TÜV Rheinland Nederland B.V.

TÜVRheinland®
Precisely Right.

Certification Report

CombICAO Applet in SSCD configuration on Cosmo V9

Sponsor and developer:	*IDEMIA* **2 Place Samuel de Champlain, 92400 Courbevoie, France**
Evaluation facility:	*Brightsight* **Brassersplein 2 2612 CT Delft The Netherlands**
Report number:	**NSCIB-CC-200735-CR**
Report version:	**1**
Project number:	**200735**
Author(s):	**Denise Cater**
Date:	**07 January 2020**
Number of pages:	**15**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**CC-20-200735**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer

IDEMIA

2 Place Samuel de Champlain, 92400 Courbevoie, France

Product and assurance level

CombICAO Applet in SSCD configuration on Cosmo V9

Assurance Package:
- EAL5 ALC_DVS.2 and AVA_VAN.5

Protection Profile Conformance:
- Protection profiles for secure signature creation device — Part 2: Device with key generation, registered under the reference BSI-CC-PP-0059-2009-MA-01, Version 2.0.1 – 23/01/2012
- Protection profiles for secure signature creation device — Part 3: Device with key import, registered under the reference BSI-CC-PP-0075, Version 1.0.2 – 24/07/2012
- Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application, registered under the reference BSI-CC-PP-0071, Version 1.0.1 – 14/11/12

Project number **200735**

Evaluation facility **Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

The Designated Body from The Netherlands under Article 30(2) and 39(2) of Regulation 910/2014 declares that:
- The IT product identified in this certificate is a Qualified Signature/Seal Creation Device (QSCD) where data is held in an entirely but not necessarily exclusively user managed environment.
- The IT product meets the requirements laid down in Annex II of Regulation (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014.
- Conformity of the IT product with the above mentioned requirements has been certified with an evaluation process that fulfils the requirements of Article 30(3.(a)) and the standards listed in the Annex of COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL7

Validity

Date of 1st issue   : **07-01-2020**

Certificate expiry : **07-01-2025**

PRODUCTS
RvA C 078
Accredited by the Dutch
Council for Accreditation

TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

TÜVRheinland®
Precisely Right.

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.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TÜVRheinland®
Precisely Right.

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.

eIDAS-Regulation

TÜV Rheinland Nederland B.V., operating the Netherlands Scheme for Certification in the Area of IT Security (NSCIB), has been notified as a Designated Certification Body from The Netherlands under Article 30(2) and 39(2) of Regulation 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 *[EU-REG]*.

1   Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the CombICAO Applet in SSCD configuration on Cosmo V9. The developer of the CombICAO Applet in SSCD configuration on Cosmo V9 is IDEMIA located in Courbevoie, France and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE consists of a CombICAO Applet composed with the certified underlying IDEMIA Java Card Cosmo V9 platform. The CombICAO Applet is a configurable applet designed primarily for identification, authentication, signature and seal generation, and as a machine readable travel document (MRTD). This TOE relates only to the Qualified Signature Creation Device or Qualified Seal Creation Device (QSCD) configuration of the CombICAO Applet, used to create advanced or qualified signature in the sense of *[EU-REG]*.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 12 December 2019 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 CombICAO Applet in SSCD configuration on Cosmo V9, 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 CombICAO Applet in SSCD configuration on Cosmo V9 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), 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]* and the Dutch Conformity Assessment Process *[DCAP]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]*.

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.

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 meets the requirements laid down in Annex II of Regulation (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014. The product meets the requirements defined in *[EU-REG]* article 29 and article 39 and thus is a QSCD in the sense of *[EU-REG]*. It will be listed on the NSCIB Certified Products list and will be notified to the European Commission (eIDAS). It should be noted that the certification results only apply 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 releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the CombICAO Applet in SSCD configuration on Cosmo V9 from IDEMIA located in Courbevoie, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SLC32GDL400G3 SLC32GDA400G3 SLC32GDA348G3 SLC32GDL348G3	IFX_CCI_000005
	SLC32PDL400	IFX_CCI_000008 IFX_CCI_000014
	Software Library - HSL	V01.22.4346-SLCx2_C65.lib
	Software Library - MCS (Mifare lib)	V02.03.3446
	Java Card Platform - ID-ONE COSMO V9 ESSENTIAL	SAAAAR 089233
Software	CombICAO applet	SAAAAR 203297

To ensure secure usage a set of guidance documents is provided together with the CombICAO Applet in SSCD configuration on Cosmo V9. Details can be found in section "Documentation" of this report.

