Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1077-2020

for

STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1

from

Giesecke+Devrient Mobile 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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1077-2020 (*)

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

STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1

from	Giesecke+Devrient Mobile Security GmbH
PP Conformance:	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 and AVA_VAN.5

SOGIS
Recognition Agreement

Common Criteria

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2

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, 5 August 2020

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - 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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] 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 Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- 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]

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 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 3 March 2005, Bundesgesetzblatt I, p. 519

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.
- 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.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

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

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 STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1 has undergone the certification procedure at BSI.

The evaluation of the product STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 28 July 2020. 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: Giesecke+Devrient Mobile Security GmbH.

The product was developed by: Giesecke+Devrient Mobile 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.

If the certified product 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: eID-Karten und hoheitliche Dokumente’ (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 Security Target 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/).

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

[5] Information Technology Security Evaluation Facility

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 5 August 2020 is valid until 4 August 2025. 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,
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 STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1 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 developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Giesecke+Devrient Mobile Security GmbH
Prinzregentenstr. 159
81677 München
Deutschland

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 STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1 provided by Giesecke+Devrient Mobile Security GmbH and based on the hardware platform Infineon Security Controller IFX_CCI_000005h from Infineon Technologies AG (refer to [21], [22]). 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], [27] and [28]. The smart card provides the following authentication mechanisms:

- Passive Authentication
- Password Authenticated Connection Establishment (PACE)
- Chip Authentication version 1, 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.

Please note that the security mechanisms Password Authenticated Connection Establishment (PACE) and Extended Access Control (EAC) are in focus of this evaluation process. The further security mechanism Basic Access Control (BAC) is subject of a separate evaluation process (refer to BSI-DSZ-CC-1076).

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

- ePass 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. The user data of the eSign Application are protected by PACE/EAC2.

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

- Electronic Document:

  STARCOS 3.7 ID ePA C1 configuration, corresponding to the ‘Electronic Document Configuration’ described in [8] and including the following applications:

  ePass Application non-compliant to ICAO ([26], [27]) with user data protection by PACE and EAC2. eID Application compliant to [24], Part 2 and eSign Application compliant to [10] with user data protection by PACE and EAC2.

- Residence Permit:

  STARCOS 3.7 ID eAT C1 configuration, corresponding to the ‘Residence Permit Configuration’ described in [8] and including the following applications:

  ePass Application compliant to ICAO ([26], [27]) with user data protection by PACE and EAC1/EAC2. eID Application compliant to [24], Part 2 and eSign Application compliant to [10] with user data protection by PACE and EAC2.

- Passport:

  STARCOS 3.7 ID ePass C1 configuration, corresponding to the ‘Passport Configuration’ described in [8] and including the following applications:

  ePass Application compliant to ICAO ([26], [27]) with user data protection by PACE and EAC1 (hereby, EAC1 is used only for data groups 3 and 4).

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 ([16] 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 certified PP 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 [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]

The PP [8] 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, CEN/ISSS, BSI-CC-PP-0059-2009-MA-02 (June 2016) [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 [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 [12]

Hereby, the PPs [11] and [12] 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 [13]

All in all, this means in result that the TOE is conformant to all the Protection Profiles [8], [9], [10], [11], [12] and [13] listed above.

Please note that in consistency to the claimed Protection Profiles the security mechanisms Password Authenticated Connection Establishment (PACE) and Extended Access Control (EAC) are in focus of this evaluation process. The further security mechanism Basic Access Control (BAC) is subject of a separate evaluation process (refer to BSI-DSZ-CC-1076).

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 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [7], 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
SF_AccessControl	The TOE provides access control mechanisms that allow among others the maintenance of different users (Manufacturer, Personalisation Agent, Country Verifying Certification Authority (CVCA), Document Verifier (DV), domestic Extended Inspection System, foreign Extended Inspection System, Administrator, Signatory).
SF_AssetProtection	When the private signature key or the signature PIN are no longer needed in the internal memory of the TOE for calculations these parts of the memory are overwritten. The TOE supports the calculation of block check values for data integrity checking. The TOE hides information about IC power consumption and command execution time ensuring that no confidential information can be derived from this data.
SF_TSFProtection	The TOE detects and resists physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation. The TOE demonstrates the correct operation of the TSF by among others verifying the integrity of the TSF and TSF data and verifying the absence of fault injections.

