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-2015/45

IDeal Citiz v2.1 Open platform

Paris, le 2 octobre 2015

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

Guillaume POUPARD
[ORIGINAL SIGNE]

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

Référence du rapport de certification

ANSSI-CC-2015/45

Nom du produit

IDeal Citiz v2.1 Open platform

Référence/version du produit

Version 2.1.0

Conformité à un profil de protection

Java Card Protection Profile – Open Configuration

Version 3.0, ANSSI-CC-PP-2010/03-M01

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

MORPHO

18 Chaussée Jules César,
95520 Osny, France

INFINEON Technologies AG

AIM CC SM PS – Am Campeon 1-12,
85579 Neubiberg, Allemagne

Commanditaire

MORPHO

18 Chaussée Jules César, 95520 Osny, France

Centre d'évaluation

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, 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 la carte à puce « IDeal Citiz v2.1 Open platform, Version 2.1.0 » développée par *MORPHO* sur un microcontrôleur fabriqué par la société *INFINEON TECHNOLOGIES.*

Ce produit est une plateforme ouverte *JavaCard,* contact et/ou sans contact, destinée à accueillir les applets de l'utilisateur pre-émission et/ou post-émission, et à leur fournir les services de sécurité détaillés dans la cible [ST] et dont les principaux sont repris au §1.2.3.

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 [PP_JC].

1.2.2. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La méthode d'identification du produit est présentée dans le guide [AGD_PRE]. La version certifiée du produit est identifiable par les éléments suivants :

- les *Card Production and Life Cycle (CPLC) Data* indiquent les valeurs suivantes :

Donnée	Valeur
IC Fabricator	0x8100
IC Type	0x7805
Operating System Identifier	0x4921
Operating System Release Date	0x5079
Operating System Release Level	0x2101

- et la valeur de la donnée *Hardware security integrity* est 0x448C448C48C6.

Le produit soumis à l'évaluation ne comporte pas de « *known applications* » au sens de [JIL_OPEN_V1.1] ; il comporte un Issuer Security Domain qui est partie intégrante de la plateforme et est couvert par la présente évaluation.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la gestion d'applications selon Global Platform, en particulier la présence de *Security Domains* ;
- la protection du chargement d'applications, en particulier *post-issuance* ;
- l'isolation, par un pare-feu, des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications ;

- divers services aux applications, disponibles à travers l'*Application Programming Interface (API) JavaCard*, comme par exemple des calculs cryptographiques.

1.2.4. Architecture

Le produit est constitué :

- d'un microcontrôleur M7892 B11 et de ses bibliothèques logicielles, développés par *INFINEON* ;
- d'un système d'exploitation développé par *MORPHO* ; ce système d'exploitation comporte une machine virtuelle JavaCard et offre la gestion de carte multi-applicative Global Platform.

1.2.5. Cycle de vie

Le cycle de vie du produit est conforme au cycle de vie standard d'une carte à puce (voir [PP0035]). Le point de livraison est situé après le chargement et la configuration du système d'exploitation dans la mémoire *Flash* du microcontrôleur.
Le cycle de vie est décliné en plusieurs variantes dans la cible de sécurité [ST], selon le support employé lors de la pré-personnalisation (micro-module, ou encartage déjà effectué) et selon le propriétaire de la clé protégeant le produit au point de livraison (propriété de MORPHO ou propriété du *pre-personalizer*).

Le microcontrôleur M7892 B11 a été développé et fabriqué par *INFINEON*. Les sites de développement et de fabrication du microcontrôleur sont détaillés dans le rapport de certification [CERT_IC].

Morpho a développé et fabriqué le produit sur les sites suivants :

MORPHO	***MORPHO CARDS CZECH***
18 Chaussée Jules César 95520 Osny France	Jelinkova 1174/3A 72100 Ostrava République Tchèque

Les guides [BADR] et [SADR] décrivent les règles de développement des applications destinées à être chargées sur cette carte.
Le guide [VAR] décrit les règles de vérification qui doivent être appliquées par l'autorité de vérification.
Afin que le chargement d'applications n'impacte pas les fonctions de sécurité certifiées au titre du présent rapport, ce chargement doit être effectué durant la personnalisation ou l'utilisation du produit, et doit mettre en œuvre les recommandations des guides [AGD_PRE] et [VAR].

