

Certification Report

BSI-DSZ-CC-1188-2023

for

TCOS ID Version 3.0 Release 1/P71

from

Deutsche Telekom Security GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111



Deutsches IT-Sicherheitszertifikat

erteilt vom



Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1188-2023 (*)

Security IC with MRTD Applications (ePass, eID, eSign)

TCOS ID Version 3.0 Release 1/P71

from Deutsche Telekom Security GmbH
PP Conformance: Common Criteria Protection Profile Machine-
Readable Electronic Documents based on BSI TR-
03110 for Official Use [MR.ED-PP], Version 2.0.3,
18 July 2016, BSI-CC-PP-0087-V2-2016-MA-01

Common Criteria PP Configuration Machine
Readable Electronic Documents – Optionales
Nachladen (Optional Post-Emission Updates)
[MR.ED-ON-PP], Version 0.9.2, 18 August 2016,
BSI-CC-PP-0090-2016

Functionality: PP conformant
Common Criteria Part 2 extended

Assurance: Common Criteria Part 3 conformant
EAL 4 augmented by ALC_DVS.2, ATE_DPT.2,
AVA_VAN.5



SOGIS
Recognition Agreement



Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 only



The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) 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 and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) 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 the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 18 April 2023

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

This page is intentionally left blank.

Contents

A. Certification.....	6
1. Preliminary Remarks.....	6
2. Specifications of the Certification Procedure.....	6
3. Recognition Agreements.....	7
4. Performance of Evaluation and Certification.....	8
5. Validity of the Certification Result.....	8
6. Publication.....	9
B. Certification Results.....	10
1. Executive Summary.....	11
2. Identification of the TOE.....	13
3. Security Policy.....	16
4. Assumptions and Clarification of Scope.....	16
5. Architectural Information.....	17
6. Documentation.....	18
7. IT Product Testing.....	18
8. Evaluated Configuration.....	19
9. Results of the Evaluation.....	20
10. Obligations and Notes for the Usage of the TOE.....	22
11. Security Target.....	23
12. Regulation specific aspects (eIDAS, QES).....	23
13. Definitions.....	23
14. Bibliography.....	26
C. Excerpts from the Criteria.....	30
D. Annexes.....	31

A. Certification

1. Preliminary Remarks

Under the BSIG¹ Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security¹
- BSI Certification and Approval Ordinance²
- BMI Regulations on Ex-parte Costs³
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1⁴ [1] also published as ISO/IEC 15408

¹ Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

² Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

³ BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at <https://www.sogis.eu>.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: <https://www.commoncriteriaportal.org>.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 and ALC_FLR components.

⁴ Proclamation of the Bundesministerium des Innern und für Heimat of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product TCOS ID Version 3.0 Release 1/P71 has undergone the certification procedure at BSI.

The evaluation of the product TCOS ID Version 3.0 Release 1/P71 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 05 April 2023. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)⁵ recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Deutsche Telekom Security GmbH.

The product was developed by: Deutsche Telekom Security GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 18 April 2023 is valid until 17 April 2028. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

⁵ Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life-cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product TCOS ID Version 3.0 Release 1/P71 has been included in the BSI list of certified products, which is published regularly (see also Internet: <https://www.bsi.bund.de> and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer⁶ of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

⁶ Deutsche Telekom Security GmbH
Untere Industriestraße 20
57250 Netphen
Germany

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is the product TCOS ID Version 3.0 Release 1/P71 provided by Deutsche Telekom Security GmbH and based on the hardware platform P71 (N7122) by NXP Semiconductors GmbH. It is an electronic Identity Card (ID_Card) representing a smart card with contactless interface programmed according to the Technical Guideline BSI TR-03110 [24] and the ICAO specifications [26] and [27]. The smart card provides the following authentication mechanisms:

- Passive Authentication
- Password Authenticated Connection Establishment (PACE)
- Chip Authentication version 1, version 2 and version 3
- Terminal Authentication version 1 and version 2

Additionally, the TOE meets the requirements of the Technical Guideline BSI TR-03116-2 [25] as part of the qualification for the use within electronic ID card projects of the Federal Republic of Germany.

The smart card contains at least one of the following applications that are all subject of the TOE's evaluation:

- ePassport Application:
With this application the TOE is intended to be used as a machine readable travel document (MRTD). The application contains the related user data (including biometric data) as well as the data needed for authentication (including MRZ).
- eID Application:
This application is intended to be used for accessing official and commercial services, which require access to the user data stored in the context of this application. The application includes the related user data and the data needed for authentication.
- eSign Application:
This application is intended to be used in the context of official and commercial services, where a qualified electronic signature of the ID_Card Holder is required. The application contains the data needed for generating qualified electronic signatures on behalf of the ID_Card Holder as well as for user authentication. The application is optional, i.e. it can optionally be activated on the ID_Card by a Certification Service Provider authorized by the ID_Card Issuer.

Two different major configurations of the TOE exist, that only differ in the installed file system or applications respectively:

- Passport:
ePassport Application compliant to ICAO ([26], [27])
- ID Document:
ePassport Application compliant to ICAO ([26], [27]), eID Application compliant to [24], Part 2 and eSign Application compliant to [9]

The TOE provides the so-called Update-in-Field mechanism. This secure update mechanism allows to install code-signed updates of the TOE Embedded Software (operating system part) by authorized staff during operational use. The TOE only installs update packages that are encrypted, integrity-protected and signed by the authority in

charge of delivering and installing updates. The TOE allows only authenticated update terminals to upload an update package to the TOE and to initiate the update procedure. Refer to the TOE’s user guidance documentation ([15] to [19]). The TOE’s evaluation only covers the Update-in-Field mechanism itself, but does not cover any update packages.

