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-2011/64

Carte à puce ID-ONE Cosmo V7.0.1-n, avec correctif 077121, masquée sur composants NXP : P5CD145 V0A (Large Dual), P5CC145 V0A (Large), P5CD128 V0A (Large Dual) et P5CC128 V0A (Large)

Paris, le 14 décembre 2011

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

Patrick Pailloux
[ORIGINAL SIGNE]

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-2011/64

Nom du produit

Carte à puce ID-ONE Cosmo V7.0.1-n, avec correctif 077121, masquée sur composants NXP P5CD145 V0A (Large Dual), P5CC145 V0A (Large), P5CD128 V0A (Large Dual) et P5CC128 V0A (Large)

Référence/version du produit

Version plateforme Java Card correspondant à toutes les configurations : 7.0.1-n

Version du correctif correspondant à toutes les configurations : 077121

Conformité à un profil de protection

[PP/0304]

Java Card System - Standard 2.1.1 Configuration Protection Profile – version 1.0b, August 2003, certifié par l'ANSSI

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

Oberthur Technologies
50 quai Michelet
92300 Levallois-Perret, France

NXP Semiconductors GmbH
Stresemannallee 101
D-22502 Hamburg, Germany

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.

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 à puce ID-One Cosmo V7.0.1-n, avec correctif 077121, plate-forme Java Card ouverte, développée par Oberthur Technologies :

- compatible avec les spécifications de Java Card 2.2.2 et de VISA GlobalPlatform 2.1.1 ;
- masquée sur des variantes (par la taille mémoire et les interfaces offertes) d'une même famille de composants développées par NXP.

Ces différentes variantes du produit sont récapitulées dans le tableau ci-après :

Dénomination de la variante du produit	Version de la plate-forme Java Card	Version du correctif de la plate-forme Java Card	Référence de la variante du composant sur lequel le logiciel est masqué	Référence masque identifiant la variante du composant
Large Dual	V7.0.1-n	077121	P5CD145 V0A	18 01 1D
Large	V7.0.1-n	077121	P5CC145 V0A	18 01 1E
Large Dual	V7.0.1-n	077121	P5CD128 V0A	18 01 3A
Large	V7.0.1-n	077121	P5CC128 V0A	18 01 3B

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 au profil de protection [PP/0304]

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 d'identification renvoyés par le produit en réponse à la commande « GET DATA » avec les tag 50 et 52 (voir [GUIDES], au « §10.1 TOE Identification du guide de préparation du produit »).

Ainsi pour la variante « Large dual » du produit sur composant P5CD145 V0A, on obtient les réponses suivantes :
- commande : 80 CA DF 50 00
- réponse : DF 50 14 00 00 21 77 05 91 57 80 00 14 31 02 66 41 21 17 **4B** 30 30 38

La valeur du champ « *Device Coding Byte* » DC2, en gras dans la réponse ci-dessus, identifie le composant P5CD0145 V0A, qui est bien le composant sous-jacent de cette variante du produit. L'ensemble des valeurs possibles du champ DC2 sont données par le tableau suivant :

Valeur du champ DC2	Référence du composant
48	P5CD128 V0A
49	P5CC128 V0A
4B	P5CD145 V0A
4A	P5CC145 V0A

- commande : 80 CA DF 52 00
- réponse : DF 52 4A 01 01 **1D** 02 02 04 90 03 02 **18 01** 04 06 **07 71 21** 01 49 CE 05 01 00 06 17 83 00 00 3F 3F 00 F9 04 00 00 00 01 00 00 00 00 00 FF FF FF 00 00 00 07 01 0F 08 0B 00 31 C0 64 1D 18 01 00 00 90 00 09 09 41 E8 01 F7 C0 03 CA E9 F2

Conformément au tableau donné au « §1.1 Présentation du produit », les valeurs (**18 01 1D**) et (**07 71 21**), en gras dans la réponse ci-dessus, correspondent à la variante « Large Dual » du produit sur composant P5CD145 V0A.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- les services de pré-personnalisation de la carte ;
- la personnalisation des applets avec la faculté de la charger, de l'installer, de la supprimer, grâce au gestionnaire GlobalPlatform Card Manager et au contrôleur de domaine de sécurité associé et du mécanisme DAP (*Data Authentication Pattern* - reconnaissance des données d'authentification) ;
- les interfaces au service des API dédiées aux applets et l'accès à ces API ;
- la gestion de GlobalPlatform ainsi que des clés de signature ;
- 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), ainsi que le protocole de canal sécurisé propriétaire (SCP03).

