Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1035-2017

for

TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE

from

T-Systems International GmbH

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1035-2017 (*)

TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE

from:	T-Systems International GmbH
PP Conformance:	Protection Profile for the Security Module of a Smart Meter Mini-HSM (Mini-HSM Security Module PP) - Schutzprofil für das Sicherheitsmodul des Smart Meter Mini-HSM, V1.0, 23 June 2017, BSI-CC-PP-0095-2017
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by 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 and 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 4

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 only

Bonn, 6 October 2017

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.

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.

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

Contents

A. Certification

1. 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[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- 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[5] [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]

2. 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.

2.1. 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.

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

[3] 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

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

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

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.sogisportal.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 recognised under SOGIS-MRA for all assurance components selected.

2.2. 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: http://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 related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

3. 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 Secure Crypto Module Version 1.0 Release 1/P60C144PVE has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0957-V2-2016. Specific results from the evaluation process BSI-DSZ-CC-0957-V2-2016 were re-used.

The evaluation of the product TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 05 October 2017. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] 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.

[6] Information Technology Security Evaluation Facility

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

4. Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only 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 levels please refer to the excerpts from the criteria at the end of the Certification Report or in the CC itself.

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-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 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 6 October 2017 is valid until 5 October 2027. 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.

4. to provide latest at of half of the certificate's validity period unsolicitedly and at his own expense current qualified evidence to the Certification Body at BSI that demonstrates that the requirements as outlined in the Security Target are up-to-date and remain valid in view of the respective status of technology. In general, this evidence is provided in the form of a re-assessment report according to the rules of the BSI Certification Scheme.

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.

5. Publication

The product TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE 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[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] 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 Secure Crypto Module Version 1.0 Release 1/P60C144PVE developed by T-Systems International GmbH.

The TOE is a Security Module that is implemented according to the Technical Guideline TR-03109-2 Annex B [19] and is intended to be used as a specific integral technical component within a so-called Smart Meter Mini-HSM in the framework of Smart Metering Systems. More detailed:

For cryptographic support of the different parties in a Smart Metering System that communicate with the so-called Smart Meter Gateway, that communicate among themselves or that are involved in the development and production processes of a Smart Meter Gateway the so-called Smart Meter Mini-HSM with an own integrated Security Module (TOE) can be used. Such Smart Meter Mini-HSM is connected from technical point of view to an Application Server via which the Mini-HSM User can invoke and use the needed cryptographic services from the Security Module (TOE) integrated in the Smart Meter Mini-HSM.

The Smart Meter Mini-HSM with its integrated Security Module (TOE) is intended to be used by the Application Server or the Mini-HSM User respectively as regular user of such Smart Meter Mini-HSM for their operation and cryptographic support in a Smart Metering System. The Smart Meter Mini-HSM with its integrated Security Module (TOE) serves as a cryptographic service provider for different cryptographic functionalities based on elliptic curve cryptography such as the generation and verification of digital signatures (e.g. for content data signature) and key agreement for TLS and content data encryption. The Security Module of the Smart Meter Mini-HSM contains the cryptographic identity of the Mini-HSM User, and it serves as a reliable source for random numbers as well as a secure storage for cryptographic keys and further (sensitive) data. These cryptographic services as provided by the Security Module (TOE) cover the following issues:

- Digital Signature Generation,
- Digital Signature Verification,
- Key Agreement for TLS,
- Key Agreement for Content Data Encryption,
- Key Pair Generation,
- Random Number Generation,
- Component Authentication via the PACE Protocol with Negotiation of Session Keys,
- Secure Messaging, and
- Secure Storage of Key Material and further (sensitive) data relevant for the Application Server or the Mini-HSM User respectively and their communication with other components and parties involved in the Smart Metering System.

The TOE's implementation follows the security module specification in the Technical Guideline TR-03109-2 Annex B [19] and makes for its access control policy use of Option 2 (see [19], chapter 3).

The TOE comprises

- the circuitry of the contact-based chip including all IC Dedicated Software being active in the Integration Phase and Operational Phase of the TOE (the integrated circuit, IC),
- the IC Embedded Software (operating system),
- the IC Application Software (file system), and
- the associated guidance documentation.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile for the Security Module of a Smart Meter Mini-HSM (Mini-HSM Security Module PP) - Schutzprofil für das Sicherheitsmodul des Smart Meter Mini-HSM, V1.0, 23 June 2017, BSI-CC-PP-0095-2017 [7].