The Security Target [6] is the basis for this certification. It is based on the following certified Protection Profile and PP Configuration and claims strict conformance to them:

- Common Criteria Protection Profile Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use (MR.ED-PP), Version 2.0.3, 18 July 2016, BSI-CC-PP-0087-V2-2016-MA-01 [7]
- Common Criteria PP Configuration Machine Readable Electronic Documents - Optionales Nachladen (Optional Post-Emission Updates) [MR.ED-ON-PP], Version 0.9.2, 18 August 2016, BSI-CC-PP-0090-2016 [8].

The PP [7] claims itself strict conformance to the following Protection Profiles:

- Protection profiles for secure signature creation device – Part 2: Device with key generation, EN 419211-2:2013, Version 2.0.1, 18 May 2013, CEN/ISSS, BSI-CC-PP-0059-2009-MA-02 [9]
- Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE (EAC PP), Version 1.3.2, 05 December 2012, BSI-CC-PP-0056-V2-2012-MA-02 [10]
- Common Criteria Protection Profile Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110 [EAC2-PP], Version 1.01, 20 May 2015, BSI-CC-PP-0086-2015 [11]

Hereby, the PPs [10] and [11] claim themselves strict conformance to the following Protection Profile:

- Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, 22 July 2014, BSI-CC-PP-0068-V2-2011-MA-01 [12]

All in all, this means in result that the TOE is conformant to the Protection Profiles [7], [8], [9], [10], [11] and [12] listed above.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_DVS.2, ATE_DPT.2, AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality / Addressed issue
Identification and authentication
Secure communication
Secure key pair generation
Signature creation

TOE Security Functionality / Addressed issue
Access control for stored objects
Update in the field
Reliability of stored information

Table 1: TOE Security Functionalities

The following TOE security features are the most significant for the TOE's operational use. The TOE ensures that

- only authenticated terminals can get access to the user data stored on the TOE and use security functionality of the card according to the access rights of the terminal,
- the card holder can control access by consciously presenting his card and/or by entering his secret PIN,
- authenticity and integrity of user data can be verified,
- confidentiality of user data in the communication channel between the TOE and the connected terminal is provided,
- inconspicuous tracing of the card is averted,
- its security functionality and the data stored inside are self-protected, and
- digital signatures can be created.

For more details please refer to the Security Target [6], chapter 7, in particular 7.1 to 7.7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.2, 3.3 and 3.4.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

TCOS ID Version 3.0 Release 1/P71

The following table outlines the TOE deliverables:

No.	Type	Identifier	Release	Form of Delivery
1	HW/ SW	NXP Secure Smart Card Controller P71 / N7122 including its IC Dedicated Software For details on the MRTD chip and the IC Dedicated Software see certification report BSI-DSZ-CC-1149-2022 and the assurance continuity maintenance report BSI-DSZ-CC-1149-2022-MA-01.	Hardware platform: NXP P71D600 Wafer-Image (ChipExe): WaferImageTCOS-ID_HW04_MB39BM01000000_CCI00_submission	Delivery type: Module: MOB6, U52 Inlay: SOM 31 (only for 'Passport') Inlay: SOM 20 (only for 'ID Document')
2	SW	TOE Embedded Software / Operating System and File System: TCOS ID Version 3.0 Release 1/P71 in the two different major configurations 'Passport' and 'ID Document' (containing at least the ePassport, eID or eSign Application with their dedicated files for the respective application in a file system)	OS version: '01 00 00 00' OS Completion Code version: '00 00' Code ELF Info: '01 00 01' Object System ELF Info: '02 00 01' ('Passport') '01 00 01' ('ID Document')	Implemented in the flash memory of the IC
3	DOC	TCOS ID card Version 3.0 Release 1, Guidance Document – Common Part, Guidance Documentation of TCOS ID Card Version 3.0 Release 1 with PACE/SAC and EAC/PSA protocol	Version 1.0.0 [15]	Document in electronic form (encrypted and signed)
4	DOC	TCOS ID card Version 3.0 Release 1, Operational Guidance – Passport, Guidance Documentation of TCOS ID Version 3.0 Release 1 with ePassport Application	Version 1.0.0 [16]	Document in electronic form (encrypted and signed)
5	DOC	TCOS ID card Version 3.0 Release 1, Operational Guidance – ID Document, Guidance Documentation of TCOS ID Version 3.0 Release 1 with ePassport, eID and eSign Application	Version 1.0.0 [17]	Document in electronic form (encrypted and signed)
6	DOC	TCOS ID card Version 3.0 Release 1, Administrator's Guidance – Passport, Guidance Documentation of TCOS ID Version 3.0 Release 1 with ePassport Application	Version 1.0.0 [18]	Document in electronic form (encrypted and signed)
7	DOC	TCOS ID card Version 3.0 Release 1, Administrator's Guidance – ID Document, Guidance Documentation of TCOS ID Version 3.0 Release 1 with ePassport, eID and eSign Application	Version 1.0.0 [19]	Document in electronic form (encrypted and signed)
8	Text Files	Authentication key (for personalization) and AE wrapper keys (key data of the Key Set for Key Set update in the framework of the Update-in-Field mechanism)	n/a	Document in electronic form (encrypted and signed)

Table 2: Deliverables of the TOE

The customer-specific Wafer-Image (ChipExe) for the TOE is labelled and identified by NXP Semiconductors GmbH as TCOS_ID_01C0_3.0.1_CCI00.

The name of the Wafer-Image file transferred from Deutsche Telekom Security GmbH to NXP Semiconductors GmbH is WaferImageTCOS-ID_HW04_MB39BM01000000_-CCI00_submission.zip.gpg.

The identification of the TOE by NXP Semiconductors GmbH is defined by the project name TCOS_ID_01C0_3.0.1_CCI00.

The wafer initialisation of the TOE based on the hardware platform P71 / N7122 is part of the NXP IC manufacturing and takes place by using the aforementioned Wafer-Image from Deutsche Telekom Security GmbH that includes all TOE parts.

