PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2020/83

eTravel Essential 1.0 avec SAC, AA et EAC activés sur composants M7794 A12/G12 (identifiant : B2 8C 01, version 01 02)

Paris, le 15 décembre 2020

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ Ti 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-2020/83

Nom du produit

eTravel Essential 1.0 avec SAC, AA et EAC activés sur composants M7794 A12/G12

Référence/version du produit

identifiant : B2 8C 01, version 01 02

Conformité à un profil de protection

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

BSI-CC-PP-0056-V2-2012, [PP EAC], version 1.3.2

Machine Readable Travel Document using Standard Inspection Procedure with PACE

BSI-CC-PP-0068-V2-2011, [PP PACE], version 1.0

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

THALES
6 rue de la Verrerie 92190
Meudon, France

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

Commanditaire

THALES
6 rue de la Verrerie 92190
Meudon, France

Centre d'évaluation

SERMA SAFETY & SECURITY
14 rue Galilée, CS 10071,
33608 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat est reconnu au niveau EAL2.

PREFACE

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

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

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

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « eTravel Essential 1.0 avec SAC, AA et EAC activés sur composants M7794 A12/G12, identifiant : B2 8C 01, version 01 02 » développé par THALES et INFINEON TECHNOLOGIES AG.

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. Ils peuvent être livrés sous forme de module, d'inlay, de couverture de passeport ou de passeport. Le produit final peut également être au format carte plastique.

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 INFINEON M7794 A12/G12 et du logiciel Firmware fournis par INFINEON ;*
- *du logiciel embarqué « eTravel Essential v1.0 » développé par THALES.*

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 du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre.

Commande produit	Réponse	Description
GET DATA « 0x9F7F »	*40 90*	*Identification du fabricant*
	77 50	*Identifiant du microcontrôleur*
	B2 8C 01	*Identification du logiciel embarqué*
	01 02	*Identification de la version du logiciel embarqué*

La procédure d'identification est décrite dans le guide « eTravel Essential 1.0 and 1.1 – Reference Manual » (voir [GUIDES]).

1.2.5 Cycle de vie

Le cycle de vie du produit est décrit au premier chapitre de la cible de sécurité [ST].

Trois types de cycle de vie 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 THALES pour initialisation et pré-personnalisation. Les composants sont ensuite livrés au client directement ou après avoir été mis sous inlays ;*
- *le cycle de vie 2 est une première alternative qui correspond au cas où THALES reçoit les composants au format inlays pour initialisation et personnalisation. Pour cela, INFINEON a préalablement transmis les modules au fabricant d'inlays ;*
- *le cycle de vie 3 est une seconde alternative qui correspond au cas où le client souhaite recevoir des composants directement d'INFINEON Dans ce cas les opérations d'initialisation et de pré-personnalisation sont effectuées sur un site d'INFINEON.*

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

Meudon	**Singapore**
6 Rue de la Verrerie	*12 Ayer Rajah Crescent*

92190 Meudon *France*	*Singapor 139941* *Singapour*
Géménos *Avenue du Pic de Bertagne* *13881 Gémenos* *France*	**Calamba** *Barangay Batino* *Calamba City, 4027 Laguna* *Philippines*
ATOS *153 avenue Jean Jaures* *93307 Aubervilliers Cedex,* *France*	**ATOS** *4 rue des vieilles vignes* *77183 Croissy Beaubourg,* *France*
Pune *Software Technology Park, MIDC* *Talawade, 411062 Pune* *India*	**La Ciotat** *Avenue du Jujubier* *ZI Athelia IV, 13705 La Ciotat,* *France*

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

1.2.6 Configuration évaluée

Le certificat porte sur la configuration, après personnalisation par l'émetteur, qui inclut les mécanismes suivants :

- *Extended Access Control;*
- *Supplemental Access Control;*
- *Active Authentication.*

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 dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « M7794 A12 / G12 » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PP0084]. Ce microcontrôleur a été certifié le 28 mai 2019 sous la référence BSI-DSZ-CC-0964-V4-2019, voir [CERT_IC].

