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-2025/53

MultiApp v4.1 Javacard Platform (version 4.1.0.4)

Paris, le 16/12/2025 | 14:30 CET

Vincent Strubel

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

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 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 Résumé

Référence du rapport de certification	**ANSSI-CC-2025/53**
Nom du produit	**MultiApp v4.1 Javacard Platform**
Référence/version du produit	**version 4.1.0.4**
Type de produit	**Cartes à puce et dispositifs similaires**
Conformité à un profil de protection	***Java Card System Protection Profile – Open Configuration, version 3*** certifié ANSSI-PP-2010-03 en mai 2012
Critère d'évaluation et version	**Critères Communs version 3.1 révision 5**
Niveau d'évaluation	**EAL5 augmenté** ALC_DVS.2, AVA_VAN.5
Référence du rapport d'évaluation	*Evaluation Technical Report SUNDANCE-P-R02 Project* référence SUNDANCE-P-R02_ETR_v1.1 version 1.1 le 25 novembre 2025
Fonctionnalité de sécurité du produit	voir 2.2.2 Services de sécurité
Exigences de configuration du produit	voir 4.2 Restrictions d'usage
Hypothèses liées à l'environnement d'exploitation	voir 4.2 Restrictions d'usage
Développeurs	**THALES DIS France SAS** 6, rue de la Verrerie, 92197 Meudon cedex, France **SAMSUNG ELECTRONICS CO.** 17 Floor, B-Tower, DSR building, Samsungjeonja-ro 1-1, Hwaseong-si, Gyenonggi-do 445-330 South Korea
Commanditaire	**THALES DIS France SAS** 6, rue de la Verrerie, 92197 Meudon cedex, 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

2 Le produit

2.1 Présentation du produit

Le produit évalué est « MultiApp v4.1 Javacard Platform, version 4.1.0.4 » développé par THALES DIS France SAS.

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. Les logiciels applicatifs ne sont pas inclus dans le périmètre de l'évaluation mais ont été pris en compte au titre de [OPEN].

2.2 Description du produit

2.2.1 *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].

2.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit 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* ;
- la suppression d'applications sous le contrôle du *Card Manager* ;
- le *secure channel* PACE conforme aux protocoles de *Global Platform* et de PACE ;
- le support cryptographique (librairies THALES DIS FRANCE SAS) ;
- 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.
- 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] « L'extradition » permet à plusieurs applications de partager un domaine de sécurité dédié.

2.2.3 *Architecture*

Le produit est une carte à puce en mode double contact/sans contact, avec un système d'exploitation JavaCard permettant l'installation d'applications *post-issuance*. Il est constitué des éléments suivants :

- le microcontrôleur S3FT9MH offrant les fonctionnalités matérielles (gestion de la mémoire et gestion des entrées/sorties) ;
- une partie native composée des éléments suivants :
  - un gestionnaire de mémoire *Memory Management* ;
  - un gestionnaire de communication *Communication* ;
  - des librairies cryptographiques propriétaires (Crypto Libs),
- un système développé selon les standards *Java Card 3.0.4* et *Global Platform 2.3* (avec *Id configuration version 1.0* and *Mapping Guidelines version 1.0*) qui permet la prise en charge et l'exécution d'applets JavaCard personnalisées et qui fournit des services d'administration des applets et de la carte à puce.

L'architecture détaillée du produit est décrite en section 2.2 « *Product Architecture* » de la cible de sécurité [ST], les éléments constituants la TOE sont détaillés en section 2.4 « *TOE Description* » de la cible de sécurité [ST], et les éléments exclus de la TOE sont spécifiés en section 2.3 « TOE Boundaries » de la cible de sécurité [ST].

Les applications déjà chargées dans le produit sont toutes identifiées dans le tableau 1, ci-après.

Bien que ces applications standards 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 les guides [AGD-Dev_Basic].

2.2.4 *Identification du produit*

La version certifiée du produit est identifiable par les éléments détaillés dans la cible de sécurité [ST] au chapitre 1.2 « *TOE Reference* ».
Ces éléments peuvent être vérifiés par l'utilisation de la commande GET DATA sur le CPLC ou les « *Gemalto proprietary Card Identity Data* ». La procédure d'identification du produit est décrite au chapitre 1.5 « *Product Identification* » dans le guide [AGD_OPE].

Le produit offre la possibilité de n'embarquer que les 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 du tableau 1 de la cible de sécurité [ST] au chapitre 1.2 « *TOE Reference* ».

La principale différence entre le produit et la TOE (la plateforme) correspond aux applications chargées pré-émission sur ce produit.

Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans le tableau ci-après. Ce tableau liste les applications et les packages inclus dans le produit, associés à leur nom et leur AID[2].

Nom, version de l'application	AID (en hexadécimal)	Nom du *package*
PureJava	A0000000018320A0100000000000000FF	com.gemalto.puredi
eID	A00000003080000000008DB00FF	com.gemalto.javacard.eid
MChipAdvance_DE V74	A0000000180F000001833032	com.gemalto.mchipadv
MPCOS	A00000001830030100000000000000FF	com.gemalto.mpcos
eSign	A00000003080000000008F500FF	com.gemalto.javacard.esign
mocServer	4D4F43415F536572766572	com.gemalto.moc.server
DualPSE_Source	A000000018300701000000000000001FF	com.gemalto.dualPSE
Plug&Play	A00000003080000000006DF00FF	com.gemalto.javacard.mspnp
PUREDI_v3.09	A0000000018320A0100000000000000FF	com.gemalto.pure
VSDC	A00000000310	com.visa.vsdc
ETravel2.3	A0000000018300B02000000000000000FF	eTravel (Virtual Pkg)
IAS V4.4.2	A000000018800000000066240FF	com.gemalto.javacard.iasclassic

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.