2.2 Security Policy

The TOE is delivered during the preparation phase after which the pre-personalisation and personalisation are performed.

The Pre-personalisation consists of:

- Authentication and secure channel using the in the certified platform implemented GP functionality using SCP02 and SCP03,
- Initialization of the TOE,
- Loading Personalization Agent keys in encrypted form,
- Storing the Initialization and Pre-Personalization data in audit records.

The Personalisation consists of:

- Authentication protocol, using the in the certified platform GP functionality for SCP02 and SCP03,
- Access control configuration,
- Encryption mechanism involved in key loading,
- Signature key import in personalization phase,
- Signature key generation in personalization phase and use phase,
- Signature key public key export in personalization phase and use phase,
- Initialization of the data structure,
- Data loading,
- Phase switching.

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 6.2 of the *[ST]*.

2.3.2   Clarification of scope

The TOE relies on the terminal operator (entity on the operational environment of the TOE) to verify that the document presenter is the legitimate holder of the TOE. This reliance on the operational environment is reflected in the usage of the terminal specified by OE.Terminal in *[ST]* section 6.2.9.9. This is further described in section 5.5 (page 45) of the guidance document "FQR 220 1307 - CombICAO Applet – AGD_OPE", which describes that the terminal operator shall determine that the document presenter is the legitimate holder of the TOE before allowing to update the PUK at the authentication terminal (TA_PMT).

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 consists of an applet and the certified Java Card platform (Cosmo v9 Essential) that can be configured to be used as an eMRTD and/or SSCD as specified in *[ST]*. The logical architecture of the TOE can be depicted as follows:
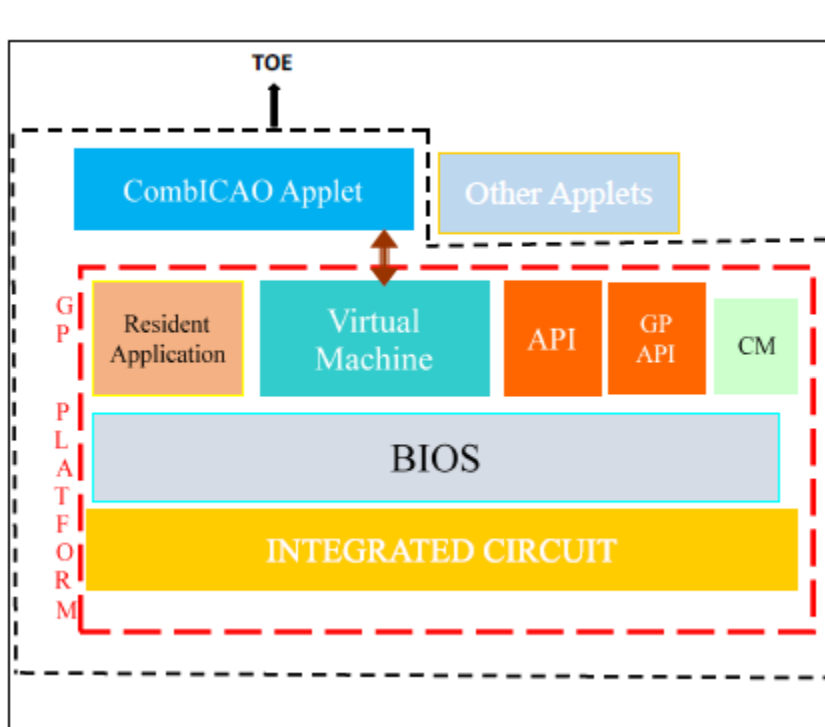
Within the framework described by [PP 419211-2], [PP 419211-3], and [PP 419211-4], the TOE allows to:

- Perform basic, advanced and qualified signature or seal generation;
- Authenticate the signatory thanks to PIN verification;
- Authenticate one (or several) administrator(s) of the TOE, that may have special rights to administrate the SCD (generation, import); and SVD generation, export for certificate generation). This administrator is the personalization agent during phase 6 and the document holder being authenticated at the terminal with TA_CMT being authenticated as R.Admin during phase 7;
- Prove the identity as QSCD to external entities, optionally, receive and store certificate info.
- Establish trusted channel, protected in integrity, authenticity and confidentiality, with trusted IT entities such as a CGA;
- Secure execution of services:
  - Signature key generation (SCD) in use phase;
  - Signature key public key (SVD) export in use phase;

