



PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2018/07

NXP JCOP 3 SECID P40 ChipDoc-Lite in SSCD Configuration (version 1.0.10)

Paris, le 12 mars 2018

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

Guillaume POUPARD
[ORIGINAL SIGNE]



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 présumées 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.

Référence du rapport de certification

ANSSI-CC-2018/07

Nom du produit

**NXP JCOP 3 SECID P40 ChipDoc-Lite in SSCD
Configuration**

Référence/version du produit

Version 1.0.10

Conformité à un profil de protection

**[PP-SSCD-Part2] Protection profiles for secure signature
creation device - Device with key generation, v2.0.1 ;
[PP-SSCD-Part3] Protection profiles for secure signature
creation device - Device with key import, v1.0.2**

Critères 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 GmbH
Troplowitzstr. 20, 22529 Hamburg, Allemagne**

Commanditaire

**NXP Semiconductors GmbH
Troplowitzstr. 20, 22529 Hamburg, Allemagne**

Centre d'évaluation

**Serma Safety & Security
14 rue Galilée, CS 10055, 33615 Pessac Cedex, France**

Accords de reconnaissance applicables



SOG-IS



Ce certificat est reconnu au niveau EAL2

Préface

La certification

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 Premier ministre 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 matières

1. LE PRODUIT	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Introduction</i>	6
1.2.2. <i>Services de sécurité</i>	6
1.2.3. <i>Architecture</i>	6
1.2.4. <i>Identification du produit</i>	6
1.2.5. <i>Cycle de vie</i>	7
1.2.6. <i>Configuration évaluée</i>	8
2. L’EVALUATION	9
2.1. REFERENTIELS D’EVALUATION	9
2.2. TRAVAUX D’EVALUATION	9
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	9
2.4. ANALYSE DU GENERATEUR D’ALEAS	9
3. LA CERTIFICATION	11
3.1. CONCLUSION	11
3.2. RESTRICTIONS D’USAGE	11
3.3. RECONNAISSANCE DU CERTIFICAT	12
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	12
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	12
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT	13
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	14
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	16

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce « NXP JCOP 3 SECID P40 ChipDoc-Lite in SSCD Configuration, version 1.0.10 » développé par NXP SEMICONDUCTORS GMBH.

Ce produit est destiné à être utilisé comme dispositif sécurisé de création de signature (*SSCD*, *Secure Signature Creation Device*).

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 de la donnée de création de signature (*Signature Creation Data* ou SCD) et de la donnée de vérification de signature (*Signature Verification Data* ou SVD) associée ;
- l'import de la donnée de création de signature (SCD) et, optionnellement, de la donnée de vérification de signature (SVD) associée ;
- l'export de la donnée de vérification de signature (SVD) pour une création de certificat électronique ;
- la création de signature électronique via un canal de confiance.

1.2.3. Architecture

Le produit est constitué :

- d'un microcontrôleur « P40C072VE » et de sa bibliothèque cryptographique V2.0 ;
- d'un système d'exploitation « JCOP_3_SECID P40 », comportant une machine virtuelle JavaCard, et utilisé comme plateforme fermée ;
- de l'*applet* « ChipDoc Lite, Version 1.0.10 » (seule cette *applet* fait partie du périmètre de la présente évaluation).

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 la méthode indiquée dans [GUIDES], qui permet :

- l'identification de l'*applet* via la commande GET DATA 00 CA 01 00 00 ;

- l'identification de la plateforme via la commande GET DATA 80 CA FF 01 01 8x 00, où x peut prendre les valeurs 1 à 5 ;
- la vérification de l'état sécurisé de la plateforme via une tentative d'effectuer la commande GlobalPlatform INSTALL [for load].

Le tableau ci-dessous résume les commandes et leurs paramètres :

Commande	Donnée d'identification attendue	Interprétation des données
GET DATA <i>applet</i> name 00 CA 01 00 00	43 68 69 70 44 6F 63 20 4C 69 74 65 90 00	« ChipDoc Lite »
GET DATA <i>applet</i> version 00 CA 01 16 00	01 00 01 0A 90 00	<i>Applet</i> version 1.0.10
GET DATA IDENTIFY (platform) 80 CA FF 01 01 8x 00	Si x = 1 : FF 01 04 81 02 05 20 90 00	IC Type: 0x0520
	Si x = 2 : FF 01 04 82 02 00 01 90 00	Release Level: 0x0001
	Si x = 3 : FF 01 04 83 02 53 31 90 00	Release Date: 0x5331
	Si x = 4 : FF 01 03 84 01 01 90 00	Patch Level: 0x01
	Si x = 5 : FF 01 06 85 04 53 31 D4 25 90 00	OSID (<i>Operating System Identifier</i>) : 0x5331D425
INSTALL [for load] 80 E6 02 00 0A 05 01 02 03 01 05 00 00 00 00 00	6D 00	Erreur signalant que l'instruction est invalide (la plateforme est déjà fermée)

