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-2017/66

IDeal Citiz v2.15-i on Infineon M7892 B11embedding MICAO SAC/EAC 1.3.69 application

Paris, le 4 décembre 2017

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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2017/66

Nom du produit

IDeal Citiz v2.15-i on Infineon M7892 B11embedding MICAO SAC/EAC 1.3.69 application

Référence/version du produit

OFFICIEL_MICAO_SAC_EAC_1_3_69_IDealCitiz_SLE78CLFX4000PM_2_1_5_0_R2

Conformité à des profils de protection

Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP)

Version 1.3.2, BSI-CC-PP-0056-V2-2012-MA-02

Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)

Version 1.0, BSI-CC-PP-0068-V2-2011

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

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

INFINEON Technologies AG

AIM CC SM PS – Am Campeon 1-12,

85579 Neubiberg, Allemagne

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

CCRA

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. Introduction 6
1.2.2. Services de sécurité 6
1.2.3. Architecture 7
1.2.4. Identification du produit 7
1.2.5. Cycle de vie 8
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 10

3. LA CERTIFICATION 11

3.1. CONCLUSION 11
3.2. RESTRICTIONS D'USAGE 11
3.3. RECONNAISSANCE DU CERTIFICAT 12
3.3.1. Reconnaissance européenne (SOG-IS) 12
3.3.2. Reconnaissance internationale critères communs (CCRA) 12

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 13

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 14

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 16

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce « IDeal Citiz v2.15-i on Infineon M7892 B11 embedding MICAO SAC/EAC 1.3.69 application » développée par *IDEMIA* sur un microcontrôleur d'*INFINEON*.

Le produit évalué est de type « carte à puce » pouvant être utilisé en mode avec et/ou sans contact. Il implémente des fonctions de document de voyage électronique qui se veulent répondre (1) aux spécifications de l'organisation de l'aviation civile internationale (ICAO), et (2) aux préconisations de la Commission Européenne pour les passeports européens biométriques (Décision d'exécution C(2013) 6181) et titres de séjour européens biométriques (Décision d'exécution C(2013) 6178). Ce produit est destiné à permettre la vérification de l'authenticité du document de voyage et à identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels ou des cartes au format ID1. Ils peuvent être livrés sous forme de module, d'*inlay*, ou de couverture de passeport. Le produit final peut également être au format carte plastique pour des applications telles que carte d'identité ou carte de résident.

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 conforme au profil de protection [PP0056V2]. Il s'agit d'une conformité stricte. Le profil de protection [PP0056V2] est strictement conforme au profil de protection [PP0068V2]. La cible de sécurité est donc également strictement conforme à [PP0068V2].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection en intégrité des données du porteur stockées dans la carte : nations ou organisations émettrices, numéro du document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait, autres données optionnelles, données biométriques additionnelles et autres données permettant de gérer la sécurité du document de voyage ;
- le contrôle d'accès aux données du porteur stockées dans la carte ;
- l'authentification du microcontrôleur par le mécanisme optionnel AA (*Active Authentication)* ;
- l'authentification entre le document de voyage et le système d'inspection lors du contrôle aux frontières par le mécanisme SAC (*Supplemental Access Control)* ;
- la protection, en intégrité et en confidentialité, à l'aide du mécanisme de *Secure Messaging*, des données lues ;

- l'authentification forte (avec validation de la chaine de certificats) entre le microcontrôleur et le système d'inspection par le mécanisme EAC (*Extended Access Control*) préalablement à tout accès aux données biométriques.

1.2.3. Architecture

Le produit est constitué :

- de la plateforme ouverte cloisonnante « IDeal Citiz v2.15-i on M7892 B11 - Java Card Open Platform », certifiée sous la référence [ANSSI-CC-2017/59] ; pour rappel, le service de génération de clés RSA de cette plateforme n'est pas revendiqué comme fonction de sécurité ;
- de l'application MICAO procurant les services eMRTD, en configuration SAC/EAC ; pour information, cette application ne fait pas appel au service de génération de clés RSA de la plateforme.

1.2.4. 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 :

1) La méthode d'identification de la plateforme est présentée dans [PLF_AGD_PRE] :

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

Donnée	Valeur attendue
IC Fabricator	0x8100
IC Type	0x7805 ou 0x7801 ou 0x7813
Operating System Identifier	0x4921
Operating System Release Date	0x7123
Operating System Release Level	0x2111

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

2) La méthode d'identification de l'applet MICAO est présentée dans le guide [MICAO_AGD_PRE] :

- les Executable Load Files et Executable Module suivants sont présents :

Objet	AID
MICAO Executable Load File	A00000024710
MICAO Executable Module	A0000002471001

- la version de l'applet MICAO est 01.03.69.0001 (dans la réponse à la commande Get Info Version).

1.2.5. Cycle de vie

Le cycle de vie du produit est présenté au chapitre 1.4.3 de la cible de sécurité [ST].

Le développement du produit, couvert par la classe d'assurance ALC de l'évaluation, s'effectue sur les sites suivants :

Nom du Site	Adresse	Phase
Voir [BSI-DSZ-CC-0782-V2-2015]		*Development (Phase 1, step 1)*
IDEMIA OSNY	18 Chaussée Jules César 95520 Osny, France	*Development (Phase 1, step 2)*
Voir [BSI-DSZ-CC-0782-V2-2015]		*Manufacturing (Phase 2, step 3)*
IDEMIA MORPHO CARDS CZECH	Jelinkova 1174/3A 72100 Ostrava République Tchèque	*Manufacturing (Phase 2, steps 3, 4 & 5)*

Le point de livraison est situé entre la Phase 2 et la Phase 3. Les phases *Personalisation of the travel document* (Phase 3) et *Operational use* (Phase 4) sont couvertes par la classe d'assurance AGD de l'évaluation. L'application MICAO est chargée avant le point de livraison. Aucune autre *known application* n'est considérée.

