Reference: 2022-35-INF-4086- v1
Target: Pública
Date: 27.06.2023

Created by: CERT10
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2022-35**
TOE	**collaborative Protection Profile (cPP) for Database Management Systems (version 1.3, 13 March 2023)**
Applicant	**600413485 - Microsoft Corporation**
References	

[EXT-7899] Certification Request

[EXT-8453] Evaluation Technical Report

Certification report of the collaborative Protection Profile (cPP) for Database Management Systems (version 1.3, 13 March 2023), as requested in [EXT-7899] dated 19/07/2022, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-8453] received on 15/03/2023.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the collaborative Protection Profile (cPP) for Database Management Systems (version 1.3, 13 March 2023).

A Protection Profile (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. 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.

A collaborative Protection Profile (cPP) is a Protection Profile developed openly by international Technical Communities (iTC) consisting of vendors, test laboratories, CCRA nations and academia.

Developer: Database Management System iTC

Sponsor: Microsoft Corporation

Certification Body: Centro Criptológico Nacional (CCN)

ITSEF: DEKRA Testing and Certification S.A.U.

Conformance: This cPP is Common Criteria v3.1 R5 Part 2 extended and Part 3 conformant and claims conformance to the EAL 2 assurance package augmented by ALC_FLR.3

Evaluation end date: 21/04/2023

All the assurance components APE_CCL.1, APE_ECD.1, APE_INT.1, APE_OBJ.2, APE_REQ.2 and APE_SPD.1 have been assigned a "**PASS**" verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the "**PASS**" VERDICT to the whole evaluation due all the evaluator actions are satisfied as defined by the Common Criteria v3.1 R5 and the Common Evaluation Methodology v3.1 R5. The Assurance Package claimed in the collaborative Protection Profile is Common Criteria v3.1 R5 Part 2 extended and Part 3 conformant and claims conformance to the EAL 2 assurance package augmented by ALC_FLR.3 (Systematic flaw remediation).

Considering the obtained evidences during the instruction of the certification request of the collaborative Protection Profile (cPP) for Database Management Systems (version 1.3, 13 March 2023), a positive resolution is proposed.

IDENTIFICATION

Protection Profile Identification: collaborative Protection Profile (cPP) for Database Management Systems (version 1.3, 13 March 2023)

Evaluation Level: Common Criteria v3.1 R5 assurance components APE_CCL.1, APE_ECD.1, APE_INT.1, APE_OBJ.2, APE_REQ.2 and APE_SPD.1.

Assurance Package claimed in the PP: Common Criteria v3.1 R5 Part 3 conformant EAL 2 assurance package augmented by ALC_FLR.3.

PROTECTION PROFILE SUMMARY

The collaborative Protection Profile (cPP) for Database Management Systems (version 1.3, 13 March 2023) specifies security requirements for a commercial-off-the-shelf (COTS) database management system (DBMS). It is structured as a base Protection Profile, able to accommodate a set of (optional) PP-Modules.

A database is an organized collection of data, generally stored and accessed electronically from a computer system. The database management system (DBMS) is the software that interacts with end users, applications, and the database itself to capture and analyze the data. The DBMS software additionally encompasses the core facilities provided to administer the database. A DBMS may be a single-user system, in which only one user may access the DBMS at a given time, or a multi-user system, in which many users may access the DBMS simultaneously.

A DBMS evaluated against this cPP will provide the following security functionality:

- 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 TOE must enforce the authorized administration role.
- Limitation of the number of concurrent sessions and restrictions on establishing sessions.

On the other hand, a DBMS conformant to this cPP will not guarantee the following:

- Physical protection mechanisms and the administrative procedures for using them are in place.
- Mechanisms to ensure the complete availability of the data residing on the DBMS are in place. The DBMS can provide simultaneous access to data to make the data available to more than one person at a given time, and it can enforce DBMS resource allocation limits to prevent users from monopolizing a DBMS service/resource. However, it cannot detect or prevent the unavailability that may occur because of a physical or environmental disaster, a storage device failure, or external threats on the underlying operating system. For such threats to availability, the environment must provide the required countermeasures.

