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-2020/65v2

Annule et remplace le rapport de certification ANSSI-CC-2020/65 pour en réduire la portée

Plateforme Java Card MultiApp V4.2 en configuration ouverte sur le composant IFX_CCI_000010h (Version 4.2.0, Java Card version 3.0.5, GP version 2.3)

Paris, le 28 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-2020/65v2

Nom du produit

Plateforme Java Card MultiApp V4.2 en configuration ouverte sur le composant IFX_CCI_000010h

Référence/version du produit

Version 4.2.0, Java Card version 3.0.5, GP version 2.3

Conformité à un profil de protection

Java Card System Protection Profile Open Configuration, version 3.0.5
certifié BSI-CC-PP-0099-2017 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
6 rue de la Verrerie,
92190 Meudon, France

INFINEON TECHNOLOGIES AG
Am Campeon 1-12,
85579 Neubiberg, Allemagne

Commanditaire

THALES
6 rue de la Verrerie,
92190 Meudon, France

Centre d'évaluation

SERMA SAFETY & SECURITY
14 rue Galilée, CS 10071,
33608 Pessac Cedex, France
92197 Meudon 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 la « Plateforme Java Card MultiApp V4.2 en configuration ouverte sur le composant IFX_CCI_000010h, version 4.2.0 », développé par THALES 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.

Dans le cadre particulier de cette certification, qui correspond à une évaluation avec réduction de portée (voir [NOTE25]), la cible de sécurité [ST] identifie clairement les évolutions du périmètre d'évaluation par rapport à celui de la certification initiale (voir [CER]). Ici, la réduction de portée correspond au retrait de la fonctionnalité PACE-CAM du périmètre d'évaluation.

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, comprenant :
  - un gestionnaire de mémoire *Memory Manager* ;

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

[2] *Target Of Evaluation*.

- 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*) ;
- une interface de programmation (*Standard Java Card 3.0.5 API*[3] *)* et d'API propriétaires THALES ;
- 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 l'utilisation des commandes GET DATA, détaillés dans la cible de sécurité [ST] :

Eléments de configuration		Origine
Gemalto Family Name (Java Card)	B0	THALES
Gemalto OS NAME (MultiApp)	85	
Gemalto Mask Name (MultiAppV42)	60	
Gemalto Product Name	5F	
Flow id version	01	
Feature Flag – Crypto Config	297D	
Feature Flag – Feature Config	FF01	
Platform Certificates	40	
Application Certificates	C0 00	
IC Fabricator	4090	INFINEON TECHNOLOGIES AG
IC type (IFX_CCI_000010h)	3401	
OS Identifier	1981	
OS release date	9218	
OS release level (4.2)	0402	

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

[3] *Application Programming Interface*.

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
a0 00 00 00 30 80 00 00 00 0a b1 01 ff	MOC Client
a0 00 00 00 30 80 00 00 00 0a b1 00 ff	MOC Server
a0 00 00 00 18 30 03 01 00 00 00 00 00 00 00 ff	MPCOS
a0 00 00 00 30 80 00 00 00 06 df 00 ff	Microsoft Plug&Play
a0 00 00 00 18 30 10 02 00 00 00 00 00 00 00 02	OATH
a0 00 00 00 18 32 0a 01 00 00 00 00 00 00 00 ff	PURE DI
AID (valeur en hexadécimal)	**Nom du *package***
a0 00 00 00 62 00 01	java.lang
a0 00 00 00 62 01 01	javacard.framework
a0 00 00 00 62 01 02	javacard.security
a0 00 00 00 18 10 46 53	com.gemalto.javacard.filesystem
a0 00 00 00 62 02 09	javacardx.apdu
a0 00 00 00 18 10 04 01	com.gemalto.javacard.util
a0 00 00 01 51 00	org.globalplatform
a0 00 00 00 62 02 01	javacardx.crypto
a0 00 00 00 18 10 02 01	com.gemalto.javacardx.crypto
a0 00 00 00 03 00 00	visa.openplatform
a0 00 00 01 51 53 50	com.gemalto.javacard.open
a0 00 00 00 18 10 02 03 01	com.gemalto.javacardx.gap
a0 00 00 00 18 10 02 03 02	com.gemalto.javacardx.gapplet
a0 00 00 00 30 80 00 00 00 0a 48 00	com.gemalto.javacard.internal
a0 00 00 00 18 10 05 01	com.gemalto.javacard.ism
a0 00 00 00 18 10 01 23	com.gemalto.javacard.securemessaging
a0 00 00 00 18 10 01 24	com.gemalto.javacard.securemessaging.builder
a0 00 00 00 18 10 01 25	
a0 00 00 00 18 10 01 08	com.gemalto.javacard.securemessaging.internal
a0 00 00 00 18 10 01 20	
a0 00 00 00 62 02 04	com.gemalto.javacard.security
a0 00 00 00 62 02 02	com.gemalto.javacard.tlv
a0 00 00 00 18 10 01 0b	javacardx.biometry1toN
a0 00 00 00 18 10 01 09	javacardx.biometry
a0 00 00 00 18 10 02 31	com.gemalto.javacardx.biometryExt
a0 00 00 00 18 10 02 30	com.gemalto.javacardx.biometry
a0 00 00 00 62 00 02	com.gemalto.javacardx.crypto.asymmetric.ecc

