



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-2014/77

eTravel Essential 1.0, configuration "full" avec application PACE

Paris, le 30 octobre 2014

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

Contre-amiral Dominique RIBAN
[ORIGINAL SIGNE]



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 présumées 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.anssi@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	ANSSI-CC-2014/77	
Nom du produit	eTravel Essential 1.0, configuration "full" avec application PACE	
Référence/version du produit	Version 1.0	
Conformité à un profil de protection	Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE (EAC PP) Version 1.3.2, BSI-CC-PP-0056-V2-2012-MA-02 Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) Version 1.0, BSI-CC-PP-0068-V2-2011	
Critères d'évaluation et version	Critères Communs version 3.1 révision 4	
Niveau d'évaluation	EAL 5 augmenté ALC_DVS.2, AVA_VAN.5	
Développeurs	Gemalto 6 rue de la verrerie, 92197 Meudon, France	Infineon Technologies AG AIM CC SM PS – Am Campeon 1-12, 85579 Neubiberg, Allemagne
Commanditaire	Gemalto 6 rue de la verrerie, 92197 Meudon, France	
Centre d'évaluation	Serma technologies 14 rue Galilée, CS – 10055, 33615 PESSAC Cedex, France	
Accords de reconnaissance applicables	CCRA 	SOG-IS 
Le produit est reconnu au niveau EAL4.		

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	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Introduction</i>	6
1.2.2. <i>Identification du produit</i>	6
1.2.3. <i>Services de sécurité</i>	6
1.2.4. <i>Architecture</i>	7
1.2.5. <i>Cycle de vie</i>	7
1.2.6. <i>Configuration évaluée</i>	8
2. L’EVALUATION	9
2.1. REFERENTIELS D’EVALUATION.....	9
2.2. TRAVAUX D’EVALUATION	9
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	9
2.4. ANALYSE DU GENERATEUR D’ALEAS.....	9
3. LA CERTIFICATION	10
3.1. CONCLUSION.....	10
3.2. RESTRICTIONS D’USAGE.....	10
3.3. RECONNAISSANCE DU CERTIFICAT	11
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	11
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	11
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....	12
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	13
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	14

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce fermée « eTravel Essential 1.0, configuration "full" avec application PACE ». Le produit est développé par la société Gemalto et embarqué sur le microcontrôleur M7794 A12/G12 de la société Infineon Technologies.

Le produit évalué 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 (OACI¹). 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 conforme au profil de protection [PP0056V2]. Il s'agit d'une conformité stricte. Le profil de protection [PP0056V2] est strictement conforme au profil de protection [PP0068V2]. La cible de sécurité est donc également strictement conforme à [PP0068V2].

1.2.2. 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 10 premiers octets de l'élément *CPLC DO* : la valeur attendue est 0x40907750B28C01000102. L'élément *CPLC DO* est obtenu par la commande *GETDATA* avec le tag 0x9F7F. Cette procédure d'identification est décrite dans [GUIDES].

1.2.3. 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

¹ Encore appelé ICAO pour *International Civil Aviation Organization*.

- 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 chaîne de certificats) entre le microcontrôleur et le système d'inspection par le mécanisme EAC (« Extended Access Control ») préalablement à tout accès aux données biométriques.

1.2.4. Architecture

Le produit est constitué de :

- un microcontrôleur Infineon M7794 A12/G12 (par exemple en configuration SLE77CLFX2400P) avec du logiciel *Firmware* fourni par Infineon ;
- un logiciel embarqué 'eTravel Essential v1.0 O.S' développé par Gemalto et comprenant :
 - o un niveau 'plateforme native' implémentant les services de bas-niveau, communs à plusieurs produits Gemalto ;
 - o un niveau 'applications' implémentant les fonctionnalités *MRTD*¹ dédiées à ce produit et stockant les données associées.

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit au premier chapitre de la cible de sécurité [ST]. Il est composé de deux variantes selon que l'*inlay* est fabriqué avant ou après la livraison.

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

La cible d'évaluation (*TOE*) est également développée ou produite sur les sites suivants :

Gemalto

6 Rue de la Verrerie
92190 Meudon
France

Gemalto

Avenue du Pic de Bertagne
13881 Gémenos
France

Gemalto

12 Ayer Rajah Crescent
Singapor 139941
Singapour

Gemalto

Avenue du Jujubier
13705 La Ciotat Cedex
France

¹ *Machine Readable Travel Document.*

Gemalto

Myllynkivenkuja 4
FI-01620 Vantaa
Finlande

Gemalto

Ul. Skarszewska 2
Pologne

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 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.

Le microcontrôleur M7794 A12/G12 a été certifié au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conformément au profil de protection [PP0035], le 3 février 2014 sous la référence BSI-DSZ-CC-0917-2014. Ce microcontrôleur a été maintenu sous la référence BSI-DSZ-CC-0917-2014-MA-01 le 12 juin 2014.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 19 septembre 2014 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 [CERT_IC]).

L'analyse de vulnérabilité indépendante réalisée dans le cadre de l'évaluation du produit final n'a pas mis 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, configuration "full" avec application PACE » 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 d'utiliser, lors de la personnalisation, les valeurs 'Security Attributes' indiquées afin que les conditions d'accès soient celles recherchées.

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'accord¹, 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. 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 signataires², des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 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, 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, 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]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> – eTravel Essential 1.0 EAC Security Target, D13154553 version 1.2, 12 septembre 2014, Gemalto. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> – Security target Lite eTravel Essential 1.0 EAC on PACE, version 1.2p, référence D1315455, Gemalto.
[RTE]	<p>Rapport technique d'évaluation :</p> <p>Evaluation Technical Report : ERODIUM Project , référence ERODIUM-FULL_ETR_v1.1 / 1.1, 19 septembre 2014, Serma Technologies.</p>
[CERT_IC]	<p>Infineon Technologies Security Controller M7794 A12 and 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.</p> <p><i>Certifié par le BSI le 3 février 2014 sous la référence BSI-DSZ-CC-0917-2014, et maintenu le 12 juin 2014 sous la référence BSI-DSZ-CC-0917-2014-MA-01.</i></p>
[CONF]	<p>Liste de configuration du produit :</p> <p>eTravelEssential10, référence D1388129-LIS-DOC eTravelEssential10, version 1.1, 8 août 2014, Gemalto.</p>
[GUIDES]	<ul style="list-style-type: none"> – eTravel Essential 1.0 AGD_PRE document, référence D1330275, version 1.0, 23 mai 2014, Gemalto ; – eTravel Essential 1.0 Operational User Guide, reference D1330276, version 1.0, 23 mai 2014, Gemalto ; – eTravel Essential 1.0 Reference Manual, reference D1325786, 15 septembre 2014, Gemalto.
[PP0035]	<p>Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.</i></p>
[PP0068V2]	<p>Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.0, 2 novembre 2011. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0068-V2-2011.</i></p>
[PP0056V2]	<p>Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), version 1.3.2, 5 décembre 2012. <i>Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0056-V2-2012-MA-02.</i></p>

Annexe 3. Références liées à la certification

<p>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.</p>	
[CER/P/01]	<p>Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.</p>
[CC]	<p>Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.</p>
[CEM]	<p>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, révision 4, ref CCMB-2012-09-004.</p>
[JIWG IC] *	<p>Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009.</p>
[JIWG AP] *	<p>Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, January 2013.</p>
[COMP] *	<p>Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.</p>
[CC RA]	<p>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 2014.</p>
[SOG-IS]	<p>« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.</p>
[REF]	<p>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), voir www.ssi.gouv.fr.</p>

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.