



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-2018/44**

### **IDeal Citiz v2.17-i on Infineon M7892 B11 embedding ID.me 1.6-i application**

*Paris, le 5 octobre 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](mailto:certification@ssi.gouv.fr)

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



Référence du rapport de certification

**ANSSI-CC-2018/44**

Nom du produit

**IDEal Citiz v2.17-i on Infineon M7892 B11 embedding  
ID.me 1.6-i application**

Référence/version du produit

**1.6-i**

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**  
8, chaussée Jules César,  
95520 Osny, France

**Infineon Technologies AG**  
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



**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](http://www.ssi.gouv.fr).



# Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
1.1. PRESENTATION DU PRODUIT .....	6
1.2. DESCRIPTION DU PRODUIT .....	6
1.2.1. <i>Introduction</i> .....	6
1.2.2. <i>Architecture</i> .....	6
1.2.3. <i>Services de sécurité</i> .....	7
1.2.4. <i>Identification du produit</i> .....	7
1.2.5. <i>Cycle de vie</i> .....	8
1.2.6. <i>Configuration évaluée</i> .....	8
<b>2. L’EVALUATION .....</b>	<b>10</b>
2.1. REFERENTIELS D’EVALUATION .....	10
2.2. TRAVAUX D’EVALUATION .....	10
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI .....	10
2.4. ANALYSE DU GENERATEUR D’ALEAS .....	11
<b>3. LA CERTIFICATION .....</b>	<b>12</b>
3.1. CONCLUSION .....	12
3.2. RESTRICTIONS D’USAGE .....	12
3.4. RECONNAISSANCE DU CERTIFICAT .....	13
3.4.1. <i>Reconnaissance européenne (SOG-IS)</i> .....	13
3.4.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....	13
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT .....</b>	<b>14</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>15</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>18</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est une *applet* Java Card « IDeal Citiz v2.17-i on Infineon M7892 B11 embedding ID.me 1.6-i application » développée par *IDEMIA* et *INFINEON TECHNOLOGIES AG*.

Ce produit offre des services d'authentification et de signature électronique (SSCD<sup>1</sup>) conformes aux spécifications IAS ECC v1.0.1. Il est embarqué sur la plateforme [CER\_PTF] préalablement certifiée et 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].

Elle se base également sur le profil de protection [PP-EAC2] pour les fonctions additionnelles du protocole EAC V2.

### 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 [CER-PTF] ;
- de l'application « ID.me v1.6-i » découpée en trois modules. Le premier module fournit les services SSCD et les deux autres qui sont optionnels, fournissent les services PKI<sup>2</sup> IAS ECC et EAC2.

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

---

<sup>1</sup> *Secure Signature Creation Device.*

<sup>2</sup> *Public Key Infrastructure.*



### 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 (SCD1) et de la donnée de vérification de signature (SVD2) 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 également données d'authentification de référence (RAD3) ;
- 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	0x7801 pour SLE78CLFX4000P
	0x7805 pour SLE78CLFX4000PM
	0x7813 pour SLE78CFX4000P
	0x7877 pour SLE78CLFX4007PM
	0x7878 pour SLE78CLFX4007P
	0x7985 pour SLE78CLFX408AP
	0x7986 pour SLE78CLFX408APM
Operating System Identifier	0x4921
Operating System Release Date	0x8030
Operating System Release Level	0x2171

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

<sup>1</sup> Signature Creation Data.

<sup>2</sup> Signature Verification Data.

<sup>3</sup> Reference Authentication Data.

- 2) La méthode d'identification de l'*applet* ID.me est présentée dans le guide [APP\_PRE] §4.1.3 pour les différentes valeurs des *Executable Load Files* et au §4.1.4 pour les différentes valeurs des *Executable Modules*.

### 1.2.5. Cycle de vie

Le cycle de vie du produit est présenté au chapitre 4 de la cible de sécurité [ST].

