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-2017/54

Plateforme JavaCard MultiApp V4.0 - PACE en configuration ouverte basée sur l'Operating System JLEP3 masquée sur le composant SLE78CLFX4000PH (M7892 G12)

Paris, le 25 septembre 2017

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-2017/54

Nom du produit

Plateforme JavaCard MultiApp V4.0 - PACE en configuration ouverte basée sur l'Operating System JLEP3 masquée sur le composant SLE78CLFX4000PH (M7892 G12)

Référence/version du produit

JavaCard version 3.0.4, GP version 2.2.1

Conformité à un profil de protection

[PP JCS-O] SUN Java Card System Protection Profile Open Configuration, version 3.0

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

Gemalto

6 rue de la Verrerie CS20001
92197 Meudon Cedex, France

Infineon Technologies AG

Am Campeon 1-12, 85579 Neubiberg,
Allemagne

Commanditaire

Gemalto

6 rue de la Verrerie CS20001
92197 Meudon Cedex, France

Centre d'évaluation

Serma Safety & Security

14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

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 Premier ministre 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

1.1. Présentation du produit

Le produit évalué est la « plateforme JavaCard MultiApp V4.0 - PACE en configuration ouverte basée sur l'Operating System JLEP3 masquée sur le composant SLE78CLFX4000PH (M7892 G12), JavaCard version 3.0.4, GP version 2.2.1 » développé par *GEMALTO* et par *INFINEON TECHNOLOGIES AG*.

Le produit est destiné à héberger et exécuter une ou plusieurs applications, dites *applets* dans la terminologie JavaCard. Ces *applets* 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-O].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par la plateforme ouverte JavaCard 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* (« l'extradition » permet à plusieurs applications de partager un domaine de sécurité dédié) ;
- la suppression d'applications sous le contrôle du *Card Manager* ;
- le *secure channel* PACE conforme aux protocoles de *Global Plateform* et de PACE ;
- l'interface de programmation permettant d'opérer de manière sûre les applications ;
- 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.

Les services de sécurité offerts par le microcontrôleur sont :

- la gestion sécurisée du cycle de vie ;
- la protection contre le « *snooping* » ;
- la protection contre les attaques par fautes ;
- la protection contre les attaques logiques ;
- le support cryptographique.

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

1.2.3. Architecture

L'architecture du produit est illustrée par la figure suivante (la TOE[1] est délimitée entre pointillé) :

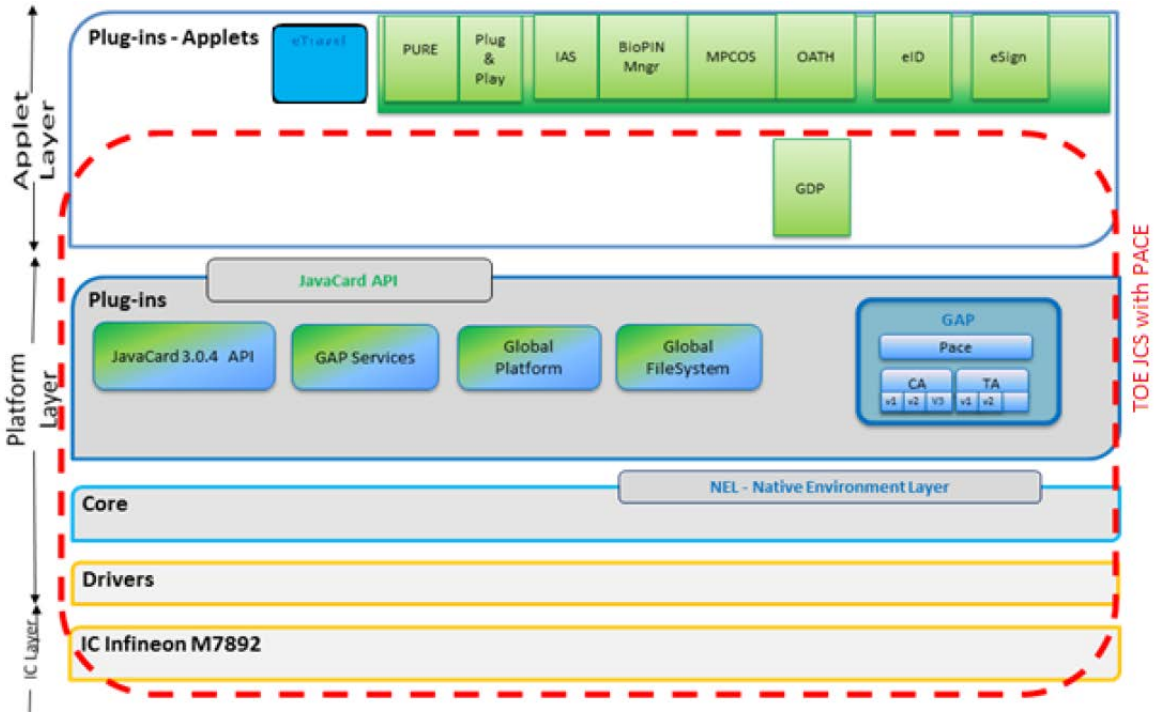


Figure 1 : Architecture du produit MultiApp V4 - PACE

La TOE est constituée des éléments suivants :

