Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1037-2018

for

STSAFE-J100-BS Smart Meter Security Module V2.1.6

from

STMicroelectronics

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-1037-2018 (*)

STSAFE-J100-BS Smart Meter Security Module V2.1.6

from	STMicroelectronics
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

SOGIS
Recognition Agreement

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, 17 May 2018

For the Federal Office for Information Security

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

Bernd Kowalski
Head of Division

L.S.

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 STSAFE-J100-BS Smart Meter Security Module V2.1.6 has undergone the certification procedure at BSI.

The evaluation of the product STSAFE-J100-BS Smart Meter Security Module V2.1.6 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 19 April 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: STMicroelectronics.

The product was developed by: STMicroelectronics.

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 17 May 2018 is valid until 16 May 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 STSAFE-J100-BS Smart Meter Security Module V2.1.6 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] STMicroelectronics
Z.I Marcianise Sud
81025 Marcianise (CE)
ITALY

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) STSAFE-J100-BS Smart Meter Security Module V.2.1.6 is a composite product consisting of a smartcard application implementing the security module of a smart meter gateway designed as a Java Card Applet integrated on STMicroelectronics STSAFE-J Java Card Platform designed on the ST31H320 hardware platform (ST31H320 security integrated circuit with dedicated software and embedded cryptographic library).

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile 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 [9], chapter 10. 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_SIG_GEN	Digital Signature Generation
SF_SIG_VER	Digital Signature Verification
SF_KA_TLS	Key Agreement for TLS
SF_KA_CDE	Key Agreement for Content Data Encryption
SF_KEY_GEN	Key Pair Generation
SF_RND_GEN	Random Number Generation
SF_PACE_AUTH	Component Authentication via PACE
SF_SM	Secure Messaging
SF_AC	Access Control
SF_CRY	Cryptographic Support
SF_PRO	Protection of data relevant for the Gateway

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 12.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 8.2. 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 [9], chapter 8.

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:

STSAFE-J100-BS Smart Meter Security Module V2.1.6

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW+ SW	STSAFE-J100-BS applet on platform STSAFE-J as QFN32 package	V2.1.6	The modules in QFN32 plastic package are packed in sealed reels and shipped by trusted carrier (UPS, DHL, etc.) to the customer.
2	DOC	Operational user guidance [OPE]	Rev. E	Signed and Encrypted pdf document delivered to customers under NDA via Email or a printed copy available only upon explicit request
3	DOC	Preparation procedures guidance [PRE]	Rev. E	Signed and Encrypted pdf document delivered to customers under NDA via Email or a printed copy available only upon explicit request

Table 2: Deliverables of the TOE

The TOE is delivered after end of phase 4 of the life cycle as defined in [6] and [9]. It is delivered as QFN32 package and is in its fully operational state, ready to be 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] and [12] must be performed.

The guidance documents [11] and [12] are provided to the customer in electronic form, signed and encrypted with PGP using a key size of at least 2048 bits.

The TOE in its certified version can be uniquely identified. The method for identification is described in detail in the operational guidance document [11] in chapter 6. The version of the TOE is coded in the elementary file EF.SecModTRInfo that can be freely with the READ RECORD command by the user. The card production life cycle data (CPLC) such as Operating System Release Date and Operating System ID can be retrieved with the GP command GET DATA for tag 0x9f7f. The values must match the data as given in [11] chapter 6 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:

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

Specific details concerning the above mentioned security policies can be found in chapter 11 of the Security Target [6] and [9].

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: Appropriate technical and/or organizational security measures in the phase of the integration of the Gateway and the TOE in the life cycle model shall be applied in order to guarantee for the confidentiality, integrity and authenticity of the assets of the TOE to be protected with respect to their protection need. In particular, for the TOE, this shall hold for the generation, installation and import of initial key, certificate and PIN material. The Integrator shall in particular take care for consistency of key material in key objects and associated certificates as far as handled in the framework of the integration of the Gateway and the TOE
- OE.OperationalPhase: Appropriate technical and/or organizational measures in the operational phase of the integrated Gateway shall be applied in order to guarantee for the confidentiality, integrity and authenticity of the assets of the TOE to be protected with respect to their protection need. In particular, this shall hold for key and PIN objects stored, generated and processed in the operational phase of the integrated Gateway
- OE.Administration: The administration of the integrated TOE, in particular related to the administration of the TOE's file and object system consisting of folders, data files and key objects, shall take place under the control of the Gateway Administrator
- OE.TrustedAdmin: The Gateway Administrator shall be trustworthy and well trained
- OE.PhysicalProtection: The TOE shall be physically and logically embedded into a Gateway that is certified according to PP-0073 [17] (whereby the integration is performed during the integration phase of the life cycle model)
- OE.KeyAgreementDH: The Gateway shall securely implement the Diffie-Hellman key agreement (ECKA-DH) according to TR-03109-2 [18] and TR-03109-3 [19]

- OE.KeyAgreementEG: The Gateway shall securely implement the ElGamal key agreement (ECKA-EG) according to TR-03109-2 [18] and TR-03109-3 [19]
- OE.PACE: The Gateway shall securely implement the PACE protocol according to TR-03110-2 [20], TR-03109-2 [18] and TR-03109-3 [19] for component authentication between the Gateway and the TOE. In the framework of the PACE protocol session keys for securing the data exchange between the Gateway and the TOE (trusted channel) are negotiated
- OE.TrustedChannel: The Gateway shall perform a trusted channel between the Gateway and the TOE for protection of the confidentiality and integrity of the sensitive data transmitted between the authenticated Gateway and the TOE

Details can be found in the Security Target [6] and [9], chapter 9.2.

5. Architectural Information

The TOE is a composite product consisting of a Java Card Applet based on a certified Java Card Platform (STSAFE-J Java Card Platform) that comprises a certified IC (ST31H320 including optional cryptographic library NESLIB). The TOE’s architecture consists of the following subsystems:

- SB01_DIS: TOE APDU command dispatcher subsystem
- SB02_SIG&AUTH: The digital signature generation/verification and authentication subsystem
- SB03_KEYADMIN&GEN: Key pair generation and key administration subsystem
- SB04_KA: Key agreement subsystem
- SB05_IAP: Internal Application subsystem
- SB06_FS: File system subsystem
- SB07_JCP: The Java Card platform STSAFE-J subsystem

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

7.1. Developer's Test according to ATE_FUN

Testing was performed by the developer using the external interfaces of the TOE, i.e. its ISO7816 APDU interface. The test scenarios cover all defined external interfaces and follow the following basic design: The parameter space for all external interfaces considers as input values:

- sample average value,
- boundary values,

- values beyond the boundary, and
- erroneous values.

Different test approaches were used with regard to functional tests, atomicity (card tearing) and termination tests.

All test scenarios were found to be well described and repeatable by stating all its ordering dependencies and preconditions to be fulfilled. Expected results in form of status words were found to be unambiguously and correctly defined with regard to its expected behaviour.

All actual results were consistent to its expected results. Thus, the developer's testing showed that the TOE matches its defined and expected behaviour and security functionality.

The tested security functionality covered inter alia:

- 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, and
- Secure Messaging.

All TSFs as described in the security target were found to be adequately addressed by developer's testing.

7.2. Evaluator Tests

Independent Testing according to ATE_IND

Approach for independent testing:

- Examination of 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 is operating as specified using iterations of developer's tests.
- Independent testing was performed at the Evaluation Body with the TOE developer test environment and additional Evaluation Body test equipment using equipment that is equivalent to the set of resources used by the developer.

TOE test configurations:

- The TOE was tested in its final configuration on a certified closed Java Card Platform on a certified IC.
- Tests were performed in both security environments SEID=01 and SEID=02, with focus on SEID=01 (Normal and Personalisation usage).

- Repetition of developer tests was performed with a test configuration differing from the final configuration. The test configuration that was used does not affect the results of the tests and results are therefore applicable on the final configuration of the TOE.

Subset size chosen:

- During sample testing the evaluator chose to repeat a subset of the developer tests at the Evaluation Body for IT Security in Essen.
- A subset of the developer's tearing tests was repeated. Sampling was performed in accordance with CC sampling rules such that no test approach, interface or test group was completely omitted.
- During independent testing the evaluator used test scripts to invoke and test functionality by using the APDU interface as defined in the user guidance of the TOE. Further penetration testing was done for AVA_VAN aspects to verify the self-protection mechanisms of the TOE using state-of-the-art attacks.

Verdict for the activity:

- During the evaluator's TSF subset testing the TOE was operated as specified.
- No unexpected behaviour was observed.

Penetration Testing according to AVA_VAN

Overview:

- The penetration testing was performed using the test environment of TÜViT.
- The TOE in its one possible configuration being intended to be covered by the current evaluation was tested.
- The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential High was actually successful.

