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-2022/38-R01

## Tachograph G1, G2V1, G2V2 on IFX_CCI_000039h (version 2.2.1.N)

Paris, le 17 Mars 2025

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

Vincent STRUBEL

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

# 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).

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

# TABLE DES MATIERES

# 1 Résumé

| |
|---|
| Référence du rapport de certification<br>**ANSSI-CC-2022/38-R01** |
| Nom du produit<br>**Tachograph G1, G2V1, G2V2 on IFX_CCI_000039h** |
| Référence/version du produit<br>**version 2.2.1.N** |
| Type de produit<br>**Cartes à puce et dispositifs similaires** |
| Conformité à un profil de protection<br>***Digital Tachograph – Smart Card (Tachograph Card)***<br>**référence BSI-CC-PP-0070, version 1.02, 15 novembre 2011**<br>certifié sous la référence BSI-CC-PP-0070-2011<br><br>***Digital Tachograph – Tachograph Card (TC PP)*, version 1.0, 9 Mai 2017**<br>certifié sous la référence BSI-CC-PP-0091-2017 |
| Critère d'évaluation et version<br>**Critères Communs version 3.1 révision 5** |
| Niveau d'évaluation<br>**EAL 4 augmenté**<br>ALC_DVS.2, ATE_DPT.2, AVA_VAN.5 |
| Référence du rapport d'évaluation<br>*Evaluation Technical Report - POSEIDON220-R01*<br>référence LETI.CESTI.POSR01.FULL.001<br>version 1.1<br>28/02/2025 |
| Fonctionnalité de sécurité du produit<br>Cf. 2.2.2 Services de sécurité |
| Exigences de configuration du produit<br>Cf. 4.2 Restrictions d'usage |
| Hypothèses liées à l'environnement d'exploitation<br>Cf. 4.2 Restrictions d'usage |
| Développeur<br>**THALES DIS**<br>6 rue de la Verrerie<br>92190 Meudon, France |
| Commanditaire<br>**THALES DIS**<br>6 rue de la Verrerie<br>92190 Meudon, France |

Centre d'évaluation

**CEA - LETI**

17 avenue des martyrs,
38054 Grenoble Cedex 9, France
35000 Rennes, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat est reconnu au niveau EAL2.

# 2 Le produit

## 2.1 Présentation du produit

Le produit évalué est « Tachograph G1, G2V1, G2V2 on IFX_CCI_000039h, version 2.2.1.N » développé par THALES DIS.

Ce produit est destiné à être utilisé 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 aux profils de protection [PP70] et [PP91].

### 2.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

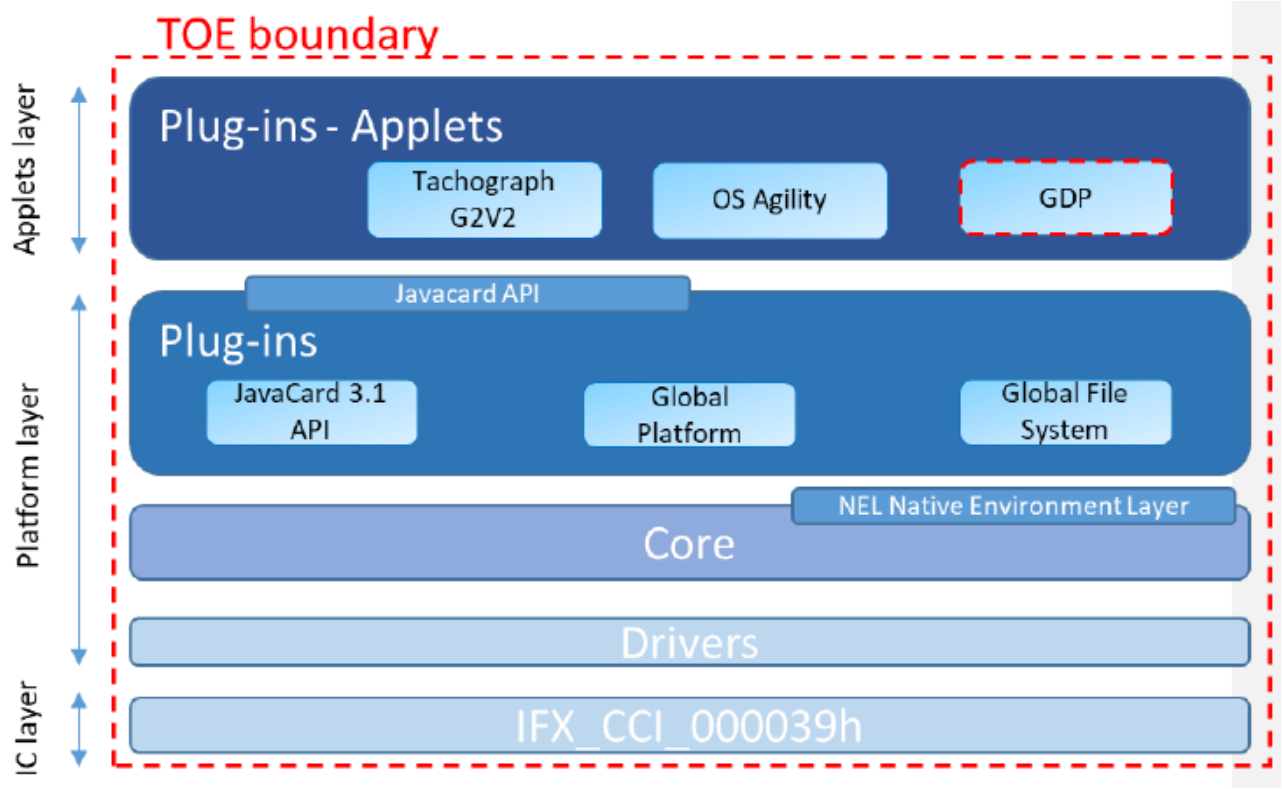
- Indentification et authentification de l'utilisateur
- l'authentification mutuelle Gen1 ou Gen2 ;
- le stockage de l'identification de la carte et des données du porteur ;
- le stockage des données d'activité ;
- la vérification des certificats Gen1 et Gen2 ;
- la génération de signature des données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