TOE Security Functionality	Addressed Issue
SF_KeyManagement	The TOE supports onboard generation of corresponding ECDSA key pairs with key length of 256, 320, 384 and 512 bit. For this the TOE uses random numbers generated by its DRG.4 deterministic random number generator. The TOE also supports onboard generation of cryptographic keys based on the ECDH compliant [TR-03111] as well as generation of ECC key pairs.
SF_SignatureGeneration	The TOE performs ECDSA digital signature verification and generation with SHA-256, SHA-384 and SHA-512 and cryptographic key sizes 256, 384 and 512 bit according to [TR-03111] and [FIPS180-4].
SF_TrustedCommunication	The TOE supports the establishment of a trusted channel/path based on mutual authentication with negotiation of symmetric cryptographic keys used for the protection of the communication data with respect to confidentiality and integrity. AES in CBC mode and AES CMAC, and 3DES in CBC mode and DES Retail-MAC are used for encryption and integrity protection of the communication data.

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] and [7], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6] and [7], 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] and [7], 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:

STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	**HW Platform** Infineon Security Controller IFX_CCI_000005h including its IC Dedicated Software (Firmware) (refer to the Certification Report BSI-DSZ-CC-1110-V3-2020 [22])	SLC52GDA448 with Firmware version 80.100.17.3 (FW-00.100.17.0-SLCx2V3), with Flash Loader FL-8.02.003-SLCx2V3, with Hardware Support Library HSL-2 (HSL-03.11.8339-SLCx2_C65)	The TOE Embedded Software is implemented in the flash storage of the IC. The delivery of the TOE is performed as already initialised and pre-personalised functional cards via secured transport to the Personalisation Centre. In addition, flash images for re-loading of the TOE Embedded Software in the framework of the TOE's personalisation are delivered to the Personalisation Centre (as encrypted and signed electronic item).
2	SW	**TOE Embedded Software** IC Embedded Software, consisting of • STARCOS 3.7 ID operating system • associated file systems for the three major TOE configurations STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1	OS version: 'B7 02' (Release 3.72) Flash Image version: '00 51' TOE configurations: ePA: '0A' eAT: '0D' ePass: '02' (retrievable via the command GET PROTOCOL DATA, see below)	
3	DATA	Personalisation-related key material	--	Items in electronic form (encrypted and signed)
4	DOC	Guidance Documentation STARCOS 3.7 ID C1 – Main Document [16]	Version 1.0	Document in electronic form (encrypted and signed)
5	DOC	Guidance Documentation for the Usage Phase STARCOS 3.7 ID C1 [17]	Version 1.3	Document in electronic form (encrypted and signed)
6	DOC	Guidance Documentation for the Initialisation Phase STARCOS 3.7 ID C1 [18]	Version 2.0	Document in electronic form (encrypted and signed)
7	DOC	Guidance Documentation for the Personalisation Phase STARCOS 3.7 ID C1 [19]	Version 2.1	Document in electronic form (encrypted and signed)
8	DOC	Starcos 3.7 ID nPA - Perso guide [20]	Version 1.10	Document in electronic form (encrypted and signed)

No	Type	Identifier	Release	Form of Delivery
9	DOC	Starcos 3.7 ID eAT - Perso guide [20]	Version 1.40	Document in electronic form (encrypted and signed)
10	DOC	Starcos 3.7 ID ePass - Perso guide [20]	Version 1.20	Document in electronic form (encrypted and signed)

Table 2: Deliverables of the TOE

The TOE Embedded Software consists of the operating system of STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1 and the different file systems for its three major configurations (Electronic Document Configuration, Residence Permit Configuration, Passport Configuration).

The TOE is finalised with its initialisation, that is with loading of the STARCOS 3.7 ID operating system and the respective file system for the different TOE configurations onto the Infineon Security Controller IFX_CCI_000005h and the following pre-personalisation step for insertion of personalisation-related key material. The delivery of the TOE is performed as already initialised and pre-personalised functional cards via secured transport to the Personalisation Centre.

The Personalisation Centre receives information about the personalisation commands and process requirements. To ensure that the Personalisation Centre receives the evaluated version of the TOE, the procedures to start the personalisation process as described in the guidance documentation [16] - [20] have to be followed.

In addition, flash images for re-loading of the TOE Embedded Software in the framework of the TOE's personalisation are delivered to the Personalisation Centre (as encrypted and signed electronic item).

The Initialiser and Personaliser can use the GET PROTOCOL DATA command (CLA = 'A0', INS = 'CA') as described in the user guidance documentation [18], chapter 5.2.5 and [19], chapter 5.2.1 to read out the chip information and identify the chip and the TOE Embedded Software including its configuration.

In particular, with P1 P2 = '9F 6A' the following TOE information can be retrieved by the command GET PROTOCOL DATA:

'47 44 00 B7 02 00 51' whereby 'B7 02' identifies the version of the STARCOS 3.7 ID operating system and '00 51' identifies the version of the flash images that belong to the three major TOE configurations.

