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-R01

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

Paris, le 08 Janvier 2025

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

Vincent STRUBEL

[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-2020/42-R01**
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 **EAL5 augmenté** ALC_DVS.2, AVA_VAN.5
Développeur **THALES DIS FRANCE SAS** 6, rue de la Verrerie 92190 Meudon, France
Commanditaire **THALES DIS FRANCE SAS** 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.

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.cyber.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, MultiApp v4.0.1 with Filter Set 1.0 » développé par THALES DIS FRANCE SAS.

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 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 erronée ;
- 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-émission ;
- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications.

1.2.3 *Architecture*

Le produit est constitué des composants présentés au chapitre 2.3 « *TOE Boundaries* » de la cible de sécurité [ST].

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 détaillés dans la cible de sécurité [ST] au chapitre 1.2 « *TOE Identification* ».

Les données d'identification sont obtenues en réponse à la commande GET DATA. La procédure d'identification est décrite au chapitre 1.5 « Product Identification » dans le guide [AGD_OPE].

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 leur nom et leur AID[1] .

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

[1] *Application Identifier.*

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 du produit est décrit au chapitre 2.5.2 *« TOE Life-cycle »* de la cible de sécurité [ST]. Il est conforme à celui décrit dans [PP0084]. Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

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 :

- 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 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 le tableau 1 du §1.2.4 ont été vérifiées conformément aux contraintes décrites dans [AGD-OPE_VA].

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [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 », voir [CER_IC].

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 [RTE].

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 niveau d'attaquant 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 niveau d'attaquant 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 1.2du 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 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-émission) 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].

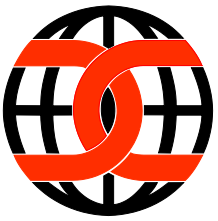
L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[2], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 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[3] , 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 :



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

[3] 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 : - *MultiAppV4.0.1 Javacard Platform with filter set 1.0 - Security Target*, référence D1514215, version1.35, 27 novembre 2024. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *MultiAppV4.0.1 Javacard Platform with filter set 1.0 - Security Target, Public version*, référence D1514215_LITE, version 3.5, 27 novembre 2024.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report – ROBIN-A-NS project*, référence ROBIN-A-NS_ETR_v1.1, version 1.1, 4 décembre 2024. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - *Evaluation Technical Report Lite for Composition – ROBIN-A-NS project*, référence ROBIN-A-NS_ETR_Lite_v1.0, version 1.0, 11 décembre 2024.
[CONF]	Liste de configuration du produit : - *MultiApp V4.0.1 with filter Set 1.0 : ALC LIS Document*, référence D1521420, version 2.00, 27 novembre 2024 ; - *Source control viewproject*, référence « Source control viewproject.txt », version 1.23.1.20, 14 mars 2017
[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 1.4, 21 mars 2024. Guide d'administration du produit [AGD_OPE] : - *MultiApp V4.0.1 : AGD_OPE document Javacard Platform*, référence D1432683, version 1.14, 21 novembre 2024. Guide d'utilisation du produit : - [TECH_LOAD] *MultiApp ID Operating System With Filter 1.0 Reference Manual*, référence D1516415A, 26 février 2020. - *MultiApp ID Operating System – Application Administration Service – Reference Manual*, référence D1519213I, 6 novembre 2024. Guides de développement d'applications : - [AGD-Dev_Basic] *Rules for applications on Multiapp certified product*, référence D1484823, version 1.2, janvier 2019 ; - [AGD-Dev_Sec] *Guidance for secure application development on Multiapp platforms*, référence D1390326, version A01, mars 2018. Guides pour l'autorité de vérification [AGD-OPE_VA] :

	- *Verification process of Gemalto non sensitive applet*, référence D1484874, version 1.0, décembre 2018 ; - *Verification process of Third Party non sensitive*, référence D1484875, version 1.2, février 2019.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - DISGEN22_ALC_GEN_v1.1 ; - DISGEN23_ALC_GEN_v1.0 ; - [CHA] DISGEN22_CHA_STAR_v1.0 ; - [CBA] DISGEN23_CUR_STAR_v1.0 ; - [GEM] DISGEN24_GEM_STAR_v1.0 ; - [LVG] DISGEN24_LVG_STAR_v1.0 ; - [MDN] DISGEN23_MDN_STAR_v1.1 ; - [MGY] DISGEN23-MGY_STAR_v1.0 ; - [PAU] DISGEN22_PAU_STAR_v1.0 ; - [SGP] DISGEN24_SGP_STAR_v1.0 ; - [SSN_SSC] DISGEN23_SSN_SSC_STAR_v1.0 ; - [TCZ] DISGEN23-TCZ_STAR_v1.0 ; - [TLH] DISGEN23_TLH_STAR_v1.0 - [VAN] DISGEN23_VAN_STAR_v1.0 ; - [VFO-CAL] DISGEN23_VFO-CAL_STAR_v1.0.
[CER_IC]	Certification Report BSI-DSZ-CC-0891-V7-2024 for M7892 Design Step G12, with specific IC dedicated firmware from INFINEON TECHNOLOGIES AG. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 8 juillet 2024, sous la référence BSI-DSZ-CC-0891-V7-2024.
[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.
[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.

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 5.0.
[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 3.2.1, février 2024.
[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 2.0, mai 2024.
[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.