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-2019/10

eTravel Next 1.0 on M7892 G12, PACE, EAC and AA activated

Version 1.29.00

Paris, le 20 février 2019

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-2019/10

Nom du produit

eTravel Next 1.0 on M7892 G12, PACE, EAC and AA activated

Référence/version du produit

Version 1.29.00

Conformité aux profils de protection

BSI-CC-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 1.0.1

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

Développeurs

Gemalto

6 rue de la Verrerie,
92190 Meudon, France

Infineon Technologies AG

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

Commanditaire

Gemalto

6 rue de la Verrerie,
92190 Meudon, France

Centre d'évaluation

Serma Safety & Security

14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat 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 Next 1.0 on M7892 G12, PACE, EAC and AA activated » développée par *GEMALTO* et par *INFINEON TECHNOLOGIES AG*.

Le produit évalué est de type « carte à puce » sans contact. Il implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (OACI[1]). 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 [PP0056V2] et [PP0068V2].

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 optionnel AA (*Active Authentication*) ;
- l'authentification entre le document de voyage et le système d'inspection lors du contrôle aux frontières par le mécanisme SAC (*Supplemental Access Control)* ;
- 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] Encore appelé ICAO pour *International Civil Aviation Organization*.

1.2.3. Architecture

Le produit est principalement:

- d'un microcontrôleur M7892 G12 (en configuration SLE78CLFX300VPH) et du logiciel *Firmware* associé développés par *INFINEON TECHNOLOGIES AG* ;
- du logiciel embarqué « eTravel Next v1.0 », développé par *GEMALTO* et comprenant les modules représentés dans la figure ci-dessous.

L'architecture du produit est décrite par la figure suivante :

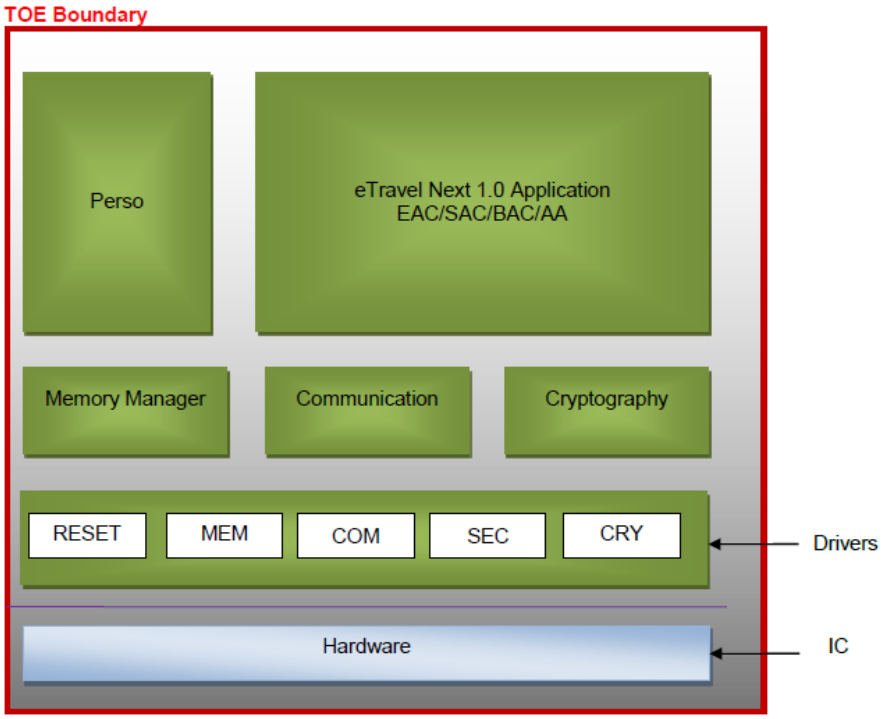

Figure 1 : Architecture

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 les [GUIDES].

Eléments de configuration		Origine
Nom et version de la TOE	eTravel Next v1.0	*GEMALTO*
Identification du logiciel	Référence : '47 65 6d 61 6c 74 6f 20 65 54 72 61 76 65 6c 20 4e 65 78 74 20 76 31 2e 30' (pour Gemalto eTravel Next v1.0) Version : '62 75 69 6c 64 20 31 2e 32 39 2e 30 30' (pour build 1.29.00)	
Identification du circuit intégré	Référence de l'IC : '00 01 00 66 00 00' (pour SLE78CLFX300VPH) Version du Firmware : '78 01 51 82'	*INFINEON TECHNOLOGIES AG*

Tableau 1 : Identification du produit

Ces éléments peuvent être vérifiés en utilisant la commande GET DATA, décrites dans [GUIDES] :

- sur le tag « Mask Info » (0x0180) pour les données du logiciel ;
- sur le tag « Manufacturer Data » (0x0183) pour les données du microcontrôleur.

