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-2018/38

eTravel 2.4 en configuration EAC SAC sur plateforme ID Motion V2.0

Paris, le 27 septembre 2018

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-2018/38

Nom du produit

eTravel 2.4 en configuration EAC SAC sur plateforme ID Motion V2.0

Référence/version du produit

Version de l'application eTravel EAC SAC : 2.4

Version de la plateforme ID Motion : 2.0

Conformité à un profil de protection

BSI-PP-0056-V2-2012-MA-02, version 1.3.2

Machine Readable Travel Document with ICAO application, Extended Access Control with PACE

BSI-CC-PP-0068-V2-2011-MA-01, version 1.01

Machine Readable Travel Document using Standard Inspection Procedure with PACE

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(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

THALES (TCS – CNES)

290 allée du Lac, 31670 Labège, 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 « eTravel 2.4 en configuration EAC SAC sur plateforme ID Motion V2.0 » développé par les sociétés *GEMALTO* et *INFINEON TECHNOLOGIES AG*.

Le produit certifié est de type « carte à puce » avec ou 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 permet la vérification de l'authenticité du document de voyage et l'identification de son porteur notamment lors du contrôle aux frontières, à l'aide d'un système d'inspection.

Ce microcontrôleur et ses logiciels embarqués ont vocation à être insérés dans la couverture des passeports 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 strictement conforme aux profils de protection [PP-EACV2] et [PP-PACE].

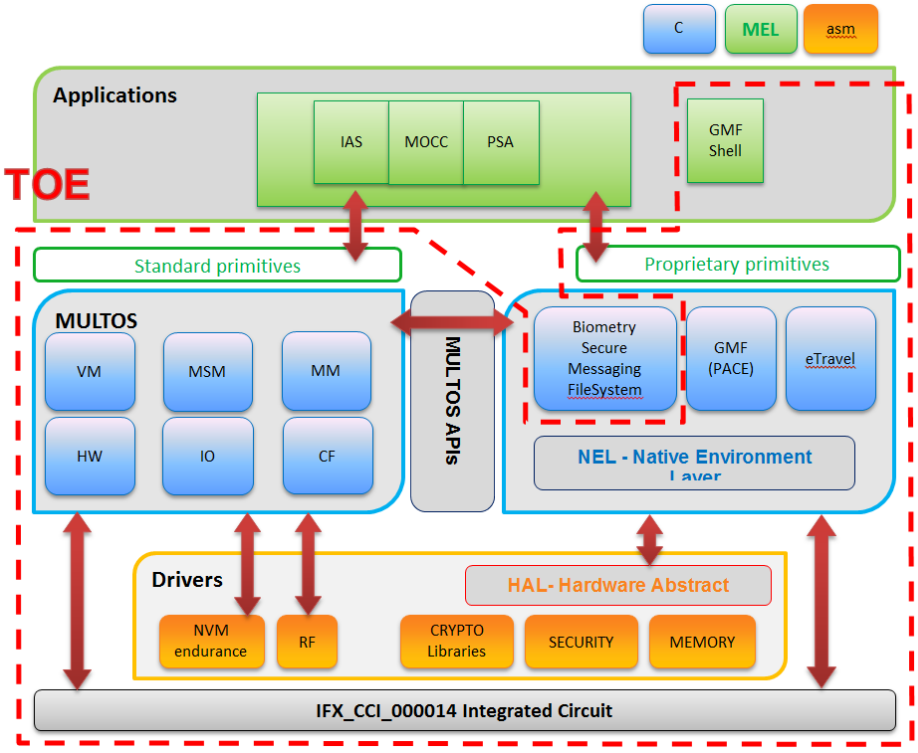
1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- ceux de la plateforme ouverte « IDMotion v2 avec OS MULTOS v4.5.2 » ;
- la protection en intégrité des données du porteur stockées dans la carte ;
- le contrôle d'accès aux données du porteur stockées dans la carte ;
- l'authentification du microcontrôleur par le mécanisme « *Active Authentication* » (AA) ;
- l'authentification entre le document de voyage et le système d'inspection lors du contrôle aux frontières par le mécanisme « *Supplemental Access Control* » (SAC) ;
- l'authentification forte (avec validation de la chaine de certificats) entre le microcontrôleur et le système d'inspection par le mécanisme « *Extended Access Control* » (EAC) préalablement à tout accès aux données biométriques ;
- la protection, en intégrité et en confidentialité des données lues à l'aide du mécanisme *Secure Messaging*.

1.2.3. Architecture

L'architecture du produit est la suivante :



VM: *Virtual Machine*
MSM: *Multos Security Manager*
MM: *Application Memory Manager Subsystem*
CF: *Cryptographic Functions subsystem*
IO: *I/O Communications subsystem*
HW: *Hardware Services subsystem*
NVM: *Non Volatile Memory*

Figure 1 – Architecture du produit

Le produit est constitué des éléments suivants :

- du microcontrôleur IFX_CCI_000014h précédemment certifié (voir [CER-IC]) ;
- de la plateforme ouverte « IDMotion v2 avec OS MULTOS v4.5.2 » certifiée sous la référence [CER-PLF] ;
- de l'application GMF[1] v1.0 ;
- de l'application native passeport eTravel v2.4 avec EAC SAC;
- du mécanisme AA.