[4] *Application Identifier.*

a0 00 00 00 62 02 09 01	com.gemalto.javacardx.crypto.asymmetric.rsa
a0 00 00 00 62 02 05	java.io
a0 00 00 00 18 80 00 00 00 06 62 40 ff	javacardx.apdu.util
4d 4f 43 41 5f 53 65 72 76 65 71	javacardx.security
a0 00 00 00 30 80 00 00 00 0a b1 00 ff	com.gemalto.javacard.iasclassic
a0 00 00 00 18 30 0b 02 01 00 00 00 00 00 00 fe	com.gemalto.moc.api
	com.gemalto.moc.server
a0 00 00 00 30 80 00 00 00 06 df 00 ff	com.gemalto.javacard.icao.lds2
a0 00 00 00 18 10 01 07	com.gemalto.javacard.mspnp
a0 00 00 00 18 10 01 0a	com.gemalto.javacard.conformance
a0 00 00 00 18 10 02 03 03	com.gemalto.javacardx.biometry.biocfg
a0 00 00 00 18 02 00 01 65 6d 76 61 70 69 00 fb	com.gemalto.javacardx.gdp
	com.gemalto.emvapi
a0 00 00 00 18 10 01 04	com.gemalto.javacard.gpimage
a0 00 00 00 18 30 0b 02 00 00 00 00 00 00 00 ff	eTravel (Virtual Package)
	gApplet (Virtual Package)
a0 00 00 00 18 10 02 04	

Applications et packages déjà chargées dans le produit

1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit par la figure ci-après, voir aussi [ST].

Phase	Description / comments		Who	Where
1	MAV4.2 platform development	Platform development & tests (1.a)	**Gemalto** GP R&D team SL Crypto team - secure environment -	**Singapore & Meudon Gemalto Development site**
	IAS+MOC applet development	- Applet Development (1.d) - Applet tests	**Gemalto** GP R&D team - secure environment -	**Singapore & Meudon Gemalto Development site**
	eTravel development	- Application Development (1.d) - Application tests	**Gemalto** GP R&D team - secure environment -	**Singapore Gemalto Development site**
	PSE team	- Platform configuration (1.c) - Script development	**Gemalto PSE team**	**Gemalto Development site**
2	IC development	IFX_CCI_000010h development	**Infineon** - Secure environment -	Infineon development site(s)
3	IC manufacturing	Manufacturing of virgin IFX_CCI_000010h integrated circuits embedding the Infineon flash loader, and protected by a dedicated transport key.	**Infineon** - Secure environment -	Infineon development site(s)
4	SC manufacturing: IC packaging & Embedding, also called "assembly"	- IC packaging & testing	**4.a) Infineon** - Secure environment – **OR** **4.b) Gemalto** Production teams - Secure environment -	**Gemalto manufacturing site**
5.a	Embedding (optional)	Put the module on a dedicated form factor (Card, inlay MFF2, other…)	**Gemalto** Production teams - Secure environment -	**Gemalto manufacturing site**
5.b	Initialization / Pre-personalization	Loading of the Gemalto software (platform and applets on top based on script generated)		
5c	Embedding (if not done during 5.a)	Put the module on a dedicated form factor (Card, inlay MFF2, other…)		
6	SC Personalization	Creation of files and loading of end-user data	**SC Personalizer** Gemalto or another accredited company - Secure environment -	SC Personalizer site
7	End-usage	End-usage for SC issuer	**SC Issuer**	Field
		Application Loading (7.a)	**SC Issuer**	Field
		End-usage for cardholder	**Cardholder**	Field

Cycle de vie du produit MultiApp V4.2

Les phases 1 et 2 correspondent au développement du produit, plus précisément :

- au développement du logiciel embarqué : le logiciel dédié au composant (*firmware*), le système d'exploitation, le système Java Card, la documentation, des applets et d'autres parties logicielles de la plateforme ;
- au développement du composant.

