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-2017/42v2

Annule et remplace le rapport de certification ANSSI-CC-2017/42 pour en réduire la portée

eTravel Essential 1.1 (EACv1 and AA activated)

Paris, le 24 janvier 2022

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

Guillaume POUPARD

[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 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-2017/42v2

Nom du produit

eTravel Essential 1.1

Référence/version du produit

EACv1 and AA activated

Conformité à un profil de protection

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

Version 1.10, BSI-CC-PP-0056-2009

Critère d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

THALES DIS
6 rue de la verrerie,
92197 Meudon, France

SAMSUNG ELECTRONICS CO.
17 Floor, B-Tower, 1-1 Samsungjeonja-ro
Hwaseong-si, Gyeonggi-do
445-330 Corée du Sud

Commanditaire

THALES DIS
6 rue de la verrerie,
92197 Meudon, France

Centre d'évaluation

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

Accords de reconnaissance applicables

CCRA

Ce certificat est reconnu au niveau EAL2

SOG-IS

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 1.1, EACv1 and AA activated » développé par THALES DIS sur un microcontrôleur de SAMSUNG ELECTRONICS CO.

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 (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 conforme au profil de protection [PP EAC]. Il s'agit d'une conformité stricte.

Dans le cadre particulier de cette certification, qui correspond à une évaluation avec réduction de portée (voir [NOTE25]), la cible de sécurité [ST] identifie clairement les évolutions du périmètre d'évaluation par rapport à celui de la certification initiale (voir [CER]). Ici, la réduction de portée correspond au retrait de la fonctionnalité PACE-CAM du périmètre d'évaluation.

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont décrits en section *1.4.3 TOE usage and security features for operational use* de la cible de sécurité [ST].

1.2.3 *Architecture*

Le produit est constitué :

- du microcontrôleur et de ses logiciels dédiés développés par SAMSUNG ELECTRONICS (*IC, IC Dedicated Software*) ;
- du système d'exploitation et de l'application MRTD développés par THALES DIS (*Embedded Software*).

1.2.4 *Identification du produit*

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La méthode d'identification du produit est présentée dans [GUIDES].

La version certifiée puis maintenue (voir [R-M01]) du produit est identifiable par les éléments suivants :

Donnée	Valeur attendue
Hardmask Identifier	0xB28C03
Softmask Number	0x01
Softmask Version	0x04

1.2.5 *Cycle de vie*

Le cycle de vie du produit est présenté au chapitre 1.4.4 de la cible de sécurité [ST].

NB : Dans le cadre particulier de cette certification, qui correspond à une évaluation avec réduction de portée, la validité des audits de site n'a pas été vérifiée.

1.2.6 *Configuration évaluée*

Le présent rapport de certification porte sur la configuration, après personnalisation par l'émetteur, qui inclut les mécanismes suivants :

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

Le présent rapport de certification porte également sur la configuration du produit obtenue sans activer le mécanisme optionnel *Active Authentication.*

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel [CEM] et aux dispositions de [NOTE25].

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 s'appuie sur les résultats d'évaluation de ce même produit certifié le 14 août 2017 sous la référence ANSSI-CC-2017/42, voir [CER]. Elle correspond à une évaluation avec réduction de portée suite à l'identification d'une vulnérabilité.

L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat [CER] n'a pas été conduite dans le cadre de cette réévaluation partielle. Le niveau de résistance d'un produit certifié se dégrade au cours du temps. Seule une réévaluation ou une surveillance de cette version du produit permettrait de maintenir le niveau de confiance dans le temps.

Le CESTI en charge de l'évaluation initiale a émis un rapport d'analyse de réduction de portée (référence [RTE_part]) pour réévaluer les composants d'assurance impactés par l'évolution de la cible de sécurité du produit.

Le rapport technique d'analyse de réduction de portée [RTE_part], remis à l'ANSSI le 19 octobre 2021, pour réévaluer les composants d'assurance ASE, ADV, ALC (hors audits), et ATE impactés par l'évolution de la cible de sécurité [ST] détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

Le rapport technique [RTE_init], remis à l'ANSSI le 11 juillet 2017 détaille les travaux initialement réalisés menés par le centre d'évaluation et atteste que la résistance du produit atteignait VAN.5 lors de son édition.