1.2.5. Cycle de vie

Le cycle de vie est décrit au chapitre 2.4 de la cible de sécurité [ST]. Comme l'illustre l'image ci-dessous, il est décomposé en quatre phases, qui reprennent les sept étapes du [PP0084] :

- phase 1 : développement (étapes 1 à 2) ;
- phase 2 : fabrication (étapes 3 à 5) ;
- phase 3 : personnalisation (étape 6) ;
- phase 4 : utilisation opérationnelle (étape 7).

Le point de livraison de la TOE est en sortie de la phase de fabrication (phase 2, étape 5).

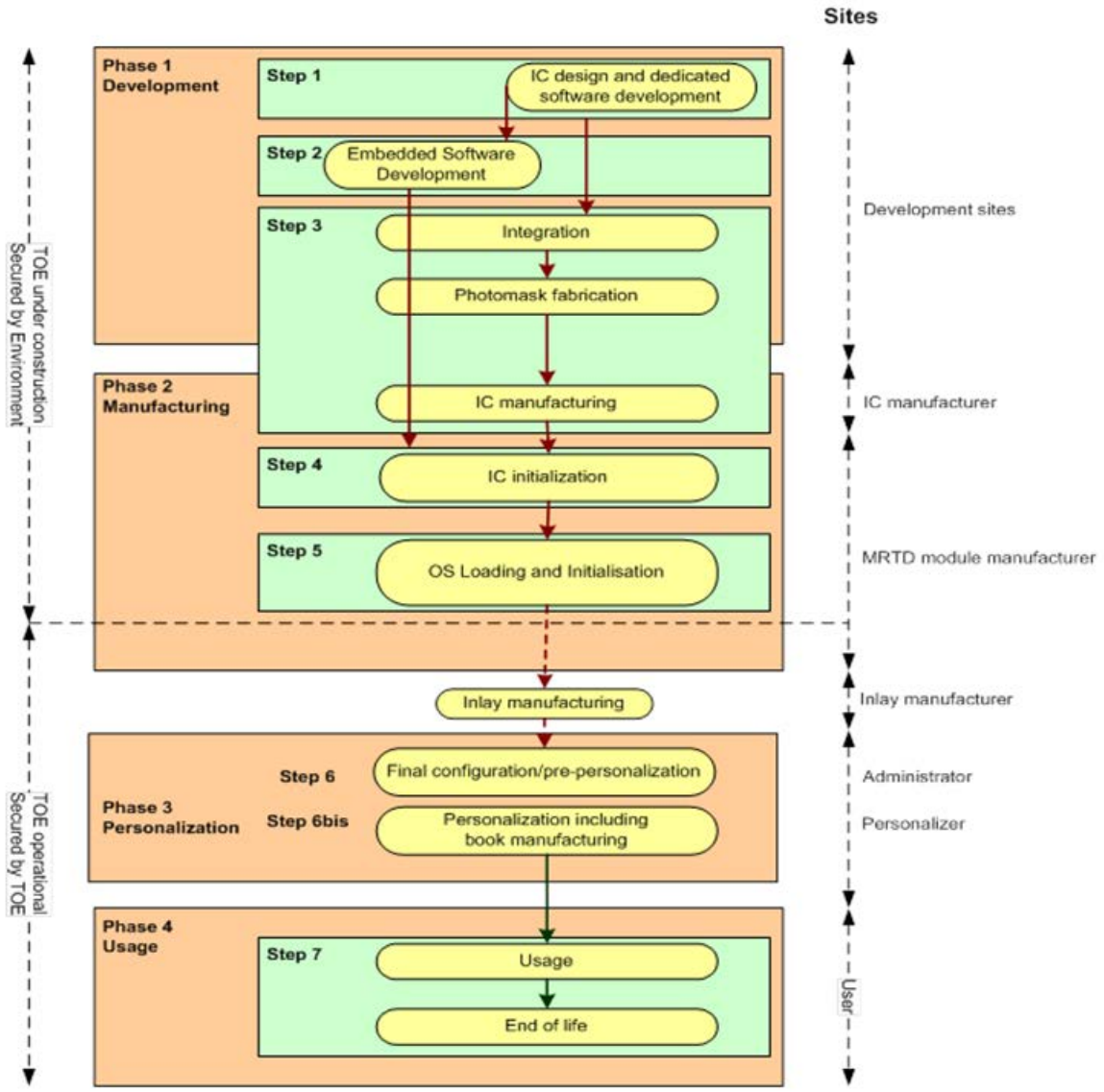

Figure 2 : Cycle de vie

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

GEMALTO Meudon 6 Rue de la Verrerie 92190 Meudon, France	*GEMALTO* Singapore 12 Ayer Rajah Crescent Singapore 139941, Singapour
GEMALTO Gémenos Avenue du Pic de Bretagne 13881 Gémenos, France	*GEMALTO* Montgomeryville 101 & 106 Park Drive Montgomeryville, PA 18 936 United States
GEMALTO Barcelona Poligono lndustrial Llevant CL Llevant 12, 08150 Parets del Valles,Barcelona, Spain	*ATOS* Aubervilliers Datacenter 153 avenue Jean Jaures, 93307 Aubervilliers, France
GEMALTO Vantaa Myllynkivenkuja 4, Vantaa, Finland, FI-01620	*ATOS* Croissy Datacenter 4 rue des vieilles vignes 77183 Croissy-Beaubourg, France
GEMALTO Tczew Ul. Skarszewska 2 33-110 Tczew, Poland	*ATOS* Bydgoszcz – (*ATOS* Poland) Biznes Park, ul. Kraszewskiego 1 85-240 Bydgoszcz, Poland

