National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

DB2 Version 8.2

Report Number: CCEVS-VR-04-0077

Dated: 17 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

Jandria Alexander

The Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

Science Applications International Corporation

Columbia. Maryland

Table of Contents

1 EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the CCEVS evaluation of the IBM Corporation DB2 Version 8.2. The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory and was completed during September 2004. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by SAIC and submitted to the validators. The evaluation determined that the product conforms to the Common Criteria Version 2.1, Part 2 extended and Part 3 and meets the requirements of EAL 4 augmented with ALC_FLR.1 (Basic Flaw Remediation).

The TOE is an IBM Corporation relational database management system. The TOE provides interfaces to clients connected to the database server. From the client, commands can be entered interactively or through an executing program to the database server to create databases, database tables, and to store and retrieve information from tables. The TOE operates as a set of software applications in an IT environment (not included in the evaluation) consisting of the hosting operating system and platform. The security services of the IT environment required by the DB2 TOE have not been evaluated and therefore, need to be determined and assessed separately. These IT security services provided by the environment include protection of the TOE security Functions (TSF) domain separation (preventing bypass of the security functions), reliable time-stamps (used in time-stamping audit records), audit generation, security management and user identification and authentication.

The DB2 TOE provides functionality to meet security requirements in the areas of: security audit (generation, association of users in events, and audit review), user data protection, (implementation of a discretionary access control policy for its objects), identification and authentication, security management and protection of the TSF (enforcement of the security policy). The TOE environment and the TOE security requirements are stated in the DB2 8.2 Security Target, September 16, 2004.

The TOE includes Personal Edition, Workgroup Server Edition, Enterprise Server Edition, and Express Edition. The TOE configuration allows for only one instance of a selected edition of DB2 to exist on a single platform.

The validation team observed the activities of the evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team's observations support the conclusion that the product satisfies the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the validation team concludes that the findings of the evaluation team are accurate, and the conclusions justified.

2 IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant (if applicable);
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	DB2 Universal Database V8.2 Workgroup Server Edition: for Windows, Linux, AIX, and Solaris DB2 Universal Database V8.2 Enterprise Server Edition: for Windows, Linux, AIX, and Solaris DB2 Universal Database V8.2 Personal Edition: for Windows and Linux DB2 Universal Database V8.2 Express Edition: for Windows and Linux
Protection Profile	None
Security Target	IBM DB2 Security Target, Version 1.0, September 16, 2004
Evaluation Technical Report	Final Evaluation Technical Report For IBM DB2, Version 1.3, 9/23/04
Conformance Result	Part 2 extended, Part 3 conformant, EAL4 augmented
Sponsor	IBM Canada, Ltd.
Developer	IBM Canada, Ltd.
Evaluators	SAIC

Validators	The Aerospace Corporation

3 SECURITY POLICY

The TOE implements the following Security Policies.

3.1 Identification and Authentication

The TOE implements an Identification and Authentication policy which is responsible for ensuring that no database operations can be performed until the DB2 Instance can confirm (using support of the operating system) that the identified user is identified and authenticated and maintaining the association of user security attributes with subsequent operations once an authenticated connection is established.

3.2 User Data Protection

The TOE implements a discretionary access control, residual information protection, and rollback policy. The TOE provides User Data Protection in the following ways:

- Making and enforcing the access decisions for databases and their associated objects that are subject to the discretionary access control policy.
- Ensuring that protected objects do not contain residual information when they are created, and,
- Providing the ability to roll back operations on database objects and their content.

3.3 Audit

The TOE enforces the generation of audit records according to how it is configured (e.g. based upon audit type), including the timestamp from the operating system in the audit records, and provides support for the review of the audit data.

3.4 TSF Protection

The TOE provides support for the Protection of the TSF security function at its interfaces by allowing access only when its security mechanisms have been successfully invoked. Additionally, the TOE collects time information from the environment (i.e., the operating system)

3.5 Security Management

The TOE provides security management functionality necessary to manage TOE data. The functionality includes support for the following:

- Management of the audit function and review of audit data, allowing access to functions that manage user security attributes (granting and revoking), and;

- Management of access control settings on databases content.

The TOE supports the roles of authorized administrator and user. As part of the security management policy, the TOE also ensures that only authorized administrators can perform functions not allowed to normal users.