With P1 P2 = '9F 65' the following TOE configuration information can be retrieved:

TOE configuration	Response Byte-Number	
	1 (configuration ID)	2 (production state)
STARCOS 3.7 ID ePA C1	'0A'	01 (initialisation phase) 02 (personalisation phase)
STARCOS 3.7 ID eAT C1	'0D'	01 (initialisation phase) 02 (personalisation phase)
STARCOS 3.7 ID ePass C1	'02'	01 (initialisation phase) 02 (personalisation phase)

Table 3: TOE Identification Data (GET PROTOCOL DATA with P1 P2 = '9F 65')

Note that according to [18], chapter 5.2.5 and [19], chapter 5.2.1, the command GET PROTOCOL DATA is available in the usage phase, but does not provide any return values.

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 [8], [9], [10], [11], [12] and [13] 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] and [7], chapter 6 and 7.

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.Lim_Block_Loader
- 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

Details can be found in the Security Target [6] and [7], chapter 4.2 as well as in the Protection Profiles [8], [9], [10], [11], [12] and [13].

5. Architectural Information

The TOE is a composite product. It is composed from the Integrated Circuit (IC) IFX_CCI_000005h from Infineon Technologies AG and the TOE Embedded Software developed by Giesecke+Devrient Mobile Security GmbH. The TOE Embedded Software contains the operating system STARCOS 3.7 ID and the different file systems for its three major configurations Electronic Document Configuration STARCOS 3.7 ID ePA C1, Residence Permit Configuration STARCOS 3.7 ID eAT C1 and Passport Configuration STARCOS 3.7 ID ePass C1. Hereby, the TOE Embedded Software includes at least the ePass, the eID or the eSign Application, depending on the chosen major configuration.

The TOE does not use the cryptographic software libraries of the Infineon hardware platform, but provides its cryptographic services by the cryptographic library developed by Giesecke+Devrient Mobile Security GmbH.

For details concerning the CC evaluation of the underlying IC see the evaluation documentation under the Certification ID BSI-DSZ-CC-1110-V3-2020 ([21], [22]).

According to the TOE design the Security Functions of the TOE as listed in Table 1 in chapter 1 are implemented by the following subsystems:

- System Library: Application framework
- Chip Card Commands: Pre-processing and processing of all implemented commands

- Security Management: Management of the security environment, security states and rule analysis
- Key Management: Search, pre-processing, use and post-processing of keys
- Secure Messaging: SM handling
- Crypto Functions: Library with an API to all cryptographic operations
- Configuration Application: Configuration of the TOE

The subsystem Configuration Application covers the different configurations of the TOE as defined in the Security Target [6], chapter 1.2, 1.2.7 and 1.2.8 and provides the related applications. These configurations and applications comply with the general definition of data structures, including access control and management of authentication with key objects and their usage attributes.

The above-listed subsystems are supported by the subsystems Runtime System, File System, Non-Volatile Memory Management, and Transport Management.

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] and [7].

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 Key Management and Crypto Functions (including Generation of Key Pairs and Creation of Digital Signatures),
- testing APDU commands related to Security Management,
- testing APDU commands related to Secure Messaging,
- testing APDU commands related to Runtime System and System Library,
- testing the commands which are used to execute the different PACE, CA and TA authentication protocols,

- testing APDU commands related to the Update-in-Field mechanism,
- penetration testing related to the verification of the reliability of the TOE,
- source code analysis performed by the evaluators,
- analysis of the conformity of the TOE's implementation of the cryptographic algorithms to the corresponding standards outlined in the Security Target [6] and [7],
- side channel analysis for SHA, AES and ECC (including ECC key generation),
- fault injection attacks (laser attacks and EM glitches),
- testing APDU commands for the initialisation, personalisation and usage phase,
- testing APDU commands for the commands using cryptographic mechanisms, and
- fuzzy testing on APDU processing.

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 as outlined in the Security Target [6] and [7]:

The TOE STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1 under certification is composed from:

- Infineon Security Controller IFX_CCI_000005h including its IC Dedicated Support Software from Infineon Technologies AG
- TOE Embedded Software that contains the operating system STARCOS 3.7 ID and the different file systems for its three major configurations (see below)
- Guidance documentation (see Table 2, rows 4 to 10, i.e. [16] to [20])
- Personalisation-related key material (see Table 2, row 3)

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

- Electronic Document:

  STARCOS 3.7 ID ePA C1 configuration, corresponding to the 'Electronic Document Configuration' described in [8] and including the following applications:

  ePass Application non-compliant to ICAO ([26], [27]), eID Application compliant to [24], Part 2 and eSign Application compliant to [10].

- Residence Permit:

  STARCOS 3.7 ID eAT C1 configuration, corresponding to the 'Residence Permit Configuration' described in [8] and including the following applications:

ePass Application compliant to ICAO ([26], [27]), eID Application compliant to [24], Part 2 and eSign Application compliant to [10].

- Passport:

  STARCOS 3.7 ID ePass C1 configuration, corresponding to the ‘Passport Configuration’ described in [8] and including the following applications:

  ePass Application compliant to ICAO ([26], [27]).

