



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-2009/49-M01

**Carte à puce ID-One Cosmo V7.0-n en configuration
Basic, avec correctif r8.0 version 01, masquée sur
composant NXP P5CC037 V0A**

Certificat de référence : ANSSI-CC-2009/49

Paris, le 22 octobre 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) [ST_complète] Cible de sécurité de référence - ID-ONE COSMO V7.0 - CLIO SECURITY TARGET For NXP - référence FQR: 110 4635 – révision 3 – 13/11/2009 - Oberthur Technologies.
- c) [ST_compatibilité] Cible de sécurité pour la composition avec les composants – ID-ONE COSMO V7.0 - CLIO SECURITY TARGET COMPATIBILITY For NXP IC - référence FQR: 110 4636 – révision 1 – 10/07/2009 - Oberthur Technologies.
- d) [ST_Lite] Cible de sécurité publique - ID-ONE COSMO V7.0 - CLIO Security Target Lite For NXP P5CC037 - référence FQR: 110 4775 – révision 1 - Oberthur Technologies.
- e) [CER] Rapport de certification ANSSI-CC-2009/49 du 19/11/2009 – Carte à puce ID-One Cosmo V7.0-n en configuration Basic masquée sur composant NXP P5CC037 V0A.
- f) [IAR] Rapport d'analyse d'impact – Impact analysis report for CLIO Project – référence FQR 110 4978 - révision 1 – 22/04/2010 - Oberthur Technologies.
- g) [SOG-IS] Reconnaissance européenne (voir plus loin).
- h) [CC RA] Reconnaissance internationale critères communs (voir plus loin).

Identification du produit maintenu

Le produit maintenu est la carte à puce ID-One Cosmo V7.0-n, plate-forme Java Card ouverte, développée par Oberthur Technologies :

- compatible avec les spécifications de Java Card 2.2.2 et de VISA GlobalPlatform 2.1.1 ;
- masquée sur composant NXP P5CC037 V0A (sans AES) ;
- avec correctif Optional Code r8.0 version 1 identifié par 069778.

Les caractéristiques du produit sont récapitulées dans le tableau ci-après :

Dénomination du produit	Version de la plate-forme Java Card	Identifiant du correctif Optional Code r8.0 version 1	Référence du composant sur lequel le logiciel est masqué	Référence masque identifiant le composant
Basic	7.0-n	069778	P5CC037 V0A	FC10 C6

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version maintenue du produit est identifiable par les éléments présents dans la réponse que donne le produit suite à la commande GET DATA (cf. [GUIDES]).

Ainsi, la commande GET DATA avec le tag DF 52 donne la réponse suivante :

- DF 52 2F 01 01 **C6** 02 02 08 25 03 02 **FC 10** 04 06 **06 97 78 01 EC AD** 05 01 00 06 14 83 00 00 3F 00 00 F9 00 00 00 00 01 00 00 96 00 69 00 00 00 07 01 01.

Dans cette réponse, on lit les éléments d'identification suivants (caractères en gras) :

- le numéro du masque est **FC10 C6** (voir tableau plus haut, colonne « Référence masque identifiant le composant ») ;
- le numéro du correctif Optional Code r8.0 Generic est **069778** en version **01**, sa signature est **ECAD**.

La commande GET DATA pour le tag DF 50 donne la réponse suivante :

- DF 50 14 **00 00 08 83 01 91 42 52 00 3A 1D 82 55 42 11 05 37 30 31 30**.

Dans cette réponse-ci, on lit les éléments d'identification suivants (caractères en gras) :

- **00 00 08 83** indique le numéro du dé ;
- **01** indique le numéro du wafer ;
- **91 42 52 00** indique le numéro du lot ;
- **3A 1D** indique les coordonnées XY du Wafer ;
- **82 55** horodatage ;
- **42** sous indice de la première fonderie ;
- **11 05 37** identifiant du composant (37 correspond à la configuration Basic (P5CC037 V0A)) ;
- **30 31 30** numéro du code ROM.

Description des évolutions

- **Garbage Collector (PR 851)**

Le récupérateur de mémoire (*Garbage Collector*) a été corrigé afin qu'il n'efface plus accidentellement des instances d'objets, ce qui provoquait une erreur fatale (*KillCard*).

- **getLastShort, getShortPart and getShort (PR 894)**

Ces méthodes ont été corrigées pour éviter des valeurs de retour qui étaient parfois erronées en raison d'un mauvais formatage (*Cast*).

- **Absence d'AES (PR 907)**

Le composant P5CC037 ne comportant de coprocesseur AES, son appel a été supprimé du logiciel embarqué sur ce composant.

- **ISO reselect (PR 909)**

La commande propriétaire permettant de passer en mode *ISO reselect* a été corrigée pour effectivement permettre cette sélection en protocole T=0.

- **SelectingApplet (PR 925)**

Le logiciel a été corrigé afin que la méthode *SelectingApplet*, dans le cas d'une nouvelle sélection d'applet en mode ISO, ne renvoie plus un statut d'erreur.

- **Référence de KillCard (PR 1001)**

Le logiciel a été corrigé de façon à remonter systématiquement la référence de l'évènement ayant provoqué le *KillCard* (erreur fatale de la carte).

- **Card Reset (PR 1002)**

Le logiciel a été corrigé de façon à ce que certains évènements sécuritaires, jugés de moindre gravité, provoquent un *Card Reset* (réinitialisation de la carte) au lieu de *KillCard* (erreur fatale de la carte).

- **Cipher.DoFinal (PR 1003)**

Le logiciel a été corrigé afin d'éviter un code d'erreur 6F8D qui était parfois renvoyé après l'exécution de *Cipher.DoFinal*, en mode 3DES 3 clés ou AES 192, due à un mauvais calcul d'adresse. Cette erreur dépendait de l'adresse de location des clés en mémoire EEPROM.

Fournitures impactées

[CONF]	CLIO Configuration List P5CxYYY – référence FQR 110 4628 – révision 5 - Oberthur Technologies
[GUIDES]	Guide d'installation du produit : - Optional Code r8.0 Generic on ID-One Cosmo V7.0-n Platform - Product Generation Description – référence 069778 00 PGD AA - Oberthur Technologies Guide d'administration du produit : - ID-One Cosmo V7.0 - Pre-Perso Guide – référence FQR 110 4379 – révision 7 - Oberthur Technologies - ID-One Cosmo V7.0 - Security recommendations – référence FQR 110 4730 – révision 2 - Oberthur Technologies - ID-One Cosmo V7.0 - Reference Guide – référence FQR 110 4483 – révision 6 - Oberthur Technologies
[ST]	Cible de sécurité complète: - ID-One Cosmo V7.0 - CLIO Security Target For P5CC037 - référence FQR 110 4677 - révision 3 - Oberthur Technologies Cible de sécurité publique: - ID-One Cosmo V7.0 - CLIO Security Target Lite For NXP P5CC037 – référence FQR 110 4775 – révision 2 - 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 1999 permet la reconnaissance, par les pays signataires de l'accord¹, 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 signataires², 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'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.