Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1118-2020

for

TCOS CSP Module Version 1.0 Release 1/P6022y

from

T-Systems International 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-1118-2020 (*)

TCOS CSP Module Version 1.0 Release 1/P6022y

from	T-Systems International GmbH
PP Conformance:	Cryptographic Service Provider (CSP) Version 0.9.8, 19 February 2019, BSI-CC-PP-0104-2019, Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au) Version 0.9.5, 8 April 2019, BSI-CC-PP-0107-2019
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant / extended EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5

SOGIS
Recognition Agreement

Common Criteria

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.

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

Bonn, 7 April 2020

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

L.S.

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

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]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [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] 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 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+ ALC_FLR components.

[4] Proclamation of the Bundesministerium des Innern 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 CSP Module Version 1.0 Release 1/P6022y has undergone the certification procedure at BSI. Specific results from the evaluation process BSI-DSZ-CC-1078 were re-used.

The evaluation of the product TCOS CSP Module Version 1.0 Release 1/P6022y was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 1 April 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: T-Systems International GmbH.

The product was developed by: T-Systems International 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 7 April 2020 is valid until 6 April 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

[5] Information Technology Security Evaluation Facility

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 TCOS CSP Module Version 1.0 Release 1/P6022y 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] T-Systems International GmbH
Untere Industriestraße 20
57250 Netphen

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 CSP Module Version 1.0 Release 1/P6022y provided by T-Systems International GmbH, based on the hardware platform P6022y by NXP.

The Target of Evaluation (TOE) is a Cryptographic Service Provider (CSP) representing a smart card with contact based interfaces programmed according to [8] (first PP in reference) with the Timestamp and Audit functionality according to [8] (second PP module in reference). The cryptographic services for users comprise

- authentication of users,
- authentication and attestation of the TOE to entities,
- data authentication and non-repudiation including time stamps,
- encryption and decryption of user data,
- trusted channel including mutual authentication of the communicating entities, encryption and message authentication proof for the sent data, decryption and message authentication verification for received data,
- management of cryptographic keys with security attributes including key generation, key derivation and key agreement, internal storage of keys, import and export of keys with protection of their confidentiality and integrity,
- generation of random bits which may be used for security services outside the TOE.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile and accompanying Module Cryptographic Service Provider (CSP) Version 0.9.8, 19 February 2019, BSI-CC-PP-0104-2019, Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au) Version 0.9.5, 8 April 2019, BSI-CC-PP-0107-2019 [8].

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 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.

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

TOE Security Functionality	Addressed issue
Key Management	The TOE implements several management functions on/with the cryptographic keys and enforce the access control security functional policies of subject on the objects (cryptographic keys). The TOE implements the functionality via the Export Key, Import Key and key management commands. Several cryptographic means and primitives support these services.
Data Encryption	The TOE provides the symmetric encryption algorithm AES with standardized key lengths of

TOE Security Functionality	Addressed issue
	128 and 256 bits.
Hybrid Encryption with MAC for User Data	The TOE provides hybrid data encryption/decryption and MAC calculation/verification of user data.
Data Integrity Mechnisms	The TOE implements cryptographic checksum functions, including hash functions used for message authentication codes (MACs). Digital signature generation and verifications is also implemented by the TOE
Authentication and Attestation of the TOE, Trusted Channel	The TOE supports secure data exchange in a trusted channel secured by cryptographic operations. The TOE enforces a protected communication by means of the PACE or Chip Authentication protocol. The trusted channel supports confidential information exchange which integrity is assured. Additionally the TOE supports attestation to ensure that the sample is a genuine sample of the certified product.
User Identification and Authentication	The TOE implements protocols for identification and authentication of users and devices.
Security Management	The TOE supports the management of security functions and its behavior.
Access Control	The access to User Data is restricted by an access control policy.
Security Audit	The TOE supports audit data generation on occurrence of several auditable events. Event data are stored in an audit trail and can be exported later.
Protection of the TSF	The access to cryptographic keys is restricted by defined rules and measures.
Import and Verification of Update Code Package	The TOE provides the functionality to load update code packages in the operational phase.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 6.1.

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 also outlined in the Security Target [6], chapter 6.

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 CSP Module Version 1.0 Release 1/P6022y.

