



**PREMIER  
MINISTRE**

*Liberté  
Égalité  
Fraternité*

**Secrétariat général de la défense  
et de la sécurité nationale**

Agence nationale de la sécurité  
des systèmes d'information

## **Certification report EUCC-ANSSI-2025-03-02**

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

Paris, the 31/03/2025

**COURTESY TRANSLATION**



## WARNING

This report is intended to provide people who request evaluations with a document to certify the level of security provided by the product under the usage or operating conditions defined in this report for the version which was evaluated. It is also intended to provide potential acquirers of the product with the conditions under which they may use the product to ensure that they meet the conditions for which the product was evaluated and certified; this is why the certification report must be read in conjunction with the evaluated usage and administration guides and with the product's security target which describes the pre-supposed threats, environmental hypotheses and usage conditions so that the user can judge whether the product is suitable for their needs in terms of security objectives.

The certification does not in itself constitute a product recommendation by the Agence nationale de la sécurité des systèmes d'information (ANSSI) and does not guarantee that the certified product is completely free of vulnerabilities that can be exploited.

All correspondence related to this report must be sent to:

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](mailto:certification@ssi.gouv.fr)

Reproduction of this document without alteration or cutting is authorized.

## FOREWORD

Certification of the security provided by information technology products and systems is governed by amended decree 2002-535 of 18th April 2002. This decree indicates that:

- The *Agence nationale de la sécurité des systèmes d'information* drafts the certification reports. These reports specify the characteristics of the security objectives proposed. They may contain any warnings that their authors consider are worth mentioning for security reasons.
- The certificates awarded by the *directeur général de l'Agence nationale de la sécurité des systèmes d'information* certify that the individual product or system submitted for evaluation meets the specified security characteristics. They also certify that the evaluations were carried out according to current rules and standards, with the required levels of competence and impartiality (article 8).

This report is in compliance with [EUCC].

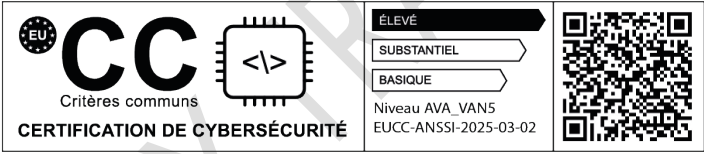

The certification procedures are available on the website [www.cyber.gouv.fr](http://www.cyber.gouv.fr).

## TABLE DES MATIERES

1	Summary .....	5
2	Product .....	7
2.1	Product presentation .....	7
2.2	Product description .....	7
2.2.1	Introduction .....	7
2.2.2	Security services .....	7
2.2.3	Architecture .....	8
2.2.4	Product identification.....	8
2.2.5	Lifecycle .....	9
2.2.6	Evaluated configuration .....	10
2.3	Product contacts.....	11
3	Evaluation.....	12
3.1	Evaluation reference bases.....	12
3.2	Evaluation work .....	12
3.3	Analysis of cryptographic mechanisms according to ANSSI technical standards .....	13
3.4	Random number generator.....	13
4	La certification .....	14
4.1	Conclusion.....	14
4.2	Usage restrictions.....	14
4.3	Certificate recognition.....	15
4.3.1	International Common Criteria Recognition (CCRA).....	15
ANNEXE A.	Documentary references for the product evaluated .....	16
ANNEXE B.	Certification references .....	18

