Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1119-2023

for

cryptovision CSP – Java Card applet providing Cryptographic Service Provider version 2.0

from

cv cryptovision GmbH

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1119-2023 (*)

cryptovision CSP – Java Card applet providing Cryptographic Service Provider version 2.0

from	cv cryptovision GmbH
PP Conformance:	Cryptographic Service Provider (CSP) Version 0.9.8, 19 February 2019, BSI-CC-PP-0104-2019, Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au) Version 0.9.5, 8 April 2019, BSI-CC-PP-0107-2019
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations , by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

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

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

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

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

Bonn, 24 January 2023

For the Federal Office for Information Security

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

Sandro Amendola L.S.
Head of Division

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- 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 3 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.sogis.eu.

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

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

3.2. International Recognition of CC – Certificates (CCRA)

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

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

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

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ 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 cryptovision CSP – Java Card applet providing Cryptographic Service Provider version 2.0 has undergone the certification procedure at BSI.

The evaluation of the product cryptovision CSP – Java Card applet providing Cryptographic Service Provider version 2.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 17 January 2023. 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: cv cryptovision GmbH.

The product was developed by: cv cryptovision GmbH.

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

5. Validity of the Certification Result

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

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

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

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited.

The certificate issued on 24 January 2023 is valid until 23 January 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

[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 cryptovision CSP – Java Card applet providing Cryptographic Service Provider version 2.0 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] cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen
Deutschland

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 a composite TOE, is named “cryptovision CSP – Java Card applet providing Cryptographic Service Provider” and was evaluated in version 2.0. It is based on a Java Card and provides cryptographic services according to protection profile and respective configuration [8].

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profiles Cryptographic Service Provider (CSP) Version 0.9.8, 19 February 2019, BSI-CC-PP-0104-2019,
Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au) Version 0.9.5, 8 April 2019, BSI-CC-PP-0107-2019 [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 ALC_DVS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 6.

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

TOE Security Functionality	Addressed issue
TSF_Access	Access Control
TSF_Admin	Administration
TSF_Secret	Secret key management
TSF_Crypto	Cryptographic operations
TSF_Secure Messaging	Secure Messaging
TSF_Auth	Authentication protocols
TSF_Integrity	Integrity protection
TSF_OS	Javacard OS Security Functionalities

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 1.3.6.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 3.1.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], 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:

cryptovision CSP – Java Card applet providing Cryptographic Service Provider version 2.0.

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
Production and delivery variant 1 (high volume)				
1		cryptovision CSP software layer package	2.0, Identification according to [16] sec. 3.2	PGP encrypted and signed e-mail to NXP.
2		JCOP 4.7 (Hardware + IC Embedded Software)	4.7, Identification according to [18] / [17]. The configuration of the SE051 is 0x045A (cf. table 4.10 in [17]). The module configuration is 0x0815 (cf. table 5.3 [17]).	Delivery as mandated by the certification of JCOP 4.7. (Cert.-ID: NSCIB-CC-0095534-2MA)
3		cryptovision CSP – Java Card configuration providing a Cryptographic Service Provider (CSP) – Preparation Guidance (AGD_PRE) (see [16])	v1.0.19, SHA-256: 621F34024754A8F833D6FAC6B8EC558598D9E8C2789615DA2ACEB96C5BF9F8DB	PGP encrypted and signed e-mail.
4		cryptovision CSP v2.0 - Java Card configuration providing a Cryptographic Service Provider (CSP) - Operational Guidance (AGD_OPE) (see [15])	v1.0.26 SHA256: C32C7EF0B11D3C05A04FE67441B03FC37BC71EAB8BC4EB3918C31797E91E974A	PGP encrypted and signed e-mail.
5		Cryptographic Keys (see [14] sec.4)	--	Transport according to NXP application note “P71 Trust Provisioning – PGP Key import for P71 products”. Keys are transferred via PGP encrypted and signed e-mail to NXP.

