PREMIÈRE 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-2023/45

MultiApp V5.1 Java Card Virtual Machine (version 5.1)

Paris, le 13 Novembre 2023

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

Vincent STRUBEL

[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-2023/45**
Nom du produit **MultiApp V5.1 Java Card Virtual Machine**
Référence/version du produit **version 5.1**
Conformité à un profil de protection **Néant**
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL 7**
Développeurs **THALES DIS FRANCE SAS** 6 rue de la Verrerie 92190 Meudon, France **THALES DIS DESIGN SERVICES** Arteparc, Bât D, Route de la côte d'Azur 13590 Meyreuil, France
Commanditaire **THALES DIS FRANCE SAS** 6 rue de la Verrerie 92190 Meudon, 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 la carte « MultiApp V5.1 Java Card Virtual Machine, version 5.1 » développé par THALES DIS FRANCE SAS et THALES DIS DESIGN SERVICES. La « plateforme MultiApp V5.1 » de la carte a déjà fait l'objet d'une certification au niveau EAL6 augmenté du composant ALC_FLR.2 (voir [CER-PLF]).

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.

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par la TOE[1] sont détaillés dans la cible de sécurité [ST] au chapitres 2.4.1 « *Architecture* ».

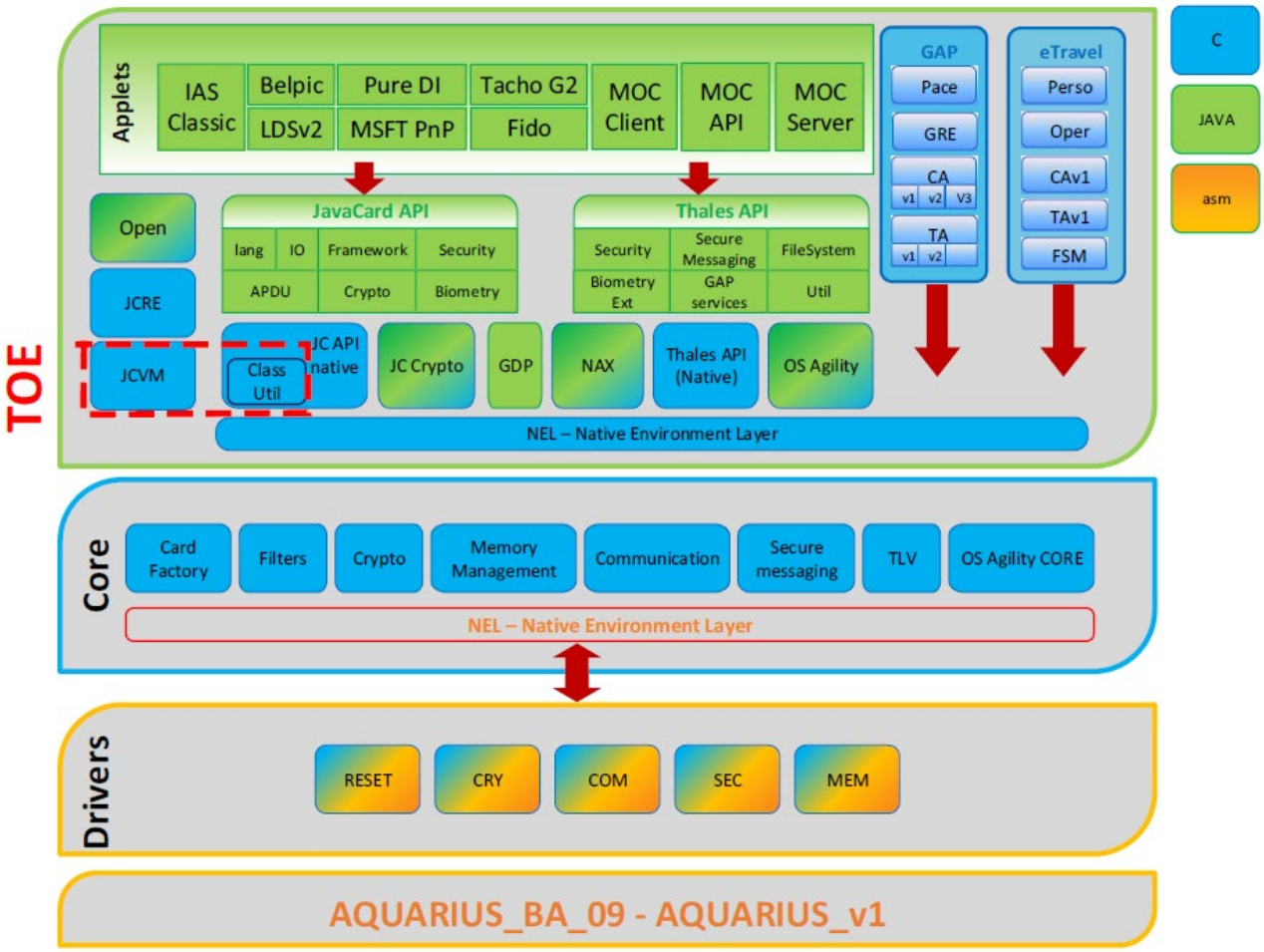
1.2.3 *Architecture*

La TOE est décrite aux chapitres 2.2 « *Product Architecture* » et 2.4.1 « *Architecture* » de la cible de sécurité [ST].

