Federal Office
for Information Security

Certification Report

BSI-CC-PP-0121-2024

for

Protection Profile for E-Voting Systems for non-political Elections, Version 1.0

developed by

Federal Office for Information Security

Federal Office for Information Security (BSI), Postfach 20 03 63, 53133 Bonn, Germany
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-CC-PP-0121-2024

Common Criteria Protection Profile

Protection Profile for E-Voting Systems for non-political Elections
Version 1.0

developed by Federal Office for Information Security

Assurance Package claimed in the Protection Profile:
Common Criteria Part 3 conformant
EAL 4 augmented by ALC_FLR.2

valid until 19 February 2034

SOGIS Recognition Agreement

Common Criteria

The Protection Profile identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version CC:2022 for conformance to the Common Criteria for IT Security Evaluation (CC), Version CC:2022. 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 Protection Profile and in conjunction with the complete Certification Report.

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 Protection Profile by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the Protection Profile 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

Bonn, 20 February 2024
For the Federal Office for Information Security

Sandro Amendola
Director-General

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 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 Act on the Federal Office for Information Security (BSIG), the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products as well as for Protection Profiles (PP).

A PP defines an implementation-independent set of IT security requirements for a category of products which are intended to meet common consumer needs for IT security. A PP claimed by a user, consumer or stakeholder for IT gives them the possibility to express their IT security needs without referring to a specific product. Product certifications can be based on Protection Profiles. For products which have been certified based on a Protection Profile an individual certificate will be issued but the results from a PP certification can be re-used for the Security Target evaluation within a product evaluation when conformance to the PP has been claimed.

Certification of the Protection Profile is carried out on the instigation of the BSI or a sponsor. A part of the procedure is the technical examination (evaluation) of the Protection Profile according to Common Criteria [1]. The evaluation is usually 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.

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 (BSIG)[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs[3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3], including PP Certification
- 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
Current version see website: http://www.gesetze-im-internet.de/bsig_2009/index.html

[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
Current version see website: http://www.gesetze-im-internet.de/bsizertv_2014/index.html

[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
Current version see website: https://www.bsi.bund.de/Gebuehrenverordnung

- Common Criteria for IT Security Evaluation (CC)[4] [1] also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Internal procedure for the issuance of a PP certificate

3 Recognition Agreements

In order to avoid multiple certification of the same Protection Profile in different countries a mutual recognition of IT security certificates - as far as such certificates are based on CC - under certain conditions was agreed. Therefore, the results of this evaluation and certification procedure can be re-used by the product certificate issuing scheme in the evaluation of a Security Target within a subsequent product evaluation and certification procedure.

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 up to and including Common Criteria (CC) Evaluation Assurance Levels EAL 4, and in addition at higher recognition levels for IT-Products related to certain technical domains only. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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.

Details on recognition, the signatory nations, technical domains and the agreement itself can be found at https://www.sogis.eu.

3.2 International Recognition of CC – Certificates (CCRA)

The international Common Criteria Recognition Arrangement (CCRA) became effective in September 2014 in its current version. It defines the recognition of certificates for IT-products 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 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.

Details on recognition, the signatory nations and the agreement itself can be found at https://www.commoncriteriaportal.org.

[4] CC:2022: Proclamation of the Federal Office for Information Security of 14 April 2023 on https://www.bsi.bund.de

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 Protection Profile for E-Voting Systems for non-political Elections, Version 1.0 has undergone the certification procedure at BSI.

The evaluation of the Protection Profile for E-Voting Systems for non-political Elections, Version 1.0 was conducted by the ITSEF Deutsche Telekom Security GmbH (Bonn). The evaluation was completed on 19 January 2024. The ITSEF Deutsche Telekom Security GmbH (Bonn) is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Federal Office for Information Security.

The Protection Profile was developed by the Federal Office for Information Security with support of the company Deutsche Telekom Security GmbH (Bonn).

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 only applies to the version of the Protection Profile as indicated.

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

For the meaning of the CC concepts and terms please refer to CC [1] Part 1 through 5.

The validity of this certificate ends as outlined on the certificate. The applicant and the sponsor of this certificate are recommended to review the technical content of the Protection Profile certified according to the evolvement of the technology and of the intended operational environment of the type of product concerned as well as according to the evolvement of the evaluation criteria. Such review should result in an update and a re-certification of the Protection Profile accordingly. Typically, technical standards are reviewed on a five years basis.

