Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2020/33

MultiApp V4 JavaCard Virtual Machine (Référence 4.0.1)

Paris, le 28 mai 2020

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

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

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

Toute correspondance relative à ce rapport doit être adressée au :

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

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2020/33

Nom du produit

MultiApp V4 JavaCard Virtual Machine

Référence/version du produit

Référence 4.0.1

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 7

Développeurs

Gemalto

6 rue de la verrerie, 92190 Meudon, France

Trusted Labs

6 rue de la verrerie, 92190 Meudon, France

Infineon Technologies AG

Am Campeon 1-12, 85579 Neubiberg, Allemagne

Commanditaire

Gemalto

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

SOG-IS

Ce certificat est reconnu au niveau EAL2

Préface

La certification

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

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le directeur général de l'Agence national de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit considéré est la carte « MultiApp V4.0.1 » développée par *GEMALTO*, *TRUSTED LABS* et *INFINEON TECHNOLOGIES AG*. La « plateforme JavaCard MultiApp V4.0.1 » de la carte a déjà fait l'objet d'une certification au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5 (voir détails en section 2.2 et [CER-PLF]).
L'objet du présent rapport de certification est le résultat de l'évaluation de la machine virtuelle « MultiApp V4 JavaCard Virtual Machine, référence 4.0.1 ».

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 services de sécurité fournis par le produit sont décrits dans [CER-PLF].

1.2.3. Architecture

La carte « Mutli App V4.0.1 » est constituée des éléments suivants :
- du microcontrôleur M7892 G12 précédemment certifié (voir [CER-IC]) ;
- de la « plateforme JavaCard MultiApp V4.0.1 » certifié au niveau EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5 (voir [CER-PLF]) ;
- des *applets* « identités » : IAS V4.4, eTravel 2.2, Pure 2.1, Plug&Play, BioPin Management, MPCOS, OATH, e-ID, e-Sign (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[1] soumise à l'évaluation au niveau EAL 7 est restreinte au :
- *linker*, pour l'installation des *applets* post-issuance ;
- *interpreter*, pour l'exécution des *bytecodes* Java Card et la mise en application des règles du *firewall* ;
- *firewall* lié aux API Java Card native, pour assurer qu'il n'y ait pas de moyen de contourner le contrôle d'accès du *firewall*.

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

L'architecture du produit est illustrée par la figure ci-après, où il est précisé :

- par un encadré rouge la présente TOE (évaluée au niveau EAL7) ;
- en pointillé rouge la TOE qui a été certifiée précédemment, voir [CER-PLF].