The following table outlines the TOE deliverables:

Type	Delivery Item	Release	Form of Delivery
HW/SW	NXP Secure Smart Card Controller P6022y VB including its IC Dedicated Support Software embedded into modules	(see HW platform BSI-DSZ-CC-1059-V2-2019) P60D145 Delivery type: Wafer, Ux Sawn Wafer, Ux HVQFN32 SMD, HN HX2QFN14 SMD, HQ Module, Xx	The hardware part of the TOE is delivered by the HW Manufacturer in an insured parcel to the Installation Agent. In the life cycle of the TOE the hardware is always protected by an authentication procedure.
SW	Operating System and File System (TOE Embedded Software)	TOE Embedded Software (the operating system and completion data) TCOS CSP Module Version 1.0 Release 1/P6022y ROM Mask: CSP_01BE_ID2.0_ROM_Daten_01.hex EEPROM-Image: CSP_01BE_ID2.0_EEPR_Dat02_KV00.hex OS Version: 01 BE Completion Code Version: 41 File System Version: 01	The software part of the TOE is implemented in ROM/EEPROM of the IC, see above. The OS and Filesystem are installed on the HW Platform by Wafer-Initialization by the HW Manufacturer.
DOC	Associated guidance documentation (Usage Guidance)	TCOS Cryptographic Service Provider Version 2.0 Release 1/P6022y TCOS Cryptographic Service Provider Version 2.0 Release 1/P6022y User guidance manual, Version 1.0.4, 24.03.2020	The guidance document of the TOE are delivered always in an encrypted and signed form. Therefore the integrity and authenticity (key validation) can be ensured during the delivery.
DOC	Associated guidance documentation (Personalization Guidance)	TCOS CSP Module Personalization Guidance, Version 1.4, 04.03.2020	The guidance document of the TOE are delivered always in an encrypted and signed form. Therefore the integrity and authenticity (key validation) can be ensured during the delivery.

Type	Delivery Item	Release	Form of Delivery
DOC	Public part of the Attestation key	The key is intended for the (extended) device attestation as genuine sample of the certified product	The public key part of the attestation key for device attestation as genuine sample of the certified product is published in [11] (see bibliography).
DOC	Initial User Admin password value	Initial password value to check that the TOE is in initial state and to change the User Admin password to the operational value	Textfile that contains the intial user admin password value as one line of hex-coded bytes. The Textfiles are delivered always in an encrypted and signed form. Therefore the integrity and authenticity (key validation) can be ensured during the delivery.
DOC	Secret Key Derivation Key -– HMAC	The Key is used for Key derivation according to [11], chapter 8.1.5.6.	Textfile that contains the Secret Key Derivation Key content as one line of hex-coded bytes. The Textfiles are delivered always in an encrypted and signed form. Therefore the integrity and authenticity (key validation) can be ensured during the delivery.

Table 2: Deliverables of the TOE

Note that the private signature key for update packets is not part of the TOE delivery, since it is used only by the developer to sign update code packages.

Regarding TOE delivery:

- Delivery of sensitive electronic data and guidance documentation: Performed via encrypted email.
- Delivery of physical TOE to Installation Agent: The chip hardware is produced by the Hardware Manufacturer and shipped to the Installation Agent.

Regarding TOE identification:

The TOE embedded software consists of the operating system TCOS CSP Module Version 1.0 Release 1/P6022y, completion data and file system. The user can use the 'Compute Attestation' command as described in sec. 7.11 [11] to read out the chip information and identify the chip as well as Embedded Software embedded in the chip

Additionally a digital signature over qualified user data as provided in the command-APDU and the Chip information data is given in the response, see [11] section 4.7.2.2.1 for more details.

3. Security Policy

The security policy enforced is defined by the selected set of Security Functional Requirements and implemented by the TOE. 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 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, random numbers generation as well as specific cryptographic services 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 sec. 6 of the Security Target [6].

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:

