Certification Report

ePass Applet on Sm@rtCafé® Expert 8.0 C1, Version 1.0

Sponsor:	***Veridos GmbH*** **Prinzregentenstraße 161,** **81677 Munich** **Germany**
Developer:	***Giesecke+Devrient Mobile Security GmbH*** **Prinzregentenstraße 159,** **81677 Munich** **Germany**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0568828-CR**
Report version:	**1**
Project number:	**0568828**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**31 October 2022**
Number of pages:	**13**
Number of appendices:	**0**

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

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.

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 ePass Applet on Sm@rtCafé® Expert 8.0 C1, Version 1.0. The developer of the ePass Applet on Sm@rtCafé® Expert 8.0 C1, Version 1.0 is Giesecke+Devrient Mobile Security GmbH located in Munich, Germany and Veridos GmbH was 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 an applet named ePass applet based on Sm@rtCafé® Expert 8.0 C1 platform, which is used as an ICAO eMRTD, which can be configured to support the different authentication mechanisms.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 31 October 2022 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 ePass Applet on Sm@rtCafé® Expert 8.0 C1, Version 1.0, 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 ePass Applet on Sm@rtCafé® Expert 8.0 C1, Version 1.0 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

- EAL5 augmented (EAL5+) assurance requirements when authentication method PACE, EAC and AA is selected. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).
- EAL4 augmented (EAL4+) assurance requirements when authentication method BAC is selected. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and ATE_DPT.2 (Testing: security enforcing modules)

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.

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the ePass Applet on Sm@rtCafé® Expert 8.0 C1, Version 1.0 from Giesecke+Devrient Mobile Security GmbH located in Munich, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware IC	Infineon Security Controller, IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh with firmware 80.306.16.0 & 80.306.16.1, optional NRG SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.15.000 and v2.11.003, optional ACL v3.33.003 and v3.02.000, optional RCL v1.10.007, optional HCLv1.13.002 and guidance, registered under the reference BSI-DSZ-CC-1107-V3-2022, reported in *[HW-CERT]*	T11 (design step)
Platform OS	Giesecke+Devrient Mobile Security GmbH, Sm@artCafé® Expert, registered under the reference CC-22-0289060, reported in *[Plat-CERT]*	8.0 C1
Software	ePass Applet on Sm@rtCafé® Expert 8.0 C1	1.0

To ensure secure usage a set of guidance documents is provided, together with the ePass Applet on Sm@rtCafé® Expert 8.0 C1, Version 1.0. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 2.3.

2.2 Security Policy

The TOE has the following main security features

- Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the connected terminal supporting the protocols BAC, SAC(PACE) as per *[ICAO_9303_11]* and EAC as per [*TR-03110_1]*
- Averting of inconspicuous tracing of the travel document as per *[TR-03110_1]*
- Self-protection of the TOE security functionality and the data stored inside as per *[TR-03110_1]*
- Means to check authenticity of the terminal, Terminal Authentication as per *[TR-03110_1]*
- Means to prove authenticity of the chip by means of Active Authentication or Chip Authentication as per *[TR-03110_1]*
- Chip authentication followed by terminal authentication used as a precondition to provide access to biometric data known as EAC, as per *[TR-03110_1]*

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 5.1 and 5.2 of the *[ST-lite]*.

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.

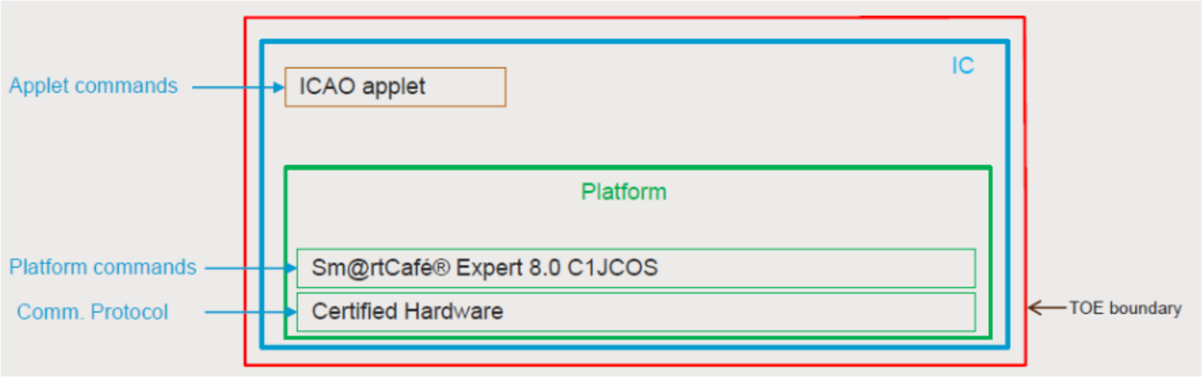
Note that the ICAO MRTD infrastructure critically depends on the objectives for the environment to be met. These are not weaknesses of this particular TOE, but aspects of the ICAO MRTD infrastructure as a whole.

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



The TOE is an applet named ePass applet based on Sm@rtCafé® Expert 8.0 C1 platform, which is used as an ICAO eMRTD, which can be configured to support the different authentication mechanisms supported by the TOE.

PACE(PIN) and EACV2 not part of the certified scope.

