National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

IBM Canada, Ltd., Ontario, CANADA

IBM DB2 Enterprise Server Edition V9.7 for Linux, Unix, and Windows

Report Number: **CCEVS-VR-VID10336-2009**
Dated: **18 August 2009**
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 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Dr. Patrick W. Mallett
The MITRE Corporation
McLean, Virginia

Mr. Daniel P. Faigin, CISSP
The Aerospace Corporation
El Segundo, California

Common Criteria Testing Laboratory

Ms. Cynthia Reese Ms. Dawn Campbell Ms. Marie Eve Pierre
Science Applications International Corporation Columbia, Maryland

This report contains material that was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report are extracted from the IBM DB2 Security Target.

TABLE of CONTENTS

ACKNOWLEDGEMENTS 2
EXECUTIVE SUMMARY 6
1 IDENTIFICATION 8
2 SECURITY POLICY 9
2.1 Audit 9
2.2 Access Control 9
2.3 Identification and Authentication 10
2.4 Security Management 11
2.5 TOE Protection 11
3 ASSUMPTIONS AND CLARIFICATION OF SCOPE 12
3.1 Usage Assumptions 12
3.1.1 Personnel Assumptions 12
3.1.2 Physical Assumptions 12
3.1.3 Connectivity Assumptions 12
3.2 Operating Environment 12
3.3 Clarification of Scope 14
4 ARCHITECTURAL INFORMATION 16
4.1 DRDA Protocol Handler 18
4.2 SQL Processing 18
4.3 SQL Manager 19
4.4 SQL Compiler 20
4.5 SQL Runtime 20
4.6 Non-SQL Processing 20
5 DOCUMENTATION 21
5.1 Design documentation 21
5.2 Guidance documentation 21

5.3 Lifecycle documentation 22
5.4 Test documentation 22
5.5 Security Target 22
6 IT PRODUCT TESTING 23
6.1 Vendor Testing 23
6.1.1 Testing Approach 23
6.1.2 Test Descriptions 23
6.1.3 Depth and Coverage 23
6.1.4 Test Results 23
6.2 Evaluator Testing 24
7 EVALUATED CONFIGURATION 25
8 RESULTS OF THE EVALUATION 26
8.1 Evaluation of the IBM DB2 Security Target (ST) (ASE) 26
8.2 Evaluation of the Development (ADV) 26
8.3 Evaluation of the Guidance Documents (AGD) 26
8.4 Evaluation of the Life Cycle Support Activities (ALC) 26
8.5 Evaluation of the Test Documentation and the Test Activity (ATE) 27
8.6 Evaluation of the Vulnerability Assessment Activity (AVA) 27
8.7 Summary of Evaluation Results 27
8.8 Assurance Requirement Results 27
8.8.1 Common Criteria Assurance Components 28
8.8.2 Testing and Vulnerability Assessment 28
8.9 Conclusions 28
8.9.1 ST Evaluation 28
8.9.2 TOE Evaluation 28
8.10 Summary of Evaluation Results 29
9 VALIDATOR COMMENTS AND RECOMMENDATIONS 30
10 SECURITY TARGET 32

11 ACRONYMS 33
12 BIBLIOGRAPHY 34

EXECUTIVE SUMMARY

This report documents the results of the Validation Panel's oversight of the evaluation of the IBM Corporation DB2 Version 9.7 product. It presents the evaluation results, justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) performed the evaluation. The Lab completed the evaluation in July 2009. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by SAIC and submitted to the Validation Panel. The evaluation determined that the product conforms to the Common Criteria Version 3.1 Revision 2, Part 2 extended and Part 3 conformant and meets the requirements of Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.1 (Basic Flaw Remediation).

This evaluation was primarily a maintenance upgrade, with two narrowly focused changes. Previous versions of IBM DB2 have undergone successful evaluations. The 9.7 evaluation introduced the following features: finer granularity in the role mechanism allowing for separation of duties, the option to use AES to protect the communication of the user ID and password to the TOE.

The TOE is an IBM Corporation relational database management system. The TOE provides interfaces to clients connected to the database server. Commands are entered from the client 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 Information Technology (IT) environment consisting of the hosting operating system and platform (not covered by the evaluation). The security services of the operational environment required by the DB2 TOE have not been evaluated and therefore, need to be determined and assessed separately. The IT security services provided by the environment include support for protection of the TOE Security Functions (TSF), 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 following areas:

- Security audit (generation, association of users in events, audit overflow detection, and audit review),
- User data protection, (implementation of a discretionary access control policy (DAC) and a label based access control (LBAC) 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 Security Target (DB2 9.7 Security Target, Revision 1.0, 3 August 2009). The TOE includes DB2 Enterprise Server Edition Versions for Linux, Unix and Windows operating systems.

The cryptography used in this product is provided by the IBM Global Security Kit (GSKIT) component and the IBM Crypto for C (ICC) component both of which were not analyzed within the scope of this evaluation. However, both have received Federal Information Processing Standard (FIPS) 140-2 validation.

The Validation Team provided oversight on the activities of the evaluation team, 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 Common Evaluation Methodology (CEM) work units), and reviewed successive versions of the ETR and test report. The Validators' observations support the CCTL's conclusion that the product satisfies the functional and assurance requirements defined in the Security Target (ST). Therefore, the Validation Panel concludes that the findings of the evaluation team are accurate, and the conclusions justified.

1 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 to identify the product.

