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-2007/02-M02

Carte IDOneClassIC : ID-One Cosmo 64 RSA v5.4.1 embarquant l'application ID One CIE v1.01.1 masquée sur composant P5CT072VOP P5CC072VOP et P5CD072VOP

Certificat de référence: 2007/02

Paris, le 19 mai 2010

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

Le vice-amiral Michel BENEDITTINI
[ORIGINAL SIGNE]

Références

a) Procédure MAI/P/01 Continuité de l'assurance.
b) IDOneClassIC CARD Security Target, réf. FQR 110 3517, édition 4, 16/01/07.
c) IDOneClassIC CARD Public Security Target, réf. 110 36 45, version 1.0, 16/01/07.
d) Rapport de certification 2007/02 - Carte IDOneClassIC : composant P5CT072VOP masqué par ID-One Cosmo 64 RSA v5.4 et embarquant l'application IDOneClassIC v1.0, 29 janvier 2007, ANSSI.
e) Rapport de maintenance M-2007/04, 23 avril 2007, ANSSI.
f) ID One CIE, Impact Analysis Report on Anterak, édition 1, réference FQR 110 4126, 28/08/2008.

Identification du produit maintenu

Le produit maintenu est la carte IDOneClassIC : ID-One Cosmo 64 RSA v5.4.1 embarquant l'application ID One CIE v1.01.1 masquée sur les composant P5CT072VOP, P5CC072VOP et P5CD072VOP, développée par Oberthur Card Systems et Philips Semiconductors GmbH.

Le produit est un appareil de création de signature sécurisée (SSCD) constitué par:
- le microcircuit sous-jacent ;
- le système d'exploitation embarquant une machine virtuelle Java (JVM) ;
- l'application SSCD.

Le code source final de l'application ID One CIE v1.01.1 est identifié par :
- Numéro de projet: P08-004;
- code SAAAR: 068382;
- Chemin PVCS : \IDGov\P08-004 - ID-One CIE SmartCard\06838x - ID-One CIE Java Applet;
- Etiquette PVCS : Liv20080611.

Les sources finales du produit Cosmo v5.4.1 sont identifiées par :
- numéro de projet : P08-004 ;
- code SAAAR : 068431 :
- chemin PVCS : \IDGov\P08-004 - ID-One CIE SmartCard\06843x - ID-One Cosmo V5.4.1 Platform;
- étiquette PVCS : Liv20080613

Sur le produit, l'applet peut être identifiée en envoyant la commande GET DATA avec le tag DF 65, les quatrième et cinquième octets de la réponse sont alors **10 11** correspondant à ID One CIE v1.01.1.

De même, pour identifier la plateforme et le microcircuit, il faut envoyer la commande GET DATA avec le tag DF 52, les troisième et quatrième octets de la réponse sont alors E9 20 correspondant à la plateforme ID One Cosmo V5.4.1, et le neuvième octet identifie le microcircuit de la façon suivante :
- 10 pour P5CC072 ;
- 11 pour P5CT072 ;
- 15 pour P5CD072.

Description des évolutions

Le produit maintenu est celui ayant fait l'objet de la certification en référence d, après application de modifications, réalisées en trois étapes:

- un correctif R3 sur V5.4 ;
- une modification d'applet sur V5.4 ;
- une application masquée sur V5.4.1.

Aucune de ces modifications n'a d'impact sécuritaire sur la TOE (*Target Of Evaluation* – cible d'évaluation).

Les changements sont détaillés dans chacun des trois paragraphes suivants :

- description des évolutions sur l'applet (au paragraphe A) ;
- description des évolutions sur la plateforme (au paragraphe B) ;
- description de l'évolution consistant à étendre les composants utilisés (au paragraphe C).

A. Description des évolutions sur l'applet

Ce paragraphe spécifie les évolutions effectuées sur le code source de l'application ID One Classic v1.0 pour aboutir à l'application ID One CIE V1.01.1

Ces évolutions sont des modifications fonctionnelles. Elles sont décrites ci-après.

1. Exposant de clé RSA

Il est désormais possible de charger l'exposant public avant le modulo.

2. Mise à jour d'un enregistrement avec moins de données

Lors d'une opération de mise à jour d'un enregistrement avec moins de données que la taille de l'enregistrement, le fichier est désormais complété avec des octets à '00'. (Le fonctionnement précédent était de conserver les anciennes données).

