Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1120-V2-2021

for

cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems

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-1120-V2-2021 (*)

cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems

from	cv cryptovision GmbH
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 2

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations and 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.

Common Criteria
Recognition Arrangement

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, 5 July 2021

For the Federal Office for Information Security

Sandro Amendola
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 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]

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

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

3 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.
- 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.

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

This certificate is recognized under CCRA-2014 for all assurance components selected.

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 SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1120-2020. The results from the evaluation process BSI-DSZ-CC-1120-2020 were re-used.

The change to the certified product is the removal of a conformance claim to a PP. The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report dated 07. April 2020 is of relevance and has to be considered when using the product. Details can be found on the following pages.

The evaluation of the technical product cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 6 April 2020. 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.

[5] Information Technology Security Evaluation Facility

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 5 July 2021 is valid until 6 April 2025. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.
4. to provide updates for the product in consultation with the Certification Body at BSI if vulnerabilities have been identified that affect the security of the product. This includes vulnerabilities of security functions provided by the underlying CSP, which also might affect the security of the TOE under consideration in this certificate.

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 SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems 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 named cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems and was evaluated in version 1.0. It is a security module application implemented as software running on the cryptovision CSP v1 CSI-applet 0x000B (Revision 0x3D5D) and CSD-applet 0x000A (cryptographic service provider). The TOE is a part of the security module of a certified technical security system (CTSS) for electronic record-keeping systems (ERS).

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile. It follows largely the Protection Profile Common Criteria Protection Profile – Security Module Application for Electronic Record-keeping Systems, BSI-CC-PP-0105-2019 but does not claim conformance to this 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 2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Functionality	Addressed issue
TSF_Management	Management of the security functionality
TSF_Log	Handling of log data and signature functionality
TSF_Auth	Authentication protocols
TSF_Update	Update functionality

Table 1: TOE Security Functionalities

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

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:

cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems,

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	*cryptovision SMAERS* *SMAERSI applet, Version 0x0105* *SMAERSD applet, Version 0x0105,*	1.0 (Revision 0x3D15)	PGP encrypted and signed e-mail from cryptovision to D-Trust.
2	DOC	*cryptovision SMAERS v1.0 – Java Card applet configuration providing a Security Module Application for Electronic Record-keeping Systems (SMAERS) - Operational Guidance (AGD_OPE)*	1.0.14 01.04.2020	PGP encrypted and signed e-mail from cryptovision to D-Trust.
3	DOC	*cryptovision SMAERS v1.0 – Java Card applet configuration providing a Security Module Application for Electronic Record-keeping Systems (SMAERS) - Preparative Guidance (AGD_PRE)*	1.0.14 02.04.2020	PGP encrypted and signed e-mail from cryptovision to D-Trust.

Table 2: Deliverables of the TOE

The TOE deliverables are provided from the application developer to D-Trust. The SMAERS application is provided to D-Trust embedded in encrypted and signed APDUs using keys under control of cryptovision. To the customer the deliverables are provided as a SW/HW combination of the cryptovision SMAERS on the platform cryptovision CSP v1.0 and both Guidance Documents per PGP encrypted and signed e-mail from cryptovision to the customer.

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:

- User Data Protection,
- Identification and Authentication,
- Security Management,
- Protection of the TSF and
- Code Update Package import.

Specific details concerning the above mentioned security policies can be found in the Security Target [6] chapter 6.1.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- OE.ERS Trustworthy electronic record-keeping system,
- OE.CSP Cryptographic service provider component,
- OE.CSPPlatform CSP as secure platform of the TOE,
- OE.Transaction Verification of Transaction,
- OE.SecOEnv Secure operational environment,
- OE.SecCommCSP Secure communication between TOE and CSP and
- OE.SUCP Signed Update Code Packages.

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

5. Architectural Information

The TOE cryptovision SMAERS consists of two Java Card applications, the SMAERSD and SMAERSI. It runs on cryptovision CSP v1 and comprises the following subsystems:

- Command Processor: Provides the main interface to the TOE and takes the decision which command will be executed by the appropriate subsystem, or that the APDU is rejected due to an unavailable instruction code.
- Configuration Manager: Provides services for application creation in terms of applet instantiation.
- User Manager: Initially creates the configured users like Admin and TimeAdmin as well as the roles CTSS and CSP for creation of transaction and system logs. Furthermore, it handles user authentication and changing reference data by using CSP functions, and returns status information on request.
- Transaction Manager: Provides services for signing transaction logs using CSP functions.
- System Log Manager: Uses CSP functions to create logs for system events such as user authentication or setting of system time.

