Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

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 / Certification report EUCC-3090-2026-65

CombICAO Applet v2.2 in EAC configuration on ID-ONE Cosmo V9.1 (ref. 203731)

Paris, le 8/6/2026 | 18:45 CEST

Vincent Strubel

Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

AVERTISSEMENT / *WARNING*

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.

This report is intended to provide individuals requesting evaluations with a document certifying the level of security provided by the product, under the usage or operating conditions defined in this report, for the version that was evaluated.

It is also intended to inform potential purchasers of the product about the conditions under which it can be used to ensure compliance with the requirements for which the product was evaluated and certified. For this reason, the certification report must be read in conjunction with the evaluated usage and administration guides, as well as the product's security target, which describes the assumed threats, environmental assumptions, and usage conditions. This allows users to determine whether the product meets their security objectives.

The certification itself does not constitute a product endorsement by the Agence nationale de la sécurité des systèmes d'information (ANSSI), nor does it guarantee that the certified product is entirely free from exploitable vulnerabilities.

Toute correspondance relative à ce rapport doit être adressée au :

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

La reproduction de ce document sans altération ni coupure est autorisée.
Reproduction of this document without alteration or cutting is authorized.

Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

PREFACE / *FOREWORD*

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;
- 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).

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

- *The Agence nationale de la sécurité des systèmes d'information drafts the certification reports. These reports specify the characteristics of the proposed security objectives. They may include any warnings authors deem necessary to mention for security reasons.*
- *The certificates issued by the Director General of ANSSI certify that the specific product or system submitted for evaluation meets the defined security characteristics. They also confirm that the evaluations were carried out according to current rules and standards, with the required levels of competence and impartiality (Article 8).*

Ce rapport est conforme à [EUCC].
This report is in compliance with [EUCC].

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

The certification procedures are available on the website www.cyber.gouv.fr.

Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

TABLE DES MATIERES / *TABLE OF CONTENT*

1 Résumé / *Summary* 5
2 Le produit / *Product* 7
2.1 Présentation du produit / *Product presentation* 7
2.2 Description du produit / *Product description* 7
2.2.1 Introduction 7
2.2.2 Services de sécurité / Security services 7
2.2.3 Architecture 7
2.2.4 Identification du produit / Product identification 8
2.2.5 Cycle de vie / Life cycle 8
2.2.6 Configuration évaluée / Evaluated configuration 8
2.3 Contacts du produit / *Product contacts* 9
3 L'évaluation / *Evaluation* 10
3.1 Référentiels d'évaluation / *Evaluation reference bases* 10
3.2 Travaux d'évaluation / *Evaluation tasks* 10
3.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI / *Analysis of cryptographic mechanisms according to ANSSI technical standards* 11
4 La certification / *Certification* 12
4.1 Conclusion / *Conclusion* 12
4.2 Restrictions d'usage / Use *Restriction* 12
4.3 Reconnaissance du certificat / *Certificate recognition* 13
4.3.1 Reconnaissance internationale critères communs (CCRA) / International Common Criteria Recognition 13
ANNEXE A. Références documentaires du produit évalué / *Documentary references for the product evaluated* 14
ANNEXE B. Références liées à la certification / Certification references 15

Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

1 Résumé / *Summary*

Référence du rapport de certification / *Certification report reference*

EUCC-3090-2026-65

Nom du produit / *Product name*

CombICAO Applet v2.2 in EAC configuration on ID-ONE Cosmo V9.1

Référence/version du produit / *Product reference/version*

ref. 203731

Type de produit / *Type of product*

Cartes à puce et dispositifs similaires
(Smart cards and similar devices)

Conformité à un profil de protection / *Conformity with a protection profile*

Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control,
version 1.10, BSI-CC-PP-0056-2009**.**

Critère d'évaluation et version / *Evaluation criteria and version*

ISO/IEC 15408-1:2009, 15408-2:2008 15408-3:2008

Critères Communs version 3.1 rev. 5

Niveau d'évaluation / *Evaluation level*

Elevé (*High*) / EAL5 augmenté (*augmented*)
ALC_DVS.2, AVA_VAN.5

Référence du rapport d'évaluation / *Evaluation report reference*

Evaluation Technical Report (ETR Full) - HYPERION-R01 on Cosmo V9.1
Ref. LETI.CESTI.HYPR01-C9.1.ETR.001
version 1.1
30/04/2026.

