Certification Report

ID-One CNS V2 on COSMO V9.1

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:	**NSCIB-CC-2500021-01-CR**
Report version:	**1**
Project number:	NSCIB-**2500021-01**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**12 February 2026**
Number of pages:	**13**
Number of appendices:	**0**

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) 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 (site) security target is a requirements specification document that defines the scope of the evaluation activities.

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

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of 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.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the ID-One CNS V2 on COSMO V9.1. The developer of the ID-One CNS V2 on COSMO V9.1 is IN Smart Identity France located in Courbevoie, France and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is the Smart Card Integrated Circuit with Embedded Software serving as a QSCD (Qualified Signature Creation Device) in accordance to its functional specification. The Smart Card chip module can be embedded in a plastic card providing a physical interface between the terminal and the chip.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 12 February 2026 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the ID-One CNS V2 on COSMO V9.1, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the ID-One CNS V2 on COSMO V9.1 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.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the ID-One CNS V2 on COSMO V9.1 from IN Smart Identity France located in Courbevoie, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SLC32GDL400G3 SLC32GDA400G3	IFX_CCI_000005
	Software Library - HSL	V01.22.4346-SLCx2_C65.lib
	Java Card Platform - ID-ONE COSMO V9.1 BIOMETRY	SAAAAR 092914
Software	ID-One CNS V2	Code version “20 33 81” Internal version “00 00 01 09”

To ensure secure usage a set of guidance documents is provided, together with the ID-One CNS V2 on COSMO V9.1. For details, see section 2.5 “Documentation” of this report.

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

2.2 Security Policy

The TOE is a composite TOE, consisting of a CNS applet, a Java Card smart card operating system and an underlying IC. The TOE is a Smart Card Integrated Circuit with Embedded Software serving as CNS application, which provides QSCD functionality.

The TOE provides the following security features:

- generation of the SCD and the correspondent SVD,
- import of the SCD and, optionally, the correspondent signature verification data (SVD)
- export the SVD for certification through a trusted channel to the CGA,
- prove the identity as QSCD to external entities
- optionally, receive and store certificate info
- switch the TOE from a non-operational state to an operational state, and
- if in an operational state, create digital signatures for data with the following steps:
    - select an SCD if multiple are present in the QSCD,
    - receive DTBS or a unique representation thereof DTBS/R through a trusted channel with SCA.
    - authenticate the signatory and determine its intent to sign,
    - apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS/R
- identification and authentication of trusted users and applications,
- data storage and protection from modification or disclosures, as needed,
- secure exchange of sensitive data between the TOE and a trusted application,
- secure exchange of sensitive data between the TOE and a trusted human interface device.

Even though Netlink Authentication is supported, it is not in scope of the certification and only usable for files out of the QSCD configuration as it does not provide any of the keys needed for this type of authentication.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

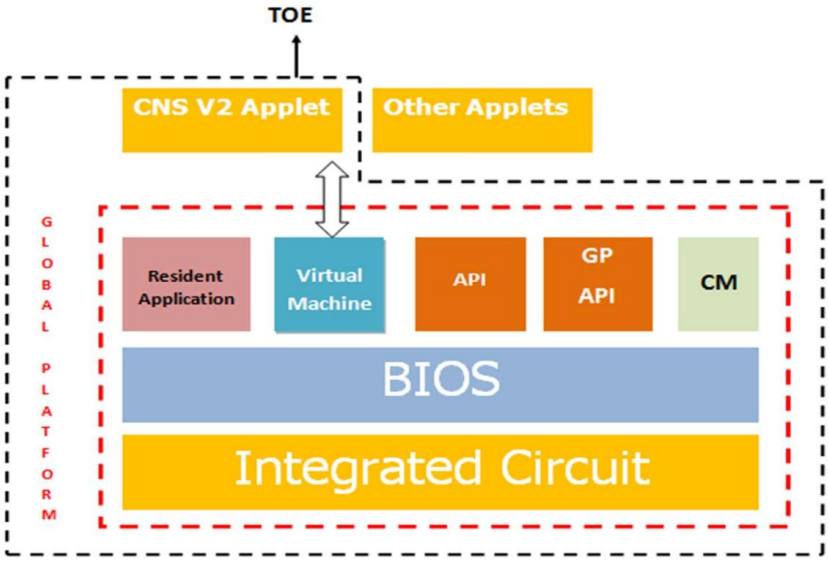
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 11.3 of the *[ST] or [ST-lite]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The TOE architecture can be depicted as follows:



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
FQR 220 1516 – ID-One CNS V2 Java Applet on Cosmo V9.1 – AGD_PRE, dated 05 November 2020	Issue 1
FQR 220 1517 – ID-One CNS V2 Java Applet on Cosmo V9.1 – AGD_OPE, dated 05 November 2020	Issue 1
FQR 220 1401 – ID-One CNS V2 Java Applet – User Guide, dated 30 October 2020	Issue 7
FQR 110 9208 – ID-One Cosmo v9.1 Biometry Pre-Perso Ed 9 01/12/2021 Guide, dated 01 December 2021	Ed 9
FQR 110 9200 – ID-One Cosmo v9.1 Biometry Reference Ed 8 16/03/2022 Guide, dated 16 March 2022	Ed 8
FQR 110 9237 – ID-One Cosmo v9.1 Biometry Applet Security Recommendations, dated 10 January 2022	Ed 3

