

Common Criteria EAL5+ o Superior

Yo, LICDA. MARIA TERESA PUIGBO, Intérprete Judicial del Juzgado de Primera Instancia, debidamente juramentado para el ejercicio de mis funciones CERTIFICO: Que he procedido a traducir las partes centrales de un documento, escrito originalmente en francés, y cuya versión al español, según mi mejor conocimiento, es el siguiente:

PRIMERO
MINISTRO

Libertad
Igualdad
Fraternidad

Sistema francés de evaluación y certificación de la seguridad de los
Tecnologías de la información

CERTIFICADO ANSSI-CC-2021/19v2

Este certificado está asociado al informe de certificación ANSSI-CC-2021/19v2

ChipDoc v3.1 sobre JCOP 4 P71 en ICAO EAC (1 y 2) con versión
de configuración
RITMO 3.1.6.52

Desarrollador: NXP SEMICONDUCTORS
Patrocinador: NXP SEMICONDUCTORS
Centro de evaluación: THALES/CNES

Criterios comunes versión 3.1, revisión 5

EAL5 Aumentado
(ALC_DVS.2, AVA_VAN.5)

Cumple con los perfiles de protección:

Documento de viaje legible por máquina con <<Aplicación ICAO>> ,
Control de acceso extendido con PACE, versión 1.3.2, BSI-CC-PP-0056-V2-2012-MA-02

Documento de viaje legible por máquina que utiliza el procedimiento de inspección estándar con PACE,
versión 1.0.1, BSI-CC-PP-0068-V2-2011-MA-01

Fecha de validez: 3 de junio de 2026

París, 28 de septiembre de 2022

El Director General de la Agencia Nacional
de seguridad de los sistemas de información

Guillermo POUPARD

[FIRMA ORIGINAL]

En el marco de la CCRA, este certificado está reconocido en el nivel EAL2.

Este certificado se emite de conformidad con el Decreto 2002-535 del 18 de abril de 2002, modificado, relativo a la evaluación y certificación de la seguridad ofrecida por los productos y sistemas de tecnología de la información.

Secretaría General de Defensa y Seguridad Nacional, Agencia Nacional de Seguridad de los Sistemas de Información
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP





El producto, objeto de esta certificación, fue evaluado por THALES/CNES con sede en Francia aplicando la Metodología Común para la Evaluación de la Seguridad de las Tecnologías de la Información, versión 3.1, revisión 5, de conformidad con los Criterios Comunes, versión 3.1, revisión 5.

Este certificado se aplica únicamente a esta versión específica del producto en su configuración evaluada. No puede separarse de su informe de certificación completo. La evaluación se llevó a cabo de conformidad con las disposiciones de la SOG-IS, la CCRA y el régimen francés. Las conclusiones del centro de evaluación, tal y como se establecen en el informe de evaluación técnica, son coherentes con la evidencia aportada.

Este certificado no constituye en sí mismo una recomendación del producto por parte de la Agencia Nacional de Seguridad de los Sistemas de Información y no garantiza que el producto certificado esté completamente libre de vulnerabilidades explotables.



República Dominicana
Procuraduría General de la República
Confirme la validez de este documento ingresando el
código CIS en portal.servicios.pgr.gob.do
Código CIS: 001-5202-5180595-8


Firma autorizada: Jennifer Beron


LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP





Rapport de maintenance ANSSI-CC-2021/19v2-M01

ChipDoc v3.2 on JCOP 4 P71 in ICAO EAC (1&2) with PACE configuration

(Version 3.2.0.52)

Certificat de référence : ANSSI-CC-2021/19v2

Paris, le 28 septembre 2022

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

Guillaume POUPARD

[ORIGINAL SIGNE]





AVERTISSEMENT

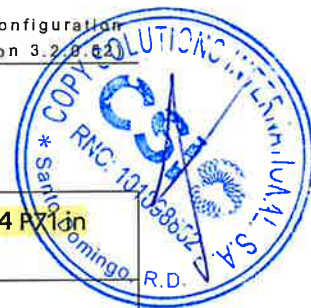
Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une réévaluation ou une surveillance 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-2021/19v2, ChipDoc v3.1 on JCOP 4 P71 in ICAO EAC (1&2) with PACE configuration (version 3.1.6.52).
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01.
[IAR]	ChipDoc v3.2 on JCOP 4 P71 v3.2.0.52 Impact Analysis Report, rev 1.0, 3 juin 2021.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[CCRA]	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 objet de la présente maintenance est « ChipDoc v3.2 on JCOP 4 P71 in ICAO EAC (1&2) with PACE 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-2021/19v2 (référence [CER]).

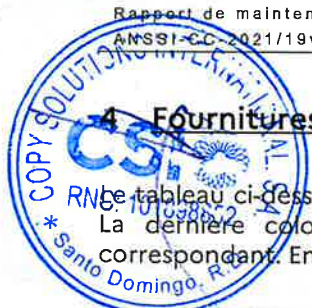
La version maintenue du produit est identifiable par les éléments suivants :

- 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 : 0x00000000000000001 ;
 - o ROM ID : 2E5AD88409C9BADB ;
 - o Platform ID : 4A335233353130314641394530343030DD0984593B0048EF ou 4A335233353130323336333130343030DCE5C19CFE6D0DCF ;
- La configuration EAC avec PACE est reconnue par la présence du fichier EF.CardAccess.

3 Description des évolutions

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

- Correction de *bugs* ;
- Ajout d'une option de configuration ;
- 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</i> , ref 678510, 22 avril 2021	[R-M01]
	<i>ChipDoc 3.2, ICAO Personalization Guide</i> , ref 678610, 23 avril 2021	[R-M01]
	<i>ChipDoc 3.2, Crypto Guide</i> , révision 1.0, 29 avril 2021	[R-M01]
	<i>ChipDoc V3 Application Note</i> , révision 1.4, 20 juin 2022	[CER]
[ST]	Cibles de sécurité de référence: <i>ChipDoc v3.2 on JCOP 4 P71 in ICAO EAC(1&2) with PACE configuration – Security Target, revision 1.2</i>, 13 juillet 2022, NXP. Version publique : <i>ChipDoc v3.2 on JCOP 4 P71 in ICAO EAC(1&2) with PACE configuration – Security Target Lite, revision 1.2</i>, 13 juillet 2022, NXP.	[R-M01]
[CONF]	<i>Configuration Item List, CDv3.2_1_04920_ALC_CIL_v2.0</i> , 19 juillet 2022	[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.