Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1003-2018

for

Smart Meter Gateway Security Module Application on MultiApp V4 Revision A

from

Gemalto SA

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-1003-2018 (*)

Smart Meter Gateway Security Module Application on MultiApp V4 Revision A

SOGIS Recognition Agreement

from	Gemalto SA
PP Conformance:	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
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5

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 and ALC_FLR only

Bonn, 18 September 2018

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

L.S.

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

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.

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

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

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

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

3. Recognition Agreements

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

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

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

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

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.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 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: 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 the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

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

4. Performance of Evaluation and Certification

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

The product Smart Meter Gateway Security Module Application on MultiApp V4 Revision A has undergone the certification procedure at BSI.

The evaluation of the product Smart Meter Gateway Security Module Application on MultiApp V4 Revision A was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 10 August 2018. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Gemalto SA.

The product was developed by: Gemalto SA.

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

5. Validity of the Certification Result

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

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

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

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 18 September 2018 is valid until 17 September 2028. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

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

[5] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.
4. to conduct a re-assessment after 5 years (i.e. after half of the validity period of the certificate has passed) in order to assess the robustness of the product against new state-of-the-art attack methods. This has to be done on the developer‘s own initiative and at his own expense. As evidence a report regarding a re-assessment or a re-certification according to the regulations of the BSI-certification-scheme shall be provided.

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 Smart Meter Gateway Security Module Application on MultiApp V4 Revision A 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] Gemalto SA
6, Rue de la Verrerie
92190 Meudon
Frankreich

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 Smart Meter Gateway Security Module Application on MultiApp V4 Revision A developed by Gemalto SA. The TOE is set up as a composite product, consisting of a specific smart card application (Java Card Applet) for the Security Module of the so-called Smart Meter Gateway that is implemented on top of the Java Card Platform JavaCard MultiApp V4.0 from Gemalto SA.

The TOE is a Smart Meter Security Module on base of the Technical Guideline BSI TR-03109-2 [25] and is 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 chip including all IC Dedicated Software being active in the Integration Phase and Operational Phase of the TOE (the integrated circuit, IC Infineon M7892 G12),
- the IC Embedded Software (operating system of the Java Card Platform JavaCard MultiApp V4.0),
- the IC Application Software (Smart Meter Gateway Security Module Applet), and
- the associated guidance documentation.

The Security Target [6] and [7] is the basis for this certification. It is based on the certified 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 [8].

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

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [7], chapter 6.2. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
SF.AUTHENTICATION	Authentication management for device and human user.
SF.DIGITAL_SIGNATURE_GENERATION	Digital signature generation management.
SF.DIGITAL_SIGNATURE_VERIFICATION	Digital signature verification management.
SF.VERIFY_CERTIFICATE	Verification of certificates in the framework of key import.
SF.KEY_AGREEMENT_TLS	Support for key agreement for TLS.
SF.KEY_AGREEMENT_CDE	Support for key agreement for content data encryption.
SF.CRYPTO	Cryptography management.
SF.INTEGRITY	Integrity monitoring for file system and data objects.
SF.MANAGEMENT	Operation management and access control for file system and objects including residual information protection.
SF.SECURE_MESSAGING	Secure messaging management.
SF.APPLET_CSM	Card security management including insecure state detection (including wrong applet life cycle transition), exception management and reaction at applet level.
Security functionality provided by the underlying Java Card Platform JavaCard MultiApp V4.0 including the IC Infineon M7892 G12	Refer for details to the documents covered by the related Certification Reports [16] and [23]. The Smart Meter Gateway Security Module Applet with its security functionality mentioned in the present table in the preceding rows makes intensive use of the security functionality provided by the underlying Java Card Platform JavaCard MultiApp V4.0 and its IC Infineon M7892 G12. This holds in particular for the TOE's cryptographic functionality.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 6.2 and 7 and [7], chapter 6.2.

The assets to be protected by the TOE are defined in the Security Target [6] and [7], chapter 3.3. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [7], chapter 3.4, 3.5 and 3.6.

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

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

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this

certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Smart Meter Gateway Security Module Application on MultiApp V4 Revision A

The following table outlines the TOE deliverables:

No.	Type	Identifier		Release	Form of Delivery
1	HW/SW	Infineon Security Controller M7892 G12 including its IC Dedicated Software (refer to the Certification Report BSI-DSZ-CC-0891-V2-2016 [23])	Smart Meter Gateway Security Module Application on MultiApp V4 The TOE is as well known under the product name 'Smart Meter Gateway Security Module V1.1'.	Revision A For identification data see below.	DFN-8 / MFF2 form factor, delivery associated to a reel
2	SW	IC Embedded Software: JavaCard MultiApp V4.0 operating system (refer to the Certification Report ANSSI-CC-2017/54 [16])			
3	SW	IC Application Software: Smart Meter Gateway Security Module Applet			
4	DOC	Preparation Guidance for Smart Meter Gateway Security Module V1.1 [11]		D1393787, Release 1.2	Document in electronic form (encrypted and signed, delivered via e-mail)
5	DOC	Operational Guidance for Smart Meter Gateway Security Module V1.1 [12]		D1393788, Release 0.9	Document in electronic form (encrypted and signed, delivered via e-mail)
6	DOC	Smart Meter Gateway Security Module V1.1 - Personalization and Operational Life Cycle (SEID01) - User Guide [13]		D1413164G	Document in electronic form (encrypted and signed, delivered via e-mail)

No.	Type	Identifier	Release	Form of Delivery
7	DOC	Smart Meter Gateway Security Module V1.1 - Integration and Pre-Personalization Life Cycle (SEID02) - User Guide [14]	D1422373F	Document in electronic form (encrypted and signed, delivered via e-mail)
8	DOC	Integration and Pre-Personalization Guideline [15]	D1386918C, Release 1.6	Document in electronic form (encrypted and signed, delivered via e-mail)
9	DOC	MultiApp V4 – AGD_PRE document – Javacard Platform [19]	D1390316, Version 1.1	Document in electronic form (encrypted and signed, delivered via e-mail)
10	DOC	MultiApp V4 – AGD_OPE document – Javacard Platform [20]	D1390321, Version 1.2	Document in electronic form (encrypted and signed, delivered via e-mail)
11	DOC	Rules for applications on Multiapp certified product [21]	D1390963_EXT, Release 1.1	Document in electronic form (encrypted and signed, delivered via e-mail)
12	DOC	MultiApp ID Operating System - Reference Manual [22]	D1392687A	Document in electronic form (encrypted and signed, delivered via e-mail)

Table 2: Deliverables of the TOE

Note: The TOE might be delivered by the developer Gemalto SA together with the so-called Key Export Tool (including related guidance documentation). However, this developer-specific tool and its related guidance documentation are neither part of the TOE and its deliverables as listed in Table 2 nor were evaluated in course of the TOE's security evaluation.

According to the Security Target [6] and [7], chapter 1.9 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 the end of Phase 4 so that the evaluation process is limited to Phases 1 to 4. The TOE is delivered from Gemalto SA to the Integrator who is responsible for the integration of the TOE (Smart Meter Gateway Security Module Application on MultiApp V4 Revision A) and the Smart Meter Gateway and for 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.

The TOE is delivered in DFN-8 / MFF2 form factor and is in its fully operational state, ready to be integrated, pre-personalised and afterwards personalized. The shipment will be performed via trusted carrier. To ensure that the evaluated version of the TOE has been received by the customer the acceptance procedures as detailed in the guidance documentation [11], chapter 3 must be performed.

The TOE in its certified version can be uniquely identified. Detailed descriptions of the method for identification of the TOE and information on the relevant identification data for the TOE (including its Java Card Platform JavaCard MultiApp V4.0 with the underlying IC Infineon M7892 G12 and its Smart Meter Gateway Security Module Applet) can be found in the guidance documents [13], chapter 2, [14], chapter 2, [15], chapter 2.2 and [20], chapter 1.5 as well as in the Security Target [6] and [7], chapter 1.6.2.1.

Identification information of the TOE is coded in the elementary file EF.SecModTRInfo that can be freely read out with the READ RECORD command by the user. Further identification data of the TOE with its underlying IC and Java Card Platform and its specific Java Card Applet can be retrieved by the GP commands SELECT and GET DATA with tag 0x9F7F and with tag 0x0103. The values must match the identification data as given in the guidance documents [13], chapter 2, [14], chapter 2, [15], chapter 2.2 and [20], chapter 1.5 as well as in the Security Target [6] and [7], chapter 1.6.2.1 in order to check for the certified TOE version.

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 on base of the TR-03109-2 [25] and according to the TOE user guidances [11], [12], [13], [14], [15], [19], [20], [21] and [22] 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. More detailed the following issues are addressed:

- Cryptographic Support,
- User Data Protection,
- Identification and Authentication,
- Security Management,
- Protection of the TSF, and
- Trusted Path/Channels.

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] and [7], chapter 6.2.

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] and [7], chapter 4.3 or in the PP [8], chapter 4.2 respectively.

5. Architectural Information

The TOE is designed and implemented as a composite product consisting of a specific Java Card Applet (Smart Meter Gateway Security Module Applet) that is implemented on a certified Java Card Platform (JavaCard MultiApp V4.0) that comprises a certified IC (Infineon Security Controller M7892 G12).

The TOE's architecture consists of the following two subsystems:

- Java Card Platform MultiApp V4.0 (including the underlying IC Infineon M7892 G12)
- Smart Meter Gateway Security Module Applet

For information on the architectural design of the Java Card Platform JavaCard MultiApp V4.0 (including the underlying IC Infineon M7892 G12) refer to [16] and [23].

The Smart Meter Gateway Security Module Applet itself consists of the following modules:

- AppletInformation_Mngt: Applet Status and Version Management
- Authentication_Mngt: Authentication Management
- Card_Mngt: Card Management
- Check_Key_Mngt: Generic SDO keys and key management
- Context_Utils_Mngt: Implementation of Applet for context management
- DataObject_Mngt: Security data Object Management
- File_Key_Mngt: File and Key Management
- Generic_ToolBox: Generic Package toolbox
- MSE_Mngt: Security Operation Management
- MainApplet_Mngt: Main Applet Management

- PACE_Utils_Mngt: PACE Utils Management
- PIN_Mngt: PIN Management
- PSO_Mngt: Signature and Certificate Operation Management
- Perso_Mngt: Implementation of Applet Methods to limit the access between perso state and beginning of operation state
- RandomGeneration_ToolBox: Random Generation toolbox
- Signature_Mngt: Signature Management for Generation and Verification
- Utils_Mngt: Utils Management

6. Documentation

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

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, on production samples or with simulator tests. For all commands and functionality tests, test cases are specified in order to demonstrate the expected behaviour including error cases. Hereby a representative sample including all boundary values of the parameter set, e.g. all command APDUs with valid and invalid inputs were tested. All in all, the developer's testing comprises the following areas:

- Check of all APDU commands including the GP commands on the underlying Java Card Platform JavaCard MultiApp V4.0 with regard to their availability.
- Test of APDU commands with good and bad cases.
- Card tearing tests.
- Protocol tests (T=0, T=1).
- Use Case tests according to BSI TR-3109-2 Annex ([26]).
- Testing of security mechanisms with use of a simulator.

The developer's aim was to cover all TSFIs that are described in the functional specification and all subsystems of the TOE design with this testing approach.

Repetition of the developer tests was performed during the independent evaluator tests. Hereby, the approach for independent testing followed by the evaluators was as follows:

- Examination of the developer's testing amount, depth and coverage analysis and of the developer's test goals and plan for identification of gaps.
- Examination whether the TOE in its intended environment operates as specified using iterations of developer's tests.

- Independent testing was performed at the evaluation body with the TOE developer's test environment and additional evaluation body test equipment using equipment that is equivalent to the set of resources used by the developer.
- The evaluators verified the developer's test results by executing a subset of the developer's tests and verifying the test log files for successful execution.

Furthermore, the evaluators have tested the TOE systematically against high attack potential during their penetration testing. Hereby, the approach for penetration testing followed by the evaluator was as follows:

- Based on a list of potential vulnerabilities applicable to the TOE in its operational environment created within the work unit AVA_VAN.5-5 the evaluators devised the attack scenarios for penetration tests when they were of the opinion that those potential vulnerabilities could be exploited in the TOE's operational environment.
- While doing this, also the aspects of the security architecture described in ADV_ARC were considered for penetration testing. All other evaluation input was used for the creation of the tests as well. Specifically the test documentation provided by the developer was used to find out if there are areas of concern that should be covered by tests of the evaluation body.
- The source code reviews of the provided implementation representation accompanied the development of test cases and were used to find test input. The code inspection also supported the testing activity by enabling the evaluators to verify implementation aspects that could hardly be covered by test cases.
- In addition, the evaluators applied tests and performed code reviews during the evaluation activity of ADV_COMP.1 to verify the implementation of the requirements imposed by the ETR for composite evaluation and the guidance of the underlying platform. This ensured confidence in the security of the TOE as a whole.

The primary focus for devising penetration tests was to cover all potential vulnerabilities identified as applicable in the TOE's operational environment for which an appropriate test set was devised.

Summary of test results and effectiveness analysis

All in all, the test results yielded that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential high was actually successful in the TOE's operational environment as defined in the Security Target [6] and [7] provided that all (security) measures required by the developer are applied. However, with respect to conformity to the Technical Guideline BSI TR-03109-2 ([25]) some deviations were encountered.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

Smart Meter Gateway Security Module Application on MultiApp V4 Revision A

There is only one configuration of the TOE.

The TOE is a composition and comprises of the following parts:

- the circuitry of the chip including all IC Dedicated Software being active in the Integration Phase and Operational Phase of the TOE (the integrated circuit, IC Infineon M7892 G12), refer to BSI-DSZ-CC-0891-V2-2016 ([23]),
- the IC Embedded Software (operating system of the Java Card Platform JavaCard MultiApp V4.0) from Gemalto, refer to ANSSI-CC-2017/54 ([16]),
- the IC Application Software (Smart Meter Gateway Security Module Applet) from Gemalto, and
- the associated guidance documentation.

The TOE functions only in contact-based mode.

The TOE is a composite product with a Java Card implementation in closed configuration with the Smart Meter Gateway Security Module Applet as a single applet instance. No post-issuance of further applets to the TOE is possible and thus the residing program code of the TOE is fixed on the Java Card Platform.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [9] 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 Java Card Platform JavaCard MultiApp V4.0 (refer to the guidance documents [19], [20], [21] and [22]) and the document ETR for composite evaluation from the Java Card Platform's evaluation ([18]) 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.

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

(iv) Functionality classes and evaluation methodology of physical and deterministic random number generators.

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

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.

The evaluation has confirmed:

- PP Conformance: 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 [9]
- 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

A complete conformity check of the TOE's implementation for fulfilment of the requirements defined in the Technical Guideline BSI TR-03109-2 [25] was not carried out in the framework of this TOE security evaluation. Furthermore, in the course of the TOE's security evaluation it turned out that the TOE's implementation deviates in some points from the Technical Guideline BSI TR-03109-2 [25] (e.g. concerning the key and PIN handling and management). In view of this, there is explicitly no statement on the TOE's conformity to the Technical Guideline BSI TR-03109-2 [25] – as this is in general part of the qualification of Smart Meter Security Modules that are intended to be used by Smart Meter Gateways in the Smart Metering System – given. In particular, when integrating the TOE into a Smart Meter Gateway and when using the TOE this issue should be taken into account.

The cryptographic algorithms outlined in Table 3 below are implemented in the Java Card Platform JavaCard MultiApp V4.0 that is part of the TOE and on which the Smart Meter Gateway Security Module Applet is set up. Except for the DRG.4-implementation the security evaluation of the implementation of all other cryptographic algorithms depicted in Table 3 was performed in the framework of the certification of the Java Card Platform JavaCard MultiApp V4.0 (refer to the Certification Report [16] and related Security Target [17]). The TOE and its specific Applet rely on the correct (i.e. standard-conform) and secure implementation of these cryptographic algorithms. The TOE's DRG.4-implementation has already been as well part of the certification of the Java Card Platform JavaCard MultiApp V4.0, but the missing evaluation according to AIS 20 (see [4]) was caught up in course of the present evaluation.

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 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:

#	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 X9.62 [32] (ECDSA), FIPS 180-4 [34] (SHA), TR-03111, chap. 4.2 [31]	Key sizes corresponding to the used elliptic curve: BrainpoolP{256, 384, 512}r1 acc. to RFC 5639 [41] NIST curves P-{256, 384} (secp{256, 384}r1) acc. to FIPS 186-3 [35]	TR-03109-3 [27], TR-03116-3, chap. 2.2 [28]	FCS_COP.1/IMP import of keys
2	Authentication	ECDSA-signature verification using SHA-{256, 384, 512}	ANSI X9.62 [32] (ECDSA), FIPS 180-4 [34] (SHA), TR-03111, chap. 4.2 [31]	Key sizes corresponding to the used elliptic curve: BrainpoolP{256, 384, 512}r1 acc. to RFC 5639 [41] NIST curves P-{256, 384} (secp{256, 384}r1) acc. to FIPS 186-3 [35]	TR-03109-3 [27], TR-03116-3, chap. 2.2 [28]	FCS_COP.1/AUTH external authentication (Gateway Administrator)
3	Authenticated Key Agreement	PACE-KA protocol PACE-ECDH-GM-AES-CBC-CMAC-128/192/256 with SHA-{1, 224, 256}	TR-03110-2, chap. 3.2 [29] (PACEv2), TR-03110-3 [30], TR-03109-2 [25]	|nonce| = 128 bit PWD size: 10-16 decimals derived AES key size: 128/192/256 bits	TR-03109-3 [27], TR-03110-2 [29]	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 [36] (AES), SP800-38A [37] (CBC), ISO 10116 [39] (CBC)	|k| = 128, 192, 256, |challenge|=64	TR-03109-3 [27], TR-03116-3, chap. 2.1 [28]	FCS_COP.1/PACE-ENC FCS_CKM.1/PACE
5	Integrity	AES in CMAC mode	FIPS 197 [36] (AES), SP800-38B [38] (CMAC), RFC 4493 [40]) CMAC)	|k| = 128, 192, 256	TR-03109-3 [27], TR-03116-3, chap. 2.1 [28]	FCS_COP.1/PACE-MAC
6	Trusted Channel	Secure messaging in ENC_MAC mode (established during PACEv2)	ISO 7816-4 [43], TR-03110-2, chap. 3.2 [29] (PACEv2)		TR-03109-3 [27], TR-03110-2 [29], TR-03116-2, chap. 3.2, 4.2 [28]	FTP_ITC.1 trusted channel between the TOE and the Smart Meter Gateway
7	Cryptographic Primitive	ECDSA signature verification / generation without Hash	TR-03111, chap. 4.2 [31]	Key sizes corresponding to the used elliptic curve: BrainpoolP{256,	TR-03109-3 [27], TR-03116-3, chap. 2.2 [28]	FCS_COP.1/VER-ECDSA FCS_COP.1/SIG-ECDSA

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
				384, 512}r1 acc. to RFC 5639 [41] NIST curves P-{256, 384} (secp{256, 384}r1) acc. to FIPS 186-3 [35]		
		Deterministic RNG DRG.4 (using the PTG.2 of the underlying IC)	AIS 20 [4], SP800-90A (Hash_DRGB) [42]	n.a.	TR-03109-3 [27], TR-03116-3, chap. 1.3.3, 8.3, 8.4 [28]	FCS_RNG.1
		ECC key generation	TR-03109-3 [27], TR-03116-3 [28]	Key sizes corresponding to the used elliptic curve: BrainpoolP{256, 384, 512}r1 acc. to RFC 5639 [41] NIST curves P-{256, 384} (secp{256, 384}r1) acc. to FIPS 186-3 [35]	TR-03109-3 [27], TR-03116-3 [28]	FCS_CKM.1/ECC
		ECKA-DH key agreement (only generation of the shared secret value)	TR-03111 [31] (EC Diffie-Hellman), ANSI X9.63 [33] (EC Diffie-Hellman)	Key sizes corresponding to the used elliptic curve: BrainpoolP{256, 384, 512}r1 acc. to RFC 5639 [41] NIST curves P-{256, 384} (secp{256, 384}r1) acc. to FIPS 186-3 [35]	TR-03109-3 [27], TR-03116-3, chap. 2.2 [28]	FCS_CKM.1/ECKA-DH used by the Smart Meter Gateway for TLS handshake
		ECKA-EG key agreement (only generation of the shared secret value)	TR-03111 [31] (EC ElGamal), ANSI X9.63 [33] (EC ElGamal)	Key sizes corresponding to the used elliptic curve: BrainpoolP{256, 384, 512}r1 acc. to RFC 5639 [41] NIST curves P-{256, 384} (secp{256, 384}r1) acc. to FIPS 186-3 [35]	TR-03109-3 [27], TR-03116-3, chap. 2.2 [28]	FCS_CKM.1/ECKA-EG used by the Smart Meter Gateway for content data encryption

Table 3: TOE cryptographic functionality

All cryptographic algorithms listed in Table 3 are implemented by the TOE on base of the Technical Guidelines BSI TR-03109-2 [25], BSI TR-03109-3 [27] and BSI TR-03116-3 [28].