The TOE Embedded Software consists of the operating system TCOS ID Version 3.0 Release 1/P71, the related completion data and the different file systems for its two major configurations 'Passport' and 'ID Document'. The Initialization Agent and Personalization Agent can use the GET CARD INFO command (option 'Get chip identification data', CLA = '80' / INS = 'AA' / P1 = '01') as described in the user guidance [15], chapter 12.1.2 to read out the chip information and identify the chip and the TOE Embedded Software embedded in the chip (only available in the TOE's life-cycle model till finalisation of the personalization phase). To open production phases for personalization a mutual authentication via the MUTUAL AUTHENTICATE command as described in the user guidance [15], chapter 12.1.5 is necessary, therefore the authenticity of the TOE is verified before further usage of the TOE.

The following identification data can be retrieved within a 32 Byte string responded by the GET CARD INFO command (option 'Get chip identification data'):

Byte #	Product Information
1	Chip Manufacturer (NXP)
2-3	Chip Type (Type ID of the Chip Manufacturer)
4-5	Firmware version of the Hardware Platform
6-11	Unique identification number for the chip
12-15	Card Operating System version
16-17	Operating System Completion Code version
18	Card Configuration Info / Operation Mode
19	Life-cycle of the selected TCOS ID Application
20-22	Code ELF Info
23-25	1 st Object System ELF Info
26-28	2 nd Object System ELF Info
29-32	RFU

Table 3: TOE Identification

Note that Bytes 6-11 (unique identification number for the chip) are chip specific data which differ for each chip used in the TOE.

The TOE is finalized and ready for delivery in the sense of the CC after finishing of the TOE's embedding, completion and initialization. Delivery is performed from the Bundesdruckerei GmbH in its role as Completion and Initialization Agent to the

personalization facility by a secured transport to a specific person of contact at the personalization site. Furthermore, the Personalization Agent receives information about the personalization commands and process requirements. To ensure that the Personalization Agent receives this evaluated version, the procedures to start the personalization process as described in the Administrator's guidance documents [18] and [19] have to be followed.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

The Security Policy of the TOE is defined according to the Protection Profiles [7], [8], [9], [10], [11] and [12] by the Security Objectives and Requirements for the chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organisation (ICAO). The Security Policy addresses the advanced security methods for authentication and secure communication, which are described in detail in the Security Target [6].

The TOE implements physical and logical security functionality in order to protect user data stored and operated on the smart card when used in a hostile environment. Hence, the TOE maintains integrity and confidentiality of code and data stored in its memories and the different CPU modes with the related capabilities for configuration and memory access and for integrity, the correct operation and the confidentiality of security functionality provided by the TOE. Therefore, the TOE's overall policy is to protect against malfunction, leakage, physical manipulation and probing. Besides, the TOE's life-cycle is supported as well as the user identification whereas the abuse of functionality is prevented. Furthermore, specific cryptographic services including crypto routines, random number generation and key management functionality are being provided to be securely used by the smart card embedded software.

Specific details concerning the above mentioned security policies can be found in the Security Target [6], chapter 6.1.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- OE.Legislative_Compliance: Issuing of the travel document
- OE.Auth_Key_Travel_Document: Travel document Authentication Key
- OE.Authoriz_Sens_Data: Authorization for Use of Sensitive Biometric Reference Data
- OE.Exam_Travel_Document: Examination of the physical part of the travel document
- OE.Ext_Insp_Systems: Authorization of Extended Inspection Systems
- OE.Prot_Logical_Travel_Document: Protection of data from the logical travel document

- OE.RestrictedIdentity: Restricted Identity and Sector's Static Key Pairs
- OE.Personalization: Personalization of travel document
- OE.Travel_Document_Holder: Travel document holder Obligations
- OE.Passive_Auth_Sign: Authentication of travel document by Signature
- OE.Chip_Auth_Key: Key Pairs needed for Chip Authentication and Restricted Identification
- OE.Terminal_Authentication: Key pairs needed for Terminal Authentication
- OE.Terminal: Terminal operating
- OE.Code_Confidentiality
- OE.Secure_Environment
- OE.Eligible_Terminals_Only
- OE.SVD_Auth: Authenticity of the SVD
- OE.CGA_Qcert: Generation of qualified certificates
- OE.SSCD_Prov_Service: Authentic SSCD provided by SSCD Provisioning Service
- OE.HID_VAD: Protection of the VAD
- OE.DTBS_Intend: SCA sends data intended to be signed
- OE.DTBS_Protect: SCA protects the data intended to be signed
- OE.Signatory: Security obligation of the Signatory
- OE.Lim_Block_Loader

Details can be found in the Security Target [6], chapter 4.2 as well as in the Protection Profiles [7], [8], [9], [10], [11] and [12].

5. Architectural Information

The TOE is a composite product. It is composed from an Integrated Circuit (IC) and the TOE Embedded Software that contains the operating system TCOS ID Version 3.0 Release 1/P71 (including the related completion data) and the different file systems for its two major configurations (Passport, ID Document). Hereby, the TOE Embedded Software includes the ePassport, eID and eSign Application respectively in dependency of the chosen major configuration.

For details concerning the underlying IC and its certification refer to the certification report BSI-DSZ-CC-1149-2022 and the assurance continuity maintenance report BSI-DSZ-CC-1149-2022-MA-01 [20].

The Security Functions of the TOE are:

- Identification and authentication
- Secure communication
- Secure key pair generation
- Signature creation
- Access control for stored objects

- Update in the field
- Reliability of stored information

According to the TOE Design these Security Functions are enforced by the following subsystems:

- Hardware (COMP_CH): Hardware Platform
- Kernel (COMP_KL): implements security relevant / critical base functions in system mode of the Hardware Platform
- Application TCOS ID 3.0 (COMP_TC30): implements TCOS ID 3.0 commands into system calls for the Kernel, processes APDUs after getting process control from the Kernel and requests resources of the Kernel

6. Documentation

The evaluated documentation as outlined in Table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target [6].