Security Objectives for the operational environment defined in Security Target	**Description according to [6]**	**Reference to Guidance [11]**
OE.CommInf Communication infrastructure	The operational environment shall provide public key infrastructure for entities in the communication networks. The trust centers generate secure certificates for trustworthy certificate holder with correct security attributes. They distribute securely their certificate signing public key for verification of digital signature of the certificates and run a directory service for dissemination of certificates and provision of revocation status information of certificates.	9.1
OE.AppComp Support of the Application component	The Application component supports the TOE for communication with users and trust centers.	9.2
OE.SecManag Security management	The operational environment shall implement appropriate security management for secure use of the TOE including user management, key management. It ensures secure key management outside the TOE and uses the trust center services to determine the validity of certificates. The cryptographic keys and cryptographic key components shall be as-signed to the secure cryptographic mechanisms they are intended to be used with and to the entities authorized for their use.	9.3
OE.SecComm Protection of communication channel	Remote entities shall support trusted channels with the TOE using cryptographic mechanisms. The operational environment shall protect the local communication channels by trusted channels using cryptographic mechanisms or by secure channel using non-cryptographic security measures.	9.4
OE.SUCP Signed Update Code Packages	The secure Update Code Package is delivered in encrypted form and signed by the authorized issuer together with its security at-tributes.	9.5
OE.Audit Review and availability of audit records	The administrator shall ensure the regular audit review and the availability of exported audit records.	9.6
OE.TimeSource External time source	The operational environment provides reliable external time source for the adjustment of the TOE internal time source.	9.7

Table 3: Security Objectives for the operational environment

Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

Detailed information on the TOE architecture can be found in the Security Target [6], section 1.3.

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.

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 its expected behaviour including error cases. Hereby a representative sample including all boundary values of the parameter set, 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 were performed during the independent evaluator tests.

During their independent testing, the ITSEF covered

- commands related to Key Management,
- commands related to Data Encryption,
- commands related to Hybrid Encryption with MAC for User Data,
- commands related to Data Integrity Mechanisms,
- commands related to Authentication and Attestation of the TOE, Trusted Channel,
- commands related to User Identification and Authentication,
- commands related to Security Management,
- commands related to Access Control,
- commands related to Security Audit,
- commands related to Protection of the TSF,
- commands related to Import and Verification of Update Code Package

and also conducted

- penetration testing related to verify the Reliability of the TOE,
- source code analysis,
- testing the commands which are used to execute the different PACE,
- side channel analyses and
- fault injection attacks.

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 configurations of the TOE:

Regarding the Hardware:

- TCOS CSP Module Version 1.0 Release 1/P6022y.

Regarding the documents:

- TCOS CSP Module Version 1.0 Release 1/P6022y, Guidance Documentation [11],
- TCOS CSP Module Version 1.0 Release 1/P6022y, Exemplary TOE Personalization in Usage Phase [12].

The user can use the ‘Compute Attestation’ command to read out the chip information and identify the chip. The parameters and the command are described in sec 7.11 of [11].

The above mentioned identification data must comply with the data given in Annex B of [11] in order for the TOE be verified as certified version, i.e.:

Data Type	Data
Chip Manufacturer	0x04
Chip Type	0x30
Card Type	0x14
OS / ROM Mask Version	0x01BE
(Pre-) completion code version	0x41
File System Version	0x01

Table 4: TOE Identification

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 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the scheme and technology was used:

AIS:

- Durchführung der Ortsbesichtigung in der Entwicklungsumgebung, AIS 1, Version 14, 11.10.2017, Bundesamt für Sicherheit in der Informationstechnik
- Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC, AIS14, Version 7, 03.08.2010, Bundesamt für Sicherheit in der Informationstechnik

- Gliederung des ETR, AIS19, Version 9, 03.11.2014, Bundesamt für Sicherheit in der Informationstechnik
- Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, AIS20, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik
- Anwendung der CC auf integrierte Schaltungen, AIS25, Version 9, 15.03.2017, Bundesamt für Sicherheit in der Informationstechnik
- Evaluationsmethodologie für in Hardware integrierte Schaltungen, AIS26, Version 10, 03.07.2017, Bundesamt für Sicherheit in der Informationstechnik
- Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, AIS31, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik
- CC-Interpretationen im deutschen Zertifizierungsschema, AIS32, Version 7, 08.06.2011, Bundesamt für Sicherheit in der Informationstechnik
- Evaluierungsmethodologie für die Vertrauenswürdigkeitsklasse EAL5+, AIS34, Version 3, 03.09.2009, Bundesamt für Sicherheit in der Informationstechnik
- Öffentliche Fassung eines Security Target (ST-lite), AIS35, Version 2, 12.11.2007, Bundesamt für Sicherheit in der Informationstechnik
- ETR-Zusatz zur Unterstützung von Smartcard Kompositionszertifizier-ungen (ETR for composition), AIS36, Version 5, 15.03.2017, Bundesamt für Sicherheit in der Informationstechnik
- Terminologie und Vorbereitung von Smartcard-Evaluierungen, AIS37, Version 3, 17.05.2010, Bundesamt für Sicherheit in der Informationstechnik
- Wiederverwendung von Evaluierungsergebnissen, AIS38, Version 2.9, 08.06.2011, Bundesamt für Sicherheit in der Informationstechnik
- Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengenerator-en, AIS46, Version 3, 04.12.2013, Bundesamt für Sicherheit in der Informationstechnik
- Regelungen zur Zertifizierung von Entwicklungs- und Produktionsstandorten nach Common Criteria (Site Certification), AIS47, Version 1.1, 04.12.2013, Bundesamt für Sicherheit in der Informationstechnik

