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-2017/20 eTravel 2.2 en configuration EAC sur SAC sur Plate-forme MultiApp v4.0

Paris, le 13 avril 2017

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

Colonel Emmanuel GERMAIN
[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-2017/20

Nom du produit

eTravel 2.2 en configuration EAC sur SAC sur Plate-forme MultiApp v4.0

Référence/version du produit

Version de l'application eTravel EAC on SAC : 2.2

Version de la plateforme Java Card MultiApp : 4.0

Conformité aux profils de protection

BSI-CC-PP-0056-V2, version 1.3.1

Machine Readable Travel Document with ICAO Application

BSI-CC-PP-0068-V2, version 1.0

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(s)

Gemalto

6 rue de la Verrerie,
92197 Meudon cedex, France

Infineon Technologies AG

AIM CC SM PS – Am Campeon 1-12,
85579 Neubiberg, Allemagne

Commanditaire

Gemalto

6 rue de la Verrerie,
92197 Meudon cedex, France

Centre d'évaluation

Serma Safety & Security

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

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL2.

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est l'application « eTravel 2.2 en configuration EAC sur SAC sur Plate-forme MultiApp v4.0 » développée par la société *GEMALTO* et embarquée sur le microcontrôleur M7892 G12 fabriqué par la société *INFINEON TECHNOLOGIES.*

Le produit implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (ICAO). Ce produit permet la vérification de l'authenticité du document de voyage et l'identification de son porteur notamment lors du contrôle frontalier, à l'aide d'un système d'inspection. Il est disponible en mode contact ou sans contact.

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels ou dans une carte plastique. Ils peuvent être intégrés sous forme de module ou d'*inlay*.

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 au profil de protection [PP-0056V2]. Il s'agit d'une conformité stricte. Le profil de protection [PP-0056V2] est strictement conforme au profil de protection [PP-0068V2]. La cible de sécurité est donc également strictement conforme à [PP-0068V2].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- ceux de la plateforme Java Card en configuration ouverte ou fermée de la carte à puce MultiApp V4.0 ;
- 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 optionnel « *Active 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 :
- du composant M7892 G12 fabriqué par *INFINEON TECHNOLOGIES* ;
- d'un système d'exploitation sous forme d'une plateforme ouverte ou fermée Java Card MultiApp V4.0. Cette plateforme est certifiée sous la référence [ANSSI-CC-2017/07] ;
- de l'application native passeport eTravel 2.2 en configuration EAC sur SAC.

Le produit s'appuie sur la librairie cryptographique développée par *GEMALTO*.

Des applications Java en dehors du périmètre de cette évaluation peuvent être chargées sur la plate-forme Java Card MultiApp V4. Toutes les applications qui sont chargées sur le produit devront respecter les guides [PLF_BADR] et [PLF_SADR].

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 présents dans la réponse que donne le produit à la commande *GET DATA* pour le tag '9F 7F' appliquée au fichier de données CPLC (voir [Guides]) :

Donnée	Valeur attendue
IC Fabricator	'40 90'
IC Type	'78 97'
Operating System Identifier	'B0 52 11'
Configuration	'00' configuration fermée '01' configuration ouverte
Operating System Release Level	'00 00'
Reference interne de la TOE (MKS Label)	MultiAppV40_EIR10_LBL05 Checkpoint 1.75

1.2.5. Cycle de vie

L'évaluation se limite aux étapes 1 à 5 correspondant aux phases 1 et 2, respectivement phase de développement et phase de fabrication telles que décrites dans le profil de protection [PP0084].

Deux cycles de vie décrits, au chapitre 2.4 de la cible de sécurité [ST] sont envisagés pour le produit dans le périmètre de l'évaluation :

- le cycle de vie 1 est le cas standard. Il correspond au cas où le composant est livré par *INFINEON* dans un site *GEMALTO* pour initialisation et pré-personnalisation. Les composants sont ensuite livrés au client directement ou après avoir été mis sous modules ou *inlays* ;
- le cycle de vie 2 est une alternative qui correspond au cas où *GEMALTO* reçoit les composants au format *inlays* pour initialisation et personnalisation. Pour cela, *INFINEON* a préalablement transmis les modules ou *wafers* au fabricant d'*inlays*.

Les sites de développement et de production du microcontrôleur sont identifiés dans le rapport de certification [CER-IC].

Au cours des opérations d'initialisation, *GEMALTO* effectue le chargement du logiciel embarqué comprenant l'application eTravel 2.2 et la plate-forme MultiApp V4.0 en utilisant le flash loader d'*INFINEON* protégé par une clé de transport spécifique.