The TOE is installed on a contactless chip of type Infineon Security Controller IFX_CCI_000005h from Infineon Technologies AG. This IC is certified under the Certification ID BSI-DSZ-CC-1110-V3-2020 (refer to [22]).

The TOE does not use the cryptographic software libraries of the Infineon hardware platform, but provides its cryptographic services by the cryptographic library developed by Giesecke+Devrient Mobile Security GmbH.

The TOE covering the IC and the TOE Embedded Software is delivered as an initialised and pre-personalised functional card. For details refer to chapter 2 of this Certification Report.

The Initialiser and Personaliser can use the GET PROTOCOL DATA command as described in chapter 2 above to read out the chip information and identify the chip and the TOE Embedded Software including its configuration during the life-cycle phases initialisation and personalisation.

In particular, with P1 P2 = ‘9F 6A’ the following TOE information can be retrieved by the command GET PROTOCOL DATA:

‘47 44 00 B7 02 00 51’ whereby ‘B7 02’ identifies the version of the STARCOS 3.7 ID operating system and ‘00 51’ identifies the version of the flash images that belong to the three major TOE configurations.

The following table describes the evaluated TOE configurations with their respective identifiers that can be retrieved with GET PROTOCOL DATA using P1 P2 = ‘9F 65’:

TOE configuration	**Response Byte-Number**	
	1 (configuration ID)	**2 (production state)**
STARCOS 3.7 ID ePA C1	‘0A’	01 (initialisation phase) 02 (personalisation phase)
STARCOS 3.7 ID eAT C1	‘0D’	01 (initialisation phase) 02 (personalisation phase)
STARCOS 3.7 ID ePass C1	‘02’	01 (initialisation phase) 02 (personalisation phase)

Table 4: Evaluated TOE configurations and identifier (GET PROTOCOL DATA with P1 P2 = ‘9F 65’)

The GET PROTOCOL DATA command and related parameters are described in the user guidance documentation [18], chapter 5.2.5 and [19], chapter 5.2.1.

The identification data as outlined in Table 4 and retrieved from the product must comply with the data given in the user guidance documentation [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. Furthermore, any DECIES domain parameters that are used when applying the Update-in-Field mechanism for loading update packages are not addressed within this evaluation. Such parameters have to be examined in view of their functional applicability by the TOE and their security impact on the TOE's cryptographic implementation in a separate evaluation process.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [14] 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 [22]) and the document ETR for composite evaluation from the IC's evaluation ([23]) have been applied in the TOE evaluation.

(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 and 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 [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]

  Indirectly conformance to the following Protection Profiles is given:

  Protection profiles for secure signature creation device – Part 2: Device with key generation, EN 419211-2:2013, CEN/ISSS, BSI-CC-PP-0059-2009-MA-02 (June 2016) [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 [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 [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]

- 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 and 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 STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1 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], [27], [28] and [31] 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 100 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 the reference https://www.bsi.bund.de).

The strength of the 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 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.

Related to the so-called Update-in-Field mechanism that is provided by the TOE, the following has to be considered: If available, certified updates of the TOE should be used. If non-certified updates are available the user of the TOE should request the sponsor to initiate and perform a re-certification of the TOE regards its update. 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 or take additional measures in order to maintain system security. Furthermore, the DECIES domain parameters that are used when applying the Update-in-Field mechanism for loading update packages shall be examined in view of their functional applicability by the TOE and their security impact on the TOE's cryptographic implementation.

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: eID-Karten und hoheitliche 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 Lite [7] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Regulation specific aspects (eIDAS, QES)

In [29] the European Parliament and the Council of the European Union have codified the conceptional requirements for qualified electronic signature devices used in the European Union. This regulation is clarified in the Commission Implementing Decision [30]. In this decision the requirements are stated that an electronic signature device must fulfil to be compliant to [29] (Article 1 and Annex).

The IT Product identified in this certificate fulfils

- PP EN 419211-2:2013 (Protection profiles for secure signature creation device - Part 2: Device with key generation (BSI-CC-PP-0059-2009-MA-02))

This Protection Profile is taken from the list of standards identified in COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016, Annex, 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].

Furthermore, the TOE must be certified using ISO/IEC 15408 and ISO/IEC 18045 in its 2008/2009 versions. The evaluation process of the TOE used the latest available version of Common Criteria [1] which is as used compatible to the ISO version cited in [30].

Therefore, the IT-product certified is technically suitable to be a compliant signature creation device according to Article 30(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 and to fulfil the requirements laid down in Article 29(1) and Annex II provided that the following operational conditions are followed:

- The obligations and notes for the usage of the TOE have to be followed as outlined in chapter 10 of this report.
- The trust service provider has to follow the operational requirements from the regulation as relevant for a compliant signature creation device as well as to follow all related obligations from its supervisory body.
- For the creation of qualified electronic signatures the product has to use the cryptographic algorithms in accordance with the SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms [31] which are depicted in Table 5.
- The trust service provider shall consider the results of the certification and the operational conditions listed above within the system risk management process for the product usage. Specifically, the evolution of limitations of cryptographic algorithms and parameters[7] as well as the evolution of attack methods related to the product or to the type of product has to be considered e.g. by a regular re-assessment of the TOE assurance.

