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 surveillance ANSSI-CC-2017/76-S01

Plateforme JavaCard MultiApp V4.0.1 - PACE en configuration ouverte masquée sur le composant M7892 G12

Certificat de référence : ANSSI-CC-2017/76

Paris, le 5 mars 2020

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

Guillaume POUPARD
[ORIGINAL SIGNÉ]

SÉCURITÉ CERTIFICATION

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-2017/76, plateforme Plateforme JavaCard MultiApp V4.0.1 - PACE en configuration ouverte masquée sur le composant M7892 G12, 18 décembre 2017.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[RS-Lab]	S01 - Surveillance Technical Report - OASIS-UP, project, référence OASIS-UP_STR_v1.2, version 1.2, 18 février 2020, Serma Safety & Security.
[ETR_COMP]	Pour le besoin des évaluations ou surveillances en composition avec ce produit le rapport technique pour la composition a été mis à jour : S01 - Surveillance Technical Report Lite for Composition - OASIS-UP project, reference OASIS-UP_STR_Lite_v1.1, version 1.1, 18 février 2020, Serma Safety & Security.

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

2. Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation *SERMA SAFETY & SECURITY*, permet d'attester que le produit « Plateforme JavaCard MultiApp V4.0.1 - PACE en configuration ouverte masquée sur le composant M7892 G12 », 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 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 être considéré comme résistant qu'à des attaques de niveau « no rating ».

Le rapport d'évaluation pour composition [ETR_COMP] a été mis à jour pour refléter les résultats de cette dernière surveillance.

La périodicité de la surveillance de ce produit est de 3 ans.

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 à la précédente surveillance apparaissent en gras.

[GUIDES]	MultiApp V4.0.1- AGD_PRE document – Javacard Platform, référence D1431347, version 1.0 du 28 septembre 2017	[CER]
	MultiApp V4.0.1 Javacard Platform - AGD_OPE document, référence D1432683, version 1.2 de février 2020	**[R-S01]**
	MultiApp ID Operating System – Reference manual, référence D1392687E, 28 mars 2018	**[R-S01]**
	Global Dispatcher Personalization Applet – User Guide, référence D1390286D du 30 mai 2017	[CER]
	Rules for applications on Multiapp certified product, référence D1484823, version 1.2 de janvier 2019	**[R-S01]**
	Guidance for secure application development on Multiapp platforms, référence D1390326, version A01 de mars 2018	**[R-S01]**
	Verification process of Gemalto non sensitive applet, référence D1484874, version 1.0 de décembre 2018	[R-S01]
	Verification process of Third Party non sensitive applet, référence D1484875, version 1.2 de février 2019	[R-S01]