[2] *Application Identifier.*

2.2.5 *Cycle de vie*

Le cycle de vie du produit se décompose en quatre étapes (développement, fabrication, personnalisation et utilisation finale). Il est illustré par la figure 6 et décrit au paragraphe 2.5 « *Life-cycle* » de la cible de sécurité [ST].

Les phases 1 à 5 correspondent 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 SAMSUNG ELECTRONICS CO.

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.

Suivant les étapes du cycle de vie, différents guides sont applicables, notamment :

- le guide [AGD-OPE] identifie les recommandations relatives à la livraison des futures applications à charger sur ce produit ;
- les guides [AGD-Dev_Basic] et [AGD-Dev_Sec] décrivent les règles de développement des applications destinées à être chargées dans le produit selon leur niveau de sensibilité ;
- le guide [AGD-OPE_VA] décrit les règles de vérification qui doivent être appliquées par l'autorité de vérification.

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit le responsable de la pré-personnalisation, le responsable de la personnalisation et le gestionnaire chargés de son administration, et comme utilisateurs les développeurs des applications à charger sur la plateforme.

Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

2.2.6 *Configuration évaluée*

Le certificat porte sur la plateforme *Java Card* ouverte identifiée dans le chapitre 1.2.4 « Identification du produit » du présent rapport de certification et supportant toutes les configurations du tableau 1 du même chapitre.

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 4.2 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 présent rapport ont été vérifiées conformément aux contraintes décrites dans [AGD-OPE_VA].

3 L'évaluation

3.1 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 et dispositifs similaires, 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).

3.2 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 « S3FT9MH », 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** ».

3.3 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.

4 La certification

4.1 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 (voir chapitre 1 Résumé).

Le certificat associé à ce rapport, référencé ANSSI-CC-2025/53 a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité de cinq ans à partir de cette date.

4.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 2.2 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 :

- la personnalisation de données confidentielles avec les mécanismes *Global Platform* SCP01 ou SCP02 doit être protégée conformément aux recommandations du guide [AGD-OPE], à savoir :
    - soit elle doit s'effectuer dans un environnement de confiance, c'est-à-dire sur un site implémentant des mesures de sécurité strictes pour sécuriser les installations physiques, l'infrastructure IT, le contrôle d'accès, les équipements et le personnel ;
    - soit les données doivent être chiffrées, en plus du chiffrement fournit par SCP01 et SCP02 ;
- 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 [GUIDES].

4.4 Reconnaissance du certificat

4.4.1 *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[3], 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 :

4.4.2 *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[4] , 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 :

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

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

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *MultiApp V4.1 : JCS Security Target*, référence D1417544, version 1.28, 1er août 2025. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *MultiApp V4.1 : JCS Security Target - public version*, référence D1417544, version 1.28p, 1er août 2025.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report, SUNDANCE-P-R02 Project*, référence SUNDANCE-P-R02_ETR_v1.1, version 1.1, 25 novembre 2025. 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,* SUNDANCE-P-R02_ETR_Lite_v1.1, version 1.1, 25 novembre 2025.
[GUIDES]	Guide d'installation du produit : - *MultiApp V4.1 : AGD_PRE document – Javacard Platform*, référence D1424307, version 1.2, 25 mai 2021. Guide d'administration du produit : - *MultiApp V4.1 : AGD_OPE document – Javacard Platform*, référence D1424308, version 2.2, 12 juillet 2024. Guide d'utilisation du produit : - *MultiApp ID Operating System – Reference manual*, référence D1392687I, 13 avril 2021 ; - *Global Dispatcher Personalization Applet – User Guide*, référence D1390286Q, 3 mai 2021. Guide de développement d'applications basiques [AGD-Dev_Basic] : - *Rules for applications on Multiapp certified product*, référence D1390963, version 1.2, novembre 2017. Guide de développement d'applications sécurisées [AGD-Dev_Sec] : - *Guidance for secure application development on Multiapp platforms*, référence : D1390326, version A05, juillet 2025. Guides pour l'autorité de vérification [AGD-OPE_VA] : - *Verification process of Gemalto non sensitive applet*, référence D1390670, version A01, février 2016 - *Verification process of Third Party non sensitive applet*, référence D1390671, version A01, février 2016.

[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - DISGEN25_ALC_GEN_v1.1 - DISGEN23_CUR_STAR_v1.0 - DISGEN24_ELC_ STAR_v1.0 - DISGEN24_GEM_STAR_v1.0 - DISGEN24_LVG_ STAR_v1.1 - DISGEN23_MDN_STAR_v1.1 - DISGEN23_MGY_STAR_v1.0 - DISGEN23_VFO-CAL_STAR_v1.0 - DISGEN24_PAU_ STAR_v1.0 - DISGEN24_SGP_STAR_v1.0 - DISGEN23_SSN_ SSC_STAR_v1.0 - DISGEN23_TLH_ STAR_v1.0 - DISGEN25_VAN_STAR_v1.0 - DISGEN25- TCZ_STAR_v1.0 - DISGEN24_PAU_ STAR_v1.0
[CER_IC]	Produit *S3FT9MH/S3FT9MV/S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional CE1 Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software (S3FT9MH_20240713)* Certifié par l'ANSSI sous la référence ANSSI-CC-2023/20-R02.
[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]	*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, ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.4.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.2.
[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.