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-3090-2026-60

Java Card MultiApp V4.2 platform in open configuration on IC IFX_CCI_000010h (4.2.0.1)

Paris, le 22/6/2026 | 12:10 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 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

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.

TABLE DES MATIERES / *TABLE OF CONTENT*

1 Résumé / *Summary*

Référence du rapport de certification / *Certification report reference*

EUCC-3090-2026-60

Nom du produit / *Product name*

Java Card MultiApp V4.2 platform in open configuration on IC IFX_CCI_000010h

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

4.2.0.1

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*

Java Card System Protection Profile - Open Configuration,
version 3.0.5
certifié/*certified* BSI-PP-0099-2017.

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*)
ALC_DVS.2, AVA_VAN.5

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

Evaluation Technical Report TARSO-1-PC-v2 Project
Ref. TARSO-1-PC-v2_ETR_v1.0
version 1.0
27/03/2026.

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

§ 2.2.2Services de sécurité / *Security services*

Résumé des menaces / *Threat summary*

Executing an application to disclose data belonging to another application
Executing an application to disclose the Java Card System code
Executing an application to disclose data belonging to the Java Card System
Executing an application to alter code
Modifying code when an application package is transmitted to the card for installation
Executing an application to alter another application's data
Modifying the initialization data (in an application package) when it is transmitted for installation
Executing an application to alter (part of) the Java Card System code
Executing an application to alter (part of) Java Card System or API data.
Impersonating an application (or even the Java Card RE) to gain illegal access to resources
Illegal impersonation of a privileged role
Unauthorized execution of a method by an applet
Executing a method fragment or arbitrary data
Executing a native method to bypass a TOE Security Function (such as the firewall)
Preventing correct operation of the Java Card System through consumption of resources

Deleting an applet or a package already in use on the card, or using the deletion functions
Installing post-issuance of an applet on the card
Keeping a reference to a garbage collected object
Disclosing/Modifying the design of the TOE by physical tampering means
Skimming (Capturing Card-Terminal Communication)
Eavesdropping on the communication between the TOE and the PACE terminal
Abuse of Functionality
Information Leakage from travel document
Physical Tampering
Malfunction due to Environmental Stress
Forgery of Data

Exigences de configuration du produit / *Product configuration requirements*
§ 3.5 Restrictions d'usage / *Use Restriction*

Hypothèses liées à l'environnement d'exploitation / *Operating environment assumptions*
§ 3.5 Restrictions d'usage / *Use Restriction*

Développeur / *Developer*

THALES DIS FRANCE SAS
6 rue de la Verrerie
92190 Meudon, France

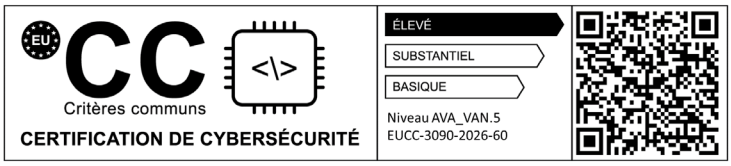
Commanditaire / *Sponsor*

THALES DIS FRANCE SAS
6 rue de la Verrerie
92190 Meudon, France

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

SERMA SAFETY & SECURITY
14 rue Galilée, CS 10071,
33608 Pessac Cedex, 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.

2 Le produit / *Product*

2.1 Présentation du produit / *Product presentation*

Le produit évalué est « Java Card MultiApp V4.2 platform in open configuration on IC IFX_CCI_000010h, 4.2.0.1 » développé par THALES DIS FRANCE SAS.

The product evaluated is «Java Card MultiApp V4.2 platform in open configuration on IC IFX_CCI_000010h, 4.2.0.1 » developed by THALES DIS FRANCE SAS.

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-JCS].

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

2.2.2 *Services de sécurité / Security services*

Les principaux services de sécurité fournis par le produit sont décrits à la fin du chapitre 2.3.1 « *Architecture* » de la cible de sécurité [ST].