Fonctionnalité de sécurité du produit / *Product's security features*

§ 2.2.2Services de sécurité / *Security services*

Résumé des menaces / *Threat summary*

Read the sensitive biometric reference data
Forgery of data on MRTD's chip
Counterfeit MRTD's chip
Abuse of Functionality
Information Leakage from MRTD's chip
Physical Tampering
Malfunction due to Environmental Stress
Tampering attempt of the TOE during preparation
Forgery of supplemental data stored in the TOE

Exigences de configuration du produit / *Product configuration requirements*

§ 4.2 Restrictions d'usage / restrictions usage

Hypothèses liées à l'environnement d'exploitation / *Operating environment assumptions*

§ 4.2Restrictions d'usage / restrictions usage

Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

Développeur / *Developer*

IN SMART IDENTITY FRANCE
2 place Samuel de Champlain
92400 Courbevoie, France

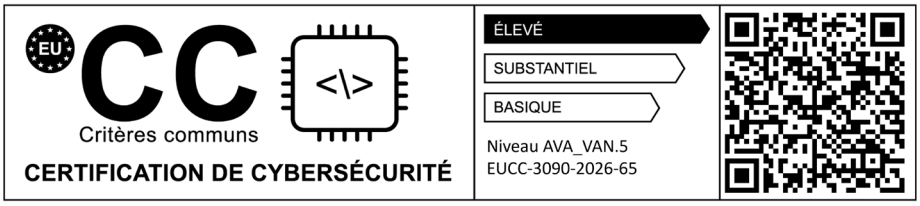
Commanditaire / *Sponsor*

IN SMART IDENTITY FRANCE
2 place Samuel de Champlain
92400 Courbevoie, France

Centre d'évaluation (CESTI) / *Evaluation center (ITSEF)*

CEA - LETI
17 avenue des martyrs,
38054 Grenoble Cedex 9, France

Marque EUCC / *EUCC Mark*



Accords de reconnaissance applicables / *Applicable recognition agreements*

CCRA

Ce certificat est reconnu au niveau EAL2.
This certificate is recognized at EAL2 level.

Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

2 Le produit / *Product*

2.1 Présentation du produit / *Product presentation*

Le produit évalué est « CombICAO Applet v2.2 in EAC configuration on ID-ONE Cosmo V9.1, ref. 203731 » développé par IN SMART IDENTITY FRANCE.

Le produit évalué est de type « carte à puce » pouvant être utilisé en modes avec et sans contact. Il implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (ICAO). Ce produit est destiné à permettre la vérification de l'authenticité du document de voyage et à identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels, dans une eCover ou dans une eDatapage. Le produit final peut prendre différentes formes, de carte ou de module.

The product evaluated is a smart card that can be used in both contact and contactless modes. It implements electronic travel document functions in accordance with the specifications of the International Civil Aviation Organization (ICAO). This product is designed to verify the authenticity of the travel document and identify its bearer during border control using an inspection system.

This microcontroller and its embedded software are designed to be inserted into the cover of traditional passports, into an eCover, or into an eDatapage. The final product can take various forms, such as a card or a module.

2.2 Description du produit / *Product description*

2.2.1 *Introduction*

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

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

Cette cible de sécurité est conforme au profil de protection [PP EAC].

This security target complies with the protection profile [PP EAC].

2.2.2 *Services de sécurité / Security services*

Les services de sécurité évalués fournis par le produit sont présentés au chapitre 2.2.1 « *Usage and major security features of the TOE* » de la cible de sécurité [ST].

The main security services provided by the product are listed at chapter 2.2.1 « Usage and major security features of the TOE » of the security target [ST].

2.2.3 *Architecture*

Le produit est constitué des éléments décrits au chapitre 2.3.2 « *TOE delivery* » de la cible de sécurité [ST].

The product is composed of the elements described in the chapter 2.3.2 "TOE delivery" of the security target [ST].

Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

2.2.4 *Identification du produit / Product identification*

La version certifiée du produit est identifiable par les éléments détaillés dans la cible de sécurité [ST] au chapitre 2.1.2 « *TOE reference* ».

The certified version of the product can be identified by the elements detailed in the security target [ST] in the 2.1.2 « TOE reference » chapter.

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire spécifiée dans les [GUIDES], ou bien par appel à une fonction. La procédure d'identification est décrite dans les guides (voir [GUIDES]).

These elements can be checked by reading registers located in a special memory area specified in [GUIDES], or by calling a function. The identification procedure is described in the guides (see [GUIDES]).