- le microcontrôleur SLE78CLFX4000PH (M7892 G12), offrant les fonctionnalités matérielles (gestion de la mémoire et gestion des entrées/sorties), et sa librairie cryptographique ;
- une partie native composée des éléments suivants :
  - un gestionnaire de mémoire *Memory Manager* ;
  - un gestionnaire de communication *Communication (I/O)* ;
  - un gestionnaire de librairies cryptographiques *Crypto Libs*,
- un système JavaCard (*Java Card System*) composé des éléments suivants :
  - un environnement *Runtime* (*JavaCard 3.0.4 Runtine Environment*) ;
  - une machine virtuelle JavaCard (*JavaCard 3.0.4 Virtual Machine*) ;
  - une interface de programmation (*JavaCard 3.0.4 Application Programming Interface*) contenant notamment le paquet propriétaire « com.gemalto.javacardx.pace » ;
  - un module GAP, qui est une extension du module PACE ;
  - un gestionnaire d'applications (*Card Manager*) ;
  - une application GDP permettant la personnalisation des applications.

Les applications déjà chargées dans le produit sont toutes identifiées dans la table 3, ci-après. Bien que ces applications standards ne soient pas incluses dans le périmètre de l'évaluation, elles

[1] *Target Of Evaluation* – cible de sécurité.

ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [OPEN]. En effet, ces applications standards 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 version certifiée du produit est identifiable par les éléments suivants, détaillés dans la cible de sécurité [ST] au chapitre 1.2 « *TOE Reference* » :

Eléments de configuration		Origine
Nom de la TOE	MultiApp V4.0 on M7892-G12	*GEMALTO*
Référence interne de la TOE	MultiAppV40_EIR10_LBL05 Checkpoint 1.75	
Données de production du produit	40 90 78 97 **12 91 61 53** 04 00	
Données d'identification propriétaire des cartes de *GEMALTO*	B0 85 55 52 01 00 40 90 78 97 79 01 00 00 00 00 00 00 ZZ ZZ ZZ ZZ 01 75	
Référence du circuit intégré	M7892-G12	*INFINEON TECHNOLOGIES AG*

Table 1 : Identification du produit

Ces éléments peuvent être vérifiés par l'utilisation de commandes GET DATA ou à la lecture de l'ATR. La procédure d'identification du produit est décrite dans le guide [AGD_OPE].

Notamment, les données d'identification propriétaires des cartes de *GEMALTO* « B0 85 55 FF 01 00 40 90 78 97 79 01 00 00 00 00 00 00 ZZ ZZ ZZ ZZ » sont obtenues en réponses 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 *GEMALTO* ;
- 85 = *Gemalto OS Name*, identifiant du nom du système d'exploitation *GEMALTO ;*
- 55 = *Gemalto Mask Number*, identifiant du masque *GEMALTO* ;
- 52= *Gemalto Product Name*, identifiant du nom de produit *GEMALTO* ;
- 01 = *Gemalto Flow version*, identifiant de la version du flux *GEMALTO* ;
- 00 = *Gemalto Filter version*, identifiant de la version du filtre *GEMALTO* ;
- 40 90 = *IC_Fabricator*, identifiant de la fonderie du composant sous-jacent (*INFINEON*) ;
- 78 97 = *IC_Type*, identifiant du composant sous-jacent (SLE78CLFX400VPHM) ;
- 79 01 = *BPU* (SLE78CLFX400VPH) ;
- 00 00 00 = *PDM Technical Product Identifier* ;
- 00 00 00 = *PDM Customer Item Identifier* ;
- ZZ ZZ ZZ ZZ = *Feature Configuration*, les valeurs dépendent des services configurés disponibles (voir figure 2 ci-après) ;
- 01 75 = *Built version*, version interne du produit qui correspond à la version du code MultiAppV40_EIR10_LBL05.

Les champs *BPU*, *PDM Technical Product Identifier* et *PDM Customer Item Identifier* sont des caractéristiques de production qui ne sont pas liées à l'identification de la TOE.

Le produit offre la possibilité d'embarquer seulement des fonctionnalités requises par le client. Par exemple, la génération de clés RSA peut être supprimée de la configuration fournie. La configuration des services disponibles est identifiable à l'aide de la table 2, où X vaut 1 si le service est disponible, 0 sinon.