The main security services provided by the product are listed at the end of chapter 2.3.1 "Architecture" of the security target [ST].

Mais aussi/*And also* :

- la protection du chargement d'applications post-émission ;
- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications.
- *Protection of the post-issuance application loading ;*
- *Isolation of the applications between different contexts and protection of the confidentiality and integrity of the application data between the applications ;*

2.2.3 *Architecture*

Le produit est constitué des éléments décrits au chapitre 2.3.1 « *Architecture* » de la cible de sécurité [ST].

The product is composed of the elements described in the chapter 2.3.1 "Architecture" of the security target [ST].

Les applications déjà chargées dans le produit sont toutes identifiées dans la cible de sécurité [ST] au paragraphe 2.2, table 1 : « *Applets identification* ».

Bien que ces applications ne soient pas incluses dans le périmètre de l'évaluation, elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [SotA OPEN]. En effet, ces applications ont été vérifiées conformément aux contraintes de développements d'applications décrites dans les guides [GUIDES]

The applications already loaded on the product are all listed in the security target [ST], under section 2.2, table 1 "Applets identification"

Although these standard applications are not included in the evaluation scope, they were considered during the evaluation process in accordance with the requirements specified in [SotA OPEN]. In fact, these standard applications were verified according to the application development constraints described in the guides [GUIDES].

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 1.3 « *TOE IDENTIFICATION* ».

The certified version of the product can be identified by the elements detailed in the 1.3 « TOE IDENTIFICATION» chapter of the security target [ST].

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]).

La principale différence entre le produit et la TOE (la plateforme) correspond aux applications chargées pré-émission sur ce produit.

The main difference between the product and the TOE (the platform) corresponds to the applications loaded pre-issue on this smart card.

Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans le document [ST] qui liste les applications et les packages inclus dans le produit, associés à leurs noms et AID[1].

All the applications present in the product configuration available to the evaluator are identified in the document [ST], which lists the applications and packages included in the product, along with their names and AIDs.

La commande GET DATA permet à l'utilisateur du produit de vérifier quelles applications et quels packages sont installés dans le produit à sa disposition.

The GET DATA command enables the product user to verify which applications and which packages are installed in the product available to them.

[1] *Application Identifier*

2.2.5 *Cycle* de vie / *Lifecycle*

Le cycle de vie du produit est décrit au chapitre 2.5 « *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 2.5 « 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].

Des applications peuvent être chargées en phase 7 *(End Usage)*. Ces chargements doivent être protégés conformément aux [GUIDES].

Applications may be loaded in phase 7 (End Usage). This loading must be protected according to [GUIDES].

Conformément à [SotA OPEN], les procédures concernant ont été analysées et auditées pendant cette évaluation.

In accordance with [SotA OPEN], these procedures were analysed and audited during this evaluation.

Les guides [GUIDES] identifient également des recommandations relatives à la livraison des futures applications à charger sur cette carte.

Par ailleurs, les guides [GUIDES] décrivent les règles de développement des applications destinées à être chargées sur cette carte et les règles de vérification qui doivent être appliquées par l'autorité de vérification.

The guides [GUIDES] also specifies recommendations related to the applications to be loaded onto this card.

Additionally, the guides [GUIDES] outline the development rules for applications intended for this card and details the verification procedures that must be followed by the verification authority.

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit le pré- « personnalisateur », le « personnalisateur » et le gestionnaire de la carte chargés de l'administration de la carte et comme utilisateurs du produit, les développeurs des applications à charger sur la plateforme.

For the evaluation, the evaluator considered the pre-personalizer, the personalizer and the card which is responsible for the administration of the smart card as the product administrator and the developer of the applets to be loaded on the platform 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.

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 3.5 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

Toutes les applications identifiées dans [ST] ont été vérifiées conformément aux contraintes décrites dans les [GUIDES].

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 3.5 of this certification report and produced according to the processes audited do not call this certification report into question.