Other relevant evaluation guidance or documentation:

- JIL Minimum Site Security Requirements, Version 2.1 , April 2018
- Joint Interpretation Library, Application of Attack Potential to Smart-cards, Joint Interpretation Working Group, Version 2.9, 2013-01.
- Joint Interpretation Library, Security Architecture requirements (ADV_ARC) for smart cards and similar devices, Joint Interpretation Working Group, Version 2.0, 2012-01.
- Joint Interpretation Library, Attack Methods for Smartcards and Similar Devices, Joint Interpretation Working Group, Version 2.2, January 2013
- Composite product evaluation for Smart Cards and similar devices, Joint Interpretation Working Group, Version 1.5, October 2017

A document ETR for composite evaluation according to AIS 36 has not been provided in the course of this certification procedure.

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 and AVA_VAN.5 augmented for this TOE evaluation.

The evaluation work performed for this certification procedure was carried out with re-use of specific parts of the procedure BSI-DSZ-CC-1078. Re-use was employed regarding

- the cryptographic functionality,
- the UCP (Update Code Package) functionality.

The evaluation has confirmed:

- PP Conformances: Cryptographic Service Provider (CSP) Version 0.9.8, 19 February 2019, BSI-CC-PP-0104-2019,
  Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au) Version 0.9.5, 8 April 2019, BSI-CC-PP-0107-2019 [8]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant / extended
  EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5

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 strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But 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 crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

Purpose	**Cryptographic Mechanism**	**Standard of Implementation**	**Key Size in Bits**	**Standard of Application / Security Level**	**Comments**
Authenticity	ECDSA signature-creation and	[ANSX9.63], [SP800-56C], [RFC 5639],	Key sizes corresponding to the elliptic curves brain-	[ECARDTR]	FCS_COP.1/CDS-ECDSA,

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application / Security Level	Comments
	verification	[FIPS186]	poolP{192, 224, 256, 320, 384, 512}{r, t}1 [RFC 5639], ansix9p{192, 256 384}r1 [FIPS186]		FCS_COP.1/VDS-ECDSA
Authenticity	RSA EMSA-PSS signature-creation and verification	[ISO14888-2], [RFC8017]	2048, 3072 bits	[ECARDTR]	FCS_COP.1/CDS-RSA, FCS_COP.1/VDS-RSA
Authenticity	Signature verification of the Update Code Package with ECDSA using SHA-512	[ECCTR], sec. 4.2.1, [FIPS 180-4], [RFC 5639]	key sizes corresponding to the elliptic curve brainpoolP512t1	[UiF], sec. 2.3.3 Security Level > 100 Bit	FCS_COP.1/ VDSUCP
Authentication	Terminal Authentication version 2	[EACTR], sec. 3.3	128 bits, 256 bits	[EACTR], sec. 3.3	FIA_API.1/TA FCS_CKM.1/ TCAP
Authentication	Chip Authentication Version 2	[EACTR], sec. 3.4	128 bits, 256 bits	[EACTR], sec. 3.4	FIA_API.1/CA FCS_CKM.1/ TCAP
Cryptographic Primitive	Hash generation with SHA-256, SHA-384 and SHA-512	[FIPS 180-4]	--	[CSPPP]	FCS_COP.1/Hash
Key derivation	AES key generation using bit string derived from input parameters with DKDF_NIST_800_108	[SP 800-108]	128 bits, 256 bits	[CSPPP]	FCS_CKM.5/AES
Key derivation	ECC key pair generation using bit string derived from input parame-ters with DKDF_ECC_PRF	[SP800-56C], [RFC 5639], [TR-03111], section 4.1.3	Key sizes corresponding to the elliptic curves brainpoolP{192, 224, 256, 320, 384, 512}{r, t}1 [RFC5639], ansix9p{192, 256 384}r1 [FIPS186]	[TR-03111]	FCS_CKM.5/ECC