## 1 Summary

Reference of the certification report	<b>EUCC-ANSSI-2025-03-02</b>
Product name	<b>Smart Tachograph G2 on MultiApp V4.0.1</b>
Product reference/version	<b>Versions 2.0.1 G and 2.0.1 H</b>
Type of product	<b>Smartcards and Similar Devices</b>
Protection profile compliance	<b>Digital Tachograph –Tachograph Card (TC PP) Protection Profile,</b> certified BSI-CC-PP-0091-2017, 19/05/2017, version 1.0
Evaluation criteria and version	<b>ISO/IEC 15408-1:2009, 15408-2:2008, 15408-3:2008</b> <b>(Critères Communs version 3.1 revision 5)</b> <b>ISO/IEC 18045:2008</b> <b>(CEM version 3.1 revision 5)</b>
Evaluation level	<b>High / EAL4 augmented</b> ALC_DVS.2, ATE_DPT.2, AVA_VAN.5
Evaluation report reference	<i>Evaluation Technical Report POSEIDON-NS Project</i> Ref. POSEIDON-NS_ETR_v1.1 version 1.1 11/02/2025
Product's security features	see 2.2.2 Security services
Threat summary	<i>Threat T.Identification_Data</i> <i>Threat T.Application</i> <i>Threat T.Activity_Data</i> <i>Threat T.Data_Exchange</i> <i>Threat T.Clone</i> <i>Duplication de la carte</i>  see chapitre 4.3 of Security Target [ST]
Product configuration requirements	see 4.2 Usage restrictions

Operating environment assumptions	see 4.2 Usage restrictions
Developer	<b>THALES DIS FRANCE SAS</b> Avenue du Jujubier ZI Athelia IV 13705 La Ciotat Cedex France
Sponsor	<b>THALES DIS FRANCE SAS</b> Avenue du Jujubier ZI Athelia IV 13705 La Ciotat Cedex France
Evaluation center (ITSEF)	<b>SERMA SAFETY &amp; SECURITY</b> 14 rue Galilée, CS 10071, 33608 Pessac Cedex, France
EUCC mark	 <p>The EUCC mark logo consists of three parts: on the left, the 'EU' flag and 'CC' with 'Critères communs' below it; in the center, a chip icon with '&lt;/&gt;' and 'CERTIFICATION DE CYBERSÉCURITÉ' below it; on the right, a table with levels: 'ÉLEVÉ' (selected), 'SUBSTANTIEL', and 'BASIQUE', followed by 'Niveau AVA_VAN5' and 'EUCC-ANSSI-2025-03-02', and a QR code.</p>
Applicable recognition agreements	 <p>The CCRA logo features the letters 'CCRA' above a stylized globe with red and black horizontal stripes.</p> <p>This certificate is recognized at EAL2.</p>

## 2 Product

### 2.1 Product presentation

The product evaluated is « Smart Tachograph G2 on MultiApp V4.0.1, Versions 2.0.1 G and 2.0.1 H » developed by THALES DIS FRANCE SAS.

This product is intended to be used by tachographs products (devices to record the activities of public transport vehicles) or by personal computers (to perform control operations on the vehicle activities).

This product is intended for use with electronic tachographs (equipment for recording the activities of a road transport vehicle) or with personal computers (to perform vehicle activity monitoring operations). The main functions of this card are:

- storage of card and cardholder identifiers to identify the cardholder, grant appropriate access rights to functions and data, and ensure activity attribution;
- storage of information related to the cardholder's activity.

### 2.2 Product description

#### 2.2.1 Introduction

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operating environment.

This security target complies with the protection profile [PP0091].

