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-2011/24-M01

NFC FlyBuy v1.1 sur S3FS91J
version du système d'exploitation en natif : 075899
version du Card Manager en Java Card : GOP Ref V1.5.p

Certificat de référence : ANSSI-CC-2011/24

Paris, le 24 octobre 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) [CER] Rapport de certification ANSSI-CC-2011/24 du 12 juillet 2011 ;
c) [IAR] NFC FlyBuy Impact Analysis Report, FQR 110 5805, Issue 3, 2 septembre 2011 ;
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, May 2000.

Identification du produit maintenu

Le produit maintenu est la plateforme (U)SIM Java Card « NFC FlyBuy v1.1 sur S3FS91J », dont la version du système d'exploitation natif est 075899 et la version du *Card Manager*[1] en Java Card est GOP Ref V1.5.p. Cette plateforme est développée par Oberthur Technologies et Samsung Electronics Co. Ltd.

Le produit maintenu est identifiable par les éléments ci-après (ils sont détaillés dans la cible de sécurité [ST] et les [GUIDES]) :

- la version du système d'exploitation natif est « **075899 »** ; cette version peut être lue dans la réponse ATR (*Answer To Reset* – réponse suite à réinitialisation) : « 3B 9F 96 80 3F C7 A0 80 31 E0 73 FE 21 1B 64 **07 58 99** 00 82 90 00 87 » ;
- la version du *Card Manager* est « GOP Ref V1.5.p » ; cette version est obtenue en codage ASCII en réponse à la commande Get Data pour « *Card Manager Release* » (version du Card Manager) : « **47 4F 50 20 52 65 66 20 56 31 2E 35 2E 70** 90 00 ».

Description des évolutions

Oberthur Technologies a modifié le code source du produit NFC FlyBuy dans le but d'implémenter des modifications fonctionnelles.
Ces modifications sont décrites dans le document [IAR].

Fournitures impactées

Les fournitures listées ci-dessous ont été mises à jour :

[ST]	Cibles de sécurité: • Security Target – FLY, reference FQR 110 5322, version 4, Oberthur Technologies ; • Security Target Lite – NFC FlyBuy, reference FQR 110 5730, version 3, Oberthur Technologies.
[CONF]	USIM V3.1 Secure PKI on S3FS91J (OX75) - Configuration List, reference FQR : 110 5685, version 4, Oberthur Technologies.
[GUIDES]	Guide de préparation du produit: • USIM V3.1 Secure PKI on S3FS91x - AGD_PRE – Delivery

[1] *Card Manager* est dénommé ISD (*Issuer Security Domain* – domaine de sécurité de l'émetteur) dans la terminologie GlobalPlatform.

	Acceptance, reference FQR 110 5367, version 3, Oberthur Technologies. Guides d'opération du produit: • USIM V3.1 Secure PKI on S3FS91J - Application Management Guide, reference FQR 110 5570, version 4, Oberthur Technologies.

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.