PREMIÈRE
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-2023/35

eTravel 3.1 EAC on BAC on MultiApp V5.1 (Version 3.1.0.0)

Paris, le 22 Septembre 2023

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

Emmanuel NAEGELEN

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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-2023/35

Nom du produit

eTravel 3.1 EAC on BAC on MultiApp V5.1

Référence/version du produit

Version 3.1.0.0

Conformité à un profil de protection

Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control, version 1.10

certifié BSI-PP-0056 le 25 mars 2009

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL5 augmenté

ALC_DVS.2 et AVA_VAN.5

Développeurs

THALES DIS FRANCE SAS
6 rue de la Verreries
92190 Meudon, France

THALES DIS DESIGN SERVICES
Arteparc, Bât D, Route de la côte d'Azur
13590 Meyreuil, France

Commanditaire

THALES DIS FRANCE SAS
6 rue de la Verreries
92190 Meudon, France

Centre d'évaluation

CEA - LETI
17 avenue des martyrs,
38054 Grenoble Cedex 9, 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 3.1 EAC on BAC on MultiApp V5.1*, Version 3.1.0.0 » développé par THALES DIS FRANCE SAS.

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 aux frontières, 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 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 au profil de protection [PP EAC].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- ceux de la plateforme « *MultiApp* V5.1 » ;
- 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 forte (avec validation de la chaine de certificats) entre le microcontrôleur et le système d'inspection par le mécanisme *Extended Access Control* (EAC) en configuration EAC sur BAC préalable à tout accès aux données biométriques ;
- la protection, en intégrité et en confidentialité, des données lues à l'aide du mécanisme de « *Secure Messaging* ».

Les principaux services de sécurité de la plateforme sont décrits dans [CER-PTF].