No	Type	Identifier	Release	Form of Delivery
Production and delivery variant 2 (local)				
6		cryptovision CSP software layer package	2.0, Identification according to [16] sec. 3.2	Encrypted and signed APDUs delivered by PGP encrypted and signed e-mail.
7		JCOP 4.7 (Hardware + IC Embedded Software)	4.7, Identification according to [18] / [17]. The configuration of the SE051 is 0x045A (cf. table 4.10 in [17]). The module configuration is 0x0815 (cf. table 5.3 [17]).	Delivery as mandated by the certification of JCOP 4.7. (Cert.-ID: NSCIB-CC-0095534-2MA)
8		cryptovision CSP – Java Card configuration providing a Cryptographic Service Provider (CSP) – Preparation Guidance (AGD_PRE) (see [16])	v1.0.19, SHA-256: 621F34024754A8F833D6FAC6B8EC558598D9E8C2789615DA2ACEB96C5BF9F8DB	PGP encrypted and signed e-mail.
9		cryptovision CSP v2.0 - Java Card configuration providing a Cryptographic Service Provider (CSP) - Operational Guidance (AGD_OPE) (see [15])	v1.0.25 SHA256: C8FE7BE95B289BC7D06F7F2E3B3A0336BA98C79D78CB8A7D036EC93AD191D075	PGP encrypted and signed e-mail.
10		Cryptographic Keys (see [14] sec.4)	--	Keys are transferred via PGP encrypted and signed e-mail.

Table 2: Deliverables of the TOE

Regarding delivery of the TOE:

There are two variants for production and delivery of the TOE. The first variant is the standard high volume production at NXP and the second variant is called local production at a third party.

In both variants the transfer of the CSP application and guidance is done via encrypted and signed e-mail which maintains confidentiality, integrity and authenticity of these deliverables. The delivery of the hardware is covered by the NXP JCOP platform certification. The JCOP 4.7 SE051 is protected by the platform mechanisms.

Also, the mandatory CSP guidance is always provided to the integrator (by the developer).

Regarding identification of the TOE:

The TOE can be identified in accordance with the described processes in [6] and [9] sec.1.3.5 referring to [16] sec.3.2. The identification of the underlying platform is done by command GET DATA (IDENTIFY) and described in the guidance as well.

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:

- Key management,
- Data encryption,
- Hybrid encryption with MAC for user data,
- Data integrity mechanisms,
- Authentication and attestation of the TOE, trusted channel,
- User identification and authentication,
- Access control,
- Security management,
- Protection of the TSF,
- Import and verification of Update Code Package,
- Time stamp,
- Access control on time stamp service, and
- Security Audit.

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 and measures to be taken by the IT environment, the user or the risk manager. The following topics are of relevance,

- OE.CommInf: Communication infrastructure,
- OE.AppComp: Support of the Application component,
- OE.SecManag: Security management,
- OE.SecComm: Protection of communication channel,
- OE.SUCP: Signed Update Code Packages,
- OE.Audit: Review and availability of audit records, and
- OE.TimeSource: External time source.

They are considered in the guidance documentation [15] sec.3.4.1.

5. Architectural Information

Details on the TOE architecture can be found in the Security Target [6] and [9].

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

Developer's testing approach:

The developer considered the following aspects when designing his test approach:

- Tests to cover all TSFI defined in developer documents,
- Good case and bad case tests for each interface defined in the respective developer document and executable on the TOE,
- Tests covering all TSF subsystems in the TOE design.

Verdict for the activity:

All test cases in each test suite were run successfully on this TOE version.

The developer's testing results demonstrate that the TOE operates as expected.

Evaluator tests (ATE_IND):

Independent testing according to ATE_IND was conducted.

The TOE was tested in the one configuration in scope of the certification.

The test results have not shown any deviations between the expected test results and the actual test results.

Evaluator tests (AVA):

Penetration testing according to AVA was also conducted.

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.

The test results have not shown any deviations between the expected test results and the actual test results.

