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-2021/54

IAS Classic v5.2 on MultiApp V5.0 (versions 5.2.0.A.C et 5.2.0.A.O)

Paris, le 4 novembre 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-2021/54

Nom du produit

IAS Classic v5.2 on MultiApp V5.0

Référence/version du produit

versions 5.2.0.A.C et 5.2.0.A.O

Conformité à un profil de protection

Protection profiles for secure signature creation device:

Part 2 : Device with key generation, v2.01, BSI-CC-PP-0059-2009-MA-02 ;
Part 3 : Device with key import, v1.0.2, BSI-CC-PP-0075-2012-MA-01 ;
Part 4 : Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, BSI-CC-PP-0071-2012-MA-01 ;
Part 5 : Extension for device with key generation and trusted communication with signature creation application, v1.0.1, BSI-CC-PP-0072-2012- MA-01 ;
Part 6 : Extension for device with key import and trusted communication with signature creation application, v1.0.4, BSI-CC-PP-0076-2013-MA-01.

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté
ALC_DVS.2, AVA_VAN.5

Développeurs

THALES DIS	**INFINEON TECHNOLOGIES AG**
6, rue de la Verrerie, 92197 Meudon cedex, France	AIM CC SM PS – Am Campeon 1-12, 85579 Neubiberg, Allemagne

Commanditaire

THALES DIS
6, rue de la Verrerie,
92197 Meudon cedex, 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 l'application « IAS Classic v5.2 on MultiApp V5.0, versions 5.2.0.A.C et 5.2.0.A.O » développée par THALES DIS et embarquée sur le microcontrôleur développé et fabriqué par INFINEON TECHNOLOGIES AG.

Ce produit est de type « carte à puce » destiné à être utilisé comme dispositif sécurisé de création de signature (SSCD[1]). Il peut être utilisé dans différents types de documents (carte d'identité, permis de conduire, carte d'entreprise, passeport, etc.) disposant d'interfaces avec et/ou sans contact.

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 aux profils de protection *Protection profiles for Secure Signature Creation Device* [PP-SSCD-Part2], [PP-SSCD-Part3], [PP-SSCD-Part4], [PP-SSCD-Part5] et [PP-SSCD-Part6].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- la création de signature ou de sceau électronique dans un environnement où la sécurité repose sur des mesures organisationnelles ;
- la génération des clés de signature (c'est-à-dire la génération de la donnée de création de signature (SCD[2]) et de la donnée de vérification de signature (SVD[3]) associée ;
- l'import des clés de signature (c'est-à-dire de la SCD et, optionnellement, de la SVD associée) ;
- l'export de clé publique (c'est-à-dire la SVD) vers le CGA[4] ;
- l'authentification du signataire par un code PIN ou des données biométriques d'empreintes digitales (*BioPIN*) ;
- l'authentification de l'administrateur (authentification mutuelle) ;
- l'intégrité des conditions d'accès aux données protégées SCD et RAD[5] ;
- l'intégrité des données à signer DTBS[6] ;
- 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] *Secure Signature Creation Device*.

[2] *Signature Creation Data*.

[3] *Signature Verification Data*.

[4] *Certifiation Generation Application*.

[5] *Reference Authentication Data*.

[6] *Data To Be Signed*.

1.2.3 *Architecture*

L'architecture du produit est décrite au chapitre 2.2 de la cible de sécurité [ST]. Elle est constituée :
- du microcontrôleur « IFX_CCI_000039h », développé par INFINEON TECHNOLOGIES AG et certifié sous la référence [CER-IC] ;
- de la plateforme *Java Card* ouverte « MultiApp V5.0 » certifiée sous la référence [CER-PTF] ;
- des applications :
  - « IAS Classic V5.2 » mise à disposition de l'utilisateur pour lui permettre de signer électroniquement ses données ;
  - « MOC server V3.1 » utilisée pour réaliser du *Match On Card*.

Des applications peuvent être chargées sur la plateforme *Java Card* ouverte, au côté des applications « IAS Classic V5.2 » et « MOC server V3.1 ». 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	IAS Classic V5.2 on MultiApp V5.0	THALES DIS
Operating System identifier	1981h	
Operating system release date	1055h	
Operating system release level	0500h	
Noms et versions des applications	- « 49 41 53 20 43 6C 61 73 73 69 63 20 76 35 » (IAS Classic v5 en ASCII) o « 35 2E 32 2E 30 2E 41 2E 43 » pour la configuration full (version 5.2.0.A.C en ASCII)) o « 35 2E 32 2E 30 2E 41 2E 4F » pour la configuration compact (version 5.2.0.A.O en ASCII)) - « 4D 4F 43 41 20 53 45 52 56 45 52 20 33 2E 31 » (MOCA SERVER 3.1 en ASCII) o « 33 2E 31 2E 30 41 » (version 3.1.0A)	
Algorithmes biométriques	- « 00 CE » (pour *Fingerprint*) - « 05 02 » (pour *Face algo*)	
IC fabricator	4090h (pour chip manufacturer IFX)	INFINEON TECHNOLOGIES AG
IC Type	0039h (pour IFX_CCI_000039h)	

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 2.3 de la cible de 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.

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

Meudon, voir [MDN]	Singapore, voir [SGP]
Gémenos, voir [GEM]	Vantaa, voir [VAN]
Tczew, voir [TCZ]	Curitiba, voir [CBA]
La Ciotat [VIG]	

Les sites de développement et de fabrication du microcontrôleur sont couverts par le certificat [CER-IC].

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

Par ailleurs, les guides [AGD-Dev_Basic] et [AGD-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.