Le produit a été développé sur les sites suivants :

GEMALTO Meudon 6 Rue de la Verrerie 92190 Meudon, France	*GEMALTO* Singapore 12 Ayer Rajah Crescent Singapor 139941, Singapour
GEMALTO Gémenos Avenue du Pic de Bretagne 13881 Gémenos, France	*GEMALTO* La Ciotat Avenue du Jujubier, ZI Athelia IV 13705 La Ciotat, France
ATOS Paris (Aubervilliers / Croissy) 4 rue des Vieilles Vignes 77 183 Croissy-Beaubourg, France	*ATOS* Bydgoszcz – (ATOS Poland) Biznes Park, ul. Kraszewskiego 1 85-240 Bydgoszcz, POLAND
GEMALTO Barcelona Poligono lndustrial Llevant CL Llevant 12, 08150 Parets del Valles,Barcelona Spain	*GEMALTO* Montgomery 101 & 106 Park Drive Montgomeryville, PA 18 936 United States
GEMALTO Curitiba Rodovia Dep. Leopoldo Jacomel, 13102 83323-410 Pinhais, PR Brazil	*GEMALTO* Vantaa Myllynkivenkuja 4, Vantaa, Finland, FI-01620
GEMALTO Tczew Ul. Skarszewska 2 33-110 Tczew, Pologne	*GEMALTO* Pont Audemer Z.l. Saint Ulfrant rue de Saint Ulkfrant 27500 Pont Audemer, France

Pour la configuration ouverte du produit, le guide [PLF_AGD_OPE] identifie également des recommandations relatives à la livraison des futures applications à charger via le système d'exploitation MultiApp V4 de cette carte.

Le guide [PLF_AGD_OPE] identifie également des recommandations relatives à la livraison des futures applications à charger via le système d'exploitation MultiApp V4 de cette carte.
Par ailleurs, les guides [PLF_BADR] et [PLF_SADR] décrivent les règles de développement des applications destinées à être chargées sur cette carte ; les guides [PLF_GTO_VA] et [PLF_THIRD_VA] décrivent les règles de vérification qui doivent être appliquées par l'autorité de vérification.

Les administrateurs du produit sont les nations ou organisations émettrices du document de voyage.

Les utilisateurs du produit sont les voyageurs et les systèmes d'inspection pendant la phase d'utilisation.

1.2.6. Configuration évaluée

Le certificat porte sur l'application eTravel 2.2 EAC sur SAC (avec mécanisme d'*Active Authentication*), sur la plateforme ouverte ou fermée MultiApp V4 masquée sur le composant, M7892 G12 telle que présentée plus haut au paragraphe 1.2.4.

Ce rapport de certification porte sur la configuration incluant les mécanismes suivants :
- *Extended Access Control* ;
- *Supplemental Access Control* ;
- *Active Authentication.*

L'évaluateur a testé la plateforme Java Card masquée sur le composant M7892 G12.

La cible d'évaluation a été évaluée selon les deux configurations suivantes :
- la configuration fermée qui correspond à un usage de l'application eTravel 2.2 EAC sur SAC seule ;
- la configuration ouverte qui correspond à un usage de l'application eTravel 2.2 EAC sur SAC parallèlement à d'autres applications *Java.*

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 et réalisé selon les processus audités ne remet pas en cause le présent rapport de certification.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « Infineon Security Controller M7892 Design Steps D11 and G12 with optional RSA2048/4096 v2.03.008, ECv2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries, symmetric crypto library v2.02.010 and with specific IC dedicated software (firmware) » au niveau EAL6 augmenté du composant ALC_FLR.1 conforme au profil de protection [PP0084]. Ce microcontrôleur a été certifié le 20/12/2016 sous la référence BSI-DSZ-CC-0891-V2-2016 (voir [CER-IC]).

L'évaluation s'appuie sur les résultats d'évaluation de la « Plateforme ouverte MultiApp V4.0 en configuration ouverte basée sur l'Operating System JLEP3 masquée sur le composant SLE78CLFX4000PH (M7892 G12) » certifiée le 8 mars 2017 sous la référence [ANSSI-CC-2017/07].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 22 février 2017, 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]. La cotation des mécanismes cryptographiques a été réalisée. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY].

Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI sous réserve de prendre en compte les recommandations se trouvant dans le manuel utilisateur [UM], dont les plus significatives sont rappelées ici :

- le bit le plus significatif de chaque nombre premier p et n utilisé pour la génération de clé doit être fixé à 1 ;
- l'algorithme de hachage doit être choisi en relation avec la taille de clés des courbes elliptiques ou de l'algorithme RSA si applicable, comme par exemple, l'usage du SHA-256 avec des clés ECC de 256 bits ;
- l'algorithme Diffie-Hellman d'échange de clés et de vérification de signature doit utiliser des clés de longueurs au moins égales à 2048 bits. L'ordre d'un sous-groupe doit être multiple d'un nombre premier d'au moins 200 bits et la conformité des paramètres de domaine avec la RFC 2785 doit être utilisée ;
- dans le cas des courbes elliptiques, pour une utilisation ne devant pas dépasser 2020, on emploiera des sous-groupes dont l'ordre est multiple d'un nombre premier d'au moins 200 bits (256 bits au-delà de 2020) ;
- l'algorithme TDES (Triple DES) 2 clés est utilisable au plus tard jusqu'en 2020 ;
- dans le cas de l'utilisation de l'algorithme TDES, la même clé ne peut être utilisée pour chiffrer plus de 2^{27} blocks.

