EUCC Certification Report

ID-A v1.1 on ID-One Cosmo X, v1.1.1

Sponsor and developer:	***IN Smart Identity France*** **2 place Samuel de Champlain** **92400 COURBEVOIE** **France**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2, 2612 CT, Delft, The Netherlands**
Report number:	**EUCC-3110-2026-2500178-01 Certification Report**
Report version:	**1**
Project number:	**EUCC-2500178-01**
Author(s):	**Alireza Rohan, TrustCB B.V.** **contact: eucc@trustcb.com**
Date:	**26 July 2026**
Number of pages:	**19**
Number of appendices:	**0**

CONTENTS

Foreword

The Common Criteria-based European Cybersecurity Certification Scheme (EUCC) is a certification scheme created under the Cybersecurity Act (CSA), Regulation (EU) 2019/881 of 17 April 2019.

The EUCC is described by Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

The Dutch implementation of the CSA is regulated in Dutch law in the 'Uitvoeringswet cyberbeveiligingsverordening' (UITVW). In this law the role of NCCA is assigned to the Dutch Authority for Digital Infrastructure (RDI), which is part of the Ministry of Economic Affairs.

TrustCB B.V. has been licensed by the RDI as a Certification Body (CB) for the task of ISO/IEC 17065 Certification Activities up to and including CSA assurance level high for ICT security products, as well as for protection profiles. Part of the procedure is the technical examination (evaluation) of the product, protection profile according to the NP002 EUCC processes published by the Dutch NCCA.

Evaluations of ICT products are performed by an IT Security Evaluation Facility (ITSEF) licensed by the Dutch NCCA as a CAB for ISO/IEC 17025 Evaluation Activities, with scope aligning to the requested Evaluation Assurance Level of the Object for the evaluation, referred to as the Target of Evaluation (TOE) in this report.

By awarding an EUCC certificate as a Common Criteria certificate, TrustCB B.V. asserts that the ICT product complies with the security requirements specified in the associated security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the ICT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the ICT product satisfies the security requirements stated in the security target.

International recognition of the certificate

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of published certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the ID-A v1.1 on ID-One Cosmo X, v1.1.1, identified in this document as either the ICT Product or as the Target of Evaluation (TOE).

The developer of the ICT Product is IN Smart Identity France located in Courbevoie, France and they also act as the sponsor of the evaluation and certification.

This Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the ICT product for their particular requirements.

The TOE comprises of the ID-A v1.1 Java Card eServices application installed on top of the ID-One Cosmo X Global Platform Java Card operating system and the Infineon SLC37 security controller. The ID-A v1.1 application is an INSI specific Java Card implementation designed to provide functionality for identification, authentication and advanced digital signature creation for national ID cards, health cards and corporate cards.

In addition, the ID-A v1.1 applet supports the following secure authentication protocols:

- PACE with
  - support for ECDH in Generic and Integrated Mapping modes (PACE-GM, PACE-IM),
  - MRZ, CAN, PIN and PUK passwords and
  - PIN/PUK suspend and resume mechanism (over contactless interface);
- Chip Authentication v2 (CAv2);
- Terminal Authentication v2 (TAv2).

Available configurations of the TOE are detailed in section 2.1 of this report.

The TOE claims conformance to the following Protection Profiles *[PP]*:

- Protection profiles for secure signature creation device — Part 2: Device with key Generation, EN 419211-2:2013, CEN/TC 224, BSI-CC-PP-0059-2009-MA-02, Version 2.0.1, June 30 2016
- Protection profiles for secure signature creation device – Part3: Device with key import, EN 419211-3:2013, CEN/TC 224, BSI-CC-PP-0075-2012-MA-01, Version 1.0.2, June 30 2016
- Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application, EN 419211-4:2013, CEN/TC 224, BSI-CC-PP-0071-2012-MA-01, Version 1.0.1, June 30 2016
- Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application, EN 419211-5:2013, CEN/TC 224, BSI-CC-PP-0072-2012-MA-01, Version 1.0.1, June 30 2016
- Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature-creation application, EN 419211-6:2013, CEN/TC 224, BSI-CC-PP-0076-2013-MA-01, Version 1.0.4, June 30 2016

The TOE is stated as a Qualified Signature Creation Device and Qualified Seal Creation Device for 3 SSCD configurations (SSCD Config #1, SSCD Config #2 and SSCD Config #3), as defined in the [ST], for the purposes of electronic identification and trust services as detailed by the [EU-eIDAS]. The evaluation by SGS Brightsight included an examination of the TOE according to the eIDAS Dutch Conformity Assessment Process Version 6 0.