1.2.6 *Configuration évaluée*

Le certificat porte sur le produit identifié au paragraphe 1.2.4 et configuré comme suit :

- l'application « IAS Classic V5.2 » est instanciée sur la plateforme *Java Card* ouverte couverte par le certificat [CER-PTF] ;
- les recommandations des [GUIDES] sont strictement appliquées pendant les phases de « Pré-personnalisation » et « Personnalisation » afin de personnaliser l'application en configuration *full* ou *compact*.

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.

Le produit contient deux algorithmes de comparaison, l'un pour les empreintes digitales (*fingerprint*) et l'autre pour la reconnaissance faciale.

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 de la « Plateforme Java Card MultiApp V5.0 », voir [CER-PTF].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 19 octobre 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 [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 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 [AGD-Dev_Basic] et [AGD-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] ;
- le chargement des applications *pré*-émission doit être protégé conformément au guide [ORG_LOAD].

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[7], 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[8] , 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 :

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

[8] 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 V5.0: IAS Classic with MOC Server v3.1 Security Target*, référence D1506187, version 1.87, 19/10/2021, THALES DIS. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *IAS Classic v5.2 with MOC Server v3.1 on MultiApp V5.0 Security Target LITE*, référence D1506187_LITE, version 1.5, 19/10/2021, THALES DIS.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report – ARGAN-C*, référence LETI.CESTI.ARC.FULL.001, version 1.1, 19/10/2021, CEA-LETI.
[ANA-CRY]	Cotation des mécanismes cryptographiques ARGAN C, référence LETI.CESTI.ARC.RT.008, version 1.2, 25/10/2021, CEA-LETI.
[CONF]	Liste de configuration du produit : - *IAS Classic v5.2 on MultiApp V5.0 : ALC LIS CC document*, référence D1552612, version 1.8, 19/10/2021, THALES DIS ; - *Configuration List for IAS Classic v5.2 sources files*, référence D1552614, version v5.2.0_mav50_21153, 22/06/2021, THALES DIS ; - *Configuration List for IAS Classic v5.2/MOC 3.1 sources files*, référence D1552615, version v3_0_1_21141, 22/06/2021, THALES DIS.
[GUIDES]	Guide d'installation et d'administration du produit [AGD_PRE_OPE] : - *MultiApp V5.0 : AGD OPE and PRE document IAS Classic v5.2*, référence D1547769, version 1.5, 19/10/2021, THALES DIS ; - *IAS Classic Applet v5.2 : Personalization Profiles Guide,* référence D1546633A, version A, 31/03/21, THALES DIS. Guide d'utilisation du produit : - *IAS Classic Applet v5.2 Reference Manual*, référence D1542053, version B, 18/05/2021, THALES DIS ; - *BioPIN Manager V3 Reference Manuel*, reference D1481720, version E, 25/06/2021, THALES DIS. Guides de développement d'applications : - [AGD-Dev_Basic] *Rules for applications on Multiapp certified product*, référence D1484823, version 1.21, février 2021, THALES DIS ; - [AGD-Dev_Sec] *Guidance for secure application development on Multiapp platforms*, référence D1495101, version 1.3a, mars 2021, THALES DIS ; Guides pour l'autorité de vérification [AGD-OPE_VA] : - *Verification process of Gemalto non sensitive applet*, référence D1484874, version 1.2, février 2021, THALES DIS ; - [ORG_LOAD] *Verification process of Third Party non sensitive*

	applet, référence D1484875, version 1.21, février 2021, THALES DIS.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - DISGEN20_ALC_GEN_v1.1 ; - [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 ; - [VIG] DISGEN20_VIG_STAR_v1.1 ; - [TCZ] DISGEN20_TCZ_STAR_v1.0.
[CER-IC]	Rapport de certification *BSI-DSZ-CC-1107-2020 for IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh design stepT11 with firmware 80.306.16.0, optional NRG™ SW05.03.4097, optional HSL v3.52.9708, UMSLC libv01.30.0564, optional SCL v2.11.003, optional ACLv3.02.000 and user guidance from Infineon Technologies AG.* Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 17 novembre 2020.
[CER-PTF]	Rapport de certification Plateforme Java Card MultiApp V5.0 (version 5.0). Certifié par l'ANSSI le 14 octobre 2021 sous la référence ANSSI-CC-2021/42.
[PP-SSCD-Part2]	*Protection profiles for secure signature creation device – Part 2: Device with key generation*, référence : prEN 419211-2:2013, version 2.0.1 datée du 18 mai 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0059-2009-MA-02.
[PP-SSCD-Part3]	*Protection profiles for secure signature creation device – Part 3: Device with key import*, référence : prEN 419211-3:2013, version 1.0.2 datée du 14 septembre 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0075-2012-MA-01.
[PP-SSCD-Part4]	*Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application*, référence : prEN 419211-4:2013, version 1.0.1 datée du 12 octobre 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0071-2012-MA-01.

[PP-SSCD-Part5]	*Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application*, référence : prEN 419211-5:2013, version 1.0.1 datée du 12 octobre 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0072-2012-MA-01.
[PP-SSCD-Part6]	*Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application*, référence : prEN 419211-6:2014, version 1.0.4 datée du 25 juillet 2014. Maintenu par le BSI le 30 juin 2016 sous la référence BSI-CC-PP-0076-2013-MA-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.

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.
[JIWG AP] *	*Mandatory Technical Document – Application of attack potential to smartcards and similar devices*, version 3.1, juin 2020.
[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.
[SOG-IS Crypto]	*SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms*, version 1.2, janvier 2020.

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