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 AVA_VAN.5.

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

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

TOE Security Functionality	Addressed issue
Digital Signature Generation	The TOE (Security Module) serves as a cryptographic service provider for the Application Server or the Mini-HSM User respectively. It generates digital signatures based on elliptic curve cryptography for different purposes (commands PSO COMPUTE DIGITAL SIGNATURE, INTERNAL AUTHENTICATE).
Digital Signature Verification	The TOE (Security Module) serves as a cryptographic service provider for the Application Server or the Mini-HSM User respectively. It verifies digital signatures based on elliptic curve cryptography for different purposes (commands PSO VERIFY DIGITAL SIGNATURE, PSO VERIFY CERTIFICATE).
Key Agreement for TLS	The TOE (Security Module) serves as a cryptographic service provider for the Application Server or the Mini-HSM User respectively. It supports the cryptographic protocol ECKA-DH up to the generation of the shared secret value (command GENERAL AUTHENTICATE / variant ECKA-DH). Hint: The key derivation function is not part of the TOE's functionality and has to be realised by the external world (here: Application Server or the Mini-HSM User respectively). The session keys derived from the shared secret value by the key derivation function are used in the framework of the so-called TLS handshake.
Key Agreement for Content Data Encryption	The TOE (Security Module) serves as a cryptographic service provider for the Application Server or the Mini-HSM User respectively. It supports the cryptographic protocol ECKA-EG up to the generation of the shared secret value (command GENERAL AUTHENTICATE / variant ECKA-EG). Hint: The key derivation function is not part of the TOE's functionality and has to be realised by the external world (here:

TOE Security Functionality	Addressed issue
	Application Server or the Mini-HSM User respectively). The session keys derived from the shared secret value by the key derivation function are used in the framework of content data encryption.
Key Pair Generation	The TOE (Security Module) serves as a cryptographic service provider for the Application Server or the Mini-HSM User respectively. It generates asymmetric key pairs based on elliptic curve cryptography for different purposes (keys for signature, TLS, content data encryption).
Random Number Generation	The TOE (Security Module) serves as a cryptographic service provider for the Application Server or the Mini-HSM User respectively. It generates random numbers by providing a deterministic random number generator of class DRG.4 (command GET CHALLENGE). Furthermore, the TOE generates random values for internal purpose and the purpose of key generation.
Component Authentication via the PACE Protocol with Negotiation of Session Keys	The TOE (Security Module) implements the PACE protocol (command GENERAL AUTHENTICATE / variant PACE). The protocol provides component authentication between the TOE (Security Module) and the external world (here: Application Server) and includes the negotiation of session keys that will be used afterwards for Secure Messaging between these two components.
Secure Messaging	The TOE (Security Module) provides Secure Messaging according to ISO 7816-4 based on AES for securing the data transfer between the TOE (Security Module) and the external world (here: Application Server) for confidentiality and integrity. Hint: The session keys used for Secure Messaging are negotiated in the framework of the PACE protocol between the TOE (Security Module) and the external world (here: Application Server).
Secure Storage of Key Material and further (sensitive) data	The TOE (Security Module) serves as device for secure storage of keys and further data relevant for the external world (here: Application Server or the Mini-HSM User respectively). The TOE (Security Module) provides mechanisms for the access control to User Data stored in and processed by the TOE. Furthermore, the TOE (Security Module) provides mechanisms for the management and access to the TSF and TSF Data. The TOE (Security Module) provides security mechanisms serving for the accuracy and reliability of the TOE security functionality. This includes in particular self-protection, secure failure status and resistance against side channel and fault injection attacks.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 6.1 and 7.

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

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

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

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

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	NXP Secure Smart Card Controller P60C144PVE including its IC Dedicated Software (refer to the Certification Report BSI-DSZ-CC-0978-V2-2017 [11])	P60C144PVE ROM Mask: SCM_01BC_ID1.5_ROM_Daten_01.hex	HN1: SMD Package HVQFN32 (SOT617-3) on multiple tray
2	SW	IC Embedded Software (TCOS operating system)	TCOS Secure Crypto Module Version 1.0 Release 1 OS Version: '01 BC' Completion Code Version: '01' (refer to Table 3)	Implemented in ROM/EEPROM of the IC
3	SW	IC Application Software (file system)	FSV01 File System Version: '01' (refer to Table 3)	Implemented in EEPROM of the IC
4	DOC	Operational Guidance for users and administrators, Guidance Documentation of TCOS Secure Crypto Module Version 1.0 Release 1 [10]	Version 1.0	Document in electronic form (encrypted and signed)
5	DATA	Text file with FORMAT-command APDUs (for opening of Phase 5 of the TOE's life cycle model)	---	Text file in electronic form (encrypted and signed)
6	DATA	Authentication Key (customer-specific)	---	Text file in electronic form (encrypted and signed)

