National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Teradata, a division of NCR, NCR World Headquarters, 1700 S. Patterson Blvd., Dayton, OH 45479

Teradata Database Version 2 Release 6.1.0 (V2R6.1.0)

Report Number: CCEVS-VR-07-0009
Dated: 15 February 2007
Version: 1.1

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

Scott Shorter
Santosh Chokhani
Orion Security Solutions
McLean, VA

Common Criteria Testing Laboratory

Dawn Campbell
Tammy Compton
Craig Floyd
Jasmine Maleki
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Teradata Database Version 2 Release 6.1.0 (V2R6.1.0) (henceforth referred to as Teradata Database). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in February 2007. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.3.

The Teradata Database is a relational database management system (RDBMS) that is designed to access, store, and operate on data using Teradata Structured Query Language (Teradata SQL), which is compatible to ANSI SQL with extensions. The database was developed to allow users to view and manage large amounts of data as a collection of related tables. The database executes as a trusted parallel application (TPA) on a symmetric multiprocessing (SMP) or massively parallel processing (MPP) database server running a commercially available operating system.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). This Validation Report applies only to the specific version of the TOE 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 provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4 augmented with ALC_FLR.3) have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC, the NCR Teradata Database Security Target, and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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 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.
- 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
TOE:	Teradata Database Version 2 Release 6.1.0 (V2R6.1.0) running on Windows Server 2003
Protection Profile	None
ST:	Teradata Database Version 2 Release 6.1.0 (V2R6.1.0) Security Target , Version 2.0, February 2007
Evaluation Technical Report	*Evaluation Technical Report for Teradata Database:* • *Part 1 (Non-Proprietary), Version 1.0, December19, 2006* • *Part 2 (Proprietary), Version 1.6, February 2, 2006*
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3 Part 2: Evaluation Methodology, Supplement: ALC_FLR- Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R

Item	Identifier
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Teradata, a division of NCR
Developer	Teradata, a division of NCR
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD

3 Security Policy

The Security Functional Policies (SFPs) implemented by Teradata Database are based upon the basic set of security policies that include policies that permit protection of user data, provide for authenticated user access, provide accountability for actions, and protect the mechanism that provides the security policies.

Note: Much of the description of the Teradata Database security policy has been extracted and reworked from the Teradata Database Security Target.

3.1 User Data Protection

The Teradata Database enforces a Discretionary Access Control (DAC) policy for object access based on user identities, object ownership, and active roles. All access to database objects subject to the DAC policy is controlled using access rights. The Teradata Database supports three types of access rights. Implicit rights (ownership rights) are implicitly granted to the immediate owner of a database or database object. Automatic rights are granted automatically by the system to the creator of a database, user, or object, and to a newly created user or database. Explicit rights are granted by any user having the WITH GRANT OPTION privilege for that right. The database ensures that the requestor has the appropriate access rights before access to a database object is allowed.

Upon initial installation of the Teradata Database, it has only one user. This user is called user DBC and will own all other databases and users in the system. User DBC also has access rights on all objects within the database with the exception of CREATE PROCEDURE and EXECUTE PROCEDURE. Typically, administrative users are created under user DBC and are granted access rights for creating and managing all other users, databases, and objects.

3.2 Identification and Authentication

The Teradata Database provides user identification and authentication through the use of user accounts and the enforcement of password policies. Users must provide a valid username and password before they can access any database objects or resources. Once identified and authenticated, all subsequent actions allowed within that user's session are based on the user's identity, access rights, and active roles.

3.3 TOE Access

The Teradata Database allows authorized administrative users to restrict access to the database based on user identities.

3.4 Security Audit

The Teradata Database automatically audits all successful and failed user logon attempts and security management actions in the event log. An authorized administrative user may search and sort logon/logoff records using SQL statements to query a defined system view. Additionally, an authorized administrative user may control the monitoring of access rights checks performed by Teradata Database and may search and sort access log records using SQL statements to query a defined system view.

3.5 Security Management

The Teradata Database provides security management functions that enable authorized administrative users to manage the secure operation of the database. These functions include management of users, user security attributes, access rights, security roles, and the audit facilities.

