PREMIÈRE 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-2023/38

ChipDoc v2 on JCOP 3 P60 in SSCD configuration (v7b4_2)

Paris, le 21 Juillet 2023

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

Vincent STRUBEL

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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-2023/38**
Nom du produit **ChipDoc v2 on JCOP 3 P60 in SSCD configuration**
Référence/version du produit **v7b4_2**
Conformité auxprofils 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.*
Critère d'évaluation et version **Critères Communs version 3.1 révision 4**
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.

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 v2 on JCOP 3 P60 in SSCD configuration, v7b4_2 » développé par NXP SEMICONDUCTORS.

Ce produit offre des services d'authentification et de signature électronique (SSCD).

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-SSCD-Part2] et [PP-SSCD-Part3].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont la génération, l'import, l'export des données de création de signatures, et la création de signatures, comme mentionnée en page 10 de la cible de sécurité [ST].

1.2.3 *Architecture*

Le produit est constitué d'une plateforme JavaCard JCOP et d'une applet ChipDoc, comme décrit en figure 1 de la cible de sécurité [ST].

1.2.4 *Identification du produit*

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

Comme mentionné au 1.3.4.2 « Identification of the TOE » de la cible de sécurité [ST], la version certifiée du produit est identifiable par les éléments *Platform ID*, *Patch ID* pour la plateforme JCOP, et par l'élément *applet version* pour ChipDoc. La méthode pour lire ces éléments et les valeurs attendues sont indiquées dans les [GUIDES].

1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit en section 1.3.2 « TOE lifecycle » de la cible de sécurité.

1.2.6 *Configuration évaluée*

Le certificat porte sur la configuration SSCD du produit.

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].

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 la plateforme déjà certifiée par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme JCOP3 P60, voir [CER_PLA].

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

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 au 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, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CER_PLA]).

Par ailleurs, comme requis dans le référentiel [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.

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 répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

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].

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 :

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 :

[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 v2 on JCOP 3 P60 in SSCD configuration, Security Target*, Rev 2.5, 14 juin 2023, NXP. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *ChipDoc v2 on JCOP 3 P60 in SSCD configuration*, *Security Target Lite*, Rev 1.6, 14 juin 2023, NXP.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report*, Chipdoc v2 *Reevaluation* 2022, CDV2_Reeval2022_ETR v3.0, 20 juin 2023, THALES / CNES.
[ANA_CRY]	*Analysis of Cryptographic Mechanisms*, Chipdoc v2 *Reevaluation* 2022, CDV2_Reeval2022_CRY v1.0, 20 mars 2023, THALES / CNES.
[CONF]	Liste de configuration du produit : CIList, CDv2.0_04912_ALC_CIL, 16 juin 2023, NXP.
[GUIDES]	Voir [ST] §1.3.4.1, Table 5, lignes "document".
[CER_PLA]	Certification report JCOP3 P60, NSCIB-CC-2200035-01-CR, 25 avril 2023.
[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.

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, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001;* - *Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002;* - *Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.*
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004*.
[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.
[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 1.2, janvier 2020.

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