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-2013/09-M01

Plateforme JavaCard de la carte à puce ID-One Cosmo V7.1-s sur composant ST23YL80C (Standard)

Certificat de référence : ANSSI-CC-2013/09

Paris, le 13/05/2014

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

Guillaume Poupard
[original signé]

SÉCURITÉ CERTIFICATION

1. Références

a) [MAI] Procédure MAI/P/01 Continuité de l'assurance ;
b) [ST] TOUTATIS Security Target, 31 mars 2014, référence FQR 110 6070, version 7, Oberthur Technologies ;
c) [CER] Plateforme JavaCard de la carte à puce ID-One Cosmo V7.1-s sur composant ST23YL80C (Standard), 29 mars 2013, ANSSI-CC-2013/09, ANSSI ;
d) [IAR] Impact analysis report for TOUTATIS, 31 mars 2014, référence FQR 110 6619, version 2, Oberthur Technologies ;
e) [SOG-IS] « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee ;
f) [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 « Plateforme JavaCard de la carte à puce ID-One Cosmo V7.1-s sur composant ST23YL80C (Standard) » développé par les sociétés Oberthur Technologies et ST Microelectronics.

Le produit « Plateforme JavaCard de la carte à puce ID-One Cosmo V7.1-s sur composant ST23YL80C (Standard) » a été initialement certifié sous la référence ANSSI-CC-2013/09 (référence c).

La version maintenue du produit est identifiable par la commande GET DATA pour le tag 'DF 52' qui donne les réponses suivantes :

Identification du microcontrôleur (tag 'DF 52', sous-tag '01')	'0C' : Standard (ST23YL80C)
Identification du masque (tag 'DF 52', sous-tag '03')	'61 01' ID-One Cosmo V7.1
Identification du patch *Generic* (tag 'DF 52', sous-tag '04') (obligatoire)	'07 97 23' Generic r3.0 (version 00)
Identification du patch *SAC* (tag 'DF 52', sous-tag '04') (optionnel)	'07 92 12' SAC r2 (version 02)

La commande GET DATA pour les tags 'DF 66' et 'DF 67' donne les réponses suivantes :

Tag 'DF 66' Version Commerciale du produit	**Tag 'DF 67' Version Interne du produit**
'076651FF 07010000 0000'	'01010F00'

La commande GET DATA pour le tag '9F 7F', donne la réponse suivante :

- *IC Fabricator* : ST Microelectronics '**47 50**' ;
- *IC Type* : ST23YRxxB (où "xx" vaut "80" ou "48") : '**B2 14**' ;
- *Operating System Identifier* : '**82 31**' ;
- *Operating System Release Date* : '**B1 5E**' ;
- *Operating System Release Level* : '**00 75**'.

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence d) mentionne qu'une modification d'une initialisation d'un pointeur pour palier à un bogue fonctionnel a été opérée.

4. Fournitures impactées

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

[CONF]	- TOUTATIS – Configuration List, Référence : FQR 110 6164, version 3 du 09 septembre 2013, Oberthur Technologies.
[GUIDES]	- ID-One Cosmo V7.1 – Pre-Perso Guide, Référence : FQR 110 6027, version 4 du 01 juillet 2013, Oberthur Technologies. - ID-One Cosmo V7.1 – Reference Guide, Référence : FQR 110 6028, version 4 du 01 juillet 2013, Oberthur Technologies.
[ST]	- TOUTATIS – Security Target, Référence : FQR 110 6070, version 7 du 31 mars 2014, Oberthur Technologies. - Cosmo v7.1-s – TOUTATIS – Java Card Open Platform – Public Security Target, Référence : FQR 110 6155, version 2, Oberthur Technologies.

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.

6. 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.

7. 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'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.