Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1094-2019

for

IBM Enterprise PKCS#11 (EP11) Firmware identifier '2b638e8e' (4768)

from

IBM Research & Development Germany

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-1094-2019 (*)

IBM Enterprise PKCS#11 (EP11)
Firmware identifier '2b638e8e' (4768)

from	IBM Research & Development Germany
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

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

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.

Bonn, 2 August 2019

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: https://www.commoncriteriaportal.org.

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

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 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 IBM Enterprise PKCS#11 (EP11), Firmware identifier '2b638e8e' (4768) has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1002-2018. Specific results from the evaluation process BSI-DSZ-CC-1002-2018 were re-used.

The evaluation of the product IBM Enterprise PKCS#11 (EP11), Firmware identifier '2b638e8e' (4768) was conducted by atsec information security GmbH. The evaluation was completed on 29 July 2019. atsec information security GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: IBM Research & Development Germany.

The product was developed by: IBM Research & Development Germany.

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 2 August 2019 is valid until 1 August 2024. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security

[5] Information Technology Security Evaluation Facility

Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

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

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product IBM Enterprise PKCS#11 (EP11), Firmware identifier '2b638e8e' (4768) 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] IBM Research & Development Germany
Schönaicher Straße 220
71032 Böblingen

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 IBM Enterprise PKCS#11 firmware (EP11), identified as ‘2b638e8e’, running on the IBM CryptoExpress 6 (4768) cryptographic coprocessor, respectively. It is an implementation of the industry-standard PKCS#11 cryptographic service provider API version v2.20 with some modifications and algorithmic extensions, adapted to requirements typical in enterprise servers. The EP11 firmware provides a stateless backend, relying mainly on host-resident, encrypted datastores to maintain sensitive state, while presenting services as a regular HSM-based PKCS#11 implementation.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

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.

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

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

TOE Security Functionality	Addressed issue
Secure key management	Keys generated by, or imported to the TOE, are always associated with their attributes. The TOE uses several attributes that affect the key management, e.g., CKA_MODIFICABLE allows to change the key attributes, while CKA_IBM_RESTRICTABLE allows attribute changes but no addition of new attributes. Key or state exported to the host is protected with regards to integrity and confidentiality using authenticated encryption using wrapping keys and MAC keys that are maintained within the TOE ("maintenance of host-based keystore"). Optionally, exported objects can be associated with session identifiers.
Cryptographic operations	The following groups of functional services are offered to users: • Generate or derive keys: AES, TDES, RSA, EC (elliptic curve, prime field, NIST P-curves, or BP curves), DSA, generic secret keys • Generate or verify digital signatures with asymmetric keys: RSA, ECDSA, DSA • Key agreement: ECDH • Encrypt or decrypt data with asymmetric keys: RSA • Encrypt or decrypt data with symmetric keys: AES, TDES • Cryptographic hash functions: SHA-1 and SHA-2 family of hash functions (SHA-224, SHA-256, SHA-384, SHA-512) • Random-number generation: DRNG (HASH_DRBG) • Storage, use, and disposal of secrets within the TOE
Application identification and authentication	The TOE distinguishes applications using its services based on either proof of possession, or cryptographic authentication, in the cases where

TOE Security Functionality	Addressed issue
	users of services need to be identified. Non-administrative services are available without authentication, unless they reference host-resident state, which involves sessions. Objects bound to sessions are usable as long as the corresponding session is registered within the TOE. Administrators are identified and authenticated through their X.509 public-key certificates, which are loaded into the TOE with the corresponding private keys resident outside the TOE. Administrators are identified through signatures on state-changing administrative commands. Lists of administrators are maintained for the whole card, and separate lists exist for each internal domain. There are several administrative commands that require the signatures of more than one administrator (with the number of signatures being configurable).
Policy enforcement	Usage restrictions combine object-level attributes and those of the domain where the request is executed. Objects feature fundamental functional restrictions, such as allowing encryption/signature generation/etc. by a given object, with the capabilities stored as attributes within each object, for instance encrypt or sign data. Domain restrictions can be defined through control points which represent a diverse set of functional-level usage restrictions, e.g., key types, key strength, but also the use of certain group of algorithms. Objects must be allowed for each of these restrictions to become eligible for use.
Administrative services	Administrative commands includes queries and commands. Queries are allowed for everyone, while administrative commands that change state need to be signed by an administrator. The TOE provides different groups of administrative commands, e.g., administrator management, key or state import/export, management of control points, etc.
Selftests	During startup, or upon demand, a set of known-answer tests are executed. Failure prohibits subsequent cryptographic operations, and may be remedied by restarting the module.
Audit	Security-relevant operations within the TOE are audited through an HSM-resident audit subsystem. It is based on a hash chain and , therefore, immune to insertion or deletion. Audit records may contain fields, which are public, and indirect, non-sensitive information derived from keys, but NEVER sensitive values. Indirect information, such as types, sizes, or truncated hashes of keys, MAY be logged. Audit records, when queried through non-administrative query, are returned without additional signatures. Administrative query responses are returned digitally signed, signing the same audit-record content, when requested. Actually recorded events are for example startup/shutdown of the TOE, time updates, selftest completion, import/export keys, etc.
Random-number generation	The TOE uses a hybrid random-number generation process. A hardware-provided “true-random” (TRNG) provides a seed, which is conditioned and then post-processed with a stateful pseudo-random generator (DRNG). The TRNG seed is obtained from the HSM-internal entropy source. The DRNG is based on a non-invertible, cryptographic hash function (SHA-256), instantiating the DRBG structure from ISO 18031:2011, C.2.2.

