EUCC Certification Report

ID-One Cosmo XE, version 8A46C1

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-3110-2026-2500109-01 Certification Report**
Report version:	**1**
Project number:	**EUCC-2500109-01**
Author(s):	**Haico Haak, TrustCB B.V.** **contact: eucc@trustcb.com**
Date:	**07 September 2026**
Number of pages:	**20**
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-One Cosmo XE, version 8A46C1, 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 is a dual-interface Java Card platform based, compatible with multi-application ID-One Cosmo product family. The functional level of the OS is based on a Java™ based multi-application platform, compliant with Java Card 3.1 Classic Edition and Global Platform 2.3 specifications.

This ID-One Cosmo XE platform is able to receive and manage different types of applications, Basic and Sensitive ones. All the platform code including GP Java application called card manager are loaded in the FLASH memory.

The TOE allows the suppression of Modules during pre -personalization or personalization with FLEXICODE mechanism.

The TOE allows the loading of optional code, Javacard applications and native code:

- Optional code can be loaded to upgrade the TOE (platform) at any time of product life cycle, this function is named JPatch.
- Native code, viewed as a library behind the JCS, can also be loaded at any time with the JBOX functionality.
- Applications can be loaded on the flash memory, at pre -personalisation, personalisation or use phase.
- Optional code (CodOp) can be loaded to upgrade an applet at any time of product life cycle.

However, the Card Issuer can forbid each of these operations before or after the issuance of the card.

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

- Java Card System - Open Configuration Protection Profile, version 3.2, July 2024 registered under the reference BSI-CC-PP-0099-V3-2024

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-3110-2026-2500109-01**, dated 07-08-2026 and with a 5-year validity.

The evaluation of the TOE was performed by SGS Brightsight B.V. located in Delft , The Netherlands. The evaluation was completed on 05-08-2026 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 (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with AVA_VAN.5 (Advanced methodical vulnerability analysis), ALC_DVS.2 (Sufficiency of security measures), ALC_FLR.3 (Systematic flaw

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

remediation), ADV_IMP.2 (Complete mapping of the implementation representation of the TSF), ADV_TDS.5 (Complete semiformal modular design), ADV_INT.3 (Minimally complex internals), ALC_CMC.5 (Advanced support), ALC_TAT.3 (Compliance with implementation standards - all parts), ATE_COV.3 (Rigorous analysis of coverage) and ATE_FUN.2 (Ordered functional testing). It also includes the assurance Composite product package as defined in *[CC]*(Part 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.

2 ICT Product details

2.1 Identification of the ICT Product

The Target of Evaluation (TOE) for this evaluation is ICT product ID-One Cosmo XE, version 8A46C1 from IN Smart Identity France located in Courbevoie, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	IFX_CCI_000039h	T11
Software	ID-One Cosmo XE	8A46C1

Additional requirements for the operational environment of the certified ICT product are described in section 5.2 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	team.eucc-certification@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 main goal of the TOE is to provide a sound and secure execution environment to critical assets that need to be protected against unauthorized disclosure and/or modification. The TOE with its security function has to protect itself and protect applets from bypassing, abuse or tampering of its services that could compromise the security of all sensitive data.

The TOE has the following features (see *[ST]* section 1.9 for the full list including details):

- Atomic Transactions
- Card Content Management

- Card Management Environment
- Cardholder Verification
- Clearing of sensitive information
- DAP Verification
- Data coherency
- Data integrity
- Encryption and Decryption
- Entity authentication/secure Channel
- Secure Messaging (SM)
- Exception
- Firewall
- GP_Dispatcher
- Hardware operating
- Key Access
- Key Agreement
- Key destruction
- Key Distribution
- Key Generation
- Key Management
- Manufacturer Authentication
- Memory failure
- Message Digest
- Pre-personalisation and Patching
- JPatch at use phase and CodOp for applets
- JBox
- Random Number
- Resident Application dispatcher
- Runtime Verifier
- Security functions of the IC
- Signature
- Unobservability
- CRC 32
- PACE
- FLEXICODE

2.3.2 Vulnerability management

The following vulnerability policy has been identified as applicable to the ID-One Cosmo XE, version 8A46C1,

Document reference: Coordinated Vulnerability Disclosure Policy, FQR 151007-196, Ed.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 1.11.

2.3.5 Patch management process

The following Patch Management process has been assessed as required by the EUCC Annex IV.4:

Patch Management Process	Version
JCVM_PATCH	FQR 151007-194

The outcome of the assessment was that the lab concluded that the TOE follows what is mandated by Article IV.4 of 2024/482. This is reported in [PATCH].

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 5.2 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].

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.