Table 1. Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	IBM DB2 Enterprise Server Edition V9.7 for Linux, Unix, and Windows
Protection Profile	None
Security Target	IBM DB2 Enterprise Server Edition V9.7 for Linux, Unix, and Windows Security Target, Revision 1.0, 3 August 2009
Evaluation Technical Report	Final Evaluation Technical Report For IBM DB2 Version 9.7, Part1 (Non Proprietary), Version 1.0, 4 August 2009; Final Evaluation Technical Report For IBM DB2 Version 9.7, Part 1 (Proprietary), Version 1.0, 4 August 2009; Final Evaluation Technical Report For IBM DB2 Version 9.7, Part 2 (Proprietary), Version 1.0, 4 August 2009
CC Version	Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 2, September 2007. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, Revision 2, September 2007
Conformance Result	Part 2 extended, Part 3 conformant, EAL4 augmented
Sponsor	IBM Canada, Ltd.
Developer	IBM Canada, Ltd.
Evaluators	SAIC, Columbia, MD
Validators	Mr. Daniel P. Faigin, CISSP, The Aerospace Corporation Dr. Patrick W. Mallett, The MITRE Corporation

2 SECURITY POLICY

The TOE supports the following security functions: Audit, Access Control, Identification and Authentication, Security Management, and TOE Protection.

2.1 Audit

DB2 records security relevant events that occur within its scope of control. These events are associated with individual users for individual accountability and can be accessed only by authorized administrators[1]. For DB2 instances and databases the audit log files are stored in files in the operational environment (i.e., underlying OS) configured during installation and the audit configuration file (db2audit.cfg) is located in each instance's security subdirectory. In addition to relying on the underlying OS to store and protect audit data stored in files, DB2 relies on the OS to provide reliable time information to record in its audit records.

2.2 Access Control

DB2 enforces an access control policy on a subset of its objects, which per the Security Target are databases**,** schemas, table spaces, tables, views, packages, procedures, functions, and methods. DB2 associates privileges and authorities with each individual user, group of users, and database role. These privileges and authorities are associated with operations that can be performed on the objects (e.g., database) that are implemented by DB2. DB2 uses identities, privileges, authorities, and access control lists associated with users, groups, roles, and objects to determine whether specific operations will be allowed when attempted by client users.

Note that while the term 'security roles' is used in this ST to distinguish authorized administrators from non-administrator users, DB2 implements this concept using a variety of authorities and privileges. DB2 implements a number of authorities–SQLADM, WLMADM, ACCESSCTRL, DATAACCESS, SYSADM, SYSCTRL, SYSMON, SYSMAINT, DBADM, or SECADM.

SYSADM authority makes a user a system administrator. The system administrator is not considered a database administrator and has no inherent privilege in the database. Users with system administrator authority have sufficient authority to run most DB2 utility programs, issue database manager commands, maintain database partition groups, table spaces, and bufferpools. SECADM makes a user a security administrator that performs database security administration, and essentially has full control of database security. DBADM authority is intended to allow management of a database, but the authority can be limited depending on whether ACCESSCTRL or DATAACCESS are also granted. As of Version 9.7, DBADM authority no longer inherently grants additional database level authorities to the applicable authorization id. The ACCESSCTRL authority provides the

[1] The term *authorized administrator* is used to generally refer to an administrator authorized (e.g., by role) to perform a corresponding function depending on the context in which the term is used.

holder with the ability to issue grant and revoke statements on objects. In previous versions of DB2, ACCESSCTRL authority was held implicitly by all database administrators. In order to preserve existing DB2 behavior, the GRANT DBADM syntax provides two new options: WITH ACCESSCTRL and WITHOUT ACCCESSCTRL. Without the DATAACCESS authority, the database administrator is restricted from accessing data in the database tables. Users with this authority can issue the database load statement; issue the select, insert, updated, and delete statements on tables, views, and nicknames; and, execute packages and routines (except further restricted audit routine). Note that, as with ACCESSCTRL authority, DATAACCESS authority was previously held implicitly by all database administrators. In order to preserve existing DB2 behavior, the GRANT DBADM syntax provides two new options: WITH DATAACCESS and WITHOUT DATAACCESS.

In addition to using privileges and authorities to control access, DB2 implements a LBAC mechanism on database table objects. The DB2 security administrator can grant (or revoke) security labels and exemptions to (or from) users as well as create and drop LBAC security objects in order to define LBAC polices for specific database tables. Once a table is configured with a LBAC policy (i.e., the table is LBAC protected relative to either rows or columns), users must additionally satisfy the LBAC access rules in order to access or modify the applicable table rows or columns. It is important to note that LBAC only applies to configured tables and that DB2 is not a multilevel system. It is assumed the TOE administrators will be cleared to the highest security level processed by the TOE.

2.3 Identification and Authentication

DB2 requires all users to be identified and authenticated before allowing them access to DB2 resources. The operational environment (i.e., host operating system, Lightweight Directory Access Protocol (LDAP) server, or Key Distribution Center (KDC) server) performs the actual authentication and association of users with groups and passes the result to DB2. DB2 subsequently enforces the result returned by the operational environment and uses the user identity and group memberships (i.e., list of groups) returned by the operational environment, along with its own associations of users, groups, and other database roles with database roles, to associate privileges, authorities, and security labels and exemptions with the authenticated user.

Note that the association between users and groups is managed within the operational environment. Operational environment user and group identities are uniquely mapped in the TOE and when a user accesses the TOE, the operational environment provides the user and all group identities associated with that user. However, database roles are defined within the TOE where users, groups, and other database roles can be associated with specific database roles.

Users who acquire a trusted connection may have the ability to use alternate identities, without further authentication, in accordance with the definition of the trusted context object associated with that trusted connection in the TOE. A trusted context definition may only be defined by a user with SECADM authority and it may be defined to require authentication or to not require authentication upon the changing of identities. They could be

configured so that they can use only a specific set of identities or alternately so that they can use any identity known to the TOE.

