



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-2020/09

ChipDoc v3 on JCOP 4 P71 in ICAO EAC with PACE configuration (Version 3.0.0.52)

Paris, le 14 février 2020

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

Guillaume POUPARD
[ORIGINAL SIGNÉ]



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-2020/09

Nom du produit

**ChipDoc v3 on JCOP 4 P71 in ICAO EAC with PACE
configuration**

Référence/version du produit

Version 3.0.0.52

Conformité à un profil de protection

**Machine Readable Travel Document with “ICAO Application”,
Extended Access Control with PACE, Version 1.3.2**

certifié BSI-CC-PP-0056-V2-2012-MA-02 le 5 décembre 2012

**Machine Readable Travel Document using Standard Inspection
Procedure with PACE, Version 1.01**

certifié BSI-CC-PP-0068-V2-2011-MA-01 le 22 juillet 2014

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.

Tropowitzstrasse, 22529 Hamburg, Allemagne

Commanditaire

NXP Semiconductors N.V.

Tropowitzstrasse, 22529 Hamburg, Allemagne

Centre d'évaluation

THALES / CNES

290 allée du Lac, 31670 Labège, 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 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 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>	7
1.2.4. <i>Identification du produit</i>	8
1.2.5. <i>Cycle de vie</i>	8
1.2.6. <i>Configuration évaluée</i>	9
2. L’EVALUATION	10
2.1. REFERENTIELS D’EVALUATION	10
2.2. TRAVAUX D’EVALUATION	10
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	10
2.4. ANALYSE DU GENERATEUR D’ALEAS.....	10
3. LA CERTIFICATION	11
3.1. CONCLUSION	11
3.2. RESTRICTIONS D’USAGE.....	11
3.3. RECONNAISSANCE DU CERTIFICAT	11
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	11
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 « ChipDoc v3 on JCOP 4 P71 in ICAO EAC with PACE configuration, Version 3.0.0.52 » développé par NXP Semiconductors N.V..

Il s'agit de documents électroniques lisibles par une machine (MRTD) qui permettent trois types d'usage basés sur l'identité électronique :

- l'identification électronique (eID) ;
- le permis de conduire électronique (eDL) ;
- le passeport électronique (ePP).

L'usage du produit est fixé lors de la personnalisation du produit. La capacité de la plateforme à recevoir des applications post-émission (caractéristique d'ouverture de la plateforme) est déterminée en fonction du service sélectionné. En effet lorsque le produit est personnalisé comme passeport électronique la plateforme est fermée. A l'inverse, lorsque le produit est personnalisé comme permis de conduire électronique ou carte d'identité électronique, alors la plateforme reste ouverte.

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_EAC] et [PP_PACE].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection en intégrité et confidentialité des données du porteur stockées dans la carte : nations ou organisations émettrices, numéro du document électronique, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait, autres données optionnelles, données biométriques additionnelles et autres données permettant de gérer la sécurité du document électronique;
- le contrôle d'accès aux données du porteur stockées dans la carte ;
- la protection, en intégrité et en confidentialité, des données lues à l'aide du mécanisme *Secure Messaging* ;
- l'authentification du microcontrôleur par le mécanisme optionnel *Active Authentication* (AA) ;
- le mécanisme *Extended Access Control* (EAC) d'authentification forte entre le microcontrôleur et le système d'inspection, utilisé préalablement à tout accès aux données biométriques, et permettant l'établissement d'un canal sécurisé (*secure messaging*) ;
- le mécanisme *Password Authenticated Connection Establishment* (PACE) pour d'une part l'authentification, et d'autre part l'établissement d'un canal sécurisé entre le microcontrôleur et le système d'inspection (*secure messaging*).

