



**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-3090-2026-69

**TEQS V1.0 Platform
(version 1.0)**

Paris, le 24/8/2026 | 17:15 CEST

Vincent Strubel



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 présumées 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.

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.

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	7
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	10
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

1 Résumé / Summary

Référence du rapport de certification / <i>Certification report reference</i>	EUC-3090-2026-69
Nom du produit / <i>Product name</i>	TEQS V1.0 Platform
Référence/version du produit / <i>Product reference/version</i>	version 1.0
Type de produit / <i>Type of product</i>	Cartes à puce et dispositifs similaires (Smart cards and similar devices)
Conformité à un profil de protection / <i>Conformity with a protection profile</i>	GlobalPlatform Technology - Secure Element Protection Profile, référence GPC_SPE_174, version 1.0. Certifié par le OC-CCN sous la référence 2020-37-INF-3429- v1
Critère d'évaluation et version / <i>Evaluation criteria and version</i>	ISO/IEC 15408-1:2009, 15408-2:2008 15408-3:2008 et ISO/IEC 18045:2008 Critères Communs version 3.1 rev. 5
Niveau d'évaluation / <i>Evaluation level</i>	Elevé (High) / EAL4 augmenté (augmented) ALC_DVS.2, AVA_VAN.5
Référence du rapport d'évaluation / <i>Evaluation report reference</i>	Evaluation Technical Report CORFOU-R01 Ref. CORFOU-R01_ETR version 2.0 08/07/2026
Fonctionnalité de sécurité du produit / <i>Product's security features</i>	§ 2.2.2 Services de sécurité / Security services
Résumé des menaces / <i>Threats summary</i>	UNAUTHORISED-CARD-MGMT LIFE-CYCLE COM-EXPLOIT BRUTE-FORCE-SCP CLFDB-DISC CVM-IMPERSONATE CVM-UPDATE BRUTE-FORCE-CVM RECEIPT TOKEN ELF-UNAUTHORISED ELF-VERSION ELF-DATA-ACCESS ELF-DATA-INTEGRITY

ELF-SESSION
 ELF-ILL-COMMAND
 ELF-RES-DATA
 UNAUTHORISED-TOE-CODE-UPDATE
 FAKE-SGNVER-KEY
 WRONG-UPDATE-STATE
 INTEG-OS-UPDATE-LOAD
 CONFID-OS-UPDATE-LOAD

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*

THALES DIS

La Vigie – Avenue du Jujubier ZI Athelia IV,
13705 La Ciotat Cedex, France

Commanditaire / *Sponsor*

THALES DIS

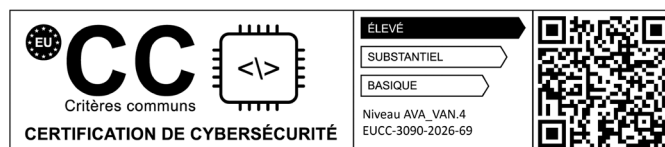
La Vigie – Avenue du Jujubier ZI Athelia IV,
13705 La Ciotat Cedex, France

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

THALES / CNES

290 allée du Lac,
31670 Labège, France

Marque EUCC / *EUCC Mark*



Accords de reconnaissance applicables / *Applicable recognition agreements*



Ce certificat est reconnu au niveau EAL2

This certificate is recognized at EAL2 level

2 Le produit / Product

2.1 Présentation du produit / Product presentation

Le produit évalué est « TEQS V1.0 Platform, version 1.0 » développé par THALES DIS.

The product evaluated is «TEQS V1.0 Platform, version 1.0 » developed by THALES DIS.

Le produit est destiné à héberger et exécuter une ou plusieurs applications, dites applets dans la terminologie Java Card. Ces applications peuvent revêtir un caractère sécuritaire différent (selon qu'elles soient « sensibles » ou « basiques ») et peuvent être chargées et instanciées avant ou après émission du produit.

The product is designed to host and run one or more applications, referred to as applets in Java Card terminology. These applications may implement different security features, depending on whether they are classified as "sensitive" or "basic", and can be loaded and instantiated either before or after the product is issued.

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-GP].

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

2.2.2 Services de sécurité / Security services

Les principaux services de sécurité fournis par le produit sont décrits dans la cible de sécurité [ST], au chapitre 4.3 « TEQS v1.0 platform description ».

The main security services provided by the product are listed at chapter 4.3 "TEQS v1.0 platform description" of the security target [ST].

2.2.3 Architecture

L'architecture du produit est décrite dans la cible de sécurité [ST], au chapitre 4.1 « Architecture of TEQS v1.0 ». La TOE est une plateforme ouverte décrite au chapitre 4.2 « TOE Boundaries » de [ST].

The product architecture is described in the security target [ST], in Chapter 4.1 "Architecture of TEQS v1.0." The TOE is an open platform described in Chapter 4.2, "TOE Boundaries" of [ST].