2.4 Security Management

DB2 includes the security roles of system administrator, security administrator, and user, implemented using DB2 authorities and privileges. DB2 allows individual users to be assigned to those security roles by virtue of group assignments in the operational environment. Management of the DB2 TOE, including the ability to select and review audit records, is restricted to appropriate administrators based on authorities. Management of DB2 objects, including management of security labels, as well as database roles and audit policies is restricted to those users that are assigned the appropriate privileges to do so.

Note that the trusted context feature effectively introduces a new security role, referred to simply as *trusted context* in this Security Target, as the users trusted by virtue of a trusted context configuration may have the ability to assert alternate identities without requiring authentication by the TOE, depending upon how the SECADM defined the associated trusted context.

2.5 TOE Protection

DB2 executes within processes provided and protected by the hosting operational environment. However, DB2 is not designed to share its process space with non-TOE entities in order to ensure that TSF resources are protected. DB2 has been designed so that each of its interfaces performs the necessary access checks before allowing access to DB2 resources. DB2 communicates between Database Partition Facility (DPF) instances, when so configured, and with clients that can be remote from the DB2 server. DB2 implements Secure Sockets Layer (SSL), using a separate GSKit product in the operational environment for cryptographic services. DB2 can be configured using the IBM Crypto for C (ICC) library to implement AES for protection of the user ID and password as it is communicated to the TOE. Otherwise, DB2 relies upon the operational environment to ensure adequate communication protections. In the case of DPF instances, a dedicated network can be configured to be used exclusively by DB2.

Remote clients need to communicate securely with DB2. If some of the hosts on the applicable network are not adequately trusted, IPSec or other host- or network-based protection mechanisms could be configured to protect any otherwise insecure network traffic.

Fenced routines execute in processes separate from the DB2 server, while unfenced routines share the DB2 server process. Given that the DB2 server must protect itself (e.g., from tampering) and its ability to do so is limited when users can create routines that execute within the same operating system process, unfenced routines are excluded from the evaluated configuration of the TOE.

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

3.1 Usage Assumptions

The expectation is that the system will 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.

3.1.1 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 access authorization to at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
- Procedures exist for granting users authorization for access to specific security levels.

3.1.2 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 that will prevent unauthorized physical access.
- The hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

3.1.3 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. It is assumed that internal communication paths to access points such as terminals are adequately protected.
- The operational environment underlying the TOE is assumed to fulfill the requirements for the operational environment described in the ST.

3.2 Operating Environment

The following components are required in the operational environment to provide the

following services to the TOE.

- **Hosting OS**: IBM AIX 6, Red Hat Enterprise Linux (RHEL) 5 update 2, SuSE Linux Enterprise Server (SLES) 10 with SP2, Microsoft Windows Server 2003 Enterprise Edition with SP2, or Solaris 10. The TOE relies on the underlying operating system to perform the following functions:
    - Instantiate the executing DB2 Instance Server process
    - Provide memory that is exclusive to the DB2 Instance Server process
    - Provide memory that does not contain residual information
    - Provide operating system user accounts that DB2 may map to DB2 user accounts
    - Provide management of operating system user accounts to include creation, modification, deletion, and revocation of rights
    - Authenticate user identities given identities and authentication data provided by clients
    - Make information available about the user identities associated with executing processes
    - Provide reliable timestamps for use by DB2 processes
    - Audit its own security functions
    - Provide access to and protection for the DB2 configuration and audit files
    - Provide access to shared memory in order to communicate with the DB2 Instance Server
    - Provide a communication facility/subsystem that allows users and other DB2 partitions to communicate with the applicable DB2 Instance Server
- **Authentication server** (when not using the services of the hosting OS): Any standard-compliant LDAP or KDC server. DB2 can be configured to utilize authentication services of a LDAP or KDC server, rather than the operating system, in its environment. When so configured, DB2 relies on the presence of a standard-compliant server to perform this function rather than the underlying operating system.
- **IBM Global Security Kit**: DB2 depends on access to an installed instance of the IBM GSKit in order to support the use of SSL when communicating with clients.
- **IBM Crypto for C (ICC)**: DB2 uses the AES-256 algorithm from this component to protect passwords as the TOE can optionally be configured to require that passwords be encrypted by associated clients.

3.3 Clarification of Scope

The Security Target specified the security requirements of the TOE, which determined the scope of the evaluation. It is the responsibility of the integrator to ensure the Objectives for the operational environment are satisfied. The IT security services provided by the environment support the protection of the TOE Security Functions (TSF), 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 scope of the evaluation includes a determination of the TOE partially protecting its interface. The TOE relies on the operational environment for protection from tampering and 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.

While DB2 can alternately be installed using a non-root install option, that configuration limits the functions of DB2 and has not been subject to evaluation. Also note that the product is shipped with libraries and programs that expose other application programming interfaces (APIs) (command line, Open Database Connectivity (ODBC), Java Database Connectivity (JDBC), etc.); the libraries and programs simply serve to convert their exposed APIs to Distributed Relational Database Architecture (DRDA) flows to the DB2 server. With the exception of those tools and utilities identified in the TOE's guidance documentation, these libraries and programs are outside the scope of the TOE.

The following products, though required for the operational environment, are outside the scope of the TOE:

- **Hosting OS:** IBM AIX 6, Red Hat Enterprise Linux (RHEL) 5 update 2, SuSE Linux Enterprise Server (SLES) 10 with SP2, Microsoft Windows Server 2003 Enterprise Edition with SP2, or Solaris 10.

- **Authentication server** (when not using the services of the hosting OS): Any standard-compliant LDAP or KDC server.

