Certification Report

ID-One Cosmo X Platform

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-2300050-01-CR**
Report version:	**1**
Project number:	**NSCIB-2300050-01**
Author(s):	**Wouter Slegers**
Date:	**15 June 2023**
Number of pages:	**11**
Number of appendices:	**0**

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

CONTENTS

Foreword 3

Recognition of the Certificate 4

International recognition 4
European recognition 4

1 Executive Summary 5

2 Certification Results 6

2.1 Identification of Target of Evaluation 6
2.2 Security Policy 6
2.3 Assumptions and Clarification of Scope 7
2.3.1 Assumptions 7
2.3.2 Clarification of scope 7
2.4 Architectural Information 7
2.5 Documentation 8
2.6 IT Product Testing 8
2.6.1 Testing approach and depth 8
2.6.2 Independent penetration testing 8
2.6.3 Test configuration 8
2.6.4 Test results 8
2.7 Reused Evaluation Results 9
2.8 Evaluated Configuration 9
2.9 Evaluation Results 9
2.10 Comments/Recommendations 9

3 Security Target 10

4 Definitions 10

5 Bibliography 11

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 Cosmo X Platform. The developer of the ID-One Cosmo X Platform 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 is a dual interface, contact or pure contactless product with a Java Card platform, compatible with multi-application ID-One Cosmo product family. The TOE is the Java Card System (JCS) Open Platform of the ID-One Cosmo product. The product may also include applets, the TOE does not.include these applets.

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 X 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 is a composite of a documentary change and the SPM formal model on the underlying Java Card System previously certified as [JC-CERT].

The TOE has been evaluated by SGS Brightsight B.V. located in Delft. The evaluation was completed on 15 June 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 the ID-One Cosmo X Platform, 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 Cosmo X Platform 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 EAL6 augmented (EAL6+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.1 (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.

[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 Cosmo X Platform from IDEMIA located in Courbevoie, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier		Version
Hardware	Infineon Security Controller t 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
Software	ID-One Cosmo X Platform	R3 + patch	093363
			099E71
		R4 + 2 patches	093364
			099441
			099E21
		R6	093366

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

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.11.

2.2 *Security Policy*

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:

□ Card content loading;

□ Extradition;

□ Asymmetric keys;

□ DAP support, Mandated DAP support;

□ DAP calculation with asymmetric cryptography;

□ Logical channels;

□ SCP02 support;

□ SCP03 support;

□ Support for contact and contactless cards different implicit selection on different interfaces and channels;

□ Support for Supplementary Security Domains;

□ Trusted path privileges;

□ Post-issuance personalisation of Security Domain;

□ Application personalisation;

□ Crypto algorithms.

See *[ST]*, Chapter 1.8 for the details.

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 5.2 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.

This composite certification builds on the underlying [JC-Cert] by adding the formal methods ADV_SPM within a month of the [JC-Cert] issuance, hence the vulnerability analysis and testing of the underlying [JC-Cert] and its [JC-ETRfC] substantially describe the relevant vulnerability analysis and testing. Users of this certificate should include [JC-Cert] and [JC-ETRfC] into their composition activities.

2.4 Architectural Information

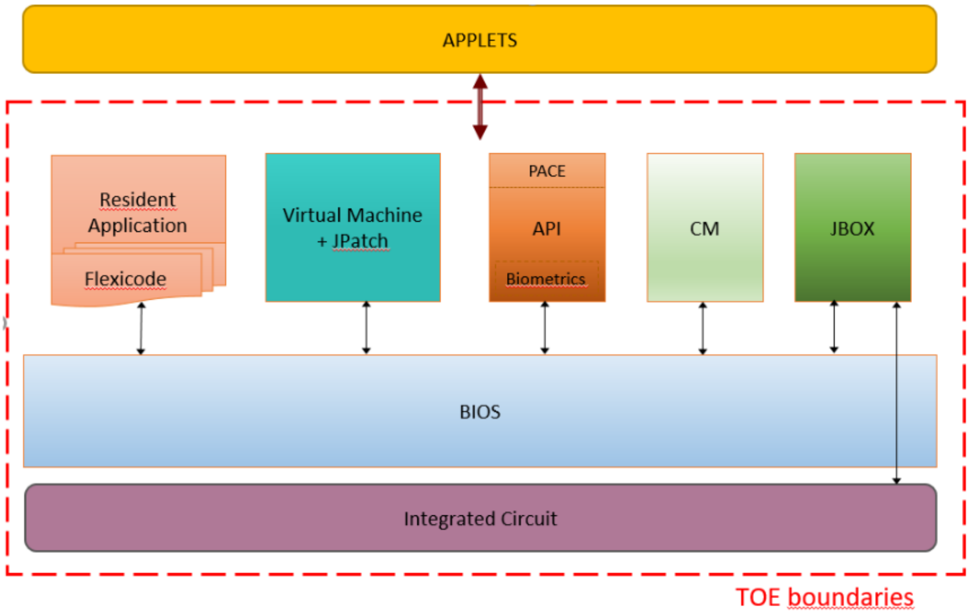
The TOE is a dual Java Card platform based, compatible with multi-application ID-One Cosmo product family.

