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-2020/49

Digital Identity on MultiApp v4.0.1 platform with Filter Set 1.0 - PACE, EAC (version 1.0)

Paris, le 18 décembre 2020

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

Guillaume POUPARD

[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-2020/49

Nom du produit

Digital Identity on MultiApp v4.0.1 platform with Filter Set 1.0, PACE, EAC

Référence/version du produit

version 1.0

Conformité à un profil 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

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, ALC_FLR.3, AVA_VAN.5

Développeurs

THALES DIS

6, rue de la verrerie,
92190 Meudon, France

INFINEON TECHNOLOGIES AG

Am Campeon 1-12,
85579 Neubiger, Allemagne

Commanditaire

THALES DIS

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

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 national 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 « Digital Identity on MultiApp v4.0.1 platform with Filter Set 1.0 - PACE, EAC, version 1.0 » développé par THALES DIS. Il s'agit d'une application en composition sur la plateforme « MultiApp V4.0.1 with Filter Set 1.0 Java Card Open Platform on M7892 G12 chip » embarquée sur le microcontrôleur « M7892 G12 » développé par INFINEON TECHNOLOGIES AG.

Le produit implémente les fonctions nécessaires à la carte nationale d'identité numérique. Ce produit, à l'aide d'un système d'inspection, permet la vérification de l'authenticité de la carte d'identité et l'identification de son porteur. Il est disponible en mode contact ou sans contact.
Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans une carte plastique.

Le produit est délivré en deux configurations issues du composant SLE78xx (microcontrôleur M7892 G12 FLASH) :

- avec une capacité RF de 56 pF (SLE78CLFX4007PHM, IC type 7879) ;
- avec une capacité RF de 27 pF (SLE78CLFX400VPHM, IC type 7897).

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 EACV2] auquel s'ajoute un addendum [ADD_DI].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- ceux de la plateforme « MultiApp V4.0.1 with Filter Set 1.0 Java Card Open Platform on M7892 G12 chip » ;
- la protection en intégrité des données du porteur stockées dans la carte ;
- le contrôle d'accès aux données du porteur stockées dans la carte ;
- la confidentialité des données sensibles (code PIN de la carte, par exemple), notamment, pendant leur transfert vers le système d'inspection ;
- l'authentification entre la carte d'identité et le système d'inspection par le mécanisme « *Supplemental Access Control* » (SAC) ;
- 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) » 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 ».*

