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 EUCC-ANSSI-2025-03-02

Smart Tachograph G2 on MultiApp V4.0.1 (Versions 2.0.1 G et 2.0.1 H)

Paris, le 31 mars 2025

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

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 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).

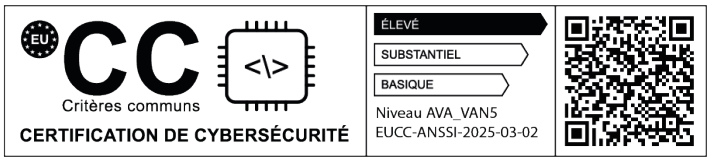
Ce rapport est conforme à [EUCC].

Les procédures de certification sont disponibles sur le site Internet www.cyber.gouv.fr.

TABLE DES MATIERES

1 Résumé

Référence du rapport de certification **EUCC-ANSSI-2025-03-02**
Nom du produit **Smart Tachograph G2 on MultiApp V4.0.1**
Référence/version du produit **Versions 2.0.1 G et 2.0.1 H**
Type de produit **Cartes à puce et dispositifs similaires**
Conformité à un profil de protection ***Digital Tachograph –Tachograph Card (TC PP) Protection Profile,*** **certifié BSI-CC-PP-0091-2017 le 19 mai 2017**, version 1.0
Critère d'évaluation et version **ISO/IEC 15408-1:2009, 15408-2:2008, 15408-3:2008** **(Critères Communs version 3.1 révision 5)** **ISO/IEC 18045:2008** **(CEM version 3.1 révision 5)**
Niveau d'évaluation **Elevé / EAL4 augmenté** ALC_DVS.2, ATE_DPT.2, AVA_VAN.5
Référence du rapport d'évaluation *Evaluation Technical Report POSEIDON-NS Project* référence POSEIDON-NS_ETR_v1.1 version 1.1 11 février 2025.
Fonctionnalité de sécurité du produit voir 2.2.2 Services de sécurité
Résumé des menaces *Threat T.Identification_Data* Modification des données d'identification de la TOE *Threat T.Application* Modification de l'application du tachygraphe *Threat T.Activity_Data* Modification des données d'activités stockées dans la TOE *Threat T.Data_Exchange* Modification des données d'activités lors d'un import ou export des données *Threat T.Clone* Duplication de la carte Voir chapitre 4.3 de la cible de sécurité [ST]

Exigences de configuration du produit voir 4.2 Restrictions d'usage
Hypothèses liées à l'environnement d'exploitation voir 4.2 Restrictions d'usage
Développeur **THALES DIS FRANCE SAS** Avenue du Jujubier ZI Athelia IV 13705 La Ciotat Cedex France
Commanditaire **THALES DIS FRANCE SAS** Avenue du Jujubier ZI Athelia IV 13705 La Ciotat Cedex France
Centre d'évaluation **SERMA SAFETY & SECURITY** 14 rue Galilée, CS 10071, 33608 Pessac Cedex, France
Marque EUCC 
Accords de reconnaissance applicables CCRA Ce certificat est reconnu au niveau EAL2.

2 Le produit

2.1 Présentation du produit

Le produit évalué est « Smart Tachograph G2 on MultiApp V4.0.1, Versions 2.0.1 G et 2.0.1 H » développé par THALES DIS FRANCE SAS.

Ce produit est destiné à être utilisé être utilisée par les tachygraphes électroniques (équipements d'enregistrement des activités d'un véhicule de transport routier) ou par des ordinateurs personnels (pour réaliser les opérations de contrôle de l'activité du véhicule).

Les principales fonctions de cette carte sont :

- le stockage des identifiants de la carte et de son porteur en vue de l'identification du porteur de la carte afin de fournir les droits d'accès appropriés aux fonctions et aux données, et d'assurer l'imputation des activités ;
- le stockage des informations relatives à l'activité du porteur de la carte.

2.2 Description du produit

2.2.1 *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 [PP0091].