[7] Future updates of the catalogue [31] may shorten or extend the acceptance time frame. This may need actions for the usage of the product to be taken.

No.	Cryptographic Mechanism	Key Size in Bits	Acceptability Deadline according to [31] as of today
1	ECDSA signature generation [ECCTR]	ECC key sizes corresponding to the used elliptic curve brainpoolP{256, 320, 384, 512}r1 [RFC 5639]	None
2	ECC key generation [ECCTR]	ECC key sizes corresponding to the used elliptic curve brainpoolP{256, 320, 384, 512}r1 [RFC 5639]	None

Table 5: Cryptographic algorithms of the TOE in accordance with [31]

For references to standards in Table 5 please refer to the bibliography in annex C of part D of this report.

For the ECDSA signature generation functionality provided by the TOE according to [10] please take into account that hashing of the signature creation data to be signed by the TOE is not provided by the TOE and has to be externally carried out by the user prior to signature creation. As well for hashing the document SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms [31], in particular in view of acceptability deadlines outlined in [31], should be considered.

Out of this, the compliance of the QSCD is confirmed under the conditions mentioned above within the following categories:

- Components and procedures for the generation of signature creation data
- Components and procedures for the storage of signature creation data
- Components and procedures for the processing of signature creation data

13. Definitions

13.1. Acronyms

AES Advanced Encryption Standard

AIS Application Notes and Interpretations of the Scheme

APDU Application Protocol Data Unit

BAC Basic Access Control

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
DECIES	Domain Parameter ECIES
DES	Data Encryption Standard
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECIES	Elliptic Curve Integrated Encryption Scheme
eID	electronic Identity Card
eIDAS	electronic IDentification, Authentication and trust Services
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
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 TOE[8] 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/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1077-2020, Security Target STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1, Version 1.11, 16 July 2020, Giesecke+Devrient Mobile Security GmbH (confidential document)

[7] Security Target Lite BSI-DSZ-CC-1077-2020, Security Target Lite STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1, Version 1.11, 16 July 2020, Giesecke+Devrient Mobile Security GmbH (sanitised public document)

[8] 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

[9] 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

[10] Protection profiles for secure signature creation device – Part 2: Device with key generation, EN 419211-2:2013, CEN/ISSS, BSI-CC-PP-0059-2009-MA-02 (June 2016)

[8] specifically

- 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 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- 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, Reuse of evaluation resultsAIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers

[11] 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

[12] 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

[13] 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

[14] ETR BSI-DSZ-CC-1077-2020, Evaluation Technical Report (ETR) – Summary for STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1, Version 1.2, 27 July 2020, SRC Security Research & Consulting GmbH (confidential document)

[15] Configuration List BSI-DSZ-CC-1077-2020, Configuration List STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1, Version 0.27, 27 July 2020, Giesecke+Devrient Mobile Security GmbH (confidential document)

[16] Guidance Documentation STARCOS 3.7 ID C1 – Main Document, Version 1.0, 17 July 2020, Giesecke+Devrient Mobile Security GmbH

[17] Guidance Documentation for the Usage Phase STARCOS 3.7 ID C1, Version 1.3, 24 July 2020, Giesecke+Devrient Mobile Security GmbH

[18] Guidance Documentation for the Initialisation Phase STARCOS 3.7 ID C1, Version 2.0, 24 July 2020, Giesecke+Devrient Mobile Security GmbH

[19] Guidance Documentation for the Personalisation Phase STARCOS 3.7 ID C1, Version 2.1, 27 July 2020, Giesecke+Devrient Mobile Security GmbH

[20] Application-specific personalisation guidance:

Starcos 3.7 ID nPA - Perso guide, Version 1.10, 17 March 2020, Giesecke+Devrient Mobile Security GmbH

Starcos 3.7 ID eAT - Perso guide, Version 1.40, 17 March.2020, Giesecke+Devrient Mobile Security GmbH

Starcos 3.7 ID ePass - Perso guide, Version 1.20, 17 March 2020, Giesecke+Devrient Mobile Security GmbH

[21] Security Target of the underlying hardware platform, Common Criteria Confidential Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h, H13, Revision 3.3, 22 April 2020, Infineon Technologies AG, BSI-DSZ-CC-1110-V3-2020 (confidential document)

Security Target Lite of the underlying hardware platform, Common Criteria Public Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h H13, Revision 1.8, 22 April 2020, Infineon Technologies AG, BSI-DSZ-CC-1110-V3-2020 (sanitised public document)

