Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1217-2024

for

TCOS eEnergy Security Module Version 2.0 Release 1/P71

from

Deutsche Telekom Security GmbH

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1217-2024 (*)

TCOS eEnergy Security Module Version 2.0 Release 1/P71

from	Deutsche Telekom Security GmbH
PP Conformance:	Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP), Version 1.03, 11 December 2014, BSI-CC-PP-0077-V2-2015
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5
valid until:	28 February 2034

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 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 only

Bonn, 29 February 2024

For the Federal Office for Information Security

Sandro Amendola
Director-General

L.S.

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

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

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

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

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

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

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[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 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

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

3. Recognition Agreements

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

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

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

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

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

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

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

3.2. International Recognition of CC – Certificates (CCRA)

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

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

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

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

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

4. Performance of Evaluation and Certification

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

The product TCOS eEnergy Security Module Version 2.0 Release 1/P71 has undergone the certification procedure at BSI.

The evaluation of the product TCOS eEnergy Security Module Version 2.0 Release 1/P71 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 16 February 2024. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

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

The product was developed by: Deutsche Telekom Security GmbH.

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

5. Validity of the Certification Result

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

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

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

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 29 February 2024 is valid until 28 February 2034. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

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

[5] Information Technology Security Evaluation Facility

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

6. Publication

The product TCOS eEnergy Security Module Version 2.0 Release 1/P71 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Deutsche Telekom Security GmbH
Untere Industriestraße 20
57250 Netphen
Germany

B. Certification Results

The following results represent a summary of

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

1. Executive Summary

The Target of Evaluation (TOE) is the product TCOS eEnergy Security Module Version 2.0 Release 1/P71 developed by Deutsche Telekom Security GmbH. The TOE is a Smart Meter Security Module according to the Technical Guideline BSI TR-03109-2 [15] intended to be used by a Smart Meter Gateway in a Smart Metering System. The TOE serves as cryptographic service provider for the Smart Meter Gateway and supports the Smart Meter Gateway for its specific cryptographic needs. These cryptographic services that are invoked by the Smart Meter Gateway for its operation in a Smart Metering System 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 data relevant for the Gateway.

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 including the Smart Meter application), and
- the associated guidance documentation.

The Security Target [6] is the basis for this certification. It is based on the certified PP Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP), Version 1.03, 11 December 2014, BSI-CC-PP-0077-V2-2015 [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 ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], 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 (Smart Meter Security Module) serves as a cryptographic service provider for the Smart Meter Gateway. It

TOE Security Functionality	Addressed issue
	generates digital signatures based on elliptic curve cryptography for different purposes (commands PSO COMPUTE DIGITAL SIGNATURE, INTERNAL AUTHENTICATE).
Digital Signature Verification	The TOE (Smart Meter Security Module) serves as a cryptographic service provider for the Smart Meter Gateway. It verifies digital signatures based on elliptic curve cryptography for different purposes (commands PSO VERIFY DIGITAL SIGNATURE, EXTERNAL AUTHENTICATE, PSO VERIFY CERTIFICATE).
Key Agreement for TLS	The TOE (Smart Meter Security Module) serves as a cryptographic service provider for the Smart Meter Gateway. 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: Smart Meter Gateway). 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 (Smart Meter Security Module) serves as a cryptographic service provider for the Smart Meter Gateway. 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: Smart Meter Gateway). 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 (Smart Meter Security Module) serves as a cryptographic service provider for the Smart Meter Gateway. 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 (Smart Meter Security Module) serves as a cryptographic service provider for the Smart Meter Gateway. It generates random numbers by providing an hybrid physical random number generator of class PTG.3 (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 (Smart Meter Security Module) implements the PACE protocol (command GENERAL AUTHENTICATE / variant PACE). The protocol provides component authentication between the TOE (Smart Meter Security Module) and the external world (here: Smart Meter Gateway) and includes the negotiation of session keys that will be used afterwards for Secure Messaging between these two components.
Secure Messaging	The TOE (Smart Meter Security Module) provides Secure Messaging according to ISO 7816-4 based on AES for securing the data transfer between the TOE (Smart Meter Security Module) and the external world (here: Smart Meter Gateway) for confidentiality and integrity. Hint: The session keys used for Secure Messaging are

TOE Security Functionality	Addressed issue
	negotiated in the framework of the PACE protocol between the TOE (Smart Meter Security Module) and the external world (here: Smart Meter Gateway).
Secure Storage of Key Material and further data relevant for the Gateway	The TOE (Smart Meter Security Module) serves as device for secure storage of keys and further data relevant for the external world (here: Smart Meter Gateway). The TOE (Smart Meter Security Module) provides mechanisms for the access control to User Data stored in and processed by the TOE. Furthermore, the TOE (Smart Meter Security Module) provides mechanisms for the management and access to the TSF and TSF Data. The TOE (Smart Meter 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 eEnergy Security Module Version 2.0 Release 1/P71