8. Evaluated Configuration

The evaluated TOE configuration is identical with the one described in table 2, which in turn is the delivered product. There is only one configuration of the TOE. For all tests the TOE is configured and parameterized, if necessary, according to the guidance documents. The cryptovision CSP TOE configuration is loaded and installed on the underlying CSP platform. The cryptovision CSP TOE needs to be installed and personalised according to the guidelines given in [15] and [16].

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 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the scheme and technology was used:

AIS:

- Durchführung der Ortsbesichtigung in der Entwicklungsumgebung, AIS 1, Version 14, 11.10.2017, Bundesamt für Sicherheit in der Informationstechnik
- Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC, AIS14, Version 7, 03.08.2010, Bundesamt für Sicherheit in der Informationstechnik
- Gliederung des ETR, AIS19, Version 9, 03.11.2014, Bundesamt für Sicherheit in der Informationstechnik
- Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, AIS20, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik
- Evaluationsmethodologie für in Hardware integrierte Schaltungen, AIS26, Version 10, 03.07.2017, Bundesamt für Sicherheit in der Informationstechnik
- Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, AIS31, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik
- CC-Interpretationen im deutschen Zertifizierungsschema, AIS32, Version 7, 08.06.2011, Bundesamt für Sicherheit in der Informationstechnik
- Öffentliche Fassung eines Security Target (ST-lite), AIS35, Version 2, 12.11.2007, Bundesamt für Sicherheit in der Informationstechnik
- ETR-Zusatz zur Unterstützung von Smartcard Kompositionszertifizierungen (ETR for composition), AIS36, Version 5, 15.03.2017, Bundesamt für Sicherheit in der Informationstechnik
- Terminologie und Vorbereitung von Smartcard-Evaluierungen, AIS37, Version 3, 17.05.2010, Bundesamt für Sicherheit in der Informationstechnik
- Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, AIS46, Version 3, 04.12.2013, Bundesamt für Sicherheit in der Informationstechnik

Other relevant evaluation guidance or documentation:

- JIL Minimum Site Security Requirements, Version 3.0 , February 2020
- Joint Interpretation Library, Application of Attack Potential to Smart-cards, Joint Interpretation Working Group, Version 3.1, 06-2020.
- Joint Interpretation Library, Attack Methods for Smartcards and Similar Devices, Joint Interpretation Working Group, Version 2.4, January 2020

- Composite product evaluation for Smart Cards and similar devices, Joint Interpretation Working Group, Version 1.5.1, May 2018

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_DVS.2 and AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformances: Cryptographic Service Provider (CSP) Version 0.9.8, 19 February 2019, BSI-CC-PP-0104-2019,
  Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au) Version 0.9.5, 8 April 2019, BSI-CC-PP-0107-2019 [8]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5

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 following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view.

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Application standard	Comments
1	Authenticity	RSA signature generation with RSASSA-PSS with SHA-256, SHA-384, SHA-512	[ISO_14888-2], [PKCS #1], [FIPS PUB 180-4]	2000-4096	[8]	Completely implemented by certified platform functionality.
2	Authenticity	ECDSA signature generation with SHA-256, SHA-384, SHA-512	[RFC5639], [TR-03111] Section 4.1.3, [FIPS186-4] Section B.4 and D.1.2.3	ECC Key sizes corresponding to the used elliptic curve brainpoolP256r1, brainpoolP384r1,	[8]	Completely implemented by certified platform functionality.

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Application standard	Comments
				brainpoolP512r, Curve P-256, Curve P-384, Curve P-521		
3	Authenticity	ECDSA signature verification with brainpoolP256r1, Curve P-256	[RFC5639], [TR-03111] Section 4.1.3, [FIPS186-4] Section B.4 and D.1.2.3	256	[23]	Completely implemented by certified platform functionality.
4	Authentication	Terminal Authentication Version 2	[TR-03110] Section 3.3	Key sizes according to ECDSA signature verification (#31 below) or RSA signature verification (#33 below)	[8]	Implemented in Java Card using certified platform functionality.
5	Authentication	Terminal Authentication Version 2 with the TOE in ICC context and user in PCD context modified by omitting the verification of the certificate chain	[TR-03110] Section 3.3	Key sizes according to ECDSA signature verification (#31 below) or RSA signature verification (#33 below)	[8]	Implemented in Java Card using certified platform functionality.
6	Authentication	Message authentication by MAC verification of received messages	[FIPS197], [NIST-SP800-38B]	128, 256	[8]	Implemented in Java Card using certified platform functionality.
7	Authenticated Key Agreement	PACE in ICC role with AES with Generic Mapping	[ICAO-Doc9303] Section 4.4	**ECC Key sizes** corresponding to the used elliptic curve: brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, Curve P-256, Curve P-384 **AES key sizes**: 128, 256	[8]	Implemented mostly in Java Card using platform functionality. Remaining parts assessed by the ITSEF.