1.2.3 *Architecture*

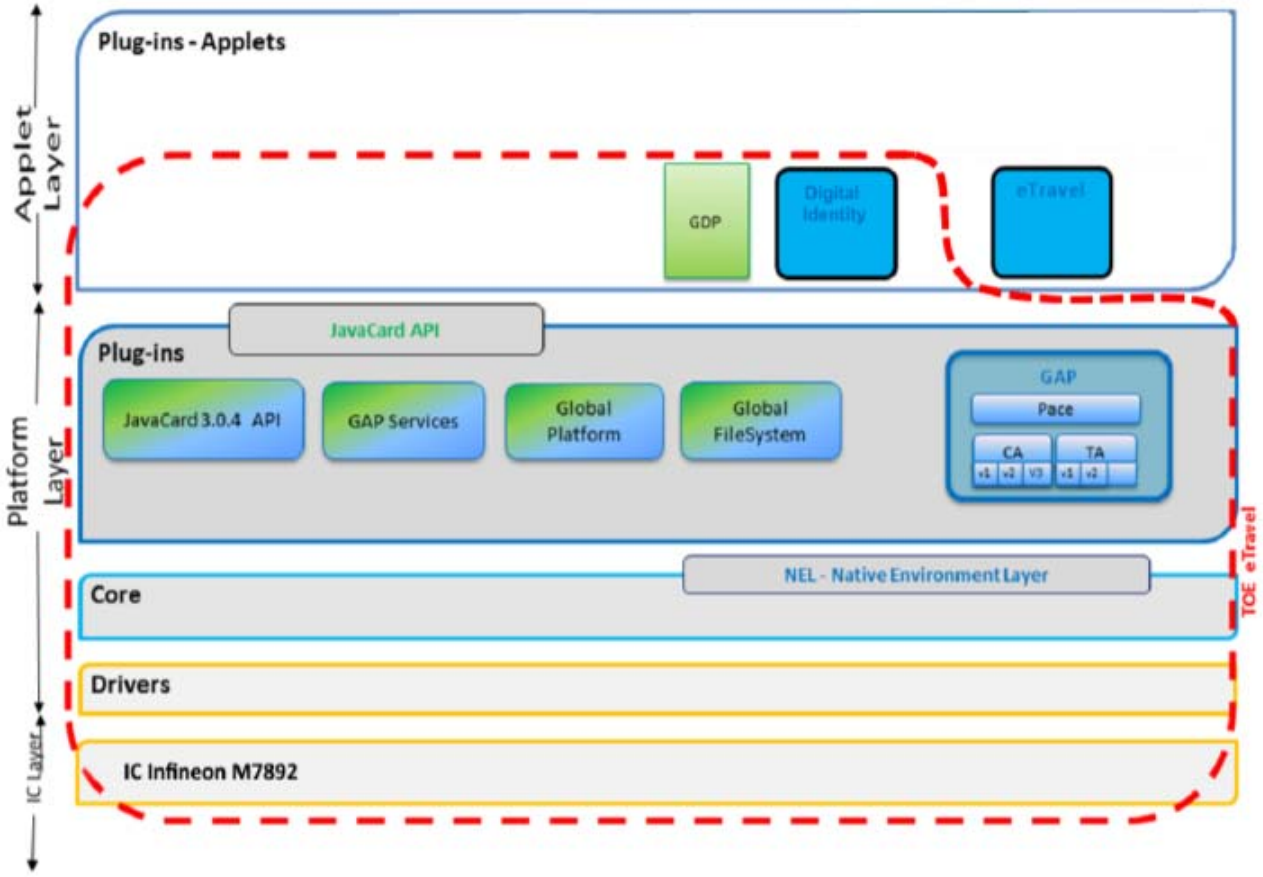

Figure 1 – Architecture du produit

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

Le produit est constitué :

- du composant M7892 G12 précédemment certifié (voir [CER-IC]) ;
- d'un système d'exploitation sous forme d'une plateforme en configuration ouverte ou fermée « MultiApp v4.0.1 with Filter Set 1.0 Java Card Open Platform on M7892 G12 chip » préalablement certifiée (voir [CER- PLF]) ;
- de l'application native *Digital Identity* avec EAC et SAC activés.

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

Des applications Java en dehors du périmètre de cette évaluation peuvent être chargées sur la plate-forme, elles devront respecter les guides [PLF_BADR] et [PLF_SADR].

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 présents dans la réponse que donne le produit à la commande *GET DATA* pour les tags « 9F 7F » et « 01 03 » (voir [GUIDES]) :

Nom	Valeur	Description
IC fabricator	40 90	INFINEON
IC Type	78 97	Configuration 1 : SLE78CLFX400VPHM
	78 79	Configuration 2 : SLE78CLFX4007PHM
Operating System release identifier	Configuration 1 : B0 56 11	MAV 4.0.1
	Configuration 2 : B0 56 0D	
Operating System release level	01 00	*MAV 4.0.1 with Filter Set 1.0*

Pour les deux configurations, toutes les applications présentes dans la configuration du produit durant son évaluation sont identifiées dans la table ci-dessous. Cette table liste les applications et les paquetages (*packages*) inclus dans le produit, associés à leurs noms et AID.