Les phases 3 et 4 correspondent à la fabrication et au conditionnement (*packaging*) du composant.

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 INFINEON 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 [STAR_MDN]	Singapore, voir [SVR_SGP]
Gémenos, voir [STAR_GEM-VZN] et [SVR_GEM]	Calamba, voir [STAR_CAL_VZN]
ATOS Marcoussis, voir [STAR_MAR]	ATOS Aubervilliers, voir [STAR_PAR]
Pune, voir [STAR_PUN]	Vantaa, voir [STAR_VAN]
Tczew, voir [STAR_TCZ]	Curitiba, voir [STAR_CBA]
Montgomeryville, voir [STAR_MGY]	Pont-Audemer, voir [STAR-PAU]

NB : Dans le cadre particulier de cette certification, qui correspond à une évaluation avec réduction de portée, la validité des audits n'a pas été vérifiée.

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*

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 version 3.1 révision 5** [CC] et à la méthodologie d'évaluation définie dans le manuel [CEM], et à la note [NOTE25].

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 s'appuie sur les résultats d'évaluation de ce même produit certifié le 26 juin 2020 sous la référence ANSSI-CC-2020/65, voir [CER]. Elle correspond à une évaluation avec réduction de portée suite à l'identification de vulnérabilité.

L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat [CER] n'a pas été conduite dans le cadre de cette réévaluation partielle. Le niveau de résistance d'un produit certifié se dégrade au cours du temps. Seule une réévaluation ou une surveillance de cette version du produit permettrait de maintenir le niveau de confiance dans le temps.

Le CESTI en charge de l'évaluation initiale a émis un rapport d'analyse de réduction de portée (référence [RTE_part]) pour réévaluer les composants d'assurance impactés par l'évolution de la cible de sécurité du produit.

Le rapport technique d'analyse de réduction de portée [RTE_part], remis à l'ANSSI le 10 juin 2021, pour réévaluer les composants d'assurance ASE, ADV, ALC (hors audits), et ATE impactés par l'évolution de la cible de sécurité [ST] détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

Le rapport technique [RTE_init], remis à l'ANSSI le 10 avril 2020, détaille les travaux initialement réalisés par le centre d'évaluation et atteste que la résistance du produit atteignait VAN.5 lors de son édition.

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

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilité de conception et de construction pour le niveau AVA_VAN.5 visé à la date de certification initiale (voir [CER]).

2.4 Analyse du générateur d'aléas

Le produit comporte un générateur de pseudo-aléa qui a fait l'objet d'une évaluation selon la méthodologie [AIS31], il répond aux exigences des classes DRG.4, comme revendiqué dans la cible de sécurité [ST].

Comme énoncé dans le document [REF], les aléas générés subissent effectivement un retraitement algorithmique 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 à la date de certification initiale (voir [CER]).

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 « Plateforme Java Card MultiApp V4.2 en configuration ouverte sur le composant IFX_CCI_000010h, version 4.2.0 », ici soumis à l'évaluation de la réduction de portée (voir [NOTE25]), répondait aux caractéristiques de sécurité spécifiées dans la nouvelle cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5 à la date de certification initiale (voir [CER]).

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 selon la sensibilité de l'application considérée (voir guides [Dev_Basic] et [Dev_Sec]) ;
- 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 :

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

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 :