3.6 Resource Utilization

The Teradata Database enforces maximum quotas and limits on various resources to ensure that those resources are protected from monopolization by any individual database user. Specifically, an authorized administrator can configure the database to enforce limits on permanent database space allocation, temporary database space usage, and spool database space usage.

3.7 Protection of the TOE Security Functions

The Teradata Database is designed with well-defined interfaces that ensure that all appropriate security checks are made before access is provided to protected database objects and resources. The Teradata Database operates as a set of cooperating processes which are managed by the underlying operating system. These processes operate as a trusted parallel application (TPA) such that no interference is allowed by processes associated with any non-TOE entities. Furthermore, the Teradata Database is designed such that its interfaces do not allow unauthorized users access to database resources.

4 Assumptions

4.1 Usage Assumptions

The Teradata database is installed, configured and administered in accordance with the evaluated configuration guidance.

The Teradata database administrator is competent and trusted not to abuse his/her privilege.

4.2 Environmental Assumptions

The Teradata database server is located in a physically protected, secure facility in order to prevent physical access to the TOE by anyone other than authorized personnel.

All users of the operating system upon which Teradata is installed are Teradata database administrators.

Communication paths between the clients and database server are protected.

Any other IT components with which the Teradata database communicates are assumed to be under the same management control and operate under the same security policy.

4.3 Overarching Policies

The security requirements enforced by the TOE were designed based on the following overarching security policies:

- **Accountability**. The users of the system shall be held accountable for their actions within the system.
- **Authorization**. Only those users who have been authorized to access the information within the system may access the system.
- **Need to Know**. Only those authorized users that have a 'need to know' for information will be provided access to the protected resources.

5 Architectural Information

Note: The following architectural description is based on the description presented in Part I of the Teradata Database ETR and in the Security Target.

The Teradata Database is comprised of several software subsystems including the Parallel Database Extension (PDE), Gateway for LAN, Session Controller, Parser and Access Module Processors (AMP). A Session Controller and a Parser subsystem are always configured together in what is called a Parsing Engine (PE) virtual processor.

The PDE subsystem is a software interface layer that operates on top of the host operating system and provides an interface between the other database subsystems and the underlying operating system software. PDE includes a BYNET driver that manages the communication devices that interconnect the hardware nodes on which the server software is resident. It provides a standard interface for inter-process communications across nodes in a multi-node environment. PDE also includes a Console module (CNS) that manages the interface for input and output generated from a Database Window (DBW) on the Console.

The Gateway for LAN subsystem provides the client communications interface to Client applications connected via a network interface. It receives all messages sent from the client to the server. This includes messages containing Teradata SQL statements as well as messages for functions such as connecting and disconnecting sessions, determining the configuration of the server, establishing the security protocols to be used between the client and server, and responding to test messages that determine the health of the server over the LAN. For messages that contain Teradata SQL, the Gateway for LAN checks those messages to ensure that they conform to the specified protocol and forwards them to a Parser subsystem. The Gateway for LAN also receives response messages from the PE

subsystems and returns them to the appropriate Client application. The Gateway for LAN also interacts with PDE for memory management and message handling services and for access to underlying operating system services.

A PE virtual processor always includes a Session Controller and a Parser subsystem. The Session Controller processes external requests to establish or terminate a logical connection between the application and the server. It also provides for the recovery of sessions following client or server failures. The Session Controller manages session activities, such as logon, password validation and logoff. The Parser decomposes SQL into relational database management processing steps. It processes external requests containing Teradata SQL by syntactically parsing the statements and generating a set of steps comprising an execution plan for the statements. Other Parser modules then access the generated steps and send them to one or more AMP subsystems for execution. Parser modules also monitor the execution of the steps, handle errors encountered during processing and return the execution results to the Gateway for return to the Client application.

An AMP subsystem physically structures the TOE managed relational data and it processes the steps of an SQL execution plan to access that data. It also manages a set of relational tables containing the description of the user defined data objects. The AMP subsystem provides access to these dictionary tables to Client applications through standard SQL and to other database subsystems as needed and is responsible for the integrity of the relational data structures. The AMP subsystem reads and writes the relational data structures from/to disk storage by making calls to the PDE subsystem which subsequently calls the underlying host operating system to perform the required physical read and write operations.

