Certification Report

TnD v5.1 on COSMO J in EAC with PACE 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-0237695-CR**

Report version: **1**

Project number: **0237695**

Author(s): **Andy Brown**

Date: **22 April 2021**

Number of pages: **13**

Number of appendices: **0**

Headoffice:
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 Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

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, 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 license 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, in order 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 and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the TnD v5.1 on COSMO J in EAC with PACE Configuration**.** The developer of the TnD v5.1 on COSMO J in EAC with PACE 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 TnD v5.1 on COSMO J is a composite product that consist of an IDEMIA applet named TnD v5.1 and its supporting library packages on top of the NXP JCOP 4 P71 contact/contactless chip platform.

The TnD v5.1 on COSMO J supports the ICAO and TR-3110-1 and -3 defined protocols for EAC1 (Chip Authentication v1 and Terminal Authentication v1), PACE (Generic Mapping, Integrated Mapping and Chip Authentication Mapping), Active Authentication (AA) and LDS2 protocol extensions for EAC1 and PACE. In addition, the TnD v5.1 on COSMO J product supports Polymorphic Authentication protocol (PMA) for privacy-protected authentication with polymorphic ID attributes.

The TnD v5.1 on COSMO J can be configured as a stand-alone application or as a combination of the following official ID document applications:

- ICAO/EAC eMRTD, including LDS2 Travel records (stamps), Visa records and Additional biometrics in accordance with ICAO *[ICAO-9303]* and *[LDS2_TR]* specifications,
- Polymorphic eMRTD according to Dutch national specification and
- EU/ISO Driving Licence compliant to ISO/IEC 18013 or ISO/IEC TR 19446.

The Polymorphic eMRTD application is in compliance with the Polymorphic eMRTD Specification of the Dutch National Office of Identity Data (written by IDEMIA). This ensures authentication to an authentication service at eIDAS High assurance level, without revealing privacy sensitive ID attributes the authentication service provider. This is accomplished by the TnD v5.1 on COSMO J's Polymorphic Authentication (PMA) protocol, which randomizes Polymorphic Pseudonym, Identity and Complementary ID attributes.

Different configurations of the TnD v5.1 on COSMO J product have been subject to separate evaluations. All functions mentioned above are in the scope of the certification of the TOE **TnD V5.1 on COSMO J in EAC with PACE Configuration** (PACE/EAC1/Polymorphic eMRTD/LDS2 configuration) considered in this Certification Report.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 22 April 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]*.

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 COSMO J in EAC with PACE 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 COSMO J in EAC with PACE 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 EAL5: augmented (EAL5+) 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 and *[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. It should be noted that the certification results only apply 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 COSMO J in EAC with PACE Configuration from IDEMIA located in Courbevoie, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2)	B1
Software	NXP JCOP 4 on P71	v4.7 R1.01.4
	TnD applet (SAAAAR 203461FF)	v5.1 (00000201)
	Common Package (SAAAAR 417641FF)	v1.0 (01010209)
	Adapter Package (SAAAAR 417651FF)	v1.0 (00000107)

In order to ensure secure usage of the TOE, a set of guidance documents is provided. Details can be found in section 2.5 of this report.

The secure identification of the TOE has been specified in the COSMO J TnD V5.1 Preparative Procedures (AGD_PRE), FQR 220 1495 of the TOE.

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

2.2 Security Policy

The TOE in the PACE/EAC1/Polymorphic/LDS2 configuration encompasses the following features:

- In Personalisation phase:
  - authentication protocol;
  - 3DES, AES128, AES192 and AES256 Global Platform secure messaging;
  - access control;
  - initialisation of the LDS;
  - data loading;
  - life-cycle phase switching to operational phase;
  - Secure import and/or on-chip generation of Chip Authentication key pairs for CAv1 and PACE-CAM;
  - Secure import and/or on-chip generation the AA key pair;
- In operational phase:
  - PACE mapping types Generic Mapping (GM), Integrated Mapping (IM) and Chip Authentication Mapping (CAM)*
    Note*: The availability of PACE-CAM depends on the TOE configuration;
  - PACE passwords: MRZ, CAN, PIN and PUK;
  - PIN verify and reset;
  - EAC1: Chip Authentication v1 (CAv1) and Terminal Authentication v1 (TAv1);
  - Active Authentication (AA);
  - After CAv1: restart ICAO secure messaging in 3DES, AES128, AES192 or AES256 cipher mode;
  - After PACE start ICAO secure messaging in 3DES, AES128, AES192 or AES256 cipher mode;
  - After EAC1: access control to DG3 and DG4 based on the effective authorization established during TAv1;
  - After EAC1: Polymorphic Authentication;

- LDS2 protocol extensions for PACE, TAv1 and CAv1 and EAC1 access control to LDS2 applications (Travel records, Visa records and Additional Biometrics);
- Automatic BAC phasing out;
- Digital Blurring of Images (DBI).

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in 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 personalized must perform proper and safe personalization 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.

