Certification Report

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

Sponsor and developer:	***IDEMIA*** **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-2300123-01-CR**
Report version:	**1**
Project number:	**2300123-01**
Author(s):	**Andy Brown**
Date:	**22 December 2023**
Number of pages:	**14**
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.

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 ID-A v1.1 on ID-One Cosmo X. The developer of ID-A v1.1 on ID-One Cosmo X is IDEMIA 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 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 *[EU-REG]* 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.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 22 December 2023 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 ID-A v1.1 on ID-One Cosmo X, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of ID-A v1.1 on ID-One Cosmo X 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 EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures), AVA_VAN.5 (Advanced methodical vulnerability analysis), and ALC_FLR.1 (Basic flaw remediation).

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.

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 is the *[ST],* for the purposes of electronic identification and trust services as detailed by the *[EU-REG]*. The evaluation by SGS Brightsight B.V included an examination of the TOE according to the eIDAS Dutch Conformity Assessment Process Version 6 0.

[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-A v1.1 on ID-One Cosmo X from IDEMIA located in Courbevoie, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier		Version
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
Platform	ID-One Cosmo X Platform		Code SAAAAR: 093363 + patch 099E71 Code SAAAAR: 093364 + patches 099441 and 099E21 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

To ensure secure usage a set of guidance documents is provided, together with the ID-A v1.1 on ID-One Cosmo X. For details, see section 2.5 “Documentation” of this report.

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

2.2 Security Policy

The TOE has the following features:

- **Authentication mechanisms**: The TOE supports the following authentication mechanisms: User authentication (PIN), Symmetric and Asymmetric Role authentication, Terminal Authentication v2, Symmetric and Asymmetric Device authentication, Chip Authentication v2, PACE protocol, GP authentication in phase 6 (personaliser) and 7 (TOE admin) and Combined Device/Role authentication.
- **Cryptographic operations**: The TOE supports high-level cryptographic operations (key generation, symmetric and asymmetric encryption and decryption, signature creation, destruction of cryptographic keys and random number generation). The implementation is mainly based on the Security Functionalities provided by the platform.
- **Trusted Channel function**: The TOE supports secure communication channel to verify authenticity and integrity as well as securing confidentiality of user data between the TOE and other devices connected.

- **Access Control function**: The TOE supports access to objects (files, directories, data and secrets) stored in the ID-A file system. It ensures secure management of secrets such as cryptographic keys.
- **Data Storage function**: The TOE supports secure storage of manufacturing data, pre-personalisation data and personalisation data. This covers also the secure storage of SCD/SVD and RAD.
- **Integrity function**: The TOE supports the verification of the integrity of sensitive user data and the integrity of the DTBS/R.
- **Electronic Services**: The TOE supports several electronic services: Client/Server authentication, Digital signature, Encryption key decipherment and Symmetric encryption and decryption.
- **Keys and PINs management**: The TOE supports the handling of cryptographic data objects, such as keys and PINs.
- **Single Sign on feature (SSO)**: The TOE may also behave as a Single Sign on (SSO). It provides access points to any other applet willing to use authentication services based on a PIN.
- **Features from the Platform***:* The TOE leverages the security features from the certified platform i.e., protection against environmental conditions and physical manipulation, security domains isolation supported by the Java Card platform and Cryptographic operations.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

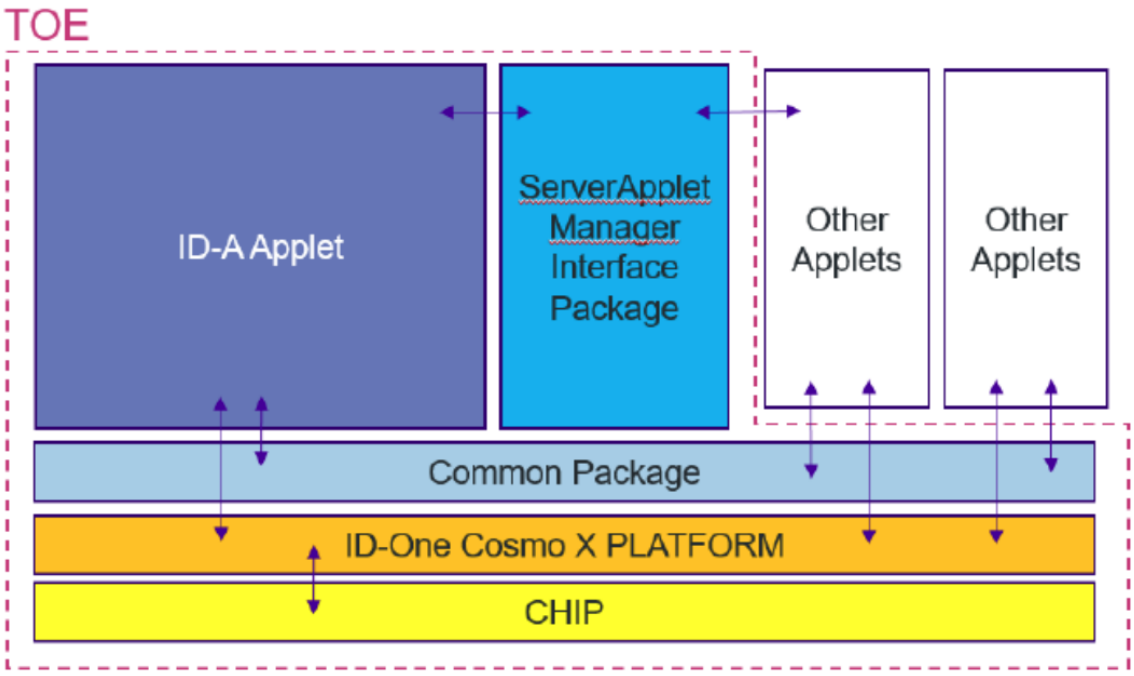
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 7.2 of the *[ST]*.

