Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-2020/47

# ChipDoc v2 on JCOP 3 P60 in ICAO EAC with PACE configuration (Version v7b4_2)

*Paris, le 22 juillet 2020*

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

# 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-2020/47

*Nom du produit*

# ChipDoc v2 on JCOP 3 P60 in ICAO EAC with PACE configuration

*Référence/version du produit*

# Version v7b4_2

*Conformité à un profil de protection*

## BSI-CC-PP-0056-V2-2012, [PP EAC], version 1.3.0

**Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE**

## BSI-CC-PP-0068-V2-2011-MA-01, [PP PACE], version 1.01

**Machine Readable Travel Document using Standard Inspection Procedure with PACE**

*Critères d'évaluation et version*

## Critères Communs version 3.1 révision 4

*Niveau d'évaluation*

## EAL 5 augmenté

**ALC_DVS.2, AVA_VAN.5**

*Développeur*

## NXP Semiconductors

**Troplowitzstrasse 20, 22529 Hamburg, Allemagne**

*Commanditaire*

## NXP Semiconductors

**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 v2 on JCOP 3 P60 in ICAO EAC with PACE configuration, Version v7b4_2 » développé par NXP Semiconductors.

Le produit certifié est de type « carte à puce » avec et sans contact. Il implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (ICAO). Ce produit est destiné à permettre la vérification de l'authenticité du document de voyage et à identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels. Le produit final peut prendre différentes formes, de carte ou de module, 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 strictement conforme au profil de protection [PP-EAC] et au profil de protection [PP-PACE].

### *1.2.2. Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- la protection en intégrité des données du porteur stockées dans la carte : nations ou organisations émettrices, numéro du document de voyage, 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 de voyage ;
- le contrôle d'accès aux données du porteur stockées dans la carte ;
- l'authentification du microcontrôleur par le mécanisme « *Active Authentication* » ou « *Chip Authentication* » ;
- l'authentification entre le document de voyage et le système d'inspection lors du contrôle aux frontières par le mécanisme « *Supplemental Access Control* » (PACE) ;
- la protection, en intégrité et en confidentialité, à l'aide du mécanisme de « *Secure Messaging* », des données lues ;
- l'authentification forte (avec validation de la chaine de certificats) entre le microcontrôleur et le système d'inspection par le mécanisme EAC (« *Extended Access Control* ») préalablement à tout accès aux données biométriques.

### *1.2.3. Architecture*

Le produit est constitué :

- d'un microcontrôleur « P6022y VB* » ([CER IC]) et de sa bibliothèque cryptographique V3.1 ([CER LIB)] ;

- d'un système d'exploitation « JCOP 3 SECID P60 (OSB) », comportant une machine virtuelle Java Card, et utilisé comme plateforme fermée ([CER PLA]) ;
- de l'*applet* « ChipDoc P60 on JCOP3 P60 in ICAO EAC with PACE configuration, version v7b4_2 ».

La version v7b4_2 de l'applet couvre la version v7b4 avec le patch optionnel ID 1 déjà certifiée ([CER APP]), à laquelle se rajoutent le patch optionnel ID 3.