A certification procedure was conducted on the TOE by TrustCB B.V., in accordance with the provisions of the EUCC as described in Commission implementing regulation (EU) 2024/482 of 31 January 2024, amended by (EU) 2024/3144 of 18 December 2024 and (EU) 2025/2462 of 8 December 2025.

The successful completion of the certification procedure resulted in TrustCB issuing an EUCC certificate, The certificate identifier is **EUCC-3110-2026-2500178-01**, dated 26-07-2026 and with a 5-year validity.

The evaluation of the TOE was performed by SGS Brightsight located in Delft, The Netherlands. The evaluation was completed on 22 May 2026 with the issuance of the evaluation technical report *[ETR]*. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CC:2022, R1 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 R1 *[CC]* (Parts 1, 2, 3, 4, 5).

The scope of the evaluation was defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the ICT Product, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL5 augmented assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) ALC_FLR.3 “Systematic flaw remediation” and AVA_VAN.5 (Advanced methodical vulnerability analysis). It also includes the assurance Composite product package as defined in *[CC]*(Part 5).

The AVA_VAN level applied during the evaluation was AVA_VAN.5. This assurance level is recognised by article 52 of [CSA] as ‘high’.

Consumers of this ICT Product are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

TrustCB B.V., as Certification Assessment Body licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC high certification activities, declares that the product will be listed on the ENISA EU Cybersecurity Certificates list and that the evaluation meets all the conditions for international recognition of Common Criteria Certificates.

Note that the certification results apply only to the specific version of the product as evaluated.

TrustCB B.V., as the Dutch eIDAS-Designated Body responsible in The Netherlands for the assessment of the conformity of qualified electronic signature and/or qualified electronic seal creation devices declares that the evaluation meets the conditions for eIDAS certification for listing on the EU eIDAS compiled list of Qualified Signature/Seal Creation Devices and Secure Signature Creation Devices.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 ICT Product details

2.1 Identification of the ICT Product

The Target of Evaluation (TOE) for this evaluation is ICT product ID-A v1.1 on ID-One Cosmo X, v1.1.1 from IN Smart Identity France located in Courbevoie, France.

The TOE is comprised of the following main components:

	Name		Version
Certified Hardware	Infineon Security Controller IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11		n/a
Certified Java Card platform	ID-One Cosmo X Platform. (ANSSI-CC-2023/06-R01)	R3 + 1 patch	Code SAAAAR: 093363 + patch 099E71
		R4 + 2 patches	Code SAAAAR: 093364 + patches 099441 and 099E21
		R6	Code SAAAAR: 093366
Software	ID-A v1.1	Config 1	Code SAAAAR: 419261FF 01010000 0101
		Config 2	Code SAAAAR: 419261FF 01010000 0201
		Config 3	Code SAAAAR: 419261FF 01010000 0101
		Config 4	Code SAAAAR: 419261FF 01010000 0201
		Config 5	Code SAAAAR: 419261FF 01010000 0301
	Common Package	Config 1	Code SAAAAR: 417641FF 01000000 0201
		Config 2	Code SAAAAR: 417641FF 01000000 0201
		Config 3	Code SAAAAR: 417641FF 01000000 0301
		Config 4	Code SAAAAR: 417641FF 01000000 0301
		Config 5	Code SAAAAR: 417641FF 01000000 0301

The TOE configurations are explained as follows:

Config 1	ID-A Applet without support for Asymmetric Role and Device Authentication
Config 2	ID-A Applet with support for Asymmetric Role and Device Authentication
Config 3	ID-A Applet without support for Asymmetric Role and Device Authentication and with functional biometric authentication
Config 4	ID-A Applet with support for Asymmetric Role and Device Authentication and with functional biometric authentication
Config 5	ID-A Applet without support for Asymmetric Role and Device Authentication and with functional biometric authentication and PIN sharing

Additional requirements for the operational environment of the certified ICT product are described in section 5.4.4 of the *[ST]*.

To ensure secure usage a set of guidance documents is provided with the TOE. For details, see section 2.6 of this report, “Supplementary Cybersecurity Information.

