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-2020/42

MultiApp v4.0.1 with Filter Set 1.0 Java Card Open Platform on M7892 G12 chip

Paris, le 17 novembre 2020

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

Guillaume POUPARD

[ORIGINAL SIGNE]

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

AVERTISSEMENT

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

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

Toute correspondance relative à ce rapport doit être adressée au :

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

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2020/42

Nom du produit

MultiApp v4.0.1 with Filter Set 1.0 Java Card Open Platform on M7892 G12 chip

Référence/version du produit

MultiApp v4.0.1 with Filter Set 1.0

Conformité à un profil de protection

Java Card Platform Protection Profile – Open configuration, version 3.0

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,
92190 Meudon, France

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

Commanditaire

THALES DIS
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

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 v4.0.1 with Filter Set 1.0 Java Card Open Platform on M7892 G12 chip » développé par les sociétés THALES DIS et INFINEON TECHNOLOGIES AG.

Le produit est délivré en deux configurations issues du composant SLE78xx (microcontrôleur M7892 G12 FLASH) :

- avec une capacité RF de 56 pF (SLE78CLFX4007PHM, IC type 7879) ;
- avec une capacité RF de 27 pF (SLE78CLFX400VPHM, IC type 7897).

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.

Cette cible de sécurité est strictement conforme au profil de protection [PP JCS-O].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- la protection des applications et leurs données associées ;
- la protection des codes et des données du *Java Card system* ;
- le contrôle, par le *Card Manager*, de la gestion des *applets* (installation, mise à jour, suppression) ;
- le retour dans un état cohérent et stable en cas d'installation d'un package ou d'une application erroné ;
- la mise à disposition de moyens de cryptographie pour les applications ;
- le contrôle d'intégrité des données sensibles de la plateforme (applications, clés internes, etc.) ;
- la gestion des réactions aux tentatives de pénétration ;
- la protection du chargement d'applications *post-issuance* ;
- 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 produit est constitué des éléments illustrés par la figure ci-dessous :

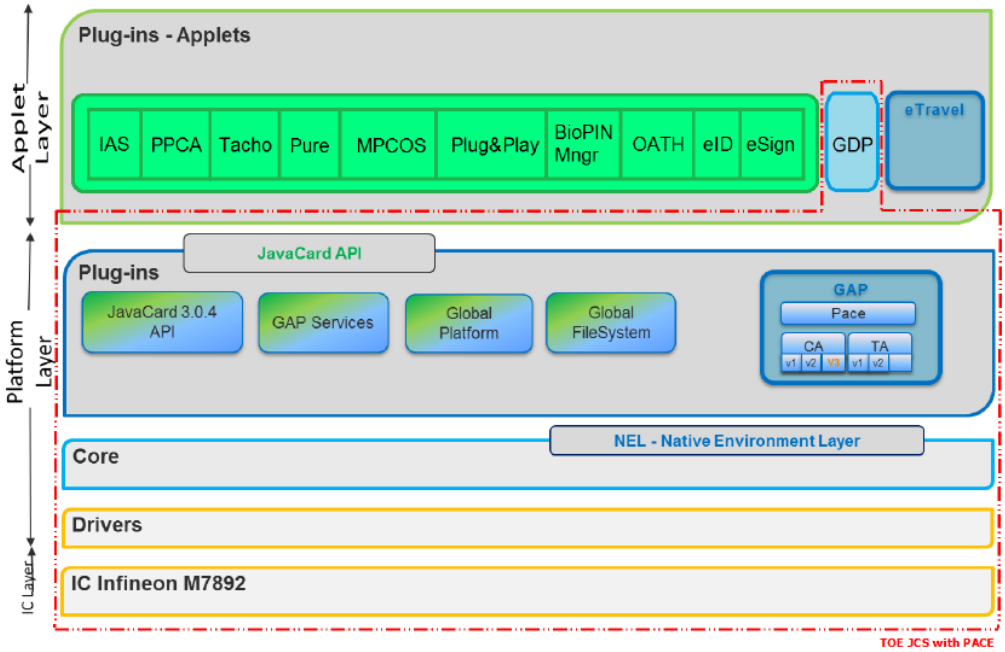

Figure 1 : Architecture du produit

Le périmètre de la TOE évalué est celui encadré de traits pointillés.

