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-2013/70

Carte IAS ECC v1.0.1 : applet version 6179 sur ID-One Cosmo v7.0.1-n R2.0, masquée sur composants NXP P5CC081 et P5CD081, en configuration Standard ou Standard Dual

Paris, le 14 février 2014

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

[Original signé]
Patrick Pailloux

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-2013/70

Nom du produit

Carte IAS ECC v1.0.1 : applet version 6179 sur ID-One Cosmo v7.0.1-n R2.0, masquée sur composants NXP P5CC081 et P5CD081, en configuration Standard ou Standard Dual

Référence/version du produit

Applet version 6179

Plateforme Cosmo v7.0.1-n R2.0

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 4

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur(s)

Oberthur Technologies
420 rue d'Estienne d'Orves, CS 40008
92705 Colombes Cedex, France

NXP Semiconductors GmbH
Stresemannallee 101
22529 Hamburg, Allemagne

Commanditaire

Oberthur Technologies
420 rue d'Estienne d'Orves, CS 40008
92705 Colombes Cedex

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 : applet version 6179 sur ID-One Cosmo v7.0.1-n R2.0, masquée sur composants NXP P5CC081 et P5CD081, en configuration Standard ou Standard Dual ». L'applet ainsi que la plateforme sont développées par Oberthur Technologies. Le composant est développé par NXP.

La cible d'évaluation (Target of Evaluation – TOE) est un logiciel sécurisé s'exécutant sur un microcontrôleur et pouvant être embarquée dans une carte à puce.

La TOE est destinée à être utilisée comme dispositif de création de signature électronique (SSCD – *Secure Signature Creation Device*) en conformité avec la directive européenne 1999/93/CE. A ce titre elle permet de réaliser des signatures électroniques avancées, et des signatures électroniques dites « qualifiées » (articles 2 et 5 de la directive précitée).

L'application IAS ECC v1.0.1 offre les deux principales fonctions attendues des produits SSCD type 2 et type 3 :
- génération et import de SCD[1]/SVD[2] ;
- création de signature.

Les autres fonctionnalités notables sont :
- gestion de plusieurs paires de SCD/SVD ;
- configuration du mode de fonctionnement de l'application (par un administrateur *ad-hoc*) ;
- authentification et établissement de canaux de confiance avec des entités distantes ;
- authentification des administrateurs ;
- protection de l'anonymat et des données échangées lors de l'utilisation en mode sans contact ;
- réalisation de services électroniques tels que : authentification client/serveur, *wraping*/*unwraping*[3] de clés de chiffrement et vérification de certificat ;
- stockage de données.

1.2. Description du produit

1.2.1. Introduction

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 aux profils de protection [BSI-PP-0005-2002] – SSCD Type 2 - et [BSI-PP-0006-2002] – SSCD Type 3. Cette conformité est choisie de

[1] *Signature Creation Data* ou données de création de signature.
[2] *Signature Verification Data* ou données de vérification de signature.
[3] Encapsulation et décapsulation de clés.

type démontrable par le développeur, les Critères Communs ayant évolué entre la rédaction des profils de protection - en CCv2.1 - et celle de la [ST] - écrite en CCv3.1 [CC].

1.2.2. 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]) :

- commande GET DATA pour l'application IAS ECC avec le tag (étiquette) DF66 : la valeur de retour doit être `DF66 02 61 79`, où **6179** désigne la version de l'applet ;
- commande GET DATA pour la plateforme ID-One Cosmo avec le tag DF50 : la valeur de retour doit contenir la sous-chaîne `DF 52 xx 01 01 1y 02 02 00 48 03 02 71 01 04 00`, où :
  - le sous-tag `01` vaut **`1F`** (configuration Standard Dual sur P5CD081) ou **`1A`** (configuration Standard sur P5CC081) ;
  - le sous-tag `03` vaut **`71 01`** pour la plateforme ID-One Cosmo v7.0.1-n R2.0 ;
  - le sous-tag `04` vaut **`00`** (pas de patch) ;
  - **`xx`** indique la longueur de la valeur de retour en octets.

