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-2021/41

MultiApp V4.2 ID (version 4.2.1)

Paris, le 23 septembre 2021

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-2021/41

Nom du produit

MultiApp V4.2 ID

Référence/version du produit

version 4.2.1

Conformité à un profil de protection

Java Card System – Open Configuration Protection Profil, version 3.0.5

certifié BSI-CC-PP-0099-2017 le 21 décembre 2017

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

THALES DIS
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 DIS
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 « MultiApp V4.2 ID, version 4.2.1 » développé par THALES DIS et INFINEON TECHNOLOGIES AG.

Ce produit est destiné à héberger et exécuter une ou plusieurs applications, dites *applets* dans la terminologie Java Card. Ces applications peuvent revêtir un caractère sécuritaire différent (selon qu'elles soient « sensibles » ou « basiques ») et peuvent être chargées et instanciées avant ou après émission du produit. Les logiciels applicatifs ne sont pas inclus dans le périmètre de l'évaluation, mais ont été pris en compte au titre de [OPEN].

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 au profil de protection [PP-JCS].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- l'initialisation du *Card Manager* et la gestion du cycle de vie de la carte ;
- l'installation, le chargement et « l'extradition »[1] d'*applets* par le *Card Manager* ;
- la suppression d'applications sous le contrôle du *Card Manager* ;
- l'interface de programmation permettant d'opérer de manière sûre les applications ;
- la personnalisation de PACE ;
- la protection du chargement d'applications post-émission ;
- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications.

1.2.3 *Architecture*

Le périmètre d'évaluation (TOE[2]) est constitué :

- du microcontrôleur IFX_CCI_000010h, développé par INFINEON TECHNOLOGIES AG et certifié sous la référence [CER-IC] ;
- du logiciel embarqué, chargé en mémoire FLASH, développé par THALES DIS, comprenant :
  - un gestionnaire de mémoire *Memory Manager* ;
  - un gestionnaire de communication (I/O) ;
  - un gestionnaire de librairies cryptographiques *Crypto Libs ;*
  - un système Java Card.

Le système Java Card est composé des éléments suivants :

- un environnement *Runtime* (*Java Card 3.0.5 Runtime Environment*) ;
- une machine virtuelle Java Card (*Java Card 3.0.5 Virtual Machine*) ;

[1] L'extradition permet à plusieurs applications de partager un domaine de sécurité dédié.

[2] *Target Of Evaluation.*

- une interface de programmation (*Standard Java Card 3.0.5 API*[3]) et d'API propriétaires THALES DIS;
- un gestionnaire d'application (*Card Manager*) ;
- une couche *GlobalPlatform* conforme à GP 2.3 avec les amendements D & E ;
- les modules *PACE secure messaging* et *Fingerprint Biometry* ;
- l'application GDP permettant la personnalisation des applications.

Les applications déjà chargées dans le produit sont toutes identifiées dans la section suivante.

Bien que certaines applications ne soient pas incluses dans le périmètre de l'évaluation, elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [OPEN]. En effet, ces applications ont été vérifiées conformément aux contraintes de développements d'applications décrites dans le guide [Dev_Basic].

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].

Eléments de configuration		Origine
Nom de la TOE	MultiApp V4.2 ID	THALES DIS
Operating system identifier	0x1981 (*for OS developer*)	
Operating system release date	0x1018 (*for January 18, 2021*)	
Operating system release level	0x0402 (*for v4.2*)	
Gemalto Family Name	0xB0	
Gemalto OS Name	0x85	
Gemalto Mask Name	0x64	
Gemalto Product Name	0x65 (*for MultiappV4.2.1*)	
IC fabricator	4090 (*for chip manufacturer Infineon*)	INFINEON TECHNOLOGIES AG
IC Type	3401 (*for SLC52GDA804*)	

Ces éléments peuvent être vérifiés en utilisant la commande GET DATA sur le CPLC (voir [GUIDES]).