#### 2.2.2 Security services

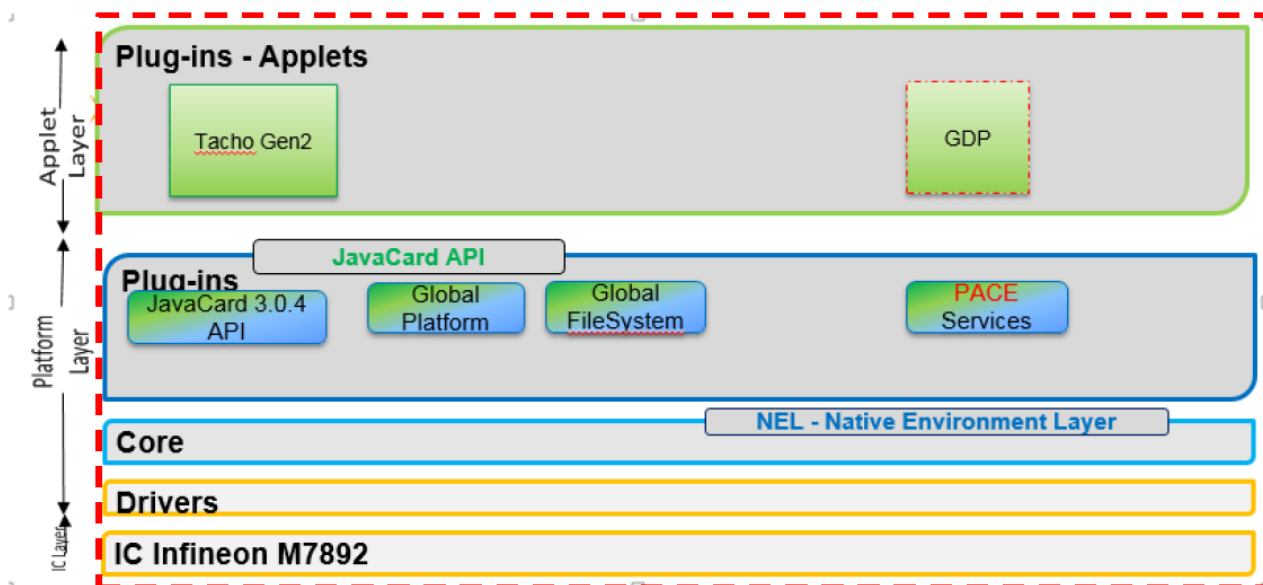
The main security services provided by the product, described at chapter 2.1 « TOE Description » of [ST], are:

- Enforce Mutual authentication Gen1 or Gen2
- Storing of card identification and card holder identification data
- Storing of Activity data (events, control activities data, faults data)
- Perform the verification of certificate Gen1 and Gen2
- Generate signature on internal data to export
- Perform the verification (integrity, authenticity) of a DSRC message
- Downloading of User Data
- Personalization of the product

### 2.2.3 Architecture

The product is composed of:

- M7892 IC which has been certified separately [CER\_IC]
- MultiApp 4.0.1 platform (including the crypto library and the OS)
- TACHO Gen2 application
- GDP application (only used during personalization and removed before the sending the final user).



A more detailed architecture is described at chapter 2 « TOE Overview » of [ST].

### 2.2.4 Product identification

The elements integrated in the product are identified in [CONF].

The following component is integrated to the product: (CPE format<sup>1</sup>):

- cpe:1.0:h:infineon:M7892\_G12:M7892\_G12\_20240708:\*\*\*\*\*

The certified version of the product is defined by the following table, detailed in [GUIDES], chapter 2.2.2 « Product identification ».

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



Configuration item		Origin
TOE name	Smart Tachograph G2 on MultiApp V4.0.1	THALES DIS FRANCE SAS
TOE ref	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 Identifier	'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)	

Those items can be verified with the command READ BINARY (see chapter 2.2.2 « *Product Identification* » of the setup guide).

#### 2.2.5 Lifecycle

The product lifecycle is described in [ST] section 2.2.7 « *Life cycle description* » and is consistent to [PP0084].

The product has been developed on the sites described below (see [SITES]):

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

United-States	USA
<b>Sopra Steria Noida Chennai &amp; Sopra Steria Chennai [SSN_SSC]</b> 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	<b>THALES DIS Calamba [CAL]</b> Building 7-A, Southern Luzon Industrial Complex Purok 3, Barangay Batino Calamba City, 4027 Laguna Philippines
<b>THALES DIS Polska [TCZ]</b> Ul. Skarszewska 2, 33-110 Tczew, Pologne Baldowska str 27, 83-110 Tczew, Pologne	<b>THALES DIS Pont-Audemer [PAU]</b> Z.I. Saint Ulfrant rue de Saint Ulfrant, 27500 Pont-Audemer France
<b>THALES Telehouse [TLH]</b> 65 rue Léon Frot 75011 Paris France	