Dans le cadre du processus de qualification renforcée, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI. Ces 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.
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 « eTravel 2.2 en configuration EAC sur SAC sur Plate-forme MultiApp v4.0 » 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], notamment :

- lors de la personnalisation, les valeurs « *Security Attributes* » indiquées dans [UM] doivent être utilisées afin que les conditions d'accès soient celles recherchées pour une configuration mettant en œuvre les fonctionnalités SAC, AA (optionnel) et EAC ;
- toutes les applications chargées sur ce produit doivent respecter les contraintes de développement de la plateforme (guides [PLF_BADR] et [PLF_SADR]) selon la sensibilité de l'application considérée ;
- les autorités de vérification doivent appliquer les guides [PLF_GTO_VAR] et [PLF_THIRD_VAR] ;
- la protection du chargement de toutes les applications sur ce produit doit être activée conformément aux indications de [PLF_AGD_PRE].

Les recommandations du chapitre « 2.3 Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI » du présent rapport devront également être mises en œuvre.

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 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 :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, la Pologne, le Royaume-Uni et la Suède.
[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**2**	Well-structured internals
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**4**	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**5**	Development tools CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**3**	Testing: modular design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - MultiApp V4 eTravel 2.2 EAC on SAC Security Target, référence D1384181, version 1.1, 2 février 2017, Gemalto. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target Lite - MultiApp V4 eTravel 2.2 EAC on PACE, référence D1384181, version 1.1p, février 2017, Gemalto.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – MINORIS MRTD Project, référence MINORIS-MRTD_ETR_v1.1, version 1.1, 21 février 2017, Serma Safety & Security.
[ANA-CRY]	Cotation des mécanismes cryptographiques : - Cryptographic Mechanisms Evaluation Report - MINORIS - MRTD Project, v1.0, MINORIS-MRTD_ETR_v1.0 / 1.0, 4 août 2016, Serma Safety & Security.
[CONF]	Liste de configuration du produit : - LIS: Configuration List for MRTD, référence : D1403184–LIS-DOC-MRTD MultiAppV4, version 1.1 du 2 février 2017, Gemalto.

[GUIDES] [AGD_PRE] [UM] [PM] [AGD_OPE] [GUIDES_PLF] [PLF_BADR] [PLF_SADR] [PLF_GTO_VA] [PLF_THIRD_VA] [PLF_AGD_PRE] [PLF_AGD_OPE]	- eTravel EAC 2.2, Preparative Guide, référence D1391898, version 1.0 du 7 avril 2016, Gemalto ; - eTravel EAC 2.2, CC Certified, référence Manual, réference D1392378A du 1er juillet 2016, Gemalto ; - Global Dispatcher Personalization Applet User Guide, référence D1390286A du 26 février 2016, Gemalto ; - eTravel EAC 2.2 Operational User Guide, référence D1391899, version 1.0 du 7 avril 2016, Gemalto ; - Rules for applications on Multiapp certified product ; référence D1390963, version 1.1 de juin 2016, Gemalto ; - Guidance for secure application development on Multiapp platforms, référence D1390326, version A01 de février 2016, Gemalto ; - Verification process of Gemalto non sensitive applet, référence D1390670, version A01 de février 2016, Gemalto ; - Verification process of Third Party non sensitive applet, référence D1390671, version A01 de février 16, Gemalto ; - MultiApp V4, Preparative Guide, référence D1390316, version 1.1 du 6 juin 2016, Gemalto ; - MultiApp V4, Operational User Guide, référence D1390321, version 1.2 du 15 février 2017, Gemalto.
[PP-0056-V2]	Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE (EAC PP), version 1.3.1, 22 mars 2012. *Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 26 mars 2012 sous la référence BSI-CC-PP-0056-V2-2012-MA-01.*
[PP-0068-V2]	Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE, Version 1.0, 2 novembre 2011. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0068-V2-2011.*

[ANSSI-CC-2017/07]	Plateforme Java Card MultiApp V4.0 en configuration ouverte basée sur l'Operating System JLEP3 masquée sur le composant SLE78CLFX4000PH (M7892 G12). *Certifiée par l'ANSSI le 8 mars 2017 sous la référence ANSSI-CC-2017/07.*
[PP0084-2014]	Protection Profile, Security IC Platform Protection Profile with augmentation packages, Version 1.0 du 13 janvier 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.*
[CER-IC]	Certification Report BSI-DSZ-CC-0891-V2-2016 for Infineon Security Controller M7892 Design Steps D11 and G12 with optional RSA2048/4096 v2.03.008, ECv2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries, symmetric crypto library v2.02.010 and with specific IC dedicated software (firmware) from Infineon Technologies AG. *Certifié par le BSI le 20 décembre 2016, sous la référence BSI-DSZ-CC-0891-V2-2016.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[JIWG IC]	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, janvier 2012.
[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.