Table 2: Deliverables of the TOE

The customer-specific ROM mask for the TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE is labelled by NXP as P60C144PHN/9E35AA. The name of the ROM file transferred from T-Systems International GmbH to NXP is SCM_01BC_ID1.5_ROM_Daten_01.hex.

The commercial numbering of the TOE by NXP is as follows:

- Final Product: P60C144PHN/9E35AA
- 12NC: 935331355157
- Application: SCM_01BC_ID1.5

The certified file system for the TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE has the version '01'.

According to the Security Target [6], chapter 1.4.4 the life cycle model of the TOE consists of the following 6 phases: Phase 1: Security Module Embedded Software Development / Phase 2: IC Development / Phase 3: IC Manufacturing, Packaging and Testing / Phase 4: Security Module Product Finishing Process / Phase 5: Security Module Integration (Integration Phase) / Phase 6: Security Module End-Usage (Operational Phase).

The TOE delivery takes place after Phase 4 so that the evaluation process is limited to Phases 1 to 4. The TOE is delivered from NXP to the Integrator who is responsible for the integration of the TOE (Security Module) and the Mini-HSM and loading of initial key and certificate material into the TOE in the framework of the integration of the TOE in Phase 5. The Smart Meter Mini-HSM that integrates the TOE is delivered to the user of such Smart Meter Mini-HSM as well as to developers and vendors of Application Servers connected to such Smart Meter Mini-HSM in order to support their implementation activities.

In order to verify that the user uses a certified TOE, the TOE can be identified using the means described in the user guidance [10], chapters 8.3.30 and 8.4.1.1. The TOE can be identified by using the command FORMAT (only in Phase 5 of the TOE's life cycle model) respective the command GET CARD INFO (in Phase 5 and 6 of the TOE's life cycle model). Via the command FORMAT (P1 P2 = '00 00') respective the command GET CARD INFO (P1 P2 = '06 00') the user can read out the chip information and identify the underlying chip as well as the TCOS operating system and initialised file system installed in the chip. To open the integration phase (Phase 5 of the TOE's life cycle model) a mutual authentication via the command FORMAT as described in the user guidance [10], chapter 8.4.1.3 is necessary, therefore the authenticity of the TOE is verified before further usage of the TOE. The following identification data can be retrieved within a 16 byte string responded by the commands FORMAT respective GET CARD INFO:

Byte	Product information	Value
1	Indicator of the chip manufacturer according to ISO 7816-6	'04'
2	Chip type (type ID of the chip manufacturer)	'14'
3 - 8	Unique identification number for the chip	-
9	Card type	'13'
10 -11	Operating system version (ROM mask version)	'01 BC'
12	Version of the pre-completion code / completion code for finalizing the operating system	'01'
13	File system version	'01'
14	'00' (RFU)	-
15	'00' (RFU)	-
16	Authentication key identifier	'13'

Table 3: TOE identification data

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 TOE is a Security Module consisting of an underlying contact-based IC and an operating system and (initial) file system according to TR-03109-2 Annex B [19] and to the TOE user guidance [10]. With this implementation the TOE builds a specific integral technical component within a so-called Smart Meter Mini-HSM. As such a Security Module, the Security Policy of the TOE is to provide secure cryptographic functionalities and related key management functions. The TOE serves as a cryptographic service provider for the user of the Smart Meter Mini-HSM or the Application Server on behalf of this user respectively with provisioning of overall system security as needed by the user in the framework of acting in Smart Metering Systems.

The TOE implements physical and logical security functionality in order to protect data (in particular keys) stored and operated on the module when used as part of the Smart Meter Mini-HSM in a hostile environment. Hence, the TOE maintains the integrity and confidentiality of code and data stored in its memories and the different CPU modes with the related capabilities for configuration, memory access and 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 random number generation and key management functionality are being provided to be securely used by the TOE embedded software.

