PREMIÈRE 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-2022/37

MultiApp V5.0 Java Card Virtual Machine (version 5.0)

Paris, le 17 octobre 2022

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 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-2022/37

Nom du produit

MultiApp V5.0 Java Card Virtual Machine

Référence/version du produit

version 5.0

Conformité à un profil de protection

Néant

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 7

Développeurs

THALES DIS FRANCE SAS
6 rue de la Verrerie
92190 Meudon, France

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

Commanditaire

THALES DIS FRANCE SAS
6 rue de la Verrerie
92190 Meudon, France

Centre d'évaluation

CEA - LETI
17 avenue des martyrs,
38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables

CCRA

Ce certificat est reconnu au niveau.

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 carte « MultiApp V5.0 Java Card Virtual Machine, version 5.0 » développée par THALES DIS FRANCE SAS et INFINEON TECHNOLOGIES AG

Le 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.

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.

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par la plateforme ouverte *Java Card* sont détaillés dans la cible de sécurité [ST] au chapitres 2.4.1 « *Architecture* ». Ils sont résumés ci-après :

- 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 protection du chargement d'applications post-émission ;
- la fonctionnalité « *OS Agility* » permettant de mettre à jour le produit en chargeant un *patch* en phase utilisateur ;
- 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*

La carte « Multi App V5.0 » est constituée des éléments suivants :

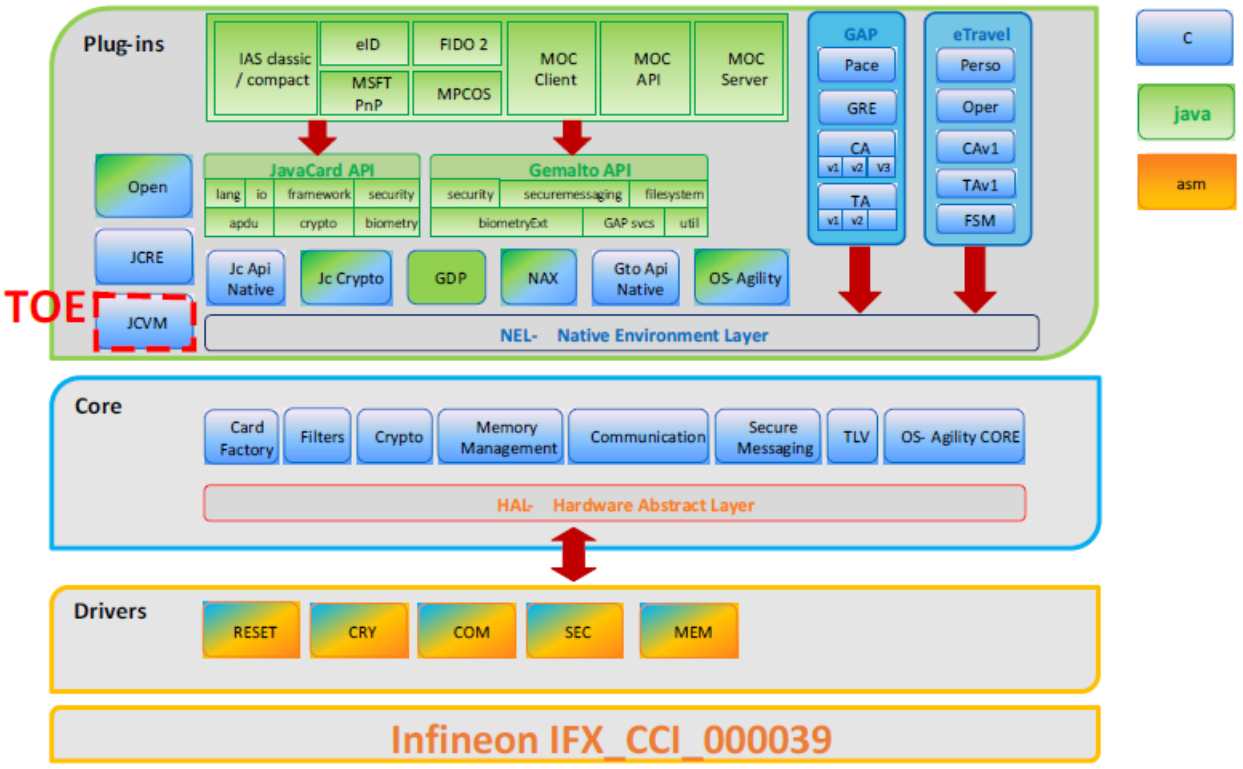
- du microcontrôleur IFX_CCI_000039h (SLC37), précédemment certifié (voir [CER-IC]) ;
- de la « plateforme JavaCard MultiApp V5.0 » certifiée au niveau EAL 6 augmenté du composant ALC_FLR (voir [CER]) ;
- des applications : IAS Classic V5.2, eTravel 2.5, Pure 3.5.0, BioPin Management v3.1, MPCOS v4.1, e-ID v1.0, MSFT PnP v1.0, Fido Authentificator v2 (ces *applets* peuvent être supprimées en fonction des besoins de l'utilisateur) ;
- des applets pouvant être chargées avant ou après le point de livraison de la plateforme.