1.2.3 *Architecture*

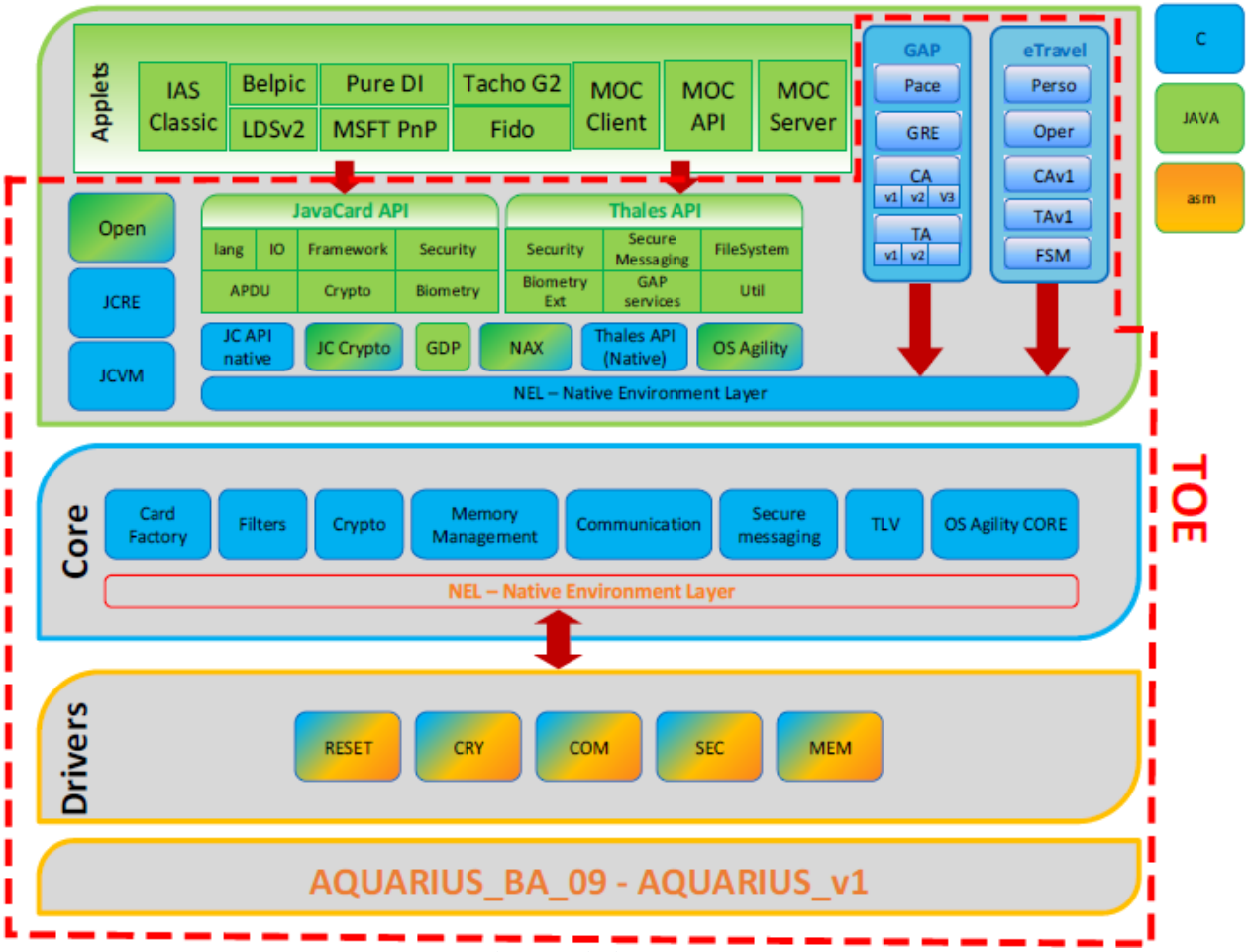

Figure 1 Limites de la TOE

Le périmètre de la TOE évaluée est celui encadré de traits pointillés rouge sur la figure ci-dessus.

Le produit est constitué :

- du microcontrôleur « AQUARIUS_BA_09 », précédemment certifié (voir [CER-IC]) ;
- d'un système d'exploitation sous forme d'une plateforme en configuration ouverte « *MultiApp* V5.1 » préalablement certifiée (voir [CER-PTF]) ;
- de l'application native passeport *eTravel* v3.1.0.0 avec EAC et BAC activés ;
- du mécanisme AA activé.

Le produit s'appuie sur la librairie cryptographique développée par THALES DIS FRANCE SAS.

Des applications peuvent être chargées sur la plateforme *Java Card* ouverte, au côté de l'application « *eTravel* v3.1.0.0 ». La conformité aux prescriptions du document [OPEN] pour le chargement d'applications a été prise en compte pour les seules applications identifiées dans le certificat de la plateforme [CER-PTF].

Bien que ces applications ne soient pas incluses dans le périmètre de l'évaluation, elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [OPEN]. En effet, ces applications ont été vérifiées conformément aux contraintes de développements d'applications décrites dans le rapport de certification [CER-PTF].

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 1.3 « *TOE Identification* ».

Eléments de configuration		Origine
Nom de la TOE	*eTravel 3.1 EAC on BAC on MultiApp* V5.1	THALES DIS FRANCE SAS
Version de la TOE	v3.1.0.0	
Operating System Identifier	« B0 6A 24 »	
Révision de l'application	« 0000 »	
IC fabricator	« 1290 »	THALES DIS DESIGN SERVICES
IC Type	« 0013 »	

Ces éléments peuvent être vérifiés en utilisant la commande GET DATA (voir [GUIDES]).

1.2.5 *Cycle de vie*

Le cycle de vie est décrit au chapitre 2.5 de la cible sécurité [ST]. Il est décomposé en sept phases conformes au profil de protection [PP0084].

Les phases 1 et 2 correspondent au développement du produit, plus précisément au développement du logiciel embarqué (*firmware*). Les phases 3 et 4 correspondent à la fabrication et au conditionnement (packaging) du produit. La phase 5 correspond au chargement de l'application.

Il est à noter que le point de livraison, ou d'émission de la carte, est en sortie de phase 5.

Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

Les sites intervenant dans le cycle de vie de la plateforme et du microcontrôleur sont listés respectivement dans [CER-PTF] et [CER-IC].

Le guide [AGD-OPE] identifie également des recommandations relatives à la livraison des futures applications à charger sur cette carte.

Pour l'évaluation, l'évaluateur a considéré comme :

- administrateur du produit : les agents qui agissent au nom de l'Etat ou de l'organisation émettrice et qui personnalisent le MRTD[1] avec des données correspondant à l'identité de l'utilisateur ;
- utilisateur du produit : le titulaire légitime du MRTD.