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Application standard	Comments
				Length of the nonce: 16 byte.		
8	Authenticated Key Agreement	Chip Authentication Version 2	[TR-03110] Section 3.4	**ECC Key sizes** corresponding to the used elliptic curve brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, Curve P-256, Curve P-384 **AES key sizes**: 128, 256	[8]	Implemented in Java Card using certified platform functionality.
9	Confidentiality	AES encryption and decryption, CBC mode	[FIPS197], [NIST SP800-38A]	128, 256	[8], [23] for FCS_COP.1/DecUCP	Implemented in Java Card using certified platform functionality. (For FCS_COP.1/DecUCP assessment by ITSEF).
10	Integrity	AES CMAC generation and verification	[FIPS197], [NIST SP800-38B]	128, 256	[8]	Implemented in Java Card using certified platform functionality.
11	Trusted Channel	Secure messaging in ENC_MAC mode, established after PACE or CA version 2 (optional with TA version 2) or based on permanently stored session keys, with AES in CBC mode and CMAC.	[ICAO-Doc9303], [FIPS197] Section 4.4, [NIST-SP800-38A], [NIST-SP800-38B]	128, 256	[8]	Implemented in Java Card using certified platform functionality.
12	Cryptographic primitive (as service of the TOE)	Deterministic RNG DRG.3	acc. to [AIS20]	None.	[8]	Completely implemented by certified platform functionality.
13	Cryptographi	Hash function SHA-	[FIPS180-4]	None.	[8]	Completely

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Application standard	Comments
	c primitive (as service of the TOE)	256, SHA-384, SHA-512				implemented by certified platform functionality.
14	Cryptographic primitive (as service of the TOE)	AES Key generation	[ISO_18033-3]	128, 256	[8]	Implemented in Java Card using certified platform functionality.
15	Cryptographic primitive (as service of the TOE)	AES Key derivation	[NIST SP800-56C]	128	[8]	Implemented in Java Card using certified platform functionality.
16	Cryptographic primitive (as service of the TOE)	ECC key pair generation with brainpoolP256r1, brainpoolP384r1, brain-poolP512r1, Curve P-256, Curve P-384, Curve P-521	[RFC5639], [TR-03111] Section 4.1.3, [FIPS186-4] Section B.4 and D.1.2.3	ECC Key sizes corresponding to the used elliptic curve brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, Curve P-256, Curve P-384, Curve P-521	[8]	Completely implemented by certified platform functionality.
17	Cryptographic primitive (as service of the TOE)	ECC key pair derivation	[RFC5639], [TR-03111] Section 4.1.3, [FIPS186-4] Section B.4 and D.1.2.3	ECC Key sizes corresponding to the used elliptic curve brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, Curve P-256, Curve P-384	[8]	Implemented in Java Card using certified platform functionality. See [15] for notes on usage.
18	Cryptographic primitive (as service of the TOE)	RSA key pair generation	[PKCS #1]	2000 bit to 4096 bit in one bit steps	[8]	Completely implemented by certified platform functionality.
19	Cryptographic primitive (as service of the TOE)	Elliptic Curve Diffie-Hellman ephemeral key agreement	[RFC5903], [RFC6954], [TR-03111] Section 4.3.3	**ECC Key sizes** corresponding to the used elliptic curve	[8]	Implemented in Java Card using certified platform functionality.