2.2.2 *Services de sécurité*

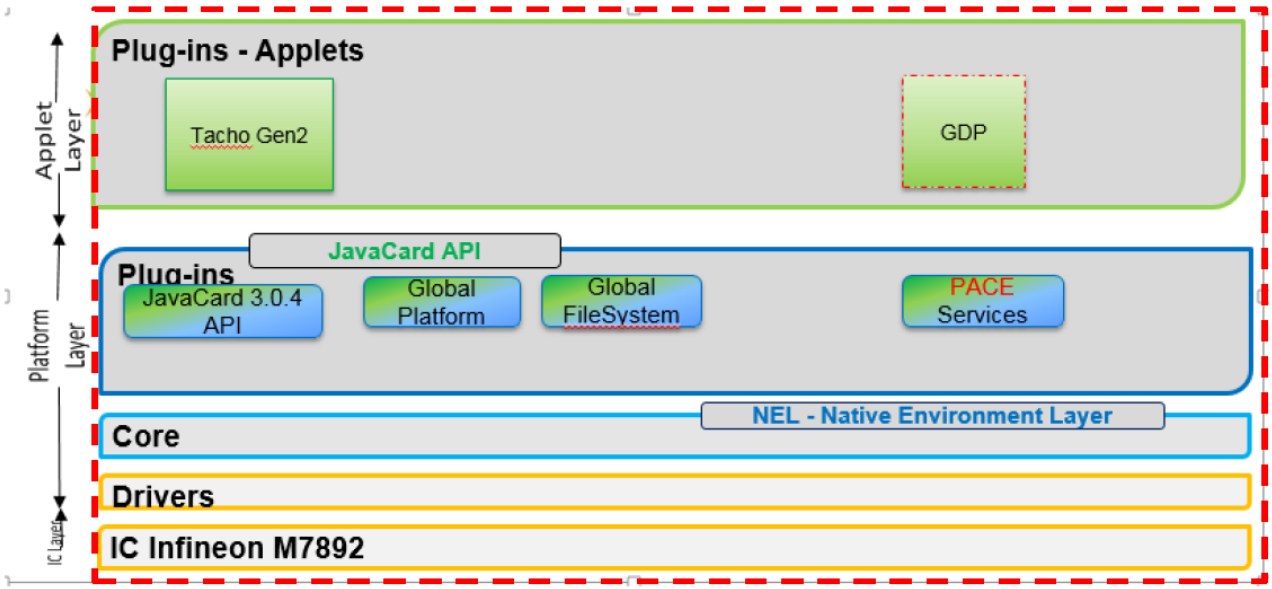
Les principaux services de sécurité fournis par le produit, comme décrits au chapitre 2.1 « *TOE Description* » de la cible de sécurité [ST], sont :

- l'authentification mutuelle Gen1 ou Gen2 ;
- le stockage de l'identification de la carte et des données d'identification du porteur ;
- le stockage des données d'activités (évènements, données de contrôle d'activités, données de fautes) ;
- la vérification des certificats Gen1 et Gen2 ;
- la génération de signature des données internes à exporter ;
- la vérification de l'intégrité et de l'authenticité du *Dedicated Short Range Communication* (DSRC) message ;
- le téléchargement des données utilisateurs ;
- la personnalisation du produit.

2.2.3 *Architecture*

Le produit est un micro-module tachygraphe constitué de :

- un composant M7892 de Infineon Technologies AG, précédemment certifié (voir [CER_IC] ;
- une plateforme MultiApp 4.0.1 (dont la bibliothèque Crypto Thales et le système d'opérations) ;
- l'application *Tachograph Generation* V2 ;
- le *Tachograph Personalization Tool* (GDP) utilise seulement pendant la personnalisation du produit. GDP est détruit avant l'envoi à l'utilisateur final.



Une description plus détaillée de l'architecture du produit est donnée au chapitre 2 « *TOE Overview* » de [ST].

2.2.4 *Identification du produit*

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

Le composant ci-dessous est intégré dans le produit évalué (format CPE[1]) :

- cpe:1.0:h:infineon:M7892_G12:M7892_G12_20240708:*:*:*:*:*:*:*

La version certifiée du produit est identifiable par les éléments du tableau ci-après, détaillés dans le guide d'installation du produit [GUIDES] au chapitre 2.2.2 « *Product identification* ».

[1] CPE (Common Platform Enumeration) est un format d'identification des produits dont la grammaire est définie ici https://nvd.nist.gov/products/cpe

Eléments de configuration		Origine
Nom de la TOE	Smart Tachograph G2 on MultiApp V4.0.1	THALES DIS FRANCE SAS
Référence de la TOE	Tachograph Gen V2 on MultiApp V4.0.1	
Applet Label	'54 41 43 48 4f 47 52 41 50 48 20 47 32' (TACHOGRAPH. G2)	
Applet Version	'32 2e 30 2e 31 2e 47' (version 2.0.1.G) '32 2e 30 2e 31 2e 48' (version 2.0.1.H)	
Operating System Idenfier	'12 91'	
Operating System release date	'70 90'	
Operating System release level	'04 00' (MAV4.0)	
IC Fabricator	'40 90'	INFINEON TECHNOLOGIES AG
IC Type	'78 97' (M7892)	

Ces éléments peuvent être vérifiés en réponse à la commande READ BINARY (voir chapitre 2.2.2 « *Product Identification* » du guide d'installation du produit.

