PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification
ANSSI-CC-2020/70
IAS Classic v5.0 with MOC Server v3.0 on MultiApp v4.2 (Version 5.0.0.A.C, version 3.0.1A)

Paris, le 9 novembre 2020

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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-2020/70

Nom du produit

IAS Classic v5.0 with MOC Server v3.0 on MultiApp v4.2

Référence/version du produit

Version 5.0.0.A.C, version 3.0.1A

Conformité à un profil de protection

Protection profiles for secure signature creation device:

Part 2 : Device with key generation, v2.0.1, BSI-CC-PP-0059-2009-MA-02 ;
Part 3 : Device with key import, v1.0.2, BSI-CC-PP-0075-2012-MA-01 ;
Part 4 : Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, BSI-CC-PP-0071-2012-MA-01 ;
Part 5 : Extension for device with key generation and trusted communication with signature creation application, v1.0.1, BSI-CC-PP-0072-2012-MA-01 ;
Part 6 : Extension for device with key import and trusted communication with signature creation application, v1.0.4, BSI-CC-PP-0076-2013-MA-01.

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté
ALC_DVS.2, AVA_VAN.5

Développeur

THALES
6, rue de la Verrerie,
92197 Meudon cedex, France

Développeurs

THALES
6, rue de la Verrerie,
92197 Meudon cedex, France

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

Commanditaire

THALES
6, rue de la Verrerie,
92197 Meudon cedex, France

Centre d'évaluation

SERMA SAFETY & SECURITY
14 rue Galilée, CS 10071,
33608 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

Ce certificat est reconnu au niveau EAL2.

SOG-IS

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « IAS Classic v5.0 with MOC Server v3.0 on MultiApp v4.2, Version 5.0.0.A.C, version 3.0.1A » développé par THALES et embarqué sur le microcontrôleur développé et fabriqué par INFINEON TECHNOLOGIES AG.

Ce produit est de type « carte à puce » 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.

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 le produit sont :

- la création de signature ou de sceau électronique dans un environnement où la sécurité repose sur des mesures organisationnelles ;
- la génération des clés de signature (c'est-à-dire la génération de la donnée de création de signature (SCD[2]) et de la donnée de vérification de signature (SVD[3]) 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) vers le CGA[4] ;
- l'authentification du signataire par un code PIN ou des données biométriques d'empreintes digitales (BioPIN) ;
- l'authentification de l'administrateur (authentification mutuelle) ;
- l'intégrité des conditions d'accès aux données protégées SCD et RAD[5] ;
- l'intégrité des données à signer DTBS[6] ;
- la protection en intégrité et en confidentialité, des données lues à l'aide du mécanisme de « Secure Messaging ».

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

[1] *Secure Signature Creation Device*.

[2] *Signature Creation Data*.

[3] *Signature Verification Data*.

[4] *Certifiation Generation Application*.

[5] *Reference Authentication Data*.

[6] *Data To Be Signed*.

1.2.3 *Architecture*

L'architecture du produit est décrite au chapitre 2.2 de la cible de sécurité [ST]. Elle est constituée :

- du microcontrôleur « IFX_CCI_000010h », développé par INFINEON TECHNOLOGIES AG et certifié sous la référence [CER-IC] ;
- de la plateforme Java Card ouverte « MultiApp V4.2 » certifiée sous la référence [CER-PTF] ;
- des applications :
  - « IAS Classic V5.0 » mise à disposition de l'utilisateur pour lui permettre de signer électroniquement ses données ;
  - « MOC server V3.0 » utilisée pour réaliser du Match On Card.

Des applications peuvent être chargées sur la plateforme Java Card ouverte, au côté des applications « IAS Classic V5.0 » et « MOC server V3.0 ». La conformité aux prescriptions du document [OPEN] pour le chargement d'applications a été prise en compte pour les seules applications identifiées dans le certificat de la plateforme [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 détaillés dans le chapitre 1.3 de la cible de sécurité [ST].

1.2.5 *Cycle de vie*

Le cycle de vie est décrit au chapitre 2.3 de la cible de sécurité [ST]. Il est décomposé en sept phases conformes au profil de protection [PP0084].

Les phases 1 et 2 correspondent au développement du produit, plus précisément au développement du logiciel embarqué (*firmware*). Les phases 3 et 4 correspondent à la fabrication et au conditionnement (*packaging*) du produit. La phase 5 correspond au chargement de l'application.