3. Mise à jour d'un enregistrement avec plus de données

Lors d'une opération de mise à jour d'un enregistrement avec plus de données que la taille de l'enregistrement, la taille de l'enregistrement est désormais augmentée (en respectant la taille du fichier).

4. Vérification de la structure TLV d'un enregistrement

Lors de l'ajout ou de la modification d'un enregistrement au format TLV, une vérification est désormais ajoutée pour s'assurer de la cohérence entre le champ L (longueur) et la longueur du champ V (Valeur) ; si une incohérence est détectée, le mot d'état 6A85 est renvoyé.

5. Mot d'état de la commande Append Record

Lorsque le terminal envoie une commande pour ajouter un enregistrement de longueur fixe au fichier, si le champ de données est plus grand que la taille nominale de l'enregistrement, l'application renvoie désormais le mot d'état 6700 au lieu de 6A80.

6. Mot d'état de la commande des commandes Read Binary / Read Record

Dans le mode CIE, le mot d'état 6282 est désormais remplacé par 9000 lorsque les données sont moins longues que les données attendues.

7. Verify PIN

Lors de la vérification d'un PIN alphanumérique, une vérification est désormais rajoutée pour s'assurer que P1=0.

8. Reset Retry Counter - AC Change

Pour se conformer à la spécification du client, lorsque le paramètre P1 de la commande Reset Retry Counter est égal à 00 (correspondant au cas des données avec données de vérification et nouvelle référence), seule la condition d'accès Unblock est désormais vérifiée en mode CIE (en revanche, en configuration Classic, les deux conditions d'accès UNBLOCK et CHANGE sont vérifiées).

9. Put Data OCI – BSO SM_3DES_MAC

Lors de la création d'un BSO canal sécurisé pour signature, si le champ "Longueur Minimum" (signifiant la longueur minimum de l'aléa) est mis à '00', il est désormais remplacé par '08'.

10. Paramètre d'installation, octet de configuration

Dans les paramètres d'installation, un octet de configuration est désormais ajouté pour permettre à la carte d'être compatible au mode CIE, CNS ou ID One Classic. Cet octet permet de configurer les fonctions suivantes de façon indépendante :

- CIE : pour activer les fonctionnalités CIE/CNS ;
- RSA CRT : permet l'utilisation de clés RSA en mode CRT ;
- chaînage et RSA 2048 : permet l'utilisation d'APDU chaînée (et donc l'utilisation du RSA 2048) ;
- vérification TLV : vérifie que la structure d'un enregistrement est bien formatée dans le mode TLV – étiquette (*tag)*, longueur, valeur - (commandes append/update) ;
- PIN Numérique : vérifie que le PIN a un format numérique (autrement dit, que ce n'est pas une phrase clé).

11. Get Data DF65

A la suite d'une commande GET DATA, avec le tag DF65, le champ de données renvoyé est désormais :

- la version de l'applet (2 octets) ;
- l'octet de configuration (1 octet) ;
- l'utilisation du CHVMan (1 octet), ou l'AID du CHVMan lorsque celui-ci a été renseigné durant l'installation.

12. Lecture d'un enregistrement au format TLV

Lors de la lecture d'un enregistrement au format TLV, la longueur de la réponse est désormais au maximum L+2 octets (même si la taille de l'enregistrement est supérieur à L+2).

13. Mot d'état renvoyé lors de la sélection d'un fichier désactivé

Lors de la sélection d'un fichier désactivé, le mot d'état renvoyé est désormais 6283 (à la place de 9000).

14. Données Secure Messaging sans SM_ENC et SM_SIG

Lorsque l'octet de CLA indique Secure Messaging, mais que dans le sens (entrée ou sortie) de l'échange de données courant, il n'y a pas de conditions SM ENC & SIG, les données sont désormais mises dans un objet PTO (au lieu de les mettre directement).

15. Optimisations de code

Des optimisations de code ont été ajoutées pour améliorer la rapidité d'exécution et la fiabilité de l'EEPROM:

- WorkingBuffer2[] est désormais un tableau COD temporaire (à la place d'EEPROM) pour améliorer la rapidité d'exécution et la fiabilité de l'EEPROM ;
- les méthodes suivantes ont été ajoutées pour optimiser la taille du code de l'applet :
    - getCurrentDFCheckActivation() ;
    - checkCla_ChainSM().

