



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-2015/15-M01**

**Plateforme Java Card en configuration ouverte de
la carte à puce MultiApp v3.1 masquée sur le
composant P60D144PVA**

(Version du patch : 1.4)

Certificat de référence : ANSSI-CC-2015/15

Paris, le 20 mai 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]



1. Références

[CER]	Plateforme Java Card en configuration ouverte de la carte à puce MultiApp v3.1 masquée sur le composant P60D144PVA (version du patch : 1.3), certificat ANSSI-CC-2015/15 du 31 août 2015.
[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 22/04/2016.
[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 la « Plateforme Java Card en configuration ouverte de la carte à puce MultiApp v3.1 masquée sur le composant P60D144PVA », version du patch 1.4, développé par la société *GEMALTO*.

Le produit « Plateforme Java Card en configuration ouverte de la carte à puce MultiApp v3.1 masquée sur le composant P60D144PVA », version du patch 1.3 a été initialement certifié sous la référence ANSSI-CC-2015/15 (référence [CER]).

La version maintenue du produit modifié par rapport à [CER] est identifiable en analysant la réponse à la commande « GET DATA » avec le tag '0103' (identification du produit) :

Nom de la famille	Java Card	B0
Nom du système d'exploitation	MultiApp ID	85
Numéro du masque	MPH149	49
Nom du produit	MultiApp ID v3.1 Combi 144K	45
Configuration du produit	Plateforme Java Card ouverte	11
Version du patch	Version 1.4	14
Fabricant du microcontrôleur	<i>NXP SEMICONDUCTORS</i>	4790
Version du microcontrôleur	P60D144PVA	6A15

Cette nouvelle version contenant le patch version 1.4, apparait au travers de la réponse précédente, paramètre « **Version du patch** » égal à **14 au lieu de 13** dans le produit initialement certifié.

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]	<p>Guide d'installation du produit :</p> <ul style="list-style-type: none"> - MultiApp ID V31 Software - AGD_PRE document - Javacard Platform, référence D1300430, version 1.0 du 19 juillet 2013, <i>GEMALTO</i>. 	[CER]
	<p>Guide d'administration du produit :</p> <ul style="list-style-type: none"> - MultiApp ID V31 Software - AGD_OPE document - Javacard Platform, référence : D1300432, version 1.4 du 20 avril 2016, <i>GEMALTO</i>. <p>Guides d'utilisation du produit :</p> <ul style="list-style-type: none"> - MultiApp ID Operating System - Reference manual, référence : D1203727D, 19 mars 2013, <i>GEMALTO</i>. - Guide de développement d'applications [AGD_Dev_Basic] : Rules for applications on Multiapp certified product, référence : D1280572, version A00 de décembre 2012, <i>GEMALTO</i>. - Guide de développement d'applications sécurisées [AGD-Dev_Sec] : Guidance for secure application development on Multiapp platforms, référence : D1280580, version A00 de décembre 2012, <i>GEMALTO</i>. - Guide pour l'autorité de vérification [AGD_OPE_VA] : Verification process of Third Party non sensitive applet loaded in POST-issuance, référence : D1322491, version A00 de février 2014, <i>GEMALTO</i>. 	<p>[R-M01]</p> <p>[CER]</p> <p>[CER]</p> <p>[CER]</p> <p>[CER]</p>

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - MultiApp V31 Delphes31 : JCS Security Target, référence : D1278582, version 1.2 du 20 avril 2016, <i>GEMALTO</i>. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - Security Target Lite MultiAppV3.1 JCS Platform, Référence : D1278582, version 1.2p d'avril 2016, <i>GEMALTO</i>. 	[R-M01]
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - LIS : Configuration List for platform, Référence : D1350417, Version 1.1, 20 avril 2016, <i>GEMALTO</i>. <p>Liste des applications et packages vérifiés [APP_List]</p> <ul style="list-style-type: none"> - Card Initialisation Specification – MultiApp v3.1 : MPH149 Filter01, Référence : D1350417, Version 3.5, 7 mars 2016, <i>GEMALTO</i>. 	<p>[R-M01]</p> <p>[R-M01]</p>

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'accord¹, 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 signataires², 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.