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application / Security Level	Comments
Key derivation	Derivation of AES-128, AES-256 keys from ECC key with ECKGA-EG and X9.6 3 Key Derivation Function	[RFC 5639], [TR-03111], section 4.1.3 and section 4.3.2.2	Key sizes corresponding to the elliptic curves brainpoolP{192, 224, 256, 320, 384, 512}{r, t}1 [RFC 5639], ansix9p{192, 256 384}r1 [FIPS186]	[TR-03111]	FCS_CKM.5/ ECKA-EG
Key derivation	Derive cryptographic keys from seed for AES-128, AES-256 keys with X9.63 Key Derivation Function and RSA EME-OAEP	[ANSI-X9.63], [RFC8017], chapter 3.5, [ISO18033-3]	seed-length=256 bits RSA key size 2000-3000 bit	[CSPPP]	FCS_CKM.1/ AES_RSA for AES key derivation with X9.63 from seed and seed encryption with RSA EME-OAEP and FCS_CKM.5/ AES_RSA for seed decryption with RSA EME-OAEP and AES key derivation with X9.63 from decrypted seed
Key generation	Seed generation for hybrid data encryption/decryption with data integ-rity	TCOS RNG [RNG]	256 bits	[CSPPP]	FCS_CKM.1/ AES_RSA for seed generation
Key agreement	PACE with Generic Mapping in ICC role	[ICAO9303], Part 11, section 4.4, [RFC 5639], [FIPS186]	Key sizes corresponding to the elliptic curves brainpoolP{192, 224, 256, 320, 384,512}{r, t}1 [RFC 5639], ansix9p{192, 256 384}r1 [FIPS186]	[EACTR]	FIA_API.1/PACE FCS_CKM.1/ PACE
Confidentiality	symmetric data encryption and decryption according to AES-128 and AES-256 in CBC	[SP800-38A], [ISO18033-3], [ISO10116], [FIPS197]	128 bits, 256 bits	[ECARDTR]	FCS_COP.1/ED FCS_COP.1/TCE AES is provided by the HW platform and covered by the HW certificate.

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application / Security Level	Comments
Confidentiality	hybrid data encryption and decryption with asymmetric key encryption according to FCS_CKM.1/ECKA-EG or FCS_CKM.1/AES_RSA and symmetric data encryption according to AES-128, AES-256 in CBC	[FIPS197] [SP800-38A] [ISO18033-3], [ISO10116], [FIPS197]	128 bits, 256 bits asymmetric key sizes see FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA	[CSPPP]	FCS_COP.1/HEM FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA AES is provided by the HW platform and covered by the HW certificate.
Confidentiality	encryption and decryption using PUF	[HWST]	128 bit	Security Level > 100 Bit	FCS_COP.1/SDE This cryptographic mechanism is provided by the under-lying HW platform and covered by the HW certificate.
Confidentiality	AES decryption of authentic encrypted Update Code Package with AES-256 in OFB mode	[FIPS197], [SP800-38A]	256 bit	[UiF], sec. 2.3.3	FCS_COP.1/DecUCP AES is provided by the HW platform and covered by the HW certificate.
Integrity	hybrid MAC calculation and verification with asymmetric key encryption according to FCS_CKM.1/ECKA-EG or FCS_CKM.1/AES_RSA and AES-128, AES-256 in CMAC	[FIPS197] [NIST-SP800-38B] [ISO18033-3], [ISO10116], [FIPS197]	128 bits, 256 bits asymmetric key sizes see FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA	[CSPPP]	FCS_COP.1/HEM FCS_COP.1/HDM FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA AES is provided by the HW platform and covered by the HW certificate.

