Certification Report

TnD v5.1 on ID-One Cosmo X (BAC Configuration)

Sponsor and developer:	***IDEMIA*** **2 place Samuel de Champlain** **92400 Courbevoie** **France**
Evaluation facility:	***Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0362718-CR**
Report version:	**2**
Project number:	**0362718**
Author(s):	**Andy Brown**
Date:	**04 October 2021**
Number of pages:	**13**
Number of appendices:	**0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

Foreword **3**

Recognition of the Certificate **4**

International recognition 4
European recognition 4

1 Executive Summary **5**

2 Certification Results **7**

2.1 Identification of Target of Evaluation 7
2.2 Security Policy 7
2.3 Assumptions and Clarification of Scope 7
2.3.1 Assumptions 7
2.3.2 Clarification of scope 8
2.4 Architectural Information 8
2.5 Documentation 9
2.6 IT Product Testing 9
2.6.1 Testing approach and depth 9
2.6.2 Independent penetration testing 9
2.6.3 Test configuration 10
2.6.4 Test results 10
2.7 Reused Evaluation Results 10
2.8 Evaluated Configuration 10
2.9 Evaluation Results 10
2.10 Comments/Recommendations 10

3 Security Target **12**

4 Definitions **12**

5 Bibliography **13**

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, TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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, TÜV Rheinland Nederland 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

The 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 TnD v5.1 on ID-One Cosmo X (BAC Configuration). The developer of the TnD v5.1 on ID-One Cosmo X (BAC Configuration) 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 composite product that consist of an IDEMIA applet named TnD v5.1 and its supporting "Common" library package on top of the Cosmo X Global Platform Java Card 3.0.5 operating system and Infineon SLC37 contact/contactless smart card security controller in **BAC configuration**.

The TOE supports the ICAO and TR-3110-1 and -3 defined protocols for Basic Access Control (BAC), Chip Authentication v1 (CAv1) and Active Authentication (AA). In addition, the TOE supports Chip Authentication v1 with AES secure messaging.

For compliancy with the protection profiles claimed in this security target, the BAC protocol MUST be configured on the TOE for each configured ID document application mentioned below.

Within the scope of the Security Target *[ST]*, TOE can be configured as a stand-alone application or as a combination of the following official ID document applications:

- ICAO/EAC eMRTD and
- EU/ISO Driving Licence compliant to ISO/IEC 18013 or ISO/IEC TR 19446.

The TOE may be used as an ISO Driving Licence (IDL) compliant to ISO/IEC 18013 or ISO/IEC TR 19446, as both eMRTD and IDL applications share the same protocols and data structure organization.

The TnD v5.1 application embeds other secure functionalities, like PACE (Generic Mapping (GM), Integrated Mapping (IM) and Chip Authentication Mapping (CAM)), Terminal Authentication v1 (TAv1), LDS2 protocol extensions for EAC1, Polymorphic Authentication protocol (PMA) for privacy-protected authentication with polymorphic ID attributes and Digital Bluring of Images (DBI), which are not in the scope of this evaluation, but are covered in the scope of other evaluated configurations of this product.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 26 August 2021 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]*. An administrative update was made to this CR and associated certificate on 04 October 2021

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the TnD v5.1 on ID-One Cosmo X (BAC Configuration), 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 TnD v5.1 on ID-One Cosmo X (BAC Configuration) 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 provides 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), ADV_FSP.5 (Complete semi-formal functional specification with additional error information), ADV_INT.2 (Well-structured internals), ADV_TDS.4 (Semiformal modular design), ALC_CMS.5 (Development tools CM coverage), ALC_TAT.2 (Compliance with implementation standards) and ATE_DPT.3 (Testing: modular design).

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).

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

TÜV Rheinland Nederland 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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the TnD v5.1 on ID-One Cosmo X (BAC Configuration) from IDEMIA located in Courbevoie, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Platform	ID-One Cosmo X	SAAAAR Code: 093363
Software	TnD applet (SAAAAR 203621FF)	v5.1 (00000208)
	Common Package (SAAAAR 417641FF)	v1.0 (01010008, Config 1) (01040007, Config 2)

To ensure secure usage a set of guidance documents is provided, together with the TnD v5.1 on ID-One Cosmo X (BAC Configuration). For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 4.

