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-2012/71

Cryptosmart card v5.0
sur plateforme Oberthur ID-One Cosmo
v7.0.1-n avec correctif 077121

Paris, le 05 octobre 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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

ANSSI-CC-2012/71

Nom du produit

Cryptosmart card v5.0 sur plateforme Oberthur ID-One Cosmo v7.0.1-n avec correctif 077121

Référence/version du produit

Version 5.0

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, ALC_FLR.3, AVA_VAN.5

Développeurs

ERCOM
6, rue Dewoitine
78140 Velizy
France

Oberthur Technologies
50 quai Michelet
92300 Levallois-Perret
France

NXP Semiconductors
Stresemannallee 101
D-22502 Hamburg
Germany

Commanditaire

ERCOM
6, rue Dewoitine
78140 Velizy
France

Centre d'évaluation

SERMA Technologies
30 avenue Gustave Eiffel
33608 Pessac
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 l'application Java Card « Cryptosmart**,** version 5.0 » développée par ERCOM et installée sur la plateforme ID-One Cosmo d'Oberthur Technologies sur composants NXP.

Ce produit est destiné à être utilisé pour établir un canal sécurisé avec un autre produit utilisant l'application Cryptosmart. Il fournit également plusieurs fonctions cryptographiques et une zone de stockage sécurisée.

1.2. Description du produit

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

1.2.1. Identification du produit

La version certifiée du produit est identifiable par les références suivantes :

	Référence
Application	Cryptosmart applet v5.0 on Oberthur ID-ONE COSMO V7.0.1 (with optional code generic r1.0 ref. 077121) masked on P5CC081 V1A or P5CD041/081 V1A
Plateforme	Carte à puce ID-ONE Cosmo V7.0.1-n, avec correctif 077121, sur composants NXP P5CD081 V1A (Standard Dual), P5CC081 V1A (Standard) et P5CD041 V1A (Basic Dual)
Composant	P5CD081 V1A, P5CC081 V1A ou P5CD041 V1A.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

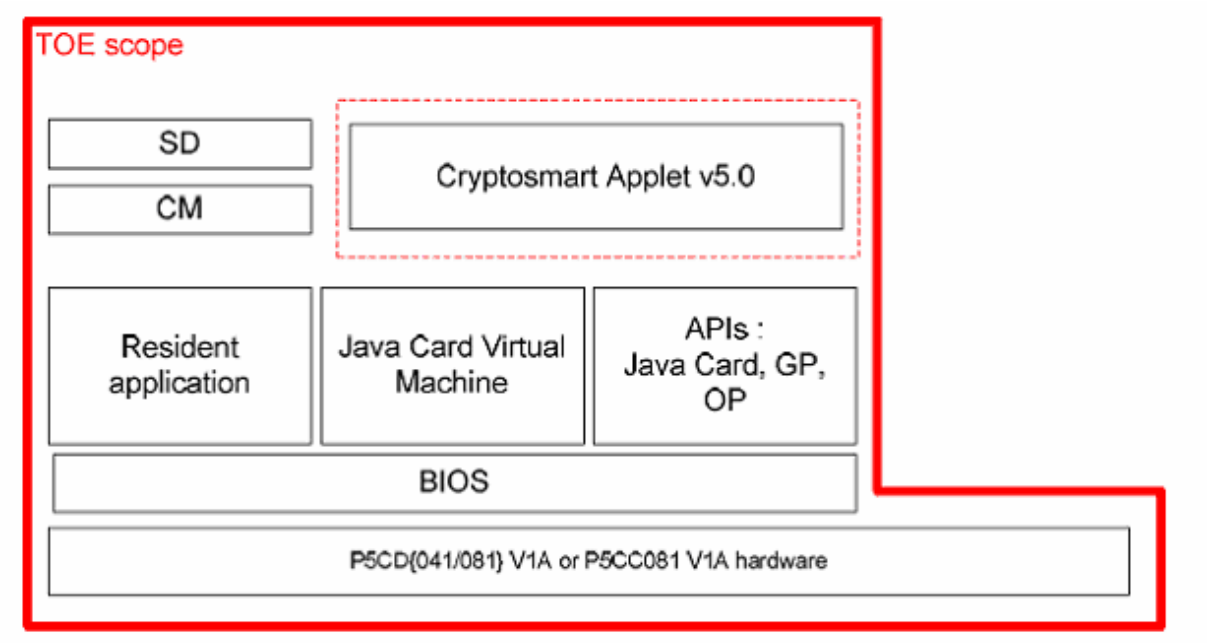
- l'authentification d'une application Cryptosmart distante et négociation d'une clé partagée avec cette dernière ;
- la mise à disposition de fonctions cryptographiques telles que :
  - l'authentification de l'utilisateur ;
  - le stockage de clés sécurisé (pour clés symétriques AES de 256 bits ou clés RSA de 2048 bits) ;
  - l'export de clés sécurisé (pour clés symétriques AES de 256 bits ou clés RSA de 2048 bits) ;
  - un sous-ensemble des fonctionnalités de PKCS#11 ;
  - la génération de clés RSA de 2048 bits ;
  - la génération de clés symétriques AES de 256 bits ;
  - la gestion des propriétés d'extractibilité des clés RSA et des clés symétriques ;
  - la gestion des usages des clés RSA et des clés symétriques ;
  - la dérivation de clés locales de chiffrement ;

- la génération de nombres aléatoires ;
- la mise à disposition d'une zone de stockage sécurisée.

