Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2009/49

Carte à puce ID-One Cosmo V7.0-n en configuration Basic masquée sur composant NXP P5CC037 V0A

Paris, le 19 novembre 2009

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 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-2009/49

Nom du produit

Carte à puce ID-One Cosmo V7.0-n en configuration
Basic masquée sur composant NXP P5CC037 V0A

Référence/version du produit

Version Plate-forme Java Card : 7.0-n

Version patch Optional Code r4.0 Generic : 069774

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

Niveau d'évaluation

EAL5 augmenté

ADV_IMP.2, ALC_DVS.2, AVA_VAN.5

Développeur(s)

Oberthur Technologies[1]
50 quai Michelet
92300 Levallois-Perret, France

NXP Semiconductors GmbH[1]
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.

[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 la carte à puce ID-One Cosmo V7.0-n, 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 composant NXP P5CC037 V0A (sans AES) ;
- patchée par Optional Code r4.0 Generic.

Les caractéristiques du produit sont récapitulées dans le tableau ci-après :

Dénomination du produit	Version de la plate-forme Java Card	Version du patch Optional Code r4.0 Generic	Référence du composant sur lequel le logiciel est masqué	Référence masque identifiant le composant
Basic	7.0-n	069774	P5CC037 V0A	FC10 C6

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 présents dans la réponse que donne le produit suite à la commande GET DATA (cf. [GUIDES]).

Ainsi, sur un produit utilisé lors de l'évaluation, la commande GET DATA pour le tag DF 52 a donné la réponse suivante :

- DF 52 2F 01 01 **C6** 02 02 08 90 03 02 **FC 10** 04 06 **06 97 74 01** E9 0B 05 01 01 06 14 83 00 01 3F 3F FF F9 00 00 00 00 01 00 00 FF 00 FF FF 00 FF 07 01 0F.

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

- le numéro du masque est **FC10 C6** ce qui correspond à ID-One Cosmo V7.0-n Basic (P5CC037 V0A) ;
- le numéro du patch Optional Code r4.0 Generic est **069774** en version **01**.

La commande GET DATA pour le tag DF 50 a donné la réponse suivante :

- DF 50 14 **00 00 08 83 01 91 42 52 00 3A 1D 82 55 42 11 05 37 30 31 30.**

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

- **00 00 08 83** indique le numéro du dé.
- **01** indique le numéro du wafer ;
- **91 42 52 00** indique le numéro du lot ;
- **3A 1D** indique les coordonnées XY du Wafer ;
- **82 55** horodatage ;
- **42** sous indice de la première fonderie ;
- **11 05 37** identifiant du composant (37 correspond à la configuration Basic (P5CC037 V0A)) ;
- **30 31 30** numéro du code ROM.

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).

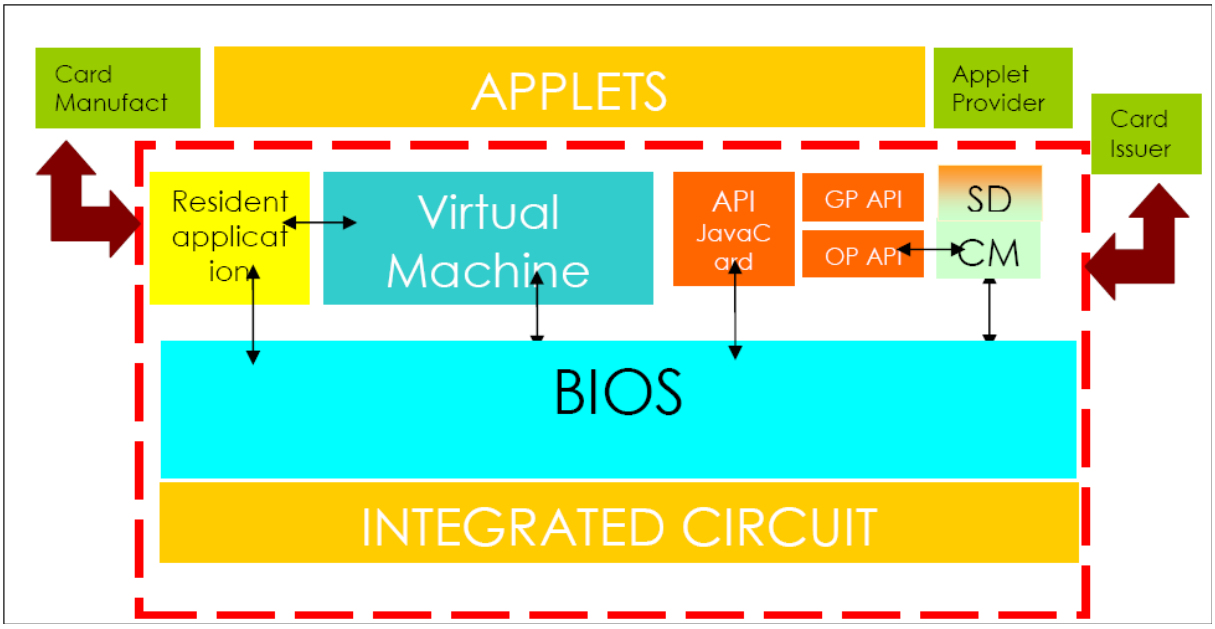
Une liste plus détaillée des services de sécurité est donnée dans [ST].

