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-2018/22

IDeal Citiz v2.15i on Infineon M7892 B11 embedding ID.me 1.4.8B Application

Paris, le 9 juillet 2018

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-2018/22

Nom du produit

IDeal Citiz v2.15i on Infineon M7892 B11 embedding ID.me 1.4.8B Application

Référence/version du produit

OFFICIEL_IDME_1_4_8B_IDealCitiz_SLE78CLFX4000PM_2_1_5_0_R2

Conformité à un profil de protection

Protection profiles for secure signature creation device :

Part 2: Device with key generation, v2.0.1 ;
Part 3: Device with key import, v1.0.2 ;
Part 4: Extension for device with key generation and trusted communication with certificate generation application, v1.0.1 ;
Part 5: Extension for device with key generation and trusted communication with signature creation application, v1.0.1 ;
Part 6: Extension for device with key import and trusted communication with signature creation application, v1.0.4.

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	Infineon Technologies AG
8 Chaussée Jules César, 95520 Osny, France	**AIM CC SM PS – Am Campeon 1-12, 85579 Neubiberg, Allemagne**

Commanditaire

Idemia

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

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

1.1. Présentation du produit

Le produit évalué est « IDeal Citiz v2.15i on Infineon M7892 B11 embedding ID.me 1.4.8B Application » développé par *IDEMIA* et *INFINEON TECHNOLOGIES AG*.

Ce produit est une carte à puce constituée d'un logiciel conforme au standard IAS ECC v1.0.1. Ce produit est destiné à être utilisé comme dispositif sécurisé de création de signature (SSCD[1]). Il peut être utilisé dans différents types de documents (carte d'identité, permis de conduire, carte d'entreprise, passeport, etc.) disposant d'interfaces avec et/ou sans contact.

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.

Elle est conforme aux profils de protection [PP-SSCD-Part2], [PP-SSCD-Part3], [PP-SSCD-Part4], [PP-SSCD-Part5] et [PP-SSCD-Part6].

1.2.2. Architecture

Le produit est constitué :

- du microcontrôleur M7892 B11 et de ses bibliothèques logicielles, certifiés sous la référence [CER-IC] ;
- de la plateforme *Java Card* ouverte cloisonnante « IDeal Citiz v2.15-i on M7892 B11-Java Card Open Platform » certifiée sous la référence [CER-PTF]. Pour rappel, le service de génération de clés RSA de cette plateforme n'est pas revendiqué comme fonction de sécurité ;
- de l'application « ID.me v1.4.8B » découpée en deux modules. Le premier module fournit les services SSCD et le second module, optionnel, fournit les services PKI[2].

Tous ces éléments font partie de la cible d'évaluation (TOE).

[1] *Secure Signature Creation Device.*
[2] *Public Key Intrastructure.*

1.2.3. Services de sécurité

Les services de sécurité fournis par le produit sont décrits dans [ST]. Les principaux services sont :

- la création de signature ou de sceau électronique ;
- la génération des clés de signature (c'est-à-dire la génération de la donnée de création de signature (SCD[1]) et de la donnée de vérification de signature (SVD[2]) associée) ;
- l'import des clés de signature (c'est-à-dire de la SCD et, optionnellement, de la SVD associée) ;
- l'export de clé publique (c'est-à-dire la SVD) ;
- l'établissement d'un canal de confiance pouvant permettre la création de signature électronique, l'import de la SCD ou l'export de la SVD dans un environnement non protégé ;
- l'authentification du porteur de carte basée sur la vérification d'un code PIN ou de données biométriques appelés aussi donnée d'authentification de référence (RAD[3]) ;
- le déblocage de la RAD.

Les principaux services de sécurité de la plateforme sont décrits dans [CER-PTF].

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 [PTF_PRE] :

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

Donnée	Valeur attendue
IC Fabricator	0x8100
IC Type	0x7805 pour SLE78CLFX4000PM
	0x7801 pour SLE78CLFX4000P
	0x7813 pour SLE78CFX4000P
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* ID.me est présentée dans le guide [APP_PRE] :

- les *Executable Load Files* suivants sont présents :

Objet	AID
Common Executable Load File	A000000002434C4A4652
LJFS Executable Load File	A000000002434C4A4653
ID.me Service Executable Load File	A000000002434C4A4654

[1] *Signature Creation Data.*
[2] *Signature Verification Data.*
[3] *Reference Authentication Data.*

PKI Service Executable Load File (optional)	A000000002434C4A4655

- en fonction du support des services PKI, les *Executable Load Files* et *Executable Module* suivants sont présents :

Objet	AID
no pki service configuration ID.me Executable Load File ID.me Executable Module	 A0000000024349444D44 A0000000024349444D4401
full service configuration ID.me Executable Load File ID.me Executable Module	 A0000000024349444D45 A0000000024349444D4501

- la version de *l'applet* « ID.me » est 1.4.8B.