1.2.3. Architecture

Le produit est constitué d'un microcontrôleur (offrant les fonctionnalités matérielles) sur lequel est installé la plateforme ID-One Cosmo. L'application Cryptosmart est chargée sur cette plateforme qui est ensuite verrouillée afin qu'aucune autre application ne puisse être installée.

L'architecture complète de la carte est présentée dans le schéma suivant :



L'évaluation a porté sur l'application Cryptosmart (encadrée en pointillés) en composition sur la plateforme.

1.2.4. Cycle de vie

L'évaluation de la plateforme [ANSSI-CC-2012/30] a couvert les phases de conception, de développement et de chargement de la plateforme (et de son code correctif) jusqu'à la livraison à ERCOM.

La présente évaluation a couvert la conception, le développement et le chargement de l'application Cryptosmart sur la carte et le verrouillage de la plateforme. Ces étapes se déroulent dans les locaux d'ERCOM et correspondent à la phase 6 du cycle de vie de la plateforme décrit au chapitre 1.2 de [ANSSI-CC-2012/30].

Le produit a été développé sur le site suivant :

ERCOM

6, rue Dewoitine
78140 Velizy
France

La plate-forme a été développée par Oberthur Technologies sur les sites suivants (cf. [ANSSI-CC-2012/30]) :

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-0555-2009]), dont le principal est :

NXP Semiconductors GmbH

Stresemannallee 101
D-22502 Hamburg
Allemagne

1.2.5. Configuration évaluée

Le certificat porte sur l'application Cryptosmart v5.0 chargée sur la plate-forme Java Card seule, telle que présentée plus haut au paragraphe « 1.2.3 Architecture » et utilisée et administrée conformément aux guides (cf. [GUIDES]).

Les tests ont été effectués sur une plateforme ID-ONE Cosmo V7.0.1-n Standard, sur composant P5CC081 en configuration fermée.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs version 3.1 révision 3 [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. 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 de l'application sur la plateforme déjà certifiée par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme ID-One Cosmo v7.0.1-n sur microcontrôleurs P5CD081V1A, P5CC081V1A et P5CD041V1A, certifiée par l'ANSSI sous la référence [ANSSI-CC-2012/30] au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5 et conforme au profil de protection Java Card [PP/0304].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 28 août 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]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Certains mécanismes analysés ne sont pas conformes aux exigences de [REF-CRY], du fait de faiblesses cryptographiques inhérentes aux spécifications auxquelles le développeur est contraint de se conformer. Par conséquent, et conformément aux guides [GUIDES], il est notamment recommandé de ne pas utiliser les mécanismes suivant :

- la signature RSA sans hachage ;
- le schéma de signature PKCS#1 v1.5 ;
- l'algorithme AES en mode ECB.

Quoi qu'il en soit, 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

2.4. Analyse du générateur d'aléas

Ce générateur a fait l'objet d'une analyse. Bien qu'il ne soit pas conforme aux exigences de [REF-CRY], cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants pour un usage direct du bloc de retraitement. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception.

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 « Cryptosmart card v5.0 sur plateforme Oberthur ID-One Cosmo v7.0.1-n avec correctif 077121, Version 5.0» 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, ALC_FLR.3 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 :

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_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**	Implementation representation 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								**3**	Systematic flaw remediation
	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 : 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 : Crytposmart Card 5.0 – Security Target version 5.0.8 révision 33 du 13/07/2012 édité par ERCOM.
[RTE]	Rapport technique d'évaluation : Evaluation Technical Report – CRYPTOSMART Project version 1.3 du 25/09/2012 édité par Serma Technologies.
[ANA-CRY]	Analyse des mécanismes cryptographiques : Cryptographic Mechanism Evaluation Report – CRYPTOSMART Project version 1.2, octobre 2012 édité par Serma Technologies.
[GUIDES]	Guide de développement : Cryptosmart Card 5.0 – Developer's guide version 5.0.1 révision 29 de mai 2011 édité par ERCOM.
[PP/0304]	Protection Profile, SUN Java Card™ System Protection Profile Collection, août 2003. *Certifié par l'ANSSI le 30 septembre 2003 sous la référence PP/0304.*
[BSI-DSZ-CC-0555-2009]	Certificat délivré par le BSI le 10 novembre 2009 pour les produits *NXP Secure Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A each with specific IC Dedicated Software.*
[ANSSI-CC-2012/30]	Certificat délivré par l'ANSSI pour le produit *Carte à puce ID-One Cosmo V7.0.1-n avec correctif 077121, sur composant NXP P5CD081 V1A (Standard Dual), P5CC081 V1A (Standard) et P5CD041 (Basic Dual)*, septembre 2012.

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to Smartcards, version 2.8 revision 1, January 2012.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.
[CCRA]	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 20 janvier 2010, 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.