La TOE est développée et produite sur les sites suivants :

Développement	<p><b>IDEMIA – Noida</b>                      Syscom Corporation Private Limited                      R&amp;D area                      D-216 and D-217 Sector - 63                      Noida 201301,                      Uttar Pradesh,                      India</p>
	<p><b>IDEMIA - Osny</b>                      18 Chaussée Jules César,                      95520 Osny,                      France</p>
Production	<p><b>IDEMIA - Ostrava</b>                      Jelinkova 1174/3A,                      72100 Ostrava,                      Czech</p>
	<p><b>IDEMIA - Haarlem</b>                      Oudeweg 32,                      2031 CC Haarlem,                      The Netherlands</p>
	<p><b>IDEMIA – Vitré</b>                      Avenue d'Helmstedt                      BP 90308                      35503 Vitré Cedex                      France</p>
	<p><b>IDEMIA - Shenzhen</b>                      4F, Great wall technology building                      No 2, Kefa Rd                      Science and technology park,                      Nanshan district                      Shenzhen, 518057                      PR of China</p>

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

Selon sa configuration, le produit peut offrir jusqu'à trois services pour répondre aux différentes infrastructures à clés publiques (PKI) possibles :



- pas de PKI ;
- PKI IAS ;
- PKI EAC : nouveau *package* qui supporte le protocole EAC version 2 [PP-EAC2].

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.

LA TOE a été vérifiée conformément aux contraintes décrites dans les guides de la plateforme, référencées 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 [CER-PTF].

L'évaluation s'appuie également sur les résultats d'évaluation du produit [CER-REU].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 7 septembre 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 scrupuleusement respectées.

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.

## 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 v2.17-i on Infineon M7892 B11 embedding ID.me 1.6-i 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 ;
- En phase de (pré-)personnalisation, si les données échangées requièrent une protection en confidentialité et intégrité (en environnement non sécurisé par exemple), le protocole SCP03 doit être utilisé avec le générateur aléatoire basé sur la norme SP800-90A et l'AES-128 ;
- les guides référencés dans le rapport de certification de la plateforme [CER-PTF] doivent être suivis. Ainsi :
  - o 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) ;
  - o les autorités de vérification doivent appliquer le guide [PTF\_VAR] ;
  - o 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<sup>1</sup>, 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<sup>2</sup>, 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 :



---

<sup>1</sup> La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : [www.sogis.org](http://www.sogis.org).

<sup>2</sup> La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : [www.commoncriteriaportal.org](http://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	
<b>ADV</b> 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
<b>AGD</b> 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
<b>ALC</b> 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
<b>ASE</b> 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
<b>ATE</b> 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
<b>AVA</b> 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"><li>- Security Target IDeal Citiz v2.17-i embedding ID.me 1.6-i application, version 1.4, référence 2018_2000034144, 5/9/2018, <i>IDEMIA</i>.</li></ul> <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"><li>- Security Target Lite IDeal Citiz v2.17-i embedding ID.me 1.6-i application, version 1.0, référence 2018_2000037323, 5/9/2018, <i>IDEMIA</i>.</li></ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"><li>- Evaluation Technical Report – DUCK, référence LETI.CESTI.DUC.RTE.001, version 1.0, 7/9/2018, <i>CEA LETI</i>.</li></ul>
[ANA-CRY]	<p>Cotation des mécanismes cryptographiques – Application ID.me 1.6i, référence LETI.CESTI.DUC.RT.002, version 1.1, 18/9/2018, <i>CEA LETI</i>.</p>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"><li>- Software Release Sheet for ID.me 1.6-I application, version 1.3, référence 2018_2000034157, 5/9/2018, <i>IDEMIA</i>.</li></ul>