2.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit au chapitre 2.2.7 « *Life cycle description* » de la cible de sécurité [ST] ; il est conforme à celui décrit dans [PP0084].

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

Thales DIS La Ciotat [LVG] Thales DIS La Ciotat ZI Athelia IV, Avenue du Jujubier 13705 La Ciotat, France	**Thales DIS Singapore** [SGP] 12 Ayer Rajah Crescent Singapor 139941 Singapour
Thales DIS Meudon [MDN] 6 Rue de la Verrerie 92190 Meudon France	**Thales DIS Vantaa** [VAN] Myllynkivenkuja 4 Vantaa Finlande, FI-01620
Thales DIS Gémenos [GEM] Avenue du Pic de Bretagne 13881 Gémenos France	**Thales DIS Curitiba** [CBA] Rodovia Dep. Leopoldo Jacomel 13102 83323-410 Pinhais PR Brésil
THALES DIS Chanhassen [CHA] 1546 Lake Dr. W, Chanhassen, MN 55317,	**THALES DIS Montgomery** [MGY] 101 Park Drive Montgomeryville, PA 18936

United-States	USA
Sopra Steria Noida Chennai & Sopra Steria Chennai [SSN_SSC] Plot No. 20 & 21, Seaview Special Economic Zone, Building 4, Sector 135, Noida, Uttar Pradesh 201304 & 2/G-2 SIPCOT IT Park, Siruseri, Kanchipuram, Tamil Nadu 603103	**THALES DIS Calamba** [CAL] Building 7-A, Southern Luzon Industrial Complex Purok 3, Barangay Batino Calamba City, 4027 Laguna Philippines
THALES DIS Polska [TCZ] Ul. Skarszewska 2, 33-110 Tczew, Pologne Baldowska str 27, 83-110 Tczew, Pologne	**THALES DIS Pont-Audemer** [PAU] Z.I. Saint Ulfrant rue de Saint Ulfrant, 27500 Pont-Audemer France
THALES Telehouse [TLH] 65 rue Léon Frot 75011 Paris France	

2.2.6 *Configuration évaluée*

Le certificat porte sur le produit identifié au chapitre 2.2.4 et configuré comme suit :

- l'application *Smart Tachograph* G2 en version 2.0.1.G est instanciée et la plateforme est fermée sans possibilité de charger et d'instancier d'autres applications ;
- l'application *Smart Tachograph* G2 en version 2.0.1.H est instanciée et la plateforme est fermée sans possibilité de charger et d'instancier d'autres applications ;
- les recommandations des guides [GUIDES] sont strictement appliquées durant la phase « *Personnalisation* » du cycle de vie, ainsi que dans la phase de pré-personnalisation.

2.3 Contacts du produit

Les informations en matière de cybersécurité du produit sont disponibles ici :

https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/driving-licence/digital-tachograph-card-project

Le développeur peut être contacté via cette adresse : psirt@thalesgroup.com.

La procédure complète de signalement d'une vulnérabilité est disponible sur le lien suivant : PSIRT | Thales Group.

Les informations sur l'Autorité nationale de certification de cybersécurité en France sont disponibles ici https://cyber.gouv.fr/cybersecurity-act.

3 L'évaluation

3.1 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 et dispositifs similaires, le guide [JIWG AP] a été appliqué. 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).

3.2 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 dans le cadre d'un schéma national reconnu au titre de l'accord du SOG-IS.

Cette évaluation a ainsi pris en compte, en application du paragraphe 4 de l'article 8 d'[EUCC], les résultats de l'évaluation du microcontrôleur *« Infineon Security Controller M7892 Design Step G12, with specific IC dedicated firmware* », voir [CER_IC].

L'évaluation a également pris en compte les résultats d'évaluation du produit « Tachograph G2 on MultiApp v4.0.1, version 2.0.1.G et version 2.0.1.H » (voir [CER_S03]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 11 février 2025, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

3.3 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] afin de configurer le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

3.4 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.

4 La certification

4.1 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 et à [EUCC].

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 (voir chapitre 1 Résumé).

Le certificat associé à ce rapport, référencé EUCC-ANSSI-2025-03-02, a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité de cinq ans à partir de cette date.

Le certificat est délivré sous accréditation du COFRAC.