#### 2.2.6 Evaluated configuration

The certificate relates to the product identified section 2.2.4 and configured as follow:

- Application *Smart Tachograph G2* (version 2.0.1.G) is instantiated and the platform is closed without any possibility to load other applications;
- Application *Smart Tachograph G2* (version 2.0.1.H) is instantiated and the platform is closed without any possibility to load other applications;
- Recommendations in [GUIDES] are strictly applied during the phase « Personalisation » of the lifecycle, and during the phase pre-personalisation.

## 2.3 Product contacts

The product's cybersecurity information is available here:

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

The developer can be contacted at this address: [psirt@thalesgroup.com](mailto:psirt@thalesgroup.com).

The complete procedure for the vulnerability handling is available here: [PSIRT | Thales Group](#).

Information on France's National Cybersecurity Certification Authority is available here <https://cyber.gouv.fr/cybersecurity-act>.

### 3 Evaluation

#### 3.1 Evaluation reference bases

The evaluation was carried out in accordance with the Common Criteria [CC], and with the evaluation methodology defined in the manual [CEM].

For assurance components not covered by the [CEM] manual, methods specific to the evaluation center and validated by ANSSI have been used.

To meet the specific requirements of Smart cards and similar devices, the [JIWG AP] guides were applied. Thus, the AVA\_VAN level has been determined using the rating scale of the [JIWG AP] guide. As a reminder, this rating scale is more demanding than the one defined by default in the standard [CC] method, used for other product categories (software products, for example).

#### 3.2 Evaluation work

The compositional evaluation was carried out in accordance with the [COMP] guide, enabling us to check that no weaknesses are introduced by integrating the software into the microcontroller already certified.

This evaluation thus took into account, in application of paragraph 4 of article 8 of [EUCC], the results of the evaluation of the microcontroller « Infineon Security Controller M7892 Design Step G12, with specific IC dedicated firmware », see [CER\_IC].

The evaluation is based on the results of the evaluation of the same product certified on « Tachograph G2 on MultiApp v4.0.1, version 2.0.1.G et version 2.0.1.H » (see [CER\_S03]).

The evaluation technical report [ETR], which was delivered to the ANSSI on 11/2/25, details the work carried out by the evaluation center and attests that all the evaluation tasks are rated as « **PASS** » .

### 3.3 Analysis of cryptographic mechanisms according to ANSSI technical standards

The cryptographic mechanisms implemented by the product's security functions (see [ST]) have been analyzed in accordance with procedure [CRY-P-01] and the results recorded in report [ETR].

This analysis identified the following non-conformities with respect to the standard [ANSSI Crypto]. They were taken into account in the independent vulnerability analysis carried out by the evaluator and did not reveal any exploitable vulnerabilities for the targeted level of attacker.

The user must refer to the [GUIDES] to configure the product in accordance with the [ANSSI Crypto], for the cryptographic mechanisms that enable it.

### 3.4 Random number generator

The RNG, which is physical and used by the final product, has been assessed through the microcontroller assessment (see [CER\_IC]).

As required by [ANSSI Crypto], the output of a hardware random number generator must undergo cryptographic algorithmic reprocessing.

The independent vulnerability analysis conducted by the evaluator did not reveal any exploitable vulnerabilities for the targeted attacker level.

## 4 La certification

### 4.1 Conclusion

The evaluation was carried out according to current rules and standards with the levels of competence and impartiality required for an approved evaluation body. All of the evaluation work carried out enables a certificate to be issued according to decree 2002-535 and to [EUCC].

This certificate attests that the product under evaluation meets the security requirements specified in its security target [ST] for the intended evaluation level (see chapter 1 Summary).

The certificate associated with this report, referenced EUCC-ANSSI-2025-03-02, has a date of issue identical to the date of signature of this report and is valid for five years from that date.

The certificate is issued under COFRAC accreditation.