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Application standard	Comments
				brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, Curve P-256, Curve P-384 **AES keys**: 128, 256		See [15] for notes on usage.
20	Cryptographic primitive (as service of the TOE)	ECKA-EG key generation	[RFC5903], [TR-03111] Section 4.1.3, [FIPS186-4] Section B.4 and D.1.2.3	ECC Key sizes corresponding to the used elliptic curve brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, Curve P-256, Curve P-384.	[8]	Completely implemented by certified platform functionality.
21	Cryptographic primitive (as service of the TOE)	ECKA-EG key derivation (for Elliptic Curve Integrated Encryption)	[RFC5639], [TR-03111] Section 4.1.3 and 4.3.2.2, [FIPS186-4] Section B.4 and D.1.2.3, [ANSI-X9.63]	ECC Key sizes corresponding to the used elliptic curve brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, Curve P-256, Curve P-384. AES keys: 128, 256	[8]	Implemented in Java Card using certified platform functionality. See [15] for notes on usage.
22	Cryptographic primitive (as service of the TOE)	AES/RSA key generation and encryption with RSA EME-OAEP	[ANS X9.63], [ISO_18033-3], [PKCS #1]	RSA key: 2000 – 4096 AES keys: 128, 256 Seed length: 256, 512 bit	[8]	Implemented in Java Card using certified platform functionality.
23	Cryptographic primitive (as service of the TOE)	AES/RSA key derivation and decryption with RSA EME-OAEP	[ANS X9.63], [ISO_18033-3], [PKCS #1], [NIST SP800-56C]	RSA key: 2000 –4096 AES keys: 128, 256	[8]	Implemented in Java Card using certified platform functionality. See [15] for

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Application standard	Comments
						notes on usage.
24	Cryptographic primitive (as service of the TOE)	AES Key wrap KWP	[NIST SP800-38F]	128	[8]	Implemented in Java Card using certified platform functionality.
25	Cryptographic primitive (as service of the TOE)	AES Key unwrap KWP	[NIST SP800-38F]	128	[8]	Implemented in Java Card using certified platform functionality.
26	Cryptographic primitive (as service of the TOE)	AES encryption and decryption, CBC mode	[NIST SP800-38A]	128, 256	[8]	Implemented in Java Card using certified platform functionality.
27	Cryptographic primitive (as service of the TOE)	Hybrid data encryption/decryption and MAC calculation/verification : ECIES or RSA with AES-CBC and AES-CMAC	[FIPS197], [NIST SP800-38A], [NIST SP800-38B], [TR-02102-1] Section 3.4	128, 256	[8]	Implemented in Java Card using certified platform functionality.
28	Cryptographic primitive (as service of the TOE)	AES CMAC generation and verification	[FIPS197], [NIST SP800-38A]	128, 256	[8]	Implemented in Java Card using certified platform functionality.
29	Cryptographic primitive (as service of the TOE)	HMAC generation and verification, HMAC-SHA256	[RFC2104], [ISO_9797-2]	256	[8]	See [15] for notes on usage.
30	Cryptographic primitive (as service of the TOE)	ECDSA signature creation with brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, Curve P-256, Curve P-384, Curve P-521	[RFC5639], [TR-03111] Section 4.1.3, [FIPS186-4] Section B.4 and D.1.2.3	ECC Key sizes corresponding to the used elliptic curve brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, Curve P-256, Curve P-384, Curve P-521.	[8]	Completely implemented by certified platform functionality.
31	Cryptographi	ECDSA signature	[RFC5639], [TR-	ECC Key	[8]	Completely

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Application standard	Comments
	c primitive (as service of the TOE)	verification with brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, Curve P-256, Curve P-384, Curve P-521	03111] Section 4.1.3, [FIPS186-4] Section B.4 and D.1.2.3	sizes corresponding to the used elliptic curve brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, Curve P-256, Curve P-384, Curve P-521.		implemented by certified platform functionality.
32	Cryptographic primitive (as service of the TOE)	RSASSA and EMSA-PSS signature creation	[ISO_14888-2], [PKCS #1]	2000-4096	[8]	Completely implemented by certified platform functionality.
33	Cryptographic primitive (as service of the TOE)	RSA and EMSAPSS signature verification	[ISO_14888-2], [PKCS #1]	2000-4096	[8]	Completely implemented by certified platform functionality.