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



2.5 Documentation

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

Identifier	Name	Version	Date
[AGD_SR]	ID-One Cosmo X Applet Security Recommendations, FQR 110 9572	Ed 7	21 March 2023
[AGD-OPE]	ID-One Cosmo X Reference Guide, FQR 110 9563	Ed 13	15 March 2023
[AGD_PAPI]	ID-One Cosmo X Javadoc, FQR 110 9616	Ed 4	17 January 2022
[AGD_BIO]	BIOMETRY ON ID-ONE COSMOX (SLC37), FQR 110 9598	Ed 2	02 February 2021
[GEN]	IDEMIA Platform Flash Image Generation, FQR 110 9402	Ed 1	27 November 2019
[JPATCH]	JCVM_PATCH, FQR 110 8805	Ed 4	23 December 2020
[JBOX]	JBox Software Configuration, FQR 110 9273	Ed 2	26 January 2021
[GPP]	GLOBAL PRIVACY FRAMEWORK, FQR 110 9567	Ed 3	25 November 2021
[AGD-PRE]	ID-One Cosmo X Pre-Perso Guide, FQR 110 9562	Ed 14	25 May 2023
[AGD-PRE-13][2]	ID-One Cosmo X Pre-Perso Guide, FQR 110 9562	Ed 13	15 March 2023
[AGD_ALP]	ID-One Cosmo X Application Loading Protection Guidance, FQR 110 9603	Ed 3	5 May 2021
[DEL]	ID-One Cosmo X Secure Acceptance Process, FQR 110 8921	Ed 1	24 September 2018
[CFCG]	ID-One Cosmo X Cryptographic French conformance Guidance, FQR 110 9745	Ed 7	21 March 2023

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

Testing of the TOE was performed in the underlying certification [JC-Cert]. The ADV_SPM activities did not lead to additional testing requirements.

2.6.2 Independent penetration testing

Penetration testing of the TOE was performed in the underlying certification [JC-Cert]. The ADV_SPM activities did not lead to additional testing requirements.

2.6.3 Test configuration

See [JC-Cert].

2.6.4 Test results

According to [JC-Cert], no exploitable vulnerabilities were found with the independent penetration tests.

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

[2] Note [AGD-PRE-13] is the version identified in the ANSSI certification (ANSSI-CC-2023/06). The only difference between[AGD-PRE] and [AGD-PRE-13] is a single update in Table 48, which does not impact any of the TOE's security functions. Therefore, the verdict of this evaluation and certification is valid for both versions of the guidance.

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 8 site certificates and 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-One Cosmo X Platform. See the [ST] and guidance for how to verify the TOE and its version.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents. 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 above evaluation results the evaluation lab concluded the ID-One Cosmo X Platform, to be **CC Part 2 extended, CC Part 3 conformant** and to meet the requirements of **EAL 6 augmented with 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 Profile *[PP_0099]*.

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 Idemia, Security Target ID-ONE COSMO X, FQR 110 9792, Ed 5, 02/06/2023 *[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:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

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

[ASE] ID-One Cosmo X Platform – Intermediate Report ASE EAL6+, 23-RPT-403, version 2.0, Dated 24 May 2023

[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

[ETR] Evaluation Technical Report ID-One Cosmo X v4.0" – EAL6+, 24-RPT-407, version 4.0, dated 13 June 2023

[ETRfC] Evaluation Technical Report for Composition ID-One Cosmo X v2.0" – EAL6+, 24-RPT-664, version 2.0, dated 13 June 2023

[JC-CERT] ANSSI, Rapport de certification ANSSI-CC-2023/06 ID-One Cosmo X (Codes SAAAAR: 093363 + patch 099E71, 093364 + patch 099441 et 099E21, 093366)

[JC-ETRfC] Evaluation Technical Report (ETR for composition) – HERA, LESTI.CESTI.HER.COMPO.001 – V1.4, 19/04/2023

[JIL-AAPS] JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020

[JIL-AAPHD] Application of Attack Potential to Hardware Devices with Security Boxes, Version 3.0, July 2020

[JIL-AM] 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

[PP_0099] Java Card System – Open Configuration Protection Profile, Version 3.0.5 December 2017, BSI-CC-PP-0099-2017

[ST] Idemia, Security Target ID-ONE COSMO X, FQR 110 9792, Ed 5, 02/06/2023

[ST-lite] Idemia, Public Security Target ID-One Cosmo X –EAL6+, FQR 110 A23D, Ed 1, 02/06/2023

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)