16. Ajout d'un PIN Biométrique

Pour permettre l'authentification utilisateur par des données biométriques (empreinte des doigts), le TEST BSO PIN a été amendé pour ajouter un "biometric PIN".

Cette fonctionnalité ne fait pas partie du périmètre du produit initialement évalué. Cette fonctionnalité, ajoutée par la suite, n'a pas été évaluée. Aussi n'est-elle pas couverte par cette maintenance de certificat.

17. PR 527

Lors de la commande Append Record sur un fichier linéaire (de taille fixe ou variable), le dernier enregistrement est désormais écrasé.

18. PR 528

La seconde commande READ, consécutive à une commande READ qui était sous canal sécurisé et qui s'est terminée par une erreur, renvoie désormais les données formatées sous canal sécurisé même si cela n'a pas été demandé.

19. Correction PR 605

Il y avait une fuite mémoire après une génération de clé RSA. Ceci pouvait être caractérisé en comparant la taille mémoire indiquée avant et après la création d'une clé RSA suivie immédiatement de sa suppression : à la fin, la taille mémoire était moindre.

20. Correction PR 646

Il y avait une fuite mémoire après une création d'un fichier aboutissant à un échec (pour cause de fichier déjà existant).

21. Modification MA21 : interdiction de la signature en mode sans contact

Si la carte fonctionne en mode sans contact, la commande de calcul d'une signature est désormais interdite (commande PSO_CDS).

22. Modification MA22 : vérification des valeurs AC & SM

Lors de la création/modification d'un objet, la cohérence des conditions AC et SM est désormais vérifiée.

23. Modification MA23 : correction de la commande Change Key Data command et chaînage

Lors de l'utilisation de l'outil de test CNS_CIE, les tests de la commande Change Key Data renvoyaient une erreur avec le mot d'état 6883.

24. Correction PR 688

La commande Update Record Previous sur un fichier cyclique n'était pas compatible avec l'ISO. En effet, elle devrait fonctionner comme un *append record*.

25. Correction PR 689

Une commande Generate Key Pair avec un exposant d'une longueur de 16 bits était rejetée.

26. Correction PR 690

La commande Put Data OCI en mode *update*, avec OCI2 absent, était rejetée.

27. Modification MA27 : Change Key Data, format des données

Conformément à la spécification CIE, les données de la commande Change Key Data, pour une clé RSA, peuvent avoir deux formats :

- la valeur du composant ;
- codée dans un Put Data OCI (<lg> <00> <valeur>).

Comme la carte ne supporte que le 1er format, la seconde méthode devrait être rejetée. Or, ce n'était pas le cas.

28. Modification MA28 : chaînage de la commande Change Key Data

Selon la spécification CIE, la valeur par défaut de l'octet de classe de la commande Change Key Data est 0x90, alors que l'application utilise 0x80 pour le chaînage. En revanche, pour la spécification ID One Classic, la valeur par défaut de l'octet de classe de la commande est 0x80, et 0x90 pour le chaînage (conformément à l'ISO).
L'application ID One CIE V1.0 (avec MA23) était uniquement conforme à la spécification CIE (et donc n'était pas compatible avec ID One Classic).

29. Modification MA29 : *Append/Update* sur des enregistrements de longueur fixe

Suivant les spécifications ISO et CIE, les commandes APPEND et UPDATE RECORD sur un fichier d'enregistrement de taille fixe (linéaire ou cyclique) doit échouer si la longueur des données n'est pas égale à la longueur de l'enregistrement. L'application V1.0 n'échouait pas si la longueur des données était plus petite (la fin de l'enregistrement était alors complétée par 00).

30. Modification MA30 : Read/Update Record par numéro d'enregistrement

Dans la version V1.0 de l'application, lors de la lecture ou de la modification d'un fichier cyclique spécifié par son numéro, il n'y avait pas d'erreur renvoyée si le numéro de l'enregistrement était supérieur au nombre d'enregistrements présents dans le fichier. En fait, la commande comptait en rebouclant.

B. Description des évolutions sur la plateforme

Ce paragraphe décrit les évolutions effectuées sur le code source de la plateforme GOP ID MX 64 (aussi appelée ID-One Cosmo V5.4) pour aboutir à la plateforme ID-One Cosmo V5.4.1.

Ces évolutions sont des modifications fonctionnelles. Elles sont décrites ci-après.