Le produit a été maintenu sous la référence [R-M01] sans impact sur le niveau de confiance certifié initialement le 14 août 2017.

2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

L'analyse cryptographique qui avait été réalisée lors de l'évaluation initiale, voir [CER], n'a pas été reconduite malgré les évolutions du référentiel dans le cadre de la présente réévaluation partielle.

2.4 Analyse du générateur d'aléa

Les résultats de l'évaluation initiale relatifs au générateur d'aléa, voir [CER], n'ont pas fait l'objet de travaux lors de la présente réévaluation.

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 soumis à l'évaluation conformément à [NOTE25], répond aux caractéristiques de sécurité spécifiées dans la cible de sécurité [ST] pour le niveau d'évaluation visé à la date de certification initiale (voir [CER]). Pour rappel, les travaux d'analyse de la réduction de portée sont centrés sur l'impact de cette réduction de portée sur les tâches de conformité de l'évaluation initiale. La résistance globale du produit aux attaques de l'état de l'art n'a pas été mise à jour depuis la certification initiale.

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 dans leur paragraphe « *Key size recommendations (RGS from ANSSI)* » et dans leurs notes « *To comply with French RGS from ANSSI* ».

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 :

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

3.3.2 *Reconnaissance internationale critères communs (CCRA)*

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

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. Références documentaires du produit évalué

[CER]	Rapport de certification ANSSI-CC-2017/42, eTravel Essential 1.1, configuration EACv1 et AA, 14 août 2017.
[R-M01]	Rapport de maintenance ANSSI-CC-2017/42-M01, eTravel Essential 1.1 (version 01.04), BAC, EAC and AA activated, 24 janvier 2019.
[ST]	Cible de sécurité de référence pour l'évaluation : - *eTravel Essential 1.1 – BAC, EAC and AA activated, Security Target, D1382407 v1.12*, 31 août 2021, THALES DIS. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *eTravel Essential 1.1 – BAC, EAC and AA activated Security Target Lite, D1382407 v1.12p*, 31 août 2021, THALES DIS.
[RTE] [RTE_init] [RTE_part]	Rapport technique d'évaluation : - *Evaluation Technical Report – HOLBOX project*, HOLBOX_ETR_v1.1, 11 juillet 2017, SERMA SAFETY & SECURITY ; - *Evaluation Technical Report for Partial Re-Evaluation, HOLBOX-PC Project*, HOLBOX-PC_ETR_PR_v1.0, 24 septembre 2021, SERMA SAFETY & SECURITY.
[CONF]	Liste de configuration du produit : eTravel Essential 1.1 ALC-LIS Document, D1405559 v1.8, 13 septembre 2021, THALES DIS.
[GUIDES]	– *eTravel Essential 1.1, AGD-PRE Document, D1404189 rev 1.2*, 25 août 2021, THALES DIS ; – *eTravel Essential 1.1, AGD-OPE Document, D1404191 rev 1.2*, 29 juin 2021, THALES DIS ; – *eTravel Essential 1.x Reference Manual, D1325786 E.11*, 7 avril 2021, THALES DIS.
[PP EAC]	*Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control*, version 1.10, 25 mars 2009. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-CC-PP-0056-2009.

ANNEXE B. 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]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 2.0.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1: Introduction and general model*, avril 2017, version 3.1, révision 4, référence CCMB-2012-09-001 ; - *Part 2 : Security functional components*, avril 2017, version 3.1, révision 4, référence CCMB-2012-09-002 ; - *Part 3 : Security assurance components*, avril 2017, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, avril 2017, 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 and similar devices*, version 2.9, janvier 2013.
[CCRA]	*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.
[NOTE25]	Note d'application: Réduction de portée d'un certificat CC, référence ANSSI-CC-NOTE-25_v1.0, version 1.0, 23 septembre 2021.

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