La TOE est constituée des éléments suivants :

- le microcontrôleur «M7892 G12 », offrant les fonctionnalités matérielles (gestion de la mémoire, gestion des entrées/sorties et accélérateurs cryptographiques) (voir [CER-IC]) ;
- une partie native composée des éléments suivants :
  - un gestionnaire de mémoire (*Memory Manager*) ;
  - un gestionnaire de communication (*Communication I/O*) ;
  - des librairies cryptographiques GEMALTO (*Crypto Libs*).
- un système *JAVA CARD* (*Java Card System*) composé des éléments suivants :
  - un environnement d'exécution (*Java Card 3.0.4 Runtine Environment*) ;
  - une machine virtuelle *Java Card* (*Java Card 3.0.4 Virtual Machine*) ;
  - une interface de programmation (*Java Card 3.0.4 Application Programming Interface*) contenant notamment le paquet propriétaire « com.gemalto.javacardx.pace » ;
  - un module GAP[1], qui est une extension du module PACE ;
  - un gestionnaire d'applications (*Card Manager*) ;
  - une application GDP[2] permettant la personnalisation des applications ;

[1] *General Authentication Procedure*

[2] *Global Dispatcher Perso*

- une application AAS[3] permettant de désinstaller et réinstaller une application avec différents paramètres.

Les applications déjà chargées dans le produit sont toutes identifiées dans le document (voir tableau 2). Bien que ces 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 [AGD-Dev_Basic].

1.2.4 *Identification du produit*

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La procédure d'identification du produit (*Tag Identity value*) est décrite dans le guide [AGD_OPE].

1.2.4.1 Configuration 1 : capacité RF de 27pF

Les données d'identification propriétaires sont obtenues en réponse à la commande GET DATA « 00 CA **01 03** ». Ces données correspondent à :

- B0 = *Gemalto Family Name*, identifiant du nom de la famille de produits (Java Card) ;
- 85 = *Gemalto OS Name*, identifiant du nom du système d'exploitation (MultiApp) ;
- 59 = *Gemalto Mask Number*, identifiant du masque (V4.0.1) ;
- xx = *Gemalto Product Name*, identifiant du nom de produit (MultiApp V4.0.1) égal à 56 pour le produit en production et FF pour le produit évalué ;
- 01 = *Flow Id version*, identifiant de la version du flux ;
- 10 = *Filter set*, identifiant de la version du filtre ;
- 40 90 = *Chip Manufacturer*, identifiant du fabricant composant sous-jacent (*INFINEON*) ;
- 78 97 = *Chip Identifier*, identifiant du composant sous-jacent (SLE78CLFX400VPHM).

Les données de production du produit sont obtenues en réponse à la commande GET DATA« 00 CA **9F 7F**». Ces données correspondent à :

- 40 90 = *IC_Fabricator* ;
- 78 97 = SLE78CLFX400VPHM ;
- 12 91 = *OS_ID*, identifiant du système d'exploitation (*GEMALTO*) ;
- 93 22 = *OS_Release_Date*, date d'émission du système d'exploitation (18/11/2019) ;
- 04 00 = *OS_Release_Level*, version du système d'exploitation (4.0).

1.2.4.2 Configuration 2 : capacité RF de 56pF

Les données d'identification propriétaires sont obtenues en réponse à la commande GET DATA « 00 CA **01 03** ». Ces données correspondent à :

- B0 = *Gemalto Family Name*, identifiant du nom de la famille de produits (Java Card) ;
- 85 = *Gemalto OS Name*, identifiant du nom du système d'exploitation (MultiApp) ;
- 59 = *Gemalto Mask Number*, identifiant du masque (V4.0.1) ;

[3] *Application Administration Service.*

- xx = *Gemalto Product Name*, identifiant du nom de produit (MultiApp V4.0.1) égal à 56 pour le produit en production et FF pour le produit évalué ;
- 01 = *Flow Id version*, identifiant de la version du flux ;
- 10 = *Filter set*, identifiant de la version du filtre ;
- 40 90 = *Chip Manufacturer*, identifiant du fabricant composant sous-jacent (*INFINEON*) ;
- 78 79 = *Chip Identifier*, identifiant du composant sous-jacent (SLE78CLFX4007PHM).

Les données de production du produit sont obtenues en réponse à la commande GET DATA « 00 CA **9F 7F**». Ces données correspondent à :

- 40 90 = *IC_Fabricator* ;
- 78 79 = SLE78CLFX4007PHM ;
- 12 91 = *OS_ID*, identifiant du système d'exploitation (*GEMALTO*) ;
- 00 51 = *OS_Release_Date*, date d'émission du système d'exploitation (2020/02/20) ;
- 04 00 = *OS_Release_Level*, version du système d'exploitation (4.0).

Pour les deux configurations, la principale différence entre le produit et la TOE (la plateforme) correspond aux applications chargées pré-émission sur ce produit. Toutes les applications présentes dans la configuration du produit durant son évaluation sont identifiées dans la table ci-dessous. Cette table liste les applications et les paquetages (*packages*) inclus dans le produit, associés à leurs noms et AID.