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

The developer tested all TOE Security Functions either on real cards or with simulator tests. For all commands and functionality tests, test cases are specified in order to demonstrate the expected behaviour including error cases. Hereby, a representative sample including all boundary values of the parameter set was tested, e.g. all command APDUs with valid and invalid inputs were tested and all functions were tested with valid and invalid inputs. Repetition of developer tests was performed during the independent evaluator tests.

Since many Security Functions can be tested by TR-03110 [24] APDU command sequences, the evaluators performed these tests with real cards. This is considered to be a reasonable approach because the developer tests include a full coverage of all security functionality. Furthermore, penetration tests were chosen by the evaluators for those Security Functions where internal secrets of the card could maybe be modified or observed during testing. During their independent testing, the evaluators covered:

- testing APDU commands related to general protection of user data and TSF data,
- testing APDU commands related to identification and authentication,
- testing APDU commands related to access control,
- testing APDU commands related to cryptographic functions (including generation of key pairs and creation of digital signatures),
- testing APDU commands related to the protection of communication (secure messaging channel),
- testing APDU commands related to the Update-in-Field mechanism,
- penetration testing related to verify the reliability of the TOE,
- source code analysis performed by the evaluators,

- testing the commands which are used to execute the different PACE, CA and TA protocols,
- side channel analysis for SHA and ECC (including ECC key generation),
- using machine learning and deep learning methods for side channel analysis,
- fault injection attacks (laser attacks and EM Glitches),
- testing APDU commands for the initialization, personalization and usage phase,
- testing APDU commands for the commands using cryptographic mechanisms.

The evaluators have tested the TOE systematically against high attack potential during their penetration testing.

The achieved test results correspond to the expected test results.

8. Evaluated Configuration

This certification covers the following TOE with its two major configurations:

The TOE TCOS ID Version 3.0 Release 1/P71 under certification is composed from:

- Integrated Circuit (IC) NXP P71 (N7122) including its IC Dedicated Software
- TOE Embedded Software that contains the operating system TCOS ID Version 3.0 (including the related completion data) and the different file systems for its two major configurations
- Guidance documentation (see Table 2, rows 3 to 7, i.e. documents [15] to [19])
- Authentication key material and completion and initialization data (see Table 2, row 8)

Hereby, this certification covers the following two major configurations of the TOE:

- Passport:
ePassport Application compliant to ICAO ([26], [27])
- ID Document:
ePassport Application compliant to ICAO ([26], [27]), eID Application compliant to [24], Part 2 and eSign Application compliant to [9]

The TOE is installed on a dual-interface chip (contact-based and contactless chip) of type P71 / N7122 from NXP Semiconductors GmbH. This IC is certified under the Certification ID BSI-DSZ-CC-1149-2022 and BSI-DSZ-CC-1149-2022-MA-01 (refer to [20]).

The TOE does not use cryptographic software libraries from NXP Semiconductors GmbH, but provides its cryptographic services by the cryptographic library developed by Deutsche Telekom Security GmbH.

The Initialization Agent and Personalization Agent can use the GET CARD INFO command (option 'Get chip identification data') as described in chapter 2 above to read out the chip information and identify the chip and the TOE Embedded Software installed on the chip during the life-cycle phases completion and initialization. The following table describes the evaluated TOE configurations with their respective identifiers:

Byte #	Data type	Content (Passport)	Content (ID Document)
1	Chip Manufacturer (NXP)	'04'	'04'

Byte #	Data type	Content (Passport)	Content (ID Document)
2-3	Chip Type	'01 20'	'01 20'
4-5	Firmware version	'B6 50'	'B6 50'
12-15	Card Operating System version	'01 00 00 00'	'01 00 00 00'
16-17	Operating System Completion Code version	'00 00'	'00 00'
18	Card Configuration Info / Operation Mode	'01'	'01'
19	Life-cycle of the TCOS ID Application	'07'	'07'
20-22	Code ELF Info	'01 00 01'	'01 00 01'
23-25	1 st Object System ELF Info	'02 00 01'	'01 00 01'
26-28	2 nd Object System ELF Info	'00 00 00'	'00 00 00'

Table 4: Evaluated TOE configurations and identifier

The GET CARD INFO command (option 'Get chip identification data') and related parameters are described in the user guidance [15], chapter 12.1.2.

The identification data as outlined in Table 4 and retrieved from the product must comply with the data given in Annex B of the user guidances [18] and [19] in order for the TOE to be verified as a certified version.

The TOE's evaluation only covers its Update-in-Field mechanism itself, but does not cover any update packages.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

- (i) Composite product evaluation for Smart Cards and similar devices according to AIS 36 (see [4]). On base of this concept the relevant guidance documents of the underlying IC platform (refer to the guidance documents covered by [20]) and the document ETR for composite evaluation from the IC's evaluation ([22]) have been applied in the TOE evaluation. Related to AIS 36 the updated version of the JIL document 'Composite product evaluation for Smart Cards and similar devices', Version 1.5.1, May 2018 was taken into account.
- (ii) Guidance for Smartcard Evaluation (AIS 37, see [4]).
- (iii) Attack Methods for Smartcards and Similar Devices (AIS 26, see [4]).
- (iv) Application of Attack Potential to Smartcards (AIS 26, see [4]).
- (v) Application of CC to Integrated Circuits (AIS 25, see [4]).

- (vi) Security Architecture requirements (ADV_ARC) for smart cards and similar devices (AIS 25, see [4]).
- (vii) Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6 (AIS 34, see [4]).
- (viii) Functionality classes and evaluation methodology of physical and deterministic random number generators (AIS 20 and AIS 31, see [4]).
- (ix) Informationen zur Evaluierung von kryptographischen Algorithmen (AIS 46, see [4]).

For smart card specific methodology the scheme interpretations AIS 25, AIS 26, AIS 34, AIS 36, AIS 37 and AIS 46 (see [4]) were used. For RNG assessment the scheme interpretations AIS 20 and AIS 31 were used (see [4]).