- Mechanisms to ensure that users properly secure the data that they retrieve from the DBMS are in place. The security procedures of the organization(s) that use and manage the DBMS must define users' data retrieval, storage, export, and disposition responsibilities.
- Mechanisms to ensure that authorized administrators wisely use DAC. Although the DBMS can support an access control policy by which users and optionally users in defined groups, are granted access only to the data that they need to perform their jobs, it cannot completely ensure that authorized administrators who are able to set access controls will do so prudently.

SECURITY ASSURANCE REQUIREMENTS

The Protection Profile was evaluated with all the evidence required to fulfil the following assurance components according to Common Criteria v3.1 R5:

- 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

SECURITY FUNCTIONAL REQUIREMENTS

collaborative Protection Profile (cPP) for Database Management Systems (version 1.3, 13 March 2023) provides, in section 6, the set of Security Functional Requirements (SFRs) the TOE to be certified has to enforce in order to fulfil the security objectives. The cPP also provides in *Appendix A* optional SFRs which could be potentially included in the Security Target.

SECURITY POLICIES

The collaborative Protection Profile (cPP) for Database Management Systems (version 1.3, 13 March 2023) defines a set of security policies to be addressed by cPP-conformant TOEs. The detail of these policies is documented in section *4.4 Organisational Security Policies*.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The collaborative Protection Profile (cPP) for Database Management Systems (version 1.3, 13 March 2023) defines, in section *4.5 Assumptions,* the assumptions and constraints to the conditions used to assure the security properties and functionalities compiled by the TOEs compliant to the cPP. These assumptions shall be applied during the evaluation of TOE compliant with this cPP in order to determine if the identified vulnerabilities are applicable and can be exploited.

CLARIFICATIONS ON NON-COVERED THREATS

The threats listed in the cPP, section *4.3 Threat,* do not constitute a risk for the TOEs compliant with collaborative Protection Profile (cPP) for Database Management Systems (version 1.3, 13 March 2023) if the threat agents have a basic attack potential according to AVA_VAN.2 assurance component and the assumptions and the organisational security policies are fulfilled.

Moreover, for any other threat not included in the list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The TOEs compliant with collaborative Protection Profile (cPP) for Database Management Systems (version 1.3, 13 March 2023) require the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are defined in section *5.2 Security Objectives for the Operational Environment* of the cPP.

EVALUATION RESULTS

The product collaborative Protection Profile (cPP) for Database Management Systems (version 1.3, 13 March 2023) has been evaluated against the Common Criteria v3.1 R5 and the Common Evaluation Methodology v3.1 R5, complemented with the supporting document Evaluation Activities for the collaborative Protection Profile for Database Management Systems (15 March 2023, version 1.1) edited by the Database Management System (DBMS) international Technical Community (iTC).

As a result of the evaluation, the verdict "**PASS**" has been assigned by the laboratory DEKRA Testing and Certification S.A.U. for all the assurance components required by the APE class: APE_CCL.1, APE_ECD.1, APE_INT.1, APE_OBJ.2, APE_REQ.2 and APE_SPD.1 as defined by the Common Criteria v3.1 R5 and the Common Evaluation Methodology v3.1 R5.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
iTC	international Technical Community

OC Organismo de Certificación

SFR Security Functional Requirement

TOE Target of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[cPP-DBMS] collaborative Protection Profile (cPP) for Database Management Systems (version 1.3, 13 March 2023).

[SD-DBMS] Evaluation Activities for the collaborative Protection Profile for Database Management Systems (15 March 2023, version 1.1).

PROTECTION PROFILE DOCUMENT

Along with this certification report, the complete Protection Profile is available in the Certification Body:

- collaborative Protection Profile (cPP) for Database Management Systems (version 1.3, 13 March 2023).

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.

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 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 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). 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 new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. 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.org.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this Protection Profile is recognized under SOGIS-MRA for all assurance components selected.

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 CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France,

Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://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 nations listed above.

The certificate of this Protection Profile is recognized under CCRA for all assurance components.