Si des applications supplémentaires sont chargées en phase *Personalization of the travel document* (Phase 3), ces applications doivent avoir été développées et être chargées en respectant les contraintes de la plateforme (voir guides [PLF_BADR], [PLF_SADR], [PLF_VAR], [PLF_AGD_PRE]).

1.2.6. Configuration évaluée

La configuration ouverte du produit a été évaluée conformément à [JIL_OPEN] : 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.

Le certificat porte sur la configuration de l'applet MICAO, après personnalisation par l'émetteur, qui inclut les mécanismes suivants :

- *Extended Access Control*;
- *Supplemental Access Control* ;
- *Active Authentication.*

Le présent rapport de certification porte également sur la configuration du produit obtenue sans activer le mécanisme optionnel *Active Authentication.*

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 5** [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 la plateforme déjà certifiée par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme « IDeal Citiz v2.1-5 – Java Card Open Platform » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PP-JC]. Cette plateforme ouverte a été certifiée sous la référence [ANSSI-CC-2017/59]. Le microcontrôleur a été certifié sous la référence [BSI-DSZ-CC-0782-V2-2015] et son niveau de résistance a été confirmé le 7 avril 2017 sous la référence [BSI-DSZ-CC-0782-V2-2015-RA-01].

L'évaluation s'appuie sur les résultats d'évaluation du produit « Applet MICAO v1.1.3 sur la plateforme IdealCitiz v2.1, en configuration SAC/EAC » certifié le 13 décembre 2016 sous la référence [ANSSI-CC-2016/80].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 26 octobre 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 a été réalisée. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations données au chapitre 6 du guide [MICAO_AGD_PRE] doivent être suivies.

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 ([RTE]) sur le code développé par *MORPHO* ; elle se base sur la certification AVA_VAN.5 du microcontrôleur et de ses bibliothèques cryptographiques ([BSI-DSZ-CC-0782-V2-2015]). 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 [BSI-DSZ-CC-0782-V2-2015]).
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 v2.15-i on Infineon M7892 B11 embedding MICAO SAC/EAC 1.3.69 application » 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 [PLF_BADR] et [PLF_SADR] selon la sensibilité de l'application considérée) ;
- les autorités de vérification doivent appliquer le guide [PLF_VAR] ;
- la protection du chargement de toutes les applications sur ce produit doit être activée conformément aux indications de [PLF_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 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 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] 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**	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 MICAO 1.3.69 on IDeal Citiz 2.1.1 SAC/EAC Configuration, 2016_2000021669, v08, 1er août 2017. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security target Lite of IDeal Citiz v2.15-i on Infineon M7892 B11 embedding MICAO SAC/EAC 1.3.69 application, 2017_2000030235, v1.0, 13 septembre 2017.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report (full ETR) – FALCON-R2, LETI.CESTI.FAR2.RTE.001-V1.1, 20 octobre 2017, *CEA LETI*.
[ANA-CRY]	Cotation des mécanismes cryptographiques Application MICAO, LETI.CESTI.FAL.RT.011, v1.0, 20 octobre 2016
[CONF]	Liste de configuration du produit : - Software Release Sheet for MICAO, 2015_2000008933 v3.5, 8 septembre 2017, *SAFRAN I&S*.
[GUIDES]	
[MICAO_AGD_PRE]	MICAO Preparative procedures, 2016_2000018607, v1.9, 27 janvier 2017, *SAFRAN I&S*;
[MICAO_AGD_OPE]	MICAO Operational Guidance, 2016_2000021834, v1.2, 17 octobre 2016, *SAFRAN I&S*;
[PLF_BADR]	IDeal Citiz v2.1.1 – Basic Applet Development Recommendations, 2015_2000013511, v1.0, 19 janvier 2016, *SAFRAN I&S*;
[PLF_SADR]	IDeal Citiz v2.1.1 – Secure Applet Development Recommendations, 2015_2000013510, v1.2, 24 mai 2017, *SAFRAN I&S*;
[PLF_VAR]	IDeal Citiz v2.1.1 – Verification Authority Rules, 2015_2000013512, v1.0, 22 janvier 2016, *SAFRAN I&S*;
[PLF_AGD_PRE]	Preparative procedure for IDealcitiz v2.1.1, 2015_2000011704, v07, 24 mai 2017, *SAFRAN I&S*;
[PLF_AGD_OPE]	Operational user guidance IDealcitiz_v2.1.1, 2015_2000011705, v07, 8 septembre 2017, *SAFRAN I&S*.

[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.*
[PP-JC]	Java Card Protection Profile – Open Configuration, version 3.0, May 2012, Oracle Corporation. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03-M01*.
[PP0068V2]	Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.0, 2 novembre 2011. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0068-V2-2011*.
[PP0056V2]	Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), version 1.3.2, 5 décembre 2012. *Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0056-V2-2012-MA-02.*
[ANSSI-CC-2017/59]	Rapport de certification ANSSI-CC-2017/59, IDeal Citiz v2.15-i on M7892 B11 – Java Card Open Platform, 9 novembre 2017, ANSSI.
[BSI-DSZ-CC-0782-V2-2015]	BSI-DSZ-CC-0782-V2-2015 for Infineon 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), 3 novembre 2015, BSI.
[BSI-DSZ-CC-0782-V2-2015-RA-01]	Assurance Continuity Reassessment Report, BSI-DSZ-CC-0782-V2-2015-RA-01, Infineon 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), 7 avril 2017, BSI.

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 : - Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[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]	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.