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-2020/37

LDS Applet EAC with PACE on ID-One Cosmo V8.2 on NXP P60D145 (version 03 00 00 00)

Paris, le 24 juin 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-2020/37

Nom du produit

LDS Applet EAC with PACE on ID-One Cosmo V8.2 on NXP P60D145

Référence/version du produit

Version de l'application : 06 70 01 2F

Version commerciale de l'application : 03 00 00 00

Identification de la plateforme : 091121

Identification des patch : 094222 et 094741

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

Développeurs

IDEMIA

2 place Samuel de Champlain
92400 Courbevoie, France

NXP Semiconductors GmbH

Troplowitzstrasse 20, 22529 Hamburg, Allemagne

Commanditaire

IDEMIA

2 place Samuel de Champlain
92400 Courbevoie, France

Centre d'évaluation

CEA - LETI

17 avenue des martyrs, 38054 Grenoble Cedex 9, 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 « LDS Applet EAC with PACE on ID-One Cosmo V8.2 on NXP P60D145, version 03 00 00 00 » développé par *IDEMIA* et *NXP SEMICONDUCTORS GMBH*.

Le produit évalué est de type « carte à puce » pouvant être utilisé en modes 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 ou d'identité 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, dans une *eCover* ou dans une *eDatapage*. 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 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 décrits au chapitre 2.1.3 de la cible de sécurité [ST]. Ils comprennent notamment :

- 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 forte (avec validation de la chaîne de certificats) entre le microcontrôleur et le système d'inspection par le mécanisme EAC (« *Extended Access Control* ») ;
- le mécanisme *Password Authenticated Connection Establishment* (PACE) pour (1) l'authentification entre le microcontrôleur et le système d'inspection, et (2) l'établissement d'un canal sécurisé fort (*Secure Messaging*) ;
- la protection, en intégrité et en confidentialité, à l'aide du mécanisme de « *Secure Messaging* », des données lues.

1.2.3. Architecture

L'architecture du produit est décrite au chapitre 2.3 de la cible de sécurité [ST]. Elle est constituée :

- du microcontrôleur P60D145 (P6022y VB), développé par *NXP SEMICONDUCTORS GMBH* et certifié sous la référence [CER-IC] ;
- de la plateforme *Java Card* ouverte « ID-One Cosmo v8.2 Platform » développée par *IDEMIA* et certifiée sous la référence [CER-PTF] ;
- des *patchs* « LDS V10.1 optional code » et « Optional Code generic DLATCH on Cosmo v8.2 » chargés sur la plateforme et développés par *IDEMIA* ;
- de l'*applet* « LDS V10.1 » développée par *IDEMIA* .

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 :

- la sélection de l'application ;
- la lecture du code SAAAAR et de la version commerciale de l'application obtenue par la commande GET DATA avec le tag DF 66. La réponse attendue est DF 66 0A **06 70 01 2F 03 00 00 00 00 00** ;
- la lecture de la version interne de l'application obtenue par la commande GET DATA avec le tag DF 67. La réponse attendue est : DF 67 04 0A 00 09 0B ;
- la lecture de l'identifiant du *patch* « LDS V10.1 optional code » par la commande GET DATA avec le tag DF 52 ;
- l'identification de la plateforme, du *patch* « Optional Code generic DLATCH on Cosmo v8.2 » et du composant telle que décrite dans le paragraphe 1.2.4 de [CER-PTF].

La version certifiée du produit est identifiable par les éléments du tableau ci-après, détaillés dans la cible de sécurité [ST] aux chapitres 1.2 et 1.3 :

Eléments de configuration		**Origine**
Nom de la TOE	LDS V10.1 in EAC configuration with PACE on ID-One Cosmo V8.2	*IDEMIA*
Nom du produit	LDS Applet EAC with PACE on ID-One Cosmo V8.2 on NXP P60D145	
Identification de l'application	06 70 01 2F (code SAAAAR) 03 00 00 00 (version commerciale)	
Identification des *patchs*	09 47 41 (Optional Code r1.0 LDS V10.1 on Cosmo v8.2) 09 42 22 (Optional Code generic DLATCH on Cosmo v8.2)	
Identification de la plateforme	091121	

1.2.5. Cycle de vie

Le cycle de vie est décrit au chapitre 3 de la cible de sécurité [ST]. Il est décomposé en sept phases conformes au [PP0084].