1.2.3. Architecture

Le produit est constitué :

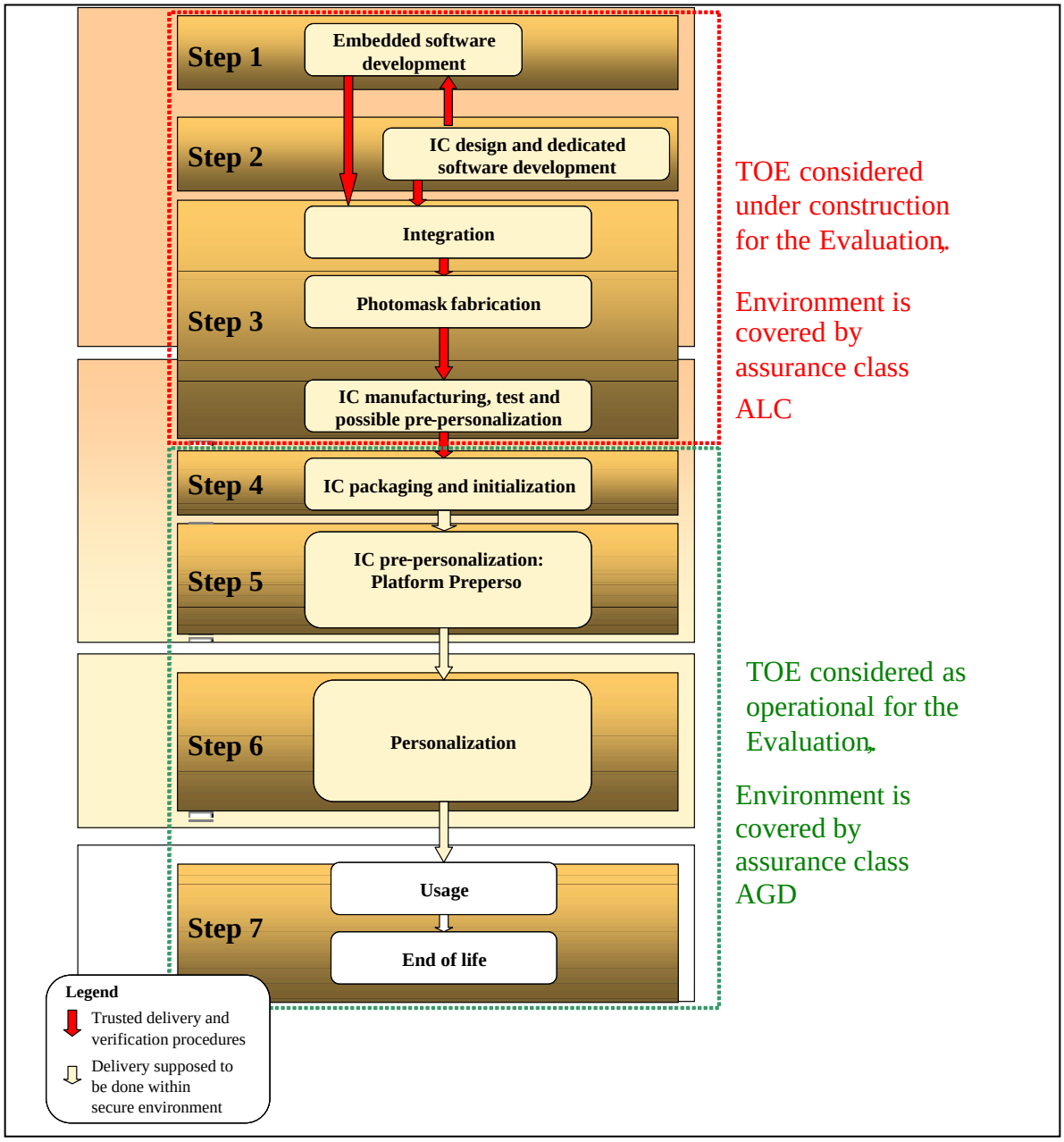
- du microcontrôleur, offrant les fonctionnalités matérielles, et de sa bibliothèque cryptographique ToolBox ;
- du BIOS assurant l'interface entre les applications natives, comme la machine virtuelle (*Virtual Machine*), et le matériel ;
- de la machine virtuelle interprétant le *byte code* des applets 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 carte reçues.

