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-2021/38

eTravel 3.0 BAC on MultiApp v4.2 (version 3.0.0)

Paris, le 23 septembre 2021

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-2021/38

Nom du produit

eTravel 3.0 BAC on MultiApp v4.2

Référence/version du produit

version 3.0.0

Conformité à un profil de protection

Machine Readable Travel Document with "ICAO Application", Basic Access Control, version 1.10

certifié BSI-CC-PP-0055-2009 le 25 mars 2009

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 4 augmenté

ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3

Développeurs

THALES DIS
6, rue de la Verrerie,
92190 Meudon, France

INFINEON TECHNOLOGIES AG
AIM CC SM PS – Am Campeon 1-12, 85579
Neubiberg, 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 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 3.0 BAC on MultiApp v4.2, version 3.0.0 » développé par THALES DIS.

Le produit évalué est de type « carte à puce » pouvant être utilisé en modes 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, dans une *eCover* ou dans une *eDatapage*. Le produit final peut prendre différentes formes, de carte ou de module.

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 BAC].

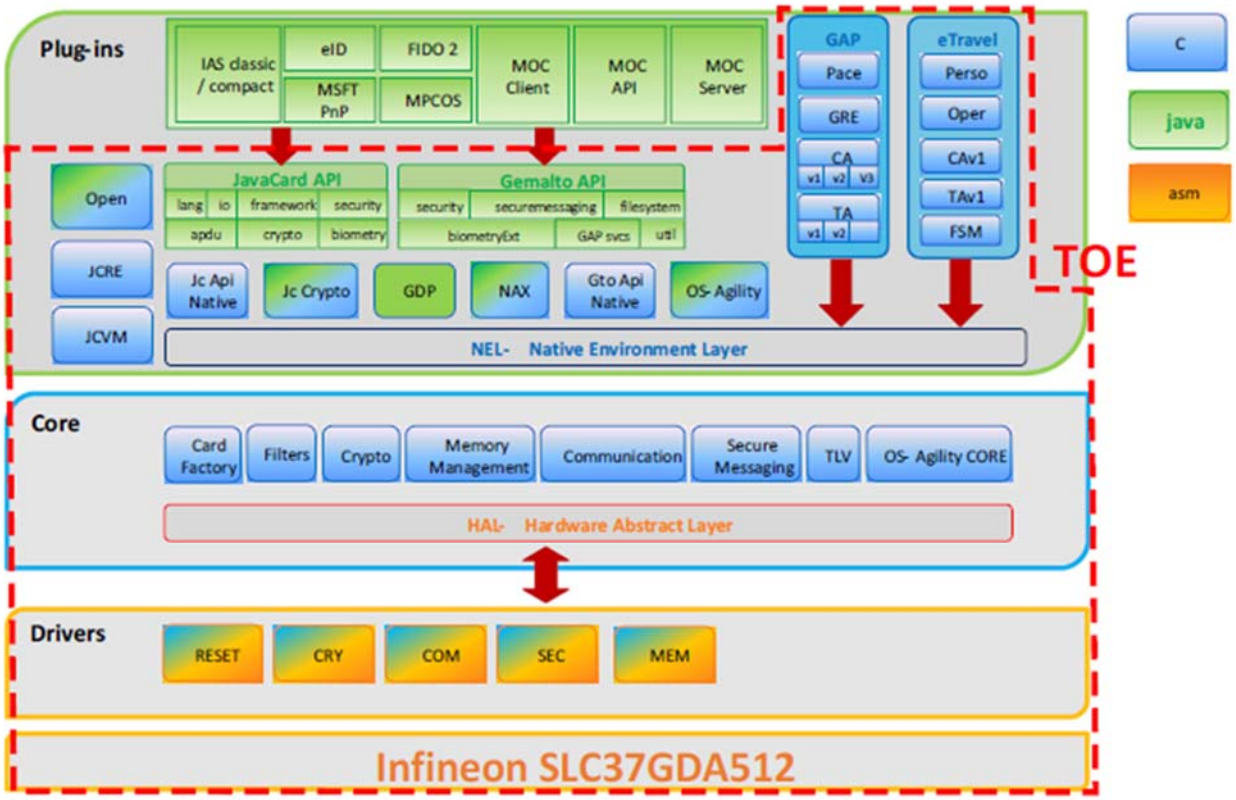
1.2.2 *Services de sécurité*

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 « *Active Authentication* » ;
- l'authentification entre le microcontrôleur et le système d'inspection lors du contrôle aux frontières par le mécanisme BAC (« *Basic Access Control* ») ;
- la protection, en intégrité et en confidentialité, à l'aide du mécanisme de « *Secure Messaging* », des données lues.