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application / Security Level	Comments
Integrity	MAC generation and verification with AES-128 and AES-256 CMAC	[FIPS197], [NIST-SP800-38B], [ISO9797-1], [SP800-38D]	128 bits, 256 bits	[ECARDTR]	FCS_COP.1/MAC FCS_COP.1/TCM AES is provided by the HW platform and covered by the HW certificate.
Integrity	HMAC generation and verification with HMAC-SHA256	[RFC2104], [ISO9797-2], [FIPS 180-4]	128 bits, 256 bits	[ECARDTR]	FCS_COP.1/ HMAC
Confidentiality	Key wrapping and unwrapping with AES-Keywrap	[SP800-38F], [FIPS197]	128 bits, 256 bits	[CSPPP]	FCS_COP.1/KW, FCS_COP.1/KU AES is provided by the HW platform and covered by the HW certificate.
Key Generation	ECC key pair generation	[RFC5639], [TR-03111] section 4.1.3, [FIPS186-4] section B.4 and D.1.2.3	Key sizes corresponding to the elliptic curves brainpoolP{192, 224, 256, 320, 384, 512}{r, t}1 [RFC5639], ansix9p{192, 256 384}r1 [FIPS186]	[CSPPP]	FCS_CKM.1/ECC FCS_CKM.1/ ECKA-EG See also BSI-DSZ-CC-1078.
Key Generation	RSA key pair generation	[RFC8017]	2048, 3072 bits	[CSPPP]	FCS_CKM.1/RSA See also BSI-DSZ-CC-1078.

Table 5: TOE cryptographic functionality

Regarding cryptographic aspects of UCP (Update Code Package) see BSI-DSZ-CC-1078.

List of referened documents and standards:

[ECCTR] Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018-06-01

[TR-03111] See [ECCTR]

[ECARDTR] Technische Richtlinie BSI TR-03116Kryptographische Vorgaben für Projekte der Bundesregierung Teil 5: Anwendungen der Secure Ele-ment API, Stand 2020, Datum: 27. Januar 2020

[TR02102] Technische Richtlinie TR-02102 Kryptographische Verfahren Empfehlungen und Schlüssellängen, Version 2019-01, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2019-02-22

[EIDAS] 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, 2014-08-28

[FIPS46] Federal Information Processing Standards Publication FIPS PUB 46-3, Data Encryption Standard (DES), Reaffirmed 1999 October 25, U.S. DoC/NIST

[FIPS180] Federal Information Processing Standards Publication FIPS PUB 180-4, Specifications for the Secure Hash Standard (SHS), March 2012

[FIPS180-4] See [FIPS180]

[FIPS186] Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), 2013-07

[FIPS186-4] See [FIPS186]

[FIPS197] Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), U.S. Department of Commerce/National Institute of Standards and Technology, 2001-11-26

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, IETF, 1997-02

[RFC5639] M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, IETF, 2010-03

[RFC8017] K. Moriarty, B. Kaliski, J. Jonsson, A. Rusch, PKCS #1: RSA Cryptog-raphy Specifications Version 2.2, RFC 8017, IETF, 2016-11

[SP800-38A] Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST Special Publication 800-38A, National Institute of Standards and Technology, 2001-12

[SP800-38B] ISO 15946, Information technology – Security techniques – Crypto-graphic techniques Recommendation for Block Cipher Modes of Oper-ation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, National Institute of Standards and Technology, May 2005

[SP800-38D] Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, NIST Special Publication 800-38D, National Institute of Standards and Technology, 2007-11

[SP800-38F] Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, NIST Special Publication 800-38F, National Institute of Standards and Technology, 2012-12

[SP800-56C] Recommendation for Key-Derivation Methods in Key-Establishment Schemes Rev.1, NIST Special Publication 800-56C, National Institute of Standards and Technology, 2018-04

[SP800-67] Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST Special Publication 800-67, Revised January 2012, National Institute of Standards and Technology, 2012-01

[ICAO9303] ICAO Doc 9303, Machine Readable Travel Documents, Seventh Edi-tion, 2015

[SP800-108] NIST Special Publication 800-108: “Recommendation for Key Derivation Using Pseudorandom Functions”, October 2009

[ISO9796-2] ISO/IEC 9796-2:2010 Information technology—Security techniques—Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, ISO, 2010-12

[ISO9797] ISO 9797-1:1999, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, ISO, 2005-01-04

[ISO9797-2] ISO/IEC 9797-2:2011, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function, ISO, 2011-05

[ISO10116] ISO/IEC 10116:2017, Information technology – Security techniques – Modes of operation for an n-bit block cipher, 2017-07

[ISO14888-2] ISO/IEC 14888-2:2008, Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms, ISO, 2008-04

[ISO18033-3] ISO/IEC 18033-3:2010 Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers, ISO, 2010-12

[ISO15946] ISO 15946, Information technology – Security techniques – Crypto-graphic techniques based on elliptic curves, 2002

[ANSX9.63] American National Standard X9.63-2001, Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Us-ing Elliptic Curve Cryptography, 2005-11

[UiF] Update im Feld unter TCOS CSP Module 1.0 R1, T-Systems International GmbH, Version 0.2, 11.10.2019 (confidential document)

[RNG] Zufallszahlengenerierung in TCOS,Version 1.01, 21.02.2019 (confidential document)

[HWST] NXP Secure Smart Card Controller P6022y VB Security Target Lite, V 2.2, 27 November 2018, BSI-DSZ-CC-1059-V2-2019, NXP Semiconductors

[CSPPP] See [8] in bibliography

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, especially

- document [11] (for proper usage/handling) and
- document [12] (for proper personalization).