2.2 Contact information related to the evaluation of the ICT Product

Holder of the EUCC Certificate

Organisation name:	IN Smart Identity France
Address:	2 Place Samuel de Champlain – 92400 Courbevoie, France
Certified product contact details	Fabrice.libotte@ingroupe.com

Developer of the certified ICT Product

ICT product developer	IN Smart Identity France

Identification of CAB

The Certification Assessment Body for this ICT Product is TrustCB B.V. TrustCB is licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC certification activities up to and including EUCC High.

TrustCB point of contact: EUCC@trustcb.com

Identification of ITSEF

Evaluation and testing for this ICT Product was performed by following ITSEF:

SGS Brightsight in Delft, The Netherlands

2.3 Security services and policies

2.3.1 Security services

The TOE consists of:

- The chip's circuitry and the IC dedicated software forming the Chip Platform (Hardware Platform);
- The IC embedded ID-One Cosmo X Global Platform Java Card operating system software consisting of
    - Java Card virtual machine, ensuring language-level security,
    - Java Card runtime environment, providing additional security features for Java card technology enabled devices,
    - Java card API, providing access to card's resources for the Applet,
    - Global Platform Card Manager, responsible for management of Applets on the card;
    - Crypto Library;
- ID-A v1.1 Applet along with Common package and interfaces in Server Applet Manager package;
- TOE Guidance documentation for the ID-A v1.1 application and the ID-One Cosmo X platform as specified in Table 4;
- The Global Platform Key Set (for TOE preparation by the Personalisation Agent).

The ID-A v1.1 application provides e-Services and national e-ID Applications based on Java Card. ID-A v1.1 is designed to be compliant with the IAS ECC v2 specification. It provides the following services:

- QSCD/SSCD containing sensitive private keys needed for generating qualified electronic signatures on behalf of the Card Holder as well as for user authentication and identification. The ID-A v1.1 application is intended to be used in the context of official and commercial services, where an electronic digital signature of the Card Holder is required and is to be certified according to [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6],
- PACE authentication as defined in to ensure a trusted channel for secure communication of the TOE with a SCA and a CGA,

- Extended Access Control Version 2 (EAC2). It consists of two parts: Chip Authentication Protocol Version 2 and Terminal Authentication Protocol Version 2.

2.3.2 Vulnerability management

The following vulnerability policy has been identified as applicable to the ID-A v1.1 on ID-One Cosmo X, v1.1.1

Document reference: Coordinated Vulnerability Disclosure Policy, FQR 151007-196, edition 3

2.3.3 Assurance Continuity policies

This is a new product certification. An assurance continuity policy was not provided.

2.3.4 Lifecycle management processes and production facilities

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 4.

2.3.5 Patch management process

Not applicable to this evaluation.

2.4 Assumptions and Clarification of Scope

2.4.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 5.4.3 of the *[ST]*.

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE and its configuration in the environment to fulfil all Assumptions described in the [ST].

2.4.2 Clarification of scope

Considering all Assumptions above, the evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

Threats addressed by the TOE and the IT environment are presented in Section 5.7 of *[ST]* and include the threats as presented in the [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6] *[PP]*, but also includes additional threats. The assumed level of expertise of the attacker for all identified threats is high.

The Organizational Security Polices (OSPs) are the same as in *[PP]*. No OSPs have been added, removed or modified.

2.5 Architectural Information

The TOE consists of an applet upon a Java Card platform designed to provide identification, authentication and advanced signature creation functionality for national ID cards, health cards and corporate cards.

The TOE can be used to create advanced or qualified signature in the sense of [eIDAS] in its Qualified Signature Creation Device (QSCD) configuration and complies with the Identification Authentication Signature for European Citizen Card IAS ECC v2 specification [IAS ECC].

The TOE supports wired communication, through the IC contacts exposed to the outside, as well as wireless communication through an antenna connected to the IC. The TOE may be used on several physical form factors: modules within an inlay, or eCover; in a contact, contactless or dual plastic card.

