PREMIÈRE
MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

**Secrétariat général de la défense
et de la sécurité nationale**

Rapport de surveillance
ANSSI-CC-2017/22-S01

IAS Classic V4.4 with MOC Server 1.1 on MultiApp V4

Certificat de référence : ANSSI-CC-2017/22

Paris, le 21 octobre 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

1 Références

[CER]	Rapport de certification ANSSI-CC-2017/22, IAS Classic V4.4 with MOC Server 1.1 on MultiApp V4, 16 juin 2017.
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01.
[R-M01]	Rapport de maintenance ANSSI-CC-2017/22-M01, IAS Classic V4.4 with MOC Server 1.1 on MultiApp V4, version de l'application IAS : 4.4.0.A, version de l'application MOC Server : 1.1.1.A, version plateforme Java Card MultiApp : 4.0.
[RS-Lab]	*MINORIS Project : Surveillance Technical Report*, référence MINORIS_S01_STR_V1.0, version 1.0, 22 juin 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.

2 Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation [CESTI], permet d'attester que le produit « IAS Classic V4.4 with MOC Server 1.1 on MultiApp V4 », 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].

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 résistants 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 [R-M01].

La périodicité de la surveillance de ce produit est de 36 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 ID V4 Software AGD document – IAS V4.4 Application*, référence D1388754, version 1.3, 10 juin 2022.**	**[R-S01]**

	***Card Personalization Specification requirement for SSCD security evaluation IAS Classic v4.4*, référence IACv44_001_CPS, version 1.4, 7 janvier 2022.**	**[R-S01]**
	IAS Classic Applet V4.4 Reference Manual, référence D1387713, version J, 26 septembre 2017.	[CER]
	BioPIN Manager V2_Reference Manual, référence D1290692, version C, 26 octobre 2016.	[CER]
	Guidance for secure application development on Multiapp platforms, référence D1390326, version A01, mars 2018.	[CER]
	MultiApp V4 AGD_PRE document – Javacard Platform, référence D1390316, version 1.1, 6 juin 2016.	[CER]
	***MultiApp V4 AGD_OPE document Javacard Platform*, référence D1390321, version 1.5, 8 juin 2022.**	**[R-S01]**
	Verification process of Gemalto non sensitive applet, référence D1390670, version A01, février 2016.	[CER]
	Verification process of Third Party non sensitive applet, référence D1390671, version A01, février 2016.	[CER]
	***Rules for applications on Multiapp certified product – MAV40*, référence D1573972, version 1.0, avril 2022.**	**[R-S01]**