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-2016/32

MIFARE DESFire EV2

Paris, le 26 mai 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 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-2016/32

Nom du produit

MIFARE DESFire EV2

Version du produit

version 1.5

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 février 2014

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, ALC_FLR.1

Développeur

NXP Semiconductors
Stresemannallee 101
22529 Hamburg, GERMANY

Commanditaire

NXP Semiconductors
Stresemannallee 101
22529 Hamburg, GERMANY

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 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT 6
1.2.1. Introduction 6
1.2.2. Identification du produit 6
1.2.3. Services de sécurité 7
1.2.4. Architecture 7
1.2.5. Cycle de vie 7
1.2.6. Configuration évaluée 8

2. L'EVALUATION 9

2.1. REFERENTIELS D'EVALUATION 9
2.2. TRAVAUX D'EVALUATION 9
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI 9
2.4. ANALYSE DU GENERATEUR D'ALEAS 9

3. LA CERTIFICATION 10

3.1. CONCLUSION 10
3.2. RESTRICTIONS D'USAGE 10
3.3. RECONNAISSANCE DU CERTIFICAT 11
3.3.1. Reconnaissance européenne (SOG-IS) 11
3.3.2. Reconnaissance internationale critères communs (CCRA) 11

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 12

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 13

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 14

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce « MIFARE DESFire EV2**,** version 1.5 » développée par *NXP SEMICONDUCTORS*.

Ce produit est destiné à être utilisé comme une carte sans-contact (ISO 14443 type A) dans des applications de transport, de contrôle d'accès, ou de paiement dans un cercle fermé d'usagers.

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]. Le logiciel étant entièrement chargé en mémoire avant le point de livraison, et le mécanisme de chargement étant alors verrouillé, aucun des « *packages for loader* » du [PP0084] n'est revendiqué.
Le produit fournit de plus des services de sécurité spécifiques correspondant à la fonctionnalité DESFire.

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 la réponse à la commande GetVersion (voir [GUIDES]) dont les champs retournés ont les valeurs attendues suivantes :

Champs	Valeur attendue
VendorID	0x04
HWType	0x01
HWSubType	0x01 ou 0x02
HWMajorVersion	0x12
HWMinorVersion	0x00
SWType	0x01
SWSubType	0x01
SWMajorVersion	0x02
SWMinorVersion	0x00

De plus, la fonctionnalité *Originality Check* (voir [GUIDES]) peut aider l'émetteur de cartes à détecter des produits contrefaits.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- authentification mutuelle en 3 échanges, et selon ISO7816-4 ;
- authentification au niveau de chaque application avec de multiples possibilités de configuration des conditions d'accès à chaque fichier ;
- service de délégation de la gestion des applications ;
- chiffrement de la communication ;
- contrôle d'intégrité de la communication (*Message Authentication Codes* MAC) ;
- numéro de série unique pour chaque carte à puce, ou génération aléatoire des UID ;
- preuve de transaction ;
- preuve d'origine ;
- preuve de proximité lors d'une transaction.

1.2.4. Architecture

Le produit est constitué :
- d'une partie matérielle principalement composée de :
  - un processeur 16 bit ;
  - 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 comprenant :
  - un logiciel d'auto-test *Test ROM Software* ;
  - un logiciel de gestion du démarrage sécurisé du microcontrôleur *IC Dedicated Boot Software* ;
  - les pilotes et bibliothèques *HAL ROM Software* ;
  - l'application *MIFARE DESFire EV2*.

Le produit ne supporte aucun logiciel embarqué additionnel ; les applications sont instanciées par l'utilisateur en mémoire non-volatile après le point de livraison.

Le produit est accompagné de guides pour l'utilisateur (voir [GUIDES]).

1.2.5. Cycle de vie

Comme indiqué au paragraphe 1.4.4 de la cible de sécurité [ST], le cycle de vie du produit s'inscrit dans le cycle de vie classique présenté dans le PP [PP0084].
Le produit n'est pas destiné à recevoir de logiciel embarqué additionnel : la phase 1 n'est pas applicable. Le logiciel embarqué a été développé au cours de la phase 2 comme « *IC Dedicated Software* ».

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

Le produit existe en variantes commerciales correspondant à différentes tailles mémoires et à différents conditionnements (voir §1.4.1.1 de [ST]). Le certificat porte sur l'ensemble de ces variantes dont les sites de fabrication sont mentionnés ci-dessus.

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 s'appuie sur les résultats d'évaluation du produit « Secure Smart Card Controller E201382 » certifié le 29 février 2016 sous la référence ANSSI-CC-2016/08 (voir [2016/08]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 17 mai 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.
Comme énoncé dans le document [REF], l'aléa qu'utilise MIFARE DESFire EV2, par exemple lors des commandes d'authentification, a effectivement subi un retraitement algorithmique de nature cryptographique.

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 « MIFARE DESFire EV2, version 1.5 » 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 ALC_DVS.2, AVA_VAN.5, ASE_TSS.2, ALC_FLR.1.

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 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								**1**	Basic flaw remediation
	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 : - MF3Dx2 MIFARE DESFire EV2 – Security Target, Rev 1.3, 29 avril 2016, NXP Semiconductors. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - MF3Dx2 MIFARE DESFire EV2 – Security Target Lite, Rev 1.5, 29 avril 2016, NXP Semiconductors.
[RTE]	Rapport technique d'évaluation : - MF3Dx2 EvaluationTechnical Report, MF3_ETR_v1.1, 13 mai 2016, Serma Safety and Security.
[CONF]	Liste de configuration du produit : - MIFARE DESFire EV2 – Configuration Item List, Rev 1.4, 29 avril 2016, NXP Semiconductors.
[GUIDES]	- MIFARE DESFire EV2 contactless multi-application IC, MF3Dx2 Product data sheet, Rev. 3.0, Ref. 226030, 4 février 2016, NXP Semiconductors ; - MF3Dx2Information on Guidance and Operation, Guidance and Operation Manual, Rev. 1.1, Ref. 274811, 29 avril 2016, NXP Semiconductors.
[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.
[2016/08]	Rapport de certification ANSSI-CC-2016/08, Secure Smart Card Controller E201382, 29 février 2016, ANSSI.

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.