La principale différence entre le produit et la TOE (la plateforme) correspond aux applications chargées pré-émission sur ce produit. Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans le tableau ci-après, associées à leur nom et leur AID[4]. Le tableau ci-après liste également les *packages* inclus dans le produit.

AID (valeur en hexadécimal)	**Nom de l'application**
a0 00 00 01 51 00 00 00	ISD
a0 00 00 00 18 0c 00 00 01 63 42 00	Ias Classic v5.0
a0 00 00 02 47 20 01	LDSv2, travel records
a0 00 00 02 47 20 02	LDSv2, visa records
a0 00 00 02 47 10 01	eTravel
a0 00 00 00 18 10 02 03 03 00	GDP
a0 00 00 00 30 80 00 00 00 0a 9a 00 ff	Fido v1.2

[3] *Application Programming Interface.*

[4] *Application Identifier.*

a0 00 00 00 30 80 00 00 00 0a b1 01 ff a0 00 00 00 30 80 00 00 00 0a b1 00 ff a0 00 00 00 18 30 03 01 00 00 00 00 00 00 00 ff a0 00 00 00 30 80 00 00 00 06 df 00 ff a0 00 00 00 18 30 10 02 00 00 00 00 00 00 00 02 a0 00 00 00 18 32 0a 01 00 00 00 00 00 00 00 ff	MOC Client MOC Server MPCOS Microsoft Plug&Play OATH PURE DI
AID (valeur en hexadécimal)	**Nom du *package***
a0 00 00 00 62 00 01 a0 00 00 00 62 01 01 a0 00 00 00 62 01 02 a0 00 00 00 18 10 46 53 a0 00 00 00 62 02 09 a0 00 00 00 18 10 04 01 a0 00 00 01 51 00 a0 00 00 00 62 02 01 a0 00 00 00 18 10 02 01 a0 00 00 00 03 00 00 a0 00 00 01 51 53 50 a0 00 00 00 18 10 02 03 01 a0 00 00 00 18 10 02 03 02 a0 00 00 00 30 80 00 00 00 0a 48 00 a0 00 00 00 18 10 05 01 a0 00 00 00 18 10 01 23 a0 00 00 00 18 10 01 24 a0 00 00 00 18 10 01 25 a0 00 00 00 18 10 01 08 a0 00 00 00 18 10 01 20 a0 00 00 00 62 02 04 a0 00 00 00 62 02 02 a0 00 00 00 18 10 01 0b a0 00 00 00 18 10 01 09 a0 00 00 00 18 10 02 31 a0 00 00 00 18 10 02 30 a0 00 00 00 62 00 02 a0 00 00 00 62 02 09 01 a0 00 00 00 62 02 05 a0 00 00 00 18 80 00 00 00 06 62 40 ff 4d 4f 43 41 5f 53 65 72 76 65 71 a0 00 00 00 30 80 00 00 00 0a b1 00 ff a0 00 00 00 18 30 0b 02 01 00 00 00 00 00 00 fe a0 00 00 00 30 80 00 00 00 06 df 00 ff a0 00 00 00 18 10 01 07 a0 00 00 00 18 10 01 0a a0 00 00 00 18 10 02 03 03 a0 00 00 00 18 02 00 01 65 6d 76 61 70 69 00 fb a0 00 00 00 18 10 01 04 a0 00 00 00 18 30 0b 02 00 00 00 00 00 00 00 ff a0 00 00 00 18 10 02 04	java.lang javacard.framework javacard.security com.gemalto.javacard.filesystem javacardx.apdu com.gemalto.javacard.util org.globalplatform javacardx.crypto com.gemalto.javacardx.crypto visa.openplatform com.gemalto.javacard.open com.gemalto.javacardx.gap com.gemalto.javacardx.gapplet com.gemalto.javacard.internal com.gemalto.javacard.ism com.gemalto.javacard.securemessaging com.gemalto.javacard.securemessaging.builder com.gemalto.javacard.securemessaging.internal com.gemalto.javacard.security com.gemalto.javacard.tlv javacardx.biometry1toN javacardx.biometry com.gemalto.javacardx.biometryExt com.gemalto.javacardx.biometry com.gemalto.javacardx.crypto.asymmetric.ecc com.gemalto.javacardx.crypto.asymmetric.rsa java.io javacardx.apdu.util javacardx.security com.gemalto.javacard.iasclassic com.gemalto.moc.api com.gemalto.moc.server com.gemalto.javacard.icao.lds2 com.gemalto.javacard.mspnp com.gemalto.javacard.conformance com.gemalto.javacardx.biometry.biocfg com.gemalto.javacardx.gdp com.gemalto.emvapi com.gemalto.javacard.gpimage eTravel (Virtual Package) gApplet (Virtual Package)