4 ASSUMPTIONS

4.1 Usage Assumptions

The system is expected to be used in what has traditionally been known as a relatively benign, or non-hostile, environment.

The Assumptions as presented in the ST are noted below.

Personnel Assumptions

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
- Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.

Physical Assumptions

The TOE is intended for application in areas that have physical control and monitoring. It is assumed that the following physical conditions will exist:

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- The hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

Connectivity Assumptions

- All connections to peripheral devices reside within the controlled access facilities. The TOE only addresses security concerns related to the manipulation of the TOE through its authorized access points. Internal communication paths to access points such as terminals are assumed to be adequately protected.

Environmental Assumptions

- The IT Environment underlying the TOE is assumed to fulfill the requirements for the IT Environment described in the ST. It is also assumed that the IT Environment will provide a suitable operational environment for the TOE where the TOE will be able to properly execute and the dependencies that the TOE has upon the IT Environment are properly fulfilled.

The ST identifies the following requirements for the IT Environment:

Security Functional Class	IT Environment Security Functional Components
Security Audit (FAU)	FAU_GEN.1b Audit data generation
User Data Protection (FDP)	FDP_RIP.2b Full residual information protection
Identification and authentication (FIA)	FIA_ATD.1b User attribute definition
	FIA_SOS.1 Verification of secrets
	FIA_UAU.2b User authentication before any action
	FIA_UAU.7 Protected authentication feedback
	FIA_UID.2b User identification before any action
Security management (FMT)	FMT_MTD.1c Management of TSF data
	FMT_MTD.1d Management of TSF data
	FMT_MTD.1e Management of TSF data
	FMT_REV.1b Revocation
	FMT_SMF.1b Specification of Management Functions
	FMT_SMR.1b Security Management Roles
Protection of the TSF (FPT)	FPT_AMT.1 Abstract Machine Testing
	FPT_RVM.1b Reference Mediation
	FPT_SEP.1 Domain Separation
	FPT_STM.1b Reliable Time Stamps

5 ARCHITECTURAL INFORMATION

DB2 is a multi-user RDBMS that operates in the context of a hosting operating system and allows authorized users to create and manage databases.

DB2 operates as a set of applications (e.g., servers) in an IT Environment consisting of all software residing on the host platform but not part of the DB2 TOE. The IT Environment provides fundamental supporting mechanisms to the TOE. It provides a trusted authentication mechanism, Domain separation, and utilities to manage system resources and I/O channels.

The TOE consists of the following logical components:

- DRDA Application Server
- SQL Processing

Together the DB2 TOE subsystems provide security functionality for audit generation, selection, review and protection; access control; identification and authentication; management of security functions; and protection of TOE security functions.

DRDA Protocol Handler

The DRDA Application Server (AS) module within DB2 allows for DB2 to act as an Application Server within the Distributed Relational Database Architecture (DRDA). The DB2 DRDA AS module architecture provides support for one or more clients, to access a specific DB2 instance or DB2 database and issue SQL and non-SQL requests against that object. Upon initiation of communication with a client, the DRDA AS performs userid/password validation. If validation of the password fails, the DRDA AS terminates conversation with the client that provided the failed password. If the password is authenticated, a DRDA session, or connection, is established and the client may begin to pass requests to DB2 for processing. These requests are of two general types: SQL requests, which are handled by the DB2 SQL Processing module, and non-SQL requests, which are handled by the DB2 Non-SQL Processing module. The DRDA AS module identifies the type of request and passes it to the appropriate module for further processing.

SQL Processing

The DB2 SQL Processing module is responsible for the analysis and execution of client requests related to the processing of Structured Query Language (SQL) statements. DB2 supports the ANSI/ISO SQL2 standard for all types of SQL statements including:

- Data Definition Language (DDL) statements that create, alter, drop, or rename database objects.
- Data Manipulation Language (DML) statements that are used to query or modify the data contained within database objects. Modification can occur in one of three ways: row insertion, row deletion, or row modification via column updates. These statements include SELECT, INSERT, UPDATE, and DELETE SQL statements.

