8.5 ALEA* ») et donnent lieu aux conclusions suivantes :

- le produit composite gardant le même générateur d'aléas que la plateforme sous-jacente, la conclusion indiquée au chapitre 2.4 du rapport de certification [ANSSI-CC-2011_01] de la plateforme sous-jacente demeure valide :
  - la génération de clé (RSA ou courbe elliptiques) doit se faire sous le contrôle de l'utilisateur ;
- ce générateur est conforme aux exigences des référentiels techniques de l'ANSSI sous réserve du complet respect des guides (voir [GUIDES] au chapitre 15 pour AGD_PRE et chapitre 11 pour AGD_OPE).

Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN 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 le produit « Carte IAS ECC v1.0.1 sur ID-One Cosmo v7.0.1-a : applet (version 3124) masquée sur ID-One Cosmo V7.0.1-a (composant Inside Secure) en configuration Standard et Basic avec correctif 075243 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté de ALC_DVS.2, ATE_DPT.2 et AVA_VAN.5.

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, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- ne pas utiliser le canal sécurisé SCP03, mais seulement SCP01 et SCP02 (comme spécifié au chapitre 4 du guide de préparation, référence 110 5535, version 3) ;
- appliquer les mesures données au chapitre 2.3 du présent rapport.

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'Autriche, l'Espagne, la Finlande, la France, l'Italie, 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 procedures
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 configuration management 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_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ASE Evaluation de la cible de sécurité	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**	1	**3**	3	**4**	**2**	Security enforcing modules
	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 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 : - Euterpe on Terpsichore A - Security target, référence 110 5534, version 5, Oberthur Technologies. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Euterpe on Terpsichore - IAS ECC v1.0.1 on ID-One Cosmo V7.0.1-a - Public Security target, référence 110 5598, version 3, Oberthur Technologies.
[RTE]	Rapport technique d'évaluation : - Evaluation technical report - Project: EUTERPEonTERPSICHORE A, référence EUTTA_ETR, version 5, THALES (TCS – CNES).
[CONF]	Liste de configuration du produit : - Euterpe on Terpsichore A - Configuration List, référence 110 5533, version 4, Oberthur Technologies.
[GUIDES]	Guide de préparation du produit : - Euterpe on Terpsichore A – AGD_PRE, référence 110 5535, version 3, Oberthur Technologies. Guide d'opération du produit : - Euterpe on Terpsichore A – AGD_OPE, référence 110 5536, version 2, Oberthur Technologies.
[ANSSI-CC-2011_01]	Certificat ANSSI délivré le 3 février 2011 pour le produit : « Carte à puce ID-ONE Cosmo V7.0.1-a masquée sur composants standard et basic AT90SC 28872RCU Rev G et AT90SC 28848RCU Rev G ».
[IASECC]	Spécifications IAS ECC v1.0.1 : EUROPEAN CARD FOR e-SERVICES AND NATIONAL e-ID APPLICATIONS - IAS ECC v1.0.1 – GIXEL – 21/03/2008: http://www.gixel.fr/includes/cms/_contenus/bibliotheque/file/CAP%20/IAS%20ECC%20v1_0_1UK.pdf
[PP/0304]	Profile de protection SUN Java Card™ System Protection Profile Collection, août 2003, version 1.0b. *Certifié par l'ANSSI sous la référence PP/0304.*

[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.
[ANSSI-CC-2010_36]	Certificat ANSSI délivré le 29 juin 2010 pour le produit : 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]	Certificat ANSSI délivré le 29 juin 2010 pour le produit: 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]	Certificat ANSSI délivré le 29 juin 2010 pour le produit : 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]	Certificat ANSSI délivré le 29 juin 2010 pour le produit : 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-2010_58]	Certificat ANSSI délivré le 1er octobre 2010 pour le produit : carte IAS ECC v1.0.1 sur ID-One Cosmo v7.0.1-n : applet version 1121, masquée sur ID-One Cosmo V7.0.1-n (composant NXP) en configuration Standard dual, Standard ou Basic dual.

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié 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.

[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir 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 du 24 octobre 2008 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr.
[REF-AUT]	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr.