Federal Office
for Information Security

Certification Report

BSI-CC-PP-0088-V2-2017

for

Base Protection Profile for Database Management Systems (DBMS PP) Version 2.12 and DBMS PP Extended Package - Access History (DBMS PP_EP_AH) Version 1.02

developed by

DBMS Working Group / Technical Community

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-0088-V2-2017

Common Criteria Protection Profile

Base Protection Profile for Database Management Systems (DBMS PP) Version 2.12 and DBMS PP Extended Package - Access History (DBMS PP_EP_AH) Version 1.02

developed by DBMS Working Group / Technical Community

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

Valid until 04. April 2027

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 3.1 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 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, 5 April 2017
For the Federal Office for Information Security

Bernd Kowalski
Head of Department

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

This page is intentionally left blank.

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 special 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 Taget 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 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.

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]
- 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], 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

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

3 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- Common Criteria for IT Security Evaluation (CC), Version 3.14[4] [1] also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation, Version 3.1 [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 ITSEC/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 ITSEC Evaluation Assurance Levels E 3 (basic), 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 nations involved.

Details on recognition, technical domains and the agreement itself can be found at http://www.sogisportal.eu.

3.2 International Recognition of CC – Certificates (CCRA)

The international Common Criteria Recognition Arrangement (CCRA) became effictive 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). In certain cases certificates issued during a transition period until September 2017 are recognised up to EAL 4.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations involved.

Details on recognition and the agreement itself can be found at http://www.commoncriteriaportal.org.

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

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 PP Base Protection Profile for Database Management Systems (DBMS PP) Version 2.12 and DBMS PP Extended Package - Access History (DBMS PP_EP_AH) Version 1.02, have undergone the certification procedure at BSI. This is a re-certification based on BSI-CC-PP-0088-2015. Specific results from the evaluation process based on BSI-CC-PP-0088-2015 were re-used.

The evaluation of the PP Base Protection Profile for Database Management Systems (DBMS PP) Version 2.12 and DBMS PP Extended Package - Access History (DBMS PP_EP_AH) Version 1.02 was conducted by the ITSEF atsec information security GmbH. The evaluation was completed on 31. März 2017. The ITSEF atsec information security GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: DBMS Working Group / Technical Community.

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 for the concept of PPs, to CC [1] Part 2 for the definition of Security Functional Requirements components (SFRs) and to CC [1] Part 3 for the definition of the Security Assurance Requirements components (SARs), for the class AVA Vulnerability assessment and for the cross reference of Evaluation Assurance Levels (EALs) and assurance components.

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.

[5] Information Technology Security Evaluation Facility

6 Publication

The PP Base Protection Profile for Database Management Systems (DBMS PP) Version 2.12 and DBMS PP Extended Package - Access History (DBMS PP_EP_AH) Version 1.02 have 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.

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 Base Protection Profile for Database Management Systems (DBMS PP) Version 2.12 and DBMS PP Extended Package - Access History (DBMS PP_EP_AH) Version 1.02 [7, 8] are established by the DBMS Working Group / Technical Community 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 Database Management Systems (Base Package)" version 2.12 as of 2017-03-23 specifies security requirements for a commercial-off-the-shelf (COTS) database management system (DBMS). The TOE type defined by the PP is a database management system.

A product compliant with this Protection Profile includes, but is not limited to, a DBMS server and can be evaluated as a software only application layered on an underlying system, i.e., operating system, hardware, network services, and/or custom software, and is usually embedded as a component of a larger system within an operational environment. This profile establishes the requirements necessary to achieve the security objectives of the Target of Evaluation (TOE) it covers and its environment. Conformant products provide access control based on user identity and, optionally, group membership, e.g., Discretionary Access Control (DAC), and generation of audit records for security relevant events. Authorized administrators are trusted to not misuse the privileges assigned to them.

Security Targets (STs) that claim conformance to this PP shall meet a minimum standard of demonstrable-PP conformance at level EAL2 augmented by ALC_FLR.2.