The scope of [PP 419211-2], [PP 419211-3], and [PP 419211-4] is extended in several ways:

- All authentication protocols (PACE) and secure messaging type (DES-128, AES128/192/256);
- Extended Access Control Version 1 as defined in [TR-03110]. It consists of two parts: Chip Authentication Protocol Version 1 and Terminal Authentication Protocol Version 1. Including the certificate management;
- All PIN management operations available after delivery point (spanning the three types of PIN: PINAuth, PINSig (called also RAD) & PUK):
  - PIN initialization;
  - Upgrade of PIN attributes;
  - PIN change, unlocking, (re-)initialization;

The Personalization and Operational phases are summarised in "Security Policy" section above.

After authentication, the TOE allows the following three operations:

1. Digital authentication
   The TOE supports digital authentication based on RSA and elliptic curves cryptography (ECC). Digital authentication is the process by which (1) the holder of TOE authenticates itself to the TOE using a PIN, releasing access right to an authentication key stored in the TOE, (2) subsequently the authentication key is used by the TOE to authenticate itself on behalf of the TOE holder. Digital authentication is useful so that the TOE holder can authenticate himself on line, without compromising any sensitive assets (PINs or authentication key).
2. Digital signature or seal
   This feature enables the signatory to electronically sign or seal documents. The signature or seal may be either advanced or qualified (compliant with [PP 419211-2] and [PP 419211-3]).
3. Encryption key decipherment
   This feature enables the document holder to store secret data on an electronic vault. The key needed to decipher the key encrypting these data is securely stored in the TOE. The document holder's computer sends the encrypted encryption key to the TOE to get the plain encryption key.

2.5 Documentation

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

Identifier	Version
FQR 220 1306 - CombICAO Applet – AGD_PRE	Ed 8
FQR 220 1307 - CombICAO Applet – AGD_OPE	Ed 9
Secure acceptance and delivery of sensitive element - FQR 110 8921	Ed 1
ID One Cosmo V9.0 Essential Reference Guide, FQR 110 8823	Ed 5
ID One Cosmo V9.0 Essential - Pre-Perso Guide, FQR 110 8797	Ed 5
ID-One Cosmo V9 Application Loading Protection Guidance, FQR: 110 8798	Ed 2

ID-One Cosmo V9 Applet Security Recommendations, FQR: 110 8794	Ed 4

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 exhaustive testing on functional specification, subsystem and SFR-enforcing module level. The testing was largely automated using industry standard and proprietary test suites. Test scripts were extensively used to verify that the functions return the expected values. The Developer used a combination of test tools to test the TOE, including use of a commercial test bench from Keolabs/Scriptis, to test the operational behaviour of the TOE according to the [TR_03110] and [ICAO-9303] conformity test specifications. These conformity tests cover all eMRTD configurations of the TOE.

As the testing was automated the evaluator selected a small sample of tests to verify the correctness of the developer testing. All test results were as expected. Because no gaps could be identified in the developer testing evidence the evaluator devised a set of eight (8) tests aiming to verify a part of the preparatory guidance and the access conditions.

For the independent functional testing performed by the evaluators, the developer provided samples and a test environment.

2.6.2 Independent Penetration Testing

The vulnerability analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD potential vulnerabilities were identified from generating questions to the type of TOE and the specified behaviour.
- For ADV_IMP a thorough implementation representation review was performed on the TOE. During this attack oriented analysis the protection against the attack scenarios 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 list in [JIL-AM]. An important source for assurance against attacks in this step is the [HW_ETRfc] of the underlying platform; no additional potential vulnerabilities were concluded from this.
- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. Several potential vulnerabilities were found to be not exploitable due to an impractical attack path for the TOE in its evaluated configuration.

2.6.3 Test Configuration

The following test benches were used for witness of developer testing:

- Oberthur Testing Framework v 1.7.2.1 (Including Python)
- Keolabs eMRTD Applicative Test Suite v 06.00 - Accreditation testing

The TOE was tested in the following configurations:

- T1; {for T=1, T=CL, and Dual executions; SCP0300 Configuration}
- T0; {for T=0 executions; SCP0300 Configuration }
- T1;USE_SCP02; {for T=1, T=CL, and Dual executions; SCP0255 Configuration }
- T0;USE_SCP02; {for T=0 executions; SCP0255 Configuration }

For the listed configurations the TOE is in Pre-personalization stage. The TOE is configured and personalized for each test of the Oberthur testing framework.

