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-2016/64

Applet ID.me v1.12
sur la plateforme IDeal Citiz v2.1

Paris, le 11 octobre 2016

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-2016/64

Nom du produit

Applet ID.me v1.12 sur la plateforme IDeal Citiz v2.1

Référence/version du produit

Applet version 1.12, plateforme version 2.1

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 4

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

MORPHO
18 Chaussée Jules César,
95520 Osny, France

INFINEON Technologies AG
AIM CC SM PS – Am Campeon 1-12,
85579 Neubiberg, Allemagne

Commanditaire

Safran Identity & Security (anciennement MORPHO)

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

Le produit est reconnu au niveau EAL4.

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 l'Applet ID.me v1.12 sur la plateforme IDeal Citiz v2.1 développée par *MORPHO* sur un microcontrôleur d'*INFINEON*.

Ce produit est destiné à être utilisé comme dispositif sécurisé de création de signature (*SSCD, Secure signature creation device*).

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 *Protection profiles for secure signature creation device* [PP-SSCD-Part2], [PP-SSCD-Part3], [PP-SSCD-Part4], [PP-SSCD-Part5] et [PP-SSCD-Part6].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par ID.me sont :

- la génération de la donnée de création de signature (*Signature Creation Data* ou SCD) et de la donnée de vérification de signature (*Signature Verification Data* ou SVD) associée ;
- l'export de la donnée de vérification de signature (SVD) pour une création de certificat électronique ;
- l'import de la donnée de création de signature (SCD) et de la donnée de vérification de signature (SVD) associée ;
- la réception et le stockage du certificat électronique ;
- le passage de l'état non-opérationnel à l'état opérationnel ;
- la création de signature électronique via un canal de confiance ;
- l'authentification de l'administrateur ;
- l'authentification du signataire par un code PIN ou des données biométriques.

1.2.3. Architecture

Le produit est constitué :

- de la plateforme ouverte cloisonnante « IDeal Citiz v2.1 Open platform » (voir [ANSSI-CC-2015/45]) ;
- de l'application ID.me procurant les services SSCD ;
- de l'application MICAO.

La cible d'évaluation (TOE) est constituée de l'application ID.me v1.12 sur la plateforme Ideal Citiz v2.1.
L'application MICAO a été prise en compte dans le processus d'évaluation conformément aux prescriptions de [JIL_OPEN] applicables aux *known applications*. Cette application a été

vérifiée conformément aux contraintes de développements d'applications décrites dans le guide [PLF_BADR] 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
Operating System Identifier	0x4921
Operating System Release Date	0x5079
Operating System Release Level	0x2101

- 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 [ID.me_AGD_PRE] :

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

Objet	AID
ID.me Executable Load File	A00000000024349444D45
LJFS Executable Load File	A000000002434C4A4653
ID.me Executable Module	A00000000024349444D4501

- la version de l'applet ID.me est 1.12 (0x01 0x0C dans la réponse à la commande GetDataForID.MeVersion).

3) 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
ID.me Executable Load File	A00000024710
ID.me Executable Module	A0000002471001

- la version de l'applet MICAO est 01.01.03.0001 (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 5.7 de la cible de sécurité [ST].

Les applications ID.me et MICAO sont chargées avant le point de livraison « *Delivery to SSCD Provisioning Service* ». Aucune autre *known application* n'est considérée.

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
MORPHO OSNY	18 Chaussée Jules César 95520 Osny, France	*SSCD Development (Phase 1)*
Voir [BSI-0782-V2]		*SSCD Development (Phase 2)*
MORPHO CARDS CZECH	Jelinkova 1174/3A 72100 Ostrava République Tchèque	*SSCD Production (Phases 3, 4 & 5)*

Le produit est ensuite livré : *Delivery to SSCD Provisioning Service*.
Les phases *SSCD preparation* (Phase 6) et *SSCD operational use* (Phase 7) sont couvertes par la classe d'assurance AGD de l'évaluation.