Table 1: TOE Security Functionalities

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

The assets to be protected by the TOE are defined in the Security Target [6], chapter 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], chapter 3.

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:

IBM Enterprise PKCS#11 (EP11), Firmware identifier '2b638e8e' (4768)

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
IBM Crypto Express 6 EP11 (4768)				
1	FW	Segment 0	32f1f0ac-fe328a14 ecc8c022 8a1199e1 3368b47b bc2bd7f2 888e0566 bfdfd73f	Embedded in HSM
2	FW	Segment 1	d608bcad-ec5513fd a6f6a026 03f241c9 dd935178 b2d07745 54089693 f7bbcbe3	Embedded in HSM
3	FW	Segment 2	b7961613-dae86fe5 301054d7 3b1e24c6 764dfb28 45e7e4b3 fc04fc01 e25bc6de	Embedded in HSM
4	FW	Segment 3	7ce8e3c2-e5988088 62e9cda8 e5acff4f 9eb58eb9 87bd1eff d0a7dbea 46e2e02c	Embedded in HSM
5	FW	Enterprise PKCS#11	2b638e8e-74ec55f7 8477a357 9331f437 db66b9d5 3523ecbb a377420b 7b9fd046	Embedded in HSM
6	HW	Crypto Engines hardcoded in the Andretta ASIC	Instantiated in the IBM 4768 Cryptographic Coprocessor	Embedded in HSM
TOE guidance				
7	DOC	Enterprise PKCS#11 (EP11) Library structure	2019-03-06 SHA256 sum: 9bf799c3b02d709dc4b86d7596ca2b292e4b e2c237c8570b4b9bc2566eb1d7ef9	Download: https://www.ibm.com/downloads/cas/WXRDPRAN

No	Type	Identifier	Release	Form of Delivery
8	DOC	4767 PCIe Cryptographic Coprocessor Installation Manual	First edition, Sept 2016 SHA256 sum: 1f6d91ae7465f3d7562bfa6b715872fa02b52391412000c530760e515013b777	Download: https://www.ibm.com/downloads/cas/RMQG64AV
9	DOC	Trusted Key Entry Workstation (TKE)	2019-02-16 SHA256 sum: 95bef88d6927c2179af3ead51d7e34e371ef310543315e907ea5e3fb9ac0e8dc	Download: https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zosv2r3izst100/$file/izst100_v2r3.pdf
HSM-enclosures (containing the TOE and non-TOE parts)				
10	HW	IBM 4768 PCIe Cryptographic Coprocessor	001	By service personnel

Table 2: Deliverables of the TOE

The TOE is delivered as part of the HSM-enclosure, which is part of the TOE environment (except for the hardware parts listed as #5 in Table 2). The TOE is exclusively delivered to the end user by dedicated IBM personnel that will also install the PCIe card in the user's environment (typically a z System). The developer does not offer the product containing the TOE by any other delivery procedure. The guidance can be obtained via https-secured download and verified using the SHA-256 hash values listed in Table 2.

The end user is able to identify the TOE by inspecting details of the cryptographic coprocessor or accelerator using the toolset of the operating system that operates the HSM device. Each of the FW segments is identified by name and by a SHA-256 hash value. The expected hash values are the ones listed in Table 2.

Please note that the TOE does not comprise the complete Cryptographic Coprocessor, but rather its firmware running inside the HSM, as well as cryptographic algorithms implemented in an ASIC and ASIC/FPGA, respectively. The evaluation of those hardware parts of the TOE was based on a VHDL code review, aspects of the life cycle (ALC) have not been examined regarding the hardware production.

