



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-2020/65

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

Paris, le 26 juin 2020

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

Guillaume POUPARD
[ORIGINAL SIGNE]



Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présumées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

ANSSI-CC-2020/65

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**

Critères 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

Accords de reconnaissance applicables



SOG-IS



Ce certificat est reconnu au niveau EAL2.

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le 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 matières

1. LE PRODUIT	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Introduction</i>	6
1.2.2. <i>Services de sécurité</i>	6
1.2.3. <i>Architecture</i>	6
1.2.4. <i>Identification du produit</i>	7
1.2.5. <i>Cycle de vie</i>	9
1.2.6. <i>Configuration évaluée</i>	10
2. L’EVALUATION	11
2.1. REFERENTIELS D’EVALUATION	11
2.2. TRAVAUX D’EVALUATION	11
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	11
2.4. ANALYSE DU GENERATEUR D’ALEAS.....	11
3. LA CERTIFICATION	12
3.1. CONCLUSION	12
3.2. RESTRICTIONS D’USAGE.....	12
3.3. RECONNAISSANCE DU CERTIFICAT	13
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	13
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	13
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....	14
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	15
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	17

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.

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 la plateforme ouverte Java Card 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 (TOE²) 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 :
 - o un gestionnaire de mémoire *Memory Manager* ;
 - o un gestionnaire de communication (I/O) ;
 - o un gestionnaire de bibliothèques cryptographiques *Crypto Libs* ;
 - o un système JAVA Card.

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

² Target Of Evaluation.

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 API¹*) 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
<i>Gemalto Family Name (Java Card)</i>	B0	<i>THALES</i>
<i>Gemalto OS NAME (MultiApp)</i>	85	
<i>Gemalto Mask Name (MultiAppV42)</i>	60	
<i>Gemalto Product Name</i>	5F	
<i>Flow id version</i>	01	
<i>Feature Flag – Crypto Config</i>	297D	
<i>Feature Flag – Feature Config</i>	FF01	
<i>Platform Certificates</i>	40	
<i>Application Certificates</i>	C0 00	
<i>IC Fabricator</i>	4090	
<i>IC type (IFX_CCI_000010h)</i>	3401	
<i>OS Identifier</i>	1981	
<i>OS release date</i>	9218	
<i>OS release level (4.2)</i>	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 configuration du produit à la disposition de l'évaluateur sont identifiées dans le tableau ci-après, associées à leur nom et leur AID². Le tableau ci-après liste également les *packages* inclus dans le produit.

¹ Application Programming Interface.

² Application Identifier.

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.gaplet
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	com.gemalto.javacard.securemessaging.internal
a0 00 00 00 18 10 01 08	com.gemalto.javacard.security
a0 00 00 00 18 10 01 20	com.gemalto.javacard.tlv
a0 00 00 00 62 02 04	javacardx.biometry1toN
a0 00 00 00 62 02 02	javacardx.biometry
a0 00 00 00 18 10 01 0b	com.gemalto.javacardx.biometryExt
a0 00 00 00 18 10 01 09	com.gemalto.javacardx.biometry
a0 00 00 00 18 10 02 31	com.gemalto.javacardx.crypto.asymmetric.ecc
a0 00 00 00 18 10 02 30	com.gemalto.javacardx.crypto.asymmetric.rsa
a0 00 00 00 62 00 02	java.io
a0 00 00 00 62 02 09 01	javacardx.apdu.util
a0 00 00 00 62 02 05	javacardx.security
a0 00 00 00 18 80 00 00 00 06 62 40 ff	com.gemalto.javacard.iasclassic
4d 4f 43 41 5f 53 65 72 76 65 71	com.gemalto.moc.api
a0 00 00 00 30 80 00 00 00 0a b1 00 ff	com.gemalto.moc.server
a0 00 00 00 18 30 0b 02 01 00 00 00 00 00 00 fe	com.gemalto.javacard.icao.lds2
a0 00 00 00 30 80 00 00 00 06 df 00 ff	com.gemalto.javacard.mspnp
a0 00 00 00 18 10 01 07	com.gemalto.javacard.conformance
a0 00 00 00 18 10 01 0a	com.gemalto.javacardx.biometry.biocfg
a0 00 00 00 18 10 02 03 03	com.gemalto.javacardx.gdp
a0 00 00 00 18 02 00 01 65 6d 76 61 70 69 00 fb	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)
a0 00 00 00 18 10 02 04	gApplet (Virtual Package)

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 *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 :

Meudon, voir [STAR_MDN]	Singapore, voir [SVR_SGP]
Gémenos, voir [STAR_GEM-VZN] et [STAR_GEM]	Calamba, voir [STAR_CAL_VZN]
ATOS Marcoussis, voir [STAR_MAR]	dATOS Aubervillier, 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]

Le tableau ci-dessous référence les rapports d'audit de site pour leur réutilisation.

