PREMIÈRE
MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense
et de la sécurité nationale

Rapport de certification
ANSSI-CC-2021/20v2

ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration (v3.1.6.52)

Paris, le 28 septembre 2022

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

Guillaume POUPARD

[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

Référence du rapport de certification

ANSSI-CC-2021/20v2

Nom du produit

ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration

Référence/version du produit

v3.1.6.52

Conformité à un profil de protection

Protection profiles for secure signature creation device
Part 2 : Device with key generation, v2.0.1, certifié BSI-CC-PP-0059-2009-MA-01
Part 3 : Device with key import, v1.0.2, certifié BSI-CC-PP-0075-2012
Part 4 : Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, certifié BSI-CC-PP-0071-2012
Part 5 : Extension for device with key generation and trusted communication with signature creation application, v1.0.1, certifié BSI-CC-PP-0072-2012
Part 6 : Extension for device with key import and trusted communication with signature creation application, v1.0.4, certifié BSI-CC-PP-0076-2013

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur

NXP SEMICONDUCTORS
Troplowitzstrasse 20,
22529 Hamburg, Allemagne

Commanditaire

NXP SEMICONDUCTORS
Troplowitzstrasse 20,
22529 Hamburg, Allemagne

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.

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 ou systèmes 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.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration, v3.1.6.52 » développé par NXP SEMICONDUCTORS.

Ce produit offre des services d'authentification et de signature électronique (SSCD) conformes à la directive [1999/93/EC]. Il est embarqué sur la plateforme JCOP préalablement certifiée [CER_PLA] qui est laissée ouverte après personnalisation. Il dispose d'interfaces avec et/ou sans contact.

1.2 Description du produit

1.2.1 *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 au profil de protection [PP-SSCD-Part2], [PP-SSCD-Part3], [PP-SSCD-Part4], [PP-SSCD-Part5] et [PP-SSCD-Part6].

Dans le cadre particulier de cette certification, qui correspond à une évaluation avec réduction de portée (voir [NOTE25]), la cible de sécurité identifie clairement les évolutions du périmètre d'évaluation par rapport à celui de la certification initiale (voir [CER]). Ici, la réduction de portée correspond au retrait du périmètre d'évaluation de certaines tailles de clefs pour la fonctionnalité « PACE-PIN », voir la note ajoutée à FCS_CKM.1/DH_PACE.

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- la génération ou l'import de donnée de création de signature (SCD) et les données de vérification de signature correspondante (SVD) ;
- l'export des SVD pour la certification à travers un canal de confiance vers l'autorité de certification (CGA) dans le cas où les SVD ont été générées par le produit ;
- la preuve d'identité en tant que SSCD à des entités externes ;
- en option, la réception et le stockage de certificats ;
- l'initialisation des données d'authentification d'utilisateurs (RAD) ;
- le basculement du SSCD d'un état non opérationnel à un état opérationnel, et dans un état opérationnel, la génération de signatures digitales avec le processus suivant :
    - la sélection d'une SCD s'il y en a plusieurs sur le produit ;
    - la réception des données à signer ou de leur représentation unique à travers un canal de confiance ;
    - l'authentification du signataire et détermination de son intention de signer ;
    - l'application de la fonction de génération de signature appropriée.

1.2.3 *Architecture*

Le produit est constitué des éléments suivants, développés par NXP :

- l'*applet* ChipDoc ;
- sa plateforme JCOP 4 , sur microcontrôleur N7121.

1.2.4 *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 valeurs suivantes :
  - Nom : 0x43686970446F63 ;
  - Version : 0x03010652 ;
  - *Card capabilities* : 0x00036FEF ;
- la plateforme est identifiée en réponse à la commande GET_DATA(IDENTIFY) par les valeurs suivantes :
  - Patch ID : 0x0000000000000001 ;
  - ROM ID : 2E5AD88409C9BADB ;
  - Platform ID : 4A335233353130314641394530343030DD0984593B0048EF ou 4A3352333531303233363331303430 30DCE5C19CFE6D0DCF ;
- la configuration SSCD de l'application est identifiée par la présence dans le fichier EF.DIR d'un AID au préfixe E828D080F.

1.2.5 *Cycle de vie*

Le cycle de vie du produit est présenté au chapitre « *TOE Lifecycle* » de la cible de sécurité.

Les sites de développement et de production de l'IC et de la plateforme sont listés dans [CER_IC] et [CER_PLA]. L'*applet* a été principalement développée sur les sites NXP de Gratkorn et d'East Kilbride Glasgow.

NB : Dans le cadre particulier de cette certification, qui correspond à une évaluation avec réduction de portée, la validité des audits n'a pas été vérifiée.

1.2.6 *Configuration évaluée*

Le certificat porte sur la configuration SSCD de l'*applet*, la plateforme restant ouverte. Aucune autre application que l'applet ChipDoc V3.1 n'est connue.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel [CEM] et aux dispositions de [NOTE25].

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).

2.2 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 dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme « JCOP 4 P71 » au niveau EAL6 augmenté des composants ASE_TSS.2 et ALC_FLR.1, conforme au profil de protection [PP0099]. Cette plateforme a été certifiée le 5 juillet 2022 sous la référence NSCIB-CC-180212, voir [CER_PLA].

L'évaluation s'appuie sur les résultats d'évaluation de ce même produit certifié le 30 juillet 2020 sous la référence ANSSI-CC-2021/18, voir [CER]. Elle correspond à une évaluation avec réduction de portée suite à l'identification de vulnérabilité.