[22] Certification Report BSI-DSZ-CC-1110-V3-2020 for Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions from Infineon Technologies AG, 13 May 2020, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[23] ETR for Composite Evaluation of the underlying hardware platform Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h, H13 from certification procedure BSI-DSZ-CC-1110-V3-2020, Version 1, 23 April 2020, TÜV Informationstechnik GmbH (confidential document)

[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

(for Part 1 – 3, Version 2.10, March 2012 is sometimes referenced in international context)

[25] Technische Richtlinie BSI TR-03116 – Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 2: eID-Karten und hoheitliche Dokumente, Stand 2020, 27 January 2020, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[26] ICAO Doc 9303-1, Specifications for electronically enabled passports with biometric identification capabilities. In Machine Readable Travel Documents – Part 1: Machine Readable Passport, Volume 2, 6th edition, 2006, ICAO

[27] ICAO Doc 9303-3, Specifications for electronically enabled official travel documents with biometric identification capabilities. In Machine Readable Travel Documents – Part 3: Machine Readable Official Travel Documents, Volume 2, 3rd edition, 2008, ICAO

[28] ICAO Machine Readable Travel Documents, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, November 2010, ICAO

[29] 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

[30] 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

[31] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2, January 2020

[32] Site Certification Report BSI-DSZ-CC-S-0132-2019 for Giesecke+Devrient Mobile Security GmbH - Development Centre Germany, 4 October 2019, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[33] Site Certification Report CCN-CC-023/2018 for Giesecke+Devrient Mobile Security Iberica S.A.U. - Development Centre Spain, 22 October 2018, National Cryptologic Centre (CCN)

[34] Site Certification Report BSI-DSZ-CC-S-0152-2020 for Giesecke+Devrient Secure Data Management GmbH, 13 March 2020, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[35] Site Certification Report BSI-DSZ-CC-S-0150-2020 for Bundesdruckerei GmbH, 20 April 2020, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[36] Site Certification Report BSI-DSZ-CC-S-0143-2019 for Linxens (Thailand) Co Ltd., 4 December 2019, 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 Lite [7] provided within a separate document

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-1077-2020

Evaluation results regarding development and production environment

The IT product STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1 (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 5 August 2020, 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) Giesecke+Devrient Mobile Security GmbH - Development Centre Germany (DCG) for Development and Testing. Refer to the Certification Report BSI-DSZ-CC-S-0132-2019 ([32]).

b) Giesecke+Devrient Mobile Security Iberica S.A.U. - Development Centre Spain (DCS) for Development. Refer to the Certification Report CCN-CC-023/2018 ([33]).

c) Giesecke+Devrient Secure Data Management GmbH (GDSDM) for Initialisation and Storage. Refer to the Certification Report BSI-DSZ-CC-S-0152-2020 ([34]).

d) Bundesdruckerei GmbH for Initialisation and Inlay Production. Refer to the Certification Report BSI-DSZ-CC-S-0150-2020 ([35]).

e) Linxens Co Ltd. for Initialisation and Inlay Production. Refer to the Certification Report BSI-DSZ-CC-S-0143-2019 ([36]).

f) For development and production sites regarding the underlying IC platform please refer to the Certification Report BSI-DSZ-CC-1110-V3-2020 ([22]).

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6] and [7]. 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] and [7]) are fulfilled by the procedures of these sites.

