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-2014/14-M01

Application IAS V4 sur la plateforme JavaCard ouverte MultiApp V3 masquée sur le composant M7820 A11

(Version du patch : 7.0)

Certificat de référence : ANSSI-CC-2014/14

Paris, le 23 mai 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

1. Références

[CER]	Application IAS V4 sur la plateforme JavaCard ouverte MultiApp V3 masquée sur le composant M7820 A11 (version du patch : 1.5), certificat ANSSI-CC-2014/14 du 7 février 2014.
[MAI]	Procédure MAI/P/01 Continuité de l'assurance.
[IAR]	Rapport d'analyse d'impact « IMPACT ANALYSIS Report – MAV3.0 Maintenance », référence D1361892, version 1.3 du 14/12/2015.
[RM-Lab]	ETR Addendum - CYLLENE3 Project référence CYLLENE3_ETR_ADD_v1.2 / 1.2 du 29 avril 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 la « Application IAS V4 sur la plateforme JavaCard ouverte MultiApp V3 masquée sur le composant M7820 A11 », **version du patch 7.0,** développé par la société *GEMALTO*.

Le produit « Application IAS V4 sur la plateforme JavaCard ouverte MultiApp V3 masquée sur le composant M7820 A11 », v**ersion du patch 1.5** a été initialement certifié sous la référence ANSSI-CC-2014/14 (référence [CER]).

La version maintenue du produit modifié par rapport à [CER] est identifiable en analysant la réponse à la commande GET DATA pour le tag '**01 03**' :

Nom de la famille	Java Card	**B0**
Nom du système d'exploitation	MultiApp ID	**85**
Numéro du masque	G260	**43**
Nom du produit	MultiApp ID V3.0 Combi 160K	**3F**
Configuration du produit	Configuration Plateforme Java Card ouverte + applet IAS activée	**31**
Version du patch	**Version 7.0**	**70**
Fabriquant du microcontrôleur	Infineon	**40 90**
Version du microcontrôleur	SLE78CLX1600P	**71 64**

Le paramètre « **Version du patch** » est égal à **70 au lieu de 15** pour le produit initialement certifié.

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) fourni par *GEMALTO*, mentionne que les modifications suivantes ont été opérées :

- Développement d'un filtre :
  - pour éviter la perte des paramètres de clé et des paramètres de clé invalide si arrachage durant la génération de clé ;
  - pour éviter des entrées invalides lors de la génération de la clé publique ELC ;
  - pour supporter l'octet CLA existant des productions précédentes et être encore conforme à la spécification «Java Card™ application programming interface, version 2.2.2» ;
  - pour corriger un bug lors de la création d'EF.CardAccess avec l'applet *eTravel* en production ;
  - pour garantir la commutation sur le protocole T=1 lorsque la réponse PSS l'indique ;
  - pour garantir une CGT correcte suite à deux caractères consécutifs durant la transmission T=1 ;
- Développement d'un *patch* pour éviter le problème de *padding* dans les lecteurs Pin Pad utilisant *GCR5500 for ZZZS (SLOVENIE*).

Dans le rapport d'analyse d'impact [IAR], il est également mentionné que le cycle de vie du produit (composant d'assurance ALC) est modifié puisque trois nouveaux sites de pré-personnalisation (*GEMALTO*) ont été ajoutés à savoir *VANTAA*, *MONTGOMERY* et *CURITIBA*.

Le CESTI en charge de l'évaluation initiale a émis un rapport d'évaluation partielle (référence [RM-Lab]) pour réévaluer les composants d'assurance ALC impactés par l'évolution du cycle de vie du produit.

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]	Guide générique : - MultiAppID V3 Software – AGD document - IAS V4 Application, Référence : D1290696, Version 1.0 du 9 avril 2013, *GEMALTO.* - Guide de personnalisation (étape 6) : Card Personalization Specification requirement for SSCD security evaluation – IAS Classic v4.0, Référence : IACv4_001_CPS_Req_For_CC_Evaluation, Version 1.5 du 25 janvier 2016, *GEMALTO*. - Guide d'administration (étape 7) : BioPIN Manager V2.0 – Reference Manual, Référence : D1290692A, Version du 17 juin 2013, *GEMALTO.* - Guide d'administration (étape 7) : IAS Classic Applet V4 – reference manual, Référence : D1266704B, Version du 5 avril 2013, *GEMALTO.*	[CER] [R_M01] [CER] [CER]
[ST]	Cible de sécurité de référence pour l'évaluation : - MultiApp V3 Cyllene3 IAS CWA Security Target, Référence : ST_D1261752, Version 1.1 du 8 décembre 2015, *GEMALTO*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - MultiApp V3 IAS CWA Security Target, Référence : ST_D1261752, Version 1.1p du 8 décembre 2015, *GEMALTO.*	[R-M01]
[CONF]	- D1292314-LIS_DOC-IAS-DOCUMENT, Version 1.3 du 8 décembre 2015, *GEMALTO.*	[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, la République de Corée, la République Tchèque, le Royaume-Uni, la Suède et la Turquie.