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-2020/76

ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration (Version 3.1.3.52)

Paris, le 30 juillet 2020

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-2020/76

Nom du produit

ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration

Référence/version du produit

Version 3.1.3.52

Conformité à un profil de protection

Protection profiles for secure signature creation device :

Part 2: Device with key generation, v2.0.1, certifié BSI-CC-PP-0059-2009-MA-01 le 21 février 2012;
Part 3: Device with key import, v1.0.2, certifié BSI-CC-PP-0075-2012 le 27 septembre 2012 ;
Part 4: Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, certifié BSI-CC-PP-0071-2012 le 12 décembre 2012 ;
Part 5: Extension for device with key generation and trusted communication with signature creation application, v1.0.1, certifié BSI-CC-PP-0072-2012 le 12 décembre 2012 ;
Part 6: Extension for device with key import and trusted communication with signature creation application, v1.0.4, certifié BSI-CC-PP-0076-2013 le 16 avril 2013.

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur

NXP Semiconductors N.V.

Troplowitzstrasse 20,
22529 Hamburg, Allemagne

Commanditaire

NXP Semiconductors N.V.

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.

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 directeur général de l'Agence national 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 matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est « ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration, Version 3.1.3.52 » développé par NXP Semiconductors N.V..

Ce produit offre des services d'authentification et de signature électronique (SSCD[1]) conformes à la directive [1999/93/EC]. Il est embarqué sur la plateforme *Java Card* [CER_PLA] préalablement certifiée (voir [CER_PLA]) qui est laissée ouverte après personnalisation. Il dispose d'interfaces avec et/ou sans contact.

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], [PP-SSCD-Part3], [PP-SSCD-Part4], [PP-SSCD-Part5] et [PP-SSCD-Part6].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la génération ou l'import de donnée de création de signature (SCD) et les données de vérification de signature correspondante (SVD) ;
- l'export des SVD pour la certification à travers un canal de confiance vers l'autorité de certification (CGA) dans le cas où les SVD ont été générées par le produit ;
- la preuve d'identité en tant que SSCD à des entités externes ;
- en option, la réception et le stockage de certificats ;
- l'initialisation des données d'authentification d'utilisateurs (RAD) ;
- le basculement du SSCD d'un état non opérationnel à un état opérationnel, et dans un état opérationnel, la génération de signatures digitales avec le processus suivant :
    - sélection d'une SCD s'il y en a plusieurs sur le produit ;
    - réception des données à signer ou de leur représentation unique à travers un canal de confiance ;
    - authentification du signataire et détermination de son intention de signer ;
    - application de la fonction de génération de signature appropriée.

1.2.3. Architecture

Le produit est constitué :

- de l'application ChipDoc V3.1 en configuration SSCD ;
- du système d'exploitation JCOP 4 en version 4.7 et révision 1.00.4 ou 1.01.4 (certifié sous la référence NSCIB-CC-180212_2, voir [CER_PLA]) ;

[1] *Secure Signature Creation Device.*

- et du microcontrôleur « NXP Secure Smart Card Controller N7121 avec son *firmware* et sa bibliothèque cryptographique dédiés » (certifié sous la référence BSI-DSZ-CC-1040, voir [CER_IC]).

Cette architecture est résumée sur la figure suivante :