- **IBM Global Security Kit**

- **IBM Crypto for C (ICC)**. In addition to non-security functions, the following security-related functions are not within the scope of the TOE (i.e., there are no corresponding security claims) even though they are shipped with the product:

- **Data Encryption Standard (DES)**: While the TOE can be configured to use DES to protect authentication credentials, this mechanism has not been subject to evaluation and as such should not be solely relied upon as an adequate means of protection.

- **Data encryption functions (ENCRYPT, DECRYPT_BIN, DECRYPT_CHAR, and GETHINT)**: Users can employ these functions to encrypt and decrypt data. However, the functions were not subject to evaluation and as such should not be solely relied upon as an adequate means of protection. Note that this is intended to

address the functions shipped with the product, but any such functions developed by end users would also not be included within the scope of evaluation.

- **Unfenced routines**: Fenced routines execute in processes separate from the DB2 server, while unfenced routines share the DB2 server process (see section 6.1.5 of the Security Target). Given that the DB2 server must protect itself (e.g., from tampering) and its ability to do so is limited when users can create routines that execute within the same operating system process, unfenced routines are excluded from the evaluated configuration of the TOE.

- **CLIENT authentication**: The TOE supports a number of authentication configurations. While for the most part the TOE administrator can choose the configuration that best fits their specific environment, the configuration whereby the client is trusted to authenticate the user is excluded from the evaluated configuration. The evaluation only addressed the configuration where the DB2 server is responsible to ensure that users are authenticated, although it relies on other configured components to do so.

4 ARCHITECTURAL INFORMATION

DB2 is a relational database management system (RDBMS) provided by IBM. As a RDBMS, DB2 supports the Structured Query Language (SQL) interface from a client that is 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. DB2 can be installed on a number of possible operating environments.

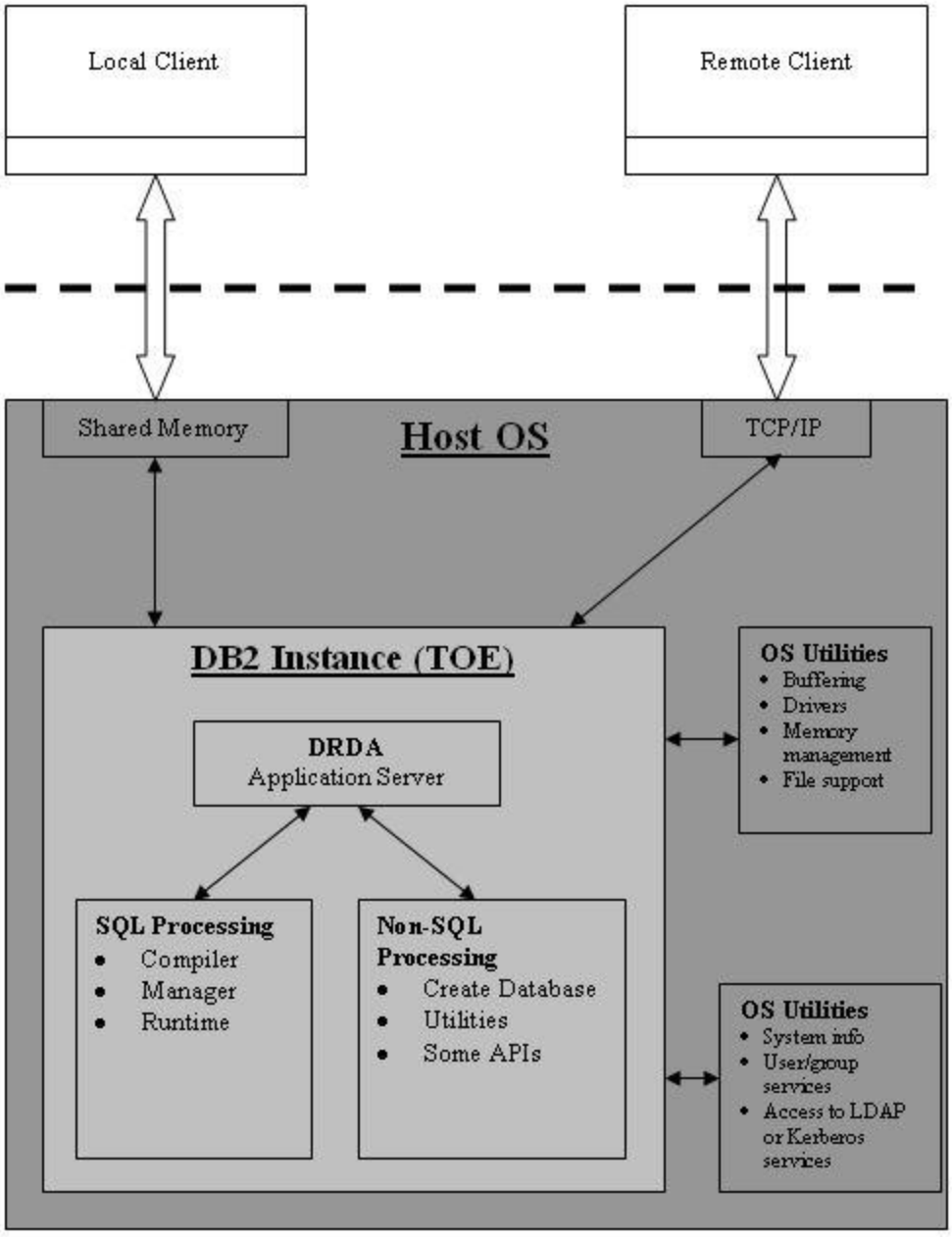

Figure 1. TOE Security Environment

DB2 operates as a set of applications (e.g., servers) in an operational environment consisting of all software residing on the host platform(s) but not part of the DB2 TOE. For the purposes of this discussion, it is referred to as the Host OS. The operational environment, including the Host OS and optionally an LDAP or KDC authentication server, provides fundamental supporting mechanisms to the TOE. In particular, the operational environment supplies a trusted authentication mechanism and utilities to manage system resources and I/O channels.