2.5 Documentation

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

Identifier	Version
Guidance Documentation ePass Applet on Sm@rtCafé® Expert 8.0 C1, dated 05 May 2022	0.3
Guidance Documentation for the Initialization and Personalization Phase ePass Applet on Sm@rtCafé® Expert 8.0 C1, dated 06 September 2022	1.1
Guidance Documentation for the Usage Phase ePass Applet on Sm@rtCafé® Expert 8.0 C1, dated 04 March 2022	0.4
EPASS Applet EPASS10-100 Personalization Concept, dated 26 August 2022	2.3
EPASS Applet EPASS10-100 Usage Phase Commands, dated 06 May 2022	1.1
Operative Guidance Sm@rtCafé® Expert 8.0 C1, dated 31 August 2022	2.3

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 performed extensive testing on functional specification, subsystem and SFR-enforcing module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The developer used a set of proprietary test suites and tools to test the TOE. This included tests on actual hardware as well as tests on simulator as measuring the ATE code coverage could only be performed in such environments. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

The underlying hardware and crypto-library test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

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 could 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 AM]*. An important source for assurance in this step was the technical report *[Plat-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 are deemed appropriate.

The total test effort expended by the evaluators was 1 week. During that test campaign, 100% of the total time was spent on logical tests.

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] (ePass Applet on Sm@rtCafé® Expert 8.0 C1, Version 1.0)*.

The TOE was tested in personalisation and operational life-cycle states with the applet version as specified in in the Security Target [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 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.

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 five (5) Site Technical Audit Reports.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number ePass Applet on Sm@rtCafé® Expert 8.0 C1, Version 1.0.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, 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 ePass Applet on Sm@rtCafé® Expert 8.0 C1, Version 1.0, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented ALC_DVS.2 and AVA_VAN.5 when PACE is used without EAC in order to conform to *[PP_0068]*, EAL5 augmented ALC_DVS.2 and AVA_VAN.5 when PACE is used with EAC in order to conform to *[PP_0056]*** and **EAL54 augmented ALC_DVS.2 and ATE_DPT.2.5 when BAC is used to conform to *[PP_0055]***. 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_*0055*]*, *[PP_*0056*]* and *[PP_*0068*]*.

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.

3 Security Target

The ePass Applet on Sm@rtCafé® Expert 8.0 C1 Security Target, Version 1.1, dated 12 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:

AES	Advanced Encryption Standard
BAC	Basic Access Control
CA	Chip Authentication
CAM	Chip Authentication Mapping
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
CVCA	Country Verifying Certification Authority
DES	Data Encryption Standard
DFA	Differential Fault Analysis
EAC	Extended Access Control
ECB	Electronic Code Book (a block-cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMA	Electromagnetic Analysis
eMRTD	electronic MRTD
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
JIL	Joint Interpretation Library
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
PKI	Public Key Infrastructure
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm

SHA	Secure Hash Algorithm
SM	Secure Messaging
SPA/DPA	Simple/Differential Power Analysis
TA	Terminal Authentication
TOE	Target of Evaluation
TRNG	True Random Number Generator

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

[COMP] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018

[ETR] Evaluation Technical Report “ePass Applet on Sm@rtCafé® Expert 8.0 C1 v1.0” – EAL5+ and EAL4+ for BaC, 22-RPT-550, Version 4.0, Dated 31 October 2022

[HW-CERT] IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh design step T11 with firmware 80.306.16.0 & 80.306.16.1,optional NRG™ SW 05.03.4097, optional HSLv3.52.9708, UMSLC lib v01.30.0564, optional SCLv2.15.000 and v2.11.003, optional ACL v3.33.003 andv3.02.000, optional RCL v1.10.007, optional HCLv1.13.002 and user guidance, dated 16 May 2022, registered under BSI-DSZ-CC-1107-V3-2022

[HW-ETRfC] EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP) Common Criteria CC 3.1, (EAL6 augmented with ALC_FLR.1), Version: 5, Project / Certification ID: 8120103228 / BSI-DSZ-CC-1107-V3, TOE: IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11, dated 11 May 2022

[HW-ST] IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11, Security Target Lite, v 4.3.1, dated 10 May 2022

[ICAO_9303_11] International Civil Aviation Organization, DOC 9303 Machine Readable Travel Documents Seventh Edition – 2015 Part 11: Security Mechanisms for MRTD's

[Plat-CERT] Certification report for Sm@rtCafé® Expert 8.0 C1, version 1.0, Dated 01 September 2022, registered under NSCIB-CC-0289060-CR

[Plat-ST] Sm@rtCafé® Expert 8.0 C1 Veridos/Giesecke+Devrient MS Security Target, Version 3.0/Status 31.08.2022

[Plat-ETRfC] Evaluation Technical Report for Composition “Sm@rtcafe Expert 8.0 C1” – EAL6+, 22- RPT-658, v4.0, 1 September 2022

[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

[PP_0055] Protection Profile Machine Readable Travel Document with “ICAO Application”, Basic Access Control (MRTD-PP), Version 1.10, 25 March 2009, registered under the reference BSI-CC-PP-0055-2009

[PP_0056] Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP), Version 1.3.2, 05 December 2012, registered under the reference BSI-CC-PP-0056-V2-2012

[PP_0068] Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE, Version 1.0.1, 22 July 2014, registered under the reference BSI-CC-PP-0068-V2-MA-01

[ST] ePass Applet on Sm@rtCafé® Expert 8.0 C1 Security Target, Version 1.1, dated 12 September 2022

[ST-lite] ePass Applet on Sm@rtCafé® Expert 8.0 C1 Security Target Lite, Version 1.1, dated 12 September 2022

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

[TR-03110_1] Federal Office for Information Security (BSI) Technical Guideline TR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token Part 1 - eMRTDs with BAC/PACEv2 and EACv1 Version 2.20, 26. February 2015

(This is the end of this report.)