La TOE[2] soumise à l'évaluation au niveau EAL 7 est restreinte à l'*interpreter*, pour l'exécution des *bytecodes*.

L'architecture du produit est illustrée par la figure ci-après, où il est précisé en pointillé rouge la présente TOE (évaluée au niveau EAL7).

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

[2] *Target of evaluation* - périmètre d'évaluation.



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 du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre 1.3 « *TOE identification* ».

Eléments de configuration		Origine
Gemalto Family Name (Java Card)	0xB0	THALES DIS FRANCE SAS
Gemalto OS NAME (MultiApp)	0x85	
Gemalto Mask Name (MultiApp V5.0)	0x5F	
Gemalto Product Name	0x5E	
Flow id version	0x01	
Platform Certificates (CC configuration)	0x40	
IC Fabricator (INFINEON)	0x4090	INFINEON TECHNOLOGIES AG
IC type (IFX_CCI_000039h)	0x0039	
OS Identifier	0x1981	
OS release date	0x1055	
OS release level (5.0)	0x0500	

Ces éléments peuvent être vérifiés par l'utilisation de la commande « GET DATA ». La procédure d'identification est décrite dans le guide [AGD_OPE] (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. Ce tableau liste les applications et les *packages* inclus dans le produit, associés à leur nom et leur AID[3] .

Nom, version de l'application	AID (en hexadécimal)	Nom du *package*
eTravel v2.5	-	NA, not an applet (resident application)
IAS Classic V5.2	A0 00 00 00 18 80 00 00 00 06 62 40 FF	com/gemalto/iasclassic
BioPIN Management v3.1	4D 4F 43 41 5F 43 6C 69 65 6E 74 4D 4F 43 41 5F 53 65 72 76 65 72	com/gemalto/moc/client com/gemalto/moc/server
MPCOS v4.1	A0 00 00 00 18 30 03 01 00 00 00 00 00 00 00 FF	com/gemalto/mpcos
PURE 3.5.0	A0 00 00 00 18 32 0A 01 00 00 00 00 00 00 00 FF	com/gemalto/puredi
eID v1.0	A0 00 00 00 30 80 00 00 00 08 DB 00 FF	com/gemalto/edi
MSFT PnP v1.0	A0 00 00 00 30 80 00 00 00 06 DF 00 FF	com/gemalto/javacard/mspnp
Fido Authentificator v2	A0 00 00 00 30 80 00 00 00 0A 9A 00 FF	com/gemalto/javacard/fido/ctap

La commande « GET STATUS » permet à l'utilisateur du produit de vérifier quelles applications et quels *packages* sont installés dans le produit à sa disposition.

[3] *Application Identifier.*

1.2.5 *Cycle de vie*

Le cycle de vie est décrit par la figure ci-après, voir chapitre 2.5 « *Life-cycle* » de la cible de sécurité [ST] :