Applet name	**AID**	**Package name**
eTravel v2.2	A0 00 00 00 18 30 0B 02 00 00 00 00 00 00 00 FF	NA
IAS Classic V4.4.2	A0 00 00 00 18 80 00 00 00 06 62 40 FF	com/gemalto/IASClassic
PPCA V1.0	A0 00 00 00 30 80 00 00 00 0A 71 00 FF	com/gemalto/javacard/ppca
BioPIN Manager v2.0	4D 4F 43 41 5F 43 6C 69 65 6E 74 4D 4F 43 41 5F 53 65 72 76 65 71 4D 4F 43 41 5F 53 65 72 76 65 72	com/gemalto/moc/client com/gemalto/moc/api 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
OATH v2.0	A0 00 00 00 18 30 10 02 00 00 00 00 00 00 00 02	com/gemalto/OATH
PURE DI 3.03	A0 00 00 00 18 32 0A 01 00 00 00 00 00 00 00 FF A0 00 00 00 18 02 00 01 65 6D 76 61 70 69 00 FB A0 00 00 00 18 30 07 01 00 00 00 00 00 00 01 FF	com/gemalto/puredi com/gemalto/emvapi com/axalto/PPSE
Privacy Manager v1.0 (also known as "eID/eSign")	A0 00 00 00 30 80 00 00 00 08 DB 00 FF A0 00 00 00 30 80 00 00 00 08 F5 00 FF	com/gemalto/edi com/gemalto/esign

Microsoft Plug & Play	A0 00 00 00 30 80 00 00 00 06 DF 00 FF	com/gemalto/javacard/mspnp

Tableau 1 : Liste des applications chargées dans le produit.

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.

1.2.5 *Cycle de vie*

Le cycle de vie est décrit au chapitre 2.4.2 de la cible de sécurité.

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 composant (*firmware*), le système d'exploitation, le système *JAVA CARD*, la documentation, certaines *applets* et d'autres parties logicielles de la plateforme ;
  - au développement du composant de sécurité ;

- la phase 3 correspond :
  - à la fabrication du composant sécurisé SLE78 (M7892) développé par INFINEON ;
  - 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 de l'IC, 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 l'étape 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]	**Singapore [SGP]**
GEMALTO	GEMALTO
6, Rue de la Verrerie	12 Ayer Rajah Crescent
92190 Meudon, France	Singapor 139941, Singapore

Gémenos [GEM] GEMALTO Avenue du Pic de Bretagne 13881 Gémenos, France	**La Ciotat [VIG]** GEMALTO Avenue du Jujubier, ZI Athelia IV 13705 La Ciotat, France
Tczew [TCZ] GEMALTO Ul. Skarszewska 2 33-110 Tczew, Pologne	**Montgomery [MGY]** GEMALTO 101 & 106 Park Drive Montgomeryville, PA 18 936 United States
Curitiba [CBA] GEMALTO Rodovia Dep. Leopoldo Jacomel, 13102 83323-410 Pinhais, PR Brazil	**Vantaa [VAN]** GEMALTO Myllynkivenkuja 4, Vantaa, Finland, FI-01620
Pont Audemer [PAU] GEMALTO Z.I. Saint Ulfrant rue de Saint Ulkfrant 27500 Pont Audemer, France	**ATOS Pune [PUN]** ATOS Embassy Tech Zone, Phase II, Rajiv Gandhi Infitech Park, MIDC, Hinjewadi Pune – 411057, India
ATOS Marcoussis [MAR] ATOS DATA 4, 3, route de Marcoussis, 91620 Nozay, France	**ATOS Aubervilliers [PAR]** ATOS 153, avenue Jean Jaurès, 933307 Aubervilliers, France
Calamba [VZN] GEMALTO Building 7-A, Southern Luzon Industrial Complex Purok 3, Barangay Batino Calamba City, 4027 Laguna, Philippines	

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

Le guide [AGD-OPE] identifie également des recommandations relatives à la livraison des futures applications à charger sur cette carte.
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 ; les guides [AGD-OPE-VA] décrivent les règles de vérification qui doivent être appliquées par l'autorité de vérification.

Pour l'évaluation, l'évaluateur a considéré comme :

- administrateur du produit : les agents qui agissent pour le compte de l'émetteur. Ils personnalisent le produit et les données applicatives correspondant aux données de l'identité de l'utilisateur ;
- utilisateur du produit : le titulaire légitime du produit.