[6] 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 produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *MultiApp V4.2 : JCS Security Target*, référence D1487827, version 1.18, 4 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 Javacard Platform Security Target Public Version*, référence D1487827, version 1.18p, 4 mai 2021.
[RTE]	Rapport technique d'évaluation : - [RTE_init] *Evaluation Technical Report*, référence TARSO_1_ETR_v1.1, version 1.1, 10 avril 2020 ; - [RTE_part] *Evaluation Technical Report for Partial Re-Evaluation*, version 1.1, 10 juin 2021. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - *Evaluation Technical Report Lite*, référence TARSO_1_ETR_Lite_v1.1, version 1.1, 10 avril 2020 ; - *Evaluation Technical Report Lite*, référence TARSO_1_ETR_Lite_v1.2, version 1.1, 10 juin 2021.
[CONF]	Liste de configuration du produit : - *Card Project Configuration Check For MultiApp v4.2*, référence D1470352, version 2.8, 2 avril 2020 ; - *Configuration Management Plan For MultiApp v4.2*, référence D1470351, version 1.3, 2 avril 2020 ; - *MultiApp V4.2 : ALC LIS document - Javacard Platform*, référence D1507344, version 1.13, 5 mai 2021 ; - *MultiApp V4.2 : ALC - CMC - CMS - TAT document - Javacard Platform*, référence D1507124, version 1.4, 9 février 2020.
[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 référence BSI-DSZ-CC-1079-2018-MA-01.
[GUIDES]	Guide d'installation du produit : - *MultiApp V4.2 : AGD_PRE document - Javacard Platform*, référence D1488512, version 1.7, 3 mai 2021. Guide d'administration du produit : - *MultiApp V4.2 : AGD_OPE document - Javacard Platform*, référence D1488511, version 1.11, 3 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 de novembre 2019 ; - [Dev_Sec] *Guidance for secure application development on Multiapp platforms*, référence D1495101, version 1.2, décembre 2019 ; - *BioPIN Manager V3.0 Reference Manual*, référence D1481720A, 14 juin 2019. Guides pour l'autorité de vérification [AGD-OPE_VA] : - *Verification process of Gemalto non sensitive applet*, référence D1495102, version 1.1, octobre 2019 ; - *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 : - [STAR_CAL_VZN] *Site Technical Audit Report - CAL-VZN Site Audit*, référence GTOGEN19_CAL-VZN_STAR_v1.0 ; - [STAR_CBA] *Site Technical Audit Report CBA*, référence GTOGEN19_CBA_STAR_v1.0 ; - [SVR_GEM-VZN] *Site Technical Audit Report - GEM-VZN Site Audit*, référence GTOGEN19_GEM-VZN_STAR_v1.0 ; - [STAR_MAR] *Site Technical Audit Report MAR*, référence GTOGEN19_MAR_STAR_v1.1 ; - [STAR_MDN] *Site Technical Audit Report MDN*, référence GTOGEN19_MDN _STAR_v1.1 ; - [STAR_MGY] *Site Technical Audit Report – MGY*, référence GTOGEN19_MGY_STAR_v1.1 ; - [STAR_PAR] *Site Technical Audit Report ATOS_PAR*, référence ATOS_PAR_STAR_v1.0 ; - [STAR-PAU] *Site Technical Audit Report GEMALTO Pont-Audemer,* référence 17-0466_PAU_STAR_v1.0 ; - [STAR_PUN] *Site Technical Audit Report PUN2*, référence GTOGEN19a_et_b_PUN2_STAR_v1.2 ; - [STAR_TCZ] *Site Technical Audit Report - TCZEW site audit*, référence 17-0466_TCZ-STAR_v1.0 ; - [STAR_VAN] *Site Technical Audit Report VAN,* référence GTOGEN19_VAN_STAR_v1.0 ; - [SVR_SGP] *Development Environment Singapore Site Visit Lite Report*, référence 17-0466-SGP_SVR-M_v1.0 ; - [SVR_GEM] *Development Environment GEMENOS Site Visit Lite Report*, référence 17-0466_GEM_SVRM_v1.1.
[PP-JCS]	*Java Card System Protection Profile - Open Configuration*, version 3.0.5. Certifié par le BSI sous la référence BSI-PP-0099-2017.

[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.
[CER]	Rapport de certification ANSSI-CC-2020/65 pour la « Plateforme Java Card MultiApp V4.2 en configuration ouverte sur le composant IFX_CCI_000010h, 26 juin 2020.
[IAR]	*IMPACT ANALYSIS Report – MultiApp v4.2 PLTF Revaluation*, référence D1545427, version 1.4, 4 mai 2021.

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.
[NOTE25]	Note d'application: Réduction de portée d'un certificat CC, référence ANSSI-CC-NOTE-25, version 1.0, 23 septembre 2021.
[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 3.0, avril 2019.
[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.
[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.
[AIS 31]	*A proposal for: Functionality classes for random number generators, AIS20/AIS31*, version 2.0, 18 Septembre 2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).

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