Applications et packages déjà chargées dans le produit

1.2.5 *Cycle de vie*

Le cycle de vie est décrit au chapitre 2.5 de la cible de sécurité [ST]. Il est décomposé en quatre 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 du logiciel embarqué (hormis le *firmware* qui est déjà masqué en phase 3) dans le composant. Il est à noter que le point de livraison, ou d'émission de la carte, est en sortie de phase 5.

Les phases 1 à 5 correspondent donc à la construction de la TOE. Elles ont été prises en compte dans la présente évaluation, avec, pour les phases 2 et 3, une réutilisation des résultats de l'évaluation du composant. Le composant est développé et fabriqué par INIFNEON TECHNOLOGIES AG. Les sites de développement et de fabrication du microcontrôleur sont détaillés dans le rapport de certification [CER-IC].

La plateforme a quant à elle été développée sur les sites suivants (voir [SITES]) :

Meudon, voir [MDN]	Singapore, voir [SGP]
Gémenos, voir [GEM]	Calamba, voir [CAL]
ATOS Marcoussis, voir [MAR]	ATOS Les Clayes-sous-Bois, voir [LCY]
Pune, voir [PUN]	Vantaa, voir [VAN]
Tczew, voir [TCZ]	Curitiba, voir [CBA]
	Pont-Audemer, voir [PAU]

La phase 6 correspond à la personnalisation du produit. Cette phase est couverte par des recommandations sécuritaires (voir [GUIDE]). La phase 7 correspond à la phase opérationnelle du produit.

Le guide [AGD_OPE] identifie également des recommandations relatives à la livraison des futures applications à charger sur cette carte.

Par ailleurs, les guides [Dev_Basic] et [Dev_Sec] décrivent les règles de développement des applications destinées à être chargées sur cette carte ; le guide [AGD_OPE_VA] décrit les règles de vérification qui doivent être appliquées par l'autorité de vérification.

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit le pré-« personnalisateur », le « personnalisateur » et le gestionnaire de la carte chargés de l'administration de la carte, et comme utilisateurs du produit les développeurs des applications à charger sur la plateforme.

1.2.6 *Configuration évaluée*

Le certificat porte sur la plateforme Java Card « MultiApp V4.2 » en configuration ouverte, masquée sur le microcontrôleur IFX_CCI_000010h, telles que présentées au chapitre « 1.2.3 Architecture ».

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.

Toutes les applications identifiées dans la table « Applications et *packages* déjà chargées dans le produit » de la section 1.2.4 ont été vérifiées conformément aux contraintes décrites dans [AGD_OPE_VA].

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [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 du microcontrôleur «IFX_CCI_000010h », voir [CER_IC].

L'évaluation s'appuie sur des résultats d'évaluation su produit « Plateforme Java Card MultiApp V4.2 » certifié en juin 2020 sous la référence ANSSI-CC-2020/65, voir [CER_INI].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 30 juillet 2021, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises 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 potentiel d'attaque visé.

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

2.4 Analyse du générateur d'aléa

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 [ANSSI Crypto], la sortie du générateur physique d'aléa subit un retraitement de nature cryptographique.