1.2.6. Configuration évaluée

La configuration ouverte du produit a été évaluée conformément à [JIL_OPEN_V1.1] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification.

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 du microcontrôleur « *Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)*» au niveau EAL6 augmenté du composant ALC_FLR.1, conforme au profil de protection [PP0035]. Ce microcontrôleur a été certifié le 11 septembre 2012 sous la référence BSI-DSZ-CC-0782-2012, et a fait l'objet d'une maintenance le 5 septembre 2013 sous la référence BSI-DSZ-CC-0782-2012-MA-01. Le niveau de résistance du microcontrôleur a été confirmé le 24 mars 2014 par le BSI.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 10 septembre 2015, 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 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 « IDeal Citiz v2.1 Open platform, Version 2.1.0 » 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 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 les guides fournis [GUIDES], notamment :

- toutes les futures applications chargées sur ce produit doivent respecter les contraintes de développement de la plateforme (guides [BADR] et [SADR] selon la sensibilité de l'application considérée) ;
- les autorités de vérification doivent appliquer le guide [VAR] ;
- la protection du chargement de toutes les applications sur ce produit doit être activée conformément aux indications de [AGD_PRE].

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.
Pour les évaluations enregistrées avant septembre 2014, 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, 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	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	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 : - Security Target – IDeal Citiz v2.1 Open Platform, référence 2014_0000002183 version 6.7, 7 septembre 2015, Morpho. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security target LITE IDeal Citiz v2.1 open platform, version 02, référence 2015_2000009094, 8 septembre 2015, Morpho.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report (full ETR) – EAGLE, reference LETI.CESTI.EAG.RTE.012 version 1.1, 9 septembre 2015, CEA-LETI.
[CONF]	Liste de configuration du produit : - Software release sheet on SLE78C(L)FX4000P(M) for IDealCitiz v2.1, référence 2015_2000006639, version 9, 8 septembre 2015, Morpho.
[GUIDES] [BADR] [SADR] [VAR] [AGD_PRE] [AGD_OPE]	Liste des guides du produit : - IDeal Citiz v2.1 – Basic Applet Development Recommendations, réf. 2014_2000001499, version 1.0, 7 juillet 2014, Morpho ; - IDeal Citiz v2.1 – Secure Applet Development Recommendations, réf. 2014_2000001501, version 1.2, 26 mars 2015, Morpho ; - IDeal Citiz v2.1 – Verification Authority Rules, réf. 2014_2000001513, version 1.0, 7 juillet 2014, Morpho ; - Preparative procedure for IDealcitiz v2.1, réf 2014_2000003597, version 07, 31 juillet 2015, Morpho ; - Operational user guidance IDealcitiz_v2.1, réf 2014_2000004459, version 03, 31 juillet 2015, Morpho.
[CERT_IC]	- Certification Report BSI-DSZ-CC-0782-2012 for Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG, 11 septembre 2012, BSI ; - Assurance Continuity Maintenance Report BSI-DSZ-CC-0782-2012-MA01, 5 septembre 2013, BSI ; - Update of evaluation results from certification procedure BSI-DSZ-CC-0782-2012. Confirmation of the reassessment dated 24 March 2014, BSI.
[PP_JC]	Java Card Protection Profile – Open Configuration, version 3.0, May 2012, Oracle Corporation. *Certifié par l'ANSSI sous la reference ANSSI-CC-PP-2010/03-M01*.

[PP0035]	Protection Profile, Security IC Platform Protection Profile, version 1.0, juin 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*

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 1.2, janvier 2012.
[JIL_OPEN_V1.1]	Certification of « Open » smart card products, version 1.1 (for trial use), 4 février 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.

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