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-2017/64

ChipDoc P60 on JCOP 3 SECID P60 (OSB) SSCD masqué sur composant P6022J VB (version v7b4)

Paris, le 20 novembre 2017

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 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-2017/64

Nom du produit

ChipDoc P60 on JCOP 3 SECID P60 (OSB) SSCD masqué sur composant P6022J VB

Référence/version du produit

Version v7b4

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

Stresemannallee 101, 22529 Hamburg, Allemagne

Commanditaire

NXP Semiconductors GmbH

Stresemannallee 101, 22529 Hamburg, Allemagne

Centre d'évaluation

THALES (TCS – CNES)

290 allée du Lac, 31670 Labège, France

Accords de reconnaissance applicables

CCRA

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

1.1. Présentation du produit

Le produit évalué est « ChipDoc P60 on JCOP 3 SECID P60 (OSB) SSCD masqué sur composant P6022J VB, version v7b4 » 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 « P6022J VB » et de sa bibliothèque cryptographique V3.1 ;
- d'un système d'exploitation « JCOP3 SECID P60 (OSB) », comportant une machine virtuelle JavaCard, et utilisé comme plateforme fermée ;
- de l'*applet* « ChipDoc P60 on JCOP 3 SECID P60 (OSB) SSCD, Version v7b4 » (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 CB 00 03 00 ;
- l'identification de la plateforme via la commande GET DATA 80 CA 00 FE 02 DF 28 00 ;
- 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 *applet* version 00 CB 00 03 00	00 07 00 04 ou 00 07 01 04	*Applet* version v7b4 ou *Applet* version v7b4 avec patch ID 1.
GET DATA IDENTIFY (platform) 80 CA 00 FE 02 DF 28 00	FE 3A DF28 37	Données propriétaires et longueur des données
	01 0C 80 00 00 00 C4 D3 D0 6D D8 21 D8 7E	Tag *EEPROM ID* Longueur *EEPROM ID* *EEPROM ID*
	02 08 02 00 00 00 00 00 00 00 ou 04 00 00 00 00 00 00 00 ou 03 00 00 00 00 00 00 00	Tag *patch ID* Longueur *patch ID* *Patch ID (PL2)* ou *Patch ID (PL4)* ou *Patch ID (PL3)*
	03 10 4A7848797979303031384438303430 30 ou 4A7848797979303031393739303430 30	Tag *platform build ID* Longueur *platform build ID* *Platform build ID (RC8)* ou *Platform build ID (RC9)*
	04 08 B8CD 9D64 C393 8D32	Tag *custom mask ID* Longueur *custom mask ID* *Custom mask ID*
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	*NXP SEMICONDUCTORS*	ALC
Etape 2	Développement	*NXP SEMICONDUCTORS*	ALC
Etape 3	Fabrication	*NXP SEMICONDUCTORS*	ALC
Etape 4	Fabrication MRTD (Pré-perso)	*NXP SEMICONDUCTORS*	ALC
Point de livraison TOE			
Etape 5	Fabrication MRTD (Pré-perso)	Fabricant MRTD ou *NX P SEMICONDUCTORS*	AGD_PRE si l'opération est effectuée par un fabricant MRTD tiers ALC si le site est un site *NXP SEMICONDUCTORS*
Point de livraison TOE			
Etape 6	Personnalisation	Personnalisateur	AGD_PRE
Etape 7	Utilisation opérationnelle	Utilisateur final	AGD_OPE

Le développement est effectué sur les sites suivants :

Développement logiciel :
NXP SEMICONDUCTORS - Site de Livingston
6 Amondvale Business Park, Almondvale Way,
Livingston, EH54 6GA,
United Kingdom

Tests logiciels et rédaction des guides utilisateur :
NXP SEMICONDUCTORS - Site de San Jose
411 East Plumeria Drive
San Jose, CA 95134
United States of America

Rédaction de la documentation relative à l'évaluation Critères Communs :
NXP SEMICONDUCTORS - Site de Gratkorn
Mikron-Weg 1, A-8101
Gratkorn, Austria

Les sites de développement du composant (respectivement, de la bibliothèque cryptographique associée, de la plateforme JavaCard) sont couverts par le certificat [CER-IC] (respectivement [CER-LIB], [CER-OS]).

1.2.6. Configuration évaluée

Le certificat porte sur le produit pour lequel :

- l'*applet* « ChipDoc P60 on JCOP 3 SECID P60 (OSB) SSCD, Version v7b4 » 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 de la plateforme JavaCard « NXP JCOP 3 SECID P60 (OSB) » au niveau EAL5 augmenté des composants AVA_VAN.5, ALC_DVS.2 et ASE_TSS.2 (sur composant P6022J) conforme au profil de protection [PP-JC]. Cette plateforme a été certifiée le 1 août 2017 sous la référence [CER-OS].
Le microcontrôleur sous-jacent [CER-IC] et sa bibliothèque cryptographique [CER-LIB] ont été certifiés moins de 18 mois avant la date du présent rapport.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 31 octobre 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 « ChipDoc P60 on JCOP 3 SECID P60 (OSB) SSCD masqué sur composant P6022J VB, version v7b4 » 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'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 [CC RA].

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.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 [CCv3.1R4]

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

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - ChipDoc P60 on JCOP 3 SECID P60 (OSB) SSCD – Security Target, v1.1, 31 octobre 2017, *NXP SEMICONDUCTORS GMBH.* Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ChipDoc P60 on JCOP 3 SECID P60 (OSB) SSCD–Security Target Lite, v1.0, 31 octobre 2017, *NXP SEMICONDUCTORS GMB.*
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report Project : Phoenix_SSCD_OSB, référence : PHX_SSCD_OSB_ETR, version : 2.0, 31 octobre 2017, *THALES (TCS – CNES).*
[CONF]	Liste de configuration du produit : - 2017_10_31_CIL_CD_v7b0x04_SSCD_on_OSB.xlsx, 31 octobre 2017.
[GUIDES]	Guide d'installation et d'utilisation du produit (pour utilisateur final) : - ChipDoc v7b4 applet in SSCD configuration – Preparation and Operation Manual, version 1.3, 30 octobre 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 le 27 septembre 2012 sous la référence BSI-CC-PP-0075-2012.*
[PP-JC]	Java Card Protection Profile – Open Configuration, Version 3.0, Mai 2012 *Maintenu par l'ANSSI sous la référence ANSSI-PP-2010-03-M1 le 25 juin 2010.*
[CER-IC]	NXP Secure Smart Card Controller P6022y VB including IC dedicated software. *Certifié par le BSI sous la référence BSI-DSZ-CC-V2-0973 le 11 octobre 2016.*
[CER-LIB]	Crypto Library V3.1.x on P6022y VB. *Certifié par le NSCIB (Netherlands Scheme for Certification in the Area of IT Security) sous la référence NSCIB-CC-15-67206-CR le 26 juillet 2016.*
[CERT-OS]	NXP JCOP 3 SECID P60 (OSB). *Certifié par le NSCIB sous la référence NSCIB-CC-98209-CR le 1 août 2016.*

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 : - 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.
[OPEN]	Certification of « Open » smart card products, version 1.1 (for trial use), 4 février 2013.
[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.