Le produit est une plateforme *JavaCard* qui ne permet pas l'installation d'autres applications post-émission.

### 2.2.3 *Architecture*

Le produit est principalement constitué :

- du composant IFX_CCI_000039 (SLC37) précédemment certifié (voir [CER_IC]) ;
- d'un système d'exploitation MultiApp V5.0 sous forme d'une plateforme *JavaCard* en configuration fermée ;
- de l'application OS-Agility dédiée au chargement de patch ;
- de l'application Tachograph G2V2.
-




### 2.2.4 *Identification du produit*

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

La version certifiée du produit est identifiable comme décrit dans le document « *Traceability* » des [GUIDES].

### 2.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit au paragraphe 1.8.5 de la cible de sécurité (voir [ST]).

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

| | |
|---|---|
| **Thales DIS La Ciotat** [LVG]<br><br>Thales DIS La Ciotat<br>ZI Athelia IV, Avenue du Jujubier<br>13705 La Ciotat,<br>France | **Thales DIS Meudon** [MDN]<br><br>6 Rue de la Verrerie<br>92190 Meudon<br>France |
| **Thales DIS Vantaa** [VAN]<br><br>Myllynkivenkuja 4<br>Vantaa<br>Finlande, FI-01620 | **Thales DIS Gémenos** [GEM]<br><br>Avenue du Pic de Bretagne<br>13881 Gémenos<br>France |
| **Thales DIS Singapore** [SGP]<br><br>12 Ayer Rajah Crescent<br>Singapor 139941<br>Singapour | **THALES DIS Polska** [TCZ]<br><br>Ul. Skarszewska 2, 33-110 Tczew; POLAND<br>Baldowska str 27, 83-110 Tczew; POLAND<br>(extension site) |
| **THALES DIS Chanhassen** [CHA]<br><br>1546 Lake Dr. W, Chanhassen,<br>MN 55317,<br>United-States | **Thales DIS Curitiba** [CBA]<br><br>Rodovia Dep. Leopoldo Jacomel<br>13102 83323-410 Pinhais<br>PR Brésil |
| **THALES DIS Pont-Audemer** [PAU]<br><br>Z.I. Saint Ulfrant rue de Saint Ulfrant,<br>27500 Pont Audemer<br>France | **THALES DIS Montgomery** [MGY]<br><br>101 Park Drive Montgomeryville,<br>PA 18936<br>USA |
| **THALES DIS Calamba** [CAL]<br><br>Building 7-A, Southern Luzon Industrial Complex Purok 3,<br>Barangay Batino Calamba City,<br>4027 Laguna<br>Philippines | **THALES DIS Chennai** [SST]<br><br>2/G-2 SIPCOT IT Park, Siruseri, Kanchipuram,<br>Tamil Nadu<br>603103 |
| **Sopra Steria Noida** [SST]<br><br>Plot No. 20 & 21, Seaview Special Economic Zone,<br>Building 4, Sector 135, Noida, Uttar Pradesh<br>201304 | **THALES Telehouse** [TLH]<br><br>65 rue Léon Frot<br>75011 Paris<br>France |

### 2.2.6 *Configuration évaluée*

Le certificat porte sur les configurations suivantes (sélectionnées au moment de la personnalisation de la carte) :

- Application Tachograph G1 v1.6;
- Application Tachograph G2V1;
- Application Tachograph G2V2

# 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, les guides [COMP] 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).

## 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 par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « IFX_CCI_000039 (SLC37) », voir [CER_IC].

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** ».

## 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 [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.

## 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 potentiel d'attaque 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.

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 (Cf § 1 Résumé).

Le certificat associé à ce rapport, référencé ANSSI-CC-2022/38-R01, 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.

