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-2023/57

IAS Classic V4.4.2 with MOC Server 1.1 on MultiApp V4.1 (version IAS 4.4.2.A, version MOC Server 1.1.1A)

Paris, le 09 Février 2024

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

Vincent STRUBEL

[ORIGINAL SIGNE]

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2023/57

Nom du produit

IAS Classic V4.4.2 with MOC Server 1.1 on MultiApp V4.1

Référence/version du produit

version IAS 4.4.2.A, version MOC Server 1.1.1A

Conformité à un profil de protection

Protection profiles for secure signature creation device:

Part 2 : Device with key generation, v2.0.1, 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

Développeur

THALES DIS FRANCE SAS

6, rue de la Verrerie,
92197 Meudon cedex, France

Commanditaire

THALES DIS FRANCE SAS

6, rue de la Verrerie,
92197 Meudon cedex, France

Centre d'évaluation

SERMA SAFETY & SECURITY

14 rue Galilée, CS 10071,
33608 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat est reconnu au niveau EAL2.

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.cyber.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est la « IAS Classic V4.4.2 with MOC Server 1.1 on MultiApp V4.1, version IAS 4.4.2.A, version MOC Server 1.1.1A » développé par THALES DIS FRANCE SAS.

Ce produit est destiné à être utilisé comme dispositif sécurisé de création de signature (SSCD[1]).

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 décrits au chapitre 2.1 « *TOE description* » de la cible de sécurité [ST]. Ils comprennent notamment :

- la création de signature ou de sceau électronique ;
- 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] ;

[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*.

- la protection en intégrité et en confidentialité, des données lues à l'aide du mécanisme de « *Secure Messaging* ».

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

1.2.3 *Architecture*

La TOE, comme décrit au chapitre 2.2 « *TOE boundaries* » de la cible de sécurité [ST], est constituée des éléments suivants :

- le microcontrôleur S3FT9MH certifié sous la référence [CER-IC] ;
- la plateforme *JavaCard* ouverte « MultiApp V4.1 » certifiée sous la référence [CER-PTF] ;
- des applications :
  - « IAS Classic V4.4.2.A » mise à disposition de l'utilisateur pour lui permettre de signer électroniquement ses données ;
  - « MOCA server V1.1.1A » utilisée pour réaliser du *Match On Card*.

Des applications peuvent être chargées sur la plateforme *JavaCard* ouverte, au côté des applications « IAS Classic V4.4.2.A » et « MOCA server V1.1.1A ». 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].

Les guides [PTF_AGD] identifient les recommandations relatives à la livraison des 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 ; les guides [AGD_OPE_VA] décrivent les règles de vérification qui doivent être appliquées par l'autorité de vérification.

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 1.2 « *TOE Reference* ».

Eléments de configuration		Origine
Nom et version de la TOE	IAS Classic V4.4.2 *with* MOC *Server 1.1 on* MultiApp V4.1	THALES DIS FRANCE SAS
Identification des applications	Référence : '49 41 53 20 43 6C 61 73 73 69 63 20 76 34' (pour IAS Classic v4) Version: '34 2E 34 2E 32 2E 41' (pour 4.4.2.A)	
	Référence : '4D 4F 43 41 20 53 45 52 56 45 52 20 31 2E 31' (pour MOCA server v1.1) Version : '31 2E 31 2E 31 41' (pour 1.1.1A)	
Identification de la plateforme	'19 81' = *OS ID* (identifiant de la plateforme) 'xx xx' = *OS Release Date*: '80 02' pour la configuration 1 ou '82 71' pour la configuration 2 '04 01' = *OS Release Level* (v4.1)	
Identification du circuit intégré	Fabriquant : « 42 50 » (pour SAMSUNG) Référence : « 16 11 » (pour S3FT9MH)	SAMSUNG ELECTRONICS CO.

