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-2016/69

Cryptosmart Card applet V5.1 sur la plateforme OBERTHUR ID-ONE COSMO V7.0.1-R2, version 816

Paris, le 26 octobre 2016

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

Guillaume POUPARD
[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 au guide 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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2016/69

Nom du produit

Cryptosmart Card applet V5.1 sur la plateforme OBERTHUR ID-ONE COSMO V7.0.1-R2, version 816

Référence/version du produit

V5.1

Conformité à un profil de protection

Aucun

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur(s)

ERCOM
6, rue Dewoitine
78140 Vélizy
France

OBERTHUR TECHNOLOGIES
420, rue d'Estienne d'Orves
92700 Colombes
France

NXP Semiconductors
Stresemannallee 101
D-22502 Hamburg
Germany

Commanditaire

ERCOM
6, rue Dewoitine
78140 Vélizy
France

Centre d'évaluation

Serma Safety & Security
14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL2.

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 « Cryptosmart Card applet V5.1 sur la plateforme OBERTHUR ID-ONE COSMO V7.0.1-R2, version 816 ».

Ce produit conçu, développé et pré-personnalisé par les sociétés *NXP*, *OBERTHUR TECHNOLOGIES* et *ERCOM*, est destiné à être utilisé pour établir un canal sécurisé (authentification et négociation de clés partagées) avec un autre produit distant contenant l'applet C*RYPTOSMART*. Ce produit propose également plusieurs fonctions de cryptographie et une zone de stockage sécurisée.

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.

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 suivants :

- la commande GET STATUS comme décrit dans [GUIDE] chapitres 6 et 16, concernant les références de l'applet :

Field designation	Byte	Field value (hexadecimal)
Applet version	7 et 8	05 01
Source version	9 à 11	00 03 30
Build version	12 à 14	F5 CD 4D FC
Compilation date and time	15 à 20	20 16 04 18 13 46

- la commande GET DATA avec le TAG égal à DF52 pour obtenir les références de l'OS[1] :

Subtag	Field designation	Field value (hexadecimal)
01	Component number	1A (contact only)
03	Mask Id and version	71 01

- la commande GET DATA avec le TAG égal à DF50 pour obtenir les références de l'IC :

Byte	Field designation	Field value (hexadecimal)
17	Device Coding Byte (DC2)	43 (P5CC081V1A) 44 (P5CD081V1A)

[1] *Operating System.*

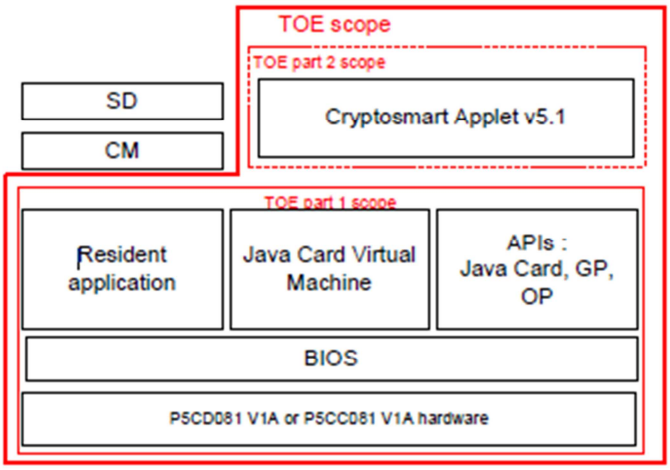
1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- l'authentification d'une application *CRYPTOSMART* distante et la négociation d'une clé partagée avec cette dernière ;
- la mise à disposition de fonctions cryptographiques telles que :
  - l'authentification de l'utilisateur en utilisant un code sécurisé ;
  - le stockage sécurisé de clés AES 256 bits ou RSA 2048 bits ;
  - l'export sécurisé de clés AES de 256 bits ou RSA de 2048 bits ;
  - un sous-ensemble des fonctionnalités de PKCS#11 ;
  - la génération de clés RSA 2048 bits ;
  - la génération de clés AES 256 bits ;
  - la gestion des propriétés d'extraction des clés RSA et AES ;
  - la gestion des propriétés d'utilisation des clés AES ;
  - l'obtention de clés locales de chiffrement en dérivant les clés internes ;
  - la génération de nombres aléatoires ;
- la mise à disposition d'une zone de stockage sécurisée.

