Docusign Envelope ID: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

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-3090-2026-90

ST31P450 including optional cryptographic library NESLIB (C04)

Paris, le 17/11/2026 | 11:40 CET

Vincent Strubel

Docusign Envelope ID: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

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 does not in itself constitute a product endorsement by the Agence nationale de la sécurité des systèmes d'information (ANSSI), and does not 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: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

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 that 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: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

TABLE DES MATIÈRES / *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 8
2.2.4 Identification du produit / Product identification 8
2.2.5 Cycle de vie / Lifecycle 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 16

Docusign Envelope ID: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

1 Résumé / *Summary*

Référence du rapport de certification / *Certification report reference* **EUCC-3090-2026-90**
Nom du produit / *Product name* **ST31P450 including optional cryptographic library NESLIB**
Référence/version du produit / *Product reference/version* **C04**
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* ***Security IC Platform Protection Profile with Augmentation Packages, version 1.0*** certifié/*certified* BSI-CC-PP-0084-2014 – 19/02/2014 avec conformité aux packages / *with compliance to packages* : *"Authentication of the security IC"* *"Loader dedicated for usage in Secured Environment only"* *"Loader dedicated for usage by authorized users only"*
Critère d'évaluation et version / *Evaluation criteria and version* **ISO/IEC 15408:2022 et ISO/IEC 18045:2022** **Critères Communs version CC:2022, rev. 1**
Niveau d'évaluation / *Evaluation level* **Elevé (*High*) / EAL5 augmenté (*augmented*)** ASE_TSS.2, ALC_DVS.2, ALC_FLR.2, AVA_VAN.5
Référence du rapport d'évaluation / *Evaluation report reference* *Evaluation Technical Report MANDALA Reevaluation 2026* Ref. MANDALA_RE2026_ETR version 2.0 05/11/2026.
Fonctionnalité de sécurité du produit / *Product's security features* § 2.2.2 Services de sécurité / *Security services*
Résumé des menaces / *Threats summary* *Inherent Information Leakage;* *Physical Probing;* *Malfunction due to Environmental Stress;* *Physical Manipulation;* *Forced Information Leakage;* *Abuse of Functionality;* *Deficiency of Random Numbers;* *Masquerade the TOE;* *Memory Access Violation;* *Diffusion of Open Samples.*

Docusign Envelope ID: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

Exigences de configuration du produit / *Product configuration requirements* § 4.2 Restrictions d'usage / *Use Restriction*
Hypothèses liées à l'environnement d'exploitation / *Operating environment assumptions* § 4.2 Restrictions d'usage / *Use Restriction*
Développeur / *Developer* **STMICROELECTRONICS** 190 Avenue Celestin Coq, 13106 Rousset, France
Commanditaire / *Sponsor* **STMICROELECTRONICS** 190 Avenue Celestin Coq, 13106 Rousset, France
Centre d'évaluation (CESTI) / *Evaluation center (ITSEF)* **THALES / CNES** 290 allée du Lac, 31670 Labège, France
Marque EUCC / *EUCC Mark* CC Critères communs CERTIFICATION DE CYBERSÉCURITÉ — ÉLEVÉ / SUBSTANTIEL / BASIQUE — Niveau AVA_VAN.5 EUCC-3090-2026-90
Accords de reconnaissance applicables / *Applicable recognition agreements* CCRA Ce certificat est reconnu au niveau EAL2 augmenté de ALC_FLR.2. *This certificate is recognized at EAL2 level augmented with ALC_FLR.2.*

Docusign Envelope ID: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

2 Le produit / *Product*

2.1 Présentation du produit / *Product presentation*

Le produit évalué est « ST31P450 including optional cryptographic library NESLIB, C04 » développé par STMICROELECTRONICS.

The product evaluated is « ST31P450 including optional cryptographic library NESLIB, C04 » developed by STMICROELECTRONICS.

Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou plusieurs applications. Il peut être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (documents d'identité sécurisés, applications bancaires, télévision à péage, transport, santé, etc.) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

The microcontroller, by itself, is not a standalone product that can be used in its current state. It is designed to host one or more applications and may be embedded in a plastic support to form a smart card. This card has multiple uses (secure identity documents, banking applications, subscription television, transport, health, etc.) depending on the application software embedded in it. These software examples are not included in the scope of this evaluation.

