PREMIER 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 certification ANSSI-CC-2021/20-R01

ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration (Version 3.1.6.52)

Paris, le 12 Février 2025

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

Vincent STRUBEL

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

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

PREFACE

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- Les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.cyber.gouv.fr.

TABLE DES MATIERES

1 Résumé 5
2 Le produit 7
2.1 Présentation du produit 7
2.2 Description du produit 7
2.2.1 Introduction 7
2.2.2 Services de sécurité 7
2.2.3 Architecture 7
2.2.4 Identification du produit 8
2.2.5 Cycle de vie 8
2.2.6 Configuration évaluée 8
3 L'évaluation 9
3.1 Référentiels d'évaluation 9
3.2 Travaux d'évaluation 9
3.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI 10
3.4 Analyse du générateur d'aléa 10
4 La certification 11
4.1 Conclusion 11
4.2 Restrictions d'usage 11
4.3 Reconnaissance du certificat 12
4.3.1 Reconnaissance européenne (SOG-IS) 12
4.3.2 Reconnaissance internationale critères communs (CCRA) 12
ANNEXE A. Références documentaires du produit évalué 13
ANNEXE B. Références liées à la certification 15

1 Résumé

Référence du rapport de certification **ANSSI-CC-2021/20-R01**
Nom du produit **ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration**
Référence/version du produit **Version 3.1.6.52**
Type de produit **Cartes à puce et dispositifs similaires**
Conformité à un profil de protection ***Protection profiles for secure signature creation device:*** *Part 2 : Device with key generation, v2.0.1, BSI-CC-PP-0059-2009-MA-02 ;* *Part 3 : Device with key import, v1.0.2, BSI-CC-PP-0075-2012-MA-01 ;* *Part 4 : Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, BSI-CC-PP-0071-2012-MA-01 ;* *Part 5 : Extension for device with key generation and trusted communication with signature creation application, v1.0.1, BSI-CC-PP-0072-2012-MA-01 ;* *Part 6 : Extension for device with key import and trusted communication with signature creation application, v1.0.4, BSI-CC-PP-0076-2013-MA-01.*
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL5 augmenté** ALC_DVS.2, AVA_VAN.5
Référence du rapport d'évaluation *Evaluation Technical Report ChipDoc v3.1 in SSCD Reevaluation*, référence CDv3.1_SSCD_ETR_RE, version 1.0, 11 décembre 2024.
Fonctionnalité de sécurité du produit Cf. 2.2.2 Services de sécurité
Exigences de configuration du produit Cf. 4.2 Restrictions d'usage
Hypothèses liées à l'environnement d'exploitation Cf. 4.2 Restrictions d'usage
Développeur **NXP SEMICONDUCTORS GERMANY GMBH** Beiersdorfstrasse 12 22529 Hamburg, Germany
Commanditaire **NXP SEMICONDUCTORS GERMANY GMBH** Beiersdorfstrasse 12

22529 Hamburg, Germany
Centre d'évaluation **THALES / CNES** 290 allée du Lac, 31670 Labège, France
Accords de reconnaissance applicables CCRA SOG-IS Ce certificat est reconnu au niveau EAL2.

2 Le produit

2.1 Présentation du produit

Le produit évalué est « ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration, Version 3.1.6.52 » développé par NXP SEMICONDUCTORS GERMANY GMBH.

Ce produit offre des services d'authentification et de signature électronique (*SSCD* : *Secure Signature Creation Device*). Il est embarqué sur la plateforme *Java Card* [CER_PLA] préalablement certifiée (voir [CER_PLA]) qui est laissée ouverte après personnalisation. Il dispose d'interfaces avec et/ou sans contact.

2.2 Description du produit

2.2.1 *Introduction*

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est conforme aux profils de protection [PP-SSCD-Part2], [PP-SSCD-Part3], [PP-SSCD-Part4], [PP-SSCD-Part5], [PP-SSCD-Part6].

2.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont décrits à la section 1.3.2 « *TOE as Secure Signature Creation Device* » de la cible de sécurité [ST].

2.2.3 *Architecture*

L'architecture du produit est décrite dans la cible de sécurité à la section 1.2 « *TOE Overview* » avec un dessin d'architecture du produit et à la section 1.3 « *TOE Description* ».

2.2.4 *Identification du produit*

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

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

- L'applet est identifiée en réponse à la commande GET_DATA par les données suivantes :
  - Nom de l'*applet* : 43 68 69 70 44 6F 63 (Chipdoc)
  - Version de l'*applet* : 03 01 06 52 (3.1.6.52)
  - *Applet capabilities* : 00 03 6f EF
- La plateforme est identifiée en réponse à la commande GET_DATA (IDENTIFY) par les données suivantes :
  - Pour la plateforme *JCOP 4 P71 v4.7 R1.00.4* : 4A335233353130314641394530343030DD0984593B0048EF
  - Pour la plateforme *JCOP 4 P71 v4.7 R1.01.4* : 4A335233353130323336333130343030DCE5C19CFE6D0DCF
  - Pour la plateforme *JCOP 4 P71 v4.7 R1.02.4 :* 4A335233353130334230314230343030CD217757309F8450

Le circuit intégré sur lequel la plateforme JCOP 4 P71 fonctionne est le microcontrôleur « *NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4)* » certifié [CER_IC].