4.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 2.2 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 :

- Les restrictions d'utilisation : chapitres 3 « *Guidance for user role: administrator* » et 4 « *Guidance for user role: user* » du guide d'utilisation du produit ;
- Les exigences de déploiement (installation, configuration, contraintes matérielles (EUCC Annex V.1.9)) : chapitre 2.2 « *TOE acceptance by the personalizer* » du guide d'installation du produit ;
- Les exigences sur l'environnement : chapitres 3.1 et 4.1 « *IT environment* » du guide d'utilisation du produit.

4.3 Reconnaissance du certificat

4.3.1 *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 :

[2] 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 : - *Tachograph Generation V2 Security Target*, référence D1432172, version 1.64, 06 février 2025. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *Security Target Lite - Tachograph Generation V2*, référence D1432172, version 1.65p, 06 février 2025.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report POSEIDON-NS Project,* référence POSEIDON-NS_ETR_v1.1, version 1.1, 11 février 2025.
[CONF]	Liste de configuration du produit : - D1436010-LIS-DOC-TACHOV2, référence D1436010, version 3.2, 07 février 2025.
[GUIDES]	Guide d'installation du produit : - *AGD-PRE: Preparative procedures SMART TACHOGRAPH G2 on MultiApp V4.0.1*, référence D1436041, version 1.6, 29 juillet 2021. Guide d'administration du produit : - *Tachograph Generation 2 Personalization Manual (*Version G*)*, référence D1427389, version 1.P, 11 mars 2020 ; - *Tachograph Generation 2 Personalization Manual (*Pour version G & H*)*, référence D1427389, version 1.Pa, 28 juillet 2021 ; - *Annex to D1427389 (Tachograph Generation 2 personalization manual) Tachograph Generation 1 Personalization Manual*, référence D1518546, version1.Ba, 28 juillet 2021. Guide d'utilisation du produit : - *AGD-OPE : Operational user Guidance procedure SMART TACHOGRAPH G2 on MultiApp V4.0.1*, référence D1436050, version 1.4, 06 février 2025.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - DISGEN24_ALC_GEN_v1.1 **;** - [CBA] DISGEN23_CUR_STAR_v1.0 ; - [GEM] DISGEN24_GEM_STAR_v1.0 ; - [MDN] DISGEN23_MDN_STAR_v1.0 ; - [SGP] DISGEN24_SGP_STAR_v1.0 ; - [TCZ] DISGEN23-TCZ_STAR_v1.0 ; - [VAN] DISGEN23_VAN_STAR_v1.0 ; - [LVG] DISGEN24_LVG_STAR_v1.0 ; - [CAL] DISGEN23_VFOCAL_STAR_v1.0 ;

	- [CHA] DISGEN22_CHA_STAR_v1.0 ; - [MGY] DISGEN23_MGY_STAR_v1.0 ; - [PAU] DISGEN22_PAU_STAR_v1.0 ; - [SSN_SSC] DISGEN23_SSN_SSC_STAR_v1.0 ; - [TLH] DISGEN23_TLH_STAR_v1.0.
[CER_IC]	*Infineon Security Controller M7892 Design Step G12, with specific IC dedicated firmware*. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*), le 08 juillet 2024 sous la référence BSI-DSZ-CC-0891-V7-2024.
[CER_S03]	Rapport de surveillance ANSSI-CC-2018/11-S03 Smart Tachograph G2 on MultiApp V4.0.1, versions 2.0.1 G et 2.0.1 H, 28 septembre 2022.
[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.
[PP0091]	*Digital Tachograph –Tachograph Card (TC PP) Protection Profile*, version 1.0, 19 mai 2017. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-CC-PP-0091-2017.

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, ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.3.
[EUCC]	Schéma européen de certification de cybersécurité fondé sur les critères communs (règlement d'exécution (UE) 2024/482) et ses amendements.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P-01, version 4.1.
[CC]	*Information technology — Security techniques — Evaluation criteria for IT security* - *Part 1: Introduction and general model:* ISO/IEC 15408-1:2009 ; - *Part 2: Security functional components:* ISO/IEC 15408-2:2008 ; - *Part 3: Security Assurance components:* ISO/IEC 15408-3:2008 ; - et correctifs techniques associés. Equivalent à la version CCRA: - *Common Criteria for Information Technology Security Evaluation* version 3.1, révision 5, parties 1 à 3, références CCMB-2017-04-001 à CCMB-2017-04-003.
[CEM]	*Information technology — Security techniques — Methodology for IT security evaluation,* ISO/IEC 18045:2008, et correctifs techniques associés. Equivalent à la version CCRA: *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG AP] *	*Mandatory Technical Document – Application of attack potential to smartcards and similar devices*, version 3.2.1, février 2024.
[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 2.0, mai 2024.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014.
[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.

*Dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.