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

Overview:

The penetration testing was performed at the site of the evaluation body TÜViT in the evaluator's test environment with the evaluator's test equipment. The samples were provided by the sponsor and by the developer. The test samples were configured and parameterized by the evaluator according to the guidance documentation. The one configuration of the TOE being intended to be covered by the current evaluation was tested. The overall result is that no deviations were found between the expected result and the actual result of the tests. Moreover, no attack scenario with an attack potential of Basic was actually successful.

Penetration testing approach:

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment created within vulnerability analysis evaluation report, the evaluator created attack scenarios for the penetration tests, where the evaluator is of the opinion that the vulnerabilities could be exploitable. While doing so, the evaluator also considered all aspects of the security architecture of the TOE being not covered by the functional developer tests.

The primary focus for devising penetration tests was to cover all potential vulnerabilities identified as applicable in the TOE's operational environment for which an appropriate test set was devised and which are not definitely covered by the underlying CSP v1 and the certified OS composite platform.

TOE test configurations:

The tests were performed with the one configuration of the TOE as it is delivered as outlined in the security target and with the version of the underlying CSP as identified in the Guidance AGD_PRE, Chapter 3.2.4 [12].

Verdict of the ITSEF:

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 of Basic was actually successful in the TOE's operational environment as defined in the security target provided that all measures required by the developer are applied.

Summary of Test Results and Effectiveness Analysis:

The test results yielded that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential basic was actually successful in the TOE's operational environment as defined in ST [6] provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE: cryptovision SMAERS Version 1 with the SMAERSI applet, Version 0x0105 (Revision 0x3D15) and SMAERSD applet, Version 0x0105 with cryptovision CSP v1 with the CSI-applet 0x000B (Revision 0x3D5D) and CSD-applet 0x000A.

The unique identification of the CSP platform is described in the guidance [12].

The CSP is not part of the TOE but part of operational environment.

Although they are delivered together with the TOE to the consumer, they are excluded from the TOE and are considered part of the IT-environment.

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.

The following guidance specific for the technology was considered (while not being mandatory during the CC certification)

(i.) TR_03151 Technical Guideline BSI TR-03151 Secure Element API (SE API), BSI, Version 1.0.1, 20. December 2018

(ii.) TR_03153 Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, BSI, Version 1.0.1, 20. Dezember 2018

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

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

- All components of the EAL 2 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-1120-2020, re-use of the evaluation tasks was possible. The focus of this re-evaluation was on a change in the security target, since there is no longer a claim of Conformance to a PP.

The evaluation has confirmed:

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

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

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

9.2. Results of cryptographic assessment

The TOE does not include cryptographic mechanisms. The only cryptographic mechanism used are implemented in the CSP platform and not part of this evaluation. Thus, no such mechanisms were part of the assessment.

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.

As the TOE relies on security functionality provided by the underlying CSP, it must be operated in conjunction with the CSP of the evaluated configuration.

In regard of the further operational environment, it is to be noted that the certification and evaluation were conducted under the condition, that the objective for the operational environment “OE.SecOEnv: Secure operational environment” (Security Target [6]) is upheld. In detail, the objective states:

> *OE.SecOEnv: Secure operational environment:*
>
> *The operational environment shall protect the electronic record-keeping system and the certified technical security system including the TOE against manipulation, perturbation and misuse. It protects the integrity of the communication between the electronic record-keeping system and 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 the ST [6] 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 itself is certified according to this certificate’s evaluation assurance level and the respective Security Target’s Security Functional Requirements. However, installation and usage of other TOE configuration items than specified in the Security Target ([6]) (and thus evaluated during the course of this certification) will void the certification status. Recertification's are 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. If non-certified Update Code Packages are available, TOE user 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 investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

Regarding Public Key Infrastructure (PKI) it is to be noted, that neither the SMAERS Protection Profile nor the Security Target ([6]) address (security-assurance- or security-functional) requirements concerning a PKI. Therefore, no PKI aspects were CC evaluated by the ITSEF in the course of the underlying CC evaluation. Hence the CC certification scope does not cover the Public Key Infrastructure. However, the developer cv cryptovision GmbH provided a (confidential) PKI concept document [17], outlining relevant PKI structures, definitions and processes. The document was considered by a dedicated BSI Section and deemed suitable.

The TOE includes guidance documentation (see table 2) which contains obligations and guidelines for the user and/or developer of the product layer on top on how to securely use this certified TOE and which measures have to be taken in order to fulfil the overall security requirements of the Security Target of the TOE.