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 strictement conforme au profil de protection [PP0084], avec le :

This security target complies strictly with the protection profile [PP0084], with:

- *package « authentication of the security IC »* ;
- *package « loader dedicated for usage in secured environment only »* ;
- *package « loader dedicated for usage by authorized users only »*.

2.2.2 *Services de sécurité / Security services*

Les services de sécurité évalués fournis par le produit sont présentés au chapitre 1.5 « *TOE overview* » de la cible de sécurité [ST].

The main security services provided by the product are listed at chapter 1.5 "TOE overview" of the security target [ST].

Docusign Envelope ID: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

2.2.3 *Architecture*

Le produit est constitué d'une partie matérielle et d'une partie logicielle, toutes deux décrites dans la cible de sécurité [ST] au chapitre 1.6 *« TOE description »*.

The product consists of a hardware part and a software part, both of which are described in the security target [ST] in section 1.6 "TOE description".

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 1.4 *« TOE Identification »*.

The certified version of the product can be identified by the elements detailed in the security target [ST] in the chapter 1.4 « TOE Identification ».

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire spécifiée dans les [GUIDES]. Il est également possible de faire appel à une fonction en ligne de commande qui renvoie les informations de configuration du produit.

These elements can be verified by reading the registers located in a special area of the memory specified in the [GUIDES]. It is also possible to use a command line function that returns the product configuration information.

2.2.5 *Cycle* de vie / *Lifecycle*

Le cycle de vie du produit est décrit au chapitre 1.7 *« TOE life cycle »* de la cible de sécurité [ST] ; il est conforme à celui décrit dans [PP0084]. 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 1.7 "TOE life cycle" of the Security Target [ST], and is compliant to [PP0084]. Reports on site audits carried out under the French scheme, which can be reused without requiring site certification, are listed in [SITES].

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: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

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:

- ST31P450 | Product - STMicroelectronics

Le développeur peut être contacté via cette adresse :

The developer can be contacted at this address:

- psirt@st.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:

- PSIRT - STMicroelectronics

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: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

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 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*

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI, 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 RTE issuance date, details the work carried out by the evaluation center and attests that all the evaluation tasks were rated as « **PASS** ».*

Docusign Envelope ID: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

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 [ACM Guidelines 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 non-conformities with respect to the standard [ACM Guidelines 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 [ACM Guidelines Crypto], pour les mécanismes cryptographiques qui le permettent.

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

Le produit comporte un générateur d'aléa. Il a été analysé conformément à la méthode d'évaluation [AIS20/31] ainsi que les dispositions décrites dans la note d'application [NOTE-24].

The product includes a random generator. It has been analyzed in accordance with the evaluation method [AIS20/31] as well as the provisions stipulated in the application note [NOTE-24].

Docusign Envelope ID: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

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-3090-2026-90 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-3090-2026-90 has an issue date identical to the signature date of this report and is valid for five years from that date.

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.

Ce certificat donne une appréciation de la résistance du produit à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le microcontrôleur ne pourra être appréciée que par une évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de l'évaluation citée au chapitre 3.

This certificate provides an assessment of the product's resistance to attacks, which are broadly generic due to the absence of any specific embedded application. Consequently, the security of a complete product built on the microcontroller can only be assessed through an evaluation of the complete product itself, based on the results of the evaluation mentioned in chapter 3.

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: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

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: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