Il est à noter que le point de livraison, ou d'émission de la carte, est en sortie de phase 5.

Le produit a été développé sur les sites suivants :

THALES Meudon [MDN] 6 Rue de la Verrerie 92190 Meudon, France	**THALES Singapore** [SGP] 12 Ayer Rajah Crescent Singapor 139941, Singapour
THALES Gémenos [GEM] et [GMN-VZN] Avenue du Pic de Bertagne 13881 Gémenos, France	**THALES Tczew** [TCZ] Ul. Skarszewska 2 33-110 Tczew, Poland
ATOS Paris (Aubervilliers / Croissy) [PAR] 4 rue des Vieilles Vignes 77 183 Croissy-Beaubourg, France	**THALES Montgomeryville** [MGY] 101 & 106 Park Drive Montgomeryville, PA 18 936 United States
THALES Pont-Audemer [PAU] Z.I. Saint Ulfrant rue de Saint Ulfran 27500 Pont-Audemer, France	**ATOS Marcoussis** [MAR] DATA 4, 3 route de Marcoussis, 91620 Nozay, France

THALES Calamba [CAL-VZN] Building 7-A, Southern Luzon Industrial Complex Purok 3, Barangay Batino Calamba City, 4027 Laguna Philippines	**ATOS Pune** [PUN2] Embassy Tech Zone, Phase II, Rajiv Gandhi Infotech Park, MIDC, Hinjewadi, Pune – 411057, India
THALES Curitiba [CBA] Cartões e Terminais Ltda, Av Nossa Sra da Boa Esperança, 367 Centro - Pinhais, PR Brazil, CEP : 83323-232	**THALES Vantaa** [VAN] Myllynkivenkuja 4, Vantaa, Finland, FI-01620

Les sites intervenant dans le cycle de vie de la plateforme et du microcontrôleur sont listés respectivement dans [CER-PTF] et [CER-IC].

1.2.6 *Configuration évaluée*

Le certificat porte sur le produit identifié au paragraphe 1.2.4. et configuré comme suit :

- les applets « IAS Classic V5.0 » et « MOC server V3.0 » instanciées sur la plateforme ouverte couverte par le certificat [CER-PTF] ;
- les recommandations du guide [GUIDES] sont strictement appliquées durant la phase « Personnalisation » du cycle de vie, ainsi que dans la phase de pré-personnalisation.

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

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 sur la plateforme déjà certifiée par ailleurs (voir [CER-PTF]).

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme « MultiApp V4.2 » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5. Cette plateforme a été certifiée le 26 juin 2020 sous la référence ANSSI-CC-2020/65, voir [CER-PTF].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 5 novembre 2020, 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 dans le [RTE]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations données dans le document [AGD_CPS] doivent être respectées.

Dans le cadre du processus de qualification renforcée, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI, voir [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 (voir [CER-PTF]).

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 « IAS Classic v5.0 with MOC Server v3.0 on MultiApp v4.2, Version 5.0.0.A.C, version 3.0.1A » 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 AVA_VAN.5 et ALC_DVS.2.

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].

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[7], 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 :

3.3.2 *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[8] , 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 :

[7] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

[8] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. 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	2	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 B. Références documentaires du produits évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - MultiAppV4.2: IAS EN Core & Extensions Security Target, référence D1491739, version 1.7, 31 août 2020, THALES. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - IAS Classic Security Target – Public version IAS Classic V5.0 with MOC Server V3.0 on MultiApp V4.2, référence D1491739, version 1.7p, 31 août 2020, THALES.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report TARSO2 Project, référence TARSO2_ETR_v1.3, version 1.3, 5 novembre 2020, SERMA SAFETY & SECURITY.
[CONF]	Liste de configuration du produit : Configuration List for dev FILES (IAS5.0), référence LIS_IAS50_CODE_1.8, 29 novembre 2019, THALES.
[GUIDES]	Guide d'installation et d'administration du produit : - [AGD_PRE_OPE] MultiApp V4.2: AGD OPE and PRE document - IAS v5.0, version 1.4, 6 mars 2020, référence D1495976, THALES ; - [AGD_CPS] Card Personalization Specification requirement for SSCD security evaluation IAS Classic v5.0, version 1.1, 5 août 2020, référence IACv50_001_CPS_Req_For_CC_Evaluation, THALES. Guide d'utilisation du produit : [AGD_USE] : - IAS Classic Applet V5.0, Reference Manual, version C, 25 février 2020, référence D1496252C, THALES ; - BioPIN Manager V3.0 – Reference Manual, version B, 6 mars 2020, référence D1481720B, THALES.
[CER-IC]	Certification Report, for IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 and including optional software libraries and dedicated firmware from Infineon Technologies AG. Certifié le 26 septembre 2018 par le BSI, puis maintenu le 3 décembre 2018 sous la reference BSI-DSZ-CC-1079-2018-MA-01.
[CER-PTF]	Plateforme MultiApp V4.2 masquée sur le composant IFX_CCI_000010h. Certifié par l'ANSSI le 26 juin 2020 sous la référence ANSSI-CC-2020/65.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - GEMALTO Development Environment ALC Classe Evaluation Report (Generic Documentary activities), référence 17-0466_ALC-GEN_V1.0, version 1.0, 23 mars 2018, Serma Safety & Security ; - GEMALTO Development Environment ALC Class Evaluation Report (Generic Documentary activities), référence GTOGEN19_V1.0, version 1.0, 1 février 2019, Serma Safety & Security ;