2.2.5 *Cycle* de vie / *Life cycle*

Le cycle de vie du produit est décrit au chapitre 2.4 *« Life Cycle »* de la cible de sécurité [ST]. Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

The product lifecycle is described in chapter 2.4 « Life Cycle » of the Security Target [ST]. Reports on site audits carried out under the French scheme, which can be reused without requiring site certification, are listed in [SITES].

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit le personnaliseur, le gestionnaire de la carte chargé de l'administration de la carte, et comme utilisateur du produit : l'utilisateur du produit final sur le terrain.

For the evaluation, the evaluator considered the customizer, the card administrator responsible for the administration of the card, as the product administrator and the end-user of the product in the field as the product user.

2.2.6 *Configuration évaluée / Evaluated configuration*

Le certificat porte sur les configurations permises par la cible de sécurité [ST] pourvu que les [GUIDES] soient respectés.

The certificate covers the configurations permitted by the security target [ST], provided that the [GUIDES] are followed.

Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

2.3 Contacts du produit / *Product contacts*

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

The product's cybersecurity information is available here:

- https://ingroupe.com/product/combicao/

Le développeur peut être contacté via cette adresse :

The developer can be contacted at this address:

- psirt@ingroupe.com

La procédure complète de signalement d'une vulnérabilité est disponible sur le lien suivant :

The complete procedure for reporting a vulnerability is available at the following link:

- https://ingroupe.com/psirt/

Les informations sur l'Autorité nationale de certification de cybersécurité en France sont disponibles ici :

Information on France's National Cybersecurity Certification Authority is available here:

- https://cyber.gouv.fr/cybersecurity-act

Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

3 L'évaluation / *Evaluation*

3.1 Référentiels d'évaluation / *Evaluation reference bases*

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

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

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

Pour répondre aux spécificités des cartes à puce et dispositifs similaires, les guides [SotA IC] et [SotA IC AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [SotA IC 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).

To meet the specific requirements of smart cards and similar devices, the [SotA IC] and [SotA IC AP] guides were applied. Thus, the AVA_VAN level was determined using the rating scale from the [SotA IC AP] guide. As a reminder, this rating scale is more demanding than the default one defined in the standard [CC] methodology, which is used for other product categories (e.g., software products).

3.2 Travaux d'évaluation / *Evaluation tasks*

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration de l'applet sur la plateforme déjà certifiée 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 de la plateforme « ID-ONE COSMO V9.1 (on SLC32) », voir [CER_PLF].

The compositional evaluation was carried out in accordance with the [COMP] guide, allowing us to verify that no weaknesses were introduced by integrating the software into the microcontroller already certified under a national scheme recognized by the SOG-IS agreement.

Accordingly, this evaluation took into account, in application of Article 8, paragraph 4 of [EUCC], the results of the evaluation of the microcontroller "ID-ONE COSMO V9.1 (on SLC32)",see [CER_PLF].

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** ».

*The Evaluation Technical Report [ETR], submitted to ANSSI on the day the ITSEF finalized it, details the work carried out by the evaluation center and attests that all the evaluation tasks were rated as « **PASS** ».*

Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

3.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI / *Analysis of cryptographic mechanisms according to ANSSI technical standards*

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].

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 [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.

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, which did not reveal any exploitable vulnerabilities at the targeted attacker level.

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.

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

Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

4 La certification / *Certification*

4.1 Conclusion / *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].

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 performed permits the delivery of a certificate in accordance with decree 2002-535 and to [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 / Summary*).

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

Le certificat associé à ce rapport, référencé EUCC-3090-2026-65 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.

The certificate associated with this report, referenced EUCC-3090-2026-65 has an issue date identical to the signature date of this report and is valid for five years from that date.

Le certificat est délivré sous accréditation Cofrac Certification de produits et services, attestation n°5-0669, liste des sites et portée disponibles sous www.cofrac.fr.

The certificate is issued under accreditation of Cofrac Certification, certificate n°. 5-0669, list of sites and scope availableat www.cofrac.fr.

4.2 Restrictions d'usage / Use *Restriction*

Ce certificat porte sur le produit spécifié au chapitre 2.2 du présent rapport de certification.

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

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].

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 outlined in the provided guides [GUIDES]

Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

4.3 Reconnaissance du certificat / *Certificate recognition*

4.3.1 *Reconnaissance internationale critères communs (CCRA) / International Common Criteria Recognition*

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[1] , des certificats Critères Communs.

This certificate is issued under the conditions of the CCRA agreement [CCRA]. The "Common Criteria Recognition Arrangement" enables the recognition of Common Criteria certificates by the signatory countries.