Phase	Description / comments		Who	Where
1	MAV5.0 platform development	Platform development & tests (1.a)	**Thales** GP R&D team SL Crypto team - secure environment -	**Thales Development site** (see §2.5.4)
	Thales applets (IAS, eTravel...) development	- Applet Development (1.d) - Applet tests	**Thales** GP R&D team - secure environment -	**Thales Development site** (see §2.5.4)
	Patch development	- Patch Development (1.e) - Patch tests	**Thales** GP R&D team - secure environment -	**Thales Development site** (see §2.5.4)
	PSE team	- Platform configuration (1.c) - Script development	**Thales PSE team**	**Thales manufacturing site** (see §2.5.4)
2	IC development	IFX_CCI_000039 development	**Infineon** - Secure environment -	Infineon development site(s)
3a	IC manufacturing	Manufacturing of virgin IFX_CCI_000039 integrated circuits embedding the Infineon flash loader, and protected by a dedicated transport key.	**Infineon** - Secure environment -	Infineon development site(s)
3b (optional)	Initialization / Pre-personalization	Loading of the Thales software (platform and applets on top based on script generated) – For WAFER init process only		
4	SC manufacturing: IC packaging & Embedding, also called "assembly"	- IC packaging & testing	**4.a) Infineon** - Secure environment – **OR** **4.b) Thales** Production teams - Secure environment -	**Thales manufacturing site** (see §2.5.4)
5.a	Embedding	Put the module on a dedicated form factor (Card, inlay MFF2, other...)	**Thales** Production teams - Secure environment -	**Thales manufacturing site** (see §2.5.4)
5.b	Initialization / Pre-personalization (Not Applicable for wafer-init process)	Loading of the Thales software (platform and applets on top based on script generated)		
6	SC Personalization	Creation of files and loading of end-user data	**SC Personalizer** Thales 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
		Patch update (7.b)	**Thales**	Field

Le périmètre de l'évaluation se limite aux deux premières étapes, correspondant aux phases 1 à 5 décrites dans le profil de protection [PP0084] :

- les phases 1 et 2 correspondent :
  - au développement du logiciel embarqué, à savoir le logiciel dédié au microcontrôleur (*firmware*), le système d'exploitation, le système *Java Card*, la documentation, certaines *applets* et d'autres parties logicielles de la plateforme ;
  - au développement du microcontrôleur sécurisé ;
- la phase 3 correspond :

  - à la fabrication du microcontrôleur sécurisé développé par INFINEON TECHNOLOGIES AG;
  - à la protection du *flash loader* à l'aide d'une clé de transport dédiée ;
  - à la pré-personnalisation (*wafer* seulement) par le chargement du logiciel THALES DIS à partir d'un script ;
- la phase 4 correspond à la mise en module du microcontrôleur, cette étape peut être réalisée par THALES DIS ou par INFINEON ;
- la phase 5 correspond à :
  - la mise en forme du module (*inlay*, *card*, autres) qui est effectuée par THALES DIS ou par d'autres sociétés ;
  - la pré-personnalisation (excepté *wafer* déjà réalisée à la phase 3) réalisée par THALES DIS en effectuant le chargement du logiciel THALES DIS à partir d'un script ;
  - la mise en forme du module (*inlay*, *card*, autres) réalisée par THALES DIS ou autres si elle n'a pas été réalisée au préalable.

La fin de cette phase correspond au point de livraison. Jusqu'à cette phase, le produit est considéré comme étant en construction. Aussi, les phases 1, 4 et 5 sont réalisées sur les sites suivants (voir [SITES]) :

Meudon [MDN]	La Ciotat [VIG]
Vantaa [VAN]	Singapore [SGP]
Tczew [TCZ]	Curitiba [CBA]
Gémenos [GEM]	

Les sites de développement et de fabrication du microcontrôleur sont couverts par le certificat [CER-IC].

Le produit permet le chargement d'applications en phase 3 (avant le point de livraison), en phase 5 (pré-émission) ou en phase 6 et 7 (post-émission) :

- le développement des applications masquées en phase 3 et identifiées dans la cible de sécurité [ST] a été réalisé sur les sites de Meudon, La Ciotat et Vantaa. Leur livraison et leur vérification ont été analysées pendant cette évaluation conformément à [OPEN] au titre des tâches ALC ;
- les chargements en phase 5 (pré-émission), 6 et 7 (post-émission) doivent être protégés conformément à [AGD_ALP].

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

Par ailleurs, les guides [AGD-Dev_Basic] et [AGD-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 administrateur du produit le « prépersonnalisateur », le « personnalisateur » et le gestionnaire de la carte chargé de l'administration de la carte, et comme utilisateur du produit les développeurs des applications à charger sur la plateforme.

