Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de maintenance M-2007/09

BULL TrustWay PCI 2400 (PCA2 version 76675628-115A S305)

Certificat de référence : DCSSI-2004/34

Paris, le 25 juin 2007

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Références

a) Procédure MAI/P/01 Continuité de l'assurance
b) BULL TrustWay PCI Cryptographic Card Security Target, version 3.2 du 7 octobre 2004, référence D00G008
c) Rapport de certification 2004/34 du 26 novembre 2004, Bull TrustWay PCI 2400(PCA2 version 76675628-115A S302)
d) Continuité d'assurance carte TrustWay PCI version S305 - Rapport d'analyse d'impact, version 1.0 du 2 mars 2007, référence D00P013

Identification du produit maintenu

Le produit maintenu est la **carte cryptographique BULL TrustWay PCI 2400 (PCA2) version 76675628-115A S305** développée par **BULL SAS**.
Le détail de la version maintenue est le suivant :

- référence de la carte : 76675628
- version hardware/firmware : 115A
- version software : S305
- version du profil : IOP_FULL_CRYPTO ; 400 signatures/seconde

Description des évolutions

Il n'y a pas de modification de l'environnement de développement.

Les modifications apportées visent à corriger les 8 anomalies suivantes :

M1 - Les anciennes cartes CP8 TB200 ne pouvaient pas être utilisées pour le rôle d'auditeur.

A la création de la carte utilisée par l'auditeur (carte « auditor »), la cible de sécurité [D00G008] impose que ce dernier soit identifié. Pour ce faire, un numéro d'identification est inscrit dans la carte à puce de l'auditeur lors de sa création. Cette opération était correctement réalisée pour les cartes Gemplus (MPCOS-EMV) mais pas pour les cartes CP8 (TB200).

M2 - Retour en erreur après CC2000_Test sous contrôle de l'administrateur

La fonction CC2000_Test peut être configurée pour être utilisable par l'administrateur (contrôle à chaque demande configuré dans le paramètre flag2 de CC2000_Configuration). Lorsque cette fonction était utilisée, certaines commandes administratives étaient ensuite refusées avec le message d'erreur « Admin in progress ».

M3 – Amélioration de l'écriture en EEPROM

Le nombre d'écritures en EEPROM est limité par la technologie. Le processus d'écriture faisait que des portions de données étaient ré-écrites inutilement. Ce processus a été optimisé afin d'éviter les écritures inutiles.

M4 – Erreur lors de la sauvegarde ou la restauration de certaines clés

La carte présentait un dysfonctionnement lors des opérations de sauvegarde ou de restauration des clés RC4 ou « Generic Secret » lorsque les longueurs de clés n'étaient pas un multiple de 8 octets.

M5 – Erreur lors des changements de mode de sauvegarde des clés

La sauvegarde des clés présentait un dysfonctionnement en cas de modification de procédure d'installation (la carte restait dans l'ancien mode).

M6 – Impossibilité de restaurer le label des clés privées

L'opération de restauration des clés privées ne restaurait pas le label privé (CKA_LABEL pour la partie privée). Le label de la clé privée était donc vide.

M7 - Résolution de cas de blocages du Safepad.

Pendant les phases d'installation et d'authentification, le Safepad se bloquait parfois (gestion du timing) et il fallait alors rebooter la carte cryptographique.

M8 - Problème lors de l'utilisation de la clé privée si la clé publique est détruite.

Le paramètre commun (module) entre la clé privée et la clé publique était détruit lors de la destruction de la clé publique ce qui ne permettait plus d'utiliser la clé privée. Ce paramètre a été rendu indépendant.

Fournitures impactées

- le logiciel
- la documentation de test
- les séquences de tests

[CONF]	Liste de configuration D00P009 version 1.6 du 21 décembre 2004

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.

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.