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 :

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

[1] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

ANNEXE A. Références documentaires du produit évalué / *Documentary references for the product evaluated*

[ST]	Cible de sécurité de référence pour l'évaluation / *Security target for the evaluation:* - *CombICAO v2.2 Applet in EAC configuration on Cosmo V9.1 Security Target*, ref. FQR 550 0052, version 9.0, 08/12/2025. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation / *For publication purposes, the following security target has been provided and validated as part of this evaluation:* - *CombICAO Applet v2.2 in EAC configuration on Cosmo V9.1 Public Security Target*, ref FQR 550 0085, version 7.0, 08/12/2025.
[RTE]	Rapport technique d'évaluation / *Evaluation Technical Report:* - *Evaluation Technical Report (ETR Full)* - HYPERION-R01 on Cosmo V9.1, ref. LETI.CESTI.HYPR01-C9.1.ETR.001, version 1.1, 30/04/2026.
[ANA_CRY]	Cotation des mécanismes cryptographiques HYPERION, ref. LETI.CESTI.HYP.RT.009, version 3.1, 30/04/2026.
[GUIDES]	Les guides du produit sont listés au chapitre 2.1.2 *« TOE reference »* de la cible de sécurité [ST]. *Product's guidance is listed in the chapter 2.1.2 "TOE reference" of the security target [ST].*
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation / *Document analysis and site audit reports for reuse:* - IDEMIA-2025_ALC_GEN_v1.0 ; - IDEMIA_2025_Noi-D_STAR_v1.0 ; - IDEMIA-2024_CRB_STAR_v1.1 ; - IDEMIA_2024_MNL_STAR_v1.1 ; - IDEMIA_2024_Haarlem_STAR_V1.0 ; - IDEMIA_2025_Noi-P_STAR_v1.0 ; - IDEMIA_2025_OST_STAR_v1.0 ; - IDEMIA_2024_SHZ_STAR_v1.0 ; - IDEMIA_2024_VTR-D_STAR_v1.1.
[CER_PLF]	Produit / *Product* ID-ONE COSMO V9.1 (on SLC32) Certifié par l'ANSSI / *Certified by* ANSSI – ref. ANSSI-CC-2020/07-R01.
[PP EAC]	*Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control*, version 1.10, 25/03/2009. Certifié BSI (*Bundesamt für Sicherheit in der Informationstechnik*), ref. BSI-CC-PP-0056-2009.

Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

ANNEXE B. Références liées à la certification / 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. *Amended decree No. 2002-535 of April 18th, 2002 relating to the evaluation and certification of the security provided by information technology products and systems.*	
[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 5.4. *Certification procedure of the security provided by information technology products and systems, ref ANSSI-CC-CER-P-01.*
[EUCC]	Schéma européen de certification de cybersécurité fondé sur les critères communs (règlement d'exécution (UE) 2024/482) et ses amendements. *European cybersecurity certification scheme based on common criteria (implementing regulation (EU) 2024/482) and its amendments.*
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version en vigueur. *Methods for carrying out cryptographic analyses, reference ANSSI-CC-CRY-P01, current version.*
[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 / *and associated technical fixes*. Equivalent à la version CCRA */ equivalent to CCRA version :* - *Common Criteria for Information Technology Security Evaluation*, version 3.1, rev. *5, vol*. 1 -> 3, ref. CCMB-2017-04-001 -> CCMB-2017-04-003.
[CEM]	*Information technology — Security techniques — Methodology for IT security evaluation,* ISO/IEC 18045:2008, et correctifs techniques associés / *and associated technical fixes* Equivalent à la version CCRA */ equivalent to CCRA version :* - *Common Methodology for Information Technology Security Evaluation*, Evaluation Methodology, version 3.1, rev. 5, ref. CCMB-2017-04-004.
[SotA IC]	*EUCC SCHEME STATE-OF-THE-ART DOCUMENT* Application *of CC to integrated circuits*, version 2, December 2024
[SotA IC AP]	*EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of attack potential to smartcards and similar devices*, version 2, February 2025

Docusign Envelope ID: DDC750D5-400A-85B5-807F-12B8C79F8F1C

[COMP] *	*EUCC SCHEME STATE-OF-THE-ART DOCUMENT Composite product evaluation for Smart Cards and similar devices for CC 3.1*, version 2, 12/2024.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2/07/2014.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques *Guide to cryptographic mechanisms: Rules and recommendations concerning the choice and sizing of cryptographic mechanisms* ANSSI-PG-083, version 2.04, 01/2020.

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

**Under the CCRA recognition agreement, the equivalent CCRA support document applies.*