- GRANT and REVOKE statements that are used to control the access to database authorities as well as privileges on database objects
- Transaction control statements that are use to manage the integrity of the database with respect to any modification made by a client. These statements include, among others, the ROLLBACK and COMMIT SQL statements..
- Miscellaneous statements used to perform a number of different actions on database objects or on the connection environment. Such statements would include the LOCK TABLE and SET statements.

The DB2 SQL Processing module is comprised of the SQL Manager, the SQL Compiler, and the SQL Runtime components.

6 DOCUMENTATION

Following is a table of the evaluation evidence used to support this evaluation:

Evidence

Category	Title(s)
Security Target	IBM Corporation DB2 8.2 Security Target, Version 1.0, 09/16/04
Configuration Management	IBM Corporation DB2 8.2 Configuration Management Plan, Revision 0.8, July 26, 2004
Life Cycle	IBM Corporation DB2 8.2 Life Cycle Document, Revision 0.7, July 26, 2004
Delivery and Operation:	IBM Corporation Delivery Procedures, Revision 0.4, 12/24/03
	Common Criteria Certification Process Document for Distributed Software (DSW) Downloads, Version 1.3, 12/16/2003
Design Documentation:	IBM Corporation Functional Specification, Revision 0.96, 07/26/04
	IBM Corporation High-level Design Specification, Revision 0.7, 07/26/04
	IBM Corporation DB2 Universal Database 8.2 Low-level Design Specification, Revision 0.5, 07/26/2004
	DB2 Access Control Mechanism FPFS, Version 0.8, 16 July 2004
	DB2 Audit Facility Design, Version 2.1, July 26, 2004
	DB2 Audit Facility FPFS, Version 1.1, July 26, 2004
	DB2 Identification & Authentication Facility Design, Version 3.1, July 26, 2003
	DB2 Identification & Authentication Facility FPFS, Version 1.1, July 26, 2004
	DB2 Security Management Facility FPFS, Version 0.41, 26 July

Category	Title(s)
	2003
	DB2 Self Protection Facilities FPFS, Version 0.4, 16 March 2004
	IBM Corporation DB2 8.2 Security Target, Version 1.0, 09/16/04
	IBM Corporation DB2 Universal Database 8.2 Security Policy Model, Revision 0.3, 07/26/2004
Guidance Documentation:	IBM® DB2 Universal Database Common Criteria Certification: Administration and User Documentation, Version 8.2, Revision 05 IBM® DB2 Universal Database Common Criteria Certification: Installing DB2 Universal Database Enterprise Server Edition and DB2 Universal Database Workgroup Server Edition, Version 8.2, Revision 08 IBM® DB2 Universal Database Common Criteria Certification: Installing DB2 Universal Database Express Edition, Version 8.2, Revision 08 IBM® DB2 Universal Database Common Criteria Certification: Installing DB2 Universal Database Personal Edition, Version 8.2, Revision 07
Test Documentation:	IBM DB2 Universal Database Version 8.2 Test Plan, Version 0.4, July 15, 2004
	DB2 Universal Database Test Coverage Analysis
Vulnerability and Assessment Documentation:	IBM Corporation DB2 Universal Database Version 8.2 Vulnerability Analysis, Version 0.3, July 26, 2004

7 IT PRODUCT TESTING

7.1 Vendor Testing

The DB2 security testing consisted mainly of automated tests augmented with a few manual procedures. The tests map to the test cases outlined in the *IBM Corporation DB2 8.2 Universal Database Functional Specification* document and demonstrate the security-relevant behavior of DB2 at the interfaces defined in the functional specification. These interfaces consist of the Command Line User Interface, SQL Interface, API Interface, and the DRDA Interface.

The goal of the tests is to demonstrate that DB2 meets the security functional requirements specified in the Security Target.

The security functions tested are those described in the Security Target: Audit, User Data Protection, Identification & Authentication, Security Management, and Protection of the TSF.

7.2 Evaluator Testing

The evaluation team performed the TOE installation, as specified in the Installation, Generation and Startup documentation, functional, independent and vulnerability testing.

The test configuration consisted of Version 8.2 of DB2 installed on four separate machines: one running the Windows 2000 operating system, one running SuSe Linux Enterprise Server 8, one running AIX 5.2, and one running Solaris 8.

