



**PREMIÈRE
MINISTRE**

*Liberté
Égalité
Fraternité*

Secrétariat général de la défense
et de la sécurité nationale

Agence nationale de la sécurité
des systèmes d'information

Rapport de maintenance ANSSI-CC-2021/18v2-M01

ChipDoc v3.2 on JCOP 4 P71 in ICAO BAC configuration

(Version 3.2.0.52)

Certificat de référence : ANSSI-CC-2021/18v2

Paris, le 28 septembre 2022

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

Guillaume POUPARD

[ORIGINAL SIGNE]



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 cette nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

1 Références

| | |
|----------|---|
| [CER] | Rapport de certification ANSSI-CC-2021/18v2, ChipDoc v3.1 on JCOP 4 P71 in ICAO BAC configuration (version 3.1.6.52). |
| [MAI] | Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01. |
| [IAR] | <i>ChipDoc v3.2 on JCOP 4 P71 v3.2.0.52 Impact Analysis Report, rev 1.0</i> , 3 juin 2021. |
| [SOG-IS] | <i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0</i> , 8 janvier 2010, Management Committee. |
| [CCRA] | <i>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security</i> , 2 juillet 2014. |

2 Identification du produit maintenu

Le produit objet de la présente maintenance est « ChipDoc v3.2 on JCOP 4 P71 in ICAO BAC configuration, (Version 3.2.0.52) » développé par la société NXP SEMICONDUCTORS.

Le produit a été certifié avec réduction de portée sous la référence ANSSI-CC-2021/18v2 (référence [CER]).

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

- l'*applet* est identifiée en réponse à la commande GET_DATA par les valeurs suivantes :
 - o Nom : 0x43686970446F63 ;
 - o Version : 0x03020052 ;
 - o *Card capabilities*: 0x00036FEF ;
- la plateforme est identifiée en réponse à la commande GET_DATA(IDENTIFY) par les valeurs suivantes :
 - o Patch ID : 0x0000000000000001 ;
 - o ROM ID : 2E5AD88409C9BADB ;
 - o *Platform ID*: 4A335233353130314641394530343030DD0984593B0048EF ou 4A335233353130323336333130343030DCE5C19CFE6D0DCF ;
- la configuration limitée à BAC est reconnue par l'absence des fichiers EF.CardAccess et EF.DG14.

3 Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que les modifications suivantes ont été opérées :

- la correction de *bugs* ;
- l'ajout d'une option de configuration ;
- le retrait d'une commande inutile en phase opérationnelle.

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] | <i>ChipDoc 3.2, User Guide Manual, ref 678510, 22 avril 2021</i> | [R-M01] |
| | <i>ChipDoc 3.2, ICAO Personalization Guide, ref 678610, 23 avril 2021</i> | [R-M01] |
| | <i>ChipDoc 3.2, Crypto Guide, révision 1.0, 29 avril 2021</i> | [R-M01] |
| | <i>ChipDoc V3 Application Note, révision 1.4, 20 juin 2022</i> | [CER] |
| [ST] | <p>Cibles de sécurité de référence: ChipDoc v3.2 on JCOP 4 P71 in ICAO BAC configuration – Security Target, revision 1.2, 13 juillet 2022, NXP.</p> <p>Version publique : ChipDoc v3.2 on JCOP 4 P71 in ICAO BAC configuration – Security Target Lite, revision 1.2, 13 juillet 2022, NXP.</p> | [R-M01] |
| [CONF] | <i>Configuration Item List, CDv3.2_1_04920_ALC_CIL_v2.0, 19 juillet 2022</i> | [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 Reconnaissance du certificat

Reconnaissance européenne (SOG-IS)

Ce certificat est 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'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

¹ La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.



Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires², des certificats Critères Communs.



² La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.