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-2015/44

NXP JAVA OS1 ChipDoc v1.0 SSCD (J3K080/J2K080)

Paris, le 13 octobre 2015

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.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2015/44

Nom du produit

NXP JAVA OS1 ChipDoc v1.0 SSCD (J3K080/J2K080)

Référence/version du produit

V1.0

Conformité à des profils de protection

Protection profiles for Secure signature creation device Part 2: Device with key generation

V1.03, BSI-CC-PP-0059-2009

Protection profiles for secure signature creation device Part 3: Device with key import

V1.0.2, BSI-CC-PP-0075-2012

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

Athena Smartcard Solutions

16615 Lark Ave, Suite 202, Los Gatos 95032 CA, USA

NXP Semiconductors Germany GmbH

Stresemannallee 101, 22529 Hamburg, Allemagne

Commanditaire

Athena Smartcard Solutions

16615 Lark Ave, Suite 202, Los Gatos 95032 CA, USA

Centre d'évaluation

Serma Technologies

14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit 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 « NXP JAVA OS1 ChipDoc v1.0 SSCD (J3K080/J2K080) » développé par Athena et NXP.

Ce produit est destiné à être utilisé pour créer des signatures électroniques. Il assure que seul l'utilisateur légitime peut utiliser la fonction de création de signature.

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 strictement conforme aux profils de protection [PP-SSCD-Part2] et [PP-SSCD-Part3].

1.2.2. Architecture

Le produit est constitué :

- d'un microcontrôleur « P60D080JVC » et de ses librairies cryptographiques, développés par NXP ;
- d'un système d'exploitation « NXP JAVA OS1 » développé par Athena, avec les fonctionnalités GlobalPlatform, comportant une machine virtuelle JavaCard, et utilisé comme plateforme fermée ;
- de l'applet « ChipDoc » implémentant les fonctionnalités SSCD.

1.2.3. Identification du produit

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

Comme décrit dans la procédure d'acceptation fournie par le développeur (voir [GUIDES]), la version certifiée du produit est identifiable par les éléments suivants :

- les CPLC DATA comportent les informations suivantes :

IC fabricator	'4790' (NXP)
IC type	'0502' (P60D080)
Operating system identifier	'8211' (Athena OS755)
Operating system release date	'4258' (15 Sept 2014)
Operating system release level	'FF02'

- la commande GETDATA-VERSION envoyée à l'instance de l'application « ChipDoc » permet d'obtenir la valeur suivante : 0x01050119 ;
- le rejet, avec réponse « *instruction not supported* », de toute commande GlobalPlatform INSTALL permet de vérifier que la plateforme est fermée.

1.2.4. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection des données de l'utilisateur (secrets permettant la signature) ;
- l'authentification du signataire (y compris séparation des rôles signataire et administrateur) ;
- la création de signature.

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit au chapitre 2.6 de la cible de sécurité.

Le composant P60D080JVC a été développé sur les sites de NXP conformément au certificat [CERT_IC].

Le logiciel embarqué a été développé sur les sites d'Athena suivants :

Athena Smartcard Inc. **Site de Los Gatos**	**Athena Smartcard Inc.** **Site de Livingston**
16615 Lark Ave, Suite 202, Los Gatos CA 95032 Etats Unis d'Amérique	6 Amondvale Business Park, Almondvale Way, Livingston, EH54 6GA, Royaume Uni

Le produit « NXP JAVA OS1 ChipDoc v1.0 SSCD » est fabriqué sur les sites de NXP conformément au certificat [CERT_IC].

1.2.6. Configuration évaluée

Le certificat porte sur le produit pour lequel :

- durant la phase « Initialisation » du cycle de vie, l'applet ChipDoc est instanciée et la plateforme est fermée ;
- durant la phase « Personalisation » du cycle de vie, les recommandations du guide [AGD_PRE] sont strictement appliquées.

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 [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 du microcontrôleur « *P60D080* » au niveau EAL5 augmenté des composants ALC_DVS.2, ASE_TSS.2 et AVA_VAN.5, conforme au profil de protection [PP0035]. Ce microcontrôleur a été certifié le 24 octobre 2014 sous la référence *BSI-DSZ-CC-0897-V2-2014*.
Cette évaluation a également pris en compte les résultats de l'évaluation de la bibliothèque cryptographique « Crypto Library v1.0 on P60x080/052/040PVC(Y/Z/A)/PVG » au niveau EAL6 augmenté des composants ASE_TSS.2 et ALC_FLR.1, conforme au profil de protection [PP0035]. Cette bibliothèque a été certifiée le 11 juin 2015 sous la référence *NSCIB-CC-12-36243-CR2*.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 16 septembre 2015, 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 [CERT_IC]).

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 JAVA OS1 ChipDoc v1.0 SSCD (J3K080/J2K080) » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

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 puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. 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] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.
[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, la Suède et la Turquie.

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**	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 : - NXP JAVA OS1 ChipDoc v1.0 SSCD (J3K080/J2K080) – Security Target, Version 1.8, 20 août 2015, Athena. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - NXP JAVA OS1 ChipDoc v1.0 SSCD (J3K080/J2K080) – Security Target Lite, Version 1.8, 20 août 2015, Athena.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report PHOENIX-SSCD_ETR_v1.2 / 1.2, 16 septembre 2015, Serma Technologies.
[CONF]	Liste de configuration du produit : - Phoenix SSCD Docs Configuration List, version 1.4, 20 août 2015, Athena.
[GUIDES] [AGD_PRE]	Guide d'installation du produit : ChipDoc v1 SSCD – Preparation Manual, version 1.4, 20 août 2015, Athena.
[AGD_OPE]	Guide d'utilisation du produit : ChipDoc v1 SSCD – Operation Manual, version 1.4, 17 août 2015, Athena.
[PP-SSCD-Part2]	Protection profiles for secure signature creation device – Part 2: Device with key generation, référence : prEN 14169-1:2009, version 1.03. *Certifié par le BSI le 11 décembre 2009 sous la référence BSI-CC-PP-0059-2009.*
[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.*
[PP0035]	Protection Profile, Security IC Platform Protection Profile, version 1.0, juin 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*
[CERT_IC]	Certification Report BSI-DSZ-CC-0897-V2- 2014 for NXP Secure Smart Card ControllerP60D080/052/040yVC(Z/A)/yVG including IC Dedicated Software MIFARE Plus MF1PLUSx0 or MIFARE Plus MF1PLUSx0 and MIFARE DESFireEV1 from NXP Semiconductors Germany GmbH, 24 octobre 2014, BSI. Certification Report NSCIB-CC-12-36243-CR2 Crypto Library V1.0 on P60x080/052/040PVC(Y/Z/A)/PVG, TÜV Rheinland Nederland B.V.

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 CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, 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 1.3, février 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.