Ces éléments peuvent être vérifiés par l'utilisation de la commande GET DATA. La procédure d'identification du produit est décrite au chapitre 2 « *TOE acceptance* » dans le guide [AGD_OPE].

1.2.5 *Cycle de vie*

Le cycle de vie est décrit au paragraphe 2.3.2 de la cible de sécurité [ST]. Il est décomposé en quatre étapes :

- développement (phases 1 à 2) ;
- fabrication (phases 3 à 5) ;
- personnalisation (phase 6) ;
- utilisation opérationnelle (phase 7).

Le périmètre de l'évaluation se limite aux deux premières étapes, correspondant aux phases 1 à 5 décrites dans le profil de protection [PP0084] :

- les phases 1 et 2 correspondent au développement du produit, plus précisément :
  - au développement du logiciel embarqué : le *firmware* dédié au microcontrôleur, le système d'exploitation, le système *Javacard,* la documentation, des *applets* et d'autres parties logicielles de la plateforme ;
  - au développement du microcontrôleur,
- les phases 3 et 4 correspondent à la fabrication et au conditionnement (packaging) du microcontrôleur ;
- la phase 5 correspond au chargement du logiciel embarqué (hormis le *firmware* qui est déjà masqué durant l'étape 3) dans le microcontrôleur. Il est à noter que le point de livraison, ou d'émission de la carte, est en sortie de phase 5.

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

1.2.6 *Configuration évaluée*

Le certificat porte sur les applications « IAS Classic V4.4.2.A » et « MOCA Server 1.1.1A » en composition sur la plateforme ouverte Java Card « MultiApp V4.1 » masquée sur le microcontrôleur S3FT9MH, telles que présentées au chapitre *« 1.2.3 Architecture »*.

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2 Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel sur la plateforme déjà certifiée par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme « MultiApp V4.1 », voir [CER-PTF].

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

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

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

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

2.4 Analyse du générateur d'aléa

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CER-IC]).

Par ailleurs, comme requis dans le référentiel [ANSSI Crypto], la sortie du générateur physique d'aléa subit un retraitement de nature cryptographique.

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

3.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- toutes les futures applications chargées sur ce produit (chargement après émission) doivent respecter les contraintes de développement de la plateforme (guides [AGD-Dev_Basic] et [AGD-Dev_Sec]), notamment toutes les applications y compris celles chargées avant émission doivent être vérifiées avec la dernière version disponible du *bytecode verifier* ;
- les autorités de vérification doivent appliquer les guides [AGD_OPE_VA] ;
- la protection du chargement de toutes les applications sur ce produit doit être activée conformément aux indications des guides [PTF_AGD] ;
- l'utilisation du protocole SCP03 est à privilégier plutôt que les protocoles SCP01 et SCP02 qui sont obsolètes et dont l'utilisation est déconseillée. Toutefois, si l'usage de l'un de ces deux derniers était rendu nécessaire, il est recommandé de le faire dans un environnement physiquement sécurisé et de chiffrer les données échangées (voir [APP_AGD]).