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le potentiel d'attaque 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 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

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 :

- toutes les futures applications chargées sur ce produit (chargement post-émission) doivent respecter les contraintes de développement de la plateforme (guides [Dev_Basic] et [Dev_Sec]) selon la sensibilité de l'application considérées ;
- les autorités de vérification doivent appliquer le guide [AGD_OPE_VA] ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement post-émission) doit être activée conformément aux indications de [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[5], 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[6] , 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 :

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

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

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *MultiApp V4.2 ID : JCS Security Target*, référence D1539135, version 1.2, 11 mai 2021. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *MultiApp V4.2 ID Javacard Platform Security Target - public version*, référence D1539135, version 1.2p, 11 mai 2021.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report TARSO11 Project*, référence 20-0467_TARSO11_ETR_V1.1, version 1.1, 30 juillet 2021.
[CONF]	Liste de configuration du produit : - *Card Project Configuration Check For MultiApp v4.2.1, référence D1540052, version 1.0, 25 février 2021 ;* - *Configuration Management Plan For MultiApp v4.2.1, référence D1539856, version 1.0, 25 février 2021 ;* - *MultiApp V4.2 ID : ALC LIS document - Javacard Platform, référence D1539142, version 1.2, 21 juin 2021 ;* - *MultiApp V4.2 ID: ALC LCD document -Javacard Platform, référence D1550285, version 1.1, 28 mai 2021.*
[GUIDES]	Guide d'installation et d'administration du produit : - [AGD_OPE] *MultiApp V4.2 ID: AGD_OPE document - Javacard Platform*, référence D1541558, version 1.7, 11 mai 2021 ; - [AGD_PRE] *MultiApp V4.2 ID: AGD_PRE document - Javacard Platform*, référence D1539140, version 1.0, 10 mai 2021 ; Guide d'utilisation du produit : - *MultiApp ID 4.2 Premium Operating System – Reference Manual*, référence D1493575E, 3 mai 2021 ; - *Global Dispatcher Personalization Applet User Guide*, référence D1390286Q, 3 mai 2021 ; Guide de développement d'applications : - [Dev_Basic] *Rules for applications on Multiapp certified product*, référence D1495100, version 1.2, novembre 2019 ; - [Dev_Sec] *Guidance for secure application development on Multiapp platforms*, référence D1495101, version 1.2, décembre 2019. - Guides pour l'autorité de vérification [AGD_OPE_VA] : o *Verification process of Gemalto non sensitive applet*, référence D1495102, version 1.1, octobre 2019 ; o *Verification process of Third Party non sensitive applet*, référence D1495103, version 1.1, octobre 2019.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - DISGEN21_GEN_ v1.0 ; - [CBA] GTOGEN19_CBA_STAR_v1.0 ; - [MDN] GTOGEN19_MDN_STAR_V1.1; - [SGP] DISGEN20_SGP_STAR_v1.0 ; - [GEM] DISGEN20_GEM_STAR_v1.0 ;

	- [VAN] GTOGEN19_VAN_STAR_v1.0 ; - [CAL] GTOGEN19_CALVZN_STAR_v1.0 ; - [MAR] GTOGEN19_MAR_STAR_v1.1 ; - [LCY] DISGEN20_LCY_STAR_v1.0 ; - [PUN] GTOGEN19a_et_b_PUN2_STAR_v1.2 ; - [TCZ] DISGEN20_TCZ_STAR_v1.0 ; - [PAU] DISGEN20_PAU_STAR.
[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 16 juin 2020 par le BSI sous la référence BSI-DSZ-CC-1079-V2-2020.
[CER_INI]	*Plateforme Java Card MultiApp V4.2 en configuration ouverte sur le composant IFX_CCI_000010h.* Certifié par l'ANSSI le 26 juin 2020 sous la référence ANSSI-CC-2020/65.
[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.
[PP-JCS]	*Java Card System Protection Profile - Open Configuration*, version 3.0.5. Certifié par le BSI sous la référence BSI-PP-0099-2017.

ANNEXE B. 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.
[CRY-P-01]	Procédure ANSSI-CC-CRY-P01 Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, 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.
[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.
[CCRA]	*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.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.

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