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-2016/39-M01

# ID-One ePass Full EAC v2 MRTD en configuration EAC et PACE avec AA masqué sur les composants P60x144PVA/PVE

**Certificat de référence : ANSSI-CC-2016/39**

*Paris, le 3 avril 2017*

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

# 1. Références

| | |
|---|---|
| [CER] | ID-One ePass Full EAC v2 MRTD en configuration EAC et PACE avec AA masqué sur les composants P60x144PVA/PVE, 23/06/2016, ANSSI-CC-2016/39. |
| [MAI] | Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance. |
| [IAR] | MINOS ePass V3 Full EACv2 and OpCode Generic r8.0 – Impact Analysis Report, version 5, 09/12/2016, référence : FQR 110 8242. |
| [SOG-IS] | Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee. |
| [CC RA] | Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014. |

# 2. Identification du produit maintenu

Le produit « ID-One ePass Full EAC v2 MRTD en configuration EAC et PACE avec AA masqué sur les composants P60x144PVA/PVE » a été initialement certifié sous la référence ANSSI-CC-2016/39 (référence [CER]). Il fait l'objet de la présente maintenance.

La version maintenue du produit est identifiable par les éléments suivants :

- nom commercial : ID-One ePass Full EAC V2 ;
- code SAAAAR[1] du code ROM : 080031 ;
- code patch obligatoire : **082458FFF905CCCB2DB3F14012A0245840BEA310081875D3851D6F4DD1923AE450D8A55D4** ;
- code patch optionnel : **082845FF62EF601FB487C51B4D653D85C94DE1BC30A13B71C5C0F457516CDAB27FFB696C4** ;
- code composant (sur 42 octets) : XXXXvvvvXX..XX où vvvv peut valoir :
  - '6A15' pour le composant P60D144PVA ;
  - '6E15' pour le composant P60D144PVE ;
  - '6A20' pour le composant P60C144PVA ;
  - '6E20' pour le composant P60C144PVE.

Il peut être décidé ou non de charger le *patch* optionnel et d'ainsi de disposer ou non de la fonction *Digitally Blurred Image*.

Les codes « SAAAAR et patch » peuvent être vérifiés par une commande GETDATA avec le tag DF66. Le code composant peut être vérifié par une commande GETDATA avec le tag 9F7F comme décrit dans [GUIDES].

[1] S : code site (0 pour la France), AAAA : article sur 4 chiffres, R : *release* ou version du logiciel.

# 3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que des corrections d'anomalies ainsi que les principales modifications fonctionnelles suivantes ont été opérées :

- suppression de restrictions lors de la phase de personnalisation de la carte ;
- ajout de condition d'accès sur les opérations de sélection des fichiers ;
- ajout, aux fichiers, d'un attribut optionnel indiquant que le fichier, une fois écrit, ne peut plus être mis à jour ;
- application automatique de l'attribut présenté précédemment à tous les objets de données qui ne sont pas spécifiques à l'OS ;
- amélioration de la manipulation atomique des objets sensibles ;
- ajout de la possibilité de vérifications basées sur de la biométrie dans le mode sans contact de la même manière qu'elles peuvent être utilisées dans le protocole contact.

# 4. Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables au produit maintenu. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du document correspondant. En particulier, [R-M01] référence la présente maintenance.

| | | |
|---|---|---|
| [GUIDES] | MINOS – MRTD FULL EAC V2 – Guidance Document – PREparative procedures, version 13, 23 novembre 2016, référence : 110 7111, Oberthur Technologies ; | [R-M01] |
| | MINOS – ID-One ePass Full EACv2 MRTD in EAC with PACE configuration – Guidance Document – PREparative procedures, version 4, référence : 110 7928, 23 novembre 2016, Oberthur Technologies. | [R-M01] |
| | MINOS – MRTD full EAC v2 – Guidance Document – OPErational user guidance, version 3, 24 juin 2015, reference 110 7565, Oberthur Technologies. | [CER] |
| [ST] | Cibles de sécurité de référence :<br>- MINOS – ID-One ePass Full EAC v2 in EAC with PACE configuration with AA on NXP P60x144 PVA/PVE – Security Target, version 4, référence : 110 7887, 21 novembre 2016, Oberthur Technologies.<br>Version publique :<br>- ID-One ePass Full EAC v2 MRTD in EAC with PACE configuration with AA on NXP P60x144 PVA/PVE – Public Security Target, version 4, référence : 110 7966, Oberthur Technologies. | [R-M01]<br>[R-M01] |
| [CONF] | MINOS ID-One ePass Full EACv2 MRTD and ID-One eIDL v1.0 Configuration List, version 4, 24 novembre 2016, référence 110 7903, Oberthur Technologies. | [R-M01] |

# 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.

# 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 réévaluation 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 :


[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, la Pologne, le Royaume-Uni et la Suède.

### *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[1], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 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 CCRA 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, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.