[1] *Machine Readable Travel Document*

1.2.6 *Configuration évaluée*

Le certificat porte sur l'application « *eTravel* v3.1.0.0 » avec les fonctionnalités EAC et BAC activées, en composition sur la plateforme *Java Card* « *MultiApp* V5.1 » en configuration ouverte, masquée sur le microcontrôleur « AQUARIUS_BA_09 », telles que présentées au chapitre « 1.2.3 Architecture ».

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 ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [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 la plateforme déjà certifiée par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la « Plateforme *Java Card MultiApp* V5.1 (version 5.1) », voir [CER-PTF].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI (voir date en bibliographie), détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « réussite ».

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

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [ANA_CRY].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises 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 d'attaquant visé.

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

2.4 Analyse du générateur d'aléa

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 [ANSSI Crypto], la sortie du générateur physique d'aléa subit un retraitement de nature cryptographique.

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant 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 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

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[2], 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].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[3] , 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 SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

[3] 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

[ST]	Cible de sécurité de référence pour l'évaluation : - *MultiApp V5.1: eTravel 3.1 EAC on BAC Security Target*, référence D1569589, version 1.33, 11 mai 2023. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *MultiApp V5.1: eTravel 3.1 EAC on BAC Security Target – Public version*, référence D1569589_LITE, version 1.0, 17 mai 2023.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report - NIGELLE-B* référence LETI.CESTI.NIB.FULL.001 - V1.0, version 1.1, 1er août 2023.
[ANA_CRY]	Cotation des mécanismes cryptographiques NIGELLE-B, référence LETI.CESTI.NIB.RT.010 - V1.0, version 1.0, 25 mai 2023.
[CONF]	Liste de configuration du produit : - *MultiApp V5.1 eTravel: ALC LIS CC document*, référence D1598852, version 1.2, 23 mai 2023.
[GUIDES]	Guide d'installation, d'administration et utilisation du produit : - [AGD-PRE] *MultiApp V5.1: AGD PRE - eTravel 3.1*, référence D1574817, version 1.2, 11 mai 2023. - [AGD-OPE] *MultiApp V5.1: AGD OPE - eTravel 3.1*, référence D1582202, version 1.2, 11 mai 2023. Guide d'utilisation du produit : - *eTravel 3.x Reference Manual*, référence D1584821, version D.2, 9 mai 2023. - *Global Dispatcher Personalization Applet User Guide*, référence D1390286, version R, 4 novembre 2022.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - DISGEN20_ALC_GEN_v1.1 ; - DISGEN21_ALC_GEN_v1.1 ; - DISGEN22_ALC_GEN_v1.1 ; - [CBA] DISGEN21_CTB_STAR_v1.1 ; - [MDN] DISGEN21_MDN_STAR_v1.1 ; - [SGP] DISGEN22_SGP_STAR_v1.0 ; - [GEM] DISGEN22_GEM_STAR_v1.0 ; - [VAN] DISGEN21_VAN_STAR_v1.0 ; - [VIG] DISGEN20_VIG_STAR_v1.1 ; - [TCZ] DISGEN20_TCZ_STAR_v1.0 ; - [CAL] DISGEN21_VFO-CAL_STAR_v1.0 ; - [LCY] DISGEN22_LCY_STAR_v1.0 ; - [MAR] DISGEN21_MAR_STAR_v1.1 ; - [CHA] DISGEN21_CHA_STAR_v1.0 ;

	- [PUN] DISGEN21_PUN_STAR_v1.0 ; - [PAU] DISGEN22_PAU_STAR_v1.0.
[CER-PTF]	Rapport de certification *MultiApp* V5.1 (version 5.1). Certifié par l'ANSSI sous la référence ANSSI-CC-2023/31.
[CER-IC]	Rapport de certification AQUARIUS_BA_09 (AQUARIUS_v1). Certifié par l'ANSSI sous la référence ANSSI-CC-2023/01.
[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*, 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 5.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[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 3.2, novembre 2022.
[COMP] *	*Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version 1.5.1, mai 2018.
[OPEN]	*Certification of « Open » smart card products*, version 1.1 (*for trial use*), 4 février 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.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.

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