### *1.2.4. Identification du produit*

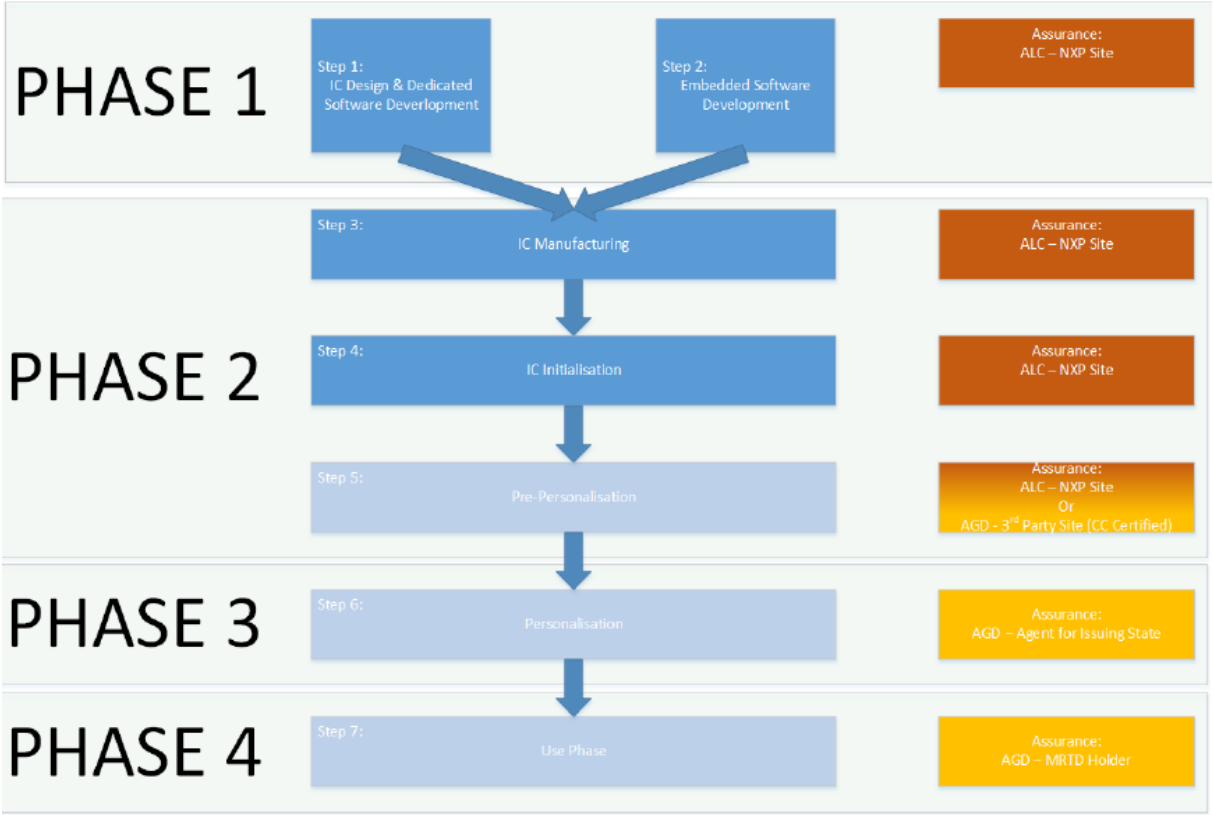
Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

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). La réponse attendue étant 00 07 00 04 en l'absence de patch, 00 07 01 04 avec le patch ID 1 ou 00 07 03 04 avec le patch ID 3 ;
- l'identification de la plateforme et du composant tel que décrit en section 2.1 de [CER PLA].

### *1.2.5. Cycle de vie*

Le cycle de vie du produit est le suivant est tel que celui en quatre phases (divisées en sept étapes) décrit dans [PP BAC]. Il est adapté lors de l'étape de pré-personnalisation afin de supporter le patching de la plateforme sur site certifié.
Ce cycle est illustré dans la figure suivante :



Le produit a été développé sur les sites suivants (voir [SITES]) :

Développement logiciel :
**NXP SEMICONDUCTORS - Site de Livingston**
6 Amondvale Business Park, Almondvale Way,
Livingston, EH54 6GA,
Royaume Uni

Tests logiciels et rédaction des guides utilisateur :
**NXP SEMICONDUCTORS - Site de San Jose**
411 East Plumeria Drive
San Jose, CA 95134
Etats-Unis d'Amérique

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

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

### *1.2.6. Configuration évaluée*

Le certificat porte sur le produit pour lequel :

- durant la phase « Initialisation » du cycle de vie, l'applet 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 EAC ou SAC :
    - EAC : le système de fichiers contient une clé BAC, la clé permettant le *Chip Authentication*, et optionnellement la clé liée à l'*Active Authentication*, des données publiques et des données sensibles (informations biométriques).
    - SAC : le système de fichiers est celui de la configuration EAC, auquel s'ajoutent des clés liées à SAC (dans la partie Master File) et des données (dans l'ADF dédié).