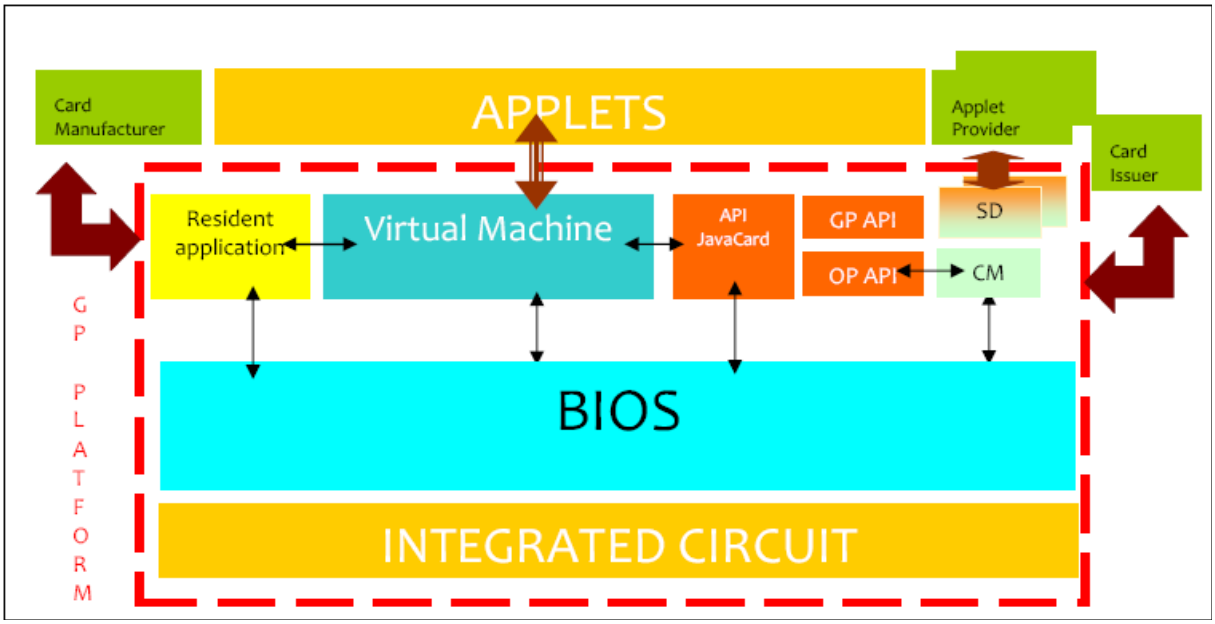
Une liste plus détaillée des services de sécurité est donnée dans [ST].

1.2.3. Architecture

Le produit est constitué :

