Docusign Envelope ID: 2DC3F82F-2A94-4EED-BB5F-AE61C0E565C5

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-2023/68v2

ChipDoc v4.1 on JCOP 4.5 P71 in ICAO EAC(1&2) with PACE configuration (Version 4.1.1.52)

Paris, le 16/2/2026 | 22:35 CET

Vincent Strubel

Docusign Envelope ID: 2DC3F82F-2A94-4EED-BB5F-AE61C0E565C5

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

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

Docusign Envelope ID: 2DC3F82F-2A94-4EED-BB5F-AE61C0E565C5

Référence du rapport de certification

ANSSI-CC-2023/68v2

Nom du produit

ChipDoc v4.1 on JCOP 4.5 P71 in ICAO EAC(1&2) with PACE configuration

Référence/version du produit

Version 4.1.1.52

Conformité à un profil de protection

Machine Readable Travel Document with « ICAO Application », Extended Access Control with PACE, version 1.3.2

Certifié BSI-CC-PP-0056-V2-2012-MA-02

Machine Readable Travel Document using Standard Inspection Procedure with PACE, version 1.0.1

Certifié BSI-CC-PP-0068-V2-2011-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

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.

Docusign Envelope ID: 2DC3F82F-2A94-4EED-BB5F-AE61C0E565C5

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.cyber.gouv.fr.

Docusign Envelope ID: 2DC3F82F-2A94-4EED-BB5F-AE61C0E565C5

TABLE DES MATIERES

1 Le produit 6
1.1 Présentation du produit 6
1.2 Description du produit 6
1.2.1 Introduction 6
1.2.2 Services de sécurité 6
1.2.3 Architecture 6
1.2.4 Identification du produit 6
1.2.5 Cycle de vie 7
1.2.6 Configuration évaluée 7
2 L'évaluation 8
2.1 Référentiels d'évaluation 8
2.2 Travaux d'évaluation 8
2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI 9
2.4 Analyse du générateur d'aléa 9
3 La certification 10
3.1 Conclusion 10
3.2 Restrictions d'usage 10
3.3 Reconnaissance du certificat 11
3.3.1 Reconnaissance européenne (SOG-IS) 11
3.3.2 Reconnaissance internationale critères communs (CCRA) 11
ANNEXE A. Références documentaires du produit évalué 12
ANNEXE B. Références liées à la certification 13

Docusign Envelope ID: 2DC3F82F-2A94-4EED-BB5F-AE61C0E565C5

1 Le produit

1.1 Présentation du produit

Le produit évalué est « ChipDoc v4.1 on JCOP 4.5 P71 in ICAO EAC(1&2) with PACE configuration, Version 4.1.1.52 » développé par NXP SEMICONDUCTORS.

Il s'agit de documents électroniques, qui permettent différents types d'usage basés sur l'identité électronique.

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 aux profils de protection [PP EACv2] et [PP PACE].

Cette cible s'appuie par ailleurs sur les prescriptions de [FID_ADD].

Dans le cadre particulier de cette certification, qui correspond à une évaluation avec réduction de portée (voir [NOTE25]), la réduction de portée correspond au retrait de la fonctionnalité « PIN de faible entropie » du périmètre d'évaluation, par ajout de restriction dans les guides.

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont indiqués au sous-chapitre 1.5.4.1 *« ICAO ePP functionalities »* et 1.5.4.2 *« Additional Functionalities »* de la cible de sécurité.

1.2.3 *Architecture*

L'architecture du produit est présentée au chapitre 1.5.1 *« TOE Components »* de la cible de sécurité.

La seule *applet* considérée lors de l'évaluation est l'*applet* ChipDoc ; aucune autre *known applet* au sens de [OPEN] n'est à reporter.

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 indiqués en table 2 et table 3 de la cible de sécurité. La procédure d'identification est fournie dans les [GUIDES].

La configuration EAC avec PACE est reconnue par la présence du fichier EF.*CardAccess*.