Optional features / Field (extarct from identity tag)	Crypto features byte A								Crypto features byte B								Other features byte 1								Other features byte 2							
bit	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
ECC	X																															
RSA									X																							
RSA-DH												X																				
RSA-OBKG													X																			
RSA 4K															X																	
PACE common																	X															
PACE DH																		X														
PACE ECC																			X													
Linker																				X												
ISM																					X											
Etravel																						X										
EAC/GAP																							X									
Biometry																									X							

Table 2 : Configuration des fonctionnalités possibles

Les données de production du produit « 40 90 78 97 12 91 61 53 04 00 » sont obtenues en réponse à la commande GET DATA CPLC « 00 CA **9F 7F**». Ces données correspondent à :

- 40 90 = *IC_Fabricator* ;
- 78 97 = *IC_Type* ;
- 12 91 = *OS_ID*, identifiant du système d'exploitation ;
- 61 53 = *OS_Release_Date*, date d'émission du système d'exploitation (19/05/2016) ;
- 04 00 = *OS_Release_Level*, niveau d'émission du système d'exploitation dans les projets du développeur (niveau 4.0).

La principale différence entre le produit et la TOE (la plateforme) correspond aux applications chargées pré-émission. Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans la table 1 qui liste les applications et les paquetages (*packages)* inclus dans le produit, associés à leurs noms et AID.
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.

Nom de l'application	***Application Identifier* (AID)**	**Nom de paquetages**
eTravel v2.2	A0 00 00 00 18 30 0B 02 00 00 00 00 00 00 00 FF	NA
IAS Classic V4.4	A0 00 00 00 18 80 00 00 00 06 62 40 FF	com/gemalto/IASClassic
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 3.0.3	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/javacard/eid com/gemalto/javacard/esign
Microsoft Plug&Play	A0 00 00 00 30 80 00 00 00 06 DF 00 FF	com/gemalto/javacard/mspnp

Table 3 : Applications déjà chargées dans le produit

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit par la figure 2 ci-après, voir aussi [ST].

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

Phase (name)	Phase (card)	Actor	Comment
Development	1. OS&applet& script Development	Developer (Gemalto)	- Development of Java Card Platform and applications -Generation of principal HEX, mapping description - Script generation for initialization and pre-personalization
	2 HW Development	IC manufacturer (Infineon)	- Development of IC
Manufacturing	3 Mask manufacturing	IC manufacturer (Infineon)	Manufacturing of virgin chip integrated circuits embedding the Infineon flash Loader and protected by a dedicated transport key.
	4 Module manufacturing	Module creation (Gemalto or Infineon)	IC packaging & testing
	5.a Embedding(Optional)	*Form factor manufacturer (Gemalto)*	*Put the module on a dedicated form factor (Card, Inlay, MFF2, other)*
	5.b Initialization / Pre-personalization	manufacturer (Gemalto)	Loading of the Gemalto software (platform and applets on top of it based on script generated)
	5.c Embedding if not done during 5.a	*Form factor manufacturer (Gemalto)*	*Put the module on a dedicated form factor (Card, Inlay, MFF2, other)*
Personalization	6 Personalization	Personalizer	- Personalization
Usage	7 Usage	Holder	- The Issuer is responsible of card delivery to the end-user

Figure 2 : Cycle de vie du produit MulptiApp V4 - PACE

Le produit a été développé sur les sites suivants :

GEMALTO Meudon 6 Rue de la Verrerie 92190 Meudon, France	*GEMALTO* Singapore 12 Ayer Rajah Crescent Singapor 139941, Singapour
GEMALTO Gémenos Avenue du Pic de Bertagne 13881 Gémenos, France	*GEMALTO* La Ciotat Avenue du Jujubier, ZI Athelia IV 13705 La Ciotat, France
ATOS Paris (Aubervilliers / Croissy) 4 rue des Vieilles Vignes 77 183 Croissy-Beaubourg, France	*ATOS* Bydgoszcz – (ATOS Poland) Biznes Park, ul. Kraszewskiego 1 85-240 Bydgoszcz, Pologne
GEMALTO Barcelona Poligono lndustrial Llevant CL Llevant 12, 08150 Parets del Valles,Barcelona, Espagne	*GEMALTO* Montgomery 101 & 106 Park Drive Montgomeryville, PA 18 936 Etats-Unis
GEMALTO Curitiba Rodovia Dep. Leopoldo Jacomel, 13102 83323-410 Pinhais, Brézil	*GEMALTO* Vantaa Myllynkivenkuja 4, Vantaa, Finlande, FI-01620
GEMALTO Tczew Ul. Skarszewska 2 33-110 Tczew, Pologne	*GEMALTO* Pont Audemer Z.l. Saint Ulfrant rue de Saint Ulfrant 27500 Pont Audemer, France
UTAC THAI LIMITED 1 237 Lasalle Road, Bangna, Bangkok 10260, Thaïlande	*UTAC THAI LIMITED 3* 73 Moo5, Bangsamak, Chachoengsao 24180, Thaïlande

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 ; 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 3 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 4** [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 « 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) » au niveau EAL6 augmenté du composant ALC_FLR.1, conforme au profil de protection [PP0084]. Ce microcontrôleur a été certifié le 20 décembre 2016 sous la référence BSI-DSZ-CC-0891-V2-2016 (voir [CER-IC]).