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 le logiciel « eTravel Next v1.0 » en configuration fermée et masqué sur le microcontrôleur M7892 G12, tel qu'il est présenté au chapitre « 1.2.3 Architecture » et identifié au chapitre « 1.2.4 Identification du produit », avec l'activation des fonctionnalités :

- *Extended Access Control* (EAC) ;
- *Supplemental Access Control* (SAC) ;
- *Active Authentication* (AA).

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 «M7892 G12» au niveau EAL6 augmenté du composant ALC_FLR.1, conforme au profil de protection [PP0084]. Le niveau de résistance du microcontrôleur a été certifié le 9 janvier 2018, sous la référence BSI-DSZ-CC-0891-V3-2018, voir [CER_IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 29 janvier 2019 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 vulnérabilité 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]).
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 Next 1.0 on M7892 G12, PACE, EAC and AA activated » 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 and 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 [CC RA].

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 :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.
[2] 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 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 Next 1.0 - PACE, EAC and AA activated Security Target, référence D1449181_ASE_ST_BAC_eTravelNext10, version 1.5 , 10 septembre 2018, *GEMALTO*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target Lite eTravel Next 1.0 - BAC and AA activated, référence D1449181_ASE_ST_EAC_eTravelNext10_Lite, version 1.5p, juillet 2018, *GEMALTO*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report PEGASUS Project, référence PEGASUS_ETR_v1.1, version 1.1, 29 janvier 2019, *SERMA SAFETY & SECURITY*.
[CONF]	Liste de configuration du produit : D1451754-LIS-DOC-eTravelNext10, référence D1451754, version 1.1, 13 septembre 2018, Gemalto
[GUIDES]	Guides d'installation, d'administration et d'utilisation du produit : – eTravel Next 1.0 AGD - PRE document, référence D1449282, version 1.2, 12 avril 2018, *GEMALTO* ; – eTravel Next 1.0 AGD - OPE document, reference D1449281, version 1.1, 14 mai 2018, *GEMALTO* ; – eTravel Next 1.0 Personalization Reference Manual, reference D1404349, 12 avril 2018, *GEMALTO* ; – eTravel Next 1.0 Administrator Reference Manual, reference D1404349, 12 avril 2018, *GEMALTO* ; – eTravel Next 1.0 Administrator Reference Manual addendum for Configuration Settings, reference D1404349, 12 avril 2018, *GEMALTO* .
[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.*
[PP0068V2]	Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, 22 juillet 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0068-V2-2011-MA-01*.

[PP0056V2]	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.*
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - GEMALTO Development Environment MEUDON Site Visit Report (Lite Report), référence 17-0118-MDN_SVR-M_V1.0, version 1.0, 31 juillet 2017, *SERMA SAFETY & SECURITY* ; - GEMALTO Development Environment Singapore Site Visit Lite Report, référence 17-0466-SGP_SVR-M_v1.0, version 1.0, 16 mai 2018, *SERMA SAFETY & SECURITY ;* - GEMALTO Development Environment GEMENOS Site Visit Lite Report, référence 17-0466_GEM_SVR-M_v1.1, version 1.1, 6 novembre 2018, *SERMA SAFETY & SECURITY* ; - GEMALTO Development Environment MGY Site Visit Report (Lite Report), référence 17-0118-MGY_SVR-M_V1.0, version 1.0, 7 août 2017, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report Barcelona, référence 17-0466_BAR_STAR_v1.0, version 1.0, 25 août 2018, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report ATOS_PAR référence ATOS_PAR_STAR_v1.0, version 1.0, 7 août 2018, *SERMA SAFETY & SECURITY* ; - GEMALTO Development Environment VANTAA Site Visit Report (Lite Report), référence 17-0118-VAN_SVR-M_V1.0, version 1.0, 5 mai 2017, *SERMA SAFETY & SECURITY* ; - GEMALTO Development Environment TCZEW Site Visit Lite Report, référence 17-0466_TCZ-SVR-M_v1.0, version 1.0, 19 avril 2018, *SERMA SAFETY & SECURITY* ; - GEMALTO Development Environment ATOS BYDGOSZCZ Site Visit Report (Lite Report), référence 17-0118_ATOS-BYD_SVR-M_V1.0, version 1.0, 7 avril 2017, *SERMA SAFETY & SECURITY* ; GEMALTO Development Environment ALC Classe Evaluation Report (Generic Documentary activities), référence 17-0466_ALC-GEN_V1.0, version 1.0, 23 mars 2018, *SERMA SAFETY & SECURITY.*

Annexe 3. 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, version 2.9, janvier 2013.
[COMP]	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.5, octobre 2017.
[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.