2.6 Supplementary Cybersecurity Information

The following website links were provided for the ID-A v1.1 on ID-One Cosmo X, v1.1.1 for the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881:

https://ingroupe.com/psirt

https://ingroupe.com/product/id-a

This link provides further details and links on:

- Guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ID-A v1.1 on ID-One Cosmo X, v1.1.1.
- The period during which the ID-A v1.1 on ID-One Cosmo X, v1.1.1 security support will be offered to end users, in particular as regards the availability of cybersecurity related updates. This is stated as: 5 years aligned with the validity of the issued EUCC certificate.
- Contact information and accepted method for receiving vulnerability information from end users and security researchers for the ID-A v1.1 on ID-One Cosmo X, v1.1.1.
- The online repository listing publicly disclosed vulnerabilities related to the ID-A v1.1 on ID-One Cosmo X, v1.1.1 and to any relevant cybersecurity advisories .

Note: The following documentation, guidance and recommendations, is provided with the product by the developer to the customer to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ID-A v1.1 on ID-One Cosmo X, v1.1.1:

Identifier	**Version**
ID-A v1.1 on ID-One Cosmo X, AGD_PRE, FQR: 151007-446	Issue: 3, 13/05/2026
ID-A v1.1 on ID-One Cosmo X, AGD_OPE, FQR: 151007-447	Issue: 3, 13/05/2026

3 Evaluation summary

3.1 Identification of used assurance components

The assurance components used in the product testing were:

- **EAL 5 augmented with ALC_DVS.2, ALC_FLR.3 and AVA_VAN.5** and
- **Composition evaluation package (COMP)**,

as defined by, and detailed in, *[CC]* and *[CEM]*.

3.2 EUCC State of the Art documents and Protection Profiles

EUCC state-of-the-art documents *[SotA Documents]* were applied as referenced in the Bibliography.

The following Protection Profiles were applied:

- Protection profiles for secure signature creation device — Part 2: Device with key Generation, EN 419211-2:2013, CEN/TC 224, BSI-CC-PP-0059-2009-MA-02, Version 2.0.1, June 30 2016
- Protection profiles for secure signature creation device – Part3: Device with key import, EN 419211-3:2013, CEN/TC 224, BSI-CC-PP-0075-2012-MA-01, Version 1.0.2, June 30 2016
- Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application, EN 419211-4:2013, CEN/TC 224, BSI-CC-PP-0071-2012-MA-01, Version 1.0.1, June 30 2016
- Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application, EN 419211-5:2013, CEN/TC 224, BSI-CC-PP-0072-2012-MA-01, Version 1.0.1, June 30 2016
- Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature-creation application, EN 419211-6:2013, CEN/TC 224, BSI-CC-PP-0076-2013-MA-01, Version 1.0.4, June 30 2016

3.3 ICT Product testing

The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

3.3.1 Testing approach and depth

The developer uses both an external and internal testing approaches. The documentation describes how the external TSFI are covered by testing and provides the internal component testing. The developer describes the test configuration in documentation and defines five groups of test units explained with more details. These tests are executed in 26 different samples with different configuration and in most cases, each test is executed in more than one sample. Moreover, the developer executes additional external test plan with the third party tool Keolabs to test the compliance to IAS ECC and EACv2.

The evaluator defined these independent tests to perform some additional verifications:

- Checking correctness of the TOE version verification process (according to the guidance documentation);
- Checking correctness of key functionalities of the TOE

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

3.3.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE. During this attack, oriented analysis the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this analysis will be performed according to the attack methods in [JIL-AMS]. An important source for assurance in this step is the technical report [ETRfC-IC-V6] and [CertRep-IC-V6] of the underlying platform.
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 1.5 weeks. During that test campaign, 0% of the total time was spent on physical attacks, 0% overcoming sensors and filters, 100% perturbation attacks, 0% retrieving keys with FA, 0% side-channel attacks, 0% exploitation of test features, 0% attacks on RNG, 0% ill-formed Java Card application, 0% software attacks, and 0% application isolation penetration tests.

3.3.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*.

3.3.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

The algorithmic security level exceeds 100 bits for all evaluated cryptographic functionality as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities.

3.4 ICT Product evaluation

3.4.1 Reused evaluation results

This was a new certification under EUCC.

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of nine site certificates or Site Technical Audit Reports.

No sites have been visited as part of this evaluation.

3.4.2 Evaluated configuration

The TOE is defined uniquely by its name and version number ID-A v1.1 on ID-One Cosmo X, v1.1.1. The TOE configurations and delivery are listed in the guidance referenced in section 2.5 of this report.