1.2.3. Architecture

Le produit est constitué :

- de l'application ChipDoc V3 en configuration ICAO EAC avec PACE ;
- 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, voir [CER_PLA]) ;
- 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 :

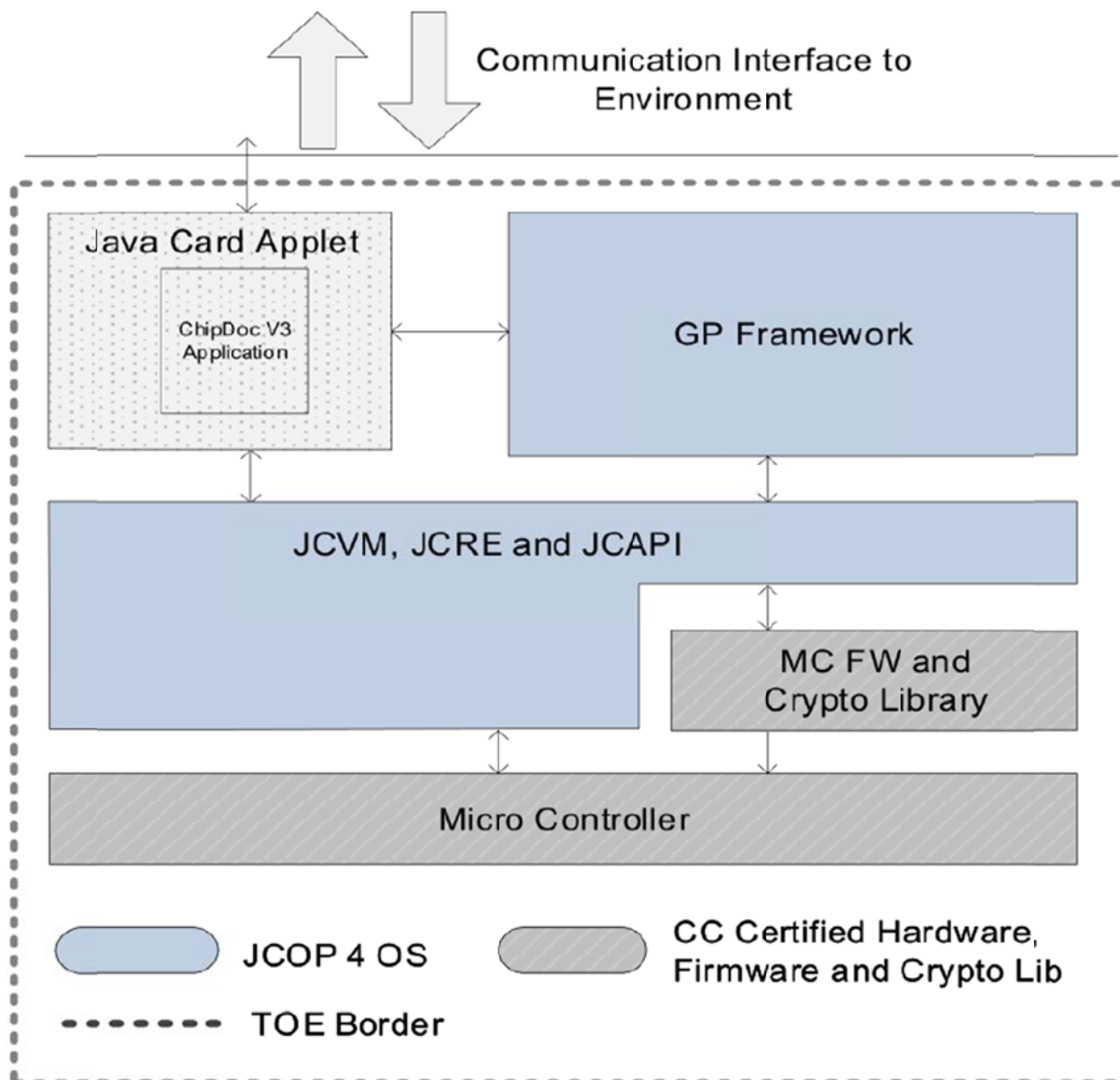


Figure 1. Architecture

Plusieurs instanciations de l'application peuvent coexister sur le produit selon la configuration choisie.

