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-2016/08

Secure Smart Card Controller E201382

Paris, le 29 février 2016

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

Contre-amiral Dominique RIBAN
[OR IGINAL S IGNE]

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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2016/08

Nom du produit

Secure Smart Card Controller E201382

Référence/version du produit

IC Hardware versions VA and VB,
ID Dedicated Support Software version 1.0

Conformité à un profil de protection

Security IC Platform Protection Profile with Augmentation Packages, version 1.0,

certifié BSI-CC-PP-0084-2014 le 19 february 2014

avec conformité à

“Package 1: Loader dedicated for usage in Secured Environment only”

Critères d’évaluation et version

Critères Communs version 3.1 révision 4

Niveau d’évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5, ASE_TSS.2

Développeur

NXP Semiconductors

Stresemannallee 101
22529 Hamburg, GERMANY

Commanditaire

NXP Semiconductors

Stresemannallee 101
22529 Hamburg, GERMANY

Centre d’évaluation

Serma Safety & Technology

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 « *Secure Smart Card Controller E201382, IC Hardware versions VA and VB, IC Dedicated Support Software version 1.0* » développé par *NXP SEMICONDUCTORS*.

Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou plusieurs applications. Il peut être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (documents d'identité sécurisés, applications bancaires, télévision à péage, transport, santé, etc.) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

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 est strictement conforme au profil de protection [PP0084], avec le package « *Loader dedicated for usage in secured environment only* ».

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 :

- une empreinte physiquement gravée à la surface du microcontrôleur dont la forme attendue est décrite dans le guide « *Wafer and delivery specification* » (voir [GUIDES]) ;
- la réponse à la commande logique *phhalSystem_GetVersion* décrite dans le guide « *System Interface Manual* » (voir [GUIDES]) ; les valeurs retournées par le produit certifié sont :

Information	Valeur	Commentaire
IC Hardware version	0x12 ou 0x13	Les deux valeurs correspondant aux deux configurations d'antenne.
IC Dedicated Software Version	0x06	Ces valeurs correspondent à « *IC Dedicated Support Software version 1.0* ».
Patch configuration identifier	0x03	
Wafer Test program version	0x00	
Manufacturer identifier	0x1	
Current enumerated Lifecyle	0x4	Signifiant « Release », i.e. *Embedded Software* chargé, *Application Management* désactivé.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection en intégrité et en confidentialité des données utilisateur et des logiciels embarqués exécutés ou stockés dans les différentes mémoires de la TOE ;
- la bonne exécution des services de sécurité fournis par la TOE aux logiciels embarqués ;
- le support au chiffrement cryptographique à clés symétriques ;
- le support à la génération de nombres non prédictibles.

1.2.4. Architecture

Le produit est constitué :

- d'une partie matérielle principalement composée par :
  - un processeur 16bit ;
  - une mémoire RAM (1.25 ko), des mémoires non-volatiles (10 ko EEPROM, 64 ko FLASH), une mémoire ROM (48 ko) ;
  - un module accélérateur AES et DES, un module de génération d'aléa, un module de communication radiofréquence ;
- d'une partie logicielle appelée *Dedicated Software* comprenant :
  - un logiciel d'auto-test *Test Software* ;
  - un logiciel de gestion du démarrage sécurisé du microcontrôleur *Boot Software* ;
  - un logiciel de chargement de code embarqué *Application Management Software* ;
  - des pilotes des modules périphériques *HAL Software, HAL library, Crypto Library*.

Le produit est accompagné de guides pour l'utilisateur.

Pour plus de détails, voir la cible de sécurité [ST].

1.2.5. Cycle de vie

Le cycle de vie du produit est présenté au paragraphe 1.4.5 de la cible de sécurité [ST]. Le logiciel *Application Management Software* est utilisé pour charger le code embarqué ; cette fonction de chargement de code est ensuite désactivée et n'est plus disponible en Phases 6 et 7.