3.4 Reconnaissance du certificat

3.4.1 *Reconnaissance européenne (SOG-IS)*

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

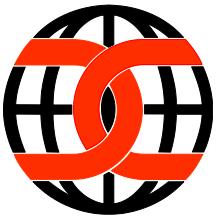
L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[7], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.4.2 *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 V4.1: IAS EN Core & Extensions Security Target*, référence D1418852, version 1.6, 25 septembre 2023. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *IAS EN Core & Extensions Security Target - public version*, référence D1418852, version 1.6p, 25 septembre 2023.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report, SUNDANCE-I-NS Project*, référence SUNDANCE-I-NS_ETR_v1.3, version 1.3, 8 janvier 2024.
[CONF]	Liste de configuration du produit : *MultiApp V4.1: ALC LIS document – IAS Classic v4.4.2*, référence D1459478, version 1.6, 25 septembre 2023.
[GUIDES]	Guide d'installation et d'administration du produit : - *MultiApp V4.1 : AGD OPE and PRE document - IAS v4.4.2*, référence D1425835, version 1.4, 15 mai 2023. Guides de personnalisation d'applications sécurisées [AGD_CPS] : - *Card Personalization Specification requirement for SSCD security evaluation IAS Classic v4.4*, référence IACv44_001_CPS_Req_For_CC_Evaluation, version 1.4, 07 janvier 2022. Guide d'installation et d'administration de la plateforme [PTF_AGD] : - *MultiApp ID Operating System – Reference Manual*, référence D1392687I, 13 avril 2021. Guides d'utilisation du produit [AGD_USE] : - *IAS Classic Applet V4.4, Reference Manual*, référence D1387713M, 29 mai 2023 ; - *BioPIN Manager V2.0 – Reference Manual*, référence D1290692C, 26 octobre 2016. Guide de développement d'applications basiques [AGD-Dev_Basic] : - *Rules for applications on MultiApp certified product*, référence D1390963, version 1.2, novembre 2017. Guide de développement d'applications sécurisées [AGD-Dev_Sec] : - *Guidance for secure application development on MultiApp platforms*, référence : D1390326, version A02, janvier 2023.

	Guides pour l'autorité de vérification [AGD_OPE_VA] : - *Verification process of Gemalto non sensitive applet*, référence D1390670, version A01, février 2016 ; - *Verification process of Third Party non sensitive applet*, référence D1390671, version A01, février 2016.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - DISGEN21_ALC_GEN_v1.0 ; - DISGEN22_ALC_GEN_v1.0 ; - DISGEN23_ALC_GEN_v1.0 ; - [CBA] DISGEN23_CUR_STAR_v1.0 ; - [MDN] DISGEN21_MDN_STAR_v1.1 ; - [SGP] DISGEN22_SGP_STAR_v1.0 ; - [GEM] DISGEN22_GEM_STAR_v1.0 **;** - [VAN] DISGEN23_VAN_STAR_v1.0 ; - [LVG] DISGEN22_LVG_STAR_v1.0 ; - [TCZ] DISGEN23_TCZ_STAR_v1.0 ; - [CAL] DISGEN23_VFO-CAL_STAR_v1.0 ; - [LCY] DISGEN22_LCY_STAR_v1.0 ; - [MAR] DISGEN21_MAR_STAR_v1.1 ; - [MGY] DISGEN23_MGY_STAR_v1.0 ; - [PUN] DISGEN23_PUN_STAR_v1.0 ; - [PAU] DISGEN22_PAU_STAR_v1.0.
[CER-IC]	Rapport de certification *S3FT9MH/S3FT9MV/S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional CE1 Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software (S3FT9MH_20220713)*. Certifié par l'ANSSI sous la référence ANSSI-CC-2023/20.
[CER-PTF]	Rapport de certification Plateforme ouverte *JavaCard* MultiApp V4.1 en configuration ouverte masquée sur le composant S3FT9MH (Version 4.1.0.2). Certifiée par l'ANSSI sous la référence ANSSI-CC-2023/30.
[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-SSCD-Part2]	*Protection profiles for secure signature creation device – Part 2: Device with key generation*, référence : prEN 419211-2:2013, version 2.0.1, 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, 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, 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, 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, 25 juillet 2014. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0076-2013-MA-01.

ANNEXE B. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER-P-01]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1 : Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - *Part 2 : Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - *Part 3 : Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	*Mandatory Technical Document – The Application of CC to Integrated Circuits*, version 3.0, février 2009.
[JIWG AP] *	*Mandatory Technical Document – Application of attack potential to smartcards and similar devices*, version 3.2, novembre 2022.
[COMP] *	*Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version 1.5.1, mai 2018.
[OPEN]	*Certification of « Open » smart card products*, version 1.1 (*for trial use*), 4 février 2013.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, version 3.0, 8 janvier 2010, Management Committee.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.

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