Annex C of Certification Report BSI-DSZ-CC-1077-2020

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 using SHA-{256, 384, 512}	[ANSI X9.62] (ECDSA) [FIPS180] (SHA) [ECCTR], chapter 4.2 (ECDSA)	Key sizes corresponding to the used elliptic curve brainpool P{256,320,384,512}r1 [RFC 5639]	[ECARDTR], chapter 5.1 [ECCTR]	Verification of certificates in Terminal Authentication FCS_COP.1/ SIG_VER_EAC1PP FCS_COP.1/ SIG_VER_EAC2PP
2		ECDSA signature verification of update packages using SHA-512	[ANSI X9.62] (ECDSA) [FIPS180] (SHA) [ECCTR], chapter 4.2 (ECDSA)	Key sizes corresponding to the used elliptic curve brainpoolP512r1 [RFC 5639]	[UiF]	FCS_COP.1/ UPD_SIG_MREDONPP
3	Authentication	PACEv2 including PACE-CAM	[EACTR], Part 2, chapter 3.2 (PACEv2) [ICAO9303], Part 11, sec. 4.4 (PACE-CAM)	Length of |Nonce| =128 bit Key sizes corresponding to the used elliptic curve brainpool P{256,320,384,512}r1 [RFC 5639]	[EACTR], Part 2, chapter 3.2 [ICAO9303], Part 11, sec. 4.4	FCS_CKM.1/ DH_PACE_EAC1PP FCS_CKM.1/ DH_PACE_EAC2PP FCS_CKM.1/CAM FCS_COP.1/CAM
4		Chip Authentication CA1	[ECCTR]	Key sizes corresponding to the used elliptic curve brainpool P{256,320,384,512}r1 [RFC 5639]	[EACTR], Part 3, chapter A.4 [EACTR], Part 1, chapter 3.4	FCS_CKM.1/CA_EAC1PP
5		Chip Authentication CA2	[EACTR], Part 2, chapter 3.4	Key sizes corresponding to the used elliptic curve brainpool P{256,320,384,512}r1 [RFC 5639]	[EACTR], Part 3, chapter A.4 [ECARDTR], chapter 5.1	FCS_CKM.1/ DH_PACE_EAC2PP (This SFR applies also for Chip Authentication v2, cf. Application Note 12 from [EAC2-PP].) FTP_ITC.1/ UPD_ITC_MREDONPP
6		Chip Authentication CA3	[EACTR], Part 2, chapter 3.5	Key sizes corresponding to the used elliptic curve brainpool P{256,320,384,512}r1 [RFC 5639]	[EACTR], Part 2, chapter 3.5 [EACTR], Part 3, chapter A.4.2.3	FCS_CKM.1/CA3 FCS_COP.1/CA3
7		Terminal Authentication v1	[EACTR], Part 1, chapter 3.5	Key sizes corresponding to the used elliptic curve brainpool P{256,320,384,512}r1 [RFC 5639]	[EACTR], Part 3, chapter A.7 [ECARDTR], chapter 5.1	FIA_UAU.1/PACE_EAC1PP FIA_UAU.5/PACE_EAC1PP
8		Terminal Authentication v2	[EACTR], Part 2, chapter 3.3	Key sizes corresponding to the used elliptic curve brainpool P{256,320,384,512}r1 [RFC 5639]	[EACTR], Part 3, chapter A.7 [ECARDTR], chapter 5.1	FIA_UAU.1/ EAC2_Terminal_EAC2PP FIA_UAU.5/PACE_EAC2PP
9	Key Agreement	ECDH For PACE and Chip	[ECCTR] (ECDH)	Key sizes corresponding to	[EACTR], Part 3, chapter A.4	FCS_CKM.1/ DH_PACE_EAC1PP

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application / Security Level	Comments
		Authentication v1 and v2		the used elliptic curve brainpool P{256,320,384,512}r1 [RFC 5639]		FCS_CKM.1/CA_EAC1PP FCS_CKM.1/ DH_PACE_EAC2PP FCS_CKM.1/CAM
10		ECDH For Chip Authentication v3	[ECCTR] (ECDH)	Key sizes corresponding to the used elliptic curve brainpool P{256,320,384,512}r1 [RFC 5639]	[EACTR], Part 2, chapter 3.5 [EACTR], Part 3, chapter A.4.2.3	FCS_CKM.1/CA3
11		ECDH Trusted channel for Updates in Field	[EACTR], Part 2, chapter 3.2 (PACEv2)	Key sizes corresponding to the used elliptic curve brainpool P512r1 [RFC 5639]	[UiF] [EACTR], Part 3, chapter A.4	FCS_CKM.1/ UPD_ITC_MREDONPP
12		ECKA For derivation of AES keys	[EACTR], Part 2, chapter 3.2 (PACEv2)	|k|=256	[UiF] [EACTR], Part 3, chapter A.4	FCS_CKM.1/ UPD_DEC_MREDONPP FCS_CKM.1/ UPD_INT_MREDONPP
13	Confidentiality	Encryption and decryption with 3DES in CBC mode	[FIPS46-3] (DES) [SP800-38A], sec. 6.2 (CBC)	|k|=112	[EACTR], Part 3, Annex F [ICAOSAC]	Secure Messaging FCS_COP.1/ CA_ENC_EAC1PP
14		Encryption and decryption with AES in CBC mode	[FIPS197] (AES) [SP800-38A], sec. 6.2 (CBC)	|k|=128, 192, 256	[EACTR], Part 3, Annex F [ICAOSAC] [UiF]	Secure Messaging FCS_COP.1/ PACE_ENC_EAC1PP FCS_COP.1/ PACE_ENC_EAC2PP FCS_COP.1/ CA_ENC_EAC1PP FCS_COP.1/ UPD_ITC_MREDONPP
15		Decryption of update packages with AES in OFB mode	[FIPS197] (AES) [SP800-38A] (OFB)	|k|=256	[UiF]	Decryption of update packages FCS_COP.1/ UPD_DEC_MREDONPP
16	Integrity	3DES in Retail-MAC mode	[FIPS46-3] (DES) [ISO9797], algorithm 3 (Retail-MAC)	|k|=112	[EACTR], Part 1 [ICAOSAC]	Secure Messaging FCS_COP.1/ CA_MAC_EAC1PP
17		AES in CMAC mode	[FIPS197] (AES) [SP800-38B] (CMAC)	|k|=128, 192, 256	[EACTR] [ECARDTR], chapters 3.2, 4.2.1 [UiF]	Secure Messaging FCS_COP.1/ PACE_MAC_EAC1PP FCS_COP.1/ PACE_MAC_EAC2PP FCS_COP.1/ CA_MAC_EAC1PP FCS_COP.1/ UPD_ITC_MREDONPP
18	Integrity Verification	SHA-256	[FIPS180]	n.a.	[UiF]	Integrity verification of update packages FCS_COP.1/ UPD_INT_MREDONPP
19	Trusted Channel	Secure messaging in ENC_MAC mode established during PACE	[EACTR]	n.a.	[EACTR]	FTP_ITC.1/PACE_EAC1PP FTP_ITC.1/PACE_EAC2PP
20		Secure messaging in	[EACTR], Part 1,	n.a.	[EACTR], Part	FCS_COP.1/