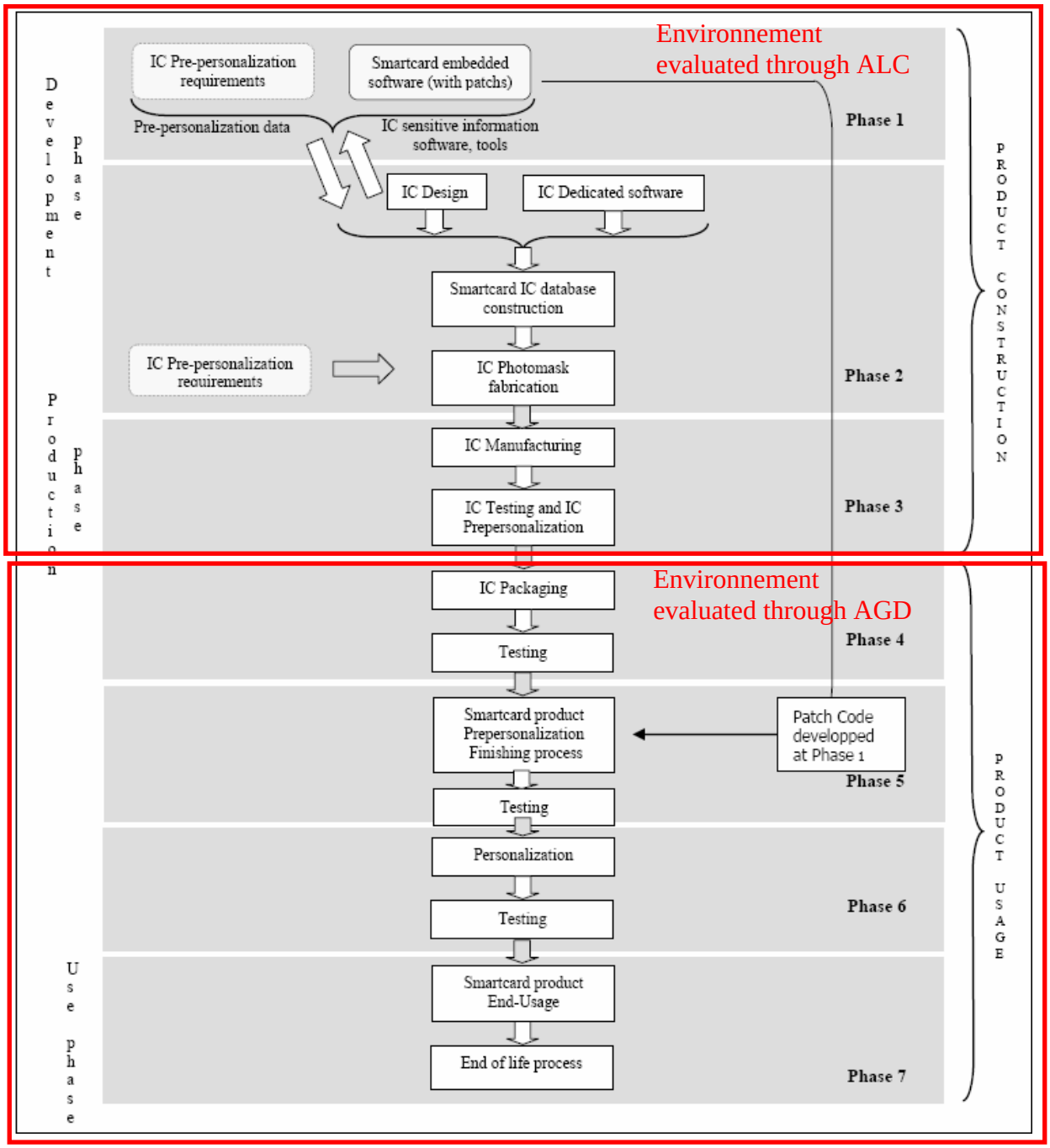
- du microcontrôleur, offrant les fonctionnalités matérielles, et de sa bibliothèque cryptographique ToolBox ;
- du BIOS assurant l'interface entre les applications natives, comme la machine virtuelle (*Virtual Machine*), et le matériel ;
- de la machine virtuelle interprétant le *byte code* des applets Java Card ;
- d'API offrant les interfaces de programmes aux applications comme la génération de clés, la négociation de clés, la signature, le chiffrement de messages ainsi que d'autres interfaces de programmes aux applications propriétaires (OCS API) ;
- de Common Open Platform, constitué du gestionnaire de la carte (*Card Manager*) et des API OPSystem and GPSystems ; il est implémenté en code natif et en Java (son *byte code* se trouve en ROM) ;
- de l'application résidente, en code natif, permettant de recevoir et de distribuer les commandes reçues par la carte.

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 :



L'évaluation a couvert la phase 1 correspondant au développement de la plateforme et de son correctif. La plateforme développée en phase 1 est masquée dans le composant en phases 2 et 3, phases couvertes par l'évaluation du composant. Le correctif développé en phase 1 est transmis et chargé en phase 5 de façon sécurisée grâce à des mesures techniques offertes par la plateforme, évaluées lors de cette évaluation. Les autres phases ont été évaluées au travers des guides du produit.

Le produit évalué correspond à celui livré à l'utilisateur à la phase 7.