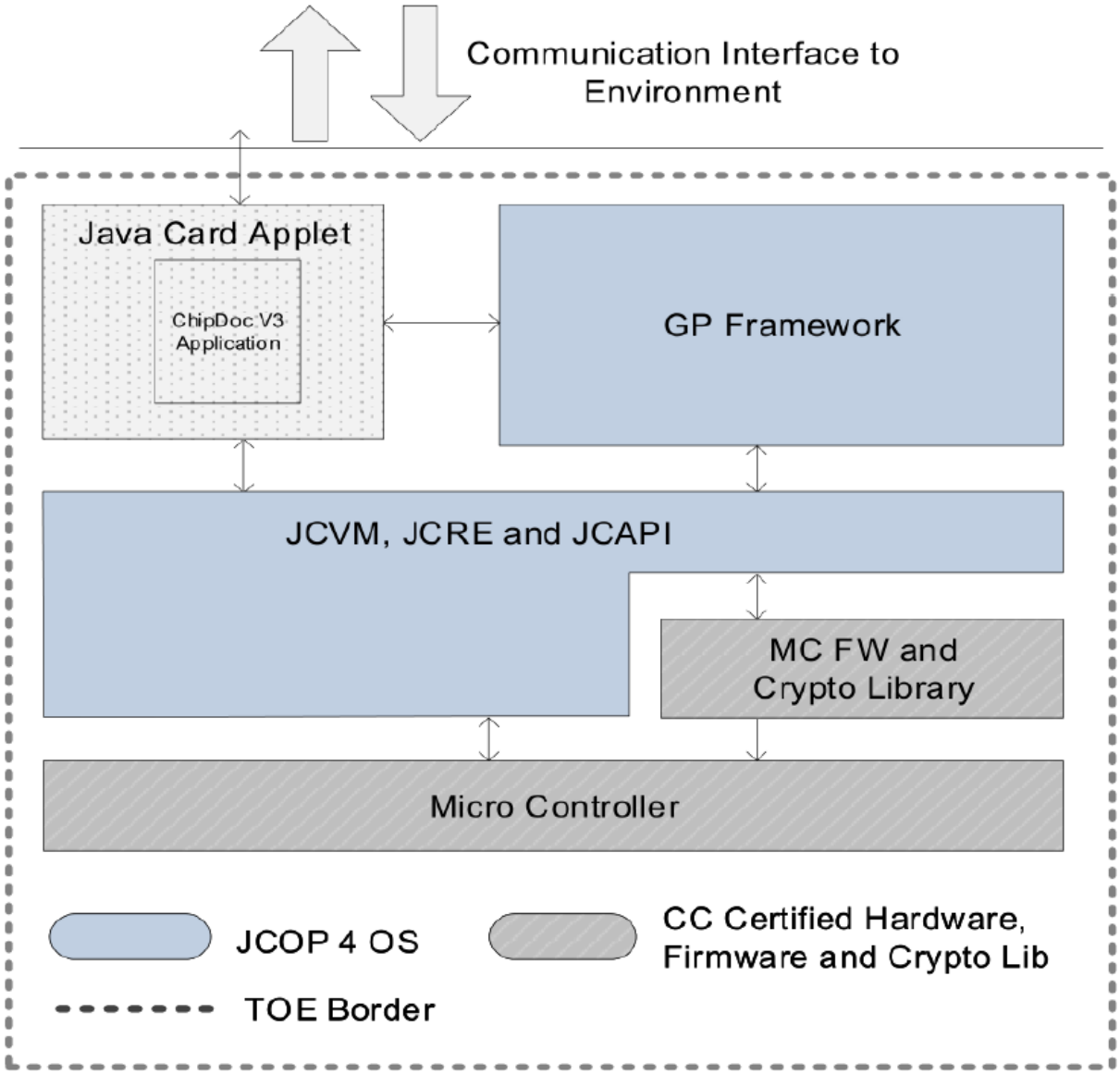

Figure 1. Architecture

La plateforme n'étant pas fermée après personnalisation, d'autres applications peuvent être chargées sur le produit, mais aucune ne l'est par défaut.

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 suivants :

- l'applet est identifiée en réponse à la commande GET_DATA par les données suivantes :
  - nom du produit (tag 0100) : 0x43686970446F63 (ChipDoc) ;
  - version du produit (tag 0116) : 0x03010352 (version 3.1.3.52) ;
  - *card capabilities* (tag 0118) : 0x00036FEF :
    - RSA, AES, *Active Authenticate*, BAC ;

        - création de DF, DH ;
- la plateforme est identifiée en réponse à la commande GET_DATA (IDENTIFY) par les données suivantes :
    - 0x4A335233531303146413945303430 30DD0984593B0048EF pour JCOP 4 P71 v4.7 R1.00.4 ;
    - 0x4A335233531303233363331303430 30DCE5C19CFE6D0DCF pour JCOP 4 P71 v4.7 R1.01.4 ;
- la configuration en SSCD de l'application est identifiée par la présence du préfixe E828BD080F dans le fichier EF.DIR.