### 4.2 Usage restrictions

This certificate relates to the product specified in chapter 2.2 of this report.

The user of the certified product must ensure compliance with the security objectives for the operating environment, as specified in the security target [ST], and follow the recommendations in the guides provided [GUIDES]. In particular :

- Restrictions on use: chapter 3 « *Guidance for user role: administrator* » and chapter 4 « *Guidance for user role: user* » of product user guidance;
- Deployment and environmental requirements (EUCC Annex V.1.9): chapter 2.2 « *TOE acceptance by the personalizer* » and chapter 3.1 and 4.1 « *IT environment* » of the setup guide.

### 4.3 Certificate recognition

#### 4.3.1 International Common Criteria Recognition (CCRA)

This certificate is issued under the conditions of the CCRA agreement [CCRA].

The « Common Criteria Recognition Arrangement » enables recognition of the Common Criteria certificates by the signatory countries<sup>2</sup>.

Recognition applies up to the assurance components of CC EAL2 level as well as the ALC\_FLR family. Certificates recognized under this agreement are issued with the following mark:



---

<sup>2</sup> The list of signatory countries of the CCRA arrangement is available on the website [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org).

## ANNEXE A. Documentary references for the product evaluated

[ST]	<p>Security target for the evaluation:</p> <ul style="list-style-type: none"> <li>- <i>Tachograph Generation V2 Security Target</i>, reference D1432172, version 1.64, 06/02/2025.</li> </ul> <p>For publication purposes, the following security target has been provided and validated as part of this evaluation:</p> <ul style="list-style-type: none"> <li>- <i>Security Target Lite - Tachograph Generation V2</i>, reference D1432172, version 1.65p, 06/02/2025.</li> </ul>
[ETR]	<p>Evaluation Technical Report :</p> <ul style="list-style-type: none"> <li>- <i>Evaluation Technical Report POSEIDON-NS Project</i>, reference POSEIDON-NS_ETR_v1.1, version 1.1, 11/2/2025.</li> </ul>
[CONF]	<p>Configuration list :</p> <ul style="list-style-type: none"> <li>- D1436010-LIS-DOC-TACHOV2, reference D1436010, version 3.2, 07/02/2025.</li> </ul>
[GUIDES]	<p>Set up guide :</p> <ul style="list-style-type: none"> <li>- <i>AGD-PRE: Preparative procedures SMART TACHOGRAPH G2 on MultiApp V4.0.1</i>, reference D1436041, version 1.6, 29/07/2021.</li> </ul> <p>Administration guide :</p> <ul style="list-style-type: none"> <li>- <i>Tachograph Generation 2 Personalization Manual (Version G)</i>, reference D1427389, version 1.P, 11/03/2020 ;</li> <li>- <i>Tachograph Generation 2 Personalization Manual (Pour version G &amp; H)</i>, reference D1427389, version 1.Pa, 28/07/2021 ;</li> <li>- <i>Annex to D1427389 (Tachograph Generation 2 personalization manual)</i></li> </ul> <p><i>Tachograph Generation 1 Personalization Manual</i>, reference D1518546, version 1.Ba, 28/07/2021.</p> <p>User guidance :</p> <ul style="list-style-type: none"> <li>- <i>AGD-OPE : Operational user Guidance procedure SMART TACHOGRAPH G2 on MultiApp V4.0.1</i>, reference D1436050, version 1.4, 06/02/2025.</li> </ul>
[SITES]	<p>Document analysis and site audit reports for reuse:</p> <ul style="list-style-type: none"> <li>- DISGEN24_ALC_GEN_v1.1 ;</li> <li>- [CBA] DISGEN23_CUR_STAR_v1.0 ;</li> <li>- [GEM] DISGEN24_GEM_STAR_v1.0 ;</li> <li>- [MDN] DISGEN23_MDN_STAR_v1.0 ;</li> <li>- [SGP] DISGEN24_SGP_STAR_v1.0 ;</li> <li>- [TCZ] DISGEN23-TCZ_STAR_v1.0 ;</li> <li>- [VAN] DISGEN23_VAN_STAR_v1.0 ;</li> <li>- [LVG] DISGEN24_LVG_STAR_v1.0 ;</li> <li>- [CAL] DISGEN23_VFOCAL_STAR_v1.0 ;</li> </ul>