Le produit s'appuie sur la librairie cryptographique développée par *GEMALTO* et les accélérateurs cryptographiques fournis par l'IC [CER-IC].

Les applications PSA[2] v0.2, IAS Classic v4.4.1C, *Biometry Secure Messaging Files System* et MOC[3] client v1.0.2A en dehors du périmètre, ont été vérifiées conformément aux prescriptions de [OPEN].

[1] *Global Master File.*
[2] *Pin Server Application.*
[3] *Match On Card – fingerprint storage.*

D'autres applications pourront être chargées sur cette plate-forme, elles devront respecter les [GUIDE].

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 à partir des éléments fournis au chapitre 1.3 « Identification » de la [ST].

Les applications présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans le tableau ci-après.

Nom, version de l'application	**Identification**	***Codelet checksum***
IAS classic v4.4.1C	0x00B8	F11BAD70
MOC client v1.0.2A	0x00B9	5BA450E4
PSA v0.2	0x00B7	E77DF2A1

Tableau 1 : Applications chargées dans le produit

La commande GET CONFIGURATION DATA (*Codelet*) permet à l'utilisateur du produit de vérifier quelles applications sont installées dans le produit à sa disposition.

1.2.5. Cycle de vie

Le cycle de vie du produit, détaillé au chapitre 2.4.2 «*TOE Life Cycle* » de la cible de sécurité [ST].

Les différents rôles d'utilisateur sont décrits au chapitre 4.1.2 de la cible de sécurité [ST].

1.2.6. Configuration évaluée

Le certificat porte sur la configuration telle que présentée au paragraphe 1.2.3.

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.
Toutes les applications identifiées dans le Tableau 1 ont été vérifiées conformément aux contraintes décrites dans [GUIDES].

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 [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 [CER-PLF].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 13 juillet 2018, 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 vulnérabilités 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 (voir [CER-PLF]).
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 2.4 en configuration EAC SAC sur plateforme ID Motion V2.0 » soumise 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 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 :

[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 : - eTravel EAC-SAC Security Target, référence ST_D1430932, version 1.92, 10/3/2018, *GEMALTO*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - IDMotion V2 eTravel v2.4 EAC-SAC Security Target Lite, référence ST_D1430932_P, version 1.1, *GEMALTO*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – BOLERO_B, référence BOLB_ETR, version 2.0, 13/7/2018, *THALES COMMUNICATIONS & SECURITY SAS*.
[CONF]	Liste de configuration du produit : - LIS__ceryneia.CC-delivery_004, *GEMALTO*; - LIS__cceryneia.Ccdoc-Labo-delivery_001, *GEMALTO*.
[GUIDES]	- Card Initialization Specification – Multos ID Motion V2, référence D1459742, version 1.5, 20/3/2017, *GEMALTO* ; - eTravel V2.4Multos on ID Motion V2.0 (CC EAL5+), référence D1445504A, 20/12/2017, *GEMALTO* ; - GMF ALU Personalization Specification, référence D1418828, version 1.0.18, 1/12/2017, *GEMALTO* ; - Multos MDRM - Multos Developer's Reference Manual, référence MAO-DOC-TEC-006, version 1.54, *GEMALTO* ; - Multos GALU - Guide to Generating Application Load Units, référence MAO-DOC-TEC-009, version 2.9, *GEMALTO* ; - Multos GLDA - Guide to Loading and Deleting, reference MAO-DOC-TEC-008, version 2.28, *GEMALTO*.
[PP-EACV2]	Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE, version 1.3.2, 5/12/2012 *Certifié et maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0056-V2-2012-MA-02.*
[PP-PACE]	Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE, Version 1.01, 22/7/2014. *Certifié et maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0068-V2-2011-MA-01.*
[CER-PLF]	Plateforme ouverte IDMotion V2 masquée sur le composant IFX_CCI_000014h, OS Multos V4.5.2, AMD version 0151v001. *Certifiée par l'ANSSI le 30/08/2018 sous la référence ANSSI-CC-2018/35.*

[PP0084]	Protection Profile, Security IC Platform Protection Profile with augmentation packages, Version 1.0 du 13/1/2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.*
[CER-IC]	Certification Report BSI-DSZ-CC-0945-2017 for Infineon Security Controller IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch and IFX_CCI_00001Dh design step H13 including optional software libraries and dedicated firmware. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 10/7/2017, sous la référence BSI-DSZ-CC-0945-2017.*

Annexe 3. Références liés 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 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.4, août 2015.
[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.