L'évaluation s'appuie sur les résultats d'évaluation de la « plateforme JavaCard MultiApp V4.0 en configuration ouverte basée sur l'Operating System JLEP3 masquée sur le composant SLE78CLFX4000PH (M7892 G12) » certifié le 8 mars 2017 sous la référence ANSSI-CC-2017/07 (voir [CER]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 7 août 2017 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 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 la « plateforme JavaCard MultiApp V4.0 - PACE en configuration ouverte basée sur l'Operating System JLEP3 masquée sur le composant SLE78CLFX4000PH (M7892 G12), JavaCard version 3.0.4, GP version 2.2.1 » 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 0 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 [GUIDE].

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

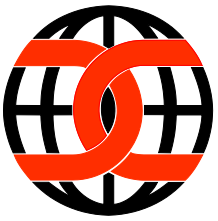
Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], 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 signataires[2], 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**	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**	1	**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 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - MultiAppV4 JCS with PACE Security Target, référence D1368111_EXT_ST_JCS_wtih_PACE_MultiAppV4, version1.0, 25/07/2017. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - MultiAppV4 JCS with PACE Security Target (Lite) Public Version, référence D1368111_EXT_ST_JCS_wtih_PACE_MultiAppV4, version 1.0p, 1/08/2017.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – OASIS-EXT project, référence OASIS-EXT_ETR_v1.1, version 1.1, 7/08/2017. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - ETR Lite for Composition – OASIS-EXT Project, référence OASIS-EXT_ETR_v1.1_lite, version 1.1, 07/08/2017.
[CONF]	Liste de configuration du produit : - LIS : Configuration list for platform, référence D1402692_EXT_LIS_DOC_JCS _MAV4.0, version 1.0, 09/07/2015 ; - List of configuration for Document system for OASIS_EXT, référence D1402692_EXT-LIS-PLF-DOCUMENT, version 1.5, 01/08/2017 ; - LIS_PLTF_CODE, référence Items_for_Pltf.zip, version 1.75, 23/06/2016.

[GUIDES]	Guide d'installation du produit [AGD_PRE] : - MultiApp V4 AGD_PRE document – Javacard Platform, référence D1390316, version 1.1 du 06/06/2016, *GEMALTO*. Guide d'administration du produit [AGD_OPE] : - MultiApp V4 AGD_OPE document – Javacard Platform, référence D1390321, version 1.2 du 15/02/2017, *GEMALTO*. Guide d'utilisation du produit : - MultiApp ID Operating System – Reference manual, référence D1392687A, 15/02/2017, *GEMALTO* ; - Global Dispatcher Personalization Applet – User Guide, référence D1390286D, 30/05/2017, *GEMALTO* ; - Guide de développement d'applications [AGD-Dev_Basic] : Rules for applications on Multiapp certified product, référence D1390963_EXT, version 1.1 de juin 2017, *GEMALTO* ; - Guide de développement d'applications sécurisées [AGD-Dev_ Sec] : Guidance for secure application development on Multiapp platforms, référence : D1390326, version A01 de février 2016, *GEMALTO*, - Guide pour l'autorité de vérification [AGD-OPE_VA] : o Verification process of *GEMALTO* non sensitive applet, référence D1390670, version A01 de février 2016, *GEMALTO* ; o Verification process of Third Party non sensitive applet, référence D1390671, version A01 de février 2016, *GEMALTO*.
[CER]	Rapport de certification ANSSI-CC-2017/07, Plateforme JavaCard MultiApp V4.0 en configuration ouverte basée sur l'Operating System JLEP3 masquée sur le composant SLE78CLFX4000PH (M7892 G12). *Certifié par l'ANSSI le 8 mars 2017 sous la référence ANSSI-CC-2017/07.*
[CER-IC]	Certification Report BSI-DSZ-CC-0891-V2-2016 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 20 décembre 2016, sous la référence BSI-DSZ-CC-0891-V2-2016.*
[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. *Certifié par le BSI sous la référence BSI-PP-0084-2014.*

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 : - Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; - Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; - Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[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 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.4, août 2015.
[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.

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