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 maintenance ANSSI-CC-2015/30-M01

Plateforme Java Card MAV31S en configuration ouverte de la carte à puce Optelio Contactless R7S masquée sur le composant P60D144JVA

(Version du patch : 1.6)

Certificat de référence : ANSSI-CC-2015/30

Paris, le 14 octobre 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

1. Références

[CER]	Rapport de certification ANSSI-CC-2015/30, Plateforme Java Card MultiApp ID V3.1S en configuration ouverte de la carte à puce Optelio Contactless R7S masquée sur le composant P60D144JVA, 31 août 2015.
[MAI]	Procédure MAI/P/01 Continuité de l'assurance.
[IAR]	Impact Analysis Report – MultiApp V3.1S Maintenance, 16 juin 2016, référence : D1403708.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, January 8th, 2010, Management Committee.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 2014.

2. Identification du produit maintenu

Le produit maintenu est « Plateforme Java Card MAV31S en configuration ouverte de la carte à puce Optelio Contactless R7S masquée sur le composant P60D144JVA, version du patch 1.6 » développé par *GEMALTO* et *NXP SEMICONDUCTORS*.

Le produit « Plateforme Java Card MultiApp ID V3.1S en configuration ouverte de la carte à puce Optelio Contactless R7S masquée sur le composant P60D144JVA, version du patch 1.4 » a été initialement certifié sous la référence ANSSI-CC-2015/30 (référence [CER]).

La version maintenue du produit est identifiable par la réponse que donne le produit à la commande *GET DATA* pour le tag '01 03'. Les éléments d'identification sont les suivants :

Nom de la famille	Java Card	**B1**
Nom du système d'exploitation	GCX7 Family	**C7**
Numéro du masque	MPH150	**F3**
Version de flux de production	Non pertinent	**xx xx**
Version du patch	Version 1.6	**1605**

La configuration de la TOE est identifiable par la réponse que donne le produit à la commande *GET DATA* pour le tag '9F 7F'. Les éléments d'identification sont les suivants :

Fabriquant du microcontrôleur	*NXP SEMICONDUCTORS*	**4790**
Version du microcontrôleur	P60D144JVA	**6A15**
Nom du fournisseur système d'exploitation	*GEMALTO*	**1981**
Date du système d'exploitation		**3310**
Niveau de release du système d'exploitation	Revision 01 ; release revision 07	**0107**

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que le patch version 1.4 est passé en version 1.6 pour s'adapter à un marché gouvernemental. Cette modification résout des *bugs* fonctionnels :

- sur le protocole sans contact ;
- sur les communications avec un modèle de téléphone particulier ;
- sur le bit de parité de la réponse de la commande du DESELECT à certaines fréquences ;
- sur l'accessibilité à MifarePlus ;
- sur l'attribution de commandes au Desfire OS ;
- sur le support d'UID aléatoire par le système Mifare AntiCollision ;
- de carte muette lors de la validation IASClassic V4 ;
- de carte muette lors du démarrage ;
- sur l'accessibilité des paramètres du domaine de clé ECC en cas d'arrachage de carte.

4. Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables, du produit évalué et sont applicables au produit maintenu. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du document correspondant. En particulier, [R-M01] référence la présente maintenance.

[GUIDES]	MultiApp ID V31S Software – AGD_PRE document – Javacard Platform, référence : D1345062, version 1.0 du 03 décembre 2014, Gemalto.	[CER]
	MultiApp ID V31S Software – AGD_OPE document – Javacard Platform, référence : D1345063, version 1.3 du 18 août 2016, Gemalto.	[R-M01]
	MultiApp ID Operating System – Reference manual, référence : D1203727D du 19 mars 2013, Gemalto.	[CER]
	Guide de développement d'applications : Rules for applications on Multiapp certified product, référence : D1280572, version A00 de décembre 2012, Gemalto.	[CER]
	Guide de développement d'applications sécurisées : Guidance for secure application development on Multiapp platforms, référence : D1280580, version A00 de décembre 2012, Gemalto.	[CER]
	Guide pour l'autorité de vérification : Verification process of Third Party non sensitive applet loaded in POST-issuance, référence : D1322491, version A00 de février 2014, Gemalto.	[CER]
[ST]	Cible de sécurité de référence: - MAV31S Open Platform JCS Security Target, version 1.3, référence : D1334796, Gemalto ; Version publique : - Security Target Lite MAV31S Open Platform JCS, version 1.3p, reference : D1334796, Gemalto.	[R-M01] [R-M01]
[CONF]	Liste de configuration du produit : - LIS: Configuration List for platform on MPH150, référence : D1348672, 18 août 2016, Gemalto. Liste des applications et packages vérifiés [App_list] : - Card Initialisation Specification – MultiApp v3.1 Santander GP (MPH150), référence : D1391811_CIS_MultiAppV31S, version 1.24, 26 juillet 2016, Gemalto.	[R-M01] [R-M01]

5. Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact mineur.
Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée, à la date de certification.

Les évolutions mineures du présent produit ne remettent pas en cause les évaluations menées en composition sur ce produit.

6. Avertissement

Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une réévaluation ou une surveillance de la nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

7. Reconnaissance du certificat

Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, version 2.1, June 2012 ».

Reconnaissance européenne (SOG-IS)

Le certificat initial a été 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[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Reconnaissance internationale critères communs (CCRA)

Le certificat initial a été émis dans les conditions de l'accord du CC RA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.