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report).
- The components ALC_DVS.2, ATE_DPT.2, AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Common Criteria Protection Profile Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use (MR.ED-PP), Version 2.0.3, 18 July 2016, BSI-CC-PP-0087-V2-2016-MA-01 [7]

Common Criteria PP Configuration Machine Readable Electronic Documents - Optionales Nachladen (Optional Post-Emission Updates) [MR.ED-ON-PP], Version 0.9.2, 18 August 2016, BSI-CC-PP-0090-2016 [8]

Conformance to the following Protection Profiles is inherited by the aforementioned Protection Profiles as follows:

Protection profiles for secure signature creation device – Part 2: Device with key generation, EN 419211-2:2013, Version 2.0.1, 18 May 2013, CEN/ISSS, BSI-CC-PP-0059-2009-MA-02 [9]

Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE (EAC PP), Version 1.3.2, 05 December 2012, BSI-CC-PP-0056-V2-2012-MA-02 [10]

Common Criteria Protection Profile Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110 [EAC2-PP], Version 1.01, 20 May 2015, BSI-CC-PP-0086-2015 [11]

Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE

(PACE PP), Version 1.01, 22 July 2014, BSI-CC-PP-0068-V2-2011-MA-01 [12]

- for the Functionality: PP conformant
Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
EAL 4 augmented by ALC_DVS.2, ATE_DPT.2, AVA_VAN.5

Additionally, the requirements of the Technical Guideline BSI TR-03116-2 [25] are met by the TOE. This is part of the qualification of TCOS ID Version 3.0 Release 1/P71 for the use within electronic passport card projects of the Federal Republic of Germany.

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The table in annex C of part D of this report gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy.

For the TOE's cryptographic functionalities, this table outlines - where applicable - the standard of application where their specific appropriateness is stated, and otherwise their security level as a kind of rating from cryptographic point of view.

According to [24], [25], [26] and [27] the algorithms are suitable for authentication, key agreement, authenticity, integrity, confidentiality and trusted channel. An explicit validity period is not given.

Please take into account that cryptographic functionalities with a security level of lower than 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related cryptographic operations are appropriate for the intended system. Some further hints and guidelines can be derived from the document 'Technische Richtlinie BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen' (refer to <https://www.bsi.bund.de>).

The strength of these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in Table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs 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, in particular the card issuing organisation and the national organisation responsible for the risk management, 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 of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

As the TOE provides the so-called Update-in-Field mechanism: If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

In addition, the following aspects need to be fulfilled when using the TOE:

If the product certified is being used as National ID-Card or National Document the operational instructions and limitations as outlined in 'Technische Richtlinie BSI TR-03116, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 2: Hoheitliche und eID-Dokumente' [25] (TR-03116-2) have to be followed when issuing and using the product. This includes the restrictions related to cryptographic algorithms and related parameters. Cryptographic algorithms and related parameters not covered by the certificate (see ST [6] and this certification report) must not be used. The latest published version of TR-03116-2 has to be followed (see <https://www.bsi.bund.de>).

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

Conformity of the IT Product identified in this certificate with the Regulation (EU) No 910/2014 as well as the related scope and restrictions are stated in a separate document [31].

13. Definitions

13.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
APDU	Application Protocol Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CA	Chip Authentication
CAM	Chip Authentication Mapping
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CMAC	Cipher-Based Message Authentication Code

cPP	Collaborative Protection Profile
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
EEPROM	Electrically Erasable Programmable Read-Only Memory
eID	electronic Identity Card
eIDAS	electronic IDentification, Authentication and trust Services
ELF	Executable Load File
EM	Electromagnetic
ETR	Evaluation Technical Report
IC	Integrated Circuit
ICAO	International Civil Aviation Organisation
ID_Card	electronic Identity Card
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MAC	Message Authentication Code
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
QES	Qualified Electronic Signature
QSCD	Qualified Signature Creation Device
ROM	Read Only Memory
RFU	Reserved for Future Use
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSCD	Secure Signature Creation Device
ST	Security Target
SVD	Signature Verification Data
TA	Terminal Authentication
TOE	Target of Evaluation

TSF TOE Security Functionality
VAD Verification Authentication Data

13.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC Part 2 and/or assurance requirements not contained in CC Part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - Named set of either security functional or security assurance requirements.

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

14. Bibliography

- [1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
<https://www.commoncriteriaportal.org>
- [2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 5, April 2017
<https://www.commoncriteriaportal.org>
- [3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen)
<https://www.bsi.bund.de/zertifizierung>
- [4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE⁷
<https://www.bsi.bund.de/AIS>
- [5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website
<https://www.bsi.bund.de/zertifizierungsberichte>
- [6] Security Target BSI-DSZ-CC-1188, Specification of the Security Target TCOS ID Version 3.0 Release 1/P71, Version 3.0.1, 27 March 2023, Deutsche Telekom Security GmbH

⁷specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 23, Version 4, Zusammentragen von Nachweisen der Entwickler
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document (but with usage of updated JIL document 'Composite product evaluation for Smart Cards and similar devices', Version 1.5.1, May 2018)
- AIS 38, Version 2.9, Reuse of evaluation results

