Certification Report

TnD v5.1 on ID-One Cosmo J V2 (EAC Configuration)

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** **The Netherlands**
Report number:	**NSCIB-CC-0237694-CR2**
Report version:	**1**
Project number:	**0237694_2**
Author(s):	**Andy Brown**
Date:	**07 December 2022**
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

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.

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 J V2 (EAC Configuration). The developer of the TnD v5.1 on ID-One Cosmo J V2 (EAC 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 consists of an IDEMIA applet named TnD v5.1 and its supporting "Common" library package and Adapter package on top of the NXP JCOP 4 P71 Platform in **EAC configuration.**

The TnD v5.1 applet on ID-One Cosmo J V2 has support for the *[ICAO-9303]* and *[TR-3110-1]* and *[TR-3110-3]* defined protocols for EAC1 (Chip Authentication v1 and Terminal Authentication v1), PACE (Generic Mapping (GM), Integrated Mapping (IM) and Chip Authentication Mapping (CAM)), Active Authentication (AA) and LDS2 protocol extensions for EAC1 and PACE. In addition, the TOE supports Polymorphic Authentication protocol (PMA) for privacy-protected authentication with polymorphic ID attributes.

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

Within the scope of the TOE's *[ST]* the TnD v5.1 applet on ID-One Cosmo J V2 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 TnD v5.1 applet on ID-One Cosmo J V2 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.

Different configurations of the TnD v5.1 applet on ID-One Cosmo J V2 have been subject to separate evaluations. All functions mentioned above are in the scope of the certification of this TOE. This Certification Report states the outcome of the Common Criteria security evaluation of the **TnD v5.1 on ID-One Cosmo J V2 (EAC Configuration).**

The TOE was evaluated initially by SGS Brightsight B.V. located in Delft and was certified on 22 April 2021. The re-evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 07 December 2022 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This second issue of the Certification Report is a result of a "recertification with major changes".

The major changes were an update of the underlying platform (leading to an updated TOE reference) and an update of the TOE ST and guidance documents.

The security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made.

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 J V2 (EAC 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 J V2 (EAC 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 provide sufficient evidence that the TOE meets the EAL5: augmented (EAL5+) assurance requirements for the

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

evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

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

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 J V2 (EAC Configuration) from IDEMIA located in Courbevoie, France.

The TOE is comprised of the following main components together with the configuration identified as specified in [ST] section 1.2:

Delivery item type	Identifier	Version
Hardware	NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4)	B1
Software	NXP JCOP4 on P71	v4.7 R1.02.4
	TnD applet (SAAAAR 203462FF)	05 01 00 00 (00 00 02 08)*
	Common Package (SAAAAR 418402FF)	01 00 00 00 (01 01 02 0C)*
	Adapter Package (SAAAAR 417652FF)	01 01 00 00 (00 00 01 08)*

*Applet GET DATA (DF67) response

To ensure secure usage a set of guidance documents is provided, together with the TnD v5.1 on ID-One Cosmo J V2 (EAC Configuration). 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 in the PACE/EAC1/Polymorphic/LDS2 configuration 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:
  - 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 EAC1: access control to DG3 and DG4 based on the effective authorization established during TAv1;
  - 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. 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.

