National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

U. S. Government Protection Profile Database Management System for Basic Robustness Environments, Version 1.0

Report Number: **CCEVS-VR-04-0080**
Dated: **30 September 2004**
Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team
Kathy Cunningham
Rashida Doss
National Security Agency
Ft. Meade, MD

Common Criteria Testing Laboratory

Evaluation Team
COACT, Inc
Rivers Ninety Five
9140 Guilford Road, Suite G
Columbia, MD 21046-2587

Table of Contents

1. Executive Summary

The evaluation of the U. S. Government Protection Profile Database Management System (DBMS) for Basic Robustness Environments, Version 1.0 was performed by COACT, Inc., CAFÉ Lab CCTL in the United States and was completed on 30 September 2004. The Protection Profile (PP) identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the APE requirements of the Common Criteria for IT Security Evaluation (Version 2.1).

This Validation Report applies only to the specific version of the PP as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

The information contained in this Validation Report is not an endorsement of the U. S. Government Protection Profile Database Management System (DBMS) for Basic Robustness Environments, Version 1.0 by any agency of the U.S. Government and no warranty of the PP is either expressed or implied.

The COACT, Inc., CAFÉ Lab evaluation team concluded that the Common Criteria requirements for a PP Evaluation have been met.

The technical information included in this report was obtained from the U. S. Government Protection Profile Database Management System (DBMS) for Basic Robustness Environments, Version 1.0, dated September 30, 2004 produced by U.S. Government and the Evaluation Technical Report (ETR) for U.S. Government Database Management System Protection Profile for Basic Robustness Environments, Dated September 30, 2004, Document No. F4-0904-008, produced by COACT, Inc., CAFÉ Lab.

1.1 Evaluation Details

Dates of Evaluation: September 2003 through September 2004
Evaluated Product: U. S. Government Protection Profile Database Management System for Basic Robustness Environments, Version 1.0, dated September 30, 2004
Developer: TRESYS and National Security Agency (NSA),
CCTL: COACT, Inc., CAFÉ Lab, Columbia, MD
Validation Team: Kathy Cunningham and Rashida Doss, National Security Agency, Ft. Meade, MD
Evaluation Class: None
PP Conformance: None

1.2 Interpretations

National Interpretations

I-0407 Empty Selections Or Assignments, 2003-08-21
I-0410 Auditing of Subject Identity For Unsuccessful Logins, 2002-01-04
I-0414 Site Configurable Prevention of Audit Loss, 2003-07-17
I-0421 Application Notes In Protection Profiles Are Informative Only, 2001-06-22
I-0427 Identification Of Standards, 2001-06-22
I-0429 Selecting One Or More, 2003-08-12

International Interpretations

003 Unique identification of configuration items in the configuration list, 2002-02-11
051 Use of 'documentation' without C&P elements, 2002-10-05
062 Confusion over source of flaw reports, 2001-07-31
065 No component to call out security function management, 2001-07-31
080 APE_REQ.1-12 does not use 'shall examine … to determine', 2000-10-15
084 Separate objectives for TOE and environment, 2001-02-16
085 SOF Claims additional to the overall claim, 2002-02-11
094 FLR Guidance Documentation Missing, 2001-07-31
103 Association of Access Control Attributes with Subjects and Objects, 2003-07-15
104 Association of Information Flow Attributes with Subjects and Objects, 2003-07-15
111 Settable Failure Limits are Permitted, 2003-10-31
137 Rules Governing Binding should be Specified, 2004-01-30
141 Some Modifications to the Audit Trail Are Authorized, 2003-07-15
201 "Other properties" in specified by assignment, 203-10-31
202 Selecting One or More items in a selection operation and using "None" in a assignment, 203-08-26

1.3 Threats to Security

The Protection Profile identified the following Threats:

T.ACCIDENTAL_ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.POOR_DESIGN	Unintentional errors in requirement specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.