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

	Phase	Acteur	Couvert par
Etape 1	Développement	<i>NXP SEMICONDUCTORS</i>	ALC
Etape 2	Développement	<i>NXP SEMICONDUCTORS</i>	ALC
Etape 3	Fabrication	<i>NXP SEMICONDUCTORS</i>	ALC
Etape 4	Fabrication SSCD (Pré-perso)	<i>NXP SEMICONDUCTORS</i>	ALC
Point de livraison TOE			
Etape 5	Fabrication SSCD (Pré-perso)	Fabricant SSCD ou <i>NXP SEMICONDUCTORS</i>	AGD_PRE si l'opération est effectuée par un fabricant SSCD tiers ALC si le site est un site <i>NXP SEMICONDUCTORS</i> audité
Point de livraison TOE			
Etape 6	Personnalisation	Personnalisateur	AGD_PRE
Etape 7	Utilisation opérationnelle	Utilisateur final	AGD_OPE

Le produit a été développé sur les sites suivants :

NXP Semiconductors – Site de Livingston

6 rue Amondvale Business Park, Almondvale Way
Livingston, EH54 6GA
United Kingdom

NXP Semiconductors – Site de Hamburg

Tropowitzstr. 20
22529 Hamburg
Germany

Les sites de développement du composant et de la bibliothèque sont respectivement couverts par le certificat [CER-IC] et [CER-LIB].

1.2.6. Configuration évaluée

Le certificat porte sur le produit pour lequel :

- l'*applet* « ChipDoc Lite, Version 1.0.10 » est instanciée et la plateforme est fermée sans possibilité de charger et d'instancier d'autres *applets* ;
- les recommandations du guide [GUIDES] sont strictement appliquées durant la phase « Personnalisation » du cycle de vie, ainsi que dans la phase de pré-personnalisation si elle est effectuée sur un site client ;
- le produit est en configuration SSCD.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [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 le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation des bibliothèques « Firmware Librairies V2.x on P40C008/012/024/040/072 VE.001 », certifiées au niveau EAL5 augmenté des composants ALC_DVS.2, ASE_TSS.2 et AVA_VAN.5 conforme au profil de protection [PP0084] le 26 juillet 2017 sous la référence [CER-LIB], et du composant « NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001 », certifié au niveau EAL5 augmenté des composants ALC_DVS.2, ASE_TSS.2 et AVA_VAN.5 conforme au profil de protection [PP0084] le 3 mai 2017 sous la référence [CER-IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 26 septembre 2017, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

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-IC]).

Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI ([REF]), la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.

Les résultats ont été pris 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 AVA_VAN.5 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 « NXP JCOP 3 SECID P40 ChipDoc-Lite in SSCD Configuration, version 1.0.10 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL5 augmenté des composants AVA_VAN.5 et ALC_DVS.2.

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'accord¹, 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 [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires², 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.org.

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

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit		
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Intitulé du composant	
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	2	Well-structured internals
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	4	4	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	4	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	2	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	3	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - JCOP_3_SECID_P40 SSCD ChipDoc-Lite Applet in SSCD Configuration on JCOP3_SECID_P40 – Security Target, référence : ST-JCOP_3_SECID_P40 SSCD-01, version 1.2, 18 septembre 2017, <i>NXP SEMICONDUCTORS GMBH</i>. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - JCOP_3_SECID_P40 SSCD ChipDoc-Lite Applet in SSCD Configuration on JCOP3_SECID_P40 – Security Target Lite, référence : ST-JCOP_3_SECID_P40 SSCD-02, version 1.2, 18 septembre 2017, <i>NXP SEMICONDUCTORS GMBH</i>.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Evaluation Technical Report – HESTIA Project, référence : HESTIA_ETR_v1.1, version 1.1, 20 septembre 2017, <i>SERMA SAFETY & SECURITY</i>.
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - Hestia_ConfigurationList_v1_4_20170921.xlsx, 21 septembre 2017.
[GUIDES]	<p>Guide d'installation et d'utilisation du produit (pour utilisateur final) :</p> <ul style="list-style-type: none"> - ChipDoc Lite 1.0 Applet – User Manual, version 1.2, 4 novembre 2016, <i>SEMICONDUCTORS GMBH</i>.
[PP-SSCD-Part2]	<p>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. <i>Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 21 février 2012 sous la référence BSI-CC-PP-0059-2009-MA-01.</i></p>
[PP-SSCD-Part3]	<p>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. <i>Certifié par le BSI le 27 septembre 2012 sous la référence BSI-CC-PP-0075-2012.</i></p>
[PP0084]	<p>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.</i></p>
[CER-IC]	<p>NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001. <i>Certifié par le NSCIB (Netherlands Scheme for Certification in the Area of IT Security) sous la référence NSCIB-CC-65655-CR2 le 3 mai 2017.</i></p>



[CER-LIB]	Firmware Librairies V2.x on P40C008/012/024/040/072 VE.001. <i>Certifié par le NSCIB (Netherlands Scheme for Certification in the Area of IT Security) sous la référence NSCIB-CC-65156-CR2 le 26 juillet 2017.</i>
-----------	--

Annexe 3. 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]	Procédure ANSSI-CC-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, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : <ul style="list-style-type: none">- 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, version 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.4, août 2015.
[CC RA]	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.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr .

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