



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-2018/01

IDEal Citiz v2.1 STC Open Platform

Paris, le 7 mars 2018

*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 présumées 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

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



Référence du rapport de certification

ANSSI-CC-2018/01

Nom du produit

IDEal Citiz v2.1 STC Open Platform

Référence/version du produit

OFFICIEL_IDealCitiz_SCR400L_2_1_0_0_04

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

IDEMIA
(ex SAFRAN I&S)
18 Chaussée Jules César,
95520 Osny, France

Starchip SAS
ArteParc Bat. E, Route de la Côte d'Azur,
13590 Meyreuil, France

Commanditaire

IDEMIA
420 rue d'Estienne d'Orves, 92700 Colombes, France

Centre d'évaluation

CEA - LETI
17 rue des martyrs, 38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables



SOG-IS



Ce certificat 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. <i>Introduction</i>	6
1.2.2. <i>Services de sécurité</i>	6
1.2.3. <i>Architecture</i>	6
1.2.4. <i>Identification du produit</i>	6
1.2.5. <i>Cycle de vie</i>	7
1.2.6. <i>Configuration évaluée</i>	7
2. L’EVALUATION	8
2.1. REFERENTIELS D’EVALUATION	8
2.2. TRAVAUX D’EVALUATION	8
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	8
2.4. ANALYSE DU GENERATEUR D’ALEAS	8
3. LA CERTIFICATION	9
3.1. CONCLUSION	9
3.2. RESTRICTIONS D’USAGE	9
3.3. RECONNAISSANCE DU CERTIFICAT	10
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	10
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	10
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT	11
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	12
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	13

1. Le produit

1.1. Présentation du produit

Le produit évalué est la plateforme *JavaCard* « IDeal Citiz v2.1 STC Open Platform, OFFICIEL_IDealCitiz_SCR400L_2_1_0_0_04 » développée par *IDEMIA* sur un microcontrôleur de *STARCHIP*.

Le produit est destiné à héberger et exécuter une ou plusieurs applications, dites *applets* dans la terminologie *JavaCard*. Ces applications peuvent revêtir un caractère sécuritaire différent (selon qu'elles sont « sensibles » ou « basiques ») et peuvent être chargées et instanciées avant ou après émission du produit.

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. 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* et des services de personnalisation s'appuyant sur des canaux sécurisés ;
- la protection du chargement d'applications *post-issuance* ;
- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications ;
- des fonctions de cryptographie symétrique et asymétrique, des fonctions de hachage, et un générateur d'aléa, disponibles aux applications à travers l'API *JavaCard*.

1.2.3. Architecture

Le produit est constitué :

- d'un microcontrôleur SCR400L, développé par *STARCHIP* ;
- d'un système d'exploitation développé par *IDEMIA* ; ce système d'exploitation comporte une machine virtuelle *JavaCard* et offre la gestion de carte multi-applicative *Global Platform*.

1.2.4. 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 attendue
<i>IC Fabricator</i>	0x5343
<i>IC Type</i>	0x000D
<i>Operating System Identifier</i>	0x4921
<i>Operating System Release Date</i>	0x7291
<i>Operating System Release Level</i>	0x2101

- la valeur de la donnée *Hardware configuration integrity* est 0xC2DB9CD0E9AABE.

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.

1.2.5. Cycle de vie

Le cycle de vie du produit est présenté au chapitre 3 de la cible de sécurité [ST]. Il se décline en quatre variantes selon l'ordre et le lieu des opérations de construction de la TOE à livrer. Pour toutes les variantes également, le produit est protégé au point de livraison par une clé diversifiée d'une clé maîtresse dédiée au Personnalisateur destinataire du produit.

Plusieurs sites concourent au développement et à la fabrication du produit. Les sites de Starchip sont listés dans le rapport de certification [CERT_IC]. Les sites d'IDEMIA sont les suivants :

- **IDEMIA**, 18 Chaussée Jules César, 95520 Osny, France, pour les activités de développement (Phase 1, step 1) ;
- **IDEMIA**, site ARTEPARC, Route de la Cote d'Azur, 13590 Meyreuil, France, pour les activités de développement (Phase 1, step 1) ;
- **IDEMIA**, Sentinel & Havelock, R&D Noida, D-217 & D-216, Sector 63, Noida, Uttar Pradesh, Inde, pour les activités de développement (Phase 1, step 1) ;
- **MORPHO CARDS CZECH**, Jelinkova 1174/3A, 72100 Ostrava, République Tchèque, pour les activités de fabrication (Phase 2, Step 5).

Le guide [AGD_OPE] identifie des recommandations relatives aux futures applications à charger sur cette carte. 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.

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].

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 « *SCR400L version G* » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PP0084]. Ce microcontrôleur a été certifié le 30 juin 2017 sous la référence ANSSI-CC-2017/14, voir [CERT_IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 17 novembre 2017, 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 vulnérabilité 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]).

Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI [REF], la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.

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 STC Open Platform », version OFFICIEL_IDealCitiz_SCR400L_2_1_0_0_04, 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 [SAGR] selon la sensibilité de l'application considérées) ;
- les autorités de vérification doivent appliquer le guide [VAR].

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'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce 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 :



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 signataires², 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 La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

² La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

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	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	2	Well-structured internals
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	4	4	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	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	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	2	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	3	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - Security Target Ideal Citiz v2.1 STC Open Platform, réf 2015_2000012136, v1.3, 19 octobre 2017, <i>SAFRAN I&S</i>. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - Security Target Lite Ideal Citiz v2.1 STC Open Platform, réf 2017_2000031680, v1.0, 6 novembre 2017, <i>IDEMIA</i>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Evaluation Technical Report : ETR – HAWK, référence LETI.CESTI.HAW.ETR.001 – v1.0, 17 novembre 2017, <i>CEA LETI</i>.
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - Software Release Sheet for IDeaCitiz v2.1 STC, réf 2017_2000027354, 7 novembre 2017, <i>SAFRAN I&S</i>.
[GUIDES] [BADR] [SADR] [VAR] [AGD_PRE] [AGD_OPE]	<p>Liste des guides du produit :</p> <ul style="list-style-type: none"> - Basic Applet Development Recommendations IDeaCitiz_v2.1 STC, réf. 2016_2000022280, v1.0, 6 juin 2017, <i>SAFRAN I&S</i> ; - Secure Applet Development Recommendations IDeaCitiz_v2.1 STC, réf. 2016_2000022281, v1.4, 7 novembre 2017, <i>SAFRAN I&S</i> ; - Verification Authority Rules IDeaCitiz_v2.1 STC, réf. 2017_2000022282, v1.0, 6 juin 2017, <i>SAFRAN I&S</i> ; - Preparative procedure for IDeaCitiz v2.1 STC, réf 2015_2000012677, v3.0, 18 octobre 2017, <i>SAFRAN I&S</i> ; - Operational user guidance, IDeaCitiz_v2.1 STC, réf 2016_2000022279, v2.0, 6 octobre 2017, <i>SAFRAN I&S</i>.
[PP_JC]	<p>Java Card Protection Profile – Open Configuration, version 3.0, May 2012, Oracle Corporation. <i>Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03-M01</i>.</p>
[PP0084]	<p>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014</i>.</p>
[CERT_IC]	<p>Microcontrôleur SCR400L version G, Rapport de certification ANSSI-CC-2017/14, 30 juin 2017.</p>

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 ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : <ul style="list-style-type: none"> - 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.
[OPEN]	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.