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 conception et le développement de la plate-forme qui sont effectués en étape 1. Les étapes 2 et 3, jusqu'à la livraison, ont été couvertes par l'évaluation du composant. La fin de l'étape 3 et les étapes 4, 5 et 6 sont couvertes par des guides. Le produit évalué correspond à celui livré à l'utilisateur à l'étape 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-0465-2008],), dont le principal est :

NXP Semiconductors GmbH1

Stresemannallee 101
D-22502 Hamburg
Allemagne

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit le pré-personnalisateur, le personnalisateur et le gestionnaire de la carte chargé de l'administration de la carte, et comme utilisateurs du produit les développeurs des applications à charger dans la plate-forme.

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]).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC], 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 de NXP P5CC037 V0A (cf. [BSI-DSZ-CC-0465-2008]), certifié par le BSI, au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP0002].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 6 octobre 2009, 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 n'a pas été réalisée par l'ANSSI.

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-n, décrite au chapitre 1.1 du présent rapport de certification, soumise à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL5 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 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 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 Grèce, 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 semi-formal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**2**	Complete mapping of the implementation representation of the TSF
	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 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	**5**	Development tools 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	**2**	Compliance with implementation standards
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**	**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**	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 COSMO V7.0 - CLIO SECURITY TARGET For NXP Référence FQR: 110 4635 - issue 2 – 15/09/2009 Oberthur Technologies Cible de sécurité pour la composition avec les composants : - ID-ONE COSMO V7.0 - CLIO SECURITY TARGET COMPATIBILITY For NXP IC Référence FQR: 110 4636 - issue 1 – 10/07/2009 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 - CLIO Security Target Lite For NXP Référence FQR: 110 4775 - issue 1 Oberthur Technologies
[RTE]	Rapport technique d'évaluation : - Evaluation technical report - Project: THALIE Référence THA_ETR - révision 2.0 – 06/10/2009 THALES-CEACI Pour le besoin des évaluations en composition avec cette plate-forme, un rapport technique pour la composition a été validé : - Evaluation technical report lite - Project: THALIE ETR LITE for composition Référence THA_ETR Lite – révision 1.0 – 18/09/2009 THALES-CEACI
[CONF]	Liste de configuration du produit - CLIO - CONFIGURATION LIST P5CxYYY Référence FQR : 110 4628 - issue: 4 – 09/16/2009 Oberthur Technologies
[GUIDES]	Guide d'installation du produit : - COP REF V02.05 - PRODUCT GENERATION DESCRIPTION – PGD 068041 00 PGD – issue 1 AB, 13/08/2009 Oberthur Technologies - ID-One Cosmo V7.0-n Applets - PRODUCT GENERATION DESCRIPTION - PGD 069671 00 PGD – issue 1 AA, 05/03/2008 Oberthur Technologies - Optional Code r4.0 Generic on ID-One Cosmo v7.0-n Platform - PRODUCT GENERATION DESCRIPTION - PGD 069774 00 PGD – issue 4 AA, 27/03/2009 Oberthur Technologies Guide d'administration du produit : - ID-One Cosmo V7.0 - Pre-Perso Guide

	FQR : 110 4379 – issue 6, 26/06/2009 Oberthur Technologies - ID-One Cosmo V7.0 - Security recommendations FQR 110 4730 – issue 1, 02/09/2009 Oberthur Technologies Guide d'utilisation du produit : - ID-One Cosmo V7.0 - Reference Guide FQR 110 4483, issue 5 Oberthur Technologies
[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-0465-2008]	Certificat BSI délivré le 20 juin 2008 pour le produit *NXP Secure Smart Card Controller P5CC037VOA with specific IC Dedicated Software*
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001.*

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, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, révision 2, ref CCMB-2007-09-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2008-04-001 version 2.5 revision 1, April 2008.
[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 2.0, April 1999, Management Committee of Agreement Group.