1.2.6 *Configuration évaluée*

Le certificat porte uniquement sur les fonctionnalités offertes par la machine virtuelle de la « plateforme JavaCard MultiApp V5.0 » décrite dans la section 1.2.3 et identifiée au paragraphe 1.2.4.

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 s'appuie sur les résultats d'évaluation du produit « Plateforme Java Card MultiApp V5.0, version 5.0 » certifié en octobre 2021 sous la référence ANSSI-CC-2021/42, voir [CER].

Cette évaluation a consisté à évaluer la machine virtuelle « MultiApp V5.0 JavaCard Virtual Machine, version 5.0 » de la plateforme, selon les plus hautes exigences des Critères communs : les composants du niveau EAL 7, qui nécessitent la mise en œuvre de méthodes formelles.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI (voir date en bibliographie), 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 [ANA-CRY].

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 [AGD-Dev_Basic] et [AGD-Dev_Sec]) selon la sensibilité de l'application considérée ;
- 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] ;
- le chargement des applications pré- émission doit être protégé conformément au guide [ORG_LOAD].

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[4], 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 :

Le présent certificat est reconnu par le SOG-IS au niveau EAL3 augmenté de ALC_FLR.3.

[4] 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[5] , 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 :

Le présent certificat est reconnu par le CCRA au niveau EAL2 augmenté de ALC_FLR.3.

[5] 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 V5: Security Target Java Card Virtual Machine*, référence D1545477, version 1.4, 02/03/2022. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *MultiApp V5 : Security Target Java Card Virtual Machine*, référence D1545477_LITE, version 1.1, 02/03/2022.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report – ARGAN-D*, référence LETI.CESTI.ARD.FULL.001, version 1.3, 20/09/2022.
[ANA_CRY]	Cotation des mécanismes cryptographiques ARGAN A, référence LETI.CESTI.ARA.RT.008, version 1.1, 03/09/2021.
[CONF]	Liste de configuration du produit : - *MultiApp V5.0 – Virtual Machine: ALC LIS CC document*, référence D1563076, version 1.6, 02/03/2022 ; - *MultiApp V5: ALC LIS Common Criteria*, référence D1544613, version 1.1, 10/12/2021.
[GUIDES]	Guide d'installation du produit [AGD_PRE] : - *MultiApp V5.0 AGD_PRE document – Javacard Platform*, référence D1536519, version 1.21, 05/03/2021. Guide d'administration du produit [AGD_OPE] : - *MultiApp V5.0 AGD_OPE document – Javacard Platform*, référence D1536518, version 1.6, 02/09/2021. Guide d'utilisation du produit : - *MultiApp ID V5 Operating System Reference Manual*, référence D152385, version B, 09/12/2020. Guides de développement d'applications : - [AGD-Dev_Basic] *Rules for applications on Multiapp certified product*, référence D1484823, version 1.21, février 2021 ; - [AGD-Dev_Sec] *Guidance for secure application development on Multiapp platforms*, référence D1495101, version 1.3a, mars 2021. Guides pour l'autorité de vérification [AGD-OPE_VA] : - *Verification process of Gemalto non sensitive applet*, référence D1484874, version 1.2, février 2021 ; - [ORG_*LOAD*] *Verification process of Third Party non sensitive applet*, référence D1484875, version 1.21, février 2021.
[SITES]	Rapports d'analyse documentaire et d'audits de sites pour la réutilisation : - DISGEN20_ALC_GEN_v1.1 ; - [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 ; - [VIG] DISGEN20_VIG_STAR_v1.1 ; - [TCZ] DISGEN20_TCZ_STAR_v1.0.
[CER-IC]	Rapport de certification *BSI-DSZ-CC-1107-V2-2021 IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh design step T11 with firmware 80.306.16.0 & 80.306.16.1, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.15.000 and v2.11.003, optional ACL v3.33.003 and v3.02.000, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance from Infineon Technologies AG.* Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 7 juillet 2021.
[CER]	Rapport de certification Plateforme Java Card MultiApp V5.0 (version 5.0). Certifié par l'ANSSI le 14 octobre 2021 sous la référence ANSSI-CC-2021/42.
[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 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]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 4.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[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.
[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.