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].

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 » au niveau EAL 6 augmenté du composant ALC_FLR.1, conforme au profil de protection [PP0084]. Ce microcontrôleur a été certifié le 26 septembre 2018 et maintenu le 3 décembre, voir [CER-IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 10 avril 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 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.

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.

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 » 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 [GUIDE], notamment :

- toutes les futures applications chargées sur ce produit (chargement *post-issuance*) doivent respecter les contraintes de développement de la plateforme selon la sensibilité de l'application considérées (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-issuance*) doit être activée conformément aux indications de [GUIDE].

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'accord¹, 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 [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires², 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 :



¹ La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

² La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit		
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Intitulé du composant	
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	2	Well-structured internals
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	4	4	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	4	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	2	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	3	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - MultiApp V4.2 : JCS Security Target, référence D1487827, version 1.11, 19 février 2020. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - MultiApp V4.2 : JCS Security Target Lite, référence D1487827p, version 1.11p, 19 février 2020.
[RTE]	<ul style="list-style-type: none"> - Evaluation Technical Report, référence TARSO_1_ETR_v1.1, version 1.1, 10 avril 2020 ; - Evaluation Technical Report Lite, référence TARSO_1_ETR_Lite_v1.1, version 1.1, 10 avril 2020.
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - 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 1.11, 2 avril 2020 ; - MultiApp V4.2 : ALC - CMC - CMS - TAT document - Javacard Platform, référence D1507124, version 1.4, 9 février 2020.
[CER-IC]	<p>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. <i>Certifié le 26 septembre 2018 par le BSI, puis maintenu le 3 décembre 2018 sous la référence BSI-DSZ-CC-1079-2018-MA-01.</i></p>
[PP-JCS]	<p>Java Card System Protection Profile - Open Configuration, version 3.0.5. <i>Certifié par le BSI sous la référence BSI-PP-0099-2017.</i></p>
[PP0084]	<p>Security IC Platform Protection Profile with Augmentation Packages, version 1.0. <i>Certifié par le BSI sous la référence BSI-PP-0084-2014.</i></p>
[STAR_CAL-VZN]	<p>Site Technical Audit Report - CAL-VZNSite Audit, référence GTOGEN19_CAL-VZN_STAR_v1.0.</p>
[STAR_CBA]	<p>Site Technical Audit Report CBA, référence GTOGEN19_CBA_STAR_v1.0.</p>
[STAR_GEM-VZN]	<p>Site Technical Audit Report - GEM-VZNSite Audit, référence GTOGEN19_GEM-VZN_STAR_v1.0.</p>

[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.
[GUIDE]	<p>Guide d'installation du produit [AGD_PRE] :</p> <ul style="list-style-type: none"> - MultiApp V4.2 : AGD_PRE document - Javacard Platform, référence D1488512, version 1.3 19 février 2020. <p>Guide d'administration du produit [AGD_OPE] :</p> <ul style="list-style-type: none"> - MultiApp V4.2 : AGD_OPE document - Javacard Platform, référence D1488511, version 1.7, 19 février 2020. <p>Guide d'utilisation du produit :</p> <ul style="list-style-type: none"> - MultiApp ID 4.2 Premium Operating System – Reference Manual, référence D1493575B, 12 février 2020 ; - Global Dispatcher Personalization Applet User Guide, référence D1390286I, 18 avril 2019 ; <p>Guide de développement d'applications :</p> <ul style="list-style-type: none"> - [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. <p>Guides pour l'autorité de vérification [AGD-OPE_VA] :</p> <ul style="list-style-type: none"> - 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.

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 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 : <ul style="list-style-type: none"> - 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, 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.
[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 .
[AIS 31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 Septembre 2011, BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>).

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