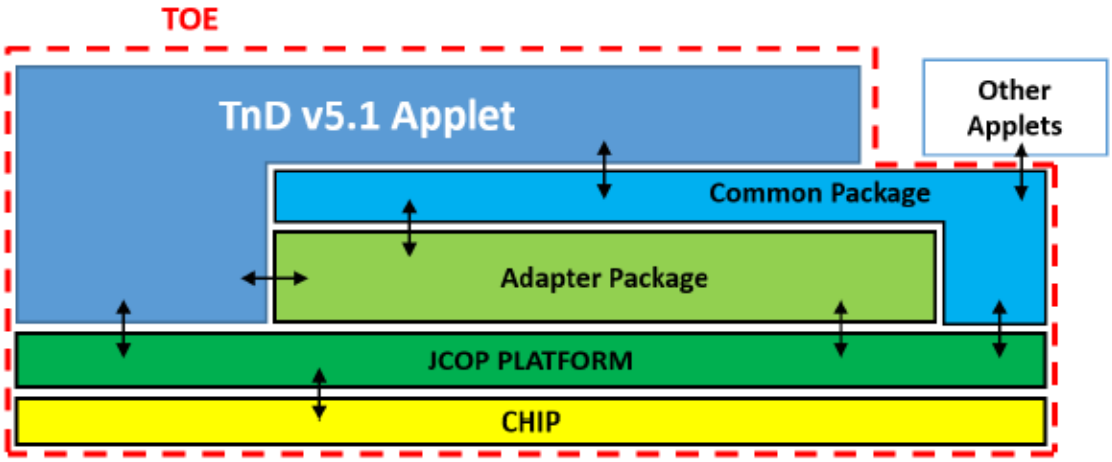
2.4 Architectural Information

The TOE is a composite product that consist of an IDEMIA applet named TnD v5.1 and its supporting “Common” and “Adapter” packages on top of the NXP JCOP 4 P71 contact and/or contactless chip Platform.

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 on several form factors (like Chip module, Chip modules on a reel, Chip modules embedded in ID3 passport booklets, Chip modules embedded in ID1 cards or ID3 holder pages, Chip modules embedded in antenna inlays, Passport booklet).

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



Logical architecture of the TOE

The TOE 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 Extended Access Control according to *[TR- 03110-1]* and *[TR-03110-3]* 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 communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE), optionally with Chip Authentication Mapping (PACE CAM).

The TOE may also be used as an ISO driving license, compliant to ISO/IEC 18013 or ISO/IEC TR 19446.

Polymorphic eMRTD extensions are present on the TOE that enable secure authentication with enhanced privacy protection features. It provides the holder the possibility to authenticate towards a service provider in a non-traceable and non-linkable manner thanks to usage of Polymorphic Pseudonyms and other Polymorphic ID attributes.

The ICAO LDS2 protocol and Logical Data Structure extensions are available in the TOE for supporting secure access and storage Electronic visas, electronic travel stamps or additional biometrics like fingerprint or an iris scan.

2.5 Documentation

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

Identifier	Version
COSMO J TnD V5.1 Preparative Procedures (AGD_PRE), FQR 220 1495	Ed 10
COSMO J TnD V5.1 Operational User Ed5 Guidance (AGD_OPE), FQR 220 1496	Ed 5
JCOP 4 P71 User manual for JCOP 4 P71, DocNo 469537	Rev. 3.7

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 has performed extensive testing on functional specification, subsystem and SFR-enforcing module level. The developer has tested the TOE both using a standardised accreditation test suite and a proprietary test suite for CC to ensure that all SFRs in the Security Target are tested. By performing an extensive requirements analysis and testing accordingly, the developer ensured that the required depth and coverage of testing is 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 PACE (-CAM), CA, TA, AA, DBI, BAC, PIN, PMA and LDS2. 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 of developer testing.

The developer test strategy already included a high depth of testing. The evaluator-defined tests focussed 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

The methodical analysis performed was conducted along the following steps:

- 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.

The results of the TOE penetration tests that were defined are presented below. The penetration testing comprised one week, 100% of which consisted of perturbation attacks.

2.6.3 Test Configuration

The configuration of the sample was the same as described in the ST.

2.6.4 Testing 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.

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).

2.7 Re-used evaluation results

There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE, by use of 10 Site Technical Audit Re-use report approaches.

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 COSMO J in EAC with PACE Configuration.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Reports for the sites *[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 COSMO J in EAC with PACE Configuration, to be **CC Part 2 extended, CC Part 3 conformant** and to meet the requirements of **EAL 5 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 *[PP0056]* and *[PP0068]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 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 need to 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. In order for the evolution of attack methods and techniques to be covered, he 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 for satisfying the AVA_VAN.5 "high attack potential". In order 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).

[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 Security Target

The Security Target TnD v5.1 on JCOP (EACwithPACE Polymorphic LDSv2), FQR 220 1510, Ed 9, 19 March 2021 *[ST]* is included here by reference.

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

4 Definitions

This list of Acronyms and the glossary of terms 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 COSMO J" – EAL5+, 20-RPT-1030, Version 9.0, 16 April 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).

[LDS2_TR] TECHNICAL REPORT LDS2 – Protocols, Version 0.8, 27 April 2017.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[PF-CERT] Certification Report JCOP 4 P71, NSCIB-CC-180212-CR3, v1, 01 March 2021.

[PF-ETRfC] Evaluation Technical Report for Composition NXP "JCOP 4 P71" – EAL6+, 19-RPT-177, v8.0, 25 February 2021.

[PF-ST] JCOP 4 P71, Security Target Lite, Rev. 4.1, 12 February 2021.

[PP0056] Protection Profile Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE (EAC PP), registered under the reference BSI-CC-PP-0056-V2-2012, Version 1.3.2, 05 December 2012.

[PP0068] Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE, registered under the reference BSI-CC-PP-0068-V2-MA-01, Version 1.0.1, 22 July 2014.

[ST-lite] TnD v5.1 on JCOP (EACwithPACE Polymorphic LDSv2) – Public Security Target, FQR 550 0184, Ed 1, 19 March 2021.

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

[ST] Security Target TnD v5.1 on JCOP (EACwithPACE Polymorphic LDSv2), FQR 220 1510, Ed 9, 19 March 2021.

[TR- 03110-1] Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20 March 2012.

[TR-03110-3] TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3: Common Specifications, version 2.10, 07 March 2012.

(This is the end of this report).