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

1.2.3 *Architecture*



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

Le produit est constitué :

- du microcontrôleur « IFX_CCI_000010h » certifié sous la référence [CER-IC] ; de la plateforme *Java Card* ouverte « MultiApp V4.2 » certifiée sous la référence [CER-PTF] ;
- l'application native « eTravel V3.0 » implémentant les spécifications *Machine Readable Travel Document* (MRTD), avec les fonctionnalités BAC et AA activées.

Des applications peuvent être chargées sur la plateforme *Java Card* ouverte, au côté de l'application « eTravel V3.0 ». 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 détaillés dans le chapitre 1.3 de la cible de sécurité [ST] au chapitre 1.3.2 « *TOE identification* ».

Eléments de configuration		Origine
Nom de la TOE	eTravel 3.0 BAC on MultiApp v4.2	THALES DIS
Operating System identifier	B0 5F 1B (pour Javacard family, Gemalto product name : MAV42, short Chip ID)	
Révision de l'application	00 00 (0.0)	
IC fabricator	40 90 (pour chip manufacturer IFX)	INFINEON TECHNOLOGIES AG
IC Type	34 01 (pour SLC52GDA804) 34 04 (pour SLC52GDA700) 34 05 (pour SLC52GDA600)	

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

La principale différence entre le produit et la TOE (la plateforme) correspond aux applications chargées pré-émission sur ce produit. Ces applications sont celles qui sont identifiées dans le rapport de certification de la plateforme.

1.2.5 *Cycle de vie*

Le cycle de vie est décrit au chapitre 2.3 de la cible de sécurité [ST]. Il est décomposé en quatre 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.

Le produit a été développé sur les sites référencés au chapitre 2.4.2 de la cible de sécurité [ST] (voir [SITES]) :

Meudon, voir [MDN]	Singapore, voir [SGP]
Gémenos, voir [GEM]	Calamba, voir [CAL]
ATOS Marcoussis, voir [MAR]	ATOS Les Clayes-sous-bois, voir [LCY]
Pune, voir [PUN]	Vantaa, voir [VAN]
Tczew, voir [TCZ]	Curitiba, voir [CBA]
Montgomeryville, voir [MGY]	Pont-Audemer, voir [PAU]

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

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

Par ailleurs, les guides [Dev_Basic] et [Dev_Sec] décrivent les règles de développement des applications destinées à être chargées sur cette carte ; le guide [AGD-OPE-VA] décrit 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 le MRTD[1] avec des données correspondant à l'identité de l'utilisateur ;
- utilisateur du produit : le titulaire légitime du MRTD.

1.2.6 *Configuration évaluée*

Le certificat porte sur l'application « eTravel v3.0 » avec les fonctionnalités BAC et AA activées, en composition sur la plateforme *Java Card* « MultiApp V4.2 » en configuration ouverte, masquée sur le microcontrôleur IFX_CCI_000010h, 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.

[1] *Machine readable travel documents.*

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 le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur «IFX_CCI_000010h », voir [CER-IC].

L'évaluation s'appuie sur des résultats d'évaluation du produit « Plateforme Java Card MultiApp V4.2 » certifié en juin 2020 sous la référence ANSSI-CC-2020/65, voir [CER-PTF].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 26 juillet 2021, 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 [RTE].