Table 3: TOE cryptographic functionality

List of referenced documents and standards:

[ISO_14888-2] Information technology – Security techniques, Digital signatures with appendix – Part 2: Integer factorization based mechanisms, 2008

[PKCS #1] PKCS #1: RSA Cryptography Standard, Version 2.2, October 27, 2012, RSA Laboratories.

[FIPS PUB 180-4] FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS), August 2015, Information Technology Laboratory National Institute of Standards and Technology.

[RFC5639] RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, IETF Trust and the persons identified as the document authors, March 2010 (http://www.ietf.org/rfc/rfc5639.txt).

[TR-03111] BSI - Technical Guideline, Elliptic Curve Cryptography, Version 2.1, 2018-06-01, Bundesamt für Sicherheit in der Informationstechnik.

[FIPS186-4] Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013, U.S. department of Commerce / National Institute of Standards and Technology (NIST).

[TR-03110-2] BSI - Technical Guideline 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 2.21, 2012-12-21, Bundesamt für Sicherheit in der Informationstechnik.

[FIPS197] Federal Information Processing Standards Publication 197, Announcing the ADVANCED ENCRYPTION STANDARD (AES), 2001-11-26, National Institute of Standards and Technology (NIST).

[NIST-SP800-38A] NIST SP800-38A, Recommendation for Block Cipher Modes of Operation, The CMAC Mode for Authentication, 2016-10, National Institute of Standards and Technology (NIST).

[ICAO-Doc9303] Machine Readable Travel Documents, ICAO Doc9303, Part 11: Security Mechanisms for MRTDSs, seventh edition, 2015[ISO_14888-2] Information technology – Security techniques, Digital signatures with appendix – Part 2: Integer factorization based mechanisms, 2008

[NIST SP800-38A] NIST SP800-38A, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, 2001, National Institute of Standards and Technology (NIST).

[AIS20] Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 2013-05-15, Herausgeber: Zertifizierungsstelle des BSI im Rahmen des Zertifizierungsschemas, Bundesamt für Sicherheit in der Informationstechnik.

[ISO_18033-3] ISO 18033-3: Information technology - Security techniques – Encryption algorithms – Part 3: Block ciphers, ISO/IEC 18033-3:2010.

[NIST SP800-56C] NIST, Recommendation for Key Derivation through Extraction-then-Expansion, Special Publication SP800-56C, November 2011

[RFC5903] RFC5903, Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2, June 2010 (https://www.ietf.org/rfc/rfc5903.txt)

[RFC6954] RFC6954, Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the Internet Key Exchange Protocol Version 2 (IKEv2), July 2013 (https://www.ietf.org/rfc/rfc6954.txt)

[ANS X9.63] American National Standard for Financial Services X9.63-2011, Public Key Cryptography for the Financial Services Industry – Key Agreement and Key Transport Using Elliptic Curve Cryptography, December 21, 2011, American National Standards Institute.

[NIST SP800-38F] NIST, SP800-38F Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, 2012

[TR-02102-1] BSI - Technische Richtlinie TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2021-01, 2021-03-24, Bundesamt für Sicherheit in der Informationstechnik.

[RFC2104] RFC2104, HMAC: Keyed-Hashing for Message Authentication, February 1997 (https://www.ietf.org/rfc/rfc2104.txt)[RFC5639] RFC

5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, IETF Trust and the persons identified as the document authors, March 2010 (http://www.ietf.org/rfc/rfc5639.txt).

[ISO_9797-2] Information Technology - Security techniques, Message Authentication Codes (MACs), Part 2: Mechanisms using a dedicated hash-function, 2011

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.