Une autre application (CPS2ter) ne faisant pas partie de la TOE peut être présente sur la carte qui fait l'objet du présent certificat. Cette application a été prise en compte par l'évaluateur pour ses tests.
Elle peut être identifiée à l'aide de la commande GET DATA avec le tag DF66 : la valeur de retour doit être `DF66 02 01 99`.

La plateforme se trouve en configuration fermée à l'issue de l'étape de pré-personnalisation (phase 5 du cycle de vie).

1.2.3. Services de sécurité

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

- la partie plateforme sous-jacente incluant en particulier :
  - les interfaces au service des API dédiées aux applets et l'accès à ces API ;
  - le pare-feu isolant les objets ou les applets ;
  - les services standards « *GlobalPlatform* » comme le canal logique et le protocole de canal sécurisé (SCP01, SCP02)[1] ;
- l'application ID-One IAS-ECC v1.0.1 (cf. [ST] pour plus de détails, notamment les §2.1.4 et § 4.1.2) :
  - SF.PIN_MGT : gestion du PIN afin d'authentifier le signataire ou l'administrateur ;

[1] Le protocole de canal sécurisé propriétaire (SCP03), conformément aux guides, ne doit pas être utilisé.

- 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.EAVESDROPPING_PROTECTION : protection contre la capture au vol de données sensibles échangées en mode sans contact ;
- SF.SAFESTATE_MGT : garantie d'états internes sûrs ;
- SF.PHYS : protection contre les attaques physiques.

1.2.4. Architecture

Le produit est constitué de :

- l'applet SSCD nommée ID-One IAS-ECC v1.0.1, version 6179 ;
- la plateforme nommée ID-One Cosmo V7.0.1-n R2.0 sous-jacente ;
- le composant sous-jacent correspondant à la plateforme, soit P5CD081 V1A ou P5CC081 V1A.

La figure suivante illustre cette architecture.

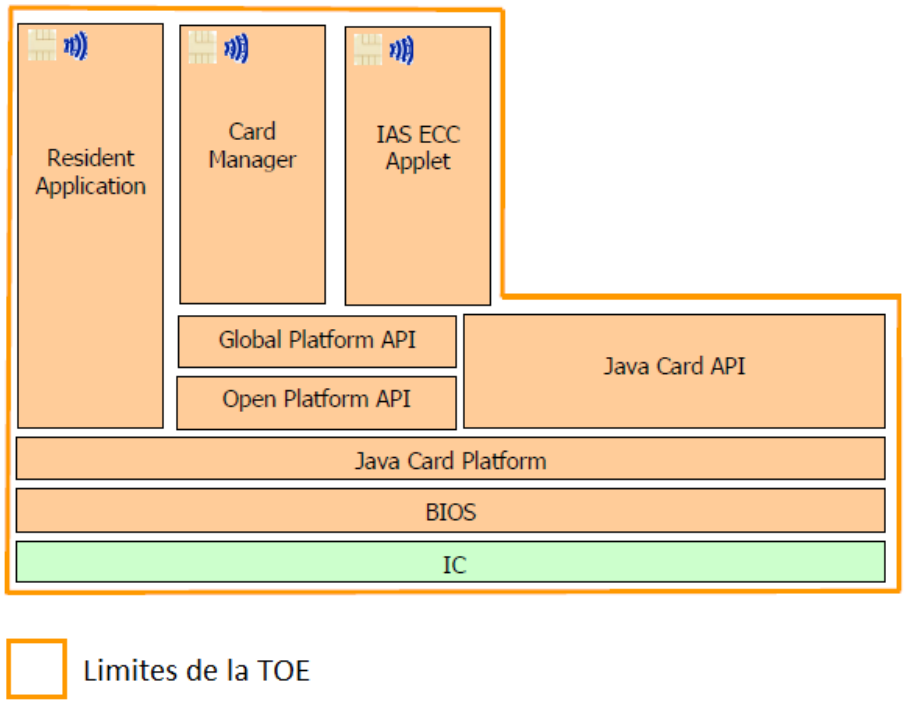

Figure 1 : Architecture de la TOE

1.2.5. Cycle de vie

Le cycle de vie du produit comporte sept phases, résumées dans la figure 2.