1.2.5. Cycle de vie

Le cycle de vie du produit, décrit au chapitre 1.3.3 de la cible de sécurité (voir [ST]), est le suivant :

- la phase de développement qui inclut :
    - la phase de design au cours de laquelle le microcontrôleur, ses logiciels dédiés et guides sont développés ;
    - la phase de fabrication où le cœur du système d'exploitation est masqué en ROM ;
    - la phase d'intégration des parties matérielles et *firmware* dans le corps du produit ;
    - la phase d'initialisation au cours de laquelle le système d'exploitation est configuré, l'applet est instanciée et les deux sont éventuellement *patchés* ;
- la phase opérationnelle qui inclut :
    - la phase de personnalisation qui peut être effectuée par soit le développeur soit par une partie tierce ;
    - la phase d'usage qui correspond au moment où l'utilisateur utilise le produit pour générer des signatures électroniques avancées.

Le logiciel applicatif du produit a été développé sur le site suivant :

NXP Gratkorn

Mikron-Weg 1
A-8101 Gratkorn
Autriche

Les autres sites de développement correspondant aux autres phases de développement du produit sont listés dans les rapports de certifications du microcontrôleur et de la plateforme (voir [CER_IC] et [CER_PLA]).

1.2.6. Configuration évaluée

Le certificat porte sur la configuration SSCD du produit.

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.
Aucune autre application autre que ChipDoc v3.1 connue n'est chargée par défaut sur le produit.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 5** [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 sur la plateforme déjà certifiée par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme « ***JCOP 4 P71*** » au niveau EAL6 augmenté des composants ASE_TSS.2 et ALC_FLR.1, conforme au profil de protection [PP_JCS]. Cette plateforme a été certifiée le 20 mars 2020 sous la référence NSCIB-CC-180212_2, voir [CER_PLA].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 17 juin 2020, 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 a été réalisée. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations suivantes doivent être suivies :

- le mécanisme de *secure messaging* avec clés symétriques est conforme avec les recommandations cryptographiques de l'ANSSI si AES est utilisé. Si DES est utilisé, l'utilisation est conforme aux recommandations de l'agence jusqu'à fin 2020 seulement si l'usage d'une même clé est limité à 2^{20} ;
- le mécanisme de génération de signature est conforme aux recommandations cryptographiques de l'ANSSI si :
  - SHA-256 est utilisé,
  - si la signature RSA est utilisée, la taille du modulus est d'au moins 2048 bits pour une conformité jusqu'en 2030, 3072 bits ensuite,
  - si la signature ECDSA est utilisée, la taille du sous-groupe est d'au moins 200 bits pour une conformité jusqu'en 2020, 256 bits ensuite ;

- le mécanisme *Chip Authentication* est conforme aux recommandations cryptographiques de l'ANSSI si :
    - si l'échange de clés Diffie-Hellman est utilisé, la taille du modulus est d'au moins 2048 pour une conformité jusqu'en 2030, 3072 ensuite,
    - si l'échange de clés ECDH est utilisé, la taille du sous-groupe est d'au moins 200 bits pour une conformité jusqu'à fin 2020, 256 bits ensuite ;
- le mécanisme PACE est conforme aux recommandations cryptographiques de l'ANSSI si :
    - si l'échange de clés Diffie-Hellman est utilisé, la taille du modulus est d'au moins 2048 pour une conformité jusqu'en 2030, 3072 ensuite,
    - si l'échange de clés ECDH est utilisé, la taille du sous-groupe est d'au moins 200 bits pour une conformité jusqu'à fin 2020, 256 bits ensuite ;
- le mécanisme de génération de clés est conforme aux recommandations cryptographiques de l'ANSSI si :
    - dans le cas d'une clé RSA, la taille du modulus est d'au moins 2048 bits pour une conformité jusqu'en 2030, 3072 bits ensuite,
    - dans le cas d'une clé ECDSA, la taille du sous-groupe est d'au moins 200 bits pour une conformité jusqu'à fin 2020, 256 bits ensuite ;
- le mécanisme d'authentification externe avec clé symétriques est conforme aux recommandations cryptographiques de l'ANSSI si :
    - lorsque DES est utilisé, l'usage d'une même clé est limité à 2^{20} blocs chiffrés pour une conformité jusqu'à fin 2020,
    - lorsqu'AES est utilisé, l'usage d'une même clé est limité à 2^{64} blocs chiffrés.