The strength of these cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, Clause 2).

According to the Technical Guidelines BSI TR-03109-3 [27] and BSI TR-03116-3 [28], these algorithms are suitable for authentication and (authenticated) key agreement and for supporting 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. The validity period of each algorithm is mentioned in the official catalogue [28].

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in Table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

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

In addition to the security requirements and hints provided in the user guidance documentation [11], [12], [13], [14], [15], [19], [20], [21] and [22], the following aspects need to be taken into account when using the TOE:

- For specifics concerning key and PIN handling and management refer to the user guidance documents [13], chapter 10, [14], chapter 10 and [15], chapter 2.3.
- The TOE might be delivered by the developer Gemalto SA together with the so-called Key Export Tool (including related guidance documentation). However, this developer-specific tool and its related guidance documentation are neither part of the TOE and its deliverables as listed in Table 2 nor were evaluated in course of the TOE's security evaluation.
- The TOE's security evaluation does not cover a complete conformity check of the TOE's implementation for fulfilment of the requirements defined in the Technical Guideline BSI TR-03109-2 [25]. Furthermore, in the course of the TOE's security evaluation it turned out that the TOE's implementation deviates in some points from the Technical Guideline BSI TR-03109-2 [25] (e.g. concerning the key and PIN handling and management). In view of this, there is explicitly no statement on the TOE's conformity to the Technical Guideline BSI TR-03109-2 [25] – as this is in general part of the qualification of Smart Meter Security Modules that are intended to be used by Smart Meter Gateways in the Smart Metering System – given. In particular, when integrating the TOE into a Smart Meter Gateway and when using the TOE this issue should be taken into account.

11. Security Target

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

12. 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
GP	Global Platform
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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 4, September 2012
https://www.commoncriteriaportal.org

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7]
https://www.bsi.bund.de/AIS

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

[7] specifically

- AIS 1, Version 13, 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 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 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 BSI-DSZ-CC-1003-2018, Security Target of Security Module for Smart Meter Gateway, D1359877, Version 2.1, 3 August 2018, Gemalto (confidential document)

[7] Security Target Lite BSI-DSZ-CC-1003-2018, Security Target Lite of Security Module for Smart Meter Gateway (PUBLIC version), D1359877, Version 2.1p, 3 August 2018, Gemalto (sanitised public document)

[8] 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 Informationstechnik (BSI)

[9] ETR BSI-DSZ-CC-1003-2018, Evaluation Technical Report – Summary (ETR Summary) for Smart Meter Gateway Security Module Application on MultiApp V4 Revision A, Version 3, 10 August 2018, TÜV Informationstechnik GmbH (confidential document)

[10] Configuration List BSI-DSZ-CC-1003-2018, Configuration List for Smart Meter Gateway Security Module Application on MultiApp V4 Revision A, File M1010878_BLITZ_SMGW v1.1,Version 1.2, 3 August 2018, and File LIS_SMGWSMV11_CAR_LBL03_1.65.1.7.1.5.1.20, Gemalto (confidential document)

[11] Preparation Guidance for Smart Meter Gateway Security Module V1.1, D1393787, Release 1.2, 3 August 2018, Gemalto

[12] Operational Guidance for Smart Meter Gateway Security Module V1.1, D1393788, Release 0.9, 17 July 2018, Gemalto

[13] Smart Meter Gateway Security Module V1.1 - Personalization and Operational Life Cycle (SEID01) - User Guide, D1413164G, 3 August 2018, Gemalto

[14] Smart Meter Gateway Security Module V1.1 - Integration and Pre-Personalization Life Cycle (SEID02) - User Guide, D1422373F, 3 August 2018, Gemalto

[15] Integration and Pre-Personalization Guideline, D1386918C, Release 1.6, 31 July 2018, Gemalto

[16] Rapport de certification ANSSI-CC-2017/54, Plateforme JavaCard MultiApp V4.0 - PACE en configuration ouverte basée sur l'Operating System JLEP3 masquée sur le composant SLE78CLFX4000PH (M7892 G12), 25 September 2017, ANSSI

[17] MultiAppV4 JCS with PACE Security Target, Version 1.0, 25 July 2017, Gemalto

[18] ETR Lite for Composition - OASIS-EXT Project, Product ref.: MultiAppV4 on Infineon Technologies AG M7892 G12, Version 1.1, 7 August 2017, Serma Safety & Security

