



**PREMIÈRE
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-2017/07-S01

Plateforme JAVACARD MultiApp V4.0 en configuration ouverte basée sur l'Operating System JLEP3 masquée sur le composant SLE78CLFX4000PH (M7892 G12)

Certificat de référence : ANSSI-CC-2017/07

Paris, le 06 septembre 2022

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

Guillaume POUPARD

[ORIGINAL SIGNE]



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

La reproduction de ce document sans altération ni coupure est autorisée.

1 Références

[CER]	Rapport de certification ANSSI-CC-2017/07, Plateforme JAVACARD MultiApp V4.0 en configuration ouverte basée sur l'Operating System JLEP3 masquée sur le composant SLE78CLFX4000PH (M7892 G12), 8 mars 2017.
[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-2017/07-M01, Plateforme JAVACARD MultiApp V4.0 en configuration ouverte basée sur l'Operating System JLEP3 masquée sur le composant SLE78CLFX4000PH (M7892 G12), 27 juin 2022.
[RS-Lab]	S01 - Surveillance Technical Report, OASIS Project, référence OASIS_S01_STR_Lite_v1.0 / 1.0, 8 juin 2022, SERMA SAFETY and 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 Project, référence OASIS_S01_STR_v1.0 / 1.0, 8 juin 2022, SERMA SAFETY and SECURITY.

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

2 Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation SERMA SAFETY AND SECURITY, permet d'attester que le produit « Plateforme JAVACARD MultiApp V4.0 en configuration ouverte basée sur l'Operating System JLEP3 masquée sur le composant SLE78CLFX4000PH (M7892 G12) », 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 lors de cette surveillances dans [GUIDES].

Ce résultat est applicable au produit maintenu sous la référence [R-M01].

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

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] et mis à jour par [R-M01].

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 AGD_OPE document - Javacard Platform, référence D1390321, version 1.5, 8 juin 2022, THALES DIS.	[S01]
	Guidance for secure application development on Multiapp platforms, référence : D1390326, version A01, mars 2018, GEMALTO.	[S01]
	<i>MultiApp V4 AGD_PRE document - Javacard Platform, référence D1390316, version 1.1, 9 février 2016, GEMALTO.</i>	[CER]
	MultiApp ID Operating System Reference Manual, référence D1392687E, 28 mars 2018, GEMALTO.	[S01]
	Rules for applications on Multiapp certified product – MAV40, référence D1573972, version 1.0, avril 2022, THALES DIS.	[S01]
	<i>Verification process of Third Party non sensitive applet, référence D1390671, version A01, février 2016, GEMALTO.</i>	[CER]
	<i>Verification process of Gemalto non sensitive applet, référence D1390670, version A01, février 2016, GEMALTO.</i>	[CER]
	RNG Design - Crypto library for MultiAppV40 (DSG_JLEP_RNG_SLE7x(ANSSI).doc x), référence MRDSECNOT1 53046, version 1.0, 2 juillet 2015, GEMALTO.	[S01]