## 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].

## 4.3 Reconnaissance du certificat

### 4.3.1 *Reconnaissance européenne (SOG-IS)*

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

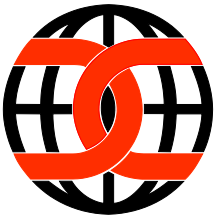
L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :


### 4.3.2 *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[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 :



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

[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 :<br>- *SECURITY TARGET TACHOGRAPH G1, G2V1, G2V2 ON IFX_CCI_000039H*, D1551037, version 1.7, 11 octobre 2024.<br>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :<br>- *SECURITY TARGET PUBLIC VERSION TACHOGRAPH G1, G2V1, G2V2 ON IFX_CCI_000039H*, D1551037, version 1.7p, 11 octobre 2024. |
| [RTE] | Rapport technique d'évaluation :<br>*Evaluation technical report – POSEIDON220-R01*, référence LETI.CESTI.POSR01.FULL.001 - V1.1, version 1.1, 28 février 2025 |
| [ANA_CRY] | « *Cotation des mécanismes cryptographiques- POSEIDON* », référence LETI.CESTI.POS.RT.007- V1.2 du 2 août 2022. |
| [CONF] | Liste de configuration du produit :<br>- ROR29917_ALC_LIS, référence R0R29917_ALC_LIS, version 1.8, 21/06/22<br>- *Source code filelisting*, référence filelisting_SGP-RND-GP-17, version R009, 13/09/2022. |
| [GUIDES] | - *Tachograph Generation 1 (version 1.6) - Personalization Manual*, référence D1564669, version 1.G, 13/09/22 ;<br>- *Tachograph Generation 2 Version 2 & Tachograph - Generation 2 Version 1 Personalization Manual*, référence D1549733, version 1.J, 13/09/22 ;<br>- *Tachograph G1, G2V1, G2V2 on IFX_CCI_000039h Traceability information*, référence D1559331, version H, 13/09/22 ;<br>- *AGD_OPE document TACHOGRAPH G2V2*, référence D1551042, version 1.2, 07/04/22 ;<br>- *AGD_PRE document TACHOGRAPH G2V2*, référence D1551041, version 1.3, 07/04/22. |
| [SITES] | Rapports d'analyse documentaire et d'audit de site pour la réutilisation :<br>- *Thales DIS Development Environment ALC Class Evaluation Report (Generic Documentary activities)*, DISGEN24_ALC_GEN_v1.1, 11 octobre 2024 ;<br>- [LVG] *Site Technical Audit Report Thales DIS La Ciotat*, DISGEN24_LVG_STAR_v1.0, 23 octobre 2024 ;<br>- [MDN] *Site Technical Audit Report Thales DIS Meudon*, DISGEN23_MDN_STAR_v1.0, 14 février 2024 ;<br>- [VAN] *Site Technical Audit Report Thales DIS Vantaa*, DISGEN23_VAN_STAR_v1.0, 2 mai 2023 ;<br>- [GEM] *Site Technical Audit Report Thales DIS Gémenos*, DISGEN24_GEM_STAR_v1.0, 18 octobre 2024 ; |

| | |
|---|---|
| | - [SGP] *Site Technical Audit Report Thales DIS PTE LTD*, DISGEN24_SGP_STAR_v1.0, 8 octobre 2024;<br>- [TCZ] *Site Technical Audit Report THALES DIS Polska Sp. Zo.o*, DISGEN23-TCZ_STAR_v1.0, 25 avril 2023 ;<br>- [CHA] *Site Technical Audit Report Thales DIS USA Inc.*, *DISGEN22_CHA_STAR_v1.0, 10 mars 2023* ;<br>- [CBA] *Site Technical Audit Report Thales DIS Curitiba*, DISGEN23_CUR_STAR_v1.0, 22 juin 2023 ;<br>- [PAU] *Site Technical Audit Report Thales DIS Pont-Audemer*, DISGEN22_PAU_STAR_v1.0, 5 décembre 2022 ;<br>- [MGY] *Site Technical Audit Report Thales DIS Montgomeryville*, DISGEN23_MGY_STAR_v1.0, 23 juin 2023 ;<br>- [CAL] *Site Technical Audit Report Verizon Thales DIS Calamba*, DISGEN23_VFO-CAL_STAR_v1.0, 10 août 2023 ;<br>- [SST] *Site Technical Audit Report Sopra Steria Noida & Sopra Steria Chennai*, DISGEN23_SSN_ SSC_STAR_v1.0, 19 mars 2024 ;<br>- [TLH] *Site Technical Audit Report Telehouse*, DISGEN23_TLH_ STAR_v1.0, 19 mars 2024 |
| [CER_IC] | Produit Infineon IFX_CCI_000039 (SLC37)<br>Certifié par le BSI sous la référence BSI-DSZ-CC-1107-V5-2024 le 4 septembre 2024 |
| [PP70] | *Digital Tachograph – Smart Card (Tachograph Card P)*, référence BSI-CC-PP-0070, version 1.02, 15 novembre 2011.<br>*Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0070-2011.* |
| [PP91] | *Digital Tachograph – Tachograph Card (TC PP), version 1.0, 9 May 2017.*<br>*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 5.0. |
| [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:*<br>- *Part 1 : Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ;<br>- *Part 2 : Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ;<br>- *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 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. |
| [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.