The limitation of validity of this PP certificate does not necessarily impact the validity period of a product certificate referring to this Protection Profile, but the certification body issuing a product certificate based on this Protection Profile should take it into its consideration on validity.

6 Publication

The Protection Profile for E-Voting Systems for non-political Elections, Version 1.0 has been included in the BSI list of the certified Protection Profiles, 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.

The Certification Report may be obtained in electronic form at the internet address stated above.

[5] Information Technology Security Evaluation Facility

B Certification Results

The following results represent a summary of

- the certified Protection Profile,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Protection Profile Overview

The Protection Profile for E-Voting Systems for non-political Elections, Version 1.0 [6] is established by the Federal Office for Information Security as a basis for the development of Security Targets in order to perform a certification of an IT-product, the Target of Evaluation (TOE).

The Protection Profile for E-Voting Systems for non-political Elections, Version 1.0 from 1 December 2023, describes as a TOE type a server software for conducting secret non-political E-votings, which implements the process of conducting the election. The Protection Profile defines a basic set of security requirements to be fulfilled by a product for E-Voting in order to perform elections in a secure way. It addresses non-political elections such as for example elections within committees or election of an equal opportunities officer. The PP utilizes a modular structure and specifies a base PP and one additional functional package. The base PP describes as a TOE type a server software consisting of one single server component. The functional package “Multi-component Server Architecture Package”, Version 1.0 from 1 December 2023, describes as a TOE type a server software which consist of more than one server components.

The TOE shall implement specific functionalities for conducting e-votings related to the different electoral phases. In the preparation phase, the election data is created, corrected if necessary, and approved by the election board. The installation and configuration of the TOE are performed by the administrator at the beginning of the preparation phase and have been completed successfully before the election execution starts. Once the election period start time is reached, the TOE starts the execution phase. The election actions of a voter occur only during the election execution. Votes can only be cast and finally stored in the ballot box from authorized voters. The TOE provides the voter, or the remote endpoints on behalf of the voter a required means to encrypt their votes. The votes are only processed in encrypted form by the TOE until they are stored in a ballot box. During the evaluation phase, the TOE provides the accumulated audit records to the election board, who has to check them for irregularities and afterwards has to initiate the vote count. Before starting the counting of votes, all votes in the intermediate ballot box are transferred to the ballot box. By counting all valid votes, and taking into account the set of election rules for cast votes, the distribution of votes for the individual candidates shall be determined. With the determination of the result of the vote count, the election execution data and the election result are made available by the TOE in such a way that they can be stored in a manner protected from subsequent manipulation. In addition, the stored data enables users outside the TOE to perform end-to-end verifiability, that is cast as intended, recorded as cast, counted as recorded, individual verifiability and universal verifiability. After the evaluation phase ends, the post-processing phase begins where the TOE can export the prepared election execution data.

When the TOE is implemented as a server software consisting of several server components, the TOE shall provide in addition a trusted channel for secure communication between the TOE components.

The assets to be protected by a TOE claiming conformance to this PP are defined in the Protection Profile [6], chapter 3.1.1. Based on these assets the security problem definition is defined in terms of assumptions, threats and organisational security policies. This is outlined in the Protection Profile [6], in the chapters 3.2, 3.3 and 3.4. Due to the modular structure of the PP, the security problem definition can be changed in case the functional package “Multi-component Server Architecture Package” is used. The functional package

defines an additional threat which shall be considered when the software system consist of more than one server component. This is defined in chapter 7.3.1 of the PP.

These assumptions, threats and organisational security policies are split into security objectives to be fulfilled by a TOE claiming conformance to this PP and security objectives to be fulfilled by the operational environment of a TOE claiming conformance to this PP. The objectives for the base PP are outlined in the PP [6], chapter 4. One additional security objective is defined in scope of the functional package and this can be found in chapter 7.4.1 of the PP.

The Protection Profile [6] requires a Security Target based on this PP or another PP claiming this PP to fulfil the CC requirements for strict conformance.

2 Security Functional Requirements

Based on the security objectives to be fulfilled by a TOE claiming conformance to this PP the security policy is expressed by the set of security functional requirements (SFR) to be implemented by a TOE. It covers the following issues: user identification and authentication, access control, user data import and export, secure communication, voting and verification, electoral evaluation according to rule sets, audit, archiving, reaching and preserving secure states and resuming the process, management of security attributes and management of security functions. The functional package introduces additional SFRs related to establishment of a trusted channel that use cryptographic mechanisms for communication between the TOE server components.