Docusign Envelope ID: 2DC3F82F-2A94-4EED-BB5F-AE61C0E565C5

1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit au chapitre 1.6 « *TOE Life Cycle* » de la cible de sécurité.

Il s'inscrit dans le cycle de vie générique définit dans [PP EACv2].

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 ICAO[1] EAC avec PACE du produit.

[1] *International Civil Aviation Organization*

Docusign Envelope ID: 2DC3F82F-2A94-4EED-BB5F-AE61C0E565C5

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM] , ainsi qu'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 s'appuie sur les résultats d'évaluation de ce même produit certifié le 19 janvier 2024 sous la référence ANSSI-CC-2023/68, 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 27 janvier 2026, 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 23 octobre 2023, 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.

Docusign Envelope ID: 2DC3F82F-2A94-4EED-BB5F-AE61C0E565C5

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 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.

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].

Par ailleurs, 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.

Docusign Envelope ID: 2DC3F82F-2A94-4EED-BB5F-AE61C0E565C5

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.

Le certificat associé à ce rapport, référencé ANSSI-CC-2023/68v2 a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité jusqu'au 19 janvier 2029.

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].

Docusign Envelope ID: 2DC3F82F-2A94-4EED-BB5F-AE61C0E565C5

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[2], 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 :

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[3] , 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 SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

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

Docusign Envelope ID: 2DC3F82F-2A94-4EED-BB5F-AE61C0E565C5

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - ChipDoc v4.1 on JCOP 4.5 P71 in ICAO EAC(1&2) *with* PACE *configuration, Security Target*, Rev 1.3, 21 janvier 2026. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ChipDoc v4.1 on JCOP 4.5 P71 in ICAO EAC(1&2) *with* PACE *configuration, Security Target Lite,* Rev 1.3, 25 novembre 2025.
[RTE_Init]	Rapport technique d'évaluation : - *Evaluation Technical Report* ChipDoc v4.1 EAC PACE 4.1, CDV4.1_PACE_4.1_ETR v1.0, 23 octobre 2023.
[RTE_Part]	*Evaluation Technical Report ChipDoc v4.1 Descope, CD_4.1_Descope_ETR,* revision 2.0, 26 janvier 2026
[ANA_CRY]	*Analysis of Cryptographic Mechanisms* ChipDoc v4.1 EAC PACE 4.1, CDV4.1_PACE_CRY_v1.0, 20 octobre 2023.
[CONF]	Liste de configuration du produit : *Configuration Item List,* CDv4.1_2_04913_ALC_CIL, 26 janvier 2026.
[GUIDES]	Voir [ST] §1.5.2, Table 5, lignes "Document".
[CER]	*ChipDoc v4.1 on JCOP 4.5 P71 in ICAO EAC(1&2) with PACE configuration (Version 4.1.1.52),* Rapport de certification ANSSI-CC-2023/68, 19 janvier 2024
[CER_IC]	Rapport de certification BSI-DSZ-CC-1149-V2-2023, NXP Secure Smart Card Controller N7122 (R1/R2/R3), 13 septembre 2023.
[CER_PLA]	Rapport de certification NSCIB-CC-0313985-CR, JCOP 4.5 P71, 2 août 2022, maintenu sous la référence NSCIB-CC-0313985_1MA2, 13 octobre 2023.
[PP EACv2]	*Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE*, version 1.3.2, 5 décembre 2012. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-CC-PP-0056-V2-2012-MA02.
[PP PACE]	*Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE*, version 1.0.1, 22 juillet 2014. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-CC-PP-0068-V2-2011-MA-01.
[FID_ADD]	*Module : Annexe PP0056v2 eDigitalIdentity document using Remote Access Control with PACE v2,* version 1.1, 21 novembre 2019.

Docusign Envelope ID: 2DC3F82F-2A94-4EED-BB5F-AE61C0E565C5

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 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, novembre 2022.
[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*), 4 février 2013.
[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.

Docusign Envelope ID: 2DC3F82F-2A94-4EED-BB5F-AE61C0E565C5

[SOG-IS Crypto]	*SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms*, version 1.2, 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.