



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-2018/45**  
**IDeal Citiz v2.16-i embarquant l'application**  
**VITALE**  
**version 1.2.18**

*Paris, le 19 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-2018/45**

Nom du produit

**IDEal Citiz v2.16-i embarquant l'application VITALE**

Référence/version du produit

**Version 1.2.18**

Conformité à un profil de protection

**Protection profiles for secure signature creation device :**

**[PP-SSCD-Part2]: Device with key generation, version 2.0.1 ;**

**[PP-SSCD-Part3]: Device with key import, version 1.0.2 ;**

**[PP-SSCD-Part4]: Extension for device with key generation and trusted communication with certificate generation application, version 1.0.1 ;**

**[PP-SSCD-Part5]: Extension for device with key generation and trusted communication with signature creation application, version 1.0.1 ;**

**[PP-SSCD-Part6]: Extension for device with key import and trusted communication with signature creation application, version 1.0.4.**

Critères d'évaluation et version

**Critères Communs version 3.1 révision 5**

Niveau d'évaluation

**EAL 4 augmenté**  
**ALC\_DVS.2, AVA\_VAN.5**

Développeurs

**Idemia**  
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, avenue 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](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> .....	7
1.2.6. <i>Configuration évaluée</i> .....	8
<b>2. L'EVALUATION .....</b>	<b>9</b>
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 .....	9
<b>3. LA CERTIFICATION .....</b>	<b>11</b>
3.1. CONCLUSION .....	11
3.2. RESTRICTIONS D'USAGE .....	11
3.3. RECONNAISSANCE DU CERTIFICAT .....	11
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> .....	11
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....	12
<b>ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT .....</b>	<b>13</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>14</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>16</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est la carte à puce « Ideal Citiz v2.16-i embarquant l'application VITALE, version 1.2.18 » développée par *IDEMIA* sur un microcontrôleur fabriqué par la société *INFINEON TECHNOLOGIES*. Il peut être utilisé en mode contact.

Ce produit offre des services de signature électronique (SSCD<sup>1</sup>) aux travers des applications ADELE, VITALE1 et VITALE2, conformes aux profils de protections listés dans le paragraphe 1.2.1, dont :

- 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<sup>2</sup>) et de la donnée de vérification de signature (SVD<sup>3</sup>) 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 appelée également données d'authentification de référence (RAD<sup>4</sup>) ;
- le déblocage de la RAD.

Ce produit est destiné à être utilisé dans le cadre de l'application SESAM Vitale ainsi que pour des applications de signature électronique ; il est livré en configuration fermée et ne permet pas le chargement d'application en post-issuance.

## 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 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, dont l'architecture est détaillée aux chapitres 1 (*Introduction*) et 3 (*TOE Overview*) de la cible de sécurité [ST], est constitué :

---

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

<sup>2</sup> *Signature Creation Data.*

<sup>3</sup> *Signature Verification Data.*

<sup>4</sup> *Reference Authentication Data.*

- du microcontrôleur M7892 B11 et de ses bibliothèques logicielles, certifiés sous la référence [CER-IC] ;
- de la plateforme *Java Card* « IDEal Citiz v2.16-i », certifiée sous la référence [CER-PTF] ;
- des applications ADELE, VITALE1 et VITALE2 contenant les fonctionnalités SSCD ;
- de l'application AIP (Application d'Initialisation et de Personnalisation) qui est une application d'administration utilisée en phase de pré-personnalisation et de personnalisation. Elle est inactive en phase « utilisation ».

Tous ces éléments à l'exception de l'application AIP font partie de la cible d'évaluation (TOE<sup>1</sup>).

### **1.2.3. Services de sécurité**

Les principaux services de sécurité fournis par le produit et décrits au chapitre 3.6 de la cible de sécurité [ST], sont :

- les mécanismes d'authentification (authentification du porteur de la carte, du mécanisme communiquant avec la carte afin d'établir un canal sécurisé, de l'administrateur de la TOE, authentification mutuelle avec l'entité communicante et authentification client/serveur) ;
- la cryptographie (génération de clés SCD/SVD ou de session, destruction de clés, authentification symétrique et asymétrique, création de signature, génération de nombres aléatoires, chiffrement/déchiffrement de message émis, génération et vérification de MAC, échange de clé Diffie-Hellman, calcul de hash, calcul et vérification de certificat, chiffrement/déchiffrement de données) ;
- la gestion de clés (importation de SCD, génération de SCD, désactivation de SCD, création, extension ou modification de certificat, création de SVD, gestion des clés d'authentification)
- la gestion de PIN ;
- la gestion de canaux sécurisés ;
- le contrôle d'accès aux différentes données de l'applet ;
- le stockage des données ;
- l'intégrité et la confidentialité des données sensibles.