L'évaluation a couvert la conception et le développement de l'applet qui sont effectués en phase 1, ainsi que les étapes de mise en micromodules, pré-personnalisation et test réalisées en phases 4 et 5.
Les phases 2 et 3, jusqu'à la livraison, ont été couvertes par l'évaluation du composant.
Enfin la phase 6 est 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 en phase 7.

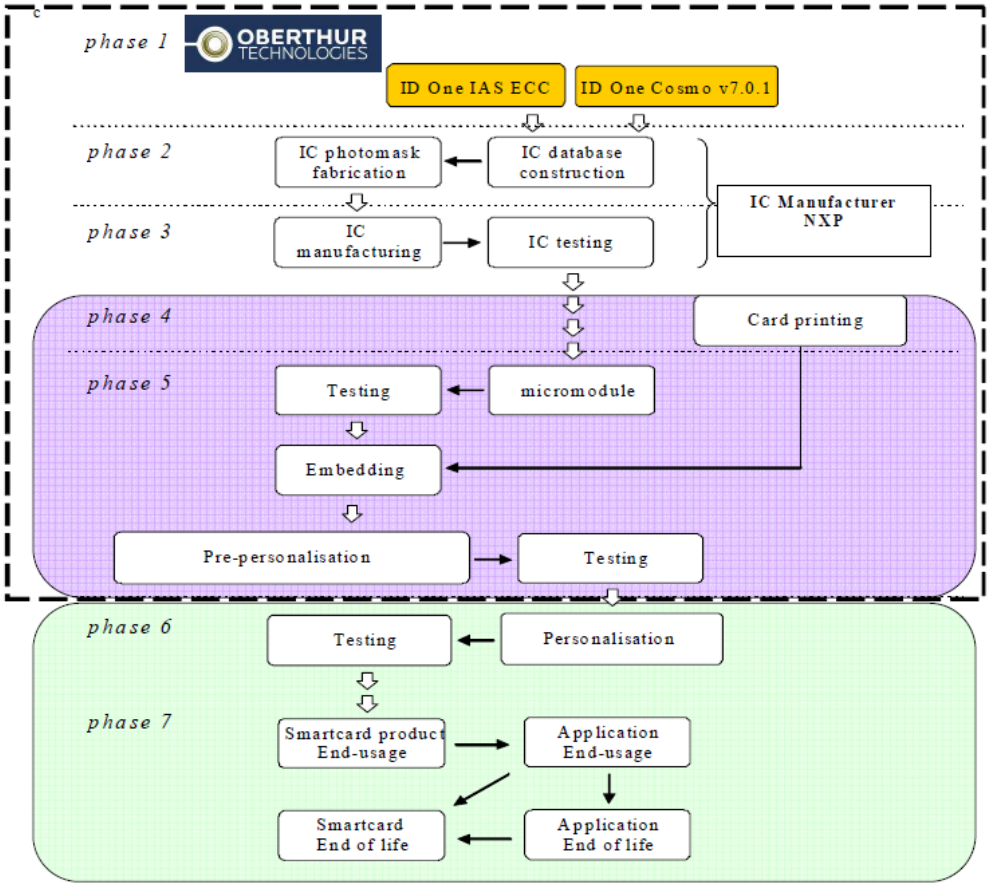

Figure 2 : Cycle de vie de la TOE

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 *Java Card* gérée selon *Global Platform*, le détail de son cycle de vie est schématisé dans la figure suivante :