Applet name	AID	*Package name*
eTravel v2.2	A0 00 00 00 18 30 0B 02 00 00 00 00 00 00 00 FF	NA
IAS Classic V4.4.2	A0 00 00 00 18 80 00 00 00 06 62 40 FF	com/gemalto/IASClassic
PPCA V1.0	A0 00 00 00 30 80 00 00 00 0A 71 00 FF	com/gemalto/javacard/ppca
BioPIN Manager v2.0	4D 4F 43 41 5F 43 6C 69 65 6E 74 4D 4F 43 41 5F 53 65 72 76 65 71 4D 4F 43 41 5F 53 65 72 76 65 72	com/gemalto/moc/client com/gemalto/moc/api com/gemalto/moc/server
MPCOS v4.1	A0 00 00 00 18 30 03 01 00 00 00 00 00 00 00 FF	com/gemalto/mpcos
OATH v2.0	A0 00 00 00 18 30 10 02 00 00 00 00 00 00 00 02	com/gemalto/OATH
PURE DI 3.03	A0 00 00 00 18 32 0A 01 00 00 00 00 00 00 00 FF A0 00 00 00 18 02 00 01 65 6D 76 61 70 69 00 FB A0 00 00 00 18 30 07 01 00 00 00 00 00 00 01 FF	com/gemalto/puredi com/gemalto/emvapi com/axalto/PPSE
Privacy Manager v1.0 (also known as "eID/eSign")	A0 00 00 00 30 80 00 00 00 08 DB 00 FF A0 00 00 00 30 80 00 00 00 08 F5 00 FF	com/gemalto/edi com/gemalto/esign
Microsoft Plug & Play	A0 00 00 00 30 80 00 00 00 06 DF 00 FF	com/gemalto/javacard/mspnp

Tableau 1 : Liste des applications chargées dans le produit.

1.2.5 *Cycle de vie*

Le cycle de vie est décrit au chapitre 2.4.2 de la cible de sécurité.

La fin de cette phase 5 (voir [PP0084]) correspond au point de livraison. Les phases, 1, 4 et 5 sont réalisées sur les sites suivants (voir [SITES]) :

Meudon [MDN] GEMALTO 6, Rue de la Verrerie 92190 Meudon, France	**Singapore [SGP]** GEMALTO 12 Ayer Rajah Crescent Singapor 139941, Singapore
Gémenos [GEM] THALES DIS Avenue du Pic de Bertagne 13881 Gémenos, France	**La Ciotat [VIG]** THALES DIS Avenue du Jujubier, ZI Athelia IV 13705 La Ciotat, France
Tczew [TCZ] GEMALTO Ul. Skarszewska 2 33-110 Tczew, Pologne	**Montgomery [MGY]** GEMALTO 101 & 106 Park Drive Montgomeryville, PA 18 936 United States
Curitiba [CBA] GEMALTO Rodovia Dep. Leopoldo Jacomel, 13102 83323-410 Pinhais, PR Brazil	**Vantaa [VAN]** GEMALTO Myllynkivenkuja 4, Vantaa, Finland, FI-01620
Pont Audemer [PAU] GEMALTO Z.I. Saint Ulfrant rue de Saint Ulkfrant 27500 Pont Audemer, France	**ATOS Pune [PUN]** ATOS Embassy Tech Zone, Phase II, Rajiv Gandhi Infitech Park, MIDC, Hinjewadi Pune – 411057, India
ATOS Marcoussis [MAR] ATOS DATA 4, 3, route de Marcoussis, 91620 Nozay, France	**ATOS Aubervilliers [PAR]** ATOS 153, avenue Jean Jaurès, 933307 Aubervilliers, France

Calamba [VZN] GEMALTO Building 7-A, Southern Luzon Industrial Complex Purok 3, Barangay Batino Calamba City, 4027 Laguna, Philippines	

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

Pour la configuration ouverte du produit, le guide [PLF_AGD_OPE] identifie des recommandations relatives à la livraison de futures applications à charger dans le produit.

Par ailleurs,

- les guides [PLF_BADR] et [PLF_SADR] décrivent les règles de développement des applications destinées à être chargées dans le produit ;
- les guides [PLF_GTO_VA] et [PLF_THIRD_VA] décrivent les règles de vérification qui doivent être appliquées par l'autorité de vérification.

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 la carte d'identité avec des données correspondant à l'identité de l'utilisateur ;
- utilisateur du produit : le titulaire légitime de la carte d'identité.