Specific details concerning the above mentioned Security Policy can be found in the Security Target [6], chapter 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:

- OE.Integration: Integration phase of the Mini-HSM and TOE
- OE.OperationalPhase: Operational phase of the Smart Meter Mini-HSM (Mini-HSM with integrated Security Module)
- OE.Implementation: Implementation of the Smart Meter Mini-HSM and Application Server
- OE.Protection: Protection of the TOE, Smart Meter Mini-HSM and Application Server
- OE.TrustedUser: Trustworthiness of the Mini-HSM User
- OE.Sign: Signature generation and verification
- OE.KeyAgreementDH: DH key agreement
- OE.KeyAgreementEG: ElGamal key agreement
- OE.Random: Random number generation
- OE.PACE: PACE

- OE.TrustedChannel: Trusted channel

Details can be found in the Security Target [6], chapter 4.2 respective in the PP [7], chapter 4.2.

5. Architectural Information

The TOE is set up as a composite product. It is composed from the Integrated Circuit (IC) P60C144PVE from NXP, the IC Embedded Software consisting of the TCOS operating system and the IC Application Software comprising a specific initial file system developed by T-Systems International GmbH.

For details concerning the CC evaluation of the underlying IC see the evaluation documentation under the Certification ID BSI-DSZ-CC-0978-V2-2017 [11].

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

- Hardware: Underlying IC including its IC Dedicated Software.
- Kernel: Manages the interfaces between all components.
- Crypt Component: Processes the cryptographic functions.
- Admin Component: Processes administrative base functions. Contains as well the TOE's file system.
- IO Component: Controls the input and output.
- ROM TCOS-Type Task: APDU processing (system, applications).

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.

Since many Security Functions can be tested by APDU command sequences, the evaluators performed these tests with real samples. 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,

- testing APDU commands related to NVM Management and File System,
- testing APDU commands related to Security Management,
- testing APDU commands related to Secure Messaging,
- penetration testing related to the verification of the Reliability of the TOE,
- source code analysis performed by the evaluators,
- side channel analysis for ECC (including ECC key generation) and hash calculation,
- fault injection attacks (laser attacks),
- testing APDU commands for the Integration Phase and Operational Phase (including personalisation and end-usage of the TOE),
- testing APDU commands for the commands using cryptographic mechanisms,
- 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 configurations of the TOE as outlined in the Security Target [6]:

TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE

There is only one configuration of the TOE.

The TOE is installed on a contact-based chip of type P60C144PVE from NXP. The underlying IC is certified under the Certification ID BSI-DSZ-CC-0978-V2-2017 (refer to [11]).

The TOE does not use the cryptographic software libraries of the hardware platform, but provides its cryptographic services by the crypto library developed by T-Systems International GmbH.

The TOE is delivered as already initialised module, i.e. the chip contains the complete IC Embedded Software (TCOS operating system) and IC Application Software (initial file system) and is embedded into a module of type HVQFN32.

The user can identify the certified TOE by the TOE response to specific APDU commands, more detailed by using the command FORMAT (only in Phase 5 of the TOE's life cycle model) or the command GET CARD INFO (in Phase 5 and 6 of the TOE's life cycle model) respectively according to the user guidance [10], chapters 8.3.30 and 8.4.1.1. See chapter 2 for details.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [8] 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 (see AIS 36). According to this concept the relevant guidance documents of the underlying platform and the document ETR for Composition from the platform evaluation (see [11] and [13]) have been applied in the TOE evaluation.

(ii) Guidance for Smartcard Evaluation.

(iii) Application of Attack Potential to Smartcards (see AIS 26).

For smart card specific methodology the scheme interpretations AIS 25, AIS 26 and AIS 36 (see [4]) were used.

For RNG assessment the scheme interpretation AIS 20 was used (see [4]).

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

A document ETR for composite evaluation according to AIS 36 has not been provided in the course of this certification procedure. It could be provided by the ITSEF and submitted to the Certification Body for approval subsequently.

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 component AVA_VAN.5 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0957-V2-2016, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the TOE's specific access control policy and on penetration testing of the implemented crypto functionality.