# 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 sur la plateforme déjà certifiée par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « ***JCOP 3 SECID P60 (OSB)*** » au niveau EAL5 augmenté des composants AVA_VAN.5, ALC_DVS.2, ASE_TSS.2 et ALC_FLR.1 (sur composant P6022J VB), conforme au profil de protection [PP JC]. Cette plateforme a été certifiée le 14 janvier 2020 sous la référence NSCIB-CC-98209-CR4, voir [CER PLA].
L'évaluation s'appuie sur les résultats d'évaluation du produit « ChipDoc P60 on JCOP 3 SECID P60 (OSB) ICAO EAC avec AA, CA et PACE masqué sur composant P6022J VB » certifié le 20 novembre 2017 sous la référence ANSSI-CC-2017/63, voir [CER APP].
Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 6 juillet 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]).
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 v2 on JCOP 3 P60 in ICAO EAC with PACE configuration, Version v7b4_2» 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].

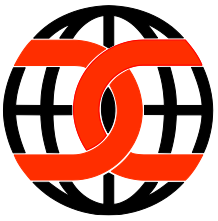
L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 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 | 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 :<br>- ChipDoc v2 on JCOP 3 P60 in ICAO EAC with PACE configuration Security Target, révision 1.7, 1 avril 2020, *NXP SEMICONDUCTORS.*<br><br>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :<br>- ChipDoc v2 on JCOP 3 P60 in ICAO EAC with PACE configuration Security Target Lite, révision 1.1, 1 avril 2020, *NXP SEMICONDUCTORS.* |
| [RTE] | Rapport technique d'évaluation :<br>- Evaluation Technical Report Project – ChipDoc V2 Re-evalution, référence ChipDocV2_RE_ETR, version 7.0, du 6 juillet 2020, *THALES.* |
| [CONF] | Liste de configuration du produit :<br>- 2020_01_04_CIL_CDv2_P60_v7b0304_ICAO, 1er avril 2020, *NXP SEMICONDUCTORS*. |
| [GUIDES] | - ChipDoc v7b4 applet in ICAO Personalization guide, référence 406917, version 1.7, 1 avril 2020, *NXP SEMICONDUCTORS* ;<br>- ChipDoc v7b4 applet in ICAO configuration – Preparation and Operation Manual, référence 414119, version 1.9, 1 avril 2020, *NXP SEMICONDUCTORS*. |
| [SITES] | Rapports d'analyse documentaire et d'audit de site pour la réutilisation :<br>- Site Technical Audit Report – NXP LIVINGSTON 2, version 1.0, référence NXP_LIVINGSTON_STAR_v1.0, *SERMA SAFETY & SECURITY*. |
| [PP EAC] | Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE, version 1.3.0, 20 janvier 2012.<br>*Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0056-V2-2012.* |
| [PP PACE] | Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE, version 1.01, 22 juillet 2014.<br>*Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0068-V2-2011-MA-01*. |
| [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.<br>*Certifié par le BSI sous la référence BSI-DSZ-CC-1059-V3-2019 le 29 novembre 2019.* |
| [CER PLA] | NXP JCOP 3.<br>*Certifié par le NSCIB sous la référence NSCIB-CC-98209-CR4 le 4 janvier 2020.* |
| [CER LIB] | Crypto Library V3.1.x on P6022y VB.<br>*Certifié par le NSCIB sous la référence NSCIB-CC-67206-CR3 le 29 mai 2018.* |
| [CER APP] | ChipDoc P60 on JCOP 3 SECID P60 (OSB) ICAO EAC avec AA et CA masqué sur composant P6022J VB (version v7b4).<br>*Certifié par l'ANSSI sous la référence ANSSI-CC-2017/63 le 20 novembre 2017.* |

# 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 :<br>- Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001;<br>- Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002;<br>- 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 3.0, avril 2019. |
| [COMP] * | Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.5.1, mai 2018. |
| [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.