1.2.6 *Configuration évaluée*

Le certificat porte sur l'application « Digital Identity on MultiApp v4.0.1 platform with Filter Set 1.0 - PACE, EAC, version 1.0 » en composition sur la plateforme « MultiApp v4.0.1 with Filter Set 1.0 Java Card Open Platform on M7892 G12 chip », telle que présentée au chapitre 1.2.3 « Architecture » et identifiée au chapitre 1.2.4 « identification du produit ».

Les fonctions, ci-après, ne sont pas incluses dans le périmètre de l'évaluation :

- « pseudonymous signature » (Psign) ECC jusqu'à 521 (fonction *Java Card RMI*) ;
- *Java Card RMI*.

Les plateformes *Java Card* ouvertes utilisées dans le cadre de cette évaluation sont masquées sur les microcontrôleurs SLE78CLFX4007PHM (IC type 7879) et SLE78CLFX400VPHM (IC type 7897), tous deux issus de la famille de microcontrôleurs M7892 G12.

La configuration ouverte de ces produits a été évaluée conformément à [OPEN] : ces produits correspondent à des plateformes ouvertes cloisonnantes. Ainsi, tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 2.2 du présent rapport de certification et réalisé selon les processus audités ne remet pas en cause le présent rapport de certification.

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 de la plateforme *Java Card* au niveau EAL5 augmenté des composants ALC_DVS.2, ALC_FLR.3 et AVA_VAN.5. Cette plateforme a été certifiée le 17 novembre 2020 sous la référence ANSSI-CC-2020/42, voir [CER_PLF].

Le niveau de résistance du microcontrôleur a été confirmé le 19 décembre 2019, voir [CER_IC].

L'évaluation s'appuie sur les résultats d'évaluation des produits suivants :

- « MultiApp v4.0.1 with Filter Set 1.0 Java Card Open Platform on M7892 G12 chip », certifié le 17 novembre 2020 sous la référence ANSSI-CC-2020/42, (voir [CER-PLF]) ;
- « eTravel v2.2 BAC on MultiApp v4.0.1 platform with Filter Set 1.0, version 1.0 », certifié le 9 décembre 2020 sous la la référence ANSSI-CC-2020/43, (voir [APP_BAC]) ;
- « eTravel v2.2 EAC/BAC on MultiApp v4.0.1 platform with Filter Set 1.0, version 1.0 », certifié 9 décembre 2020 sous la la référence ANSSI-CC-2020/44, (voir [APP_EAC/BAC]) ;
- « eTravel v2.2 EAC/SAC on MultiApp v4.0.1 platform with Filter Set 1.0, version 1.0 », certifié le 9 décembre 2020 sous la la référence ANSSI-CC-2020/45, (voir [APP_EAC/SAC]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 10 novembre 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 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.

Dans le cadre du processus de qualification renforcée, l'évaluateur n'a pas rouvert l'expertise de l'implémentation de la cryptographie, il s'appuie sur les travaux déjà réalisés dans le cadre de la certification de la plateforme (voir [CER-PLF]) et sur ceux effectués lors des évaluations des produits [APP_BAC], [APP_EAC/BAC] et [APP_EAC/SAC]. Les résultats de ces travaux 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 [CER-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 (voir [CER-PLF]).
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 « Digital Identity on MultiApp v4.0.1 platform with Filter Set 1.0 - PACE, EAC, version 1.0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL5 augmenté des composants ALC_DVS.2, ALC_FLR.3 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] et celles mentionnées dans les guides de la plateforme [GUIDES_PLF], notamment :

- toutes les futures applications chargées sur ce produit (chargement post-issuance) doivent respecter les contraintes de développement de la plateforme (guides [PLF_BADR] et [PLF_SADR] selon la sensibilité de l'application considérée ;
- les autorités de vérification doivent appliquer les guides [PLF_GTO_VA] et [PLF_THIRD_VA] ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement post-issuance) devra être activée conformément aux indications de [PLF_AGD_PRE].

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].

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.eu.