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 4.3 of *[ST]* and include the threats as presented in the *[PP0099]*, but also includes additional threats. The assumed level of expertise of the attacker for all identified threats is High.

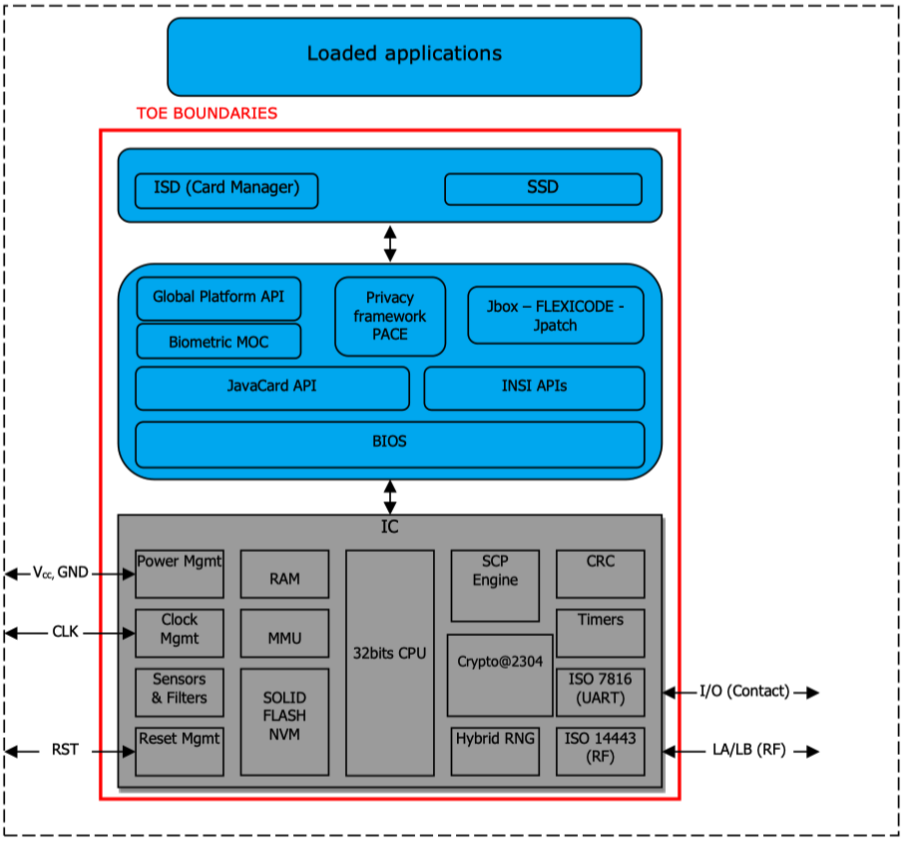
The Organizational Security Polices (OSPs) are the same as in *[PP0099]*, and 5 additional OSPs were added.

The following functionality is present without specific security claims:

- Crypto1 see Section 1.8.4 of *[ST]*
- Cipurse Section 1.8.5.12 of *[ST]*

2.5 Architectural Information

The logical architecture, originating from the Security Target *[ST]* of the TOE can be depicted as follows:



2.6 Supplementary Cybersecurity Information

The following website links were provided for the ID-One Cosmo XE, version 8A46C1 for the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881:

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

https://ingroupe.com/psirt/

These links provides further details/links on TOE-specific information as well as information on how to reach the Product Security Incident Response Team.

- Guidance and recommendations to assist end users of the TOE with the secure configuration, installation, deployment, operation and maintenance of the ID-One Cosmo XE, version 8A46C1.
- The period during which the ID-One Cosmo XE, version 8A46C1 security support will be offered to end users of the TOE, in particular as regards the availability of cybersecurity related updates..
- Contact information and accepted method for receiving vulnerability information from end users and security researchers for the ID-One Cosmo XE, version 8A46C1.
- the online repository listing publicly disclosed vulnerabilities related to the ID-One Cosmo XE, version 8A46C1 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-One Cosmo XE, version 8A46C1:

Identifier	Version
ID-One Cosmo XE on SCL37, Applet Security Recommendations, FQR 151007-203	4
User Guidance Document ID-One Cosmo XE on SLC37, FQR 151007-172	3

ID-One Cosmo XE on SLC37 JAVADOC, FQR 151007-232	1
Biometry, FQR 151 007-201	1
Platform Flash Image Generation, FQR 151 007-209	1
JCVM_PATCH, FQR 151007-194	1
Jbox SW Configuration, FQR 151007-207	1
Global Privacy Framework, FQR 151007-205	1
Pre-Perso Guide ID-One Cosmo XE on SLC37, FQR 151007-171	3
Application Loading Protection Guidance, FQR 151 007-204	1
Secure Acceptance Process, FQR 151 007-208	1

3 Evaluation summary

3.1 Identification of used assurance components

The assurance components used in the product testing were:

- **EAL 5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5 and ALC_FLR.3** 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 were applied as referenced in the Bibliography.