If the TOE is subject to an evaluation in a composite product or system, it must be examined if the required measures have been correctly and effectively implemented by the product layer on top.

At the point in time when evaluation and certification results are reused, there might be an updated documentation available. Therefore, the certified products list on the BSI website has to be checked for latest information on reassessments, recertifications or maintenance result available for the product.

In addition, the following aspects need to be fulfilled when using the TOE:

Usage of the cv cryptovision CSP with the CSI-Package-ID/Version: D2 76 00 00 98 43 53 49 00 0B

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

AGD	Guidance Documents
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
PKI	Public Key Infrastructure
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-1120-V2-2021, Version 1.42, 29.06.2021, cryptovision SMAERS - Java Card applet providing Security Module Application for Electronic Record-keeping Systems Security Target, cryptovision

[7] Evaluation Technical Report, Version 1, 06.04.2020, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), TÜV Informationstechnik GmbH, (confidential document)

[8] n/a

[9] “Evaluation Methodology for Protection Profiles Security Elements with Application Separation”, v0.1.3, 21.12.2017, Bundesamt für Sicherheit in der Informationstechnik

[10] ALC, Version 1.4, 03.03.2020, cryptovision CSP - cryptovision SMAERS Life - cycle definition, configuration management and development security at cv cryptovision (Document class ALC), cryptovision

[7] specifically

- AIS 14 Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik.
- AIS 19 Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 9, 2014-11-03, Bundesamt für Sicherheit in der Informationstechnik.
- AIS 26, Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 26, Evaluationsmethodologie für in Hardware Integrierte Schaltungen, Version 10, 2017-07-03, Bundesamt für Sicherheit in der Informationstechnik
- AIS 26 BSI-ADPA-SC, Auswahl geeigneter Chips für DPA-Messungen, Version 1.1, 2008-12-07, Bundesamt für Sicherheit in der Informationstechnik.
- AIS 26 BSI-ATT-SC Special Attack Methods for Smartcards and Similar Devices, Version 1.4, 2011-06-08, Bundesamt für Sicherheit in der Informationstechnik.
- AIS 26 CCDB-IC-EVL, CC Supporting Document Mandatory Technical Document – Requirements to perform Integrated Circuit Evaluations, Version 1.1, May 2013, CCDB-2013-05-001.
- AIS 26 JIL-AP-SC Joint Interpretation Library – Application of Attack Potential to Smartcards, Version 2.9, January 2013.
- AIS 26 JIL-ATT-SC, Joint Interpretation Library – Attack Methods for Smartcards and Similar Devices, Version 2.2, January 2013, confidential.
- AIS 26 JIL-IC-EVL, Joint Interpretation Library – Requirements to perform Integrated Circuit Evaluations, Version 1.1, February 2013
- AIS 32, Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 7, 2011-06-08, Bundesamt für Sicherheit in der Informationstechnik.
- AIS 45, Joint Interpretation Library – Minimum Site Security Requirements, Version 2.2, April 2019.

[11] AGD_OPE, 1.0.14, 01.04.2020, cryptovision SMAERS v1.0 – Java Card applet configuration providing a Security Module Application for Electronic Record-keeping Systems (SMAERS) - Operational Guidance (AGD_OPE), cryptovision

[12] AGD_PRE, Version 1.0.14, 02.04.2020, cryptovision SMAERS v1.0 – Java Card applet configuration providing a Security Module Application for Electronic Record-keeping Systems (SMAERS) - Preparative Guidance (AGD_PRE), cryptovision

[13] CL, Version 7, 06.04.2020, Configuration List, file: 2020_04_02_conflist_SMAERS_CSP_JCOP4_v6.xlsx, cryptovision

[14] n/a

[15] TR-03151, Version 1.0, 05.06.2018, Technical Guideline BSI TR-03151, Secure Element API (SE API), BSI

[16] TR-03153, Version 1.0, 05.06.2018, Technische Richtlinie BSI TR-03153, Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, BSI

[17] PKI-Konzept, Version 6, 02.04.2020, PKI-Konzept für das TSE-Modul für die TSE-Produktion bei der D-Trust GmbH, D-Trust

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-1120-V2-2021

Evaluation results regarding development and production environment

The IT product cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems, (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations and 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 5 July 2021, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (ALC_CMC.2, ALC_CMS.2, ALC_DEL.1)

are fulfilled for the development site of the TOE listed below:

a) cv cryptovision GmbH
Munscheiderstr. 14
45886 Gelsenkirchen
Germany

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

Note: End of report