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	NXP Secure Smart Card Controller P71D600 (N7122) including its IC Dedicated Software (refer to the Certification Report BSI-DSZ-CC-1149-V3-2023 [11])	Hardware platform: P71D600 (N7122) Wafer-Image (ChipExe): WaferImageTCOS-ESM20_HW04_MB6D6M01000000.out.chipexe	Hard macro instantiated within a wafer, module and/or package, e.g. HVQFN

No	Type	Identifier	Release	Form of Delivery
2	SW	IC Embedded Software (TCOS operating system)	TCOS eEnergy Security Module Version 2.0 Release 1/P71 OS Version: '01 C1' Completion Code Version: '01' (refer to Table 3)	Implemented in Flash memory/EEPROM of the IC
3	SW	IC Application Software (file system including the Smart Meter application)	FSV01 File System Version: '01' (refer to Table 3)	Implemented in Flash memory/EEPROM of the IC
4	DOC	Operational Guidance for users and administrators, Guidance Documentation of TCOS eEnergy Security Module 2.0 Release 1 [10]	Version 1.0.0	Document in electronic form (encrypted and signed)
5	DATA	Activation command APDUs (for opening personalization and integration processes 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 Wafer-Image (ChipExe) for the TOE is labelled and identified by NXP Semiconductors GmbH as TCOS eEnergy 2.0 R1, sample.

The name of the Wafer-Image file transferred from Deutsche Telekom Security GmbH to NXP Semiconductors GmbH is WaferImageTCOS-ESM20_HW04_MB6D6M01000000_-submission_2.zip.gpg.

The identification of the TOE by NXP Semiconductors GmbH is defined by the project name SE042.

The wafer initialisation of the TOE based on the hardware platform P71D600 (N7122) is part of the NXP IC manufacturing and takes place by using the aforementioned Wafer-Image from Deutsche Telekom Security GmbH that includes all TOE parts.

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 Semiconductors GmbH to the Integrator who is responsible for the integration of the TOE (Smart Meter Security Module) and the Smart Meter Gateway and loading of initial key and certificate material into the TOE in the framework of the integration of the TOE in Phase 5. The TOE is as well delivered to the developers of Smart Meter Gateways in order to support their implementation activities. To ensure that the evaluated TOE version is received, the procedures to start the

personalization and integration processes as described in the user guidance document [10] have to be followed.

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 8.3.29 and 8.4.1.1. The TOE can be identified by using the command FORMAT (only till Phase 5 of the TOE's life-cycle model) respective the command GET CARD INFO (in Phase 6 of the TOE's life-cycle model). Via the command FORMAT (P1 P2 = '00 00' for option ‘Reading of chip information’) 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 personalization and 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: NXP Semiconductors GmbH	'04'
2	Chip type (type ID of the chip manufacturer)	'20'
3 - 8	Unique identification number for the chip	-
9	Card type: TCOS eESM	'10'
10 -11	Operating system version (ROM mask version)	'01 C1'
12	Version of the completion code for finalizing the operating system	'01'
13	File system version	'01'
14	'00' (RFU)	'00'
15	'00' (RFU)	'00'
16	Authentication key version	'11'

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 Security Policy of the TOE as a Smart Meter Security Module consisting of an underlying contact-based IC and an operating system and (initial) file system according to TR-03109-2 [15] and to the TOE user guidance [10] is to provide secure cryptographic functionalities and related key management functions for usage by the Smart Meter Gateway and its Gateway Administrator. The TOE serves as a cryptographic service provider for the Smart Meter Gateway with provisioning of overall system security in view of Smart Meter Gateway needs.

The TOE implements physical and logical security functionality in order to protect user data stored and operated on the module when used as part of the Smart Meter Gateway in a hostile environment. Hence the TOE maintains integrity and confidentiality of code and data stored in its memories and the different CPU modes with the related capabilities for configuration and memory access and for integrity, the correct operation and the

confidentiality of security functionality provided by the TOE. Therefore the TOE's overall policy is to protect against malfunction, leakage, physical manipulation and probing. Besides, the TOE's life-cycle is supported as well as the user Identification whereas the abuse of functionality is prevented. Furthermore, specific cryptographic services including 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 policies 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 Gateway and TOE
- OE.OperationalPhase: Operational phase of the integrated Gateway
- OE.Administration: Administration of the TOE
- OE.TrustedAdmin: Trustworthiness of the Gateway Administrator
- OE.PhysicalProtection: Physical protection of the TOE
- OE.KeyAgreementDH: DH key agreement
- OE.KeyAgreementEG: ElGamal key agreement
- OE.PACE: PACE
- OE.TrustedChannel: Trusted channel

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

5. Architectural Information

The TOE is set up as a composite product. It is composed from the Integrated Circuit (IC) P71D600 (N7122) from NXP Semiconductors GmbH, the IC Embedded Software consisting of the TCOS operating system and the IC Application Software comprising a specific file system developed by Deutsche Telekom Security GmbH.

For details concerning the CC evaluation of the underlying IC see the evaluation documentation under the Certification ID BSI-DSZ-CC-1149-V3-2023 [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 (COMP_CH): Hardware Platform
- Kernel (COMP_KL): implements security relevant base functions in system mode of the Hardware Platform
- TCOS eESM Application (COMP_APP): implements TCOS commands into system calls for the Kernel, processes APDUs after getting process control from the Kernel and requests resources of the Kernel

6. Documentation

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

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

7. IT Product Testing

The developer tested all TOE Security Functions either on real modules 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 module 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 eEnergy Security Module Version 2.0 Release 1/P71

There is only one configuration of the TOE.

The TOE is installed on a contact-based chip of type P71D600 (N7122) from NXP Semiconductors GmbH. The underlying IC is certified under the Certification ID BSI-DSZ-CC-1149-V3-2023 (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 Deutsche Telekom Security GmbH.

The TOE is delivered as already initialised component (in type of wafer, module and/or package, e.g. HVQFN), i.e. the chip contains the complete IC Embedded Software (TCOS operating system) and IC Application Software (file system including the Smart Meter application).

The user can identify the certified TOE by the TOE response to specific APDU commands, more detailed by using the command FORMAT (only till Phase 5 of the TOE's life-cycle model) respective the command GET CARD INFO (in Phase 6 of the TOE's life-cycle model) according to the user guidance [10], chapters 8.3.29 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) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

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

The following guidance specific for the technology was used:

(i) Composite product evaluation for Smart Cards and similar devices according to AIS 36 (see [4]). On base of this concept the relevant guidance documents of the underlying IC platform (refer to [11]) and the document ETR for composite evaluation from the IC’s evaluation (refer to [13] and [11]) have been applied in the TOE evaluation. Related to AIS 36 the updated version of the JIL document ‘Composite product evaluation for Smart Cards and similar devices’, Version 1.5.1, May 2018 was taken into account.

(ii) Guidance for Smartcard Evaluation (AIS 37, see [4]).

(iii) Attack Methods for Smartcards and Similar Devices (AIS 26, see [4]).

(iv) Application of Attack Potential to Smartcards (AIS 26, see [4]).

(v) Application of CC to Integrated Circuits (AIS 25, see [4]).

(vi) Security Architecture requirements (ADV_ARC) for smart cards and similar devices (AIS 25, see [4]).

(vii) Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6 (AIS 34, see [4]).

(viii) Functionality classes and evaluation methodology of physical and deterministic random number generators (AIS 20 and AIS 31, see [4]).

(ix) Informationen zur Evaluierung von kryptographischen Algorithmen (AIS 46, see [4]).

For smart card specific methodology the scheme interpretations AIS 25, AIS 26, AIS 34, AIS 36, AIS 37 and AIS 46 (see [4]) were used. For RNG assessment the scheme interpretations AIS 20 and AIS 31 were applied (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 components ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP), Version 1.03, 11 December 2014, BSI-CC-PP-0077-V2-2015 [7]
- for the Functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

Additionally, the requirements of the Technical Guideline TR-03109-2 [15] are met. This is part of the qualification of the TCOS eEnergy Security Module Version 2.0 Release 1/P71 intended to be used by Smart Meter Gateways in the Smart Metering System.

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.

The evaluation was performed as a composite evaluation according to AIS 36 (see [4]) and therefore relies on the platform certification of the used IC. Refer to certification ID BSI-DSZ-CC-1149-V3 ([11], [12]). The TOE’s cryptographic functionality (except for the IC’s symmetric and asymmetric co-processors) is implemented by Deutsche Telekom Security GmbH and assessed in the framework of the composite evaluation.