	Phase	Acteur	Couvert par
Phase 1	Développement du logiciel embarqué	*IDEMIA*	ALC
Phase 2	Développement du microcontrôleur	*NXP SEMICONDUCTORS GMBH*	ALC
Phase 3	Fabrication du microcontrôleur	*NXP SEMICONDUCTORS GMBH*	ALC
Phase 4	Conditionnement (*packaging*) du produit	*IDEMIA*	AGD_PRE
Phase 5	Pré-Personnalisation	*IDEMIA*	AGD_PRE
Phase 6	Personnalisation	Personnalisateur	AGD_PRE
Phase 7	Utilisation opérationnelle	Utilisateur final	AGD_OPE

La livraison de la TOE s'opère à la fin de la phase 3. Après cette phase, elle est considérée comme auto-protégée.

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

***IDEMIA* – Courbevoie** [CRB] 2, place Samuel de Champlain 92400 Courbevoie, France	***IDEMIA* – Pessac** [PSC] Bâtiment Elnath, 11 avenue de Canteranne, 33600 Pessac, France
***IDEMIA* – Manila** [MNL] 19F BPI – Philam Life Makati Building, 6811 Ayala Ave., 1209 Makati City, Philippines	

Les sites de développement du microcontrôleur et de la plateforme sont couverts par les certificats [CER-IC] et [CER-PTF].

1.2.6. Configuration évaluée

Le certificat porte sur le produit identifié au paragraphe 1.2.4. et configuré comme suit :

- l'*applet* « LDS V10.1 in EAC configuration with PACE on ID-One Cosmo V8.2 » est instanciée sur la plateforme ouverte couverte par le certificat [CER-PTF] ;
- les recommandations du guide [GUIDES] sont strictement appliquées durant la phase « Personnalisation » du cycle de vie, ainsi que dans la phase de pré-personnalisation.

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.

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 (voir [CER-PTF]).
Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme « ID-One Cosmo V8.2 » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5. Cette plateforme a été certifiée le 16 juin 2020 sous la référence ANSSI-CC-2020/26, voir [CER-PTF].

L'évaluation s'appuie sur les résultats d'évaluation du produit « LDS Applet EAC with PACE on ID-One V8.2 Platform on NXP P60D145 (version 03 00 00 00) » certifié en novembre 2019 sous la référence ANSSI-CC-2019/49, voir [CER-JAS].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 8 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 conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Afin que les mécanismes analysés soient conformes aux exigences des référentiels cryptographiques de l'ANSSI ([REF]), les recommandations du guide [JAR_GCQR] doivent être respectées.
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]).
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 (voir [CER-PTF]).
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 « LDS Applet EAC with PACE on ID-One Cosmo V8.2 on NXP P60D145, version 03 00 00 00 » 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 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], notamment :

- le développement des applications sensibles doit respecter les contraintes listées dans [AGD-Dev_Sec] ;
- les autorités de vérification doivent appliquer les exigences définies au chapitre *TOE Guidance* de la cible de sécurité [ST] sur toutes les applications chargées sur ce produit ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement *post-issuance*) doit être activée conformément aux indications décrites dans les guides [AGD_ALP] et [AGD_PLF].