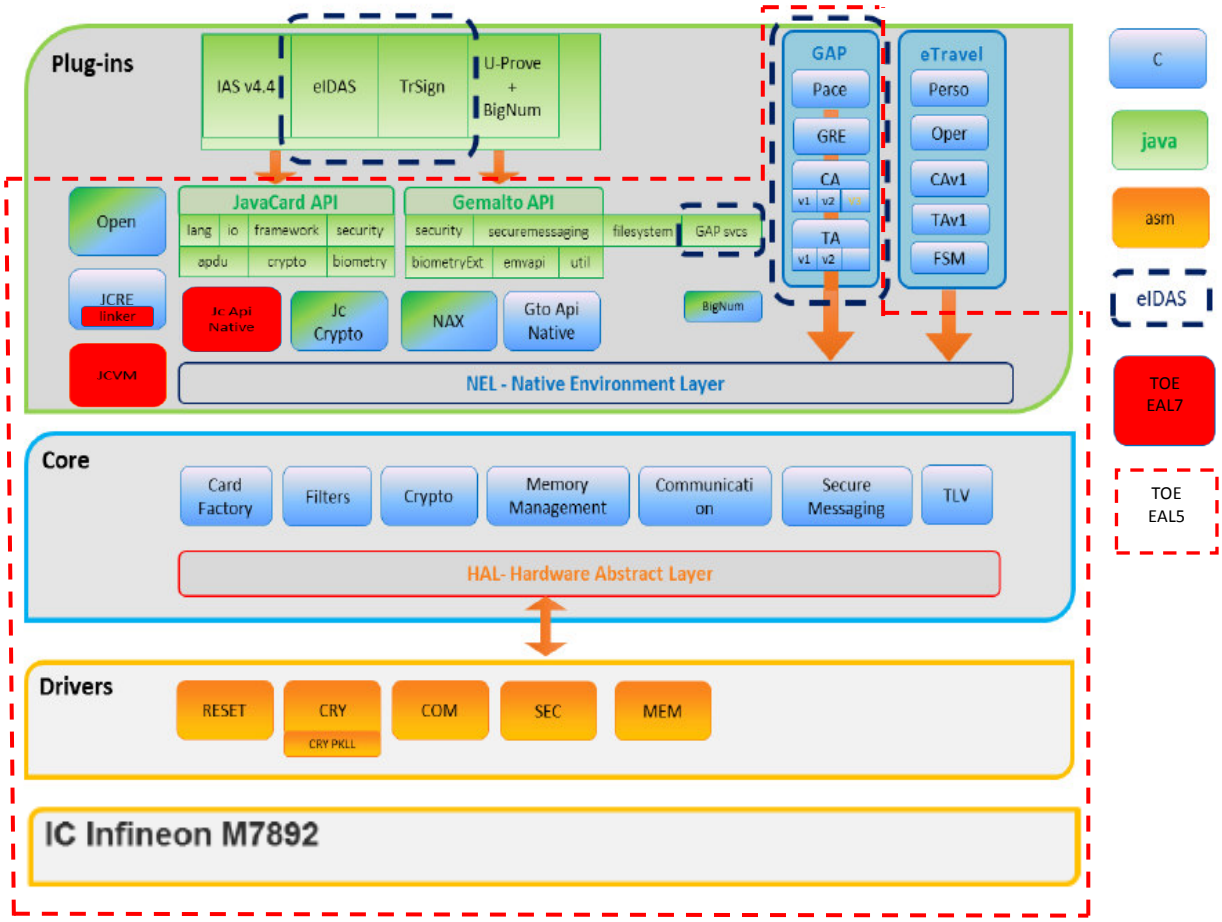

Figure 1 : Architecture du produit « MultiApp V4.0.1 »

1.2.4. Identification du produit

Les éléments constitutifs du produit, dont sa machine virtuelle, sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par les éléments du tableau ci-après, détaillés dans le guide [AGD_OPE].

Configuration de la TOE	Données lues	Origine
Family name et *OS Name*	B0 85	*GEMALTO*
Mask Number V4.0.1	59	
product name MultiApp V4.0.1	56 ou ff	
Flow version	01	
Filter version	02	
Operating System Identifier	12 91	
Operating System Release Date 2017/03/31	70 90	
Operating System Release Level 4.0	04 00	
Donnée d'identification du circuit intégré *INFINEON* M7892 G12	40 90 78 97	*INFINEON TECHNOLOGIES AG*

Tableau 1 : Identification du produit « MultiApp V4.0.1 »

1.2.5. Cycle de vie

Le cycle de vie du produit « MultiApp V4.0.1 » détaillé au chapitre « *2. TOE Overview* » de la cible de sécurité [ST]. Il est similaire à celui décrit dans [CER-PLF], excepté l'ajout du site de développement *TRUSTED LABS* pour le support EAL 7 à Meudon (développement du modèle formel et de la documentation associée), voir [STAR].

1.2.6. Configuration évaluée

Le certificat porte uniquement sur les fonctionnalités offertes par la machine virtuelle de la « plateforme JavaCard MultiApp V4.0.1 » décrite dans la section 1.2.3 et identifiée dans la section 1.2.4.