- [7] Common Criteria Protection Profile Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED-PP], Version 2.0.3, 18 July 2016, BSI-CC-PP-0087-V2-2016-MA-01
- [8] Common Criteria PP Configuration Machine Readable Electronic Documents – Optionales Nachladen (Optional Post-Emission Updates) [MR.ED-ON-PP], Version 0.9.2, 18 August 2016, BSI-CC-PP-0090-2016
- [9] Protection profiles for secure signature creation device – Part 2: Device with key generation, EN 419211-2:2013, Version 2.0.1, 18 May 2013, CEN/ISSS, BSI-CC-PP-0059-2009-MA-02
- [10] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE (EAC PP), Version 1.3.2, 05 December 2012, BSI-CC-PP-0056-V2-2012-MA-02
- [11] Common Criteria Protection Profile Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110 [EAC2-PP], Version 1.01, 20 May 2015, BSI-CC-PP-0086-2015
- [12] Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, 22 July 2014, BSI-CC-PP-0068-V2-2011-MA-01
- [13] Evaluation Technical Report BSI-DSZ-CC-1188, Evaluation Technical Report (ETR) - TCOS ID Version 3.0 Release 1/P71, Version 1.1, 05 April 2023, SRC Security Research & Consulting GmbH (confidential document)
- [14] Configuration List BSI-DSZ-CC-1188, Konfigurationsliste von TCOS ID Version 3.0 Release 1/ NXP P71D600, Version 1.0, 28 March 2023, Deutsche Telekom Security GmbH (confidential document)
- [15] TCOS ID card Version 3.0 Release 1, Guidance Document – Common Part, Guidance Documentation of TCOS ID Card Version 3.0 Release 1 with PACE/SAC and EAC/PSA protocol, Version 1.0.0, 28 March 2023, Deutsche Telekom Security GmbH
- [16] TCOS ID card Version 3.0 Release 1, Operational Guidance – Passport, Guidance Documentation of TCOS ID Version 3.0 Release 1 with ePassport Application, Version 1.0.0, 28 March 2023, Deutsche Telekom Security GmbH
- [17] TCOS ID card Version 3.0 Release 1, Operational Guidance – ID Document, Guidance Documentation of TCOS ID Version 3.0 Release 1 with ePassport, eID and eSign Application, Version 1.0.0, 28 March 2023, Deutsche Telekom Security GmbH
- [18] TCOS ID card Version 3.0 Release 1, Administrator’s Guidance – Passport, Guidance Documentation of TCOS ID Version 3.0 Release 1 with ePassport Application, Version 1.0.0, 28 March 2023, Deutsche Telekom Security GmbH
- [19] TCOS ID card Version 3.0 Release 1, Administrator’s Guidance – ID Document, Guidance Documentation of TCOS ID Version 3.0 Release 1 with ePassport, eID and eSign Application, Version 1.0.0, 28 March 2023, Deutsche Telekom Security GmbH
- [20] Certification Report BSI-DSZ-CC-1149-2022 for NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1) from NXP Semiconductors Germany GmbH, 30 June 2022, Bundesamt für Sicherheit in der

Informationstechnik (BSI)

Assurance Continuity Maintenance Report BSI-DSZ-CC-1149-2022-MA-01 for NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2) from NXP Semiconductors Germany GmbH, 30 November 2022, Bundesamt für Sicherheit in der Informationstechnik (BSI)

- [21] Security Target Lite BSI-DSZ-CC-1149-2022, NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1), Version 1.3, 06 May 2022, NXP Semiconductors Germany GmbH (sanitised public document)
- Security Target Lite BSI-DSZ-CC-1149-2022-MA-01, NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2), Version 1.4, 14 October 2022, NXP Semiconductors Germany GmbH (sanitised public document)
- [22] Evaluation Technical Report for Composite Evaluation (ETR COMP), BSI-DSZ-CC-1149, Version 3, 10 May 2022, TÜV Informationstechnik GmbH (confidential document)
- [23] Certification Report BSI-DSZ-CC-S-0208-2022 for Bundesdruckerei GmbH manufacturing site for ePassport, eCover, eID card, RP card, -inlay of Bundesdruckerei GmbH, 23 June 2022, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- [24] Technical Guideline BSI TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, February 2015
- Part 2 – Protocols for electronic IDentification, Authentication and Trust Services (eIDAS), Version 2.21, December 2016
- Part 3 – Common Specifications, Version 2.21, December 2016
- Part 4 – Applications and Document Profiles, Version 2.21, December 2016
- [25] Technische Richtlinie BSI TR-03116 – Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 2: Hoheitliche und eID-Dokumente, 8 March 2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- [26] ICAO Doc 9303, Machine Readable Travel Documents, 8th Edition, 2021, ICAO
- [27] ICAO Machine Readable Travel Documents, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, November 2010, ICAO
- [28] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal L 257, 28 August 2014
- [29] COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016, laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

- [30] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2, January 2020
- [31] Certificate of Conformity pursuant to Article 29 (1), 39 (1) and Annex II of the Regulation (EU) No. 910/2014 for TCOS ID Version 3.0 Release 1/P71, April 2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC Part 1 chapter 10.5.
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1.
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8.
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12.
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17.
- The table in CC Part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at <https://www.commoncriteriaportal.org/cc/>

D. Annexes

List of annexes of this certification report

- Annex A: Security Target provided within a separate document ([6])
- Annex B: Evaluation results regarding development and production environment
- Annex C: Overview and rating of cryptographic functionalities implemented in the TOE

Annex B of Certification Report BSI-DSZ-CC-1188-2023

Evaluation results regarding development and production environment



The IT product TCOS ID Version 3.0 Release 1/P71 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 18 April 2023, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1)

are fulfilled for the development and production sites of the TOE listed below:

- a) Deutsche Telekom Security GmbH, Untere Industriestraße 20, 57250 Netphen-Dreis-Tiefenbach, Germany (Development).
- b) Bundesdruckerei GmbH, Kommandantenstraße 18, 10969 Berlin, Germany, BSI-DSZ-CC-S-0208-2022 [23] (Completion, Initialization, Inlay Assembly, Inlay Embedding).
- c) For development and production sites regarding the underlying IC platform (including IC Manufacturing, Wafer Initialization, Inlay Assembly) please refer to the certification report BSI-DSZ-CC-1149-2022 and the assurance continuity maintenance report BSI-DSZ-CC-1149-2022-MA-01 [20].

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life-cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.

