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-2011/10-M01

Plateforme Java Card en configuration ouverte de la carte à puce MultiApp V2 masquée sur composants de la famille SLE66

Certificat de référence : ANSSI-CC-2011/10

Paris, le 3 juillet 2012

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Références

a) [MAI] Procédure MAI/P/01 Continuité de l'assurance.
b) [ST] Cible de sécurité – MultiApp V2 Cyllene: JCS Security Target, référence : D1132888, version 1.3 du 28/04/2011, Gemalto.
c) [CER] Rapport de certification ANSSI-CC-2011/10 – Plateforme Java Card en configuration ouverte de la carte à puce MultiApp V2 masquée sur composants de la famille SLE66, du 28 avril 2011, ANSSI.
d) [SOG-IS] « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
e) [CC RA] Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, Mai 2000.

Identification du produit maintenu

Le produit maintenu est la plateforme ouverte Java Card du produit « MultiApp v2 » qui est une carte à puce pouvant être en mode contact ou dual. Le produit est développé par la société Gemalto et embarqué sur l'un des microcontrôleurs SLE66CLX360PEM m1588 k11/a15, SLE66CLX360PE m1587 k11/a15, SLE66CLX800PEM m1580 k11/a15, SLE66CLX800PE m1581 k11/a15, SLE66CX800PE m1599 k11/a15, SLE66CLX1440PEM m2090/a13, SLE66CLX1440PE m2091/a13 ou SLE66CX1440PE m2093/a13 fabriqués par la société Infineon Technologies AG.

La plateforme ouverte Java Card est destinée à fournir des services de sécurité aux applets qui seront installées et chargées sur la carte.

D'autres applications, en dehors du périmètre de cette évaluation, sont embarquées dans la ROM du produit, notamment :
- l'application native passeport eTravel EAC ;
- l'applet IAS Classic destinée à faire de la signature électronique.

La version maintenue du produit est identifiable par les éléments présents dans la réponse que donne le produit suite à la commande GET DATA. Ces éléments sont les mêmes que ceux du produit certifié sous la référence [CER]. La commande GET DATA pour le tag 01 03 doit donner la réponse suivante : B0 85 xx yy vv 27 40 90 00 zz uu 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00. La signification des octets est donnée dans le rapport de certification [CER].

Description des évolutions

Deux nouvelles applications sont chargées en EEPROM sur le produit, et restent en dehors du périmètre d'évaluation :
- une application de transport Calypso, développée par la société SpirTech ;
- une application de signature électronique CIE/CNS, développée par Gemalto.

La cible de sécurité ([ST]) du produit maintenu reste la même que celle du produit initial, qui prévoit le chargement d'applets en *post-issuance*.

Le CESTI qui avait réalisé l'évaluation initiale du produit a revu ces nouvelles applications (le code source ainsi que le code compilé lui ont été fournis) et a pu ainsi vérifier la mise en oeuvre des recommandations de la plate-forme. Il confirme que ces nouvelles applications n'ont pas d'impact sur la sécurité du produit certifié.

Les nouvelles applications chargées sur le produit ont les identifiants suivants :

Application	Identifiant	Développeur
Calypso	Calypso_MAV2v1.0	SpirTech
CIE/CNS	CIE/CNS_MAV2v1.0	Gemalto

Fournitures impactées

Les fournitures suivantes ont été mises à jour :

[CONF]	Liste de configuration : - MultiApp V2 Cyllene M1: ALC Configuration List Référence : D1250832 Version 0.5 du 1er février 2012 Gemalto

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.

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 ré-évaluation ou une surveillance de la nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

Reconnaissance du certificat

Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, ref. CCIMB-2004-02-009, version 1.0, February 2004 ».

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 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, Singapour, la Suède et la Turquie.