2.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit à la section 1.3.3 « *TOE Life Cycle* » de la cible de sécurité [ST].

2.2.6 *Configuration évaluée*

Le certificat porte sur la configuration SSCD du produit.

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

Aucune autre application autre que ChipDoc v3.1 connue n'est chargée par défaut sur le produit.

3 L'évaluation

3.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

3.2 Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel sur la plateforme déjà certifiée par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme « *JCOP 4 P71*», voir [CER_PLA].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

3.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [ANA_CRY].

Cette analyse a identifié des non-conformités par rapport aux référentiels [ANSSI Crypto] et [SOG-IS Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme aux référentiels [ANSSI Crypto] et [SOG-IS Crypto], pour les mécanismes cryptographiques qui le permettent.

3.4 Analyse du générateur d'aléa

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur [CER_IC] et de la plateforme [CER_PLA]. Comme requis dans les référentiels [ANSSI Crypto] et [SOG-IS Crypto], la sortie du générateur physique d'aléa subit un retraitement de nature cryptographique.

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

4 La certification

4.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé (Cf § 1 Résumé).

Le certificat associé à ce rapport, référencé ANSSI-CC-2021/20-R01, a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité de cinq ans à partir de cette date.

4.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 2.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

4.3 Reconnaissance du certificat

4.3.1 *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[1], 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 :

4.3.2 *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[2] , 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] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

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

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration Security Target*, référence CDv3.1_3_41039_ST_CDv3.1_SSCD, version 3.9, 2 décembre 2024. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration Security Target Lite*, référence CDv3.1_2_41339_STLite_CDv3.1_SSCD, version 3.9, 2 décembre 2024.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report ChipDoc v3.1 SSCD Reevaluation*, référence CDv3.1_SSCD_ETR_RE, version 1.0, 11 décembre 2024.
[ANA_CRY]	*Analysis of Cryptographic Mechanisms ChipDoc v3.1 Reevaluation*, référence CDV3.1_RE_CRY_SSCD, version 1.0, 4 décembre 2024.
[CONF]	Liste de configuration du produit : - *Configuration Item List*, référence CDv3.3_2_04922_ALC_CIL_v2.2, version 2.2, 3 décembre 2024.
[GUIDES]	- *ChipDoc 3.1 User Guide Manual*, version 3.0, 17 août 2020. - *ChipDoc 3.1 SSCD Personalization Guide*, référence 519124, version 2.4, 2 décembre 2024. - *ChipDoc 3.1 Crypto Guide,* référence CDv3.1_2_03210_ChipDoc3.1_Crypto_Guide, version 1.0, 4 décembre 2020. - *ChipDoc V3 ChipDoc V3 Application Note, référence 635916, version 1.6, 2 décembre 2024.*
[SITES]	Les sites intervenants dans le cycle de vie du produit sont identifiés dans les rapports de certification du produit [CER_IC] et du produit [CER_PLA]. L'applet a été principalement développée sur les sites NXP de Gratkorn et d'East Kilbride Glasgow.
[CER_PLA]	Produit JCOP 4 P71 Certifié par le NSCIB sous la référence NSCIB-CC-2300172-01 le 4 avril 2024.
[CER_IC]	Produit NXP *Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4)* Certifié par le BSI sous la référence BSI-DSZ-CC-1136-V4-2024 le 5 mars 2024.

[PP-SSCD-Part2]	*Protection profiles for secure signature creation device – Part 2: Device with key generation*, référence : prEN 419211-2:2013, version 2.0.1 datée du 18 mai 2013. Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 30 juin 2016 sous la référence BSI-CC-PP-0059-2009-MA-02.
[PP-SSCD-Part3]	*Protection profiles for secure signature creation device – Part 3: Device with key import*, référence : prEN 419211-3:2013, version 1.0.2 datée du 14 septembre 2013. Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 30 juin 2016 sous la référence BSI-CC-PP-0075-2012-MA-01.
[PP-SSCD-Part4]	*Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, référence : prEN 419211-4:2013, version 1.0.1 datée du 12 octobre 2013.* *Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 30 juin 2016 sous la référence BSI-CC-PP-0071-2012-MA-01.*
[PP-SSCD-Part5]	*Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application*, référence : prEN 419211-5:2013, version 1.0.1 datée du 12 octobre 2013. Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 30 juin 2016 sous la référence BSI-CC-PP-0072-2012-MA-01.
[PP-SSCD-Part6]	*Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application*, référence : prEN 419211-6:2014, version 1.0.4 datée du 25 juillet 2014. Maintenu par le BSI le 30 juin 2016 sous la référence BSI-CC-PP-0076-2013-MA-01.

ANNEXE B. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER-P-01]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1 : Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - *Part 2 : Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - *Part 3 : Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	*Mandatory Technical Document – The Application of CC to Integrated Circuits*, version 3.0, février 2009.
[JIWG AP] *	*Mandatory Technical Document – Application of attack potential to smartcards and similar devices*, version 3.2.1, février 2024.
[COMP] *	*Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version 1.5.1, mai 2018.
[OPEN]	*Certification of « Open » smart card products*, version 1.1 (*for trial use*), version 2.0, mai 2024.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, version 3.0, 8 janvier 2010, Management Committee.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.

[SOG-IS Crypto]	*SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms*, version 1.3, février 2023.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.