Annex C of Certification Report BSI-DSZ-CC-1188-2023

Overview and rating of cryptographic functionalities implemented in the TOE

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application / Security Level	Comments
1	Authenticity	ECDSA-signature verification of card verifiable certificates using SHA-{1, 256, 384, 512}	[ECCTR], sec. 4.2.1	Key sizes corresponding to the used elliptic curve brainpoolP{256, 320, 384, 512}{r, t}1 [RFC 5639], ansix9p{256, 384}r1 [FIPS186]	[EACTR], Part 3, Appendix A.6	FCS_COP.1/ SIG_VER_EAC1PP FCS_COP.1/ SIG_VER_EAC2PP FCS_COP.1/UPD_ITC (for cryptographic key size of 512 bit only)
2	Authenticity	Digital signature verification of update packages ECDSA using SHA-512	[ECCTR], sec. 4.2.1	Key sizes corresponding to the used elliptic curve brainpoolP512t1 [RFC 5639]	[UiF]	FCS_COP.1/UPD_SIG
3	Authentication	PACEv2 including PACE-CAM	[EACTR] (PACEv2) [ICAO9303], Part 11, sec. 4.4 (PACE-CAM)	Length of [Nonce]=128 bit Key sizes corresponding to the used elliptic curve brainpoolP{256, 320, 384, 512}{r, t}1 [RFC 5639], ansix9p{256, 384}r1 [FIPS186]	[EACTR], Part 2, sec 3.2 [ICAO9303], Part 11, sec. 4.4	FCS_CKM.1/ DH_PAGE_EAC1PP FCS_CKM.1/ DH_PAGE_EAC2PP FCS_CKM.1/CAM FCS_COP.1/CAM
4	Authentication	Chip Authentication v1 based on ephemeral-static ECDH in combination with AES	[ECCTR]	Key sizes corresponding to the used elliptic curve brainpoolP{256, 320, 384, 512}{r, t}1 [RFC 5639], ansix9p{256, 384}r1 [FIPS186]	[EACTR], Part 1, sec. 3.4, Part 3, Annex A.4	FCS_CKM.1/ CA_EAC1PP
5	Authentication	Chip Authentication v2 based on ephemeral-static ECDH in combination with AES	[ECCTR]	Key sizes corresponding to the used elliptic curve brainpoolP{256, 320, 384, 512}{r, t}1 [RFC 5639], ansix9p{256, 384}r1 [FIPS186]	[EACTR], Part 2, sec. 3.4 and 3.6, Part 3, Annex A.4	FCS_CKM.1/ DH_PAGE_EAC2PP (This SFR applies also for Chip Authentication v2, cf. Application Note 12 from [EAC2-PP].) FIA_API.1/ RI_EAC2PP (Restricted Information after Terminal Authentication v2 and Chip Authentication v2 according to [EACTR],

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application / Security Level	Comments
						Part 2 is included here.) FTP_ITC.1/UPD
6	Authentication	Chip Authentication v3 based on ephemeral-static ECDH in combination with AES	[ECCTR]	Key sizes corresponding to the used elliptic curve brainpoolP{256, 320, 384, 512}{r, t}1 [RFC 5639], ansix9p {256, 384}r1 [FIPS186]	[EACTR], Part 2, sec 3.5 and 3.7, Part 3, Annex A.4.2.3	FCS_COP.1/CA3 FCS_CKM.1/CA3
7	Authentication	Terminal Authentication v1 based on ECDSA using SHA-{1, 256, 384, 512}	[ECCTR], sec. 4.2.1	Key sizes corresponding to the used elliptic curve brainpoolP{256, 320, 384, 512}r1 [RFC 5639], ansix9p{256, 384}r1 [FIPS186]	[EACTR], Part 1, sec. 3.5, Part 3, Annex A.7	e.g. FIA_UAU.1/ PACE_EAC1PP FIA_UAU.4/ PACE_EAC1PP
8	Authentication	Terminal Authentication v2 based on ECDSA using SHA-{1, 224, 256, 384, 512}	[ECCTR], sec. 4.2.1	Key sizes corresponding to the used elliptic curve brainpoolP{256, 320, 384, 512}r1 [RFC 5639], ansix9p{256, 384}r1 [FIPS186]	[EACTR], Part 2, sec. 3.3, Part 3, Annex A.7	e.g. FIA_UAU.1/ EAC2_Terminal_EAC2PP
9	Key Agreement	ECDH using SHA-{1, 256} For PACE and Chip Authentication v1 and v2	[ECCTR], sec. 4.3.2	Key sizes corresponding to the used elliptic curve brainpoolP{256, 320, 384, 512}{r, t}1 [RFC 5639], ansix9p{256, 384}r1 [FIPS186]	[EACTR], Part 3, Annex A.4, Part 1, sec. 3.4, Part 2, sec. 3.2 and 3.4	FCS_CKM.1/ DH_PACE_EAC1PP FCS_CKM.1/ CA_EAC1PP FCS_CKM.1/ DH_PACE_EAC2PP FCS_CKM.1/CAM
10	Key Agreement	ECDH using SHA-{256, 384, 512} For Chip Authentication v3	[ECCTR], sec. 4.3.2	Key sizes corresponding to the used elliptic curve brainpoolP{256, 320, 384, 512}{r, t}1 [RFC 5639], ansix9p{256, 384}r1 [FIPS186]	[EACTR], Part 2, sec 3.5, Part 3, Annex A.4.2.3	FCS_CKM.1/CA3
11	Key Agreement	ECDH using SHA-256 Trusted channel for Updates in Field	[ECCTR], sec. 4.3.2	Key sizes corresponding to the used elliptic curve brainpoolP512t1 [RFC 5639]	[EACTR], Part 3, Annex A.4	FCS_CKM.1/ UPD_ITC