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.

Also note that the UCP (Update Code Package) mechanism itself (as described in [13]) is certified according to this certificate's evaluation assurance level and the respective Security Target's Security Functional Requirements. However, installation and usage of other TOE configuration items than specified in the Security Target ([6]) (and thus evaluated during the course of this certification) will void the certification status. Recertifications are required in order to maintain a valid certification status in cases where such TOE changes are to be applied. As a consequence, only certified updates of the TOE should be used via a respective UCP deployment procedure. If non-certified Update Code Packages are available, TOE user discretion is advised on whether the sponsor should provide a re-certification. In the meantime a risk management process of the system using the TOE should examine and decide on the usage of not yet certified updates and patches. Or take additional measures in order to maintain overall system security.

Some security measures require additional configuration or control or measures to be followed by a product layer on top. For this reason the TOE includes usage- and configuration guidance documentation (see table 2) which contain obligations and guidelines for the developer of the product layer on top on how to securely use this certified TOE and which measures have to be taken. In the course of the inclusion of the TOE into the top layer product or system it must be ensured that the required measures have been correctly and effectively followed. This is in line with preliminaries laid out in the document for the “coordinated PP” concept [9].

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)

None.

13. Definitions

13.1. Acronyms

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
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation

cPP	Collaborative Protection Profile
CSP	Cryptographic Service Provider
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UCP	Update Code Package

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, Rev. 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[7] 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-1118-2020, Version 1.0.1, 27.02.2020, “Specification of the Security Target TCOS CSP Module Version 1.0 Release 1/P6022y”, T-Systems International GmbH

[7] Evaluation Technical Report, Version 1.2, 01.04.2020, “Evaluation Report – Evaluation Technical Report (ETR) - TCOS CSP Module Version 1.0 Release 1/P6022y”, SRC Security Research & Consulting, (confidential document)

[8] Protection Profile (PP-0104) and Protection Profile-Module (PP-0107): Cryptographic Service Provider (CSP) Version 0.9.8, 19 February 2019, BSI-CC-PP-0104-2019,
Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au) Version 0.9.5, 8 April 2019, BSI-CC-PP-0107-2019

[9] “Evaluation Methodology for Protection Profiles Security Elements with Application Separation”, v0.1.3, 21.12.2017, Bundesamt für Sicherheit in der Informationstechnik (document can be requested from BSI)

[10] Configuration list for the TOE, “Konfigurationsliste von TCOS CSP Module Version 1.0 Release 1/NXP P60D145 VB”, 24.03.2020, v1.0.1, T-Systems International GmbH (confidential document)

[11] “TCOS Cryptographic Service Provider Version 2.0 Release 1/P6022yTCOS Cryptographic Service Provider Version 2.0 Release 1/P6022y User guidance manual”, Version 1.0.4, 24.03.2020, T-Systems International GmbH (confidential document)

[12] “TCOS CSP Module Personalization Guidance”, Version 1.4, 04.03.2020, T-Systems International GmbH (confidential document)

[13] “Update im Feld unter TCOS CSP Module 1.0 R1”, T-Systems International GmbH, Version 0.2, 11.10.2019 (confidential document)

[7] See secton 9.1 for list of used AIS

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 detailled 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.

Annex B: Evaluation results regarding development
and production environment

Annex B of Certification Report BSI-DSZ-CC-1118-2020

Evaluation results regarding development and production environment

The IT product TCOS CSP Module Version 1.0 Release 1/P6022y (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 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 7 April 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, production (and delivery) sites of the TOE listed below:

Site name	Function	Address
T-Systems International	Development	T-Systems International GmbH Untere Industriestraße 20 57250 Netphen-Dreis-Tiefenbach Germany
NXP (multiple sites)	Inlay Embedding, Wafer Initialization and Delivery to the Installation Agent	See BSI-DSZ-CC-1059-V2-2019 for address information

Table 6: Development, production (and delivery) sites

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.