31. Modification MP1 : APIs retirées– applications en ROM

Pour permettre la mise en ROM de l'application "ID-One CIE Java Applet", les fonctionnalités suivantes ont été retirées (problème de capacité en mémoire ROM du composant) :

- package com.oberthurcs.javacard.diffiehellman ;
- package com.oberthurcs.javacard.certificate ;
- package javacard.security.KeyAgreement ;
- package com.oberthurcs.javacard.utilSM ;
- support de la cryptographie Courbes Elliptiques ;
- package com.oberthurcs.javacard.authentic.biometry.optional ;
- package com.oberthurcs.javacard.utilBER_Reader ;
- package com.oberthurcs.javacard.utilhashtable ;
- package com.oberthurcs.javacard.utilLByteArray.

32. Correction PR226

Selon la SRS, un Get Data sur l'étiquette DF50 devrait retourner 16 octets, mais seulement 9 l'étaient.

33. Correction PR370

Suivant la SRS, un Get Data sur l'étiquette DF52 devrait retourner la valeur des symboles LOCK_USB et LOCK_ECDSA, ce qui n'était pas le cas.

34. Correction PR270

Après un appel à genKeyPair(), avec le paramètre ALG_RSA et pour une clé de longueur 2048, la partie privée n'était pas correcte. Lors de l'utilisation de la méthode getExponent() et getModulus() sur la partie privée, 0 était retourné au lieu de 256.

35. Correction PR273

Pour réaliser un calcul RSA SFM, la plateforme appelait toujours la fonction crypto Crypto_RSA_SFM_public(), ce qui correspond à une implémentation non sécurisée du RSA.

36. Correction PR320

Dans le protocole T=1, lorsqu'un APDU cas 1 était envoyé, le paramètre P3 dans le buffer APDU pouvait avoir une valeur différente de 0. La valeur de ce paramètre était celle de la commande précédente.

37. Correction PR464

Lorsque la carte était arrachée pendant l'exécution de Util.ArrayCopyNonAtomic(), l'ATR devenait 3B0269F9 et la carte était bloquée.

38. Correction PR486

Lorsque la carte était arrachée pendant l'exécution de JCSystem.resquestObjectDeletion(), la carte se mettait en fin de vie (« se tuait » dans le jargon carte à puce).

39. Correction PR489

Lorsque la carte était arrachée pendant l'exécution du « ramasse miette », la carte devenait muette.

40. Modification MP2 : correction sur le mécanisme anti-arrachement

Lorsque la carte était arrachée pendant l'écriture, en EEPROM, du résultat d'un calcul de chiffrement DES, l'application était verrouillée.

41. Modification MP3 : modification de l'ATR et des CPLC

L'octet "mask version", dans les octets historiques de l'ATR, était positionné à 2.0.
Les octets "CPLC Rom Identifiers" ont également été mis à jour pour désormais identifier le produit maintenu.

42. Correction PR491

Pendant des tests d'arrachements avec utilisation du mode transactionnel, une carte s'était verrouillée et était devenue muette (ATR = FF FF ...).

43. Correction PR313

Lorsqu'un espace temporaire était alloué en EEPROM (parce que la RAM était pleine), une exception EXCEPTION_INVALID_ACCESS était générée si cette allocation avait lieu pendant une transaction.

44. Correction PR236

Lors d'une opération de chiffrement avec l'algorithme ALG_RSA_NOPAD, l'appel à la méthode update(), avec un message d'entrée de la taille de la clé, puis l'appel à la méthode doFinal(), avec une longueur à 0, générait une exception crypto ILLEGAL_USE.

45. Correction PR231

Lors d'un déchiffrement avec l'algorithme ALG_RSA_PKCS1, lorsque la méthode doFinal() était appelée avec un mauvais message d'entrée (sans octet de *padding* à 00), une exception NULL_POINTER_EXCEPTION était générée (à la place d'une exception ILLEGAL_USE).

46. Modification MP4 : modification de la protection contre l'arrachement

Après les problèmes précédents concernant l'arrachement, le code source a été analysé et d'autres problèmes potentiels ont été trouvés et corrigés.

47. Modification MP5 : modification de la librairie TCL

La librairie TCL a été mise à jour pour être conforme à la spécification ISO 14443.