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application / Security Level	Comments
12	Key Agreement	ECKA for derivation of AES keys	[ECCTR], sec. 4.3.2	k =256	[EACTR] [UiF]	FCS_CKM.1/ UPD_DEC FCS_CKM.1/ UPD_INT The agreed keys are input for key derivation of AES 256 bit keys, see FCS_COP.1/UPD_DEC.
13	Confidentiality	Encryption and Decryption for Secure Messaging, AES in CBC mode	[FIPS197] (AES) [SP800-38A] (CBC)	k =128, 192, 256	[EACTR], Part 3, Annex F [ICAOSAC]	FCS_COP.1/ CA_ENC_EAC1PP FCS_COP.1/ PACE_ENC_EAC1PP FCS_COP.1/ PACE_ENC_EAC2PP
14	Confidentiality	Decryption of update packages AES-256 in OFB mode	[FIPS197] (AES) [SP800-38A] (OFB)	k =256	[UiF]	FCS_COP.1/ UPD_DEC
15	Integrity	Secure Messaging, AES in CMAC mode	[FIPS197] (AES) [SP800-38B] (CMAC)	k =128, 192, 256	[EACTR], Part 3, Annex F [ICAOSAC]	FCS_COP.1/ PACE_MAC_EAC1PP FCS_COP.1/ CA_MAC_EAC1PP FCS_COP.1/ PACE_MAC_EAC2PP
16	Integrity	Hash value calculation of update packages SHA-256	[FIPS180]	n.a.	[EACTR] [UiF]	FCS_COP.1/UPD_INT
17	Trusted Channel	Secure messaging in ENC_MAC mode is established during PACE	[EACTR] (PACE)	-	[EACTR]	FTP_ITC.1/ PACE_EAC2PP FTP_ITC.1/ PACE_EAC1PP
18	Trusted Channel	Secure messaging in ENC_MAC mode is established during Chip Authentication v1 after PACE	[EACTR]	-	[EACTR]	FCS_COP.1/ CA_MAC_EAC1PP FCS_COP.1/ CA_ENC_EAC1PP
19	Trusted Channel	Secure messaging in ENC_MAC mode is established during Chip Authentication v2 after PACE	[EACTR]	-	[EACTR] [UiF]	FCS_COP.1/ PACE_MAC_EAC2PP FCS_COP.1/ PACE_ENC_EAC2PP (These SFRs apply also for Chip Authentication v2, cf. Application Note 15 and 17 from [EAC2-

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application / Security Level	Comments
						PP].) FTP_ITC.1/ CA2_EAC2PP FTP_ITC.1/UPD
20	Trusted Channel	Secure messaging in ENC_MAC mode is established during Chip Authentication v3 after PACE	[EACTR]	-	[EACTR]	FCS_CKM.1/CA3 FTP_ITC.1/CA3
21	Cryptographic Primitive	Hybrid physical RNG PTG.3	[AIS31] / [AIS20] [TCOS RNG]	n.a.	[ECARDTR] [TCOS RNG]	FCS_RND.1/EAC2PP
22	Cryptographic Primitive	Hash for key derivation SHA-{1, 224, 256, 384, 512}	[FIPS180]	n.a.	[EACTR]	FCS_COP.1/ SHA_EAC2PP See also above in rows 1, 2, 7, 8, 9, 10, 11, 12 and 16.
23	Cryptographic Primitive	ECDSA-signature generation	[ECCTR]	Key sizes corresponding to the used elliptic curve brainpoolP{256, 320, 384, 512}{r, t}1 [RFC 5639], ansix9p{256, 384}r1 [FIPS186]	Security level > 120 bit	FCS_COP.1/SSCDPP
24	Cryptographic Primitive	ECC Key generation for ECDH and ECDSA	[ECCTR] [TCOS RNG], sec. 5	Key sizes corresponding to the used elliptic curve brainpoolP{256, 320, 384, 512}{r, t}1 [RFC 5639], ansix9p{256, 384}r1 [FIPS186]	Security level > 120 bit	FCS_CKM.1/SSCDPP FCS_CKM.1/ DH_PACE_EAC1PP FCS_CKM.1/ DH_PACE_EAC2PP FCS_CKM.1/CAM FCS_CKM.1/ CA_EAC1PP FCS_CKM.1/CA3 FCS_CKM.1/ UPD_ITC FCS_COP.1/CAM FCS_COP.1/CA3 FIA_UAU.1/ PACE_EAC1PP FIA_UAU.4/ PACE_EAC1PP FIA_UAU.1/ EAC2_Terminal_EAC2 PP

Table 5: TOE cryptographic functionality

Bibliography for Table 5:

- [AIS20] Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- [AIS31] Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- [EAC2-PP] Common Criteria Protection Profile Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110 [EAC2-PP], Version 1.01, 20 May 2015, BSI-CC-PP-0086-2015
- [EACTR] Technical Guideline BSI TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, February 2015
- Part 2 – Protocols for electronic IDentification, Authentication and Trust Services (eIDAS), Version 2.21, December 2016
- Part 3 – Common Specifications, Version 2.21, December 2016
- Part 4 – Applications and Document Profiles, Version 2.21, December 2016
- [ECARDTR] Technische Richtlinie BSI TR-03116 – Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 2: Hoheitliche und eID-Dokumente, 8 March 2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- [ECCTR] Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.10, 01 June 2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- [FIPS180] Federal Information Processing Standards Publication FIPS PUB 180-4, Specifications for the Secure Hash Standard (SHS), March 2012, U.S. Department of Commerce/National Institute of Standards and Technology
- [FIPS186] Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013, U.S. Department of Commerce/National Institute of Standards and Technology
- [FIPS197] Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), November 2001, U.S. Department of Commerce/National Institute of Standards and Technology
- [ICAO9303] ICAO Doc 9303, Machine Readable Travel Documents, 8th Edition, 2021, ICAO
- [ICAOSAC] ICAO Machine Readable Travel Documents, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, November 2010, ICAO
- [RFC 5639] M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, March 2010, IETF

- [SP800-38A] Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST Special Publication 800-38A, December 2001, National Institute of Standards and Technology
- [SP800-38B] Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, May 2005, National Institute of Standards and Technology
- [TCOS RNG] Zufallszahlengenerierung in TCOS, Version 1.4, 13 January 2023, Deutsche Telekom Security GmbH (confidential document)
- [UiF] Spezifikation 'Update im Feld' aus Applikationssicht, Version 0.12, 04 August 2022, Deutsche Telekom Security GmbH (confidential document)

Note: End of report