Penetration testing approach:

- 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 supported testing activity by enabling the evaluator to verify implementation aspects that could hardly be covered by test cases.
- 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.

TOE test configurations:

- The evaluators used TOE samples for testing that were configured according to the ST. For exceptional cases, open samples where used that do not represent the TOE but were required to adequately test the security behaviour of the TOE.

Verdict for the activity:

- The overall test result is 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 [6] and [9] provided that all measures required by the developer are applied.

7.3. Summary of Test Results and Effectiveness Analysis

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 [6] and [9] provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

STSAFE-J100-BS V.2.1.6.

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 Operational Phase of the TOE (the integrated circuit, IC), ST31H320 including optional cryptographic library NESLIB, Rapport de maintenance ANSSI-CC-2015/59-M01, April 20, 2016
- The Embedded Software:
  - Operating System STSAFE-J Java Card Platform Common Criteria Certified Version by STMicroelectronics
  - The Applet STSAFE-J100-BS version V.2.1.6 by STMicroelectronics
- The associated guidance documentation

The TOE is a composite product with a closed Java Card implementation with a single applet, the STSAFE-J100-BS applet as a single instance. No post-issuance of further applets is possible to the TOE.

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 (see AIS 36). According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations (i.e. on hardware [13] and [14]) have been applied in the TOE evaluation.

(ii) Guidance for Smartcard Evaluation

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

For RNG assessment the scheme interpretations AIS 20 was 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 components 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 [8]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by AVA_VAN.5

Additionally, the requirements of the Technical Guideline TR-03109-2 [18] are met. This is part of the qualification of the STSAFE-J100-BS Smart Meter Security Module V2.1.6 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.

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
Authenticity	ECDSA-signature generation without hashing Id-ecdsa-plain-signatures	ANSI_X9.62 [24] (ECDSA) FIPS_180-2 [25] (SHA)	Key sizes of used elliptic curve brainpoolP{256,384,512}r1 [31]	TR-03109-2 [18]

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application
		TR-03111 [22]	NIST P-{256,384} [26]	
	ECDSA-signature verification without hashing Id-ecdsa-plain-signatures ECDSA-signature verification with hash parameter Id-ecdsa-plain-SHA256/SHA384/SHA512	ANSI_X9.62 [24] (ECDSA) FIPS_180-2 [25] (SHA) TR-03111 [22]	Key sizes of used elliptic curve brainpoolP{256,384,512}r1 [31] NIST P-{256,384} [26]	TR-03109-2 [18]
Authentication	ECDSA-signature verification with hash parameter Id-ecdsa-plain-SHA256/SHA384/SHA512	TR-03109-3 [19], TR-03109-2 [18], TR-03116-3 [23]	Key sizes corresponding to the used elliptic curve brainpool P{256,384,512}r1 [31] NIST P-{256,384} [26]	TR-03109-2 [18]
	ECDSA-signature generation without hashing Id-ecdsa-plain-signatures			
Authenticated Key Agreement	PACE protocol PACE-ECDH-GM-AESCBC-CMAC-128/192/256	TR-03110-2 [20], TR-03109-3 [19], TR-03109-2 [18]	PWD size: minimum 10 char. Maximum 64 char. Derived AES key size: 128/192/256 bits	TR-03109-2 [18]
Key Agreement	ECKA-DH	TR-03111 [22]	Key sizes corresponding to the used elliptic curve brainpool P{256,384,512}r1 [31] NIST P-{256,384} [26]	TR-03109-2 [18]
	ECKA-EG			
Confidentiality	AES in CBC mode	FIPS197 [27] (AES), ISO 10116 [29] (CBC)	Key sizes: 128, 192 and 256 bits	TR-03109-2 [18]
Integrity	AES in CMAC mode	FIPS197 [27] (AES), RFC4493 [30] (CMAC)	Key sizes: 128, 192 and 256 bits	TR-03109-2 [18]
Trusted Channel	Secure messaging in ENC_MAC mode and key established with PACE protocol	ISO7816 [28], TR-03110-3 [21]	AES key sizes: 128/192/256 bits	TR-03109-2 [18]
Cryptographic Primitive	True Random Generator (TRNG) class PTG.2 Deterministic Random Generator (DRBG) class RNG DRG.3	Hash_DRBG of SP800-90A [32]	n.a.	TR-03109-2 [18] / AIS31/20 [4]

Table 3: TOE cryptographic functionality

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

According to TR-03109-2 [18] the algorithms are suitable for Authenticity, Authentication, Authenticated Key Agreement, Key Agreement, Confidentiality and Integrity. An explicit validity period is not given.