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 en se référant au guide [KIW-PRE] §3.

Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans le guide [KIW-PRE] §3.

### **1.2.5. Cycle de vie**

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

---

<sup>1</sup> *Target of Evaluation.*

Le produit a été développé sur les sites suivants :

<p><b>IDEMIA - Osny</b> 18 Chaussée Jules César, 95520 Osny, France</p>	<p><b>IDEMIA – Meyreuil</b> Site ARTEPARC, Route de la côte d'Azur 13590 Meyreuil, France</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***

Le certificat porte sur la configuration telle que présentée au paragraphe 1.2.

## 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].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 1<sup>er</sup> octobre 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 8 du guide [KIW-PRE] doivent être 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 v2.16-i embarquant l'application VITALE, version 1.2.18 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 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 scrupuleusement les recommandations se trouvant dans les guides fournis [GUIDES].

### 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<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 :



---

<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).

### 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<sup>1</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 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 4+	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	4	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	1	Implementation representation of TSF
	ADV_INT					2	3	3			
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	3	3	Basic 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	4	4	Problem tracking 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	1	1	Well-defined development tools
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	1	1	Testing: basic 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"> <li>- Security Target IDEal Citiz v2.16-i embedding VITALE application, référence 2017_2000024672, version 1.3, 24 septembre 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 v2.16-i embedding vitale application, référence 2018_2000035874, version 1.2, 24 septembre 2018, <i>IDEMIA</i>.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- KIWI - Rapport Technique d'Evaluation, référence LETI.CESTI.KIW.ETR.001, version 2.1, 1 octobre 2018, <i>CEA-LETI</i>.</li> </ul>
[ANA-CRY]	<p>Cotation des mécanismes cryptographiques – KIWI, référence LETI.CESTI.KIW.RT.007, version 1.0, 24 mai 2018, <i>CEA-LETI</i>.</p>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> <li>- VITALE2 applet 1st source – Software Release Sheet, référence 2018_2000035218, version 1.5, 24 septembre 2018, <i>IDEMIA</i>.</li> </ul>
[GUIDES]	<p>[KIW-OPE] Guide d'utilisation Manuel utilisateur, référence 2018_2000033538, version 1.4, 11 septembre 2018, <i>IDEMIA</i>.</p> <p>[KIW-PRE] Guide d'utilisation Manuel de Pré-Personnalisation – Personnalisation, référence 2018_2000033539, version 1.6, 19 septembre 2018, <i>IDEMIA</i>.</p>
[CER-PTF]	<p>IDEal Citiz v2.16-i on M7892 B11 – Java Card Open Platform.</p> <p><i>Certifiée par l'ANSSI le 8 janvier 2018 sous la référence ANSSI-CC-2017/74.</i></p>
[CER-IC]	<p>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).</p> <p><i>Maintenu par le BSI le 9 janvier 2018 sous la référence BSI-DSZ-CC-0782-V4-2018.</i></p>
[PP-SSCD-Part2]	<p>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.</p> <p><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>



[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. <i>Certifié par le BSI le 27 septembre 2012 sous la référence BSI-CC-PP-0075-2012.</i>
[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. <i>Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0071-2012.</i>
[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. <i>Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0072-2012.</i>
[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. <i>Certifié par le BSI le 16 avril 2013 sous la référence BSI-CC-PP-0076-2013.</i>

### Annexe 3. Références liées à la certification

<p>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.</p>	
[CER/P/01]	<p>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.</p>
[CC]	<p>Common Criteria for Information Technology Security Evaluation :</p> <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]	<p>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.</p>
[JIWG IC] *	<p>Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.</p>
[JIWG AP] *	<p>Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.</p>
[COMP] *	<p>Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.5, octobre 2017.</p>
[OPEN]	<p>Certification of « Open » smart card products, version 1.1 (for trial use), 4 février 2013.</p>
[CC RA]	<p>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.</p>
[SOG-IS]	<p>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.</p>
[REF]	<p>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>.</p> <p>Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>.</p>

Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS\_B3), voir [www.ssi.gouv.fr](http://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.