Also note that the UCP (Update Code Package) mechanism is certified according to this certificate's evaluation assurance level and the respective Security Target's Security Functional Requirements, not the update deployment procedure itself. Installation and usage of other TOE configuration items than specified in the Security Target ([6]) (and thus evaluated during the course of this certification) could void the certification status of the used device. Thus, recertifications could be required in order to maintain a valid certification status in cases where such TOE changes are to be applied. As a consequence, only certified updates of the TOE should be used via a respective UCP deployment procedure (which is not in scope of this certification). If non-certified Update Code Packages are available, TOE user's discretion is advised on whether the sponsor should provide a re-certification. In the meantime a risk management process of the system using the TOE should examine and decide on the usage of not yet certified updates and patches. Or take additional measures in order to maintain overall system security.

Some security measures require additional configuration or control or measures to be followed by a product layer on top. For this reason the TOE includes usage- and configuration guidance documentation (see table 2) which contain obligations and guidelines for the developer of the product layer on top on how to securely use this certified TOE and which measures have to be taken. In the course of the inclusion of the TOE into the top layer product or system it must be ensured that the required measures have been correctly and effectively followed according to the rules laid out by the certification procedure of the top layer product, for example the JIL rules or [11].

Overall, for usage of the product, the information provided for TOE users/administrators in the guidance documentation [15] and [16], especially for the secure module application ([15] sec.3.5.1), the cryptographic functionality (see [16] sec.3.5.2), the ACL table ([15] sec. 3.5.3) and the integration ([15] sec.3.5.4) is to be followed. In case special attention regarding certain functionality shall be applied, the [9] already refers to the user guidance [15] in a Developer Note.

The TOE is based on a certified Java Card and provides a Java Card interface for any application which is loaded on the chip. The CSP functionality can be used together with the basic Java Card functionality of the underlying Java Card OS by an application loaded on the chip. Due to this architectural structure an application developer has to follow the guidance documentation of the CSP (i.e. [15] and [16]) as well as the guidance documentation of the Java Card (i.e. [17]). An evaluator of such an application has to consider the obligations in the ETR for Composition of the CSP as well as the obligations in the ETR for Composition of the underlying Java Card (i.e. [10]).

In general, all security hints and requirements of [13] – [24] need to be considered during usage of the TOE or composite product development, if applicable.

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. Regulation specific aspects (eIDAS, QES)

None.

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
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
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target

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

[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-1119-2023, Version 1.16, 2022-11-17, “cryptovision – Java Card applet providing Cryptographic Service Provider – Security Target”, cv Cryptovision GmbH (confidential document)

[7] Evaluation Technical Report, Version 3, 2022-11-22, ”EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY)”, TÜV Informationstechnik GmbH, (confidential document)

[8] Cryptographic Service Provider (CSP) Version 0.9.8, 19 February 2019, BSI-CC-PP-0104-2019,
Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au) Version 0.9.5, 8 April 2019, BSI-CC-PP-0107-2019, Bundesamt für Sicherheit in der Informationstechnik. and
Common Criteria Protection Profile Configurations “Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au), Protection Profile-Module CSP Time Stamp Service and Audit (PPM-TS-Au)”, BSI-CC-PP-0107-2019, Version 0.9.5, Bundesamt für Sicherheit in der Informationstechnik.

[9] Security Target Lite BSI-DSZ-CC-1119-2023, Version 1.16, 2022-11-21, „cryptovision – Java Card applet providing Cryptographic Service Provider – Security Target Lite“, cv Cryptovision GmbH (sanitised public document)

[10] ETR for composite evaluation according to AIS 36 Version 2, 2022-11-29, ”EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP)”, TÜV Informationstechnik GmbH (confidential document)

[11] “Evaluation Methodology for Protection Profiles Security Elements with Application Separation”, v0.1.3, 21.12.2017, Bundesamt für Sicherheit in der Informationstechnik (document can be requested from BSI)

[12] “Configuration list”, 2022-11-22, cv Cryptovision GmbH

[13] Lebenszyklus von SMAERS, CSP und TSE sowie User/Rollen bei SMAERS und CSP, Version 1.6, 2022-09-02, cv Cryptovision GmbH