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.

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]) puis lors de l'évaluation de la plateforme (voir [CER_PLA]).

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 v3.1 on JCOP 4 P71 in SSCD configuration, Version 3.1.3.52» 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 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], notamment :

- toutes les futures applications chargées sur ce produit (chargement post-émission) doivent respecter les contraintes de développement de la plateforme (voir [CER_PLA]) ;
- les autorités de vérification doivent appliquer le guide de la plateforme (voir [CER_PLA]) ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement post-émission) doit être activée conformément aux indications des guides de la plateforme (voir [CER_PLA]) ;
- les mécanismes PSO *Decrypt*, PSO *Encrypt*, d'authentification mutuelle et de *secure messaging* SCP03 ne sont pas inclus dans le périmètre de cette évaluation et ne doivent pas être utilisés.

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 :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

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[1], 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 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**	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	2	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	5	5	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - ChipDoc v3.1 on P71 in SSCD configuration – Security Target, révision 2.4, datée du 16 juin 2020, *NXP SEMICONDUCTORS.* Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration – Security Target Lite, révision 2.4, datée du 16 juin 2020, *NXP SEMICONDUCTORS.*
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report Project : ChipDoc_v3.1_SSCD, référence ChipDoc_v3.1_SSCD_ETR, révision 1.0, daté du 17 juin 2020, *THALES.*
[ANA-CRY]	Analysis of Cryptographic Mechanisms – Project : ChipDoc v3.1 SSCD, référence CDv3.1_SSCD_CRY, révision 1.0, daté du 26 juin 2020, *THALES.*
[CONF]	Liste de configuration du produit : - ChipDoc v3.1 ICAO - Configuration Item List, référence 2020_06_16_CIL_CDv3.1_P71_v3.1.3.52_SSCD, daté du 16 juin 2020, *NXP SEMICONDUCTORS* ; - ChipDoc v3.1 P71 – Life-Cycle Support CM Scope (ALC_CMS), révision 1.0, daté du 2 septembre 2019, *NXP SEMICONDUCTORS.*
[GUIDES]	Guide d'installation du produit : - ChipDoc 3.1 – SSCD Personalization Guide, version 2.1, daté du 3 juin 2020, *NXP SEMICONDUCTORS.* Guide d'utilisation du produit : - ChipDoc 3.1 – User Guide Manual, version 2.9, daté du 20 avril 2020, *NXP SEMICONDUCTORS.*
[CER_IC]	Rapport de certification, BSI-DSZ-CC-1040-2019 for NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library, 14 juin 2019. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-DSZ-CC-1040-2019.*
[CER_PLA]	Certification Report, JCOP 4 P71, version 1, 20 mars 2020. *Certifié par le NSCIB (Netherland Scheme for Certification in the Area of IT Security) sous la référence NSCIB-CC-180212_2.*
[PP_JCS]	Protection Profile, Java Card System – Open Configuration Protection Profile, version 3.0.5, 20 décembre 2017. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-0099-2017.*

[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-SSCD-Part4]	Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, référence : prEN 14169-4:2012, version 1.0.1 datée du 14 novembre 2012. *Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0071-2012.*
[PP-SSCD-Part5]	Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, référence : prEN 14169-5:2012, version 1.0.1 datée du 14 novembre 2012. *Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0072-2012.*
[PP-SSCD-Part6]	Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application, référence : prEN 14169-6:2013, version 1.0.4 datée du 3 avril 2013. *Certifié par le BSI le 16 avril 2013 sous la référence BSI-CC-PP-0076-2013.*
[1999/93/EC]	Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (e-Signatures Directive).

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, 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, version 3.0, avril 2019.
[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.
[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.