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 :

1La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.
2La 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 : - Security Target JASON-R2 EAC with PACE, référence FQR 550 0014, version 8, 03/06/2020, *IDEMIA*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - LDS V10.1 Applet in EAC with PACE Configuration Public Security Target, référence FQR 550 0077, version 4, 03/06/2020, *IDEMIA*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – JASON-R2, référence LETI.CESTI.JAR.ETR.001 – V2.3, 08/06/2020, *CEA-LETI*.
[ANA-CRY]	Cotation des mécanismes cryptographiques – JASON-R, référence LETI.CESTI.JAR.RT.001-V1.0, 06/09/2019, *CEA-LETI*.
[CONF]	Liste de configuration du produit : - JASON-R2 – Configuration List, référence FQR 220 1428, version 7, 03/06/2020, *IDEMIA*.
[GUIDES] [JAR_GCQR] [AGD-Dev_Sec] [AGD_ALP] [AGD_PLF]	Guide d'installation du produit : - JASON-R2 – Guidance Document – Preparative Procedures, référence FQR 220 1424, version 5, 03/06/2020, *IDEMIA*. Guide d'utilisation du produit : - JASON-R2 – Guidance Document – Operational user guidance, référence FQR 220 1425, version 3, 07/02/2020, *IDEMIA* ; - LDS V10 on ID-One Cosmo V8.2 Platform – Recommandations pour la compatibilité avec le référentiel de qualification renforcée, référence FQR 110 9321, version 2, 23/10/2019, *IDEMIA*. Guide d'installation et d'administration de la plateforme : - ID-One Cosmo V8.2 on P60D145 – Applet Security Recommandations, référence FQR 110 8963, version 4, 18/03/2019, *IDEMIA* ; - ID-One Cosmo V8.1-n Application Loading Protection Guidance, référence FQR 110 8001, version 1, 11/10/2016, *IDEMIA* ; - ID-One Cosmo V8.2 Reference Guide, référence FQR 110 8885, version 8, 02/06/2020, *IDEMIA* ; - ID-One Cosmo V8.2 Pre-perso Guide, référence FQR 110 8875, version 9, 02/06/2020, *IDEMIA*.

[SITES]	Rapports d'analyse documentaire : - IDEMIA Development Environment ALC Class Evaluation Report (Generic Documentary activities), référence IDEMIA R&D site 2018_GEN_v1.0, 29/11/2018, *SERMA SAFETY & SECURITY* ; - IDEMIA Development Environment ALC Class Evaluation Report (Generic Documentary activities), référence IDEMIA R&D site 2018_GEN_v1.1, 19/06/2019, *SERMA SAFETY & SECURITY*. Rapports d'audit de site pour la réutilisation : - [CRB] Site Technical Audit Report CRB, référence IDEMIA R&D site 2018_CRB_STAR_v1.3, 26/06/2019, *SERMA SAFETY & SECURITY* ; - [PSC] Site Technical Audit Report PSC, référence IDEMIA R&D site 2018_PSC_STAR_v1.2, 18/12/2019, *SERMA SAFETY & SECURITY* ; - [MNL] Site Technical Audit Report MNL, référence IDEMIA R&D site 2018_MNL_STAR_v1.2, 07/11/2019, *SERMA SAFETY & SECURITY*.
[CER-IC]	BSI-DSZ-CC-1059-2018 for NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software from NXP Semiconductors Germany GmbH. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 18 mai 2018, sous la référence BSI-DSZ-CC-1059-2018*.
	BSI-DSZ-CC-1059-V3-2019 for NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software from NXP Semiconductors Germany GmbH. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 29 novembre 2019, sous la référence BSI-DSZ-CC-1059-V3-2019*.
[CER-PTF]	Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145. *Certifié par l'ANSSI le 16 juin 2020 sous la référence ANSSI-CC-2020/26*.
[CER-JAS]	LDS Applet EAC with PACE on ID-One V8.2 Platform on NXP P60D145 (version 03 00 00 00). *Certifié par l'ANSSI le 13 novembre 2019 sous la référence ANSSI-CC-2019/49*.
[PP0084]	Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014*.

[PP EAC]	Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE, version 1.3.2, 5 décembre 2012. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0056-V2-2012-MA-02*.
[PP PACE]	Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE, version 1.01, 22 juillet 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0068-V2-2011-MA-01*.

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.