DB2 is realized as a running server (i.e., DB2 Instance) and a set of commands (i.e., DB2 Commands) that can be exercised by appropriate users. Both the server and the commands rely upon services provided by the operating system to instantiate themselves and offer their services in turn. In particular, the server uses operating system services to communicate with local and remote DB2 clients using shared memory and network services, respectively. Similarly, the DB2 Commands use operating system services to store configuration data (i.e., in files) and to act as a local client to communicate with the server in order to facilitate necessary management services.

A DB2 Server may be configured as a partitioned instance. This optional configuration is known as Data Partitioning Feature (DPF). Each data partition is composed of a complete DB2 Server and a subset of the data stored in all the databases managed by the DB2 Server instance. These partitions may be either "logical" (meaning they run on the same host machine) or "physical" (they run on different host machines). Combinations of both logical and physical partitions are also supported. From a user perspective, the partitioned aspect of the instance is transparent. The user may interact with DB2 as if it was a single server.

DB2 also provides a "trusted context" feature. Trusted contexts are database objects that provide a specification for a trust relationship between the database and an external entity. The trust relationship is based on three attributes: an authorization ID, a data stream encryption attribute, and an IP address (or addresses). The user associated with any connection that matches the definition of a trusted context object is considered "trusted" by the database. Users trusted in this manner (e.g., "trusted servers") can be configured such that they are allowed to modify some of the security attributes associated with their database connections. Specifically, they can be configured such that the "user" associated with an existing connection to be changed. Depending on the DB2 configuration, this may or may not require authentication of the new user identity. Furthermore, the trusted context object can define database roles that can be assigned to trusted context sessions. During the initial connection or during an authorization name (i.e., user) change, the session will be assigned an additional database role if a) one is defined explicitly for the applicable authorization name, or b) there is a default database role defined. When explicitly defined for an authorization name, the session would be assigned that role. Otherwise, the session would be assigned the default database role for the trusted context. If neither is defined then no additional role will be assigned to the trusted context.

The end-user identity assertion aspect of this function is intended for multi-tier environments where the middle tier, typically an application server, might already perform authentication of end users. Trusted contexts provide a mechanism for the

database to trust the middle tier and effectively establish connections on behalf of end users without necessarily supplying the credentials (password) of the end user to the database. For the purpose of this document, Trusted Context users are treated like any other client.

DB2 also supports the use of SSL with clients. As such, users of DB2 can choose to enable that feature, though it is not necessary particularly when other means of client communication protection are configured in the operating environment of DB2. The Common Criteria evaluation design documentation describes DB2 in terms of two subsystems: the Security Management subsystem and the Server subsystem. The Security Management subsystem is responsible to provide the tools and server interfaces necessary for administrators and other users to manage the security-relevant configuration of DB2. Note that the Security Management subsystem implements only some of the security management related functions. However, it is so named because it provides all of the interfaces that are to be used for security management. In the case where the security management functions are implemented, entirely or in part, in the Server subsystem, the Security Management subsystem provides the user interface and interacts with the Server subsystem to achieve the function. The Server subsystem is responsible to implement database instances, offering interfaces for the creation and manipulation of databases and associated database objects.

4.1 DRDA Protocol Handler

The DRDA Application Server (AS) module within DB2 allows DB2 to act as an Application Server within the Distributed Relational Database Architecture (DRDA). DRDA is an Open Group standard used in the management of distributed data. The DB2 DRDA AS module architecture provides support for one or more DRDA Application Requestors (DRDA AR), commonly referred to as clients, to access a specific DB2 instance or DB2 database and issue SQL and non-SQL requests against that object. Upon initiation of communication between a client and the DB2 DRDA AS module, a common "security mechanism" is negotiated. This mechanism may be one of a number of different security protocols; for the purpose of this TOE, the only allowed security mechanism is the "Userid, Password" mechanism as described in the DRDA standard. 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.

4.2 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 American National Standards Institute (ANSI)/ International Organization for Standardization (ISO) SQL2 standard for all types of SQL statements including:

- Data Definition Language (DDL) statements that create, alter, drop, rename, or transfer ownership of 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 (Data Control Language (DCL)) statements that control the access to database authorities as well as privileges on database objects.
- Transaction control statements that 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. The DB2 SQL Processing module is comprised of three distinct components: the SQL Manager, the SQL Compiler, and the SQL Runtime components. The responsibilities of these components as they relate to the processing of SQL statements are described in the following sections.

4.3 SQL Manager

The SQL Manager is responsible for accepting SQL requests from the client, validating them, and then coordinating any subsequent processing of the request to ensure it is properly answered. The SQL Manager can accept SQL requests related to static or dynamic SQL statements. Static SQL statements have their contents made known to DB2 prior to the request arriving from the client through a process called "binding," which results in the statement being compiled by the SQL Compiler and the resultant information being stored in the DB2 system catalogs for later use. Dynamic SQL statements are unknown to DB2 until the request arrives, at which time they are compiled by the SQL Compiler. The information produced by the SQL compiler contains the executable form of the statement, referred to as a section, a list of the required privileges for any client wishing to run the section as well as a list of the database objects upon which the section is dependent for its execution integrity.