[19] MultiApp V4 – AGD_PRE document – Javacard Platform, D1390316, Version 1.1, 6 June 2016, Gemalto

[20] MultiApp V4 – AGD_OPE document – Javacard Platform, D1390321, Version 1.2, 12 May 2017, Gemalto

[21] Rules for applications on Multiapp certified product, D1390963_EXT, Release 1.1, June 2017, Gemalto

[22] MultiApp ID Operating System - Reference Manual, D1392687A, 15 February 2017, Gemalto

[23] Certification Report BSI-DSZ-CC-0891-V2-2016 for Infineon Security Controller, M7892 Design Steps D11 and G12, with optional RSA2048/4096 v2.03.008, EC v2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries, symmetric crypto library v2.02.010 and with specific IC dedicated software (firmware) from Infineon Technologies AG, BSI

[24] Technische Richtlinie BSI TR-03109-1: Smart Meter Gateway - Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, Version 1.0, 18.03.2013, Bundesamt für Sicherheit in der Informationstechnik, BSI

[25] Technische Richtlinie BSI TR-03109-2: Smart Meter Gateway - Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, Version 1.1, 15.12.2014, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[26] Technische Richtlinie BSI TR-03109-2 Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, 17.12.2014, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[27] Technische Richtlinie BSI TR-03109-3: Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen, Version 1.1, 17.04.2014, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[28] Technische Richtlinie BSI TR-03116-3: Kryptographische Vorgaben für Projekte der Bundesregierung – Teil 3: Intelligente Messsysteme, März 2015, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[29] Technical Guideline BSI TR-03110-2, Advanced Security Mechanisms for Machine Readable Travel Documents - Part 2 - Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.20, 2015, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[30] Technical Guideline BSI TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents - Part 3 - Common Specifications, Version 2.20, 2015, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[31] Technical Guideline BSI TR-03111: Elliptic Curve Cryptography, Version 2.0, 28.06.2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

[33] American National Standard X9.63, Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011, American National Standards Institute (ANSI)

[34] Federal Information Processing Standards Publication 180-4 (FIPS PUB 180-4), Secure Hash Standard (SHS), March 2012, U.S. Department of Commerce/National Institute of Standards and Technology (NIST)

[35] Federal Information Processing Standards Publication 186-3 (FIPS PUB 186-3), Digital Signature Standard (DSS), 2009, U.S. Department of Commerce/National Institute of Standards and Technology (NIST)

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

[37] Recommendation for Block Cipher Modes of Operation: Methods and techniques, NIST Special Publication 800-38A, 2001, National Institute of Standards and Technology (NIST)

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

[39] ISO/IEC 10116, Information technology – Security techniques – Modes of operation for an n-bit block cipher, 2006, International Organization for Standardization (ISO)

[40] RFC 4493 - The AES-CMAC Algorithm, June 2006, JH. Song, R. Poovendran, J. Lee, T. Iwata, IETF

[41] Elliptic Curve Cryptography (ECC), Brainpool Standard Curves and Curve Generation, RFC 5639, March 2010, IETF

[42] Special Publication 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Rev. 1, April 2014, National Institute of Standards and Technology (NIST)

[43] ISO/IEC 7816-4, Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange, 2014, International Organization for Standardization (ISO)

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 10.4.
- 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 11.
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 12 to 16.
- 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 http://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target Lite [7] provided within a separate document

Annex B: Evaluation results regarding development and production environment

Annex B of Certification Report BSI-DSZ-CC-1003-2018

Evaluation results regarding development and production environment

The IT product Smart Meter Gateway Security Module Application on MultiApp V4 Revision A (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations and by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 18 September 2018, 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) Gemalto Singapore, 12 Ayer Rajah Crescent, Singapore 139941, Singapore (SW development).

b) Gemalto Pont Audemer, Z.I. Saint Ulfrant, Rue de Saint Ulfrant, 27500 Pont Audemer, France (TOE packaging, testing and pre-personalisation)

c) For development and production sites regarding the underlying Java Card Platform JavaCard MultiApp V4.0 including the underlying IC Infineon M7892 G12 please refer to the Certification Reports ANSSI-CC-2017/54 ([16]) and BSI-DSZ-CC-0891-V2-2016 ([23]).

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6] and [7]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [7]) are fulfilled by the procedures of these sites.

Note: End of report