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 potentiel d'attaque 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 potentiel d'attaque 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], notamment :

- toutes les futures applications chargées sur ce produit (chargement post-émission) doivent respecter les contraintes de développement de la plateforme (guides [Dev_Basic] et [Dev_Sec]) selon la sensibilité de l'application considérées ;
- les autorités de vérification doivent appliquer le guide [AGD-OPE_VA] ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement post-émission) doit être activée conformément aux indications de [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 : - *MultiAppV4.2: eTravel 3.0 BAC Security Target*, référence D1492121, version 1.9, 24 juin 2021. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *Security Target Public version eTravel 3.0 BAC*, référence D1492121, version 1.9p, 24 juin 2021.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report TARSO-3 Project*, référence TARSO_3_ETR_v1.4, version 1.4, 26 juillet 2021.
[CONF]	Liste de configuration du produit : - *Configuration List for dev FILES (IAS5.0)*, référence LIS_MAV42_CODE_1.54, 3 novembre 2020 ; - *MultiApp V4.2 : ALC LIS document eTravel v3.0*, référence D1512359, version 1.10, 24 juin 2021 ; - *MAV42_Crypto Lib Project Listing,* référence D1509949, version 1.0, 25 octobre 2019.
[GUIDES]	Guide d'installation et d'administration du produit : - [AGD_OPE] *MultiApp V4.2: AGD OPE document - eTravel v3.0*, version 1.6, 24 juin 2021, référence D1497879 ; - [AGD_PRE] *MultiApp V4.2: AGD PRE document - eTravel v3.0*, version 1.6, 24 juin 2021, référence D1497880. Guide d'utilisation du produit : - [AGD_USE] *eTravel v3.0 - Reference Manual*, 22 juin 2021, référence D1498198C ; - *MultiApp ID 4.2 Premium Operating System Reference Manual*, 3 mai 2021, référence D1493575*E ;* - *Global Dispatcher Personalization Applet User Guide*, référence D1390286Q, 3 mai2021. Guide de développement d'applications : - [Dev_Basic] *Rules for applications on Multiapp certified product*, référence D1495100, version 1.2 de novembre 2019 ; - [Dev_Sec] *Guidance for secure application development on Multiapp platforms*, référence D1495101, version 1.2, décembre 2019 ; - Guides pour l'autorité de vérification [AGD-OPE_VA] : o *Verification process of Gemalto non sensitive applet*, référence D1495102, version 1.1, octobre 2019 ; o *Verification process of Third Party non sensitive applet*, référence D1495103, version 1.1, octobre 2019.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - GTOGEN19_GEN_v1.0 ; - [CBA] GTOGEN19_CBA_STAR_v1.0 ; - [MDN] GTOGEN19_MDN_STAR_V1.1 ; - [SGP] DISGEN20_SGP_STAR_v1.0 ; - [GEM] DISGEN20_GEM_STAR_v1.0 ;

	- [VAN] GTOGEN19_VAN_STAR_v1.0 ; - [CAL] GTOGEN19_CALVZN_STAR_v1.0 ; - [MAR] GTOGEN19_MAR_STAR_v1.1 ; - [MGY] GTOGEN19_MGY_STAR_v1.1 ; - [TCZ] DISGEN20_TCZ_STAR_v1.0 ; - [LCY] DISGEN20_LCY_STAR_v1.0 ; - [PUN] GTOGEN19a_et_b_PUN2_STAR_v1.2 ; - [PAU] DISGEN20_PAU_STAR.
[CER-IC]	*Certification Report for IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 and including optional software libraries and dedicated firmware from Infineon Technologies AG*. Certifié le 16 juin 2020 par le BSI sous la référence BSI-DSZ-CC-1079-V2-2020.
[CER-PTF]	Plateforme Java Card MultiApp V4.2 en configuration ouverte sur le composant IFX_CCI_000010h. Certifié par l'ANSSI le 26 juin 2020 sous la référence ANSSI-CC-2020/65.
[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 BAC]	*Protection Profile, Machine Readable Travel Document with "ICAO Application", Basic Access Control*, version 1.10, 25 mars 2009. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-CC-PP-0055-2009.

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]	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.
[CRY-P-01]	Procédure ANSSI-CC-CRY-P01 Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, 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.
[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.
[AIS31]	*A proposal for: Functionality classes for random number generators, AIS20/AIS31*, version 2.0, 18 septembre 2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).

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