The SQL Manager processes SQL requests from a client by matching the request to a specific SQL statement. Once the statement has been identified and its related information acquired (from either the DB2 system catalogs or the SQL Compiler), the SQL Manager then enforces the discretionary access control policy by ensuring that the required privileges for the section are held by the primary authorization name (a specific user identifier), or by any relevant secondary authorization names (the identifiers for any relevant groups to which the primary authorization name belongs and roles to which any other authorization name belongs[2]), associated with the request from the client. If the

[2] Note that users, groups, and other roles can be assigned to roles. As such, role hierarchies are supported.

privileges are held, then the section is passed to the SQL Runtime component for execution.

4.4 SQL Compiler

The SQL Compiler is responsible for analyzing an SQL statement and producing an efficient executable form of that statement, called a “section”, as well as additional information about that section such as its object dependencies and required privileges. The SQL Compiler parses an SQL statement into an internal representation, or model, of the statement that is then used to analyze the scope and intent of the statement. Additional information is added to the internal model, where appropriate, from the DB2 system catalogs in order to represent properly the full extent of the statement’s use of any database objects. Once complete, the internal model is then analyzed and optimized in order to produce the most efficient plan to satisfy the statement. The SQL Compiler then generates an executable form of the statement using the internal DB2 constructs and operators used by the SQL Runtime component.

4.5 SQL Runtime

Note that users, groups, and other roles can be assigned to roles. As such, role hierarchies are supported. The SQL Runtime component is responsible for the actual execution of the section related to the request and the production of any response to the client required by the request. The success or failure of the actual execution as well as any additional response is given back to the SQL Manager for return to the client.

4.6 Non-SQL Processing

The DB2 Non-SQL Processing module is responsible for the analysis and execution of all those client requests not concerned with SQL statements. Such requests are used to invoke a number of Application Program Interfaces (APIs) and utilities provided by DB2 that do not use SQL statements to perform their specified actions. There exist a number of these APIs and utilities at both the DB2 Instance level as well as at the individual database level within a DB2 instance. Each API and utility provided by DB2 has an assigned privilege or authority requirement as defined by DB2. The DB2 Non-SQL Processing module enforces the discretionary access control policy for these non-SQL requests by ensuring that the required privilege or authority is held by either the primary authorization name or secondary authorization names where applicable, of the requestor.

5 DOCUMENTATION

The following documentation was used as evidence for the evaluation of the TOE. Documents that are publically available are shown in **boldface**.

5.1 Design documentation

Document	Revision	Date
IBM DB2 V9.7 Enterprise Server Edition Functional Specification	0.33	2009-07-07
IBM DB2 V9.7 Enterprise Server Edition High-level Design Specification	0.3	2009-07-02
IBM DB2 V9.7 Enterprise Low-level Design Specification	0.2	2009-04-24
DB2 Access Control Mechanism FPFS	0.1	2008-11-17
DB2 Audit Facility Design	0.2	2008-11-17
DB2 Audit Facility FPFS	0.21	2009-04-24
DB2 Identification & Authentication Facility Design	0.21	2009-04-24
DB2 Identification & Authentication Facility FPFS	0.21	2009-04-24
DB2 Security Management Facility FPFS	0.1	2008-11-13
DB2 Self Protection Facilities FPFS	0.11	2009-04-24
DB2 9.7 Fast Communication Manager Design	0.11	2009-04-24
IBM DB2 V9.7 Enterprise Server Edition for Linux, Unix, and Windows Security Target	1.0	2009-08-03
IBM DB2 V9.7 Enterprise Server Edition Security Architecture Document	0.3	2009-07-02

5.2 Guidance documentation

Document	Revision	Date
Common Criteria Certification: Installing IBM DB2 Version 9.7 Enterprise Server Edition for Linux, UNIX, and Windows, IBM Document No. GC14-7215-00	7	N/A
IBM DB2 9.7 for Linux, UNIX, and Windows: Common Criteria Certification: Administration and User Documentation – Volume 1, IBM Document No. SC14-7213-00	6	N/A
IBM DB2 9.7 for Linux, UNIX, and Windows: Common Criteria Certification: Administration and User Documentation – Volume 2, IBM Document No. SC14-7214-00	5	N/A
IBM DB2 9.7 Delivery Procedures	0.1	2009-02-17

5.3 Lifecycle documentation

Document	Revision	Date
IBM DB2 Enterprise Server Edition Version 9.7 for Linux, Unix, and Windows Configuration Management Plan	0.1	2009-02-17
IBM DB2 Enterprise Server Edition Version 9.7 for Linux, Unix, and Windows Life Cycle Document	0.1	2009-02-17

5.4 Test documentation

Document	Revision	Date
IBM DB2 Enterprise Server Edition Version 9.7 For Linux, Unix, and Windows Test Plan	0.2	2009-04-26
DB2 Universal Database Version V9.7 Test Coverage Analysis	0.3	2009-05-08
IBM DB2 Enterprise Server Edition Version 9.7 For Linux, Unix, and Windows Test Suite Readme Document	0.5	2009-05-13

5.5 Security Target

Document	Revision	Date
IBM DB2 V9.7 Enterprise Server Edition for Linux, Unix, and Windows Security Target	1.0	2009-08-03

6 IT PRODUCT TESTING

6.1 Vendor Testing

The description of the vendor suite is documented in the "IBM DB2 Enterprise Server Edition Version 9.7 For Linux, Unix, and Windows Test Plan" in the section describing the test cases for the Common Criteria.