3.4.3 Assessment against each assurance requirement

ASE

ASE	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1
Security objectives	ASE_OBJ.2
Extended components definition	ASE_ECD.1
Security requirements	ASE.REQ.2
TOE summary specification	ASE.TSS.1
Consistency of Composite product ST	ASE.COMP.1

ADV

ADV	
Security architecture	ADV_ARC.1
Functional specification	ADV_FSP.5
Implementation representation	ADV_IMP.1
TSF internals	ADV_INT.2
TOE design	ADV_TDS.4
Composite design compliance	ADV_COMP.1

AGD

AGD	
Operational user guidance	AGD_OPE.1
Preparative procedures	AGD_PRE.1

ALC

ALC	
CM capabilities	ALC_CMC.4
CM Scope	ALC_CMS.5
Delivery	ALC_DEL.1
Development security	ALC_DVS.2
Life cycle definition	ALC_LCD.1
Flaw remediation	ALC_TAT.2
Tools and techniques	ALC_FLR.3
Integration of composition parts and consistency check of delivery procedures	ALC_COMP.1

.**ATE**

ATE	
Coverage	ATE_COV.2
Depth	ATE_DPT.3

Functional tests	ATE_FUN.1
Independent testing	ATE_IND.2
Composite functional testing	ATE_COMP.1

AVA

AVA	
Vulnerability analysis	AVA_VAN.5
Composite vulnerability assessment	AVA_COMP.1

3.5 Results of the evaluation

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report, other evaluator documents and developer documentation *[DEV_DOCS].*

The verdict of each claimed assurance requirement is "**Pass**".

Based on the evaluation results the evaluation lab concluded the ID-A v1.1 on ID-One Cosmo X, v1.1.1, to be **CC:2022 R1 1 Part 2 Conformant, CC:2022 R1 Part 3 conformant**, at an assurance level recognised by article 52 of [CSA] as '**High**' with **AVA_VAN.5** and to meet the requirements of **EAL 5 augmented with ALC_DVS.2, ALC_FLR.3 and aVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

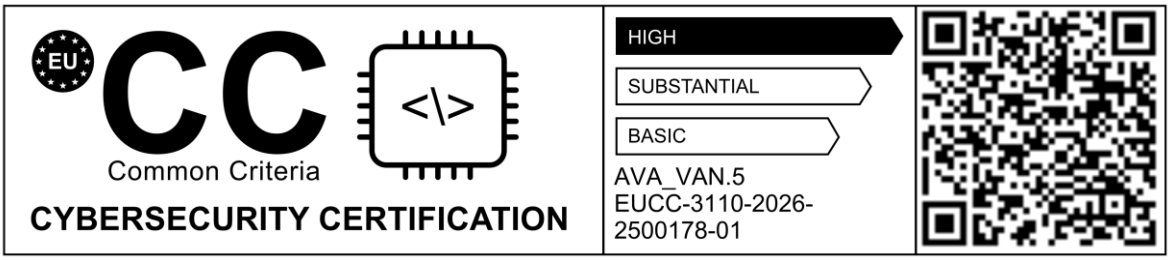
The Security Target claims 'strict' conformance to the Protection Profiles [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6].

3.6 Certificate information and scheme label

A Certificate has been issued recognising this evaluation result as follows:

Unique identifier: EUCC-3110-2026-2500178-01

Date of issuance: 26-07-2026 and with a validity period of **5 years**.



3.7 Comments and Recommendations

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 “high attack potential”. To be protected against attackers with a “high attack potential”, appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

4 Security Target

The certification references the following security target:

ID-A v1.1 on Cosmo X - Security Target, FQR 151007-438, rev 3.0, 19 May 2026 *[ST]*.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

5 Glossary

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information and communication technologies product as defined by [EUCC]
ITSEF	IT Security Evaluation Facility
EUCC	European Cybersecurity Certification Scheme [EU-EUCC], created under the Cybersecurity Act [EU-CSA] and detailed in Commission Implementing Regulation (EU) 2024/482
PP	Protection Profile
SotA	EUCC State-of-the-Art document
TOE	Target of Evaluation; the object of the certification activity described by this report