La TOE soumise à l'évaluation au niveau EAL 7 est restreinte à l'*interpreter*, pour l'exécution des *bytecodes*.

L'architecture du produit est illustrée par la figure ci-après, où il est précisé en pointillé rouge la présente TOE (évaluée au niveau EAL7).

[1] *Target of evaluation* - périmètre d'évaluation.



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* » et dans le guide [AGD_OPE] au chapitre 1.6 « *Product identification* ».

Eléments de configuration		Origine
Family Name (Java Card)	0xB0	THALES DIS FRANCE SAS
OS NAME (MultiApp)	0x85	
Mask Number (MultiApp V5.1)	0x68	
Product Name	0x6A	
Flow identification version	0x01	
Filter Set	0x00	
Platform Certificates (CC configuration)	0x40	
IC Fabricator / Chip manufacturer	0x1290	
IC type	0x0013	

Operation System Identifier	0x1981	
Operation System release date	0x3055	
Operation System release level (5.1)	0x0510	

Ces éléments peuvent être vérifiés par l'utilisation de la commande GET DATA. La procédure d'identification est décrite dans le guide [AGD_OPE] (voir [GUIDES]).

La principale différence entre le produit et la TOE (la plateforme) correspond aux applications chargées pré-émission sur ce produit.

Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans le tableau ci-après. Ce tableau liste les applications et les *packages* inclus dans le produit, associés à leur nom et leur AID[2].

Nom, version de l'application	AID (en hexadécimal)	Nom du *package*
GDP	A00000001810020303	com/gemalto/javacardx.gdp
LDSV2 v1.1	A0000000183O0B0201000000000000FE	com/gemalto/javacard/icao/lds2
TachoG2V2	A0000000308000000000A2800FF	com/gemalto/tacho
BelPIC v1.8	A0000000308000000000043417	com/gemalto/belpic
eTravel v3.1	A0000000183O0B0200000000000000FF	N/A (Natif)
IAS Classic V5.2.1	A0000000188000000000066240FF	com/gemalto/iasclassic
BioPIN Management v3.1	4D4F43415F436C69656E74 4D4F43415F536572766572	com/gemalto/moc/client com/gemalto/moc/server
MPCOS v4.1	A0000000183003010000000000000FF	com/gemalto/mpcos
PURE DI 3.05	A0000000183320A01000000000000000FF	com/gemalto/puredi
Privacy Manager v1.0	A0000000308000000008DB00FF	com/gemalto/edi
MSFT PnP v1.0	A0000000308000000006DF00FF	com/gemalto/javacard/mspnp
Fido Authentificator v2.1	A0000000308000000000A9A00FF	com/gemalto/javacard/fido/ctap

La commande GET STATUS permet à l'utilisateur du produit de vérifier quelles applications et quels *packages* sont installés dans le produit à sa disposition.

[2] *Application Identifier.*

1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit par la figure ci-après, voir chapitre 2.5 de la cible de sécurité [ST].

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 logiciel embarqué, à savoir le logiciel dédié au microcontrôleur (*firmware*), le système d'exploitation, le système *Java Card*, la documentation, certaines *applets* et d'autres parties logicielles de la plateforme ;
  - au développement du microcontrôleur sécurisé ;
- la phase 3 correspond :
  - à la fabrication du microcontrôleur sécurisé ;
  - à la protection du *flash loader* à l'aide d'une clé de transport dédiée ;
  - à la pré-personnalisation (*wafer* seulement) par le chargement du logiciel THALES DIS à partir d'un script ;
- la phase 4 correspond à la mise en module du microcontrôleur, cette étape peut être réalisée par THALES DIS ;
- la phase 5 correspond à :
  - la mise en forme du module (*inlay*, *card*, autres) qui est effectuée par THALES DIS ou par d'autres sociétés ;
  - la pré-personnalisation (excepté *wafer* déjà réalisée à la phase 3) réalisée par THALES DIS en effectuant le chargement du logiciel THALES DIS à partir d'un script ;
  - la mise en forme du module (*inlay*, *card*, autres) réalisée par THALES DIS ou autres si elle n'a pas été réalisée au préalable.

La fin de cette phase correspond au point de livraison. Jusqu'à cette phase, le produit est considéré comme étant en construction. Aussi, les phases, 1, 4 et 5 sont réalisées sur les sites [SITES].