	<ul style="list-style-type: none"> <li>- [CHA] DISGEN22_CHA_STAR_v1.0 ;</li> <li>- [MGY] DISGEN23_MGY_STAR_v1.0 ;</li> <li>- [PAU] DISGEN22_PAU_STAR_v1.0 ;</li> <li>- [SSN_SSC] DISGEN23_SSN_SSC_STAR_v1.0 ;</li> <li>- [TLH] DISGEN23_TLH_STAR_v1.0.</li> </ul>
[CER_IC]	<p><i>Infineon Security Controller M7892 Design Step G12, with specific IC dedicated firmware.</i></p> <p>Certified by BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>), 08/07/2024, reference BSI-DSZ-CC-0891-V7-2024.</p>
[CER_S03]	<p>Surveillance report ANSSI-CC-2018/11-S03 Smart Tachograph G2 on MultiApp V4.0.1, versions 2.0.1 G and 2.0.1 H, 28/09/2022.</p>
[PP0084]	<p><i>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages</i>, version 1.0, 13/01/2014.</p> <p>Certified by BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>), reference BSI-PP-0084-2014.</p>
[PP0091]	<p><i>Digital Tachograph –Tachograph Card (TC PP) Protection Profile</i>, version 1.0, 19/05/2017.</p> <p>Certified by BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>), reference BSI-CC-PP-0091-2017.</p>

## ANNEXE B. Certification references

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 procedure of the security provided by information technology products and systems, reference ANSSI-CC-CER-P-01, version 5.3.
[EUCC]	European cybersecurity certification scheme based on common criteria (implementing regulation (EU) 2024/482) and its amendments.
[CRY-P-01]	Methods for carrying out cryptographic analyses, reference ANSSI-CC-CRY-P01, version 4.1.
[CC]	<p><i>Information technology — Security techniques — Evaluation criteria for IT security</i></p> <ul style="list-style-type: none"> <li>- Part 1: Introduction and general model: ISO/IEC 15408-1:2009 ;</li> <li>- Part 2: Security functional components: ISO/IEC 15408-2:2008 ;</li> <li>- Part 3: Security Assurance components: ISO/IEC 15408-3:2008 ;</li> <li>- et correctifs techniques associés.</li> </ul> <p>Equivalent to CCRA version:</p> <ul style="list-style-type: none"> <li>- Common Criteria for Information Technology Security Evaluation version 3.1, revision 5, part 1 to 3, references CCMB-2017-04-001 to CCMB-2017-04-003.</li> </ul>
[CEM]	<p><i>Information technology — Security techniques — Methodology for IT security evaluation</i>, ISO/IEC 18045:2008, and associated technical fixes.</p> <p>Equivalent to CCRA version :</p> <p><i>Common Methodology for Information Technology Security Evaluation, Evaluation Methodology</i>, version 3.1, revision 5, reference CCMB-2017-04-004.</p>
[JIWG AP] *	<i>Mandatory Technical Document – Application of attack potential to smartcards and similar devices</i> , version 3.2.1, February 2024.
[COMP] *	<i>Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices</i> , version 1.5.1, May 2018.
[OPEN]	<i>Certification of « Open » smart card products</i> , version 2.0, May 2024.
[CCRA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security</i> , 2/07/2014.
[ANSSI Crypto]	Guide to cryptographic mechanisms: Rules and recommendations concerning the choice and sizing of cryptographic mechanisms, ANSSI-PG-083, version 2.04, January 2020.

\* SOG-IS document; under the CCRA recognition agreement, the equivalent CCRA support document applies.