T.POOR_IMPLEMENTATION	Unintentional or intentional errors in implementing of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted).
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.
T.UNIDENTIFIED_ACTIONS	Failure of the authorized administrator to identify and act upon unauthorized actions may occur.

2. Identification

2.1 PP and TOE Identification

PP: U. S. Government Protection Profile Database Management System for Basic Robustness Environments, Version 1.0, dated September 30, 2004.

CC Identification – *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, ISO/IEC 15408.

CEM Identification – *Common Evaluation Methodology for Information Technology Security*, Part 1: Introduction and General Model, Version 0.6, January 1997; *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999.

2.2 PP Overview

The "U.S. Government Protection Profile Database Management Systems for Basic Robustness Environments" specifies security requirements for a commercial-off-the-shelf (COTS) database

system that includes, but is not limited to, DBMS clients and DBMS servers and will 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) and its environment.

Conformant products provide access control based on user identity (e.g., Discretionary Access Control (DAC)) and generation of audit records for security relevant events. The IT environment must provide the following functionality: identification and authentication, security administration and audit record storage, and audit review. A conformant product, in conjunction with its IT environment that satisfies all the requirements in this protection profile, provides necessary security services, mechanisms, and assurances to process administrative, private, and sensitive/proprietary information. The intended environment for conformant products has a relatively low threat for the sensitivity of the data processed. Authorized users, including authorized administrators, of the TOE generally are trusted not to attempt to circumvent access controls implemented by the TOE to gain access to data for which they are not authorized.

This PP defines:

- assumptions about the security aspects of the environment in which the TOE will be used;
- security objectives of the TOE and its environment;
- functional and assurance requirements to meet those security objectives; and
- rationale demonstrating how the requirements meet the security objectives, and how the security objectives address the threats.

A TOE conformant to this PP satisfies the specified functional requirements, as well as the Basic Robustness assurance requirements that are expressed in Section 5.3 TOE Security Assurance Requirements. The assurance requirements were originally based upon Evaluated Assurance Level (EAL) 2 requirements augmented from part 3 of the Common Criteria with Flaw Remediation (ALC_FLR.2), and Misuse-Examination Guidance (AVA_MSU.1).

These explicit assurance requirements were deemed necessary by NSA to reduce the ambiguity in the associated CC assurance families and to provide the level of assurance appropriate for basic robustness environments. For more detail information on the assurance requirements, reference Section 5.3 of this PP.

2.3 IT Security Environment

The TOE described in this PP is intended to operate in environments having a basic level of robustness.

A Basic Robustness TOE is considered sufficient for low threat environments or where compromise of protected information will not have a significant impact on mission objectives. This implies that the motivation of the threat agents will be low in environments that are suitable for TOEs of this robustness. In general, basic robustness results in “good commercial practices”

that counter threats based in casual and accidental disclosure or compromise of data protected by the TOE

Basic robustness allows processing of data at a single sensitivity level in an environment where users are cooperative and threats are minimum. Authorized users of the TOE are cleared for all information managed by the DBMS, but may not have the need-to-know authorization for all of the data. Hence, the risk that significant damage will be done due to compromise of data is low.

Entities in the IT environment on which the TOE depends for security functions must be of at least the same level of robustness as the TOE.

The TOE in and of itself is not of sufficient robustness to store and protect information of such criticality that the integrity or secrecy is critical to the survival of the enterprise.

The term, "enclave", further characterizes the environment in which the TOE is intended to operate. An enclave is under the control of a single authority and has a homogeneous security policy, including personnel and physical security, to protect it from other environments. An enclave can be specific to an organization or a mission and it may contain multiple networks. Enclaves may be logical, such as an operational area network, or be based on physical location and proximity. Any local and external elements that access resources within the enclave must satisfy the policy of the enclave.

The DBMS is expected to interact with other IT products that reside in the host OS, in the IT environment in which the host computer and host OS reside, outside that environment but inside the enclave. The IT and non-IT mechanisms used for secure exchanges of information between the DBMS and such products are expected to be administratively determined and coordinated. Similarly, the IT and non-IT mechanisms for negotiating or translating the DAC policy involved in such exchanges are expected to be resolved by the organizations involved.