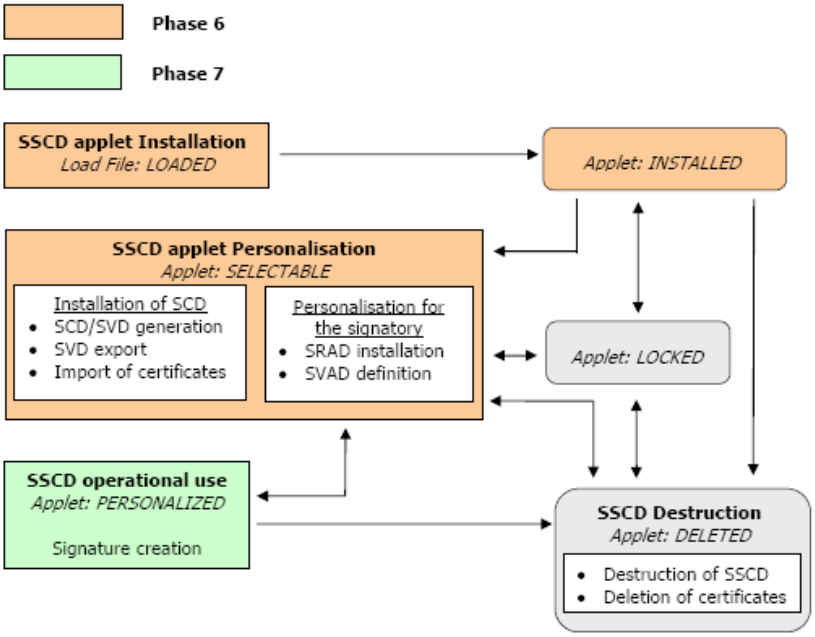

Figure 3 : Cycle de vie de l'applet SSCD

Le produit a été développé sur les sites suivants :

Oberthur Technologies (Phase 1)

420 rue d'Estiennes d'orves
400008 CS
92705 Colombes Cedex
France

Oberthur Technologies (Phase 1)

Parc scientifique UNITEC 1
4 allée du Doyen Georges Brus – Porte 2
33600 Pessac
France

Oberthur Technologies (Phases 4, 5)

Av. d'Helmstedt - BP90308
35503 VITRE Cedex
FRANCE

Le *Card manager* est désactivé en fin de phase 5. La carte passe alors en configuration « fermée » et il n'est plus possible de charger des applications.

Pour l'évaluation, l'évaluateur a considéré trois types d'administrateurs du 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 hachage, du type de cryptographie pour l'authentification, du type de protocole d'échange) ;
    - 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 et déblocage 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 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 les clés de services électroniques.

1.2.6. Configuration évaluée

Le certificat porte sur le produit tel que décrit plus haut au paragraphe 1.2.3 Architecture et configuré conformément aux [GUIDES].

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [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 [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG 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 le microcontrôleur déjà certifié par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation des microcontrôleurs NXP P5CD081 et P5CC081 au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conformes au profil de protection [PP0035]. Ces microcontrôleurs ont été initialement certifiés le 10 novembre 2009 sous la référence BSI-DSZ-CC-0555-2009.

Le niveau de résistance des microcontrôleurs a été confirmé le 12 juin 2013 dans le cadre d'une réévaluation sous la référence BSI-DSZ-CC-0857-2013.

L'évaluation de l'applet n'a pas été réalisée en composition sur la plateforme au sens des CC, mais l'évaluateur a considéré les fonctionnalités de la plateforme utilisées par l'applet IAS ECC pour ses travaux.
L'évaluation s'appuie sur les résultats d'évaluation des produits certifiés sous la référence [ANSSI-CC-2010/58] et [ANSSI-CC-2010/40].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 12 septembre 2013, 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. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations suivantes doivent être appliquées :

- des clés RSA de taille inférieure à 2048 bits ne doivent pas être utilisées ;
- la fonction SHA-1 ne doit pas être utilisée pour la création de signatures ;

- le mécanisme d'authentification symétrique basé sur l'algorithme 3DES-CBC doit être utilisé uniquement avec des aléas de taille au moins 8 octets, et 2^{27} authentifications au maximum doivent être effectuées avec la même clé ;
- l'algorithme de MAC[1] DES-CBC-MAC ne doit pas être utilisé pour calculer plus de 2^{27} MAC avec la même clé ;
- l'échange de clés *Diffie-Hellman* dans Z/pZ ne doit pas être utilisé pour des valeurs de p de taille inférieure à 2048 bits ;
- l'échange de clés *Diffie-Hellman* dans le corps des entiers modulo p utilisant des sous-groupes dont l'ordre est multiple d'un nombre premier p ne doit pas être utilisé pour des valeurs de p de taille inférieure à 200 bits ;
- le schéma de signature RSA PKCS#1v1.5 utilisé avec la fonction SHA-256 doit utiliser des clés RSA de taille au moins 2048 bits et dédiées exclusivement à cet usage.