All applications identified in [ST] were verified according to the constraints described in [GUIDES].

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://www.thalesgroup.com/en/search/public-security/civil-identity/thales-eucc-certification-civil-identity

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:

- https://www.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 du schéma européen EUCC.

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 « *IFX_CCI_000010h in design step G12* », 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 European EUCC scheme.

Accordingly, this evaluation took into account, in application of Article 8, paragraph 4 of [EUCC], the results of the evaluation of the microcontroller "IFX_CCI_000010h in design step G12 " (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 the day it was finalized by the ITSEF, 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 [RTE].

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 [RTE].

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-3090-2026-60 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-3090-2026-60 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 [GUIDES]) selon la sensibilité de l'application considérées ;
- *all the future applications loaded on this product (post-issue loading) must respect the platform development constraints [GUIDES] depending on the sensitivity of the applications in question ;*
- les autorités de vérification doivent appliquer le guide [GUIDES] ;
- *the verification authorities must apply the guide [GUIDES] ;*
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement post-émission) doit être activée conformément aux indications de [GUIDES] ;
- *the loading protection for all future applications loaded on this product (post-issue loading) must be activated according to the indications in [GUIDES] ;*

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[2] , 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 :

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

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

[ST]	Cible de sécurité de référence pour l'évaluation / *Security target for the evaluation:* - *MultiApp V4.2: JCS Security Target*, ref. D1487827, version 1.22, 24/02/2026. 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:* - *MultiApp V4.2: JCS Security Target Lite*, ref. D1487827, version 1.22p, 20/03/2026.
[RTE]	Rapport technique d'évaluation / *Evaluation Technical Report :* - *Evaluation Technical Report TARSO-1-PC-v2 Project*, ref. TARSO-1-PC-v2_ETR_v1.0, version 1.0, 27/03/2026. 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 Lite For Composition TARSO-1-PC-v2 Project*, ref. TARSO-1-PC-v2_ETR_Lite_v1.0, version 1.0, 27/03/2026.
[GUIDES]	Voir la liste TOE guidance documentation au chapitre 2.5.4 « *TOE Delivery* » de la cible de sécurité [ST]. *See the TOE guidance documentation list in chapter 2.5.4 "TOE Delivery" 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:* - DISGEN25_ALC_GEN_v1.2 ; - DISGEN24_CHA_STAR_v1.0 ; - DISGEN25_CUR_STAR_v1.1 ; - DISGEN24_ELC_STAR_v1.1 ; - DISGEN24_GEM_STAR_v1.0 ; - DISGEN24_LVG_STAR_v1.1 ; - DISGEN23_MDN_STAR_v1.1 ; - DISGEN25- MGY_STAR_v1.0 ; - DISGEN24_PAU_STAR_v1.0 ; - DISGEN24_SGP_STAR_v1.0 ; - DISGEN23_SSN_SSC_STAR_v1.1 ; - DISGEN25_TCZ_STAR_v1.0 ; - DISGEN23_TLH_STAR_v1.0 ; - DISGEN25_VAN_STAR_v1.0 ; - DISGEN25_VFO-CAL_STAR_v1.0.
[CER_IC]	Produit / *Product* IFX_CCI_000010h in design step G12 Certifié par le / *Certified by* BSI – ref. EUCC-3087-2025-12-0001

[PP-JCS]	*Java Card System Protection Profile - Open Configuration*, version 3.0.5. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*), ref. BSI-PP-0099-2017.

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. 002, version 1.1, 22/07/2024.

[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.
[SotA COMP] *	*EUCC SCHEME STATE-OF-THE-ART DOCUMENT Composite product evaluation for Smart Cards and similar devices for CC :2022,* version 1, February 2025.
[SotA OPEN]*	*EUCC SCHEME STATE-OF-THE-ART DOCUMENT CERTIFICATION OF "OPEN" SMART CARD PRODUCTS*, version 1.1, October 2023.
[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.*