La plate-forme a été développée par Oberthur Technologies sur les sites suivants :

Oberthur Technologies - Levallois

50 quai Michelet
92300 Levallois-Perret
France

Oberthur Technologies - Nanterre

71-73, rue des Hautes Pâtures
92726 Nanterre
France

Oberthur Technologies - Bordeaux

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

Le microcontrôleur a été développé et fabriqué par NXP sur ses sites (cf. [BSI-DSZ-CC-0645-2010]), dont le principal est :

NXP Semiconductors GmbH1

Stresemannallee 101
D-22502 Hamburg
Allemagne

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit les rôles *Card Issuer*, *Application Provider*, *Controlling authority* et comme utilisateurs du produit les rôles *Card Manufacturer*, *Card Issuer*, *Application Provider*, *Controlling authority* (cf. [ST] au « §3.6.8 Roles » pour plus de détails).

1.2.5. Configuration évaluée

Le certificat porte sur la plate-forme Java Card seule, telle que présentée plus haut au paragraphe « 1.2.3 Architecture » et configurée conformément au guide de personnalisation (cf. [GUIDES]).

Dans les échantillons utilisés pour les tests, la ROM contenait 2 applications dans un état désactivé : « IAS ECC Java Applet light V1.2 » et « CHV interface ». Elles sont en dehors du périmètre de l'évaluation.

Les tests ont été effectués sur la variante du produit intitulée « Large Dual » sur composant P5CD145 V0A.

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.

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 du microcontrôleur « *NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO and P5CC128V0A, MSO;each including IC Dedicated Software* » au niveau EAL5 augmenté des composants ASE_TSS.2, ALC_DVS.2, et AVA_VAN.5, conforme au profil de protection [PP0035]. Ce microcontrôleur a été certifié par le BSI (cf. [BSI-DSZ-CC-0645-2010]).

Cette évaluation a également pris en compte les résultats de l'évaluation de la version précédente du produit certifié par l'ANSSI (cf. [ANSSI-CC-2010/40]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 18 novembre 2011, 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 selon les référentiels techniques de l'ANSSI [REF-CRY], [REF-KEY] et [REF-AUT] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas du produit était en dehors du périmètre de l'évaluation et n'a pas été analysé.

Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction 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 la « carte à puce ID-ONE Cosmo V7.0.1-n, avec correctif 077121, masquée sur composants NXP P5CD145 V0A (Large Dual), P5CC145 V0A (Large), P5CD128 V0A (Large Dual) et P5CC128 V0A (Large) » soumise à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 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 , 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 :

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 5+	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	5	Complete semiformal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	TSF internal description
	ADV_TDS		1	2	3	4	5	6	4	Semiformal modular design
AGD 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	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			1	1	1	1	2	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	Compliance with implementation standards
ASE 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	2	3	3	4	3	Testing : modular design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing : sample
AVA 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 : - TERPSICHORE - ST ID-ONE Cosmo V7.0.1-n - P5Cx128V0A and P5Cx145V0A, référence FQR: 110 5382, révision 5, 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 COSMO V7.0.1 - TERPSICHORE Security Target Lite for P5Cx128V0A and P5Cx145V0A, - référence FQR 110 5384, révision 3, Oberthur Technologies.
[RTE]	Rapport technique d'évaluation : - Evaluation technical report - Project: TERPSICHORE-N145, référence TERN145_ETR, révision 3.0, THALES-CEACI. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - Evaluation technical report lite - Project: TERPSICHORE-N145, référence TERN145_ETR Lite, révision 3.0, THALES-CEACI.
[CONF]	Liste de configuration du produit : - TERPSICHORE - CONFIGURATION LIST NXP référence FQR 110 4964, révision 8, Oberthur Technologies.
[GUIDES]	Guide de préparation du produit : - ID-One Cosmo V7.0.1 - Pre-Perso Guide, référence FQR 110 4910, révision 5, Oberthur Technologies. Guide d'opération du produit : - ID-One Cosmo V7.0.1 - Reference Guide, - référence FQR 110 4911, révision 4, Oberthur Technologies. Guide d'utilisation du produit : - ID-One Cosmo V7.0.1 - Security recommendations, - référence FQR 110 4912, révision 4, Oberthur Technologies.
[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.*

[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, August 2003. »
[BSI-DSZ-CC-0645-2010]	Certificat délivré par le BSI le 23/07/2010 pour le produit : « *NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO and P5CC128V0A, MSO;each including IC Dedicated Software* »
[ANSSI-CC-2010/40]	Certificat ANSSI délivré le 06/07/2010 pour le produit : « 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) »

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