1.2.6 *Configuration évaluée*

Le certificat porte sur « MultiApp v4.0.1 with Filter Set 1.0 Java Card Open Platform on M7892 G12 Chip ». Les plateformes évaluées sont en composition sur les microcontrôleurs SLE78CLFX400VPHM et SLE78CLFX4007PHM issus de la famille de composants M7892.

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 2.2 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 le tableau 2 du §1.2.4 ont été vérifiées conformément aux contraintes décrites dans [AGD-OPE_VA].

Le produit contient deux algorithmes de comparaison, l'un pour les empreintes digitales (*fingerprint*) et l'autre pour la reconnaissance fasciale. Seul le *fingerprint* a été inclus dans le périmètre cette évaluation.

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 « M7892 G12 » au niveau EAL6 augmenté du composant ALC_FLR.1, conforme au profil de protection [PP0084]. Ce microcontrôleur a été certifié le 19 décembre 2019 sous la référence BSI-DSZ-CC-0891-V4-2019, voir [CER-IC].

L'évaluation s'appuie sur les résultats d'évaluation du produit « Plateforme Java Card MultiApp V4.0.1 » certifié le 18 décembre 2017 sous la référence ANSSI-CC-2017/76, voir [CER] et sur la surveillance de ce produit [SUR].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 16 octobre 2020, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

La cotation des mécanismes cryptographiques a été réalisée conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus sont inclus dans le [RTE]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI. 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

2.4 Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CER-IC]).

Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI [REF], la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.

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 « MultiApp v4.0.1 with Filter Set 1.0 Java Card Open Platform on M7892 G12 chip » 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 [GUIDES], notamment :

- toutes les futures applications chargées sur ce produit (chargement *post-issuance*) doivent respecter les contraintes de développement de la plateforme (guides [AGD-Dev_Basic] et [AGD-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-issuance*) doit être activée conformément aux indications de [TECH_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 :

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 :

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

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

ANNEXE A. Niveau d'évaluation du produit

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

ANNEXE B. Références documentaires du produits évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - MultiAppV4.0.1 with filter set 1.0 Javacard Platform - Security Target, référence D1514215, version1.17, 25/9/2020, THALES DIS. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - MultiAppV4.0.1 with filter set 1.0 Javacard Platform - Security Target, Public version, D1514215_LITE, version1.8, 2/10/2020, THALES DIS.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – ROBINA project, référence ROBINA_ETR_v1.2, version 1.2, 16/10/2020, *SERMA SAFETY & SECURITY.* Pour le besoin des évaluations en composition avec la plateforme un rapport technique pour la composition a été validé : - Evaluation Technical Lite Report – ROBINA Project, référence ROBINA_ETR_Lite_v1.2, version 1.2, 16/10/2020, SERMA SAFETY & SECURITY.
[CONF]	Liste de configuration du produit : - MultiApp V4.0.1 with FilterSet 1.0 : ALC LIS document – Javacard Platform, référence D1521420, version 1.7, 2/10/2020, THALES DIS ; - Source control viewproject, référence « Source control viewproject.txt », version 1.23.1.20, 14/3/2017, THALES DIS.

[GUIDES]	Guide d'installation du produit [AGD_PRE] : - MultiApp V4.0.1 with filter Set 1.0 AGD_PRE document – Javacard Platform, référence D1431347, version 1.1, 14/2/2020, THALES DIS. Guide d'administration du produit [AGD_OPE] : - MultiApp V4.0.1 with filter set 1.0 Javacard Platform - AGD_OPE document, référence D1432683, version 1.11, 24/9/2020, THALES DIS. Guide d'utilisation du produit : - [TECH_LOAD] MultiApp ID Operating System With Filter 1.0 Reference Manual, référence D1516415A, 26/2/2020, THALES DIS ; - Global Dispatcher Personalization Applet – User Guide, référence D1390286D du 30/05/2017, THALES DIS ; - CNIe – Electronic Personalization Specification and Application Administration Service, reference D1518028, version 1.4, 7/2/2020, THALES DIS ; - MultiApp ID Operating System Application Service – Reference Manual, reference D1519213C, 22/9/2020, THALES DIS ; Guides de développement d'applications : - [AGD-Dev_Basic] Rules for applications on Multiapp certified product: qualification level, référence D1484823, version 1.2, janvier 2019, THALES DIS ; - [AGD-Dev_Sec] Guidance for secure application development on Multiapp platforms, référence D1390326, version A01, mars 2018, THALES DIS ; Guides pour l'autorité de vérification [AGD-OPE_VA] : - Verification process of Gemalto non sensitive applet: qualification level, référence D1484874, version 1.0, décembre 2018, THALES DIS ; - Verification process of Third Party non sensitive applet : qualification level, référence D1484875, version 1.2, février 2019, THALES DIS.
[CER-IC]	Certification Report BSI-DSZ-CC-0891-V4-2019 for Infineon Security Controller M7892 Design Steps D11 and G12 with optional RSA2048/4096 v2.03.008, ECv2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries, symmetric crypto library v2.02.010 and with specific IC dedicated software (firmware) from INFINEON TECHNOLOGIES AG. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 19 décembre 2019, sous la référence BSI-DSZ-CC-0891-V4-2019.
[CER]	Plateforme Java Card MultiApp V4.0.1- PACE en configuration ouverte masquée sur le composant M7892 G12. Certifiée par l'ANSSI le 18 décembre 2017 sous la référence ANSSI-CC-2017/76.
[SUR]	Plateforme Java Card MultiApp V4.0.1- PACE en configuration ouverte masquée sur le composant M7892 G12. Surveillée par l'ANSSI le 5 mars 2020 sous la référence ANSSI-CC-2017/76-S01.