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.

11. Security Target

For the purpose of publishing, the Security Target [9] 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

AIS	Application Notes and Interpretations of the Scheme
APDU	Application Protocol Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
OSP	Organizational Security Policy
PIN	Personal Identification Number
PP	Protection Profile
RNG	Random Number Generator

SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
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
http://www.commoncriteriaportal.org

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

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

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

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

[6] Security Target BSI-DSZ-CC-1037-2018, Version Rev.I, September 19th, 2017, STSAFE-J100-BS Security Target, STMicroelectronics (confidential document)

[7] Evaluation Technical Report, Version 4, April 17th, 2018, Evaluation Technical Report Summary, TÜV Informationstechnik GmbH, (confidential 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

[9] Security Target BSI-DSZ-CC-1037-2018, Version Rev. A, April 9th, 2018, STSAFE-J100-BS Security Target Public Version, STMicroelectronics (sanitised public document)

[10] Configuration list for the TOE, Version 2.1.6, Kerkey2 SMARAGD ConfigList (confidential document)

[11] Operational Guidance documentation for the TOE, Rev. E, STSAFE-J100-BS – Operational user guidance, STMicroelectronics

[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 23, Version 3, Zusammentragen von Nachweisen der Entwickler
- AIS 26, Version 9, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 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 4, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 45, Version 2, Erstellung und Pflege von Meilensteinplänen
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[12] Preparative Procedures Guidance documentation for the TOE, Rev. E, STSAFE-J100-BS – Preparative procedures guidance, STMicroelectronics

[13] Rapport de certification ANSSI-CC-2017/23, Plate-forme STSAFE-J, en configuration fermée, version 1.1.4, sur le composant ST31H320 A03, 2017-03-23, ANSSI.

[14] Evaluation Technical Lite Report for composition, STSafe-J Project, STSafe-J on STMicroelectronicsST31H320 A03, Version 1.1, 2017-03-07, SERMA.

[15] Security guidelines for application development on the STSAFE-J100 secure solution, Rev. 2, 2017-01-27, STMicroelectronics.

[16] STSAFE-J on ST31H320 User Manual - Proprietary API Documentation Rev. A, STMicroelectronics.

[17] CC Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Version 1.3, 2014-03-31, BSI-CCPP-0073-2014, Bundesamt für Sicherheit in der Informationstechnik

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

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

[20] Technische Richtlinie 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 2.10, 2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[21] Technische Richtlinie TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents - Part 3 - Common Specifications, Version 2.10, 2012-03-20, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[22] Technische Richtlinie TR-03111, Elliptic Curve Cryptography, Version 2.0, 2012-06-28, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[23] Technische Richtlinie TR-03116-3: Kryptographische Vorgaben für Projekte der Bundesregierung – Teil 3: Intelligente Messsysteme, April 2016, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[24] American National Standard for Financial Services ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), November 16, 2005, American National Standards Institute (ANSI)

[25] Federal Information Processing Standards Publication FIPS PUB 180-2, Secure Hash Standard (SHS), August 2002, National Institute of Standards and Technology (NIST)

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

[27] Federal Information Processing Standards Publication FIPS PUB 197, Advanced Encryption Standard (AES), 2001-11-26, National Institute of Standards and Technology (NIST)

[28] ISO/IEC 7816-4:2013, Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange, 2013, International Organization for Standardization (ISO)

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

[30] RFC 4493 - The AES-CMAC Algorithm, June 2006, JH. Song, R. Poovendran

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

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

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 provided within a separate document.

Annex B: Evaluation results regarding development and production environment

Annex B of Certification Report BSI-DSZ-CC-1037-2018

Evaluation results regarding development and production environment

The IT product STSAFE-J100-BS Smart Meter Security Module V2.1.6 (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 17 May 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) STM/Incard Marcianise, STMicroelectronics Z.I. Marcianise SUD I-81025 Marcianise (CE), Italy (SW Development/Production)

b) For development and production sites regarding the platform please refer to the Certification Report ANSSI-CC-2017/23 ([13]).

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] and [9]) are fulfilled by the procedures of these sites.

Note: End of report