9.2. Results of cryptographic assessment

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.[7]

#	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 180-4 (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	Authentication	ECDSA-signature verification using SHA-{256, 384, 512}	ANSI X9.63 (ECDSA), FIPS 180-4 (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/ AUTH external authentication (Gateway Administrator)
3	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/GWA, FIA_UAU.4, FIA_UAU.5
4	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
5	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
6	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 Smart Meter Gateway
7	Cryptographic Primitive	ECDSA signature verification / generation	TR-03111, chap. 4.2	Key sizes corresponding to the used elliptic	TR-03116-3, chap. 2.2	FCS_COP.1/ VER-ECDSA

[7]For references to crypto standards please refer to TR-03109-3 [16] or TR-03116-3 [17] respectively.

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
		without Hash		curve: BrainpoolP{256, 384, 512}r1 acc. to RFC 5639 NIST curves P-{256, 384} (secp{256, 384}r1) acc. to FIPS 186		FCS_COP.1/ SIG-ECDSA
		Hybrid physical RNG PTG.3	AIS 20/31	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 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-DH used by the Smart Meter Gateway 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 Smart Meter Gateway 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 [15], TR-03109-3 [16] and TR-03116-3 [17]. 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 [16] and TR-03116-3 [17], the algorithms are suitable for securing integrity, authenticity and confidentiality of the data stored in and processed by the TOE as a Smart Meter Security Module that is intended to be used by the Smart Meter Gateway in the Smart Metering System. For the validity period of each algorithm refer to the Technical Guideline TR-03116-3 [17].

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.

In particular, the following aspects, requirements and recommendations need to be considered when using the TOE and its security functionality (including cryptographic functionality): Refer to the user guidance [10], chapters 9.1 to 9.9.

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.

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

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

HVQFN	Quad Flat No Leads Package
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

13.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 5, April 2017
https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen)
https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8]
https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website
https://www.bsi.bund.de/zertifizierungsreporte

[8] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document (but with usage of updated JIL document ‘Composite product evaluation for Smart Cards and similar devices’, Version 1.5.1, May 2018)
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[6] Security Target for BSI-DSZ-CC-1217-2024, Specification of the Security Target TCOS eEnergy Security Module 2.0 Release 1, Version 2.0.1, 1 February 2024, Deutsche Telekom Security GmbH

[7] Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP) - Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, Version 1.03, 11 December 2014, BSI-CC-PP-0077-V2-2015, Bundesamt für Sicherheit in der Informatiostechnik (BSI)

[8] Evaluation Technical Report BSI-DSZ-CC-1217, TCOS eEnergy Security Module Version 2.0 Release 1/P71, Version 1.1, 16 February 2024, SRC Security Research & Consulting GmbH (confidential document)

[9] Configuration List BSI-DSZ-CC-1217, Konfigurationsliste von TCOS eESM Version 2.0 Release 1/NXP P71D600, Version 1.0, 13 February 2024, Deutsche Telekom Security GmbH (confidential document)

[10] Guidance Documentation BSI-DSZ-CC-1217, Operational Guidance for users and administrators, Guidance Documentation of TCOS eEnergy Security Module 2.0 Release 1, Version 1.0.0, 4 February 2024, Deutsche Telekom Security GmbH

[11] Certification Report BSI-DSZ-CC-1149-V3-2023 for NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3) from NXP Semiconductors GmbH, 13 December 2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[12] Security Target Lite BSI-DSZ-CC-1149-V3-2023, NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2R3), Version 1.8, 1 December 2023, NXP Semiconductors GmbH (sanitised public document)

[13] ETR for composite evaluation according to AIS 36, NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2R3), BSI-DSZ-CC-1149-V3-2023, Version 2, 1 December 2023, TÜV Informationstechnik GmbH (confidential document)

[14] Technische Richtlinie BSI TR-03109-1: Smart Meter Gateway - Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, Version 1.1, 2021, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[15] 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)

[16] 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)

[17] Technische Richtlinie BSI TR-03116-3: Kryptographische Vorgaben für Projekte der Bundesregierung – Teil 3: Intelligente Messsysteme, 2022 (Stand 2023), Bundesamt für Sicherheit in der Informationstechnik (BSI)

C. Excerpts from the Criteria

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

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

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

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment.

Annex B of Certification Report BSI-DSZ-CC-1217-2024

Evaluation results regarding development and production environment

The IT product TCOS eEnergy Security Module Version 2.0 Release 1/P71 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 29 February 2024, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1)

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

a) Deutsche Telekom Security GmbH, Untere Industriestraße 20, 57250 Netphen, Germany (development and test).

b) For development and production sites regarding the platform and wafer initialisation please refer to the Certification Report BSI-DSZ-CC-1149-V3-2023 ([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.

Note: End of report