	- [MDN] Site Technical Audit Report MDN, référence GTOGEN19_MDN_STAR_V1.1, version 1.1, 27 novembre 2019, Serma Safety & Security ; - [SGP] GEMALTO Development Environment Singapore Site Visit Lite Report, référence 17-0466-SGP_SVR-M_v1.0, version 1.0, 16 mai 2018, Serma Safety & Security ; - [GEM] GEMALTO Development Environment GEMENOS Site Visit Lite Report, référence 17-0466_GEM_SVR-M_v1.1, version 1.1, 6 novembre 2018, Serma Safety & Security ; - [GEM-VZN] Site Technical Audit Report – GEM-VZN Site Audit, référence GTOGEN19_GEM-VZN_STAR_v1.0, version 1.0, 9 juillet 2019, Serma Safety & Security ; - [MGY] Site Technical Audit Report MGY, référence GTOGEN19_MGY_STAR_V1.1, version 1.1, 19 décembre 2019, Serma Safety & Security ; - [PAU] Site Technical Audit Report Pont-Audemer, référence 17-0466_PAU_STAR_v1.0, version 1.0, 30 octobre 2018, Serma Safety & Security ; - [CBA] Site Technical Audit Report CBA, référence GTOGEN19_CBA_STAR_v1.0, version 1.0, 24 avril 2019, Serma Safety & Security ; - [CAL-VZN] Site Technical Audit Report – CAL-VZN, référence GTOGEN19_CAL-VZN_STAR_v1.0, version 1.0, 29 juillet 2019, Serma Safety & Security ; - [PUN2] Site Technical Audit Report ATOS Pune (PUN2), référence GTOGEN19a_et_b_PUN2_STAR_v1.2, version 1.2, 5 mars 2020, Serma Safety & Security ; - [VAN] Site Technical Audit Report VAN, référence GTOGEN19_VAN_STAR_v1.0, version 1.0, 14 mai 2019, Serma Safety & Security ; - [TCZ] Site Technical Audit Report GEMALTO TCZEW, référence 17-0466_TCZ_STAR_v1.0, version 1.0, décembre 2018, Serma Safety & Security ; - [PAR] Site Technical Audit Report ATOS_PAR, référence ATOS_PAR_STAR_v1.0, version 1.0, 7 août 2018, Serma Safety & Security ; - [MAR] Site Technical Audit Report MAR, référence GTOGEN19_MAR_STAR_v1.1, version 1.1, 5 décembre 2019, Serma Safety & Security.
[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 30 juin 2016 sous la référence BSI-CC-PP-0059-2009-MA-02.
[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. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0075-2012-MA-01.
[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. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0071-2012-MA-01.

[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. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0072-2012-MA-01.
[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. Maintenu par le BSI le 30 juin 2016 sous la référence BSI-CC-PP-0076-2013-MA-01.
[PP0084]	*Protection Profile, Security IC Platform Protection Profile with Augmentation Packages*, version 1.0, 13 janvier 2014. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-PP-0084-2014.

ANNEXE C. 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 and similar devices*, version 3.1, juin 2020.
[COMP] *	*Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version 1.5.1, mai 2018.
[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.
	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 www.ssi.gouv.fr.
	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.

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