FQR 110 9238 – ID-One Cosmo V9.1 Biometry Application Loading Protection Guidance, dated 09 October 2019	Ed 1
FQR 110 8921 – Secure acceptance and delivery of sensitive elements, dated 24 September 2018	Ed 1
FQR 110 9242 – Java Card API on ID-One Cosmo V9.1 platform	Ed 1
FQR 110 9402 – ID-One Cosmo v9.1 Biometry Cosmo Flash Image Generation, dated 27 November 2019	Ed 1
FQR 110 8805 – JCVM_PATCH, dated 23 August 2019	Ed 2

2.6 IT 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.

2.6.1 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.

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.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD no potential vulnerabilities were identified from generating questions to the type of TOE and the specified behaviour.
- For ADV_IMP a thorough implementation representation review was performed on the TOE. During this attack-oriented analysis, the protection against the attack scenarios was analysed using the knowledge gained from all previous evaluation classes. This resulted in the identification of additional potential vulnerabilities. This analysis was performed according to the attack list in [JIL-AP]. An important source for assurance against attacks in this step is the [91_ETRfC] of the underlying platform; no additional potential vulnerabilities were concluded from this.
- After the first implementation representation review, the Developer decided to update the product in order to improve the security of the TOE and address some of the identified potential vulnerabilities. A second implementation representation review was performed to analyse the code modifications, following the same approach as for the first review.
- All potential vulnerabilities were analysed using the knowledge gained from the two implementation representation reviews, all the evaluation classes and the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. All potential vulnerabilities were found to be not exploitable due to the security mechanisms of the certified Java Card platform, which rendered all the potential attack paths impractical. No penetration tests were defined.

The total test effort expended by the evaluators was 1 week. During that test campaign, 100% of the total time was spent on Perturbation attacks, 0% on side-channel testing, and 0% on logical tests.

2.6.3 Test configuration

The TOE used for testing was: ID-One CNS V2 on SLC32GDA400G3.

2.6.4 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.

2.7 Reused Evaluation Results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and penetration testing has been renewed.

There has been extensive reuse of the ALC aspects for the sites involved in the software component of the TOE. Sites involved in the development and production of the hardware platform were reused by composition.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number ID-One CNS V2 on COSMO V9.1.

2.9 Evaluation Results

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

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

Based on the above evaluation results the evaluation lab concluded the ID-One CNS V2 on COSMO V9.1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_DVS.2 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 Profile *[EN419211-2], [EN419211-3], [EN419211-4], [EN419211-5] and [EN419211-6]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" 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).

3 Security Target

The IN Groupe CNS V2 on Cosmo V9.1 Security Target, Version 5, Dated 16 January 2026 *[ST]* is included here by reference.

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

4 Definitions

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

IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
QSCD	Qualified Signature Creation Device
TOE	Target of Evaluation

5 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, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[EN419211-2]	EN 419 211-2:2013, 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
[EN419211-3]	EN 419 211-3:2013, Protection profiles for secure signature creation device - Part 3: Device with key import, V1.0.2, registered under the reference BSI-CC-PP-0075-2012-MA-01
[EN419211-4]	EN 419 211-4:2013, Protection profiles for Secure signature creation device — Part 4: Device with key generation and trusted communication with certificate generation application, V1.0.1, registered under the reference BSI-CC-PP-0071-2012-MA-01
[EN419211-5]	EN 419211-5:2013, Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted communication with signature creation application, V1.0.1, registered under the reference BSI-CC-PP-0072-2012-MA-01
[EN419211-6]	EN 419211-6:2014 Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature creation application, Version 1.0.4, registered under the reference BSI-CC-PP-0076-2013-MA-01
[ETR]	Evaluation Technical Report “ID-One CNS V2 on Cosmo V9.1” – EAL4+, 26-RPT-081, Version 2.0, Dated 27 January 2026
[HW-CERT]	BSI-DSZ-CC-1110-V7-2024 for Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 from Infineon Technologies AG, Version 1.0, 30 September 2024.
[HW-ETRfC]	ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC1110-V7-2024, Version 3, 2023-12-01, ETR for composite evaluation (EFC), TÜV Informationstechnik GmbH (confidential document)
[PLAT_CERT]	Rapport de certification ANSSI-CC-2020/07-R01 Plateforme ID-One Cosmo V9.1 masquée sur le composant IFX SLC32 (Identification du matériel 092915), Paris, le 09 Mai 2025
[PLAT_ETRfC]	Evaluation Technical Report: ETR for composition - PYRRHA-R01, v1.5, 24/04/2025
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2.1, February 2024

[JIL-AMS]	Attack Methods for Smartcards and Similar Devices, Version 2.5, May 2022 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	IN Groupe CNS V2 on Cosmo V9.1 Security Target, Version 5, Dated 16 January 2026
[ST-lite]	IN Groupe CNS V2 on Cosmo V9.1 Public Security Target, Version 2, Dated 16 January 2026
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)