6 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, CC:2022 Parts 1, 2, 3, 4 and 4, R1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 R1, November 2022
[CCMB-2024-002]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1
[CC2022_TP]	Transition Policy to CC:2022 and CEM:2022
[PLAT-CERT]	Certificate ANSSI-CC-2023/06-R1, 18 December 2024
[PLAT-ETRfC]	Evaluation Technical Report: ETR for composition – HERA-R01, v1.1, 25/11/2024
[PLAT-ST]	Security Target Lite ID-ONE COSMO X, FQR 110 A19A, Ed 3, 13/09/2024
[DEV_DOCS]	- ID-One Cosmo X, Reference Guide, FQR 110 9563, Edition 13, 15/03/2023 - ID-One Cosmo X, Pre-Perso Guide, FQR 110 9562, Revision 13.0, 15/03/2023 - ID-One Cosmo X on SLC37, Applet Security Recommendations, FQR 110 9572, Issue 9, 24/09/2024 - ID-One Cosmo X, Application Loading Protection Guidance, FQR 110 9603, Issue 3, 05/05/2021 - ID-A v1.1 on ID-One Cosmo X, Configuration List, Issue: 1.5, 20/07/2026 - ID-A Application Product Generation Description (PGD), Issue: 1-AD, 11/05/2026
[eIDAS-REP]	Assessment Reporting Sheet eIDAS "ID-A v1.1 on ID-One Cosmo X v1.1.1", 26-RPT-663, version 4.0, 24 July 2026
[PP-SSCD2]	EN 419211-2:2013, Protection profiles for secure signature creation device - Part 2: Device with key Generation, V2.0.1, registered under the reference BSI-CC-PP-0059-2009-MA-02
[PP-SSCD3]	EN 419211-3:2013, Protection profiles for secure signature creation device - Part3: Device with key import, V1.0.2, registered under the reference BSI-CC-PP-0075-2012-MA-01
[PP-SSCD4]	EN 419211-4:2013, Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application, V1.0.1, registered under the reference BSI-CC-PP-0071-2012-MA-01
[PP-SSCD5]	EN 419211-5:2013, Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application, V1.0.1, registered under reference BSI-CC-PP-0072-2012-MA-01
[PP-SSCD6]	EN 419211-6:2014 Protection profiles for secure signature creation device - Part6: Extension for device with key import and trusted channel to signature-creation application, V1.0.4, registered under the reference BSI-CC-PP-0076-2013-MA-01
[ETR]	Evaluation Technical Report “ID-A v1.1 on ID-One Cosmo X v1.1.1” – EAL5+, 26-RPT-323, v8.0, 24 July 2026

[EU-CSA]	REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[EU-eIDAS]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
[EU-EUCC]	COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
[EU-EUCC-amdt.1]	Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
[EU-EUCC-amdt.2]	Commission Implementing Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art documents
[HW-CERT]	Federal Office for Information Security, Certification Report, BSI-DSZ-CC-1107-V6-2025 for IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 with firmware 80.306.16.0 & 80.306.16.1 & 80.312.02.0, optional NRG™ SW 05.03.4097, opt.HSL v3.52.9708, UMSLC lib v01.30.0564, opt. SCL v2.15.000 and v2.11.003, opt. ACL v3.02.000 and v3.33.003 and v3.34.000 and 3.35.001, opt. RCL v.1.10.007, opt. HCL v1.13.002 and guidance, V1.0, July 10th 2025
[HW-ETRfC]	Evaluation Technical Report for Composite Evaluation (ETR COMP), BSI-DSZ-CC-1107-V6-2025, Version 1, 06/06/2025
[HW-ST]	IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 Security Target Lite, Revision 7.3, 06/05/2025
[SotA_AAPS]	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 and certification for CC: 2022 Version 1, February 2025
[SotA_MSSR]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Minimum Site Security Requirements, Version 2, February 2025.
[SotA_QSCD]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices according to eIDAS Regulation (EU) 910/2014, as amended by Regulation (EU) 2024/1183. Version 1, February 2025

[SotA_SARC]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Security Architecture requirements (ADV_ARC) for smart cards and similar devices extended to Secure Sub Systems in SoCs, version 1.1, October 2023
[ST]	ID-A v1.1 on Cosmo X - Security Target, FQR 151007-438, rev 3.0, 19 May 2026
[ST-lite]	ID-A v1.1 on Cosmo X – Public Security Target, FQR 151007-418, rev. 4.0, 20 July 2026
[ST-SAN]	Sanitization of a security target for publication, [EUCC] Annex V section V.2, ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)