

## Common Criteria EAL5+ o Superior

Yo, **LIC. SANTO C. SIERRA**, 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:

**PRIMER  
MINISTRO**

**Secretaría General de Defensa y Seguridad Nacional**

**Libertad**

**Igualdad**

**Fraternidad**

**Agencia de Seguridad Nacional**

**Sistemas de información**

**Informe de mantenimiento**

**ANSSI-CC-2021/20v2-M01**

**ChipDoc v3.2 en JCOP 4 P71 en configuración SSCD  
(Versión 3.2.0.52)**

**Certificado de referencia: ANSSI-CC-2021/20v2**

**París, 28 de septiembre de 2022**

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

**Guillermo POUPARD**

**[FIRMA ORIGINAL]**



## ADVERTENCIA

El nivel de resistencia de un producto certificado se degrada con el tiempo. Como parte de este mantenimiento no se realizó un análisis de vulnerabilidad de esta versión del producto con respecto a nuevos ataques que han aparecido desde que se emitió el certificado. Sólo una reevaluación o seguimiento de esta nueva versión del producto permitiría mantener el nivel de confianza en el tiempo.



Toda correspondencia relacionada con este informe deberá dirigirse a:

Secretaría General de Defensa y Seguridad Nacional Agencia Nacional de Seguridad  
de los Sistemas de Información  
Centro de certificación 51, boulevard de la Tour Maubourg 75700 París cedex 07 SP

[certificación@ssi.gouv.fr](mailto:certificación@ssi.gouv.fr)

Se autoriza la reproducción de este documento sin alteración ni corte.

## 1 Referencias

|          |                                                                                                                                                                 |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [CER]    | Informe de certificación ANSSI-CC-2021/20v2, ChipDoc v3.1 en JCOP 4 P71 en configuración SSCD (versión 3.1.6.52).                                               |
| [PODER]  | Procedimiento: Continuidad del seguro, referencia ANSSI-CC-MAI-P-01.                                                                                            |
| [Y]      | Informe de análisis de impacto de ChipDoc v3.2 sobre JCOP 4 P71 v3.2.0.52, revisión 1.0, 3 de junio de 2021.                                                    |
| [SOG-ES] | Acuerdo de Reconocimiento Mutuo de Certificados de Evaluación de Seguridad de Tecnologías de la Información, versión 3.0, 8 de enero de 2010, Comité Directivo. |
| [ADRC]   | Acuerdo sobre el reconocimiento de certificados de Criterios Comunes en el ámbito de la seguridad de las tecnologías de la información, 2 de julio de 2014.     |

## 2 Identificación del producto mantenido

El producto sujeto a este mantenimiento es " ChipDoc v3.2 en JCOP 4 P71 en configuración SSCD, (Versión 3.2.0.52)" desarrollado por NXP SEMICONDUCTORS. El producto ha sido certificado con reducción de rango bajo la referencia ANSSI-CC-2021/20v2 (referencia [CER]).

La versión mantenida del producto se identifica mediante los siguientes elementos:

El subprograma se identifica en respuesta al comando GET\_DATA mediante los siguientes valores:

Nombre: 0x43686970446F63;

Versión: 0x03020052;

Capacidades de la tarjeta: 0x00036FEF;

La plataforma se identifica en respuesta al comando GET\_DATA(IDENTIFY) mediante los siguientes valores:

ID del parche: 0x000000000000000001;

Identificación de ROM: 2E5AD88409C9BADB;

Identificación de la plataforma:

4A335233353130314641394530343030DD0984593B0048EF o

4A335233353130323336333130343030DCE5C19CFE6D0DCF;

La configuración SSCD de la aplicación se identifica por la presencia en el archivo EF.DIR de un AID con el prefijo E828D080F.

## 3 Descripción de los desarrollos

El Informe de Análisis de Impacto de Seguridad (IAR) menciona que las modificaciones Se realizaron las siguientes operaciones:

Corrección de errores;

Añadiendo una opción de configuración;

La retirada de un pedido innecesario en la fase operativa.

