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-2008/37-M01

Carte Linqus USIM 128K, référence T1004530 B1 / version 1.1 :

Certificat de référence : DCSSI-2008/37

Paris, le 12 mars 2010,

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

Patrick Pailloux
[ORIGINAL SIGNE]

Références

a) Procédure MAI/P/01 Continuité de l'assurance
b) « ASE – Security Target ; TOE: ESIGN PKI signature application on GemXplore Generations G152B-EP3B OS platform, running on Infineon SLE88CFX4002P/m8834b17 chip; Ref T1004530 A3 / Version 1.0; Product: Linqus USIM 128K smartcard ; Based on SSCD Type 3 », référence ASE10448, version 1.4
c) « Rapport de certification DCSSI-2008/37 - Carte Linqus USIM 128K, référence T1004530 A3 / version 1.0 », 3 octobre 2008
d) « Impact Analysis Report - Clock stop issue on GemXplore Generations G152B-EP3B », référence T1004530_RD-IAR_09-0910.1, version 1.0
e) [SOG-IS] « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 2.0, April 1999, Management Committee of Agreement Group.
f) [CC RA] « Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security », May 2000.

Identification du produit maintenu

Le produit maintenu est la « Carte Linqus USIM 128K : composant SLE88CFX4002P/m8834b17 masqué par la plateforme GemXplore Generations G152B-EP3B et embarquant l'application de signature ESIGN, version 1.1 » développée par GEMALTO et Infineon Technologies AG.

Description des évolutions

La modification du produit concerne la gestion du passage en mode basse consommation du composant. Dans certains cas de figure, l'implémentation du produit initialement évalué entraîne l'activation à tort du mutisme de la carte. Ce mutisme est provoqué par un temps de traitement trop long entre l'appel d'une fonction d'émission d'un bloc de données et l'appel d'une fonction demandant au composant de passer en mode basse consommation alors qu'entre temps, l'horloge externe est stoppée. L'utilisation d'une autre fonction d'émission d'un bloc de données pour le dernier bloc à transmettre permet de faire passer automatiquement le composant en mode basse consommation à la fin de l'émission du dernier octet et ceci, avant que l'horloge externe ne soit stoppée. Ce dernier évènement arrivant après que le traitement d'émission soit terminé, le composant ne considère plus qu'il s'agit d'un comportement anormal et n'active plus le mécanisme de mutisme.
Cette correction de la plateforme GemXplore Generations G152B-EP3B est réalisée par un patch en EEPROM du code de l'exécutable de la ROM.

Fournitures impactées

[ST]	« ASE – Security Target ; TOE: ESIGN PKI signature application on GemXplore Generations G152B-EP3B OS platform, running on Infineon SLE88CFX4002P/m8834b17 chip; Ref T1004530 B1 / Version 1.1; Product: Linqus USIM 128K smartcard ; Based on SSCD Type 3 », référence ASE10448, version 1.5
[CONF]	« Bosphore project - List of evaluation documentation », référence BOS_DOC_10448, version 1.5

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.

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

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 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 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 :

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 ».

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, 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.