[14] cryptovision CSP 2.0, cryptovision SMAERS 2.0, Life cycle definition, configuration management and development security at cv cryptovision (Document class ALC), Version 2.7, 2022-09-27, cv Cryptovision GmbH

[15] Cryptovision CSP v2.0 - Java Card configuration providing a Cryptographic Service Provider (CSP) - Operational Guidance (AGD_OPE), Version 1.0.26, 2022-11-21, cv Cryptovision GmbH

[16] cryptovision CSP – Java Card configuration providing a Cryptographic Service Provider (CSP) – Preparation Guidance (AGD_PRE), Version 1.0.19, 2022-11-17, cv Cryptovision GmbH

[17] JCOP 4.7 SE051 User manual for JCOP 4.7 SE051, Revision 1.5, 2022-06-14, NXP Semiconductors

[7] See secton 9.1 for list of used AIS

[18] Evaluation Technical Report for Composition NXP “JCOP 4.7 SE051” – EAL6+, Report nr. 21-RPT-1132, NSCIB-CC-0095534_2, version 2.0, 2021-11-22, Brightsight

[19] JCOP 4.7 SE051 Anomaly Sheet, Rev. 1.3, 2021-07-01, NXP Semiconductors

[20] Certification Report JCOP 4.7 SE051, NSCIB-CC-0095534-CR2, v1, 2021-11-25, TÜV Rheinland

and

Assurance Continuity Maintenance Report JCOP 4.7 SE051, NSCIB-CC-0095534-2MA, v1, 2022-07-05, TÜV Rheinland

[21] JCOP 4.7 SE051 Security Target Lite, Revision 2.1, 2022-06-29, NSCIB-CC-0095534, NXP Semiconductors

[22] Certification Report BSI-DSZ-CC-1136-2021 for NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2) from NXP Semiconductors Germany GmbH, 2021-02-10, Bundesamt für Sicherheit in der Informationstechnik

and

Certification Report BSI-DSZ-CC-1136—V2-2022 for NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3) from NXP Semiconductors Germany GmbH, 2022-06-07, Bundesamt für Sicherheit in der Informationstechnik

[23] Security Upgrade for Card Content Management Card Specification v2.2 - Amendment E, version 1.0, November 2011, GlobalPlatform Inc.

[24] cryptovision CSP v2.0 – Security Implementation Guideline and Overview of Security Mechanism, Version 1.0.5, 2022-08-29, cv Cryptovision GmbH

C. Excerpts from the Criteria

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

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

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

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

Annex B of Certification Report BSI-DSZ-CC-1119-2023

Evaluation results regarding development and production environment

The IT product cryptovision CSP – Java Card applet providing Cryptographic Service Provider version 2.0 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 24 January 2023, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1) are fulfilled for the development and production sites of the TOE listed below:

Name of site / Company name	Address	Type of site
cv cryptovision GmbH	Munscheidstr. 14, 45886 Gelsenkirchen, Germany	SW Development

Table 4: Relevant development/production sites

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.

The development and production sites of the underlying JCOP platform with certification ID NSCIB-CC-0095534-CR2 are listed in [18] sec.4.2. Therein it is further referred to the development and production sites of the underlying platform (IC and cryptographic library) with certification ID BSI-DSZ-CC-1136-2021 and BSI-DSZ-CC-1136-V2-2022. In summary, the following delivery sites, as mentioned in [22], are also relevant (but evaluated in a different procedure) and utilized within this composite certification procedure:

- NXP Hamburg TC: NXP Semiconductors, Germany GmbH, Troplowitzstr. 20, 22529 Hamburg, Germany.
- NXP ATBK: NXP Semiconductors Thailand (ATBK), 303 Moo 3 Chaengwattana Rd., Laksi, Bangkok 10210, Thailand.
- NXP ATKH: NXP Semiconductors Taiwan Ltd (ATKH), #10, Chin 5th Road, N.E.P.Z, Kaohsiung 81170, Taiwan, R.O.C.

Note: End of report