The evaluation has confirmed:

- PP Conformance: Protection Profile for the Security Module of a Smart Meter Mini-SM (Mini-HSM Security Module PP) – Schutzprofil für das Sicherheitsmodul des Smart Meter Mini-HSM, V1.0, 23 June 2017, BSI-CC-PP-0095-2017 [7]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by AVA_VAN.5

Additionally, the requirements of the Technical Guideline TR-03109-2 Annex B [19] are met. This is part of the qualification of the TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE that is intended to be used as an integral technical component within a so-called Smart Meter Mini-HSM.

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 following cryptographic algorithms are used by the TOE to enforce its security policy[8]:

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
1	Authenticity	ECDSA-signature verification using SHA-{256, 384, 512}	ANSI X9.63 (ECDSA), FIPS 180-2 (SHA), TR-03111, chap. 4.2	Key sizes corresponding to the used elliptic curve: BrainpoolP{256, 384, 512}r1 acc. to RFC 5639 NIST curves P-{256, 384} (secp{256, 384}r1) acc. to FIPS 186	TR-03116-3, chap. 2.2	FCS_COP.1/IMP import of keys
2	Authenticated Key Agreement	PACE-KA with SHA-{1, 224, 256}	TR-03110-2, chap. 3.2 (PACEv2)	|Nonce| = 128 bit	TR-03110-2, TR-03116-2, chap. 3.2, 4.2	FCS_CKM.1/PACE FIA_UID.1 FIA_UAU.1 FIA_UAU.4 FIA_UAU.5
3	Confidentiality	AES in CBC mode	FIPS 197 (AES), SP800-38A (CBC)	|k| = 128, 192, 256, |challenge|=64	TR-03116-3, chap. 2.1	FCS_COP.1/PACE-ENC FCS_CKM.1/PACE
4	Integrity	AES in CMAC mode	FIPS 197 (AES), SP800-38B (CMAC)	|k| = 128, 192, 256	TR-03116-3, chap. 2.1	FCS_COP.1/PACE-MAC
5	Trusted Channel	Secure messaging in ENC_MAC mode (established during PACEv2)	ISO 7816-4 TR-03110-2, chap. 3.2 (PACEv2)		TR-03110-2, TR-03116-2, chap. 3.2, 4.2	FTP_ITC.1 trusted channel between the TOE and the Application Server
6	Cryptographic Primitive	ECDSA signature verification / generation without Hash	TR-03111, chap. 4.2	Key sizes corresponding to the used elliptic curve: BrainpoolP{256, 384, 512}r1 acc. to RFC 5639 NIST curves P-{256, 384} (secp{256, 384}r1) acc. to FIPS 186	TR-03116-3, chap. 2.2	FCS_COP.1/VER-ECDSA FCS_COP.1/SIG-ECDSA
		Deterministic RNG DRG.4	AIS 20	n.a.	TR-03116-3, chap. 1.3.3, 8.3, 8.4	FCS_RNG.1
		ECKA-DH	TR-03111 (EC Diffie-Hellman)	Key sizes corresponding to the used elliptic	TR-03116-3, chap. 2.2	FCS_CKM.1/ECKA-DH used by the

[8] For references to crypto standards please refer to TR-03109-3 [20] or TR-03116-3 [21] respectively.

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
				curve: BrainpoolP{256, 384, 512}r1 acc. to RFC 5639 NIST curves P-{256, 384} (secp{256, 384}r1) acc. to FIPS 186		Application Server or the Smart Meter Mini-HSM user respectively for TLS handshake
		ECKA-EG	TR-03111 (EC ElGamal)	Key sizes corresponding to the used elliptic curve: BrainpoolP{256, 384, 512}r1 acc. to RFC 5639 NIST curves P-{256, 384} (secp{256, 384}r1) acc. to FIPS 186	TR-03116-3, chap. 2.2	FCS_CKM.1/ECKA-EG used by the Application Server or the Smart Meter Mini-HSM user respectively for content data encryption

Table 4: TOE cryptographic functionality

All cryptographic algorithms listed in table 4 are implemented by the TOE on the base of the Technical Guidelines TR-03109-2 Annex B [19], TR-03109-3 [20] and TR-03116-3 [21]. For that reason an explicit validity period is not given.

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, Clause 2). According to the Technical Guidelines TR-03109-3 [20] and TR-03116-3 [21], the algorithms are suitable for securing integrity, authenticity and confidentiality of the data stored in and processed by the TOE as a Security Module that is intended to be used as an integral technical component within a so-called Smart Meter Mini-HSM in the Smart Metering System. For the validity period of each algorithm refer to the Technical Guideline TR-03116-3 [21].