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 s'appuie sur les résultats d'évaluation de la plateforme « Plateforme JavaCard MultiApp V4.0.1 - PACE en configuration ouverte masquée sur le composant M7892 G12, JavaCard version 3.0.4, GP version 2.2.1 » certifiée le 18 décembre 2017 sous la référence ANSSI-CC-2017/76, voir [CER-PLF], et surveillée le 5 mars 2020 sous la référence ANSSI-CC-2017/76-S01, voir [SUR-PLF].

Cette évaluation a consisté à évaluer la machine virtuelle « MultiApp V4 JavaCard Virtual Machine, référence 4.0.1 » 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 13 mai 2020, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

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

2.4. Analyse du générateur d'aléas

Le 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, voir [CER-PLF].
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 JavaCard Virtual Machine, référence 4.0.1 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 7.

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].

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 CC. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL 7 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[2], des certificats Critères Communs.
La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL 2 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 7	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	6	Complete semi-formal functional specification with additional formal specification
	ADV_IMP				1	1	2	2	2	Complete mapping of the implementation representation of the TSF
	ADV_INT					2	3	3	3	Minimally complex internals
	ADV_SPM						1	1	1	Formal TOE security policy model
	ADV_TDS		1	2	3	4	5	6	6	Complete semiformal modular design with formal high-level design presentation
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	5	Advanced support
	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	2	Measurable life-cycle model
	ALC_TAT				1	2	3	3	3	Compliance with implementation standards - all parts
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	3	Rigorous analysis of coverage
	ATE_DPT			1	1	3	3	4	4	Testing: implementation representation
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	3	Independent testing - complete
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 : - Security Target : MultiApp V4 Java Card Virtual Machine, référence D1391107, version 1.8, 7 février 2020. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Javacard Virtual Machine on MultiApp V4.0.1 Platform – Security Target, référence D1391107, version 1.8p.
[RTE]	Evaluation Technical Report OASIS7 Project, référence OASIS7-JCS_ETR_v1.5, version 1.5, 12 mai 2020.
[CONF]	Liste de configuration du produit, référence CP-2018-RT-581-1.1_CL.
[CER-IC]	Certification Report BSI-DSZ-CC-0891-V4-2019 for Infineon Security Controller M7892 Design Steps D11 and G12 with specific IC dedicated firmware and optional software from Infineon Technology AG. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 19 décembre 2019.*
[CER-PLF]	Rapport de certification ANSSI-CC-2017/76, Plateforme JavaCard MultiApp V4.0.1 - PACE en configuration ouverte masquée sur le composant M7892 G12. *Certifié par l'ANSSI le 18 décembre 2017.*
[SUR-PLF]	Rapport de surveillance ANSSI-CC-2017/76-S01, Plateforme JavaCard MultiApp V4.0.1 - PACE en configuration ouverte masquée sur le composant M7892 G12. *Surveillé par l'ANSSI le 5 mars 2020.*
[STAR]	Site Technical Audit Report MDN (Meudon), référence GTOGEN19_MDN_STAR_v1.1, novembre 2019.
[GUIDES]	- MultiApp V4.0.1- AGD_PRE document – Javacard Platform, référence D1431347, version 1.0 du 28 septembre 2017 ; - **[AGD_OPE] MultiApp V4.0.1 Javacard Platform - AGD_OPE document, référence D1432683, version 1.2 de février 2020* ;** - **MultiApp ID Operating System – Reference manual, référence D1392687, version E, 28 mars 2018* ;** - **Rules for applications on Multiapp certified product, référence D1484823, version 1.2 de janvier 2019* ;** - **Guidance for secure application development on Multiapp platforms, référence D1390326, version A01 de mars 2018* ;** - Verification process of Gemalto non sensitive applet, référence D1484874, version 1.0 de décembre 2018 ; - Verification process of Third Party non sensitive applet, référence D1484875, version 1.2 de février 2019.

* Guides contenant de nouvelles recommandations sécuritaires par rapport à l'évaluation initiale, voir [CER-PLF].

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 3.0, avril 2019.
[CCRA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.

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