For the KEOLABS test suite, all tests are performed in the operational life-cycle state, and do not allow TOE identification. These samples are personalised according to the ePassport profiles mentioned in the ATE.

For evaluator independent testing, the TOE was tested in the following configuration:

- Configuration 3: SSCD

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 vulnerability analysis.

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   Evaluated Configuration

The TOE is defined uniquely by its name and version number CombICAO Applet in SSCD configuration on Cosmo V9.

2.8   Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] and which references an ASE Intermediate Report and other evaluator documents.

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

Based on the above evaluation results the evaluation lab concluded the CombICAO Applet in SSCD configuration on Cosmo V9, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 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 Profiles *[PP 419211-2]*, *[PP 419211-3]* and *[PP 419211-4]*.

2.9   Comments/Recommendations

The user guidance as outlined in section 2.5 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 with respect to 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 need to be fulfilled by the operational environment of the TOE. In particular that TOE relies on the terminal operator (entity on the operational environment of the TOE) to verify that the document presenter is the legitimate holder of the TOE before allowing to update the PUK at the authentication terminal.

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.

3 Security Target

The CombICAO Applet in SSCD configuration on Cosmo v9 – Security Target, FQR 110 8784 version 8.0 *[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:

CA	Chip Authentication
CGA	Certificate Generation Application
DCAP	Dutch Conformity Assessment Process
EAC	Extended Access Control
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MRTD	Machine Readable Travel Document
NSCIB	Netherlands Scheme for Certification in the area of IT security
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
PUK	PIN Unblocking Key
QSCD	Qualified Signature/Seal Creation Device
SCD	Signature Creation Device
SVD	Signature Verification Device
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.
[CR-419211-2]	Certification Report for Protection profiles for secure signature creation device — Part 2: Device with key Generation, CEN/TC 224, BSI-CC-PP-0059-2009-MA-02, Version 2.0.1, 30 June 2016.
[CR-419211-3]	Certification Report for Protection profiles for secure signature creation device – Part3: Device with key import, CEN/TC 224, BSI-CC-PP-0075-2012-MA-01, Version 1.0.2, 30 June 2016.
[CR-419211-4]	Certification Report for Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application, version 1.0.1, CEN/TC 224, BSI-CC-PP-0071-2012-MA-01, 30 June 2016
[DCAP]	Dutch Conformity Assessment Process v3.0, dated 28-02-2019
[EU-REG]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014
[ETR]	Evaluation Technical Report CombICAO Applet in SSCD configuration on Cosmo V9, 19-RPT-140, Version 5.0, 12 December 2019.
[ICAO_9303]	ICAO Doc 9303, Machine Readable Travel Documents, Seventh Edition, 2015 – Security Mechanisms for MRTDs
[HW-CERT]	NSCIB-CC-200833-MA, v1, 01 August 2019
[HW-ETRfC]	Evaluation Technical Report for Composition ID-ONE COSMO V9 ESSENTIAL – EAL5+, 18-RPT-647, v6.0, 29 July 2019
[HW-ST]	SCYLLA Security Target, FQR 110 8779, Ed2
[JIL_AM]	Attack Methods for Smartcards and Similar Devices (controlled distribution), Version 2.3, April 2019
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[PP 419211-2]	EN 419211-2:2013, Protection Profiles for secure signature creation device - Part 2: Device with key Generation, BSI-CC-PP-0059-2009-MA-01, V2.0.1.
[PP 419211-3]	EN 419211-3:2013, Protection profiles for secure signature creation device - Part 3: Device with key import, BSI-CC-PP-0075, V1.0.2.
[PP 419211-4]	EN 419211-4:2013, Protection Profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application, BSI-CC-PP-0071, version 1.0.1
[ST]	CombICAO Applet in SSCD configuration on Cosmo v9 – Security Target, FQR 110 8784 version 8.0.
[ST-lite]	CombICAO Applet in SSCD configuration on Cosmo v9 – Public Security Target, FQR 110 9320, version 3.0, 20 November 2019
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

TÜVRheinland®
Precisely Right.

[TR_03110]   Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI)

(This is the end of this report).