Le produit permet le chargement d'applications en phase 3 (avant le point de livraison), en phase 5 (pré-émission) ou en phase 6 et 7 (post-émission) :

- le développement des applications masquées en phase 3 et identifiées dans la cible de sécurité [ST] a été réalisé sur les sites de Meudon, La Ciotat et Vantaa. Leur livraison et leur vérification ont été analysées pendant cette évaluation conformément à [OPEN] au titre des tâches ALC ;
- les chargements en phase 5 (pré-émission), 6 et 7 (post-émission) doivent être protégés conformément à [AGD-Dev].

Le guide [AGD_OPE] identifie également des recommandations relatives à la livraison des futures applications à charger sur ce produit.

Par ailleurs, le guide [AGD-Dev] décrit 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 le « prépersonnalisateur », le « personnalisateur » et le gestionnaire de la carte chargé de l'administration de la carte, et, comme utilisateur du produit, les développeurs des applications à charger sur la plateforme.

1.2.6 *Configuration évaluée*

Le certificat porte sur la configuration de la plateforme telle qu'elle est identifiée au paragraphe 1.2.4.

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 a consisté à évaluer la machine virtuelle « MultiApp V5.1 JavaCard Virtual Machine, version 5.0 » de la plateforme MultiApp V5.1, selon les plus hautes exigences des Critères communs : les composants du niveau EAL 7, qui nécessitent la mise en œuvre de méthodes formelles.

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 [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 niveau d'attaquant 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 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].

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[3], 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[4] , 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 :

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

[4] 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 V5.1 : Security Target Java Card Virtual Machine*, référence D1586135, version 1.5, 6 juin 2023. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *MultiApp V5.1 Java Card Virtual Machine Security Target – Public version*, référence D1586135_LITE, version 1.1, 6 juin 2023.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report – NIGELLE-D*, référence LETI.CESTI.NID.FULL.001, version 1.1, 19 septembre 2023.
[ANA_CRY]	Cotation des mécanismes cryptographiques NIGELLE-A, référence LETI.CESTI.NIA.RT.012, version 1.0, 6 avril 2023.
[CONF]	Liste de configuration du produit : - *MultiApp V5.1 Virtual Machine : ALC LIS CC document*, référence D1599661, version 1.2, 6 juin 2023 ; - *MultiApp V5.1 : ALC LIS Common Criteria*, référence D1595903, version 1.0, 27 mars 2023. - *MultiApp V5.1 Virtual Machine : ALC LIS Common Criteria*, référence D1599659, version 1.0, 30 mai 2023.
[GUIDES]	Guide d'installation du produit [AGD_PRE] : - *MultiApp V5.1: AGD_PRE document – JavaCard Platform*, référence D1574816, version 1.8, 30 mars 2023. Guide d'administration du produit [AGD_OPE] : - *MultiApp V5.1 : AGD_OPE document - JavaCard Platform*, référence D1574815, version 1.8, 30 mars 2023. Guide d'utilisation du produit : - *MultiApp ID V5 Operating System Reference Manual*, référence D152385, version C, 7 décembre 2022. Guides de développement et de protection des applications : - [AGD-Dev] *MultiApp Guidance Document for secure development for MultiApp products*, référence D1539156, version 1.2, 24 mars 2023.
[SITES]	Rapports d'analyse documentaire et d'audits de sites pour la réutilisation : - DISGEN21_ALC_GEN_v1.0 ; - DISGEN22_ALC_GEN_v1.1 ; - [CBA] DISGEN21_CTB_STAR_v1.1 ; - [MDN] DISGEN21_MDN_STAR_v1.1 ; - [SGP] DISGEN22_SGP_STAR_v1.0 ; - [GEM] DISGEN22_GEM_STAR_v1.0 ; - [VAN] DISGEN21_VAN_STAR_v1.0 ; - [VIG] DISGEN22_LVG_STAR_v1.0 ; - [TCZ] DISGEN20_TCZ_STAR_v1.0 ; - [CAL] DISGEN21_VFO-CAL_STAR_v1.0 ; - [LCY] DISGEN22_LCY_STAR_v1.0 ;

	- [MAR] DISGEN21_MAR_STAR_v1.1 ; - [CHA] DISGEN21_CHA_STAR_v1.0 ; - [PUN] DISGEN21_PUN_STAR_v1.0 ; - [PAU] DISGEN22_PAU_STAR_v1.0.
[CER_IC]	Rapport de certification AQUARIUS_BA_09, AQUARIUS_v1. Certifié par l'ANSSI sous la référence ANSSI-CC-2023/01.
[CER-PLF]	Rapport de certification MultiApp V5.1 (version 5.1). Certifiée par l'ANSSI sous la référence [ANSSI-CC-2023/31].
[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]	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.