[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								**3**	*Systematic Flaw Remediation*
	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 : - *Digital Identity on MultiApp v4.0.1 platform with Filter Set 1.0, PACE, EAC Security Target*, référence D1516266, version 1.16, 25/9/2020, THALES DIS. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *Digital Identity on MultiApp v4.0.1 platform with Filter Set 1.0, PACE, EAC Security Target-Public*, référence D1516266_LITE, version 1.4, 24/9/2020, THALES DIS.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report ROBINC Project*, référence ROBINC_ETR_v1.1, version 1.1 du 10/11/2020, SERMA SAFETY & SECURITY.
[CONF]	Liste de configuration du produit : - *eTravel 2.2 and Digital Identity with FilterSet 1.*0 : ALC LIS document, référence D1521422, version 1.5, 27/10/2020, THALES DIS ; - *LIS of source code for CNIe classic on label CNIEV1_08_BinDelivery*, reference CNIEV1_08_BinDelivery, version 1.81.1.45.1.18, 20/4/2020, THALES DIS ; - *LIS of source code for CNIe G320 on label CNIEV1G320_02_BinDelivery*, reference CNIEV1G320_02_BinDelivery, version 2.81.1.45.1.23, 25/9/2020, THALES DIS.

[GUIDES]	- [AGD_PRE] *MultiApp V4.0.1: AGD PRE document - eTravel v2.2 & Digital identity on MultiApp v4.0.1 with filter set 1.0*, référence D1433280, version 1.2, 3/4/2020, THALES DIS ; - [AGD_OPE] *MultiApp V4.0.1: AGD OPE document - eTravel v2.2 & Digital identity 1.0 on MultiApp v4.0.1 with filter set 1.0*, référence D1433279, version 1.2, 5/3/2020, THALES DIS ; - [UM] *eTravel v2.2 with Filter 1.0*, reference D1516624B, 27/2/2020, THALES DIS ;
[GUIDES_PLF]	- [PLF_BADR] *Rules for applications on Multiapp certified product: qualification level*, référence D1484823, version 1.2, janvier 2019, THALES DIS ; - [PLF_SADR] *Guidance for secure application development on Multiapp platforms*, référence : D1390326, version A01, mars 2018, THALES DIS ; - [PLF_GTO_VA] *Verification process of Gemalto non sensitive applet: qualification level*, référence D1484874, version 1.0, décembre 2018, THALES DIS ; - [PLF_THIRD_VA] *Verification process of Third Party non sensitive applet : qualification level*, référence D1484875, version 1.2, février 2019, THALES DIS ; - [PLF_AGD_PRE] *MultiApp V4.0.1 with filter Set 1.0 AGD_PRE document – Javacard Platform*, référence D1431347, version 1.1, 14/2/2020, THALES DIS ; - [PLF_AGD_OPE] *MultiApp V4.0.1 with filter set 1.0 Javacard Platform - AGD_OPE document*, référence D1432683, version 1.11, 24/9/2020, THALES DIS ; - CNIe – *Electronic Personalization Specification and Application Administration Service*, reference D1518028, version 1.4, 7/2/2020, THALES DIS ; - *MultiApp ID Operating System Application Service – Reference Manual*, reference D1519213C, 22/9/2020, THALES DIS.