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application / Security Level	Comments
		ENC_MAC mode established during Chip Authentication CA1 after PACE	chapter 3.4		3, chapter A.4 [ECARDTR], chapter 5.1	CA_ENC_EAC1PP FCS_COP.1/ CA_MAC_EAC1PP
21		Secure messaging in ENC_MAC mode established during Chip Authentication v2 after PACE	[EACTR], Part 2, chapter 3.3	n.a.	[ICAO9303] [EACTR], Part 1 [ECARDTR], chapter 3.2, 4.2	FTP_ITC.1/CA_EAC2PP
22		Secure messaging in ENC_MAC mode established during Chip Authentication CA3 after PACE	[EACTR], Part 2, chapter 3.5	n.a.	[EACTR], Part 2, chapter 3.5	FTP_ITC.1/CA3
23	Cryptographic Primitive	Deterministic RNG DRG.4	[AIS20] [AIS31] [ISO18031], Appendix C.3.2	n.a.	[ECARDTR], chapter 1.3.3, 8.3, 8.4	Generation of the random nonce for PACE; CA and TA FCS_RND.1/EAC2PP
24		Hash for key derivation SHA-{1, 224, 256, 384, 256}	[FIPS180]	n.a.	[ECARDTR]	FCS_COP.1/SHA_EAC2PP See also above in rows 1, 2, 7, 8, 9, 10, 11, 12 and 18
25		ECDSA signature generation using SHA-{256, 384, 512}	[ANSI X9.62] (ECDSA) [FIPS180] [ECCTR], chapter 4.2	Key sizes corresponding to the used elliptic curve brainpool P{256,320,384,512}r1 [RFC 5639]	Security level > 100 bit	FCS_COP.1/SSCDPP
26		ECC Key generation for ECDH and ECDSA	[ECCTR], chapter 4.2	Key sizes corresponding to the used elliptic curve brainpool P{256,320,384,512}r1 [RFC 5639]	Security level > 100 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_MREDONPP 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 6: TOE cryptographic functionality

Bibliography for Table 6:

[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)

[ANSIX9.62] American National Standard X9.62, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), November 2005, ANSI

[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

[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

(for Part 1 – 3, Version 2.10, March 2012 is sometimes referenced in international context)

[ECARDTR] Technische Richtlinie BSI TR-03116 – Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 2: eID-Karten und hoheitliche Dokumente, Stand 2020, 27 January 2020 9, 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)

[FIPS46-3] Federal Information Processing Standards Publication FIPS PUB 46-3, Data Encryption Standard (DES), Reaffirmed October 25 1999, U.S. Department of Commerce/National Institute of Standards and Technology

[FIPS180] Federal Information Processing Standards Publication 180-4 (FIPS PUB 180-4), Secure Hash Standard (SHS), August 2015, U.S. Department of Commerce/National Institute of Standards and Technology (NIST)

[FIPS197] Federal Information Processing Standards Publication 197 (FIPS PUB 197), Advanced Encryption Standard (AES), November 2001, U.S. Department of Commerce/National Institute of Standards and Technology (NIST)

[ICAO9303] ICAO Doc 9303, Machine Readable Travel Documents, Seventh Edition, 2015, ICAO

[ICAOSAC] ICAO Machine Readable Travel Documents, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, November 2010, ICAO

[ISO18031] ISO/IEC 18031:2005, Information technology – Security techniques – Random bit generation, 2005, ISO

[ISO9797] ISO 9797-1:1999, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, January 2005, ISO

[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, 2001, National Institute of Standards and Technology (NIST)

[SP800-38B] Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, 2005, National Institute of Standards and Technology (NIST)

[UiF] UiF Konzept, Version 1.2, 7 November 2018, Giesecke+Devrient Mobile Security GmbH

Note: End of report