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-2013/65-M01

Application Mobile MasterCard PayPass V1 - M/Chip 4, version V01.00.04A, sur plateforme NFC FlyBuy Platinum V2 sur composant ST33F1ME

Certificat de référence : ANSSI-CC-2013/65

Paris, le 09 avril 2014

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

[Original signé]

Guillaume Poupard

SÉCURITÉ CERTIFICATION

1. Références

a) [MAI] Procédure MAI/P/01 Continuité de l'assurance.
b) [ST] Security target JUBA, Mobile MasterCard PayPass – M/Chip 4 on NFC FlyBuy Platinum, référence FQR 110 6389, version 1.0, Oberthur Technologies.
c) [CER] Rapport de certification ANSSI-CC-2013/65, Application Mobile MasterCard PayPass V1 - M/Chip 4, version V01.00.04, sur plateforme NFC FlyBuy Platinum V2 sur composant ST33F1ME, 24 décembre 2013, ANSSI.
d) [IAR] JUBA Impact Analysis Report Sharedpin Package Removal, FQR 110 6975, Issue 2, 27 mars 2014, Oberthur Technologies.
e) [SUR_PLATF] Rapport de surveillance ANSSI-CC-2012/39-S01, NFC FLYBUY PLATINUM V2 sur composant ST33F1ME, 1 avril 2014, ANSSI.
f) [SOG-IS] « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee.
g) [CC RA] Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, may 2000.

2. Identification du produit maintenu

Le produit maintenu est « Application Mobile Mastercard PayPass V1 – M/Chip 4, version V01.00.04A sur plateforme NFC FlyBuy Platinum V2 sur composant ST33F1ME » développé par Oberthur Technologies et STMicroelectronics.

Le produit « Application Mobile MasterCard PayPass V1 – M/Chip 4, version V01.00.04, sur plateforme NFC FlyBuy Platinum V2 sur composant ST33F1ME » a été initialement certifié sous la référence ANSSI-CC-2013/65 (référence c).

La version maintenue du produit est identifiable par les éléments suivants :

Eléments de configuration		**Origine**
Nom de la TOE	Mobile MasterCard PayPass V1 – M/Chip 4 sur plateforme NFC FlyBuy Platinum V2 sur ST33F1ME	Oberthur Technologies
Référence interne de la TOE	MasterCard Mobile PayPass V1 – Version V01.00.04A	
Identification Hardware	0768910	
Applet SAAAAR code	081861	
Identification du *Card Manager*	GOP Ref V1.8.v	
Identification de l'applet	03100514000510000	
Label PVCS pour l'application	MC_MOBILE_AEPMR3_APPLET_V01.00.04_A	
Label PVCS ROM	USIM_V31_NFC_V2_EAL4_CCD2_0768910	
Nom du circuit intégré	ST33F1ME	STMicroelectronics

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence d) mentionne que la modification suivante a été opérée : suppression du package *sharedpin* de l'applet MC Mobile AEPMR3 V01.00.04. En effet, ce mécanisme permettant de partager un code PIN avec d'autres applets externes n'est pas utilisé dans la pratique.

4. Fournitures prises en compte

Suite à la surveillance de la plateforme (référence e), le guide opérationnel suivant a été mis à jour :

[GUIDE]	USIM V3.1 NFC V2 EAL4+ 768K on CCD2 Application Management Guide, reference FQR 110 5887, version 4, Oberthur Technologies.

5. Fournitures impactées

Suite à cette maintenance, les fournitures suivantes ont également été mises à jour depuis le certificat initial :

[CONF]	« Configuration list for AEPMR3 CC no sharedpin applet », reference FQR 110 6993, édition 1, Oberthur Technologies.
[ST]	- « Security target JUBA, Mobile MasterCard PayPass – M/Chip 4 on NFC FlyBuy Platinum V2», reference FQR 110 6389, version 2, Oberthur Technologies ; - « Security target - lite JUBA, Mobile MasterCard PayPass – M/Chip 4 on NFC FlyBuy Platinum V2 », référence FQR 110 6672, version 2, Oberthur Technologies.

6. 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.

7. 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.

8. 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 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.