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-2016/04-M01

Application IAS V4.2.0.B sur la plateforme JavaCard ouverte MultiApp V3.1 masquée sur le composant P60D144PVA

(Version du patch : 1.4)

Certificat de référence : ANSSI-CC-2016/04

Paris, le 20 mai 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

1. Références

[CER]	Application IAS V4.2.0.B sur la plateforme JavaCard ouverte MultiApp V3.1 masquée sur le composant P60D144PVA (version du patch : 1.3), certificat ANSSI-CC-2016/04 du 9 février 2016.
[MAI]	Procédure MAI/P/01 Continuité de l'assurance.
[IAR]	Rapport d'analyse d'impact « IMPACT ANALYSIS Report – MAV3.1 Maintenance », référence D1389791, version 1.1 du 24/04/2016.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, juillet 2014.

2. Identification du produit maintenu

Le produit maintenu est l'« Application IAS V4.2.0.B sur la plateforme JavaCard ouverte MultiApp V3.1 masquée sur le composant P60D144PVA », version du patch 1.4**,** développé par la société *GEMALTO*.

Le produit « Application IAS V4.2.0.B sur la plateforme JavaCard ouverte MultiApp V3.1 masquée sur le composant P60D144PVA », version du patch 1.3 a été initialement certifié sous la référence ANSSI-CC-2016/04 (référence [CER]).

La version maintenue du produit modifié par rapport à [CER] est identifiable par les éléments présents dans la réponse que donne le produit suite à la commande GET DATA (voir GUIDES]).
L'applet IAS est identifiable par les éléments présents dans la réponse que donne le produit suite à la commande GET DATA sur le CPLC :

- pour le tag '**C0**' on obtient la référence de l'applet : **49 41 53 20 43 6C 61 73 73 69 63 20 76 34** (IAS Classic v4) ;
- pour le tag '**C1**' on obtient la version de l'applet : **34 2E 32 2E 30 2E 42** (version 4.2.0.B).

Le rapport d'analyse d'impact de sécurité (référence [IAR]) fourni par *GEMALTO*, mentionne que la modification a été opérée car une même fonction gère deux modules fonctionnels et non sécuritaires qui ont accès à une même variable. Le problème survient lors du lancement de l'un des deux modules qui a pour effet de remettre à zéro la variable alors que l'autre module avait au préalable sauvegardé une valeur. Pour remédier à ce problème, un patch a été développé par *GEMALTO* de manière à ne plus écraser cette variable d'où cette maintenance.

3. Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables, du produit évalué qui 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]	Guide générique : - MultiApp ID V31 Software AGD Document – IAS V42 Application, Référence D1326533, Version 1.0, 8 avril 2014, *GEMALTO*. Guide de personnalisation : - Card Personalization Specification requirement for SSCD security evaluation IAS Classic v4.2, Référence : IACv42_001-CPS_Req_For_CC_Evaluation, Version 1.0 du 27 septembre 2013, *GEMALTO*. Guides d'administration : - BioPIN Manager V2.0 – Reference Manual, Référence : D1290692A, Version du 17 juin 2013, *GEMALTO*. Guides d'administration : - IAS Classic Applet V4.2 – Reference Manual, Référence : D1307695A, 23 octobre 2013, *GEMALTO*.	[CER]
[ST]	Cible de sécurité de référence pour l'évaluation : - MultiApp V31 Delphes31 : IAS EN Core & Extensions Security Target, Référence : D1354681, Version 1.1, avril 2016 *GEMALTO*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target Lite MultiAppV3.1 IAS Classic V4.2 EN + Ext, Référence : D1354681 version 1.1p, avril 2016, *GEMALTO*.	[R-M01]

[CONF]	- LIS-DOC-IAS-DOCUMENT, Référence : D1327264, Version 1.0, 15 avril 2014, *GEMALTO*.	[CER]

4. 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.

5. 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.

6. 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, la République de Corée, la République Tchèque, le Royaume-Uni, la Suède et la Turquie.