The following Protection Profile was applied:

Java Card System - Open Configuration Protection Profile, version 3.2, July 2024, as certified under the reference BSI-CC-PP-0099-V3-2024 by CAB Bundesamt für Sicherheit in der Informationstechnik (BSI)

3.3 ICT Product testing

Testing (depth, coverage, functional tests, independent 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 performed extensive testing on functional specification, subsystem and SFR-enforcing module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

The underlying hardware and crypto-library test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

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 it was performed according to the *[SotA_AAPS]*. An important source for assurance in this step is the technical report *[HW-ETRfC]* 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 14 man-weeks in total for testing and reporting. During that test campaign 0% of the total time was spent on physical attacks, 0% on overcoming sensors and filters, 36% on perturbation attacks and retrieving keys with FA, 57% side-channel attacks, 0%

exploitation of test features, 0% attacks on RNG, 7% software attacks and 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.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits 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.

For composite evaluations, please consult the *[ETRfC]* for details.

3.4 ICT Product evaluation

3.4.1 Reused evaluation results

This is 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 7 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-One Cosmo XE, version 8A46C1.

The TOE of the evaluated product is an open and isolating platform according to *[SotA_COSP]*. The platform provides isolating mechanisms that follows the Java Card specification and was evaluated according to *[SotA_COSP]*.

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

The *[ST]* contains all relevant information for this class and the according families according to EAL5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5 and ALC_FLR.3 and the COMP package.

ADV

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

Developer Evidence, i.e. implementation representation was provided that enabled the evaluator to ensure that all relevant aspects for this class and the according families according to EAL5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5 and ALC_FLR.3 and the COMP package are met by the TOE.

AGD

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

The guidance documentation for the TOE, as outlined in the *[ST]* is provided that contains all relevant information for this class and the according families according to EAL5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5 and ALC_FLR.3 and the COMP package.

ALC

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

The TOE Life Cycle is covered by audited sites and Developer Documentation has been provided that contains all relevant information for this class and the according families according to EAL5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5 and ALC_FLR.3 and the COMP package.

ATE

ATE	
Coverage	ATE_COV.3
Depth	ATE_DPT.3
Functional tests	ATE_FUN.2
Independent testing	ATE_IND.2
Composite functional testing	ATE_COMP.1

The developer provided Test documentation, a test witnessing session was performed and independent testing was performed. The provided information enabled the evaluator to positively assess that the TOE meets this class and the according families according to EAL5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5 and ALC_FLR.3 and the COMP package.

AVA

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

A vulnerability analysis was performed and penetration tests based on the analysis were conducted. No deviation from the expected result was detected. Therefore, the TOE meets this class and the according families according to EAL5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5 and ALC_FLR.3 and the COMP package.

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]* and Site Technical Audit Report(s) for the referenced site(s) *[STAR]* [2].

To support composite evaluations according to *[COMP]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

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

Based on the evaluation results the evaluation lab concluded the ID-One Cosmo XE, version 8A46C1, to be **CC:2022 R1 Part 2 extended, 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 ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5 and ALC_FLR.3**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'demonstrable' conformance to the Protection Profile *[PP0099]*.

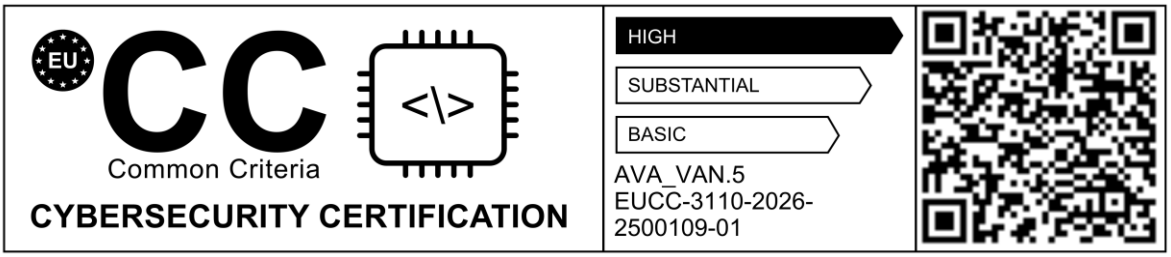
3.6 Certificate information and scheme label

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

Unique identifier: EUCC-3110-2026-2500109-01

Date of issuance: 07-08-2026 and with a validity period of **5 years**.

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.