[PP JCS-O]	*Java Card System Protection Profile - Open Configuration, version 3.0. Profil de protection.* *Certifié par l'ANSSI le 25 juin 2010 et maintenu le 29 mai 2012 sous la référence ANSSI-CC-PP- 2010/03-M01.*
[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.

[SITES]	Rapports d'analyse documentaire : - Gemalto Development Environment ALC Class Evaluation (Generic Documentary activities), référence GTOGEN19_GEN_V1.0, 12 février 2019, SERMA SAFETY & SECURITY. Rapports d'audit de site pour la réutilisation : - [MDN] : Site Technical Audit Report MDN, référence GTOGEN19_MDN_STAR_v1.1, 27 novembre 2019, SERMA SAFETY & SECURITY ; - [SGP] : Development Environment Singapore Site Visit Lite Report, référence 17-0466-SGP_SVR-M_v1.0, mai 2018, SERMA SAFETY & SECURITY ; - [GEM] : THALES DIS Development Environment – THALES DIS Géménos Site Technical Audit Report – DISGEN20_GEM_STAR_v1.0, août 2020, SERMA SAFETY & SECURITY ; - [VIG] : THALES DIS Development – THALES DIS la Ciotat Environment LA CIOTAT Site Technical Audit Report, référence DISGEN20_VIG_STAR_v1.0, 18 août 2020, SERMA SAFETY & SECURITY ; - [TCZ] : Site Technical Audit Report – TCZEW site audit, référence 17-0466-TCZ_STAR_v1.0, décembre 2018, SERMA SAFETY & SECURITY ; - [MGY] : Site Technical Audit Report MGY, référence GTOGEN19_MGY_STAR_v1.1, 19 décembre 2019, SERMA SAFETY & SECURITY ; - [CBA] : Site Technical Audit Report CBA, référence GTOGEN19_CBA_STAR_v1.0, avril 2019, SERMA SAFETY & SECURITY ; - [VAN] : Site Technical Audit Report VAN, référence GTOGEN19_VAN_STAR_v1.0, mai 2019, SERMA SAFETY & SECURITY ; - [PAU] : Site Technical Audit Report GEMALTO Pont-Audemer, référence 17-0466-PAU_STAR_v1.0, octobre 2018, SERMA SAFETY & SECURITY ; - [PUN] : Site Technical Audit Report PUN2, référence GTOGEN19a et b_PUN2_STAR_v1.2, mars 2020, SERMA SAFETY & SECURITY ; - [MAR] : Site Technical Audit Report MAR, référence GTOGEN19_MAR_STAR_v1.1, 5 décembre 2019, SERMA SAFETY & SECURITY ; - [PAR] : Site Technical Audit Report ATOS_PAR, référence ATOS_PAR_STAR_v1.0, août 2018, SERMA SAFETY & SECURITY ; - [VZN] : o Site Technical Audit Report – CAL-VZN Site Audit, référence GTOGEN19_CAL-VZN_STAR_V1.0, juillet 2019, SERMA SAFETY & SECURITY ; o Site Technical Audit Report – GEM-VZN Site Audit, référence GTOGEN19_GEM-VZN_STAR_V1.0, juillet 2019, SERMA SAFETY & SECURITY.

ANNEXE C. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1: Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - *Part 2: Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - *Part 3: Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation :* - *Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	*Mandatory Technical Document - The Application of CC to Integrated Circuits*, version 3.0, février 2009.
[JIWG AP] *	*Mandatory Technical Document - Application of attack potential to smartcards*, 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.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.

	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), voir www.ssi.gouv.fr.
[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.