2.2 Security Policy

The TOE encompasses the following features:

- In Personalization phase:
  - Authentication protocol for personalization agent authentication;
  - 3DES, AES128, AES192 and AES256 Global Platform secure messaging;
  - Access control;
  - Creation and configuration of application instances and their logical data structure;
  - Secure data loading;
  - Secure import and/or on-chip generation of Chip Authentication key pair for CAv1;
  - Secure import and/or on-chip generation of the AA key pair;
  - Life-cycle phase switching to operational phase.
- In operational phase:
  - Chip Authentication v1 (CAv1);
  - Active Authentication (AA);
  - After CAv1: restart ICAO secure messaging in 3DES, AES128, AES192 or AES256 cipher mode.

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

Note that the ICAO MRTD infrastructure critically depends on the objectives for the environment to be met. These are not weaknesses of this particular TOE, but aspects of the ICAO MRTD infrastructure as a whole.

The environment in which the TOE is personalised must perform proper and safe personalisation according to the guidance and referred ICAO guidelines.

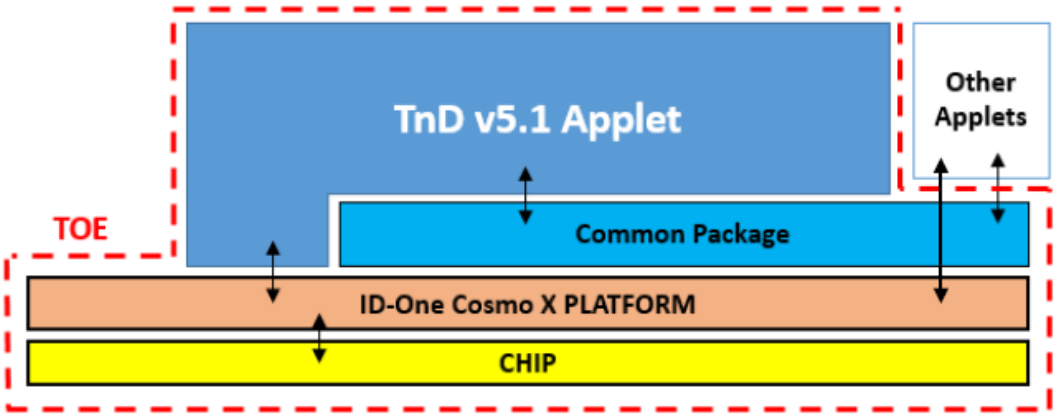
The environment in which the TOE is used must ensure that the inspection system protects the confidentiality and integrity of the data send and read from the TOE.

2.4 Architectural Information

From physical/hardware point of view, the TOE is a bare microchip with its external interfaces for communication. The physical medium on which the microchip is mounted is not part of the target of evaluation because it does not alter nor modify any security functions of the TOE.

The TOE may be used in several form factors, like wafer, chip modules on a reel, chip modules embedded in ID3 passport booklets or ID3 holder pages, chip modules embedded in ID1 cards, chip modules embedded in antenna inlays, etc.

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



Logical architecture of the TOE.

The Target of Evaluation (TOE), addressed by the security target, is an electronic travel document representing a contactless/contact based smart card or passport programmed according to Logical data structure (LDS). Electronic Passport is specified in *[ICAO-9303]*, additionally providing the Chip Authentication v1 and Active Authentication according to *[ICAO-9303]*. The TOE may also be used as an ISO driving license, compliant to ISO/IEC 18013 or ISO/IEC TR 19446.

The TOE supports:

- Basic Access Control (BAC) protocol,
- Chip Authentication v1 (CAv1) protocol with AES128, ASE192, AES256 extensions,
- Active Authentication (AA)

The “TnD v5.1 on Cosmo X” TOE consists of:

- The MRTD’s chip circuitry and the IC dedicated software;
- The IC embedded software being the “ID-One Cosmo X platform” consisting of:

  - Java Card virtual machine, ensuring language-level security;
  - Java Card runtime environment, providing additional security features for Java card technology enabled devices;
  - Java card API, providing access to card's resources for the Applet;
    Global Platform Card Manager, responsible for management of Applets on the card.
  - Crypto Library.
- TnD v5.1 Applet along with its Common (library) Package loaded in non-volatile (FLASH) memory.
- The associated guidance documentation in *[AGD_PRE]* and *[AGD_OPE]*;
- The Personalization Agent Key set (see *[AGD_PRE]*).