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.

In addition, the following requirements need to be considered and fulfilled when using the TOE's (cryptographic) functionality: Refer to the user guidance [10], chapters 4.1.5.5, 9.3.1, 10.2 (including subchapters).

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. Definitions

12.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
APDU	Application Protocol Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CBC	Cipher Block Chaining
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CMAC	Cipher-based MAC
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECKA	Elliptic Curve Key Agreement
ECKA-DH	Elliptic Curve Key Agreement - Diffie-Hellman
ECKA-EG	Elliptic Curve Key Agreement - ElGamal
ETR	Evaluation Technical Report
ID	Identifier
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
KA	Key Agreement
MAC	Message Authentication Code
NVM	Non Volatile Memory
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
RFU	Reserved for Future Use
SAR	Security Assurance Requirement
SFP	Security Function Policy

SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. 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.

13. 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
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 5, April 2017
http://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[9]
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-1035-2017, Specification of the Security Target TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE, Version 1.0.1, 29 September 2017, T-Systems International GmbH

[7] Protection Profile for the Security Module of a Smart Meter Mini-HSM (Mini-HSM Security Module PP) - Schutzprofil für das Sicherheitsmodul des Smart Meter Mini-HSM, V1.0, 23 June 2017, BSI-CC-PP-0095-2017, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[8] Evaluation Technical Report BSI-DSZ-CC-1035-2017, TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE, Version 1.0, 05 October 2017, SRC Security Research & Consulting GmbH (confidential document)

[9] specifically

- AIS 1, Version 13, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 23, Version 3, Zusammentragen von Nachweisen der Entwickler
- AIS 26, Version 9, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[9] Configuration List BSI-DSZ-CC-1035-2017, Konfigurationsliste von TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE, Version 1.4, 05 October 2017, T-Systems International GmbH (confidential)

[10] Guidance Documentation BSI-DSZ-CC-1035-2017, Operational Guidance for users and administrators, Guidance Documentation of TCOS Secure Crypto Module Version 1.0 Release 1, Version 1.0, 05 October 2017, T-Systems International GmbH

[11] Certification Report BSI-DSZ-CC-0978-V2-2017 for NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE with IC Dedicated Software, 27 September 2017, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[12] Security Target Lite BSI-DSZ-CC-0978-V2-2017, NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE, Rev. 2.62, 14 September 2017, NXP Semiconductors (sanitised public document)

[13] ETR for composite evaluation according to AIS 36, NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE, BSI-DSZ-CC-0978-V2, Version 2, 14 September 2017, TÜV Informationstechnik GmbH (confidential document)

[14] Product Data Sheet, SmartMX2 family P60x080/144 VA/VE, Secure high performance smart card controller, Release 5.4, 14 August 2015, NXP Semiconductors

[15] Instruction Set for the SmartMX2 family, Secure smart card controller, Release 3.1, 2 February 2012, NXP Semiconductors

[16] Information on Guidance and Operation, NXP Secure Smart Card Controller P60x144/080 VA/VE, Rev. 2.8, 07 July 2017, NXP Semiconductors

[17] Technische Richtlinie BSI TR-03109-1: Smart Meter Gateway - Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, Version 1.0, 2013, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[18] Technische Richtlinie BSI TR-03109-2: Smart Meter Gateway - Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, Version 1.1, 2014, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[19] Technische Richtlinie BSI TR-03109-2 Anhang B: Smart Meter Mini-HSM – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, Version 1.0, 2017, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[20] Technische Richtlinie BSI TR-03109-3: Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen, Version 1.1, 2014, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[21] Technische Richtlinie BSI TR-03116-3: Kryptographische Vorgaben für Projekte der Bundesregierung – Teil 3: Intelligente Messsysteme, January 2017, Bundesamt für Sicherheit in der Informationstechnik (BSI)

C. Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

“Objectives

EAL 1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL 5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL 6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL 6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL 7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL 7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

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

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-1035-2017

Evaluation results regarding development and production environment

The IT product TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE (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 advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 6 October 2017, 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.1, ALC_LCD.1, ALC_TAT.1)

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

a) T-Systems International GmbH, Untere Industriestraße 20, 57250 Netphen (development and test).

b) For development and production sites regarding the platform and wafer initialisation please refer to the Certification Report BSI-DSZ-CC-0978-V2-2017 ([11]).

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.

This page is intentionally left blank.