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



The TOE is composed of the following elements:

- Infineon SLC37 microcontroller including the firmware for booting and low level functionality of the microcontroller e.g. writing to flash memory as well as software for implementing cryptographic operations.
- The ID-One Cosmo X Java Card platform, which can be split into the following components:
  - Software for implementing a Java Card Virtual Machine, a Java Card Runtime Environment and a Java Card Application Programming Interface.
  - Software for implementing content management.
  - Support for PACE secure channel establishment.
- The ID-A v1.1 applet, which can be produced in 5 configurations:
  - 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.
- The associated guidance documentation.

2.5 Documentation

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

Identifier	**Version**
IDEMIA, ID-A v1.1 on ID-One Cosmo X, AGD_OPE, FQR : 401 9412	Issue 4
IDEMIA, ID-A v1.1 on ID-One Cosmo X, AGD_PRE, FQR : 401 9411	Issue 5

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 TOE was tested thoroughly by the developer covering all the security functions and aspects of the TSF.

The following developer tests were witnessed and used to sample and check the actual test results:

- Tests related to the PIN authentication mechanism.
- Tests related to test RSA and RSA-PSS signature creation for different combinations of key lengths and digest algorithms.
- Tests related to test ECC signature creation for different combinations of key lengths and digest algorithms.
- Tests related to Device Authentication Asymmetric scheme.
- Tests related to Device Authentication Asymmetric with privacy protection scheme.
- Tests related to Device Authentication Symmetric scheme.
- Tests related to Role Authentication asymmetric scheme.
- Tests related to Role Authentication symmetric scheme.
- Tests related to Client/Server Authentication functionality.
- Tests related to Key generation functionality.
- Tests related to Digital signature under a secure channel.
- Tests related to Encryption key decipherment functionality.
- Tests related to EACv2 secure channel functionality.
- Tests related to PACE secure channel functionality.
- Tests related to Key import functionality.

Additionally, some negative tests were executed with specific TOE configurations not supporting the tested functionality

All tests gave the expected outcome.

The evaluator selected a small sample of tests to verify the correctness of the developer testing. For the testing performed by the evaluators, the developer has provided samples. The evaluator devised and executed a set of tests aiming to verify the correctness of the TOE verification process, the User Authentication, Digital signature authentication and Device Authentication.

All tests gave the expected outcome.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted as follows:

- 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 was performed on the TOE. During this attack-oriented analysis the protection of the TOE was analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. This analysis was performed according to the attack methods in *[JIL-AM].* During this assessment part the technical report *[PLT-ETRfC]* and *[PLT-CERT]* of the underlying platform was used in the analysis.

- All potential vulnerabilities were 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 were not exploitable. The potential vulnerabilities were addressed by penetration testing, a guidance update or in other ways that were deemed appropriate.

2.6.3 Test configuration

The TOE was tested using Config 4 as representative for all configurations.

The Evaluators provided an equivalency argumentation for why the configuration used was valid for all configurations.

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

There is no reuse of evaluation results in this certification

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.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number ID-A v1.1 on ID-One Cosmo X as described in the identification part of this report, section 2.1.

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-A v1.1 on ID-One Cosmo X, to be **CC Part 2 extended, CC Part 3 conformant** and to meet the requirements of **EAL 5 ALC_DVS.2, AVA_VAN.5 and ALC_FLR.1**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profiles *[EN419211-2], [EN419211-3], [EN419211-4], [EN419211-5], [EN 419211-6].*

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 ID-A v1.1 on Cosmo X - Security Target, FQR 110 A1E3, Ed 2, 26 October 2023 *[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: Include the list of acronyms from the ETR that have been included in this Certification Report and then check that this list is complete and in alphabetical order.

DCAP	Dutch Conformity Assessment Process
DTBS	Data to be signed
DTBS/R	Data to be signed or its unique representation
ITSEF	Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands scheme for certification in the area of IT security
PP	Protection Profile
PACE	Password Authenticated Connection Establishment
QSCD	Qualified Signature Creation Device
SCD	Signature Creation Data
SSCD	Secure Signature Creation Device
SVD	Signature Verification Data
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 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
[EN419211-3]	EN 419211-3:2013, 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 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 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 channel to signature creation application, V1.0.1, registered under the reference BSI-CC-PP-0072-2012-MA-01
[EN 419211-6]	EN 419211-6:2014, Protection profiles for secure signature creation device – Part 6: 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” – EAL5+, 23-RPT-959, Version 2.0, 13 December 2023
[EU-REG]	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
[PLT-CERT]	ID-One Cosmo X Platform, NSCIB-CC-2300050-01, Version 1, 15 June 2023
[PLT-ETRfC]	Evaluation Technical Report for Composition ID-One Cosmo X v2.0 – EAL6+, 24-RPT-664, version 2.0, dated 13 June 2023
[PLT-ST]	Public Security Target ID-ONE COSMO X EAL6+, FQR 110 A23D, Edition 1, 02 June 2023
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022
[JIL-AMS]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022

[ST]	ID-A v1.1 on Cosmo X - Security Target, FQR 110 A1E3, Ed 2, 26 October 2023
[ST-lite]	ID-A v1.1 on Cosmo X - Public Security Target, FQR 110 A1E4, Ed 2, 26 October 2023
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)