3. Security Policy

The Operational Security Policies defined for the TOE:

P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ROLES	The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

4. Assumptions

Personnel and Physical Assumptions

The specific conditions below are assumed to exist in a PP-compliant TOE environment.

A.AUDIT_REVIEW	The IT environment will provide the proper mechanisms to handle review of the TOE audit logs.
A.AUDIT_STORAGE	The IT environment will provide a means for secure storage of the TOE audit logs and management of that data.
A.DOMAIN_SEPARATION	The IT environment will provide a separate domain for the TOE's operation.
A.I_AND_A	It is assumed that the IT environment will provide identification and authentication mechanisms for the TOE.
A.NO_BYPASS	The IT environment will ensure the TSF cannot be bypassed in order to gain access to TOE data.
A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance
A.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration and support of the DBMS.
A.PHYSICAL	It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
A.ROBUST_ENVIRONMENT	It is assumed that the IT environment is at least as robust as the TOE.
A.SECURE_COMMS	It is assumed that the IT environment will provide a secure line of communications between the remote user and the TOE.

A.TIME_STAMPS	It is assumed that the IT environment will provide the TOE with the necessary reliable timestamps.

5. Architectural Information

This PP does not dictate a specific architecture. The TOE may operate in several different architectures, for example:

- A stand-alone system workstation running both the DBMS server and a DBMS client and serving one online user at a given time;
- A network of workstations or terminals running DBMS clients and communicating with a DBMS server simultaneously; these devices may be hardwired to the host computer or be connected to it by means of local or wide-area networks.
- A network of workstations communicating with one or more application servers, which in turn interact with the DBMS on behalf of the workstation users or other subjects (e.g., a DBMS server interacting with a transaction processor that manages user requests).
- A network of workstations communicating with several distributed DBMS servers simultaneously; the DBMS servers may all be within a single local area network, or they may be distributed geographically.

This PP allows each of these architectures as well as others to be supported in each configuration, where the TOE is the DBMS server application, and possibly DBMS procedures that reside on an application server, as well as the DBMS clients on user workstations. The other configuration components are external IT entities.