.

2.5 Documentation

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

Reference	Identifier	Version
[AGD_OPE]	TnD v5.1 on ID-One Cosmo X - Operational User Guidance (AGD_OPE)	FQR 220 1580 Ed 1
[AGD_PRE]	TnD v5.1 on ID-One Cosmo X - Preparative Procedures (AGD_PRE)	FQR 220 1579 Ed 3

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 tested the TOE using both a standardised accreditation test suite and a proprietary test suite for Common Criteria to ensure that all SFRs in the Security Target were tested. By performing an extensive requirements analysis and testing accordingly, the developer ensured that the required depth and coverage of testing was achieved.

For the testing performed by the evaluators, the sample of repeated developer tests was chosen to get a coverage of all the features while ensuring to cover all product configurations, i.e., including CA, AA, and BAC, as well as configurations where relevant platform functionality is not available. Additionally, this sample allowed the evaluator to observe different cryptographic algorithms including RSA, ECDSA, and ECDH. Finally, the sample included a range of different important (internal) applet security features, such as certificate chaining, the state machine, access control of the file system, slow down, verification failure, and certificate attribute checking, covering both the personalization as well as the operational phase. The repetition was performed through witnessing.

The developer test strategy already included a high depth of testing. The evaluator-defined tests focused on the verification of specific countermeasures and on passport traceability, in addition to a verification of the preparatory guidance.

2.6.2 Independent penetration testing

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considered 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 resulted in the identification of (additional) potential vulnerabilities. This analysis was performed according to the attack methods in *[JIL-AAPS].* An important source for assurance in this step was the technical report *[PF-ETRfC]* of the underlying platform.

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

For the BAC TOE, no penetration tests were defined. There is no exploitable potential vulnerability that is commensurate with the AVA_VAN.3 attack potential.

2.6.3 Test configuration

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

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.

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 has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 10 Site Technical Audit Reuse 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 TnD v5.1 on ID-One Cosmo X (BAC Configuration).

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Report(s) for the site(s) *[STAR]* [2].

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

Based on the above evaluation results the evaluation lab concluded the TnD v5.1 on ID-One Cosmo X (BAC Configuration), to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL4 augmented with ALC_DVS.2, ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.2 and ATE_DPT.3**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profile *[PP0055]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE.

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.

[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.

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.

3 Security Target

The Security Target TnD v5.1 on ID-One Cosmo X (BAC Configuration), FQR 550 0159, Ed 4, 11 August 2021 *[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:

AA	Active Authentication
BAC	Basic Access Control
CA	Chip Authentication
CAM	Chip Authentication Mapping
CAN	Card Access Number
DBI	Digital Blurring of Images
EAC	Extended Access Control
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
eMRTD	electronic MRTD
GM	Generic Mapping
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
IM	Integrated Mapping
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LDS	Logical Data Structure
MAC	Message Authentication Code
MRTD	Machine Readable Travel Document
NSCIB	Netherlands Scheme for Certification in the area of IT security
PACE	Password Authenticated Connection Establishment
PIN	Personal Identification Number
PP	Protection Profile
PUK	Personal Unblocking Key
TA	Terminal Authentication
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
[ETR]	Evaluation Technical Report “TnD v5.1 on ID-One Cosmo X” – EAL5+, 21-RPT-601, Version 5.0, 11 August 2021
[ICAO-9303]	International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – 7th edition, 2015
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 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 2.5, 28 March 2019
[PF-CERT]	Rapport de certification ANSSI-CC-2021/29, ID-One Cosmo X, (Code SAAAAR : 093363), 05 July 2021
[PF-ETRfC]	Evaluation Technical Report (ETR for composition) – ZEUS, v1.2, 01 June 2021
[PF-ST]	Security Target Lite ID-ONE Cosmo X, FQR 110 9730 Ed 3
[PP0055]	Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application”, Basic Access Control, BSI-CC-PP-0055-2009, Version 1.10, 25 March 2009
[ST]	Security Target TnD v5.1 on ID-One Cosmo X (BAC Configuration), FQR 550 0159, Ed 4, 11 August 2021
[ST-lite]	TnD v5.1 on ID-One Cosmo X (BAC Configuration), FQR 550 0245, Ed3, 11 August 2021
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)