[SITES]	Rapports d'audit de site pour la réutilisation : - [MDN] : *Site Technical Audit Report MDN*, référence GTOGEN19_MDN_STAR_v1.1, 27 novembre 2019, SERMA SAFETY & SECURITY ; - [SGP] : *Development Environment Singapore Site Visit Lite Report*, référence 17-0466-SGP_SVR-M_v1.0, mai 2018, SERMA SAFETY & SECURITY ; - [GEM] : *THALES DIS Development Environment*, THALES DIS GEMENOS Site Technical Audit Report, référence DISGEN20_GEM_STAR_v1.0, août 2020, SERMA SAFETY & SECURITY ; - [VIG] : *THALES DIS Development Environment*, THALES DIS LA CIOTAT Site Technical Audit Report, référence DISGEN20_VIG_STAR_v1.0, 18 août 2020, SERMA SAFETY & SECURITY ; - [TCZ] : *Site Technical Audit Report – TCZEW site audit*, référence 17-0466-TCZ_STAR_v1.0, référence 17-0466_TCZ-STAR_v1.0, décembre 2018, SERMA SAFETY & SECURITY ; - [MGY] : *Site Technical Audit Report MGY*, référence GTOGEN19_MGY_STAR_v1.1, 19 décembre 2019, SERMA SAFETY & SECURITY ; - [CBA] : *Site Technical Audit Report CBA*, référence GTOGEN19_CBA_STAR_v1.0, avril 2019, SERMA SAFETY & SECURITY ; - [VAN] : *Site Technical Audit Report VAN*, référence GTOGEN19_VAN_STAR_v1.0, mai 2019, SERMA SAFETY & SECURITY ; - [PAU] : *Site Technical Audit Report GEMALTO Pont-Audemer*, référence 17-0466-PAU_STAR_v1.0, octobre 2018, SERMA SAFETY & SECURITY ; - [PUN] : *Site Technical Audit Report PUN2*, référence GTOGEN19a et b_PUN2_STAR_v1.2, mars 2020, SERMA SAFETY & SECURITY ; - [MAR] : *Site Technical Audit Report MAR*, référence GTOGEN19_MAR_STAR_v1.1, 5 décembre 2019, SERMA SAFETY & SECURITY ; - [PAR] : *Site Technical Audit Report ATOS_PAR*, référence ATOS_PAR_STAR_v1.0, août 2018, SERMA SAFETY & SECURITY ; - [VZN] o *Site Technical Audit Report – CAL-VZN Site Audit*, référence GTOGEN19_CAL-VZN_STAR_V1.0, juillet 2019, SERMA SAFETY & SECURITY ; o *Site Technical Audit Report – GEM-VZN Site Audit*, référence GTOGEN19_GEM-VZN_STAR_V1.0, juillet 2019, SERMA SAFETY & SECURITY.
[PP JCS-O]	*Java Card System Protection Profile - Open Configuration, version 3.0. Profil de protection.* Certifié par l'ANSSI le 25 juin 2010 et maintenu le 29 mai 2012 sous la référence ANSSI-CC-PP- 2010/03-M01.
[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 EACV2]	*Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE*, version 1.3.2, 5 décembre 2012. Certifié et maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-CC-PP-0056-V2-2012-MA-02.
[PP SAC]	*Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE*, Version 1.0.1, 22 juillet 2014. Certifié et maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-CC-PP-0068-V2-2011-MA-01.
[ADD_DI]	Module : *Annexe PP0056v2 Digital Identity document using Remote Access Control with PACE v2 + Note Security service correction deployment*, version 1.1, 21 novembre 2019.
[CER-PLF]	*MultiApp v4.0.1 with Filter Set 1.0 Java Card Open Platform on M7892 G12 chip*. Certifiée par l'ANSSI le 17/11/2020 sous la référence ANSSI-CC-2020/42.
[APP_BAC]	*eTravel v2.2 BAC on MultiApp v4.0.1 platform with Filter Set 1.0*. Certifiée par l'ANSSI le 9 décembre 2020 sous la référence ANSSI-CC-2020/43.
[APP_EAC/BAC]	*eTravel v2.2 EAC/BAC on MultiApp v4.0.1 platform with Filter Set 1.0*. Certifiée par l'ANSSI le 9 décembre 2020 sous la référence ANSSI-CC-2020/44.
[APP_EAC/SAC]	*eTravel v2.2 EAC/SAC on MultiApp v4.0.1 platform with Filter Set 1.0*. Certifiée par l'ANSSI le 9 décembre 2020 sous la référence ANSSI-CC-2020/45.
[CER-IC]	*Certification Report BSI-DSZ-CC-0891-V4-2019 for Infineon Security Controller M7892 Design Steps D11 and G12 with optional RSA2048/4096 v2.03.008, ECv2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries, symmetric crypto library v2.02.010 and with specific IC dedicated software (firmware) from* INFINEON TECHNOLOGIES AG. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 19 décembre 2019, sous la référence BSI-DSZ-CC-0891-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*, version 3.0, avril 2019.
[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.
[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.