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-2009/19-M01

ID One™ ePass v2.1 en configuration EAC RSA et ECC sur composants P5CD040V0B, P5CD080V0B, P5CD144V0B

Certificat de référence : ANSSI-2009/19

Paris, le 21 septembre 2010

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Références

a) [MAI] Procédure MAI/P/01 Continuité de l'assurance.
b) [ST] Cible de sécurité – ID One™ ePass v2.1 with EAC configuration RSA & ECC – Public Security Target FQR 110 4642, révision 1 Oberthur Technologies.
c) [CER] Rapport de certification ANSSI-2009/19 du 23 juillet 2009 - ID One™ ePass v2.1 en configuration EAC RSA et ECC sur composants P5CD040V0B, P5CD080V0B, P5CD144V0B.
d) [IAR] Rapport d'analyse d'impact – Impact analysis report for Heimdall project – codop R3.0 & R4.0, référence FQR 110 4841 issue 5 du 16/03/2010, Oberthur Technologies.
e) [TR9303] Doc 9303, Machine Readable Travel Documents, Part3 vol.1 Third Edition – 2008, Machine Readable Official Travel Documents, MRtds with Machine Readable Data Stored in Optical Character Recognition Format
f) [ISO 7816] ISO/IEC 7816-4:2005 Identification cards, Integrated circuit cards, Part 4: Organization, security and commands for interchange.
g) [ISO 1373-6] ISO/IEC CD 10373-6.2, Identification cards - Test methods – Part 6: Proximity cards, 12/12/2008.

Identification du produit maintenu

Le produit maintenu est la carte - ID One™ ePass v2.1 en configuration EAC RSA et ECC. Il est développé par la société Oberthur Technologies et embarqué sur les microcontrôleurs P5CD040V0B, P5CD080V0B, P5CD144V0B développés et fabriqués par la société NXP.

La lecture du fichier EF.TOE avec la commande *ReadBinary* permet d'obtenir les informations d'identification, notamment l'identification du correctif intitulé *Optional Code r3.0 for ePass v2.1* contenant les évolutions objet de ce rapport (cf. **Patch ID**) :

Eléments de configuration	
Nom de la TOE	- ID One™ ePass v2.1 en configuration EAC RSA et ECC sur composants P5CD040V0B, P5CD080V0B, P5CD144V0B
Code ROM ID	04 03 06 95 91
Patch ID	04 03 07 09 4**3 (3** correspondant à Optional Code r**3**.0 for ePass v2.1, cf. plus bas**)**
PP EAC ID	04 01 26
PP BAC ID	04 01 17
Support of EAC/AA /BAC security features	04 01 0X, où X = b1|0|b2|b3 avec b1 = EAC, ici = 1 b2 = AA b3 = BAC, ici = 1 (EAC needs BAC to be activated)
Nom de l'IC / Identification de l'IC	P5CD040 : ATR = 4F 54 49 44 25 94 xx xx xx xx P5CD080 : ATR = 4F 54 49 44 28 94 xx xx xx xx P5CD144 : ATR = 4F 54 49 44 2B 94 xx xx xx xx

Description des évolutions

Les évolutions, décrites ci-après, correspondent au correctif *Optional Code r3.0 for ePass v2.1* qui sera chargé sur le produit maintenu. Ce correctif reprend les modifications apportées dans *Optional Code r1.0 for ePass v2.1* et dans *Optional Code r2.0 for ePass v2.1* qui ont été évaluées lors de la certification [CER].

MRZ sur 3 lignes

La norme [TR9303] a été mise à jour depuis la certification du produit en mai 2009. La nouvelle version inclut la spécification d'un MRZ sur trois lignes, dont le contenu a été modifié par rapport aux versions préliminaires utilisées lors du développement du produit. Afin d'être conforme à ces spécifications et d'éviter une erreur lors du calcul des clés LDS (*Logical Data Structure* – structure logique des données) entraînant une erreur d'authentification, des déplacements (*offsets*) ont été modifiés.

Commande *Readbinary*

Un statut d'erreur (0x6F8C) était systématiquement renvoyé par la commande *ReadBinary* lorsque moins de 4 octets étaient lus. Ce statut n'est désormais renvoyé que s'il y a effectivement moins d'octets disponibles dans la zone de donnée lue que d'octets demandés.

Lecture de données avec Le=0

La lecture d'une donnée avec le paramètre Le=0 (longueur = 256 octets) entraînait une réponse d'une longueur supérieure à 256 octets, y compris dans le mode *short length APDU*, ce qui n'est pas conforme à la norme [ISO 7816]. Désormais, si Le=0, la longueur des données utiles à renvoyer est bornée à 231 (bien inférieure à 256, laissant ainsi la marge pour être complétées, le cas échéant, par les données nécessaires lors d'un dialogue en canal sécurisé).

Fournitures impactées

Les fournitures suivantes ont été mises à jour :

[EAC-ST3]	HEIMDALL – Security Target – EAC, FQR 110 4293 revision 6, Oberthur Technologies
[EAC-ST-PUB3]	ID One™ ePass v2.1 with EAC configuration RSA & ECC configuration – Public Security Target, FQR 110 4642 revision 3, Oberthur Technologies
[STD3]	ePass V2.1 on NXP P5CDXXX, Software Test Description, 069591 01 STD AB, Oberthur Technologies
[STR3]	Optional Code r3.0 For ePass V2.1 – After masking with Codop, Software Test Report, 070943 01 STR AA, Oberthur Technologies
[PGD3]	Optional Code r3.0 For ePass V2.1, Product Generation Description, 070943 00 PGD AA, Oberthur Technologies
[CONF3]	Heimdall – configuration list, FQR 110 4535 revision 3, 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.