Dans le cas où la plateforme ne serait pas fermée (personnalisation ICAO pour de l'identité électronique ou du permis de conduire électronique) 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 :
 - o nom du produit (tag 0100) : 0x43686970446F63 (ChipDoc) ;
 - o version du produit (tag 0116) : 0x03000052 (version 3.0.0-52);
 - o *card capabilities* (tag 0118) : 0x00036FEF :
 - ECC, RSA, AES, PACE avec MRZ et CAN, EAC v1, *Active Authenticate*, BAC ;
 - création de DF, PACE *mapping* DH, PACE ECDH, PACE *mapping* CAM, *secure messaging* complet ;
 - EAC v2, PACE avec PIN et PUK ;
- la plateforme est identifiée en réponse à la commande GET_DATA (IDENTIFY) par les données suivantes :
 - o 0x4A335233353130314641394530343030DD0984593B0048EF pour JCOP 4 P71 v4.7 R1.00.4 ;
 - o 0x4A335233353130323336333130343030DCE5C19CFE6D0DCF pour JCOP 4 P71 v4.7 R1.00.4.

1.2.5. Cycle de vie

Le cycle de vie du produit suit le cycle en quatre phases (sous-divisés en sept étapes) décrit dans [PP_PACE]. Ce cycle est également décrit dans la cible de sécurité (voir [ST]). Il est résumé dans la figure suivante :





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 ICAO EAC avec PACE. Cette configuration se décline en trois usages qui peuvent être instanciés :

- passeport électronique, auquel cas le produit est fermé ;
- permis de conduire électronique, auquel cas la plateforme reste ouverte ;
- identification électronique, auquel cas la plateforme reste également ouverte.

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 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], 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 23 juillet 2019 sous la référence NSCIB-CC-190212, voir [CER_PLA].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 12 février 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 selon le référentiel technique de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilité 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]) 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 on JCOP 4 P71 in ICAO EAC with PACE configuration, Version 3.0.0.52 » 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 composant(s) 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]) ;

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 :

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 signataires¹, 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	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"> - ChipDoc v3 on P71 in ICAO EAC with PACE configuration – Security Target, révision 1.5, datée du 7 octobre 2019, <i>NXP SEMICONDUCTORS</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"> - ChipDoc v3 on JCOP 4 P71 in ICAO EAC with PACE configuration – Security Target Lite, revision 1.0, datée du 12 février 2019, <i>NXP SEMICONDUCTORS</i>.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Evaluation Technical Report Project : ChipDoc_v3_EAC, référence ChipDoc_v3_EAC_ETR, révision 4.0, daté du 12 février 2020, <i>THALES</i>.
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - ChipDoc v3 ICAO - Configuration Item List, référence 2019_10_08_CIL_CDv3_P71_ICAO, daté du 8 octobre 2019, <i>NXP SEMICONDUCTORS</i> ; - ChipDoc v3 P71 – Life-Cycle Support CM Scope (ALC_CMS), révision 1.0, daté du 2 septembre 2019, <i>NXP SEMICONDUCTORS</i>.
[GUIDES]	<p>Guide d'installation du produit :</p> <ul style="list-style-type: none"> - ChipDoc 3.0 – ICAO Personalization Guide, version 2.5, daté du 20 août 2019, <i>NXP SEMICONDUCTORS</i>. <p>Guide d'utilisation du produit :</p> <ul style="list-style-type: none"> - ChipDoc 3.0 – User Guide Manual, version 2.5, daté du 7 octobre 2019, <i>NXP SEMICONDUCTORS</i>.
[CER_IC]	<p>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. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-DSZ-CC-1040-2019.</i></p>
[CER_PLA]	<p>Certification Report, JCOP 4 P71, version 1, 23 juillet 2019. <i>Certifié par le NSCIB (Netherland Scheme for Certification in the Area of IT Security) sous la référence NSCIB-CC-180212.</i></p>
[PP_JCS]	<p>Protection Profile, Java Card System – Open Configuration Protection Profile, version 3.0.5, 20 décembre 2017. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0084-2014.</i></p>



[PP_EAC]	Protection Profile, Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP), version 1.3.2, 5 décembre 2012. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0056-V2-2012-MA-02.</i>
[PP_PACE]	Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), version 1.01, 22 juillet 2014. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0068-V2-MA-2011.</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, 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.