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 surveillance ANSSI-CC-2020/33-S01

MultiApp V4 JavaCard Virtual Machine

(Référence 4.0.1)

Certificat de référence : ANSSI-CC-2020/33

Paris, le 22 avril 2022

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ Ti CERTIFICATION

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

AVERTISSEMENT

La surveillance du produit ne constitue pas en soi une recommandation d'utilisation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit 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

1 Références

[CER]	Rapport de certification ANSSI-CC-2020/33, MultiApp V4 JavaCard Virtual Machine, référence 4.0.1, 28 mai 2020.
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01.
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01.
[R-M01]	Rapport de maintenance ANSSI-CC-2017/76-M01, Plateforme JavaCard MultiApp v4.0.1 – PACE en configuration ouverte masquée sur le composant M7892 G12, 22 mars 2022.
[RS-Lab]	*Surveillance Technical Report*, référence OASIS7_S01_STR_v1.0/v1, 18 mars 2022, SERMA SAFETY & SECURITY.

Note : Le produit objet de la présente surveillance a été initialement développé par la société GEMALTO devenue aujourd'hui THALES DIS FRANCE SAS.

2 Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation SERMA SAFETY & SECURITY, permet d'attester que le produit « MultiApp V4 JavaCard Virtual Machine, référence 4.0.1 », initialement certifié sous la référence [CER], peut être considéré comme résistant à des attaques de niveau AVA_VAN.5 dans les mêmes conditions et restrictions d'usage que celles définies dans [CER], complétées par les recommandations sécuritaires additionnelles intégrées au fil des surveillances successives dans [GUIDES].

Il est à noter que de nouvelles recommandations sécuritaires ont été ajoutées au titre de la présente surveillance. Si ces recommandations ne sont pas mises en œuvre, le produit ne peut pas être considéré comme résistant à des attaques de niveau AVA_VAN.5.

Le rapport de surveillance [RS-Lab] permet également d'attester que le cycle de vie du produit est conforme aux composants de la classe ALC définis dans [CER], complété par la maintenance [R-M01].

La périodicité de la surveillance de ce produit est de 60 mois.

3 Guides applicables

Le tableau ci-dessous liste les guides applicables du produit évalué. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du guide correspondant.

En particulier, [R-S01] référence la présente surveillance.

Les guides contenant de nouvelles recommandations sécuritaires par rapport au certificat initial apparaissent en gras.

[GUIDES]	*MultiApp V4.0.1- AGD_PRE document – Javacard Platform*, référence D1431347, version 1.0, 28 septembre 2017.	[CER]
	***MultiApp V4.0.1 Javacard Platform - AGD_OPE document, référence D1432683*, version 1.3, 2 décembre 2021.**	**[R-S01]**
	MultiApp ID Operating System – Reference manual, référence D1392687, version E, 28 mars 2018.	[CER]
	Rules for applications on Multiapp certified product, référence D1484823, version 1.2, janvier 2019.	[CER]
	Guidance for secure application development on Multiapp platforms, référence D1390326, version A01, mars 2018.	[CER]
	Verification process of Gemalto non sensitive applet. Qualification level, référence D1484874, version 1.0, décembre 2018.	[CER]
	Verification process of Third Party non sensitive applet. Qualification level, référence D1484875, version 1.2, février 2019.	[CER]