<p>[GUIDES]</p> <p>[APP_PRE]</p> <p>[APP_Perso]</p> <p>[APP_OPE]</p> <p>[APP_UM]</p> <p>[PTF_BADR]</p> <p>[PTF_SADR]</p> <p>[PTF_VAR]</p> <p>[PTF_PRE]</p> <p>[PTF_OPE]</p> <p>[GPJ_API]</p>	<p>Guides d'installation du produit :</p> <ul style="list-style-type: none"> <li>- ID.me 1.6-i application - Preparative Procedures, version 1.5, référence 2018_2000034155, 5/9/2018, <i>IDEMIA</i> ;</li> <li>- ID.me 1.6-i application - Personalization Specification, version 1.5, référence 2018_2000034156, 20/8/2018, <i>IDEMIA</i>.</li> </ul> <p>Guide opérationnel du produit :</p> <ul style="list-style-type: none"> <li>- ID.me 1.6-i - Operational Guidance, version 1,3, référence 2018_2000034153, 31/5/2018, <i>IDEMIA</i>.</li> </ul> <p>Guide utilisateur du produit :</p> <ul style="list-style-type: none"> <li>- ID.me 1.6-i - User Manual, version 1.4, référence 2018_2000034154, 20/8/2018, <i>IDEMIA</i>.</li> </ul> <p>Guides de la plateforme :</p> <ul style="list-style-type: none"> <li>- IDeal Citiz v2.1.3 – Basic Applet Development Recommendations, référence 2018_2000033656, version 0.1, 1/2/2018, <i>IDEMIA</i> ;</li> <li>- IDeal Citiz v2.1.3 – Secure Applet Development Recommendations, référence 2018_2000033655, version 0.3, 12/4/2018, <i>IDEMIA</i> ;</li> <li>- IDeal Citiz v2.1.3 – Verification Authority Rules, référence 2018_2000033657, version 0.1, 1/2/2018, <i>IDEMIA</i> ;</li> <li>- Preparative procedure for Idealcitiz v2.1.3, référence 2018_2000031819, version 1.0, 12/6/2018, <i>IDEMIA</i> ;</li> <li>- IDeal Citiz_v2.1.3 OPE - Operational User Guidance, référence 2018_2000031818, version 1.0, 12/6/2018, <i>IDEMIA</i> ;</li> <li>- IDeal Citiz_v2.1.3 Global Platform and JavaCard API, référence 2017_2000031074, version 2.0, 18/4/2018, <i>IDEMIA</i>.</li> </ul>
<p>[PP-SSCD-Part2]</p>	<p>Protection profile for secure signature creation device – Part 2: Device with key generation, version 2.0.1, 23 janvier 2012.  <i>Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 21 février 2012 sous la référence BSI-CC-PP-0059-2009-MA-01.</i></p>
<p>[PP-SSCD-Part3]</p>	<p>Protection profile for secure signature creation device – Part 3: Device with key import, version 1.0.2, 25 juillet 2012.  <i>Certifié par le BSI le 27 septembre 2012 sous la référence BSI-CC-PP-0075-2012.</i></p>
<p>[PP-SSCD-Part4]</p>	<p>Protection profile for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, version 1.0.1, 19 novembre 2012.  <i>Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0071-2012.</i></p>



[PP-SSCD-Part5]	Protection profile for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, version 1.0.1, 19 novembre 2012. <i>Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0072-2012.</i>
[PP-SSCD-Part6]	Protection profile for secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application, version 1.0.4, 3 avril 2013. <i>Certifié par le BSI le 16 avril 2013 sous la référence BSI-CC-PP-0076-2013.</i>
[PP-EAC2]	Protection profile for Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110, version 1.01, BSI-CC-PP-0086, Version 1.01, 26 juin 2015. <i>Certifié par le BSI le 13 juillet 2015 sous la référence BSI-CC-PP-0086-2015.</i>
[CER-PTF]	IDeal Citiz v2.17-i on M7892 B11 – Java Card Open Platform. <i>Certifiée par l'ANSSI le 2 juillet 2018 sous la référence ANSSI-CC-2018/27.</i>
[CER-IC]	Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware). <i>Maintenu par le BSI le 9 janvier 2018 sous la référence BSI-DSZ-CC-0782-V4-2018.</i>
[CER-REU]	IDealCitiz 2.15i on Infineon M7892 B11 embedding ID.me 1.4.8B application. <i>Certifiée par l'ANSSI le 9 juillet 2018 sous la référence ANSSI-CC-2018/22.</i>

### 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"> <li>- Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001;</li> <li>- Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002;</li> <li>- Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.</li> </ul>
[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 1.5, octobre 2017.
[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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .

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