The Protection Profile may be extended by functionality related to TOE access history, which is defined by the "DBMS PP Extended Package - Access History" version 1.02 as of 2017-03-23. The extended package can only be claimed in combination with the DBMS PP base package, and the resulting combination defines the same functionality as the previous version 2.07 of the DBMS PP already certified as BSI-CC-PP-0088-2015.

The assets to be protected by a TOE claiming conformance to this PP are defined in the Protection Profile [7], chapter 4. 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 [7], chapter 4.

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. These objectives are outlined in the PP [7], chapter 5, and the EP [8], chapter 4.

The Protection Profile [7] requires a Security Target based on this PP or another PP claiming this PP to fulfil the CC requirements for demonstrable 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:

- FAU: Security Audit
- FDP: User data protection

- FIA: Identification and Authentication
- FMT: Security Management
- FPT: Protection of the TSF
- FTA: TOE Access

A DBMS evaluated against the base package of the DBMS PP will provide the following security services:

- Discretionary Access Control (DAC) limits access to objects based on the identity of the subjects or groups to which the subjects and objects belong, and which allows authorized users to specify how the objects that they control are protected.
- Audit Capture for creation of information on all auditable events.
- Authorized administration role to allow authorized administrators to configure the policies for discretionary access control, identification and authentication, and auditing. The product must enforce the authorized administration role. Some administrative tasks may be delegated to specific users (which by that delegation become administrators although they can only perform some limited administrative actions). Ensuring that those users cannot extend the administrative rights assigned to them is a security functionality the product has to provide.

The Extended Package - Access History of the DBMS PP covers an additional security objective for DBMS evaluated against that package in combination with the base package. When claimed, the security services of the DBMS will be extended by functionality related to access history that allows trained users to review their access history in order to help identify unauthorized access attempts.

These TOE security functional requirements are outlined in the PP [7], chapter 7, and in the EP [8], chapter 6. They are selected from Common Criteria Part 2 and some of them are 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 2 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) [6] 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.

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

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-CC-PP-0088-2015, re-use of specific evaluation tasks was possible. The previous version (version 2.07) of the base Protection Profile included the security objective O.ACCESS_HISTORY, and evaluations of DBMS performed with a PP claim to version 2.07 (BSI-CC-PP-0088-2015) can be considered equivalent to an evaluation claiming conformance to this version of the PP [7] and the extended package – Access History [8]. The focus of this re-evaluation was therefore on verifying that the base PP solves its security problem without meeting the security objective O.ACCESS_HISTORY, which was moved to the optional extended package for increased adaptivity.

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

5 Obligations and notes for the usage

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

none

6 Protection Profile Document

The Protection Profile Base Protection Profile for Database Management Systems (DBMS PP) Version 2.12 and DBMS PP Extended Package - Access History (DBMS PP_EP_AH) Version 1.02 [7, 8] are being provided within a separate document as Annex A of this report.

7 Definitions

7.1 Acronyms

AH	Access History
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
COTS	Commercial Off The Shelf

DBMS	Database Management System
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
EP	Extended Package
ETR	Evaluation Technical Report
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
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.

Database Management System - A suite of programs that typically manage large structured sets of persistent data, offering ad hoc query facilities to many users. They are widely used in business applications.

Discretionary Access Control - A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. Those controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

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.

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

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] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

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

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[6].

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

[6] Evaluation Technical Report, Version 2, 2017-03-29, Final Evaluation Technical Report, atsec information security GmbH (confidential document)

[7] Protection Profile for Database Management Systems (DBMS PP) Base Package, Version 2.12, 2017-03-23, BSI-CC-PP-0088-V2, DBMS Working Group / Technical Community

[8] DBMS PP Extended Package – Access History (DBMS PP_EP_AH), Version 1.02, 2017-03-23, BSI-CC-PP-0088-V2, DBMS Working Group / Technical Community

[6] specially

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, Reuse of evaluation results

C Annexes

List of annexes of this certification report

Annex A: Protection Profile Base Protection Profile for Database Management Systems (DBMS PP) Version 2.12 and DBMS PP Extended Package - Access History (DBMS PP_EP_AH) Version 1.02 [7, 8] provided within a separate document.

Note: End of report

This page is intentionally left blank.