The TOE security functional requirements for the base PP are outlined in the PP [6], chapter 6.1. For the functional package, additional SFRs are defined and they are outlined in chapter 7.5.1. The SFRs are selected from Common Criteria Part 2 and one of them is newly defined. Thus the SFR claim is called:

Common Criteria Part 2 extended

3 Assurance Requirements

The TOE security assurance package claimed in the Protection Profile is based entirely on the assurance components defined in part 3 of the Common Criteria. Thus, this assurance package is called:

Common Criteria Part 3 conformant
EAL 4 augmented by ALC_FLR.2

(for the definition and scope of assurance packages according to CC see [1], part 3 for details).

4 Results of the PP-Evaluation

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 Application Notes and Interpretations of the Scheme (AIS) [4] as relevant for the TOE.

As a result of the evaluation the verdict PASS is confirmed for the assurance components of the class APE (Protection Profile evaluation).

The following assurance components were used:

APE_INT.1 PP introduction
APE_CCL.1 Conformance claims
APE_SPD.1 Security problem definition
APE_OBJ.2 Security objectives
APE_ECD.1 Extended components definition
APE_REQ.2 Derived security requirements

The results of the evaluation are only applicable to the Protection Profile as defined in chapter 1.

5 Obligations and notes for the usage

The following aspects need to be fulfilled when using the Protection Profile:

- The Protection Profile contains application notes, the author of a product specific Security Target needs to consider when creating a Security Target and implementing a TOE that claims conformance to this PP.

6 Protection Profile Document

The Protection Profile for E-Voting Systems for non-political Elections, Version 1.0 [6] is being provided within a separate document as Annex A of this report.

7 Definitions

7.1 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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

7.2 Glossary

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

Ballot Box - Storage of the cast votes, where the cast votes cannot be changed. The ballot box is part of the TOE.

Election Action - Includes identification and authentication with voting eligibility verification, ballot filling, correction and initiation of voting, display of the vote, casting or recasting of the vote, and feedback to the voter.

Election Board - This includes both the persons who have organizational responsibility for and manage the e-voting, as well as all "vicarious agents" (e.g. employees of an e-voting service provider commissioned with the processing) who, on behalf of and under the control of senior personell of the election board, carry out the administration of the e-voting servers, initiate a resumption, end the election process, start the post-processing phase and start the counting of votes with determination of the election result.

Election Data - Data created outside the TOE that is imported in the preparation phase containing data needed to define election parameters.

Election Execution Data - Data used and generated in the electoral phases, required to be exported in the post-processing phase and stored in a tamper-proof manner after the election.

Evaluation Phase - During the evaluation phase the TOE counts the cast votes and determines the election result according to the set of election rules.

Execution Phase - During the execution phase, voters can perform their individual election action. The election board can start and stop the election execution during the election period.

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

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

Informal - Expressed in natural language.

Intermediate Ballot Box - Storage of the cast votes in an encrypted form with the possibility of modification, upstream of the ballot box. Unlike the ballot box, the intermediate ballot box allows to have a vote linked to the voter to allow re-voting. A technically conditioned intermediate storage during the transmission does not belong to it. The intermediate ballot box is part of the TOE.

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

Post-processing Phase - During the post-processing phase the TOE can export election execution data to enable end-to-end verifiability after the election.

Preparation Phase - During the preparation phase election board members can import election data into the TOE and set parameters used in following electoral phases.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

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 - A set of software, firmware and/or hardware possibly accompanied by guidance.

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.

8 Bibliography

[1] ISO-Version:
ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements
https://www.iso.org/standard/72891.html
https://www.iso.org/standard/72892.html
https://www.iso.org/standard/72906.html
https://www.iso.org/standard/72913.html
https://www.iso.org/standard/72917.html

CCRA-Version:
CC:2022 R1, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements
https://www.commoncriteriaportal.org/index.cfm

[2] ISO-Version:
ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
https://www.iso.org/standard/72889.html

CCRA-Version:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal.org/index.cfm

[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[6].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website

[6] specially

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

[6] Protection Profile for E-Voting Systems for non-political Elections, Version 1.0, 2023-12-1, Federal Office for Information Security

[7] Evaluation Technical Report, Version 1.1, 2024-01-10, Evaluation Technical Report Summary, Deutsche Telekom Security GmbH (confidential document)

C Annexes

List of annexes of this certification report

Annex A: Protection Profile for E-Voting Systems for non-political Elections, Version 1.0 [6] provided within a separate document.

Note: End of report