6.1.1 Testing Approach

The developer testing approach is described in "IBM DB2 Enterprise Server Edition Version 9.7 for Linux, Unix, and Windows Test Plan". The testing of the DB2 security functions is automated. These tests were mapped to the test cases outlined in the Functional Specification document. Together they demonstrate the security-relevant behavior of DB2 at the interfaces defined in that document: the Command Line User Interface, SQL Interface, API Interface, and the DRDA Interface. The results of the tests demonstrated that DB2 meets the security functional requirements specified in the Security Target. The security functions that were tested are the same as those mentioned in the Security Target: Audit, User Data Protection, Identification & Authentication, Security Management, and Protection of the TSF.

6.1.2 Test Descriptions

The test procedure descriptions are documented in a collection of text files that include several test cases. For each test case within the text file, a description of what is tested (equivalent to a test case in the Functional Specification document) and an overview of how it is tested is provided.

A test package is provided for each platform included in the test configuration. The test package includes several directories, each containing test output, test source files, the expected test results, and the actual test results.

6.1.3 Depth and Coverage

The amount of testing performed as it relates to the required functionality is described in the rationale for ATE_COV work units. The depth of testing performed as it relates to the High Level design is described in the rationale for the ATE_DPT work units in the Evaluation Technical Report.

6.1.4 Test Results

The test suite consisted of automated tests. For each test description file, there is corresponding file that describes the expected results and another file that provides the actual results of a test run. Additional files are also generated detailing any inconsistencies between the expected results and the actual results.

6.2 Evaluator Testing

The evaluation team performed the TOE installation, as specified in the Installation, Generation and Startup documentation and performed functional, independent and vulnerability testing. The test configuration consisted of Version 9.7 of DB2 installed on the following platforms: Windows 2003 operating system and RHEL 5.

The following product options were installed on the indicated platforms:

- Enterprise Server Edition on the Windows 2003 platform: Optional features: with DPF configured twice on two DPF installations
- Enterprise Server Edition on RHEL 5 platform: Optional features: with single partition configured
- Enterprise Server Edition on AIX 6 platform: with single partition configured

The test tools used by the developer test suite are documented in the "IBM DB2 Enterprise Server Edition Version 9.7 for Linux, Unix, and Windows Test Plan".

The above test configurations were compared to the TOE identification included in the ST and found to be consistent by the CCTL. All platforms included in the ST were included in the vendor test configuration and sufficiently represented in the evaluator test configuration.

The DB2 security testing consisted of automated test procedures. The tests map to the test cases outlined in "IBM DB2 V9.7 Enterprise Server Edition Functional Specification" 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 results of the evaluator testing demonstrated that DB2 meets the security functional requirements specified in the Security Target. The security functions tested were those described in the Security Target: Audit, User Data Protection, Identification & Authentication, Security Management, and Protection of the TSF. Team tests for audit and access control were performed with passing results. A penetration test for access control (LBAC) was performed with a passing result. The evaluation team ensured the Functional Specification substantiated the TSS in the evaluation of the functional specification (rationale in the ADV_FSP work units). The evaluation team then ensured the vendor's test approach and test suite completely addressed the functional specification in its evaluation of the Test evidence (rationale in the ATE_COV work units).

7 EVALUATED CONFIGURATION

IBM DB2 Enterprise Server Edition Version 9.7 for Linux, Unix, and Windows (the TOE) is a Relational Database Management System (RDBMS) developed by IBM Canada, Ltd., 8200 Warden Avenue East, Markham, Ontario L6G 1C7, Canada and sold by IBM Corporation, Route 100, Somers, NY, USA 10589.

In the evaluated configuration, the TOE can be installed on the following platforms:

- AIX 6
- SuSE Linux Enterprise Server v10 with SP2
- RedHat Linux (RHEL 5) update 2
- Windows Server 2003 with SP2
- Solaris 10

8 RESULTS OF THE EVALUATION

The evaluation was conducted based upon CC version 3.1 Revision 2 and CEM version 3.1 Revision 2. The evaluation determined the IBM DB2 TOE to be Part 2 extended and Part 3 conformant, and that the TOE meets the Part 3 Evaluation Assurance Level (EAL 4) requirements augmented with ALC_FLR.1

8.1 Evaluation of the IBM DB2 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.

8.2 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 security architecture description, a functional specification, basic modular design, and a sample of the implementation representation. 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.

8.3 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 administer the TOE securely.

8.4 Evaluation of the Life Cycle Support Activities (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 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. The evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely.

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.

8.5 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 results of the vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

8.6 Evaluation of the 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 evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

8.7 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 tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

8.8 Assurance Requirement Results

The assurance requirements for the TOE evaluation are those required by EAL4.

8.8.1 Common Criteria Assurance Components

The CEM work units associated with EAL4 are distributed amongst the ETR sections in chapter 15 of the ETR. Collectively, the ETR sections in chapter 15 encompass all CEM work units for EAL4. Each ETR section includes the CEM work units associated with that ETR section title (e.g. ACM). Within each ETR section, for each CEM work unit the following is provided:

- Verdict
- Verdict Rationale

The rationale justifies the verdict using the CC, the CEM, and any interpretations and the evaluation evidence examined. The rationale demonstrates how the evaluation evidence meets each aspect of the criteria.

The work performed contains a description of the action performed or the method used to apply the work unit.

8.8.2 Testing and Vulnerability Assessment

In addition to ETR sections, the evaluators developed a Test Plan/Report Part to capture the detail beyond the CEM work unit information. This detail is described within the CEM guidance for the testing and vulnerability assessment work units. Primarily, the additional detail is focused on team test procedures, penetration test procedures, results from running the vendor's sample, and the justification of running the vendor's sample.

The evaluation team prepared a Draft of the Test Plan/Report prior to testing that addressed the selection of vendor tests to run, the team test procedures, and the penetration test procedures. After performing the test, the Test Report Part was updated to include the actual results from the vendor sample run and the team test. The Test Report is included in the "IBM DB2 9.7 Part 2 Final ETR Proprietary" ETR document, chapter "IBM DB2 Team Test Report".