Enfin, les mécanismes suivants ne sont pas reconnus conformes au référentiel cryptographique de l'ANSSI ([REF]) :

- le schéma de signature PKCS#1v1.5 pour l'authentification client/serveur s'il est utilisé sans hachage pour la signature de données dont la taille atteint ou dépasse un tiers de celle du module ;
- le mécanisme RSA-PKCS#1v1.5 pour le déchiffrement de clés symétriques chiffrées à l'aide d'une clé asymétrique.

Dans le cadre du processus de qualification renforcée, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI [EXP-CRY]. Ces 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 si les recommandations contenues dans [GUIDES] sont correctement appliquées.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [BSI-DSZ-0857-2013]).
Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI ([REF]), la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.
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.

[1] *Message Authentication Code*, ou code d'authentification de message.

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 : applet version 6179 sur ID-One Cosmo v7.0.1-n R2.0, masquée sur composants NXP P5CC081 et P5CD081, en configuration Standard ou Standard Dual » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants ALC_DVS.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].

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 :

[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.

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[1], 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 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 TSF
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	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 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
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**	**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**	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 (NXP) Security target*, version 8, référence : FQR : 110 5165, Oberthur Technologies. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *IAS ECC v1.0.1 On ID-OneTM Cosmo V7.0.1-n R2 Card (Standard and standard Dual) Public Security target*, version 1, référence : FQR 110 6731 Ed1, Oberthur Technologies.
[RTE]	Rapport technique d'évaluation : - *Evaluation technical report. Project : EUTERPEandMELPOMENEonTERPSICHORE3*, version 2.0, référence : TERP3_ETR / Revision: 2.0, THALES Communications & Security.
[BSI-DSZ-CC-0555-2009]	*NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A each with IC dedicated Software*, référence : BSI-DSZ-CC-0555-2009, 10 novembre 2009, BSI.
[BSI-DSZ-CC-0857-2013]	*NXP Secure Smart Card Controllers P5CD016/021/041/051 and P5Cx081 V1A/V1A(s)*, référence : BSI-DSZ-CC-0857-2013, 12 juin 2013, BSI.
[ANSSI-CC-2010-58]	Rapport de certification ANSSI-CC-2010/58 Carte IAS ECC v1.0.1 sur ID-One Cosmo v7.0.1-n : applet version 1121, masquée sur IDOne Cosmo V7.0.1-n (composant NXP) en configuration Standard dual, Standard ou Basic dual, référence : ANSSI-CC-2010/58, 1er octobre 2010, ANSSI.
[ANSSI-CC-2010-40]	Rapport de certification ANSSI-CC-2010/40 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), référence : ANSSI-CC-2010/40, 6 juillet 2010, ANSSI.
[ANA-CRY]	Cotation de mécanismes cryptographiques - Qualification EUTERPE, référence : N°722/ANSSI/ACE/LCC, ANSSI.
[EXP-CRY]	Evaluation technical report. Project : EUTERPEandMELPOMENEonTERPSICHORE3, version 2.0, référence : TERP3_ETR / Revision: 2.0, THALES Communications & Security.
[CONF]	Liste de configuration du produit : - *Euterpe on Terpsichore N3 Configuration List*, version 2, référence : FQR : 110 6616, Oberthur Technologies.

[GUIDES]	Guides d'installation du produit : - *ID-One Cosmo V7.0.1-n R2.0 Pre-Perso Guide*, version 2, référence : FQR 110 6407, Oberthur Technologies ; - *ID-One Cosmo V7.0.1-n R2.0 Reference Guide*, version 2, référence : FQR 110 6408, Oberthur Technologies ; Guide d'administration du produit : - *Euterpe on Terpsichore AGD_PRE*, version 7, référence : FQR : 110 5171, Oberthur Technologies. Guide d'utilisation du produit : - *Euterpe on Terpsichore AGD_OPE*, version 5, référence : FQR : 110 5170, Oberthur Technologies.
[PP0005]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0005-2002T.*
[PP0006]	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.*
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*

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, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, révision 4, ref CCMB-2012-09-004.
[JIWG IC]*	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009.
[JIWG AP]*	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, January 2013.
[COMP]*	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.
[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]	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 (RGS_B_1), voir www.ssi.gouv.fr.
	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 (RGS_B_2), voir www.ssi.gouv.fr.
	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 (RGS_B_3), voir www.ssi.gouv.fr.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.