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 3.2 « TOE Identification ».

The certified version of the product can be identified by the elements detailed in the 3.2 « TOE Identification » chapter of the security target [ST].

2.2.5 Cycle de vie / Lifecycle

Le cycle de vie du produit est décrit au chapitre 4.5 « 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 4.5 "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].

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit le « pré personnalisateur », le « personnalisateur » et le gestionnaire de la carte chargé de l'administration de la carte et comme utilisateur du produit le propriétaire du smartphone comme indiqué chapitre 4.5 « TOE Life Cycle » de la cible de sécurité [ST].

For the evaluation, the evaluator considered the "pre-personalizer," the "personalizer," and the card manager responsible for card administration to be the product administrators, and the smartphone owner to be the product user, as indicated in Chapter 4.5, "TOE Life Cycle," of the security target [ST].

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.

La configuration ouverte du produit a été évaluée conformément à [SotA OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 4.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

The product's open configuration was evaluated according to [SotA OPEN]: this product corresponds to an open partitioning platform. Therefore, any new loaded applications that are compliant with the constraints indicated in chapter 4.2 of this certification report and produced according to the processes audited do not call this certification report into question.

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:

- thalesgroup.com/en/search/enterprise/mobile-communications/thales-eucc-certification-mobile-communications-solutions

Le développeur peut être contacté via cette adresse :

The developer can be contacted at this address:

- psirt@thalesgroup.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:

- thalesgroup.com/en/global/group/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>

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

L'évaluation en composition a été réalisée en application du guide [SotA COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié dans le cadre d'un schéma national reconnu au titre de l'accord du SOG-IS.

Cette évaluation a ainsi pris en compte, en application du paragraphe 4 de l'article 8 d'[EUCC], les résultats de l'évaluation du microcontrôleur « S3SSE2A », voir [CER_IC].

The compositional evaluation was carried out in accordance with the [SotA 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 "S3SSE2A" (see [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** ».

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

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 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.

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-3090-2026-69 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-3090-2026-69 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.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES]. Notamment :

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]. In particular :

- toutes les futures applications chargées sur ce produit (chargement post-émission) doivent respecter les contraintes de développement de la plateforme (guides [AGD-APP-Dev]) selon la sensibilité de l'application considérées ;
- *all the future applications loaded on this product (post-issue loading) must respect the platform development constraints [AGD-APP-Dev] depending on the sensitivity of the applications in question ;*
- les autorités de vérification doivent appliquer le guide [AGD-OPE_VA] ;
- *the verification authorities must apply the guide [AGD-OPE_VA] ;*
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement post-émission) doit être activée conformément aux indications de [AGD_APP-Dev] ;
- *the loading protection for all future applications loaded on this product (post-issue loading) must be activated according to the indications in [AGD_APP-Dev] ;*
- le chargement des applications pré- émission doit être protégé conformément au guide [AGD_APP-Dev] ;
- *the loading of the pre-issue applications must be protected according to the guide [AGD_APP-Dev] ;*

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 signataires¹, 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.

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

[ST]	Cible de sécurité de référence pour l'évaluation / <i>Security target for the evaluation</i>: - <i>TEQS V1.0 Platform Security Target</i>, référence D1620313, version 1.4, 29/04/2026. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation / <i>For publication purposes, the following security target has been provided and validated as part of this evaluation</i>: - <i>TEQS V1.0 Platform Security Target – Public version</i>, référence D1620313, version 1.4, 25/06/2026.
[RTE]	Rapport technique d'évaluation / <i>Evaluation Technical Report</i> : - <i>Evaluation Technical Report CORFOU-R01</i>, ref. CORFOU-R01_ETR, version 2.0, 08/07/2026. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé / <i>For the purpose of composition evaluations with this microcontroller, a technical report for composition has been validated</i>: - <i>Evaluation Technical Report for composite evaluation CORFOU-R01</i>, Ref : CORFOU-R01_ETRLite, version 2.0, 08/07/2026.
[ANA_CRY]	<i>Analysis of Cryptographic Mechanisms TEQS v1.0 - CORFOU</i>, référence TEQS_V1.0_CRY, version 1.0, 17 mars 2025.
[GUIDES]	Guide d'installation du produit / <i>Product installation guide</i> : - <i>Preparative guidance On CC platforms – TEQS V1.0</i>, référence D1622628, version 1.1, novembre 2024. Guides d'administration et d'utilisation du produit / <i>Product administration and user guides</i> : - <i>Operational guidance on CC platforms – TEQS V1.0, With or Without Controlling Authority And Optional Verification Authority</i>, référence D1622715, version 1.2, 11/2024 ; - <i>Guidance for profile set up vs. JavaCard System Protection Profile</i>, référence D1578508, version 1.6, 04/072024 ; - <i>Patch Loading Management for Certified Secure Elements – External Procedure</i>, référence D1344508, version A04, 03/2022 ; - <i>Operational guidance on CC platforms for Verification Authority – TEQS V1.0</i>, référence D1622983, version 1.0, 07/2024 ; - <i>TEQS V1.0 Platform - Identification & Configurability</i>, référence D1627926, version 1.5, 12/02/2025 ; - <i>TEQS v1.0 APDU Guide</i>, référence D1621521, version 1.1, 5/072024. Guides de développement d'applications / <i>Application Development Guides [AGD_APP-Dev]</i> :