8.9 Conclusions

The conclusions for the ST evaluations and the TOE evaluations are addressed below.

8.9.1 ST Evaluation

Each verdict for each CEM work unit in the ASE ETR is a "PASS". Therefore, the IBM DB2 Enterprise Server Edition version 9.7 Security Target is a CC compliant ST.

8.9.2 TOE Evaluation

The verdicts for each CEM work unit in the ETR sections included in chapter 15 are each "PASS". Therefore, the IBM DB2 TOE (see below product identification) satisfies the IBM DB2 9.7 Security Target, when configured according to the following guidance documentation: Common Criteria Certification: Installing IBM DB2 Version 9.7 Enterprise Server Edition for Linux, UNIX, and Windows – Revision 7.

8.10 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.

9 VALIDATOR COMMENTS AND RECOMMENDATIONS

This evaluation was primarily a maintenance upgrade, with two narrowly focused changes that affected a few SFRs, and that were mostly independent from other product functionality. The Validation Panel's observations support the evaluation team's conclusion that the DB2 9.7 meets the claims stated in the Security Target. The following are some recommendations and guidance for those integrating this product into a system:

1. The audience should be aware of the impact of configuring the TOE to perform synchronous vs. asynchronous auditing and note the benefits and drawbacks of each approach. A characterization of the audit loss for asynchronous auditing can be found in the Administration Guidance document.

2. There are limitations of the Encrypt/Decrypt UDF approach: namely, that this function allows users to issue instructions to encrypt and decrypt data within DB2. However, IBM generally discourages use of this function since there are a number of known weaknesses (e.g., applicable passphrases are not adequately protected). This function does not serve to allow any access controls, etc. to be violated, but if users were to rely on this mechanism to protect data that would be a mistake. Note that we have been informed it is only in the product due to some backward compatibility issues (for product users).

3. There are limitations to the creation of user accounts and passwords in the Operational environment passwords that might be of concern to the integrator. These limitations can be found in the Administration Guidance documentation.

4. The audience should understand that the scope of the evaluation does not address the protection of the connection to the LDAP or Kerberos servers (e.g. whether or not is encrypted). This may of interest for the integrator.

5. Whether user clients echo passwords or not is not really under the control of the DB2 server. DB2 cannot prevent users from building scripts and put passwords in them. However, when using the provided client, the normal connection interfaces would not echo passwords. It comes down to whether the product knows it is dealing with a password at that point in time and there are areas where the product does not know and hence cannot prevent echoing.

6. The audience should be aware of the implications of the access checking approach for static and dynamic DML. Static DML packages appear to have access checking performed only at the time of binding—at that time, the access is checked for the user bound to that package. To use a given package, the user must be explicitly authorized to do so. Specifically, DB2 checks if the user holds EXECUTE privilege on the package. This is always checked.

7. DB2 also maintains privileges dependencies after a package is bound. If in the future the user who bound the package loses any of the privileges they needed to bind the package, that package becomes invalid and cannot be used unless it is rebound by a user who has the required privileges. For Dynamic DML statements,

the privilege checking is performed for a user when the DML is initially prepared. Subsequent executions for the same user have no privilege checking. Only if these executions are within the same unit of work or in a different unit of work but there were no changes. In other words, if a user prepares a statement and then loses the privileges they needed to prepare that statement, the execution will re-prepare the statement and it will fail if the user still lacks the needed privilege.

8. The scope of the evaluation assumes the administrator is at System High with respect to the LBAC mechanism.

9. Although database commands are available through the CLP, such use is not in accordance with administrative guidance and may introduce unknown risks.

10. Proper protection of the operating environment is important, as this was a key assumption in the vulnerability testing.

11. Passwords used within scripts are stored in plaintext. As such, users and administrators must ensure that such scripts are protected from unauthorized disclosure.

12. The TOE records audit information in multiple audit logs (instance, database, node, etc.). No mechanism is provided to obtain a unified view of these logs. It is the responsibility of integrators of this product to provide appropriate audit log integration and reduction tools.

13. The cryptography used in this product is provided by the IBM Global Security Kit (GSKIT) component and the IBM Crypto for C (ICC) component. Both of which were not analyzed within the scope of this evaluation. However, both components have received Federal Information Processing Standard (FIPS) 140-2 validation.

10 SECURITY TARGET

The IBM Corporation DB2 Version 9.7 Enterprise Server Edition for Linux, Unix, and Windows Security Target, version 1.0, 3 August 2009 is included here by reference.

11 ACRONYMS

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CM	Configuration Management
DAC	Discretionary Access Control
DDL	Data Definition Language
DML	Data Manipulation Language
DRDA	Distributed Relational Database Architecture
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
LBAC	Label Based Access Control
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PP	Protection Profile
RDBMS	Relational Database Management System
SFR	Security Functional Requirement
SQL	Structured Query Language
ST	Security Target
TCSEC	Trusted Computer System Evaluation Criteria
TOE	Target of Evaluation

TSF TOE Security Function TSFI TOE Security Function Interface

12 BIBLIOGRAPHY

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2007, Version 3.1 Revision 2
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated September 2007, Version 3.1 Revision 2
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated September 2007, Version 3.1 Revision 2
4. Common Evaluation Methodology for Information Technology Security Evaluation, Evaluation Methodology, dated September 2007, Version 3.1 Revision 2
5. Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R
6. Evaluation Technical Report for IBM DB2 9.7 Part 2 (Proprietary), Revision 1.0
7. IBM Corporation DB2 9.7 Security Target, Revision 1.0, 3 August 2009.
8. NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001