Des applications peuvent être chargées en phase *SSCD preparation* (Phase 6). Ces applications doivent être développées et 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 et réalisé selon les processus audités ne remet pas en cause le présent rapport de certification.
Le présent rapport de certification porte également sur la configuration du produit obtenue sans embarquer l'application MICAO.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [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 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 le 2 octobre 2015 sous la référence [ANSSI-CC-2015/45].

Le niveau de résistance du microcontrôleur a été confirmé le 3 novembre 2015, voir [BSI-0782-V2]. Le niveau de résistance de la plateforme ouverte a été confirmé le 29 janvier 2016 dans le cadre du processus de surveillance, voir [ANSSI-CC-2015/45-S01].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 24 juin 2016, 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 [ID.me_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-0782-V2]). 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-0782-V2]).
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 « Applet ID.me v1.12 sur la plateforme IDeal Citiz v2.1 » 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 :

- dans le cadre de la qualification renforcée du produit, les recommandations au chapitre 4.10 du guide [ID.me_AGD_PRE] doivent être suivies ;
- 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.
Pour les évaluations enregistrées avant septembre 2014, la reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR lorsque les dépendances CC sont satisfaites.
Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.
[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

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 for ID.me on IDeal Citiz v2.1, 2014_0000002194, Index 05, 8 décembre 2015, Morpho. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target Lite for ID.me on IDeal Citiz v2.1, 2016_2000019402, version 1, août 2016, Morpho.
[RTE]	Evaluation Technical Report (full ETR) – LETI.CESTI.FAL.RTE.012-v1.2, 23 juin 2016, Leti.
[ANA-CRY]	Cotation des mécanismes cryptographiques – Application ID.me, LETI.CESTI.FAL.RT.010, v1.0, 17 décembre 2015, Leti.
[CONF]	Software Release Sheet for ID.ME, 2015_2000008075, version 06, 2 février 2016, Morpho.
[GUIDES]	
[ID.me_AGD_PRE]	ID.me Preparative Guide, 2014_2000002907,v1.3, 20 octobre 2015, Morpho.
[ID.me_UM]	ID.me User Manual, 2014_2000000211, v07, 7 septembre 2015, Morpho.
[ID.me_AGD_OPE]	ID.me Operational Guide, 2014_2000002909, v1.0, 30 septembre 2015, Morpho.
[ID.me_PM]	ID.me Application Personalisation Specification, 2014_0000001563, v12, 7 septembre 2015, Morpho.
[MICAO_AGD_PRE]	MICAO Preparative procedures, 2015_2000006884, v4.0, 1 décembre 2015, Morpho.
[PLF_BADR]	IDeal Citiz v2.1 – Basic Applet Development Recommendations, réf. 2014_2000001499, version 1.0, 7 juillet 2014, Morpho.
[PLF_SADR]	IDeal Citiz v2.1 – Secure Applet Development Recommendations, réf. 2014_2000001501, version 1.3, 3 décembre 2015, Morpho.
[PLF_VAR]	IDeal Citiz v2.1 – Verification Authority Rules, réf. 2014_2000001513, version 1.0, 7 juillet 2014, Morpho.
[PLF_AGD_PRE]	Preparative procedure for IDealcitiz v2.1, réf 2014_2000003597, version 07, 31 juillet 2015, Morpho.
[PLF_AGD_OPE]	Operational user guidance IDealcitiz_v2.1, réf 2014_2000004459, version 03, 31 juillet 2015, Morpho.

[PP_JC]	Java Card Protection Profile – Open Configuration, version 3.0, May 2012, Oracle Corporation. Certifié par l'ANSSI sous la reference ANSSI-CC-PP-2010/03-M01.
[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.*
[ANSSI-CC-2015/45]	IDeal Citiz v2.1 Open platform, Rapport de certification ANSSI-CC-2015/45, 2 octobre 2015.
[BSI-0782-V2]	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.
[ANSSI-CC-2015/45-S01]	IDeal Citiz v2.1 Open platform, Rapport de surveillance ANSSI-CC-2015/45-S01, 29 janvier 2016.

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 CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, 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, mai 2000.
[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.