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:* - ST31P450 C04 *including optional cryptographic library* NESLIB *Security Target*, ref. SMD_ST31P450_ST_19_001, version C04.1, 21/08/2026. 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:* - ST31P450 C04 *including optional cryptographic library* NESLIB *Security Target for composition,* ref. SMD_ST31P450_ST_19_002, version C04.1, September 2026.
[RTE]	Rapport technique d'évaluation / *Evaluation Technical Report :* - *Evaluation Technical Report* MANDALA *Reevaluation* 2026, ref. MANDALA_RE2026_ETR, version 2.0, 05/11/2026. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé / *For the purpose of composition evaluations with this microcontroller, a technical report for composition has been validated*: - *Evaluation Technical Report for composite evaluation* MANDALA C04 *Reevaluation* 2026, ref. MANDALA_C04_RE2026_ETRLite, version 1.0 01/10/2026.
[ANA_CRY]	*Analysis of Cryptographic Mechanisms* MANDALA *Reevaluation* 2026, ref. MANDALA_C04_RE2026_CRY, version 1.0, 02/10/2026.
[GUIDES]	La Table 16 de la cible de sécurité [ST] indique les guides du produit. Cette table donne pour chaque guide l'indication de sa version et de sa date de parution. *Table 16 in the Security Target [ST] lists the product's guidance. This table gives for each guide its version and issuance date.*
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation / *Document analysis and site audit reports for reuse:* - STM_2025_ALC_GEN_v1.2 ; - STM_2025_CB-JY-LH_STAR_v1.1 ; - STM_2025_DNP_STAR_v1.0 ; - STM_2025_DPE_STAR_v1.0 ; - STM_2025_Feiliks_STAR_v1.0 ; - STM_2023_Pantos_STAR_v1.0 ; - STM_2024_ST AMK1_STAR_v1.0 ; - STM_2023_TPY-AMK6_STAR_v1.0 ; - STM_2025_ST_Bouskoura_STAR_v1.0 ; - STM_2024_ST_Calamba_STAR_v1.1 ; - STM_2024_ST_Catania_ST_Palermo_STAR_v1.0 ; - STM_2024_ST_Crolles_STAR_v1.0 ;

Docusign Envelope ID: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

	- STM_2023_RST_CMP_STAR_v1.3 ; - STM_2024_ST Ljubljana_STAR_v1.0 ; - STM_2025_ST_Loyang_STAR_v1.1 ; - STM_2024_ST_Rennes_STAR_v1.0 ; - STM_2025_STS_Shenzhen-STS_Shenzhen_Lab_STAR_v1.0 - STM_2025_ST_Sophia_STAR_v1.0 ; - STM_2024_ST_Tunis_STAR_v1.0 ; - STM_2024_Teradyne_STAR_v1.2 ; - STM_2024_ST Zaventem_STAR_v1.0.
[PP0084]	*Protection Profile, Security IC Platform Protection Profile with Augmentation Packages*, version 1.0, 13/01/2014. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*), ref. BSI-PP-0084-2014.

Docusign Envelope ID: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

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 5.5. *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 15408-1:2022 ; - *Part 2: Security functional components:* ISO/IEC 15408-2:2022 ; - *Part 3: Security Assurance components:* ISO/IEC 15408-3:2022 ; - *Part 4: Framework for the specification of evaluation methods and activities*: ISO/IEC 15408-4:2022 ; - *Part 5: Pre-defined packages of security requirements*: ISO/IEC 15408-5:2022. Equivalent à la version CCRA */ equivalent to CCRA version :* - *Common Criteria for Information Technology Security* Evaluation, version CC:2022, rev. 1, vol. 1 -> 5, ref. CCMB-2022-11-001 -> CCMB-2022-11-005.
[CEM]	*Information technology — Security techniques — Evaluation criteria for IT security, ISO/IEC 18045:2022* Equivalent à la version CCRA / *equivalent to CCRA version :* - *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology,* version CC:2022, rev. 1, ref. CCMB-2022-11-006.
[CC-Errata]	*Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1)*, ref. 001, version 1.2, 15/10/2025.

Docusign Envelope ID: FD07ACE6-1C75-8E60-8092-37162C5FBB4F

[CC2022-Transition]	*Transition policy to CC:2022 and CEM:2022*, ref. CCMC-2023-04-001, 20/04/2023.
[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.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 02/07/2014.
[ACM GuidelinesCrypto]	*European Cybersecurity Certification Group Sub-group on Cryptography Agreed Cryptographic Mechanisms*, version 2.0, April 2025.
[AIS20/31]	*A proposal for: Functionality classes for random number generators, AIS20/AIS31*, version 2.0, 18/09/2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).
[NOTE-24]	Note d'application – Evaluation de générateurs d'aléa selon AIS20/31 dans le schéma français *Application note - Evaluation of random number generators according to AIS20/31 in the French scheme* Ref. ANSSI-CC-NOTE-24, version en vigueur */ current version.*

*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.*