1.2.5. Cycle de vie

Le cycle de vie du produit est présenté au chapitre 4 de la cible de sécurité [ST]. Il est composé des phases listées dans le tableau suivant, pouvant être regroupées en quatre étapes :

- le développement (phases 1 et 2) ;
- la production (phases 3 à 5) ;
- la préparation (phase 6) ;
- l'état opérationnel (phase 7).

Le point de livraison de la TOE est en sortie de la phase 4.

Phases	Tâches	Classes d'assurance	Acteurs ou Sites
1	Développement du logiciel embarqué	ALC	*IDEMIA* (Osny) [CER-PTF]
2	Développement du microcontrôleur	ALC	Sites de [CER-IC]
3	Fabrication	ALC	Sites de [CER-IC]
4	*Packaging*	ALC	Sites de [CER-IC] *IDEMIA* (Noida, Ostrava, Harlem)
Point de livraison de la TOE			
5	Pré-personnalisation	AGD_PRE	Agent de pré-personnalisation
6	Personnalisation	AGD_PRE	Agent de personnalisation
7	Utilisation	AGD_OPE	Utilisateur final

Le produit a été développé sur les sites suivants :

***IDEMIA* - Osny**	***IDEMIA* - Ostrava**	***IDEMIA* - Haarlem**	***IDEMIA* - Noida**
18 Chaussée Jules César, 95520 Osny, France	Jelinkova 1174/3A, 72100 Ostrava, Czech	Oudeweg 32, 2031 CC Haarlem, The Netherlands	Syscom Corporation Private Limited Plot No. 60-61, NSEZ, Phase-II Dadri Road, Noida-201305, Uttar Pradesh, India

Les sites de développement de la plateforme et du composant sont couverts par les certificats [CER-PTF] et [CER-IC].

1.2.6. Configuration évaluée

Le certificat porte sur les configurations suivantes :

- l'application « ID.me v1.4.8B » sans le support des services PKI ;
- l'application « ID.me v1.4.8B » avec les services PKI (en *full service configuration*).

La configuration ouverte du produit a été évaluée conformément à [OPEN] dans le cadre de la certification de la plateforme [CER-PTF]. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées dans [CER-PTF] ne remet pas en cause le présent rapport de certification.

L'application « ID.me v1.4.8B » a été vérifiée conformément aux contraintes décrites dans les guides de la plateforme, référencés dans [CER-PTF].

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].

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 de la plateforme « IDeal Citiz v2.15-i on M7892 B11 – 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 a été certifiée le 9 novembre 2017 sous la référence ANSSI-CC-2017/59, voir [CER-PTF].

L'évaluation s'appuie sur les résultats d'évaluation du produit « ID.me 1.28 on IDeal Citiz MOSID V2.1.1 » certifié le 15 novembre 2016 sous la référence ANSSI-CC-2016/70, voir [CER-REU].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 12 mars 2018, 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 4.10 du guide [APP_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]. 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 [CER-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 v2.15i on Infineon M7892 B11 embedding ID.me 1.4.8B 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 :

- les recommandations des [GUIDES] doivent être strictement appliquées pendant les phases de « Pré-personnalisation » et « Personnalisation », en particulier lors de la configuration du support des services PKI ;
- les guides référencés dans le rapport de certification de la plateforme [CER-PTF] doivent être suivis. Ainsi :
    - toutes les futures applications chargées sur ce produit doivent respecter les contraintes de développement de la plateforme (guides [PTF_BADR] et [PTF_SADR] selon la sensibilité de l'application considérée) ;
    - les autorités de vérification doivent appliquer le guide [PTF_VAR] ;
    - la protection du chargement de toutes les futures applications chargées sur ce produit doit être activée conformément aux indications de [PTF_PRE].