#### 4 Suministros aplicables

En la siguiente tabla se enumeran los suministros, incluidas las guías aplicables al producto al que se le realiza el mantenimiento. La última columna identifica el origen de la consideración por parte de ANSSI del documento correspondiente. En particular, [R-M01] hace referencia al presente mantenimiento.

|         |                                                                                                                                                               |         |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| [GUIAS] | de ChipDoc 3.2, n.º de pieza 678510, 22 de abril de 2021                                                                                                      | [R-M01] |
|         | ChipDoc 3.2, Guía de personalización de SSCD, ref. 678710, 26 de abril de 2021                                                                                | [R-M01] |
|         | ChipDoc 3.2, Guía de criptografía, revisión 1.0, 29 de abril de 2021                                                                                          | [R-M01] |
|         | de ChipDoc V3, revisión 1.4, 20 de junio de 2022                                                                                                              | [CER]   |
| [CALLE] | Objetivos de seguridad de referencia:<br>ChipDoc v3.2 en JCOP 4 P71 en configuración SSCD -<br>Objetivo de seguridad, revisión 1.2, 13 de julio de 2022, NXP. | [R-M01] |
|         | Versión pública:<br>ChipDoc v3.2 en JCOP 4 P71 en configuración SSCD -<br>Objetivo de seguridad<br>Lite, revisión 1.2, 13 de julio de 2022, NO.               |         |
| [CONF.] | Lista de elementos de configuración,<br>CDv3.2_1_04920_ALC_CIL_v2.0, 19 de julio de 2022                                                                      | [R-M01] |

#### 5 Conclusiones

Se considera que los desarrollos enumerados anteriormente tienen un impacto menor. Por tanto, el nivel de confianza en esta nueva versión del producto es idéntico al de la versión certificada.

#### 6 Reconocimiento del certificado

Reconocimiento europeo (SOG-IS)

Este certificado se emite bajo los términos del Acuerdo SOG-IS [SOG-IS].

El Acuerdo de Reconocimiento Europeo SOG-IS 2010 permite el reconocimiento, por parte de los países firmantes del acuerdo, de los certificados ITSEC y Common Criteria. El reconocimiento europeo se aplica, para tarjetas inteligentes y dispositivos similares, hasta el nivel ITSEC E6 High y CC EAL7 cuando se cumplen las dependencias CC. Los certificados reconocidos bajo este acuerdo se emiten con la siguiente marca:

## Reconocimiento internacional de criterios comunes (CCRA)

Este certificado se emite bajo los términos del Acuerdo CCRA [CCRA].

El acuerdo « Acuerdo de reconocimiento de criterios comunes » permite el reconocimiento, por parte de los países firmantes, de los certificados Criterios comunes.



Traducido a petición de la parte interesada y registrada en mi protocolo. En Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los dieciocho (18) del mes de Febrero del año Dos Mil Veinticinco (2025).



República Dominicana  
Procuraduría General de la República  
Confirme la validez de este documento ingresando el  
código CIS en [portal.servicios.pgr.gob.do](http://portal.servicios.pgr.gob.do)  
Código CIS: 001-5202-2728220-3

*Jenifer Barrera*  
Firma autorizada: Jenifer Barrera



*Lic. Santo C. Sierra*  
**LIC. SANTO C. SIERRA**  
INTERPRETE JUDICIAL  
HELP





## Rapport de maintenance ANSSI-CC-2021/20v2-M01

### ChipDoc v3.2 on JCOP 4 P71 in SSCD configuration (Version 3.2.0.52)

Certificat de référence : ANSSI-CC-2021/20v2

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](mailto:certification@ssi.gouv.fr)

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



## 1 Références

|          |                                                                                                                                             |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------|
| [CER]    | Rapport de certification ANSSI-CC-2021/20v2, ChipDoc v3.1 on JCOP 4 P71 in SSCD 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 SSCD 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-2021/20v2 (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 SSCD de l'application est identifiée par la présence dans le fichier EF.DIR d'un AID au préfixe E828D080F.

## 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, SSCD Personalization Guide, ref 678710, 26 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]     | Cibles de sécurité de référence:<br>ChipDoc v3.2 on JCOP 4 P71 in SSCD configuration – Security Target, révision 1.2, 13 juillet 2022, NXP.<br><br>Version publique :<br>ChipDoc v3.2 on JCOP 4 P71 in SSCD configuration – Security Target Lite, révision 1.2, 13 juillet 2022, NXP. | [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'accord<sup>1</sup>, 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 :

<sup>1</sup> La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : [www.sogis.eu](http://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 signataires<sup>2</sup>, des certificats Critères Communs.



<sup>2</sup> La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org).