Le produit est développé sur les sites suivants :

Nom du Site	Adresse	Fonction principale
NXP HAMBURG	Stresemannallee 101 22529 Hamburg, Germany	Phase 2, design
NXP GRATKORN	Mikron-weg 1, 8101 Gratkorn, Austria	Phase 2, design
NXP BANGALORE	Manayata Tech Park, Nagavara, Bengaluru, Kamataka 560045, India	Phase 2, design
REC ZILINA	Vysokoskolakov 1757/1 010 01Zilina, Slovakia	Phase 2, validation

SSMC SINGAPORE	70 passir Ris Industrial Drive 1, Singapore 519527	Phase 3, Data Preparation and Wafer fabrication
TOPPAN KOREA	91, Wonjeonk-ro 290 beon-gil, Icheon-Si, Gyeonggi-do 467-842, Korea	Phase 3, Maskshop
APB THAILAND	APB, 303 Moo 3, Chaengwattana Rd, Laksi, Bangkok 10210, Thailand	Phase 4, Assemblage
CHIPBOND TAIWAN	No. 3, Li-Hsin Rd. V Science Based Industrial Park Hsin-Chu City Taiwan, R.O.C	Phase 4, Assemblage
NEDCARD	Bijsterhuizen 25-29 NL-6604LM Wijchen, Netherlands	Phase 4, Assemblage
NXP EINDOVEN	High Tech Campus 60 5656G AG Eindhoven Netherlands	Support (IT Secure room)
ATOS BYDGOSZCZ	Biznes Park ul. Kraszewskiego 1 85-240 Bydgoszcz, Poland	Support (IT Secure room)
NXP LEUVEN	Interleuvenlaan 80 B-3001 Leuven, Belgium	Support (gestion infrastructure IT)

1.2.6. Configuration évaluée

Comme décrit dans la cible de sécurité [ST], le produit existe en deux configurations (VA et VB), chacune dédiée à l'un des deux types d'antennes à connecter au produit. Le certificat porte sur ces deux configurations.

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

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 16 février 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 selon le référentiel technique de l'ANSSI [REF], 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.5 visé.

2.4. Analyse du générateur d'aléas

Le produit comporte un générateur d'aléa physique, et un générateur de pseudo-aléa.
Ces générateurs ont fait l'objet d'une évaluation selon la méthodologie [AIS20/AIS31] et ils répondent respectivement aux exigences de la classe PTG.2 et de la classe DRG.3, comme revendiqué dans la cible de sécurité.
Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants pour un usage direct des sorties du générateur d'aléa physique. 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. Comme énoncé dans le document [REF] il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléas n'a pas révélé de faiblesse.

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 « Secure Smart Card Controller E201382, IC Hardware versions VA and VB, IC Dedicated Support Software version 1.0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ASE_TSS.2, ALC_DVS.2, AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

Ce certificat donne une appréciation de la résistance du produit à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le micro-circuit ne pourra être appréciée que par une évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de l'évaluation citée au chapitre 2.

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 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 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, 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	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**2**	Well-structured internals
	ADV_SPM						**1**	1		
	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	**2**	TOE summary specification with architectural design summary
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**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 : - NXP Secure Smart Card Controller E201382, Security Target, Rev. 1.3, 12 février 2016, NXP. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - NXP Secure Smart Card Controller E201382, Security Target Lite, Rev. 1.2, 12 février 2016, NXP.
[RTE]	Rapport technique d'évaluation : - E20 Evaluation Technical Report, E20_ETR_v1.1, 15 février 2016, Serma Technologies. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - E20 Evaluation Technical Report, E20_ETR-Lite_v1.0, E20_ETR-Lite_v1.0, 15 février 2016, Serma Technologies.
[CONF]	Liste de configuration du produit : - GOP10RS805 Configuration Item List, Rev 00.06, 12 février 2016, NXP.
[GUIDES]	- E201382 EMBRACE secure smart card controller - Objective data sheet, rév. 1.3, 28 août 2015, réf. 254213, NXP ; - E201382 EMBRACE - Application Management, rév. 1.2, 30 septembre 2015, réf. 279912, NXP ; - E201382 EMBRACE - Crypto Library, rév. 1.4, 13 octobre 2015, réf. 280014, NXP ; - E201382 EMBRACE - Instruction Set Manual, rév. 1.1, 25 juin 2015, réf. 277311, NXP ; - E201382 EMBRACE - System Interface Manual, rév. 1.4, 13 janvier 2016, réf. 279814, NXP ; - NXP Secure Smart Card Controller E201382 - Information on Guidance and Operation, rév. 1.4, 12 janvier 2016, réf. 281114, NXP ; - E201382 VA and VB - Wafer and delivery specification, rév. 1.1, 2 février 2016, réf. 340611, NXP.
[PP0084]	Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la* référence BSI-CC-PP-0084-2014 le 19 février 2014.

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.
[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.
[AI20/AIS 31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 September 2011, BSI (Bundesamt für Sicherheit in der Informationstechnik).

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