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: Crypto1 and Cipurse, which are out of scope as there are no security claims relating to these.

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-One Cosmo XE Security Target, FQR 151007-193, Ed. 6, 09 July 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:

AES	Advanced Encryption Standard
AID	Applet Identifier
APDU	Application Protocol Data Unit
API	Application Programmer Interface
BIOS	Basic Input/Output System
CAB	Conformance Assessment Body
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CLFDB	Ciphered Load File Data Block
CM	Card Manager
CPLC	Card Production Life Cycle
cPP	Collaborative Protection Profile
DAP	Data Authentication Pattern
DBI	Digitally Blurred Image
DES	Cryptographic module "Data Encryption Standard"
DSK	Dump Secret Key
EAL	Evaluation Assurance Level
EC	Elliptic Curves
ECC	Elliptic Curve Cryptography
EUCC	EU Common Criteria
GP	Global Platform
IC	Integrated Circuit
ICT	Information and Communication Technology
INSI	IN Smart Identity
ISD	Issuer Security Domain
ISK	Initialization Secret Key
IT	Information Technology
JCP	Java Card Platform
JCRE	Java Card Runtime Environment
JCS	Java Card System

JSK	JPatch Secret Key
LSK	Load Secret Key
MOC	Match-On-Card
MRTD	Machine readable travel document
MSK	Master Secret Key
NA	Not Applicable
NCCA	National Cybersecurity Certification Authrity
OSP	Organizational Security Policy
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
PUK	Personal Unlocking Key
RNG	Random Number Generation
RSA	Cryptographic module "Rivest, Shamir, Adleman"
SCP	Smart Card Platform
SF	Security Function
SFP	Security Function Policy
SHA-1	Cryptographic module "Secure hash standard"
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
VM	Virtual Machine

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 5, 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 1.2
[DEV_DOCS]	ID-One Cosmo XE on SCL37, Applet Security Recommendations, FQR 151007-203, Version 4, 01 June 2026 User Guidance Document ID-One Cosmo XE on SLC37, FQR 151007-172, Version 3, 01 June 2026 ID-One Cosmo XE on SLC37 JAVADOC, FQR 151007-232, Version 1, 04 November 2025 Biometry, FQR 151 007-201, Version 1, 25 March 2025 Platform Flash Image Generation, FQR 151 007-209, Version 1, 28 March 2025 JCVM_PATCH, FQR 151007-194, Version 1, 21 March 2025 Jbox SW Configuration, FQR 151007-207, Version 1, 27 March 2025 Global Privacy Framework, FQR 151007-205, Version 1, 26 March 2025 Pre-Perso Guide ID-One Cosmo XE on SLC37, FQR 151007-171, Version 3, 01 June 2026 Application Loading Protection Guidance, FQR 151 007-204, Version 1, 26 March 2025 Secure Acceptance Process, FQR 151 007-208, Version 1, 28 March 2025 ID_One Cosmo XE Configuration List, Version 1.0, 11 June 2026
[ETR]	Evaluation Technical Report “ID-One Cosmo XE” – EAL5+, 26-RPT-339, Version 5.0, 5 August 2026
[ETRfC]	ETR for Composite Evaluation Title Evaluation Technical Report for Composition “ID-One Cosmo XE” – EAL5+, 26-RPT-341, Version 4.0, 8 July 2026
[PATCH]	EUCC-2500109-01 CSC-219 - Patch Management, 28 July 2026, Project no. 16261
[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-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]	BSI-DSZ-CC-1107-V6-2025, Smartcard 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 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
[HW-ETRfC]	Evaluation Technical Report for Composite Evaluation (ETR COMP) 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 , BSI-DSZ-CC-1107-V6, version 1, 06 June 2025
[HW-ST]	Security Target Lite BSI-DSZ-CC-1107-V6-2025, 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, v7.3, 06 May 2025
[PP0099]	Java Card System - Open Configuration Protection Profile, version 3.2, July 2024 registered under the reference BSI-CC-PP-0099-V3-2024
[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_COSP]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT CERTIFICATION OF “OPEN” SMART CARD PRODUCTS VERSION 1.1, October 2023
[SotA_MSSR]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Minimum Site Security Requirements, Version 2, 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
[SotA_STAR]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT, STAR methodology, version 1, February 2025
[SotA_CRYPTO]	EUCC SCHEME, GUIDELINES ON CRYPTOGRAPHY, Agreed Cryptographic Mechanisms, Version 2, May 2025
[ST]	ID-One Cosmo XE Security Target, FQR 151007-193, Ed. 6, 09 July 2026
[ST-lite]	ID-One Cosmo XE Public Security Target, FQR 151007–268 Ed2, 09 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.)