3.4. Reconnaissance du certificat

3.4.1. Reconnaissance européenne (SOG-IS)

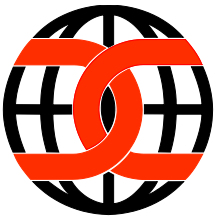
Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

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 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 :

3.4.2. 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 of IDeal Citiz v2.15I on Infineon M7892 B11 embedding ID.me 1.4.8B application, version 09, référence 2017_2000024606, 7 septembre 2017, *IDEMIA* (ex. *SAFRAN I&S*). 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 v2.15I on Infineon M7892 B11 embedding ID.me 1.4.8B application, version 1.0, référence 2017_2000026889, 13 octobre 2017, *IDEMIA* (ex. *SAFRAN I&S*).
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – PHENIX, version 1.2, référence LETI.CESTI.PHE.RTE.001, 12 mars 2018.
[ANA-CRY]	Cotation des mécanismes cryptographiques – Application ID.me, version 1.0, référence LETI.CESTI.PHE.RT.008, 28 avril 2017.
[CONF]	Liste de configuration du produit : - ALC – ID.me Software Release Sheet, version 1.3, référence 2017_2000026007, 9 mars 2018, *IDEMIA* (ex. *SAFRAN I&S*).

[GUIDES] [APP_PRE] [APP_Perso] [APP_OPE] [APP_UM] [PTF_BADR] [PTF_SADR] [PTF_ VAR] [PTF_PRE] [PTF_OPE]	Guides d'installation du produit : - ID.me Preparative Procedure, version 2.7, référence 2016_2000016364, 13 juillet 2017, *IDEMIA* (ex. *SAFRAN I&S*) ; - ID.me Personalization Specification, version 2.9, référence 2015_2000014062, 17 mars 2017 *IDEMIA* (ex. *SAFRAN I&S*). Guides d'installation du produit : - ID.me Operational Guidance, version 2.1, référence 2016_2000016363, 23 février 2017, *IDEMIA* (ex. *SAFRAN I&S*) ; - ID.me User Manual, version 3.0, référence 2015_2000014061, 9 août 2017, *IDEMIA* (ex. *SAFRAN I&S*). Guides de la plateforme : - IDeal Citiz v2.1.1 – Basic Applet Development Recommendations, réf. 2015_2000013511, v1.0, 19 janvier 2016, *IDEMIA* (ex. *SAFRAN I&S*) ; - IDeal Citiz v2.1.1 – Secure Applet Development Recommendations, réf. 2015_2000013510, v1.2, 24 mai 2017, *IDEMIA* (ex. *SAFRAN I&S*) ; - IDeal Citiz v2.1.1 – Verification Authority Rules, réf. 2015_2000013512, v1.0, 22 janvier 2016 *IDEMIA* (ex. *SAFRAN I&S*) ; - Preparative procedure for IDealcitiz v2.1.1, réf 2015_2000011704, v07, 24 mai 2017, *IDEMIA* (ex. *SAFRAN I&S*) ; - Operational user guidance IDealcitiz_v2.1.1, réf 2015_2000011705, v07, 8 septembre 2017, *IDEMIA* (ex. *SAFRAN I&S*).
[PP-SSCD-Part2]	Protection profiles for secure signature creation device – Part 2: Device with key generation, référence : prEN 14169-2:2012, version 2.0.1 datée du 23 janvier 2012. *Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 21 février 2012 sous la référence BSI-CC-PP-0059-2009-MA-01.*
[PP-SSCD-Part3]	Protection profiles for secure signature creation device – Part 3: Device with key import, référence : prEN 14169-3:2012, version 1.0.2 datée du 24 juillet 2012. *Certifié par le BSI le 27 septembre 2012 sous la référence BSI-CC-PP-0075-2012.*
[PP-SSCD-Part4]	Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, référence : prEN 14169-4:2012, version 1.0.1 datée du 14 novembre 2012. *Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0071-2012.*

[PP-SSCD-Part5]	Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, référence : prEN 14169-5:2012, version 1.0.1 datée du 14 novembre 2012. *Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0072-2012.*
[PP-SSCD-Part6]	Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application, référence : prEN 14169-6:2013, version 1.0.4 datée du 3 avril 2013. *Certifié par le BSI le 16 avril 2013 sous la référence BSI-CC-PP-0076-2013.*
[CER-PTF]	IDeal Citiz v2.15-i on M7892 B11 – Java Card Open Platform. *Certifiée par l'ANSSI le 9 novembre 2017 sous la référence ANSSI-CC-2017/59.*
[CER-IC]	Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013, and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware). *Certifié par le BSI le 5 septembre 2017 sous la référence BSI-DSZ-CC-0782-V3-2017.*
[CER-REU]	ID.me 1.28 on IDeal Citiz MOSID V2.1.1. *Certifiée par l'ANSSI le 15 novembre 2016 sous la référence ANSSI-CC-2016/70.*

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 1.4, 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.