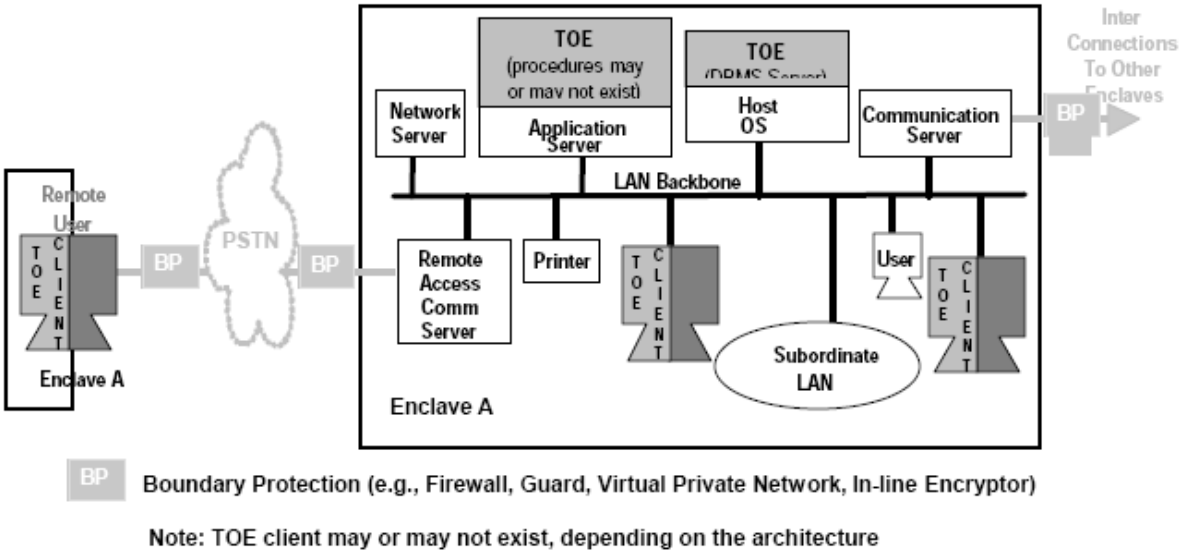

Figure 1 - Depiction of TOE Configuration

Figure 1 shows an enclave, in which DBMS users access the TOE via a local area network (LAN) and also possibly using a dial-up connection. Users in other enclaves will access the LAN

and the host computers and servers on it by way of one or more boundary protection mechanisms (e.g., a firewall) and then through a communications server or router to the LAN. Depending on the particular enclave configuration and the DBMS access policy that it supports, all users (both inside and outside the enclave) may then access an application server, which either connects the TOE user to the enclave computer on which the TOE operates or manages the complete user/DBMS session.

6. Documentation

U. S. Government Database Management System Protection Profile for Basic Robustness Environments, Version 1.0, Dated September 30, 2004.

7. Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the APE section of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of the APE assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., APE) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone, electronic mail, and meetings. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. No constraints or assumptions were identified in performing this evaluation.

Chapter 4, Evaluation Results, in the Evaluation Team's ETR, states:

"The *U.S. Government Database Management System Protection Profile (PP) for Basic Robustness Environments* was successfully evaluated."

Chapter 5, Conclusions, in the Evaluation Team's ETR, states:

"The *U.S. Government Database Management System Protection Profile for Basic Robustness Environments* has satisfied the requirements of the *APE Assurance Requirement*s. The PP was assessed against the requirements as stated in the *Common Methodology for Information Technology Security Evaluation Part 2, Version 1.0*."

8. Validation Comments/Recommendations

The validation team had no recommendations concerning the U. S. Government Database Management System Protection Profile for Basic Robustness Environments, Version 1.0.

Comments

This PP evaluation precedes the certification and publication of the *U.S. Government Protection Profile for Single-level Operating Systems in Environments Requiring Basic Robustness*, Version 0.3, dated 29 January 2004, which at the time of certification was under development.

9. Abbreviations

Abbreviations	Long Form
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CEM	Common Evaluation Methodology
CIM	Consistency Instruction Manual for Development of U.S. Government Protection Profiles for Use in Basic Robustness Environments
CM	Configuration Management
COTS	Commercial off the shelf
CSP	Critical Security Parameters
DAC	Discretionary Access Control
DBMS	Database Management System
DID	Defense in Depth
DoD	Department of Defense
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IATF	Information Assurance Technical Framework
IT	Information Technology
I&A	Identification and Authentication
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OR	Observation Report
PP	Protection Profile
PPRB	Protection Profile Review Board
QA	Quality Assurance
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSE	TOE Security Environment
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification
TTAP/CCEVS	Trusted Technology Assessment Program / Common Criteria Evaluation and Validation Scheme

10. Bibliography

The evaluation and validation methodology was drawn from the following:

[CC_PART1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, dated August 1999, version 2.1.

[CC_PART2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, dated August 1999, version 2.1.

[CC_PART2A] Common Criteria for Information Technology Security Evaluation Part 2: Annexes, dated August 1999, version 2.1.

[CC_PART3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, dated August 1999, version 2.1.

[CEM_PART 1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[CCEVS_PUB1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0 May 1999.

[CCEVS_PUB2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000.

[CCEVS_PUB3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 0.5, February 2001

[CCEVS_PUB 4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme

Publication #4, Version 1, March 20, 2001

[CCEVS_PUB 5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, August 2000.

[PPRB_CG_Basic] Protection Profile Review Board, Protection Profile Consistency Guidance for Basic Robustness, Version 2.0, dated 1 March 2004