L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat [CER] n'a pas été conduite dans le cadre de cette réévaluation partielle. Le niveau de résistance d'un produit certifié se dégrade au cours du temps. Seule une réévaluation ou une surveillance de cette version du produit permettrait de maintenir le niveau de confiance dans le temps.

Le CESTI en charge de l'évaluation initiale a émis un rapport d'analyse de réduction de portée (référence [RTE_part]) pour réévaluer les composants d'assurance impactés par l'évolution de la cible de sécurité du produit.

Le rapport technique d'analyse de réduction de portée [RTE_part], remis à l'ANSSI le 1er août 2022, pour réévaluer les composants d'assurance ASE, ADV, ALC (hors audits), et ATE impactés par l'évolution de la cible de sécurité [ST] détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

Le rapport technique [RTE_init], remis à l'ANSSI le 20 mai 2021 détaille les travaux initialement réalisés menés par le centre d'évaluation et atteste que la résistance du produit atteignait VAN.5 lors de son édition.

2.3 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 au référentiel [ANSSI 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 potentiel d'attaque visé.

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

2.4 Analyse du générateur d'aléa

Le générateur de nombres aléatoires 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 le référentiel [ANSSI 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.

3 La certification

3.1 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 conformément à [NOTE25], répond aux caractéristiques de sécurité spécifiées dans la cible de sécurité [ST] pour le niveau d'évaluation visé à la date de certification initiale (voir [CER]). Pour rappel, les travaux d'analyse de la réduction de portée sont centrés sur l'impact de cette réduction de portée sur les tâches de conformité de l'évaluation initiale. La résistance globale du produit aux attaques de l'état de l'art n'a pas été mise à jour depuis la certification initiale.

3.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 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], notamment :

- toutes les futures applications chargées sur ce produit (chargement post-émission) doivent respecter les contraintes de développement de la plateforme (voir [CER_PLA]) ;
- les autorités de vérification doivent appliquer le guide de la plateforme (voir [CER_PLA]) ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement post-émission) doit être activée conformément aux indications des guides de la plateforme (voir [CER_PLA]).

3.3 Reconnaissance du certificat

3.3.1 *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 :

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

3.3.2 *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 :

[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, rev 3.6, 13 juillet 2022. 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, rev 3.6, 13 juillet 2022.
[RTE_Part]	Evaluation Technical Report, ChipDoc v3.1 Scope Reduction, ChipDoc_v3.1_ScopeReduction_ETR, révision 1.0, 26 juillet 2022, THALES.
[RTE_Init]	*Evaluation Technical Report, project ChipDoc V3.1 SSCD2*, référence CDV31_SSCD2_ETR, révision 3.0, 20 mai 2021.
[ANA-CRY]	*Analysis of Cryptographic Mechanisms, project ChipDoc V3.1 SSCD2*, référence CDV31_SSCD2_CRY, révision 2.0, 6 mai 2021.
[CONF]	Configuration Item List, CDv3.1_2_04920_ALC_CIL_v2.0, 19 juillet 2022.
[GUIDES]	– ChipDoc 3.1 User Guide Manual, ref 518830, 17 août 2020 ; – ChipDoc 3.1 SSCD Personalization Guide, ref 519122, 13 août 2020 ; – ChipDoc 3.1 Crypto Guide, révision 1.0, 4 décembre 2020 ; – ChipDoc V3 Application Note, révision 1.4, 20 juin 2022.
[PP0099]	*Java Card Protection Profile – Open Configuration, version 3.0.5,* décembre 2017. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-CC-PP-0099-2017.
[PP-SSCD-Part2]	*Protection profiles for secure signature creation device – Part 2: Device with key generation*, référence : prEN 14169-2:2012, version 2.0.1 datée du 23 janvier 2012. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 21 février 2012 sous la référence BSI-CC-PP-0059-2009-MA-01.
[PP-SSCD-Part3]	*Protection profiles for secure signature creation device – Part 3: Device with key import*, référence : prEN 14169-3:2012, version 1.0.2 datée du 24 juillet 2012. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 27 septembre 2012 sous la référence BSI-CC-PP-0075-2012.
[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 14169-4:2012, version 1.0.1 datée du 14 novembre 2012. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 12 décembre 2012 sous la référence BSI-CC-PP-0071-2012.
[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 14169-5:2012, version 1.0.1 datée du 14 novembre 2012. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 12 décembre 2012 sous la référence BSI-CC-PP-0072-2012.

[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 14169-6:2013, version 1.0.4 datée du 3 avril 2013. Certifié par le BSI le 16 avril 2013 sous la référence BSI-CC-PP-0076-2013.
[CER]	Rapport de certification ANSSI-CC-2021/20, ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration (version 3.1.6.52), 4 juin 2021.
[CER_IC]	*Certification Report BSI-DSZ-CC-1136-V2-2022, NXP Secure Smart Card Controller N7121 with ICDedicated Software and Crypto Library (R1/R2/R3),* 7 juin 2022.
[CER_PLA]	*Certification Report JCOP 4 P71, NSCIB-CC-180212-CR4*, 5 juillet 2022.

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, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 4.0.
[CRY-P-01]	Procédure ANSSI-CC-CRY-P01 Modalités pour la realisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, ANSSI.
[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 3.1, juin 2020.
[COMP] *	*Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version 1.5.1, mai 2018.
[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.
[NOTE25]	*Note d'application : Réduction de portée d'un certificat CC, référence ANSSI-CC-NOTE-25_v1.0, version 1.0, 23 septembre 2021.*

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