48. Modification MP6 : modification du WTX de la couche TCL

Pour communiquer en TCL, le SmartMX demande que tous les coprocesseurs crypto soient éteints.
Ainsi, dans la version précédente de la plateforme, lorsqu'elle avait besoin de plus de temps pour finir son opération, et pour éviter que le lecteur n'atteigne la limite de temps d'attente, une trame WTX était automatiquement envoyée au lecteur suite à une interruption *timer*. Cette interruption *timer* attendait la fin des opérations cryptographiques, éteignait les crypto-processeurs, envoyait la trame WTX, et réactivait les crypto-processeurs. Cependant, quand l'interruption éteignait le coprocesseur FameX, les indicateurs CRY et RZero étaient également remis à zéro.
Désormais, par l'intermédiaire de la fonction CRYPTO_setFamexeFlags(), ces indicateurs sont remis à leur valeur initiale.

49. Modification MP7 : attente de la fin d'écriture EEP avant toute exécution de code

Dans le service d'interruption WatchPoint, avant de se rendre dans le code optionnel en EEPROM, la fin d'écriture en EEPROM est désormais attendue pour éviter une collision d'accès à la MMU.

C. Description de l'évolution consistant à étendre les composants utilisés

Ce paragraphe décrit l'ajout d'un nouveau composant.

50. Utilisation du composant NXP P5CD072V0P

La carte IDOneClassIC a été certifiée (référence d) et maintenue (référence e) avec l'applicatif embarqué sur le composant P5CT072VOP et P5CC072VOP. Cette carte existe aussi avec l'applicatif embarqué sur le composant P5CD072VOP.

Ces trois composants sont identiques aux options de configuration près, programmées en fin de production par Philips Semiconductors (définition des interfaces accessibles et des tailles mémoires adressables). Ils sont couverts par le même rapport de certification du BSI, émis le 28 mars 2006 sous la référence BSI-DSZ-CC-0348-2006. D'après le rapport de certification du BSI, les trois composants sont en tous points comparables du point de vue de la sécurité.

La carte IDOneClassIC, dans sa version utilisant ce composant P5CD072VOP, est donc également équivalente du point de vue de la sécurité à la version certifiée.

Cotation des mécanismes cryptographiques et analyse du générateur d'aléas selon le référentiel technique de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée par l'ANSSI conformément à son référentiel technique [REF-CRY] (Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010, voir www.ssi.gouv.fr).

Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] (Cotation de mécanismes cryptographiques – ANTERAK, n° 1111/ANSSI/ACE du 30 avril 2010) et donnent lieu aux conclusions suivantes :

- la génération d'aléa du produit n'est pas conforme au référentiel [REF-CRY] ; cela impacte la génération des clés asymétriques ; toutefois, une mise en œuvre suivant les recommandations mentionnées dans les [GUIDES] du produit peut être reconnue conforme au référentiel [REF-CRY] ;
- le mécanisme de chiffrement symétrique en mode CBC sans valeur initiale n'est pas conforme au référentiel [REF-CRY] ; il y a un risque lié à son utilisation. En particulier, le déterminisme de ce mécanisme ne permet pas de masquer le fait que les mêmes informations sont transmises dans deux messages distincts ;
- de même, un risque est identifié si la fonction de signature est utilisée sans que le résultat de l'opération ne soit vérifié avant son renvoi ; toutefois, une mise en œuvre suivant les recommandations mentionnées dans les [GUIDES] du produit peut être reconnue conforme au référentiel [REF-CRY] ;
- concernant la fonction de signature, le produit délègue le calcul du hachage du message à l'application appelante ; la fonction de hachage utilisée doit satisfaire les exigences du référentiel [REF-CRY] pour lui être conforme.

Fournitures impactées

- fournitures pour l'application :

Type	Documents	Référence d'origine (V1.0)	nouvelle référence (V1.01.1)
[GUIDES]	PGD	066771 00 PGD AA	068382 00 PGD AA
[GUIDES]	Guidance	FQR 110 3558 Ed 1	FQR 110 4134 Ed 2
[CONF]	Configuration List	FQR 110 3580 Ed2	FQR 110 3580 Ed6

- fournitures pour la plateforme :

Type	Documents	Référence d'origine (V5.4)	nouvelle référence (V5.4.1)
[GUIDES]	PGD	064471 00 PGD AB	068431 00 PGD AA
[CONF]	Configuration List	FQR 110 3580 Ed2	FQR 110 3580 Ed6

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)

L'accord de reconnaissance européen du SOG-IS de 2010 (« *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee*) 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 (*Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000*).

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 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.