1.2.4. Architecture

Le produit est constitué d'un microcontrôleur *NXP* P5CC081V1A ou *NXP* P5CD081V1A sur lequel est installé la plateforme ID-ONE COSMO V7.0.1-R2 d'*OBERTHUR TECHNOLOGIES*. L'applet « Cryptosmart » est ensuite instanciée sur cette plateforme.
L'architecture complète de la carte est la suivante :



1.2.5. Cycle de vie

L'évaluation a couvert la conception, le développement, le chargement de l'application « Cryptosmart », la pré-personnalisation de la carte et la désactivation du *Java Card Manager* pour empêcher l'effacement de l'application « Cryptosmart » et interdire le chargement d'autres applications. Ces étapes se déroulent dans les locaux d'*ERCOM*, elles correspondent à la phase 6 du cycle de vie. Une fois ces étapes effectuées, le produit est livré à l'utilisateur final.
Le produit a été développé et testé par les sociétés *NXP*, *OBERTHUR TECHNOLOGIES* et *ERCOM*.
Il est également pré-personnalisé sur le site suivant :

ERCOM
6 rue Dewoitine
78140 Vélizy-Villacoublay
FRANCE

+++++++L'évaluateur a considéré que les produits sont délivrés aux clients sans aucune clé installée. Charge à l'administrateur du client de personnaliser les cartes pour chacun des utilisateurs finaux, en utilisant le logiciel nommé « Card administration station » délivré par *ERCOM*. Ce logiciel permet notamment d'inscrire dans les cartes, les clés cryptographiques et les certificats nécessaires au bon fonctionnement des échanges sécurisés.

1.2.6. Configuration évaluée

Le certificat porte sur l'applet « Cryptosmart v5.1 » chargée sur la plateforme JavaCard en mode fermé fournie par la société *OBERTHUR TECHNOLOGIES*, telle que présentée au paragraphe 1.2.4 et utilisée conformément au guide [GUIDE]. Cette plateforme est conforme à « Java Card 2.2.2 » et « GlobalPlatform 2.1.1 », l'interface sans contact est désactivée, seul le mode avec contact est opérationnel.

Les tests d'évaluation ont été réalisés sur une plateforme ID-ONE COSMO V7.0.1-R2 en mode fermé portée sur les composants NXP P5CC081v1.A. Bien que l'évaluateur n'ait pas effectué de tests avec le composant NXP P5CD081v1.A, il a considéré que ce dernier était si proche techniquement de celui évalué qu'il donnerait les mêmes résultats. Donc par extension, les plates formes évaluées sont ID-ONE COSMO V7.0.1-R2 en mode fermé sur les composants NXP P5CC081v1.A et NXP P5CD081v1.A déjà certifiés par ailleurs [CERT_IC].

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 P5CC081V1A » et « NXP P5CD081V1A » au niveau EAL5 augmenté des composants ALC_DVS.2, ASE_TSS.2 et AVA_VLA.5 [CERT_IC], conforme au profil de protection [PP].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 25 octobre 2016, 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 au référentiel technique de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI. 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.

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.

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 [CERT_IC]).
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.

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 applet V5.1 sur la plateforme OBERTHUR ID-ONE COSMO V7.0.1-R2, version 816 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL4 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 le guide fourni [GUIDE].

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 lorsque les dépendances CC sont satisfaites. 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 EAL2 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, le Qatar, 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				**3**				**3**	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: 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 : - Cryptosmart card 5.1 – Security Target, version 5.1.2 du 31 mai 2016, *ERCOM*.
[RTE]	Rapport technique d'évaluation : - Cryptosmart card v5.1 EvaluationTechnical Report, référence Cryptosmart_5_1_ETR_v1.2, version 1.2 du 25 octobre 2016, *SERMA SAFETY & SECURITY*.
[ANA-CRY]	Cryptosmart card 5.1 Cryptographic Mechanism Evaluation Report, référence Cryptosmart_5_1_Cryptography_v1.1, version 1.1 du 4 octobre 2016, *SERMA SAFETY & SECURITY*.
[EXP-CRY]	[RTE] Annexe 1.
[CONF]	Liste de configuration du produit : - Cryptosmart card 5.1 - Configuration list, version 5.1 révision 68, référence 2011B/270, *ERCOM*.
[GUIDE]	Guide de développement : - Cryptosmart Card 5.1 - Developer's guide, version 5.1 révision 63 de mai 2016, *ERCOM*.
[PP]	*Security IC Platform Protection profile*, version 1.0 du 15 juin 2007 [BSI-CC-PP-0035-2007].
[CERT_IC]	Rapport de certifications BSI-DSZ-CC-0857-V2-2015 pour les produits NXP Secure Smart Card Controllers P5CD016/021/041/051 and P5Cx081V1A/ V1A(s) d'*NXP Semiconductors*, 27 avril 2015.

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, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.4, août 2015.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[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 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), 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_B3), 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.