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 services

The TOE provides cryptographic services for asymmetric and symmetric ciphers, including key generation and key destruction policies.

User identification and authentication

The TOE provides user authentication (via sessions) and administrator authentication (via certificates).

Domain control point access control policy

The TOE enforces an access control policy that affects the functions (mainly allowing or disallowing a function) that are triggered by requests for TOE keys or state.

Object security attribute access control policy

The TOE enforces an access control policy, which allows or disallows an operation triggered by a session request on TOE objects based on the attributes bound on that object.

Session object access control policy

The TOE enforces an access control policy, which allows or disallows an operation triggered by a session request on a TOE key or state based on the existence and validity of a session, and the association of a TOE key or state with a session.

Domain access control policy

The TOE verifies the attributes of user data when imported or exported from outside the TOE. The control is based on domain identifiers and does not allow usage of objects from one domain in another except if the related operation is a card-level administrative request.

This includes the consistent interpretation of attributes of cryptographic keys when shared with an external entity.

Inter-TSF detection of modification

The TOE rejects TSF data transmitted from an external IT product if the data integrity check fails. That includes signature verification of administrator commands.

Auditing

The TOE creates audit events for its operation (e.g. startup) as well as key management and administrator operation, including a timestamp from a reliable time source. The audit events are provided in a user-interpretable format, and the audit trail is protected against unauthorized deletion, and prevents overwriting of recent audit events when the audit trail becomes full.

Residual information protection

Previous information from a resource is made unavailable upon deallocation.

Management of TSF

The TOE provides management functions to administrators:

- manage administrators
- manage control points

The TOE provides management functions to users:

- manage their session data
- manage their object key attributes

TSF protection through self-tests

The TOE runs self tests to demonstrate the correct operation of the cryptographic primitives, and ensures a secure state through prohibiting further operation in case the self tests fail.

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:

- Key generation by IT environment
- Analysis of TOE audit data
- Personal security
- Availability of cryptographic key and key material
- Physical protection

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

5. Architectural Information

Internal software is divided into four layers, i.e. the segments 0 to 3. The base two layers, and a stub in the third layer control security and configuration of the module:

- Layer 0: Permanent POST 0 (Power-on Self Test) and Miniboot 0 (security bootstrap). This code is in ROMmed flash, bootstrapping the entire module, effectively non-modifiable.
- Layer 1: Rewritable POST 1 and Miniboot 1, responsible for self-test and some card-level management functionality. The upper two layers customize the operation of each individual device.
- Layer 2: System software. Supervisor-level code, including any system-provided device drivers, but excluding the startup stub.
- Layer 3: Application code, including userspace drivers, if any.

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 testing

379 automated tests have been executed on the 4768 CryptoExpress card.

All tests were successfully executed with the results being consistent with the expected results.

7.2. Evaluator testing and penetration testing

The evaluator repeated all automated developer tests on the 4768 model. In addition, 10 new additional functional evaluator tests have been executed on the 4768 model.

All test were executed successfully with no relevant deviations from the expected function behavior.

7.3. Evaluator penetration testing

The evaluator performed 8 penetration tests on the 4768 model.

All test were executed successfully with no relevant deviations from the expected function behavior that could be exploitable in the intended environment of the TOE.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The evaluated configuration requires the TOE (or rather its enclosing HSM) to be installed in an IBM zSeries mainframe that runs a Common Criteria evaluated version of the z/OS operating system. The TOE is accessed via ICSF and TKE.

Function-wise, the guidance documentation provides configuration requirements specific to the evaluated configuration through mandatory control point settings. Details of the required control point settings are documented in [9], Enterprise PKCS#11 (EP11) Library structure, appendix ‘Wire format’, section 8.3.

Furthermore, the following activities are not allowed in the evaluated configuration:

- manual key import
- key transport with enforced attribute binding (no separation of keys and attributes)
- firmware updates

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 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)

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1002-2018, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on firmware changes and card 4768 as new platform.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target ’
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

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

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.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available, the user of the TOE should request the sponsor to provide a re-certification. In the meantime, a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
ASIC	Application-Specific Integrated Circuit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FPGA	Field-Programmable Gate Array
FW	Firmware
HSM	Hardware Security Module
HW	Hardware
ICSF	Integrated Cryptographic Service Facility
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PCIe	Peripheral Component Interconnect Express
PKCS	Public Key Cryptography Standards
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TKE	Trusted Key Entry
TOE	Target of Evaluation
TSF	TOE Security Functionality