L'évaluation s'appuie sur les résultats d'évaluation du produit « eTravel Essential 1.0, avec SAC, AA et EAC activés, sur composant M7794 A12/G12 » certifié le 10 septembre 2015 sous la référence ANSSI-CC-2015/32, voir [CER].

*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 a été réalisée. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations suivantes doivent être suivies :

- *la "Mutual Authentication for personalisation phase" doit être faite avec la commande P2 valant "83" ;*
- *EAC doit être éxécuté avec l'AES ;*
- *PACE doit être éxécuté avec l'AES ;*
- *RSA et DH doivent utiliser des clés d'au moins 2048 bits jusqu'en 2030, et d'au moins 3072 bits après ;*
- *ECDSA et ECDH doivent utiliser des clés d'au moins 256 bits.*

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 [CERT_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 Essential 1.0 avec SAC, AA et EAC activés sur composants M7794 A12/G12, identifiant : B2 8C 01, version 01 02 » 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 :

3.3.2 Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

[1] *La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.*

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 :

[2] *La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.*

ANNEXE A. 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	2	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 B. Références documentaires du produits évalué

[ST]	*Cible de sécurité de référence pour l'évaluation :* - *Erodium2: eTravel Essential 1.0 EAC on PACE Security Target, reference : D1315455, version 1.7, 10 juin 2020, THALES.* *Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :* - *eTravel Essential 1.0 EAC on PACE Security Target Lite, reference : D1315455, version 1.7p, THALES.*
[RTE]	*Rapport technique d'évaluation :* - *Evaluation Technical report ERODIUM2, référence : ERODIUM2_ETR_v1.0, version 1.0, du 06/07/2020.*
[ANA-CRY]	*Voir [RTE]*
[CONF]	*Liste de configuration du produit :* *D1338129-LIS-DOC-eTravelEssential10, version 1.5, 10/06/2020, THALES.*
[GUIDES]	- *eTravel Essential 1.0 AGD_PRE document, version 1.2, février 2020, référence : D1330275 ;* - *eTravel Essential 1.0 Operational User Guide, version 1.1, février 2020, référence : D1330276 ;* - *eTravel Essential 1.0 and 1.1, version E.5, octobre 2019, référence : D1325786.*
[SITES]	*Rapports d'audit de site pour la réutilisation :* - *Site Technical Audit Report – GEM VZN site audit, version 1.0, juilliet 2019 ;* - *Site Technical Audit Report – CAL-VZN site audit, version 1.0, juilliet 2019 ;* - *Site Technical Audit Report – MDN, version 1.1, novembre 2019 ;* - *Site Technical Audit Report ATOS_PAR, version 1.0, août 2018 ;* - *Site Technical Audit Report – PUN2, version 1.2, mars 2020 ;* - *Site Technical Audit Report – TCZEW site audit, version 1.0, décembre 2018 ;* - *Site Technical Audit Report VAN, version 1.0, mai 2019 ;* - *Development Environment GEMENOS Site Visit Lite Report, version 1.1, novembre 2018 ;* - *Development Environment Singapore Site Visit Lite Report, version 1.0, mai 2018 ;* - *Development Environment LA CIOTAT Site Visit Lite Report, version 1.1, novembre 2018.*
[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 (EAC PP), version 1.3.2, 5 décembre 2012.* *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 (PACE PP), 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.*
[CER]	*eTravel Essential 1.0, avec SAC, AA et EAC activés, sur composant M7794 A12/G12.* *Certifié le 10 septembre 2015 sous la référence ANSSI-CC-2015/32.*
[CERT_IC]	*BSI-DSZ-CC-0964-V4-2019 for Infineon Technologies Security Controller M7794 A12/G12 with optional RSA2048/4096 v1.02.013 or V2.00.002, EC v1.02.013 or v2.00.002 and Toolbox v1.02.013 or v2.00.002 libraries and with specific IC dedicated software.* *Certifié par le BSI le 28 mai 2019 sous la référence BSI-DSZ-CC-0964-V4-2019.*

ANNEXE C. 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 and similar devices, 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.*
	Gestion des clés cryptographiques — Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.
	Authentification — Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), 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.*