The following product types were installed on the following platforms:

Workgroup Server Edition: Solaris platform

Enterprise Server Edition: AIX platform

Personal Edition: Linux platform

Express Edition: Windows platform

The evaluation team ran a subset of the vendor test suite, ensuring that the team selected tests from each security function. The evaluation team also factored in the TOE functionality and ensured that they ran several tests exercising the database's primary security function, Access Control (or User Data Protection (UDP)).

8 EVALUATED CONFIGURATION

In the evaluation configuration, the TOE can be installed upon AIX 5, SuSE Linux Enterprise Server V8, Windows 2000 Professional, Server, or Advanced Server, Solaris 8 as reflected in the following list.

DB2 Universal Database V8.2 Workgroup Server Edition: for Windows, Linux, AIX, and Solaris

DB2 Universal Database V8.2 Enterprise Server Edition: for Windows, Linux, AIX, and Solaris

DB2 Universal Database V8.2 Personal Edition: for Windows and Linux

DB2 Universal Database V8.2 Express Edition: for Windows and Linux

9 RESULTS OF THE EVALUATION

The evaluation was conducted based upon the Common Criteria (CC), Version 2.1, dated August 1999 [1,2,3]; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999 [5]; and all applicable National and International Interpretations in effect as of the start of the evaluation. The interpretations identified to apply to the evaluation are: RI-3, 4, 8, 51, 65, 94, 103, 141, and 202.

The evaluation confirmed the product as being Part 2 extended and Part 3 EAL 4 augmented compliant. The details of the evaluation are recorded in the Evaluation Technical Report, which is controlled by the SAIC CCTL. The product was evaluated and tested against the claims presented in the IBM Corporation DB2 8.2 Security Target, Version 1.0, 16 September 2004.

The validation team followed the procedures outlined in the Common Criteria Evaluation Scheme [CCEVS] publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

Evaluation of the IBM DB2 V8.2 Security Target (ST) (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the IBM DB2 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 4 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation.

Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 4 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer.

Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification, a high-level design document, a low-level design document, and a security policy model. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Additionally, the evaluation team ensured that the security policy model document clearly describes the security policy rules that were found to be consistent with the design documentation.

Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE.

Evaluation of the Life Cycle Support (ALC)

The evaluation team applied each EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE.

The evaluation team also applied the ALC_FLR.1 related work units from the Flaw Remediation CEM Supplement (Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R). The evaluation team ensured the developer has a process to track flaws, document flaws, address flaws, and provide flaw information to TOE users.

Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE security functional requirements are enforced by the TOE. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor test suite, the independent tests, and the penetration test further demonstrated the claims in the ST.

10 VALIDATOR COMMENTS AND RECOMMENDATIONS

The validator observations support the evaluation team's conclusion that the DB2 V8.2 meets the claims stated in the Security Target. The Security Target delineates the security requirements of the TOE, which determined the scope of the evaluation. The security requirements allocated to the IT environment have not been verified as part of the DB2 TOE evaluation. The IT security services provided by the environment support the protection of the TOE security Functions (TSF) including domain separation, reference mediation (preventing bypass of the security functions), reliable time-stamps (used in time-stamping audit records), audit generation, security management and user identification and authentication. The FPT_SEP.1 requirement is allocated exclusively to the IT environment. Therefore, the scope of the evaluation does not include a determination of the ability of the TOE to protect itself from tampering or the ability to maintain a security domain that is protected from interference and tampering by untrusted subjects or to enforce separation between the security domains of subjects in the TOE Scope of control. Other SFRs allocated exclusively to the IT environment include FIA_SOS.1, FIA_UAU.7 and FPT_AMT.1. Therefore the IT environment is also exclusively responsible for meeting the strength metrics for authentication secrets, obscuring feedback during authentication, and providing abstract machine testing.

11 SECURITY TARGET

The IBM Corporation DB2 8.2 Security Target, Version 1.0, 16 September 2004 is included here by reference.

12 GLOSSARY

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

13 BIBLIOGRAPHY

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

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

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes; dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements; dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

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

[7] Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R

[8] Evaluation Technical Report for IBM DB2 Part 2 (Proprietary), Revision 1.3, September 23, 2004.

[9] IBM Corporation DB2 8.2 Security Target, Version 1.0, 16 September 2004.

[10] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001