13.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

Package - named set of either security functional or security assurance requirements

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

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

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

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

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

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

14. Bibliography

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

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

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

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

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, Reuse of evaluation results

[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-1094-2019, Version 1, Rev. 288, 2019-03-20, IBM Enterprise PKCS#11, IBM Research Zürich and IBM Böblingen/Poughkeepsie

[7] Evaluation Technical Report, Version 2, 2019-07-10, Final Evaluation Technical Report, atsec information security GmbH (confidential document)

[8] Configuration lists for the TOE:

Configuration list of static content measured by SHA256 hashes, Version 1.0, 2016-12-12, IBM (confidential document)

EP11 configuration list BOE, Version 1, 2019-03-27, IBM (confidential document)

EP11 configuration list (BOE) for documentation files, Version 1, 2017-07-14, IBM (confidential document)

Configuration list from git, Charlotte part; Version 1, Date 2019-03-14, IBM (confidential document)

Notes for the configuration list from git, Charlotte part; Version 1, Date 2019-03-14, IBM (confidential document)

Hardware configuration list for IBM 4765 and 4767 EP11 HSMs, Version 1.0, 2017-08-31, IBM (confidential document)

[9] Guidance documentation of the TOE:

Enterprise PKCS#11 (EP11) Library structure, 2019-03-06, IBM

4767 PCIe Cryptographic Coprocessor Installation Manual, First edition, September 2016, IBM

Trusted Key Entry Workstation (TKE), z/OS Version 2 Release 3 , 2019-02-16, IBM

C. Excerpts from the Criteria

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

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

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

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Overview and rating of cryptographic functionalities implemented in the TOE

Annex B of Certification Report BSI-DSZ-CC-1094-2019

Overview and rating of cryptographic functionalities implemented in the TOE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
1	Cryptographic Primitive	TDES encryption and decryption (ECB and CBC mode)	FIPS 46-3 NIST SP 800-38A (2001 Edition)	168	No
2	Cryptographic Primitive	AES encryption and decryption (ECB and CBC mode)	FIPS 197 NIST SP 800-38A (2001 Edition)	128, 192, 256	No (EBC)
					Yes (CBC)
3	Cryptographic Primitive	SHA-1	FIPS 180-4	N/A	No
4	Cryptographic Primitive	SHA-{224, 256, 384, 512}	FIPS 186-4	N/A	Yes
5	Cryptographic Primitive	RSA encryption, decryption, signature generation, and signature verification	RFC 3447 (PKCS#1 V2.1)	2048, 3072, 4096	Yes
6	Cryptographic Primitive	DSA signature generation and verification	FIPS 186-4	{L=2048, N=224} {L=2048, N=256} {L=3072, N=256}	Yes
7	Cryptographic Primitive	ECDSA signature generation and verification (NIST curves)	ANSI X9.62-2005 FIPS 186-4	192	No
				224, 256, 320, 384, 521	Yes
8	Cryptographic Primitive	ECDSA signature generation and verification (Brainpool curves)	ANSI X9.62-2005 RFC 5639	192	No
				224, 256, 320, 384, 512	Yes
9	Cryptographic Primitive	ECDSA signature generation and verification (secp256k1 curve)	ANSI X9.62-2005 SEC2 v2	256	Yes
10	Cryptographic Primitive	ECDH (NIST curves)	ANSI X9.62-2001 FIPS 186-4	192	No
				224, 256, 320, 384, 521	Yes
11	Cryptographic	ECDH	ANSI X9.62-2001	192	No

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
	Primitive	(Brainpool curves)	RFC 5639	224, 256, 320, 384, 512	Yes
12	Cryptographic Primitive	ECDH (secp256k1 curve)	ANSI X9.62-2001 SEC2 v2	256	Yes
13	Key Generation	RSA	FIPS 186-4 (algorithm C9)	2048, 3072, 4096	Yes
14	Key Generation	DSA	FIPS 186-4 Section (4.4.1)	{L=2048, N=224} {L=2048, N=256} {L=3072, N=256}	Yes
15	Key Generation	ECDSA (NIST and Brainpool curves)	FIPS 186-4 (Section 6.2.1) FIPS 186-4 RFC 5639	192	No
				224, 256, 320, 384, 512, 521	Yes
16	Random Number Generation	Hash_DRBG with SHA-256 (seeded by an internal noise source)	NIST SP 800-90A (revision 1) FIPS 186-4	N/A	N/A

Table 3: TOE cryptographic functionality

Note: End of report