	- <i>GlobalPlatform Card - Composition Model - Security Guidelines for Basic Applications</i>, référence GPC_GUI_050, version 2.0, 11/2014 - <i>Guidance for Secure application development Thales Embedded Secure Elements (eSE)</i>, référence D1623097, version 1.0, 02/2025. Guide pour l'autorité de vérification / <i>Guide for the Verification Authority</i> [AGD_OPE_VA] : - <i>Application Verification for Certified Secure Elements – External Procedure</i>, référence D1258682, version C03, 02/2021.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation / <i>Document analysis and site audit reports for reuse:</i> - DISGEN26_ALC_GEN_v1.0 ; - DISGEN24_LVG_STAR_V1.1 ; - DISGEN24_SGP_STAR_V1.0 ; - DISGEN24_GEM_STAR_V1.0 ; - DISGEN25_T CZ_STAR_v1.0 ; - DISGEN24_PAU_STAR_v1.0 ; - DISGEN23_SSN_SSC_STAR_v1.0 ; - DISGEN23_TLH_STAR_v1.0 ; - DISGEN23_VFO-CAL_STAR_v1.0.
[CER_IC]	Produit / <i>Product</i> S3SSE2A Certifié par l'ANSSI / <i>Certified by ANSSI</i> – ref. ANSSI-CC-2024/26-R01
[PP-GP]	<i>GlobalPlatform Technology - Secure Element Protection Profile</i>, version 1.0, référence GPC_SPE_174. Certifié par OC-CCN (<i>Organismo de Certificación, Centro Criptológico Nacional</i>) le 18 mars 2021 sous la référence 2020-37-INF-3429-v1.
[PP0084]	<i>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages</i>, version 1.0, 13/01/2014. Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>), ref. BSI-PP-0084-2014.

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. <i>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.</i>	
[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. <i>Certification procedure of the security provided by information technology products and systems, ref ANSSI-CC-CER-P-01.</i>
[EUCC]	Schéma européen de certification de cybersécurité fondé sur les critères communs (règlement d'exécution (UE) 2024/482) et ses amendements. <i>European cybersecurity certification scheme based on common criteria (implementing regulation (EU) 2024/482) and its amendments.</i>
[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. <i>Methods for carrying out cryptographic analyses, reference ANSSI-CC-CRY-P01, current version.</i>
[CC]	<i>Information technology — Security techniques — Evaluation criteria for IT security</i> - <i>Part 1: Introduction and general model: ISO/IEC 15408-1:2009 ;</i> - <i>Part 2: Security functional components: ISO/IEC 15408-2:2008 ;</i> - <i>Part 3: Security Assurance components: ISO/IEC 15408-3:2008 ;</i> - <i>et correctifs techniques associés / and associated technical fixes.</i> Equivalent à la version CCRA / <i>equivalent to CCRA version :</i> - <i>Common Criteria for Information Technology Security Evaluation, version 3.1, rev. 5, vol. 1 -> 3, ref. CCMB-2017-04-001 -> CCMB-2017-04-003.</i> -
[CEM]	<i>Information technology — Security techniques — Methodology for IT security evaluation, ISO/IEC 18045:2008, et correctifs techniques associés / and associated technical fixes</i> Equivalent à la version CCRA / <i>equivalent to CCRA version :</i> - <i>Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, version 3.1, rev. 5, ref. CCMB-2017-04-004.</i>
[SotA IC]*	<i>EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of CC to integrated circuits, version 2, December 2024.</i>

[SotA IC AP]*	<i>EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of attack potential to smartcards and similar devices, version 2, February 2025.</i>
[SotA COMP] *	<i>EUCC SCHEME STATE-OF-THE-ART DOCUMENT Composite product evaluation for Smart Cards and similar devices for CC 3.1, version 2, December 2024.</i>
[SotA OPEN]*	<i>EUCC SCHEME STATE-OF-THE-ART DOCUMENT CERTIFICATION OF "OPEN" SMART CARD PRODUCTS, version 1.1, October 2023.</i>
[CCRA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2/07/2014.</i>
[ANSSI Crypto]	Guide des mécanismes cryptographiques: Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques <i>Guide to cryptographic mechanisms: Rules and recommendations concerning the choice and sizing of cryptographic mechanisms</i> 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.*