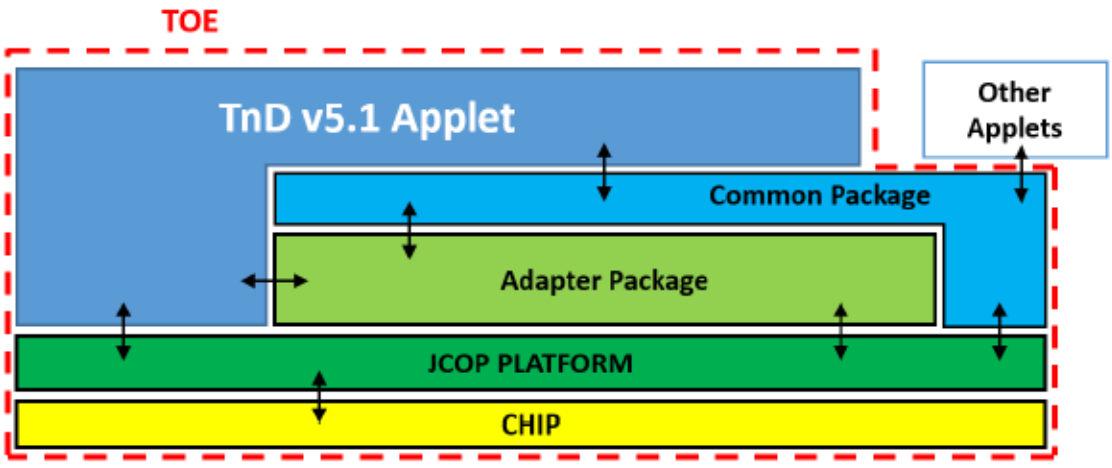
2.4 Architectural Information

The TOE is a configuration of a composition that consists 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 physical part of 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:



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 Extended Access Control.

2.5 Documentation

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

Identifier	Version
TnD v5.1 on ID-One Cosmo J - Preparative Procedures (AGD_PRE), FQR 220 1495	Ed 13
TnD v5.1 on ID-One Cosmo J - Operational User Guidance (AGD_OPE), FQR 220 1496	Ed 7
JCOP 4 P71 User Manual for JCOP 4 P71	Rev. 4.2

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer 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 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, TA, AA, DBI anid BAC. 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 focused on the verification of specific countermeasures and on passport traceability in addition to a verification of the preparatory guidance.

During the re-certification, no additional repeated developer tests, nor independent developer tests, were executed by the evaluator. It was determined that the only change to the TOE implementation was in the underlying Crypto Library which was determined not to impact the functional test results of the TOE.

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.

In the baseline evaluation, penetration testing comprised one week, 100% of which consisted of perturbation attacks.

In this first re-certification it was determined that the changes did not modify the results of vulnerability analysis and that all previous test results remain valid and relevant. The evaluation justified this through analysis of the latest updates of security requirements documents, any advances in state of the art attack techniques and any new attack methods applicate to the TOE.

2.6.3 Test configuration

In the baseline evaluation there was some testing on an earlier version of the TOE. The final version of the TOE as described in the [ST] was analysed to confirm that the test results remained valid for these test. All other testing was on configurations of the samples as described in the ST

In this first re-certification, samples were not required since, as described in section 2.6.1 and 2.6.2, no repeated developer testing nor independent testing was required as a result of the updated vulnerability analysis.

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.

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 Reused Evaluation Results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and any resultant need for penetration testing has been renewed. For this first re-certification it has been determined from the analysis that no further penetration testing was required.

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 11 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 TnD v5.1 on ID-One Cosmo J V2 (EAC Configuration) together with the configuration identified as specified in *[ST]* section 1.2.

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 J V2 (EAC 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]*.

[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 Security Target claims 'strict' conformance to the Protection Profile *[PP_0056]*.

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 Security Target TnD v5.1 on ID-One Cosmo J V2 (EAC configuration), FQR 220 1509, Ed 11, 16 September 2022 *[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
DBI	Digital Blurring of Images
EAC	Extended Access Control
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
eMRTD	electronic MRTD
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
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
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.

[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 12.0, 06 December 2022
[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-CR5, v1
[PF-ETRfC]	Evaluation Technical Report for Composition NXP “JCOP 4 P71” – EAL6+, 19-RPT-177, v14.0, 14 September 2022
[PF-ST]	JCOP 4 P71, Security Target Lite, Rev. 4.8, 08 August 2022
[PP_0056]	Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control, Version 1.10, 25 March 2009, registered under the reference BSI-CC-PP-0056-2009
[ST]	Security Target TnD v5.1 on ID-One Cosmo J V2 (EAC configuration), FQR 220 1509, Ed 11, 16 September 2022
[ST-lite]	TnD v5.1 on ID-One Cosmo J V2 (EAC Configuration) Public Security Target, FQR 550 0183, Ed 4, 21 November 2022
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006
[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-03110-2]	Technical Guideline TR-03110-2, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 2 – Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE),and Restricted Identification (RI), 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.)