Other components exist in the Teradata Database environment and interface to the database, but are excluded from the definition of the TOE. These components include:

- The operating system on which the database executes
- The database server node upon which the database software and underlying operating system operates
- The disk storage subsystem and its associated SCSI or Fibre Channel interface.
- The Console's Database Window (DBW) software.
- The Teradata Tools and Utilities (Client) applications including the Call Level Interface (CLI) software that processes messages sent to, and received from, the database.

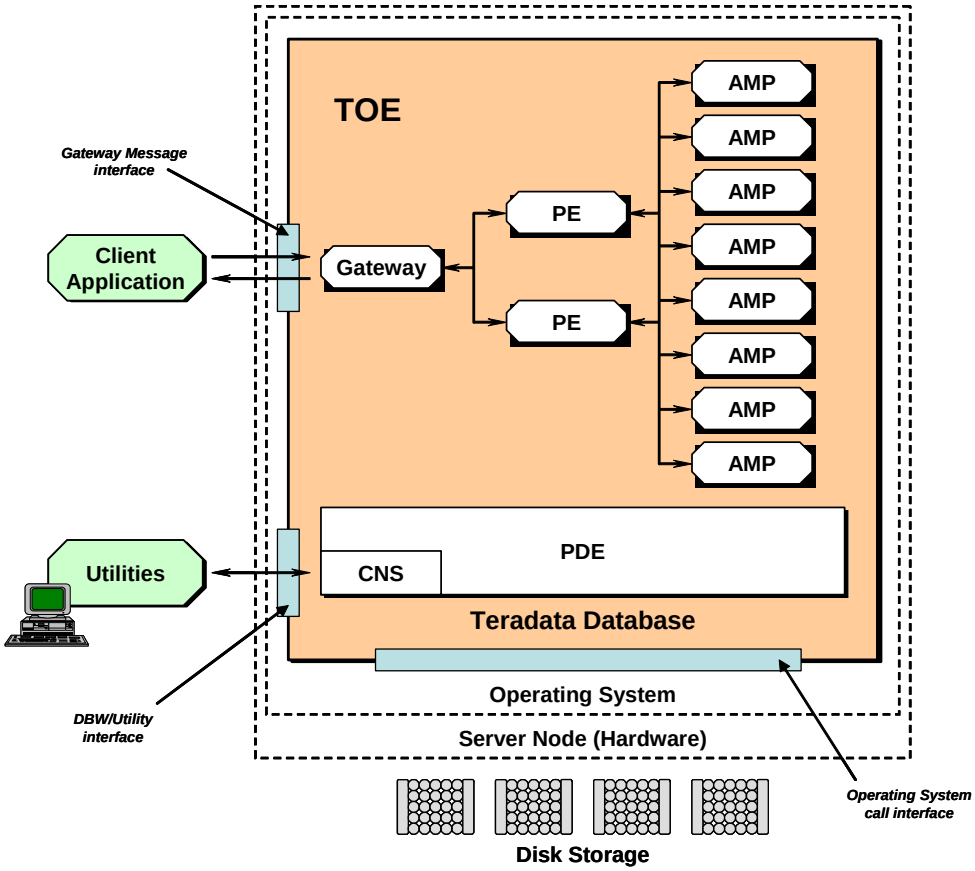
There are two external interfaces to the Teradata Database. The Gateway Message interface receives text messages containing service requests from Client applications and returns text message responses to the applications upon completion of a service request. The DBW/Utility interface provides for Console access to executable processes of the PDE subsystem.

The Teradata Database makes calls to the underlying operating system to access operating system services and to access the associated disk storage subsystem.

Note that the TOE is defined as a software-only TOE. As such, the Server Node (Hardware) and Disk Storage is specifically outside the TOE boundary. (The disk storage

resides in a separate disk array cabinet that is packaged completely separately from the Server Node hardware. In some very small environments where the Teradata Database may be running on a standalone server platform, the disk storage may be packaged as part of the server platform.)

Figure 5-1 TOE Physical Boundaries



6 Documentation

The following documentation was used as evidence for the evaluation of the Teradata Database:[1]

6.1 Configuration Management

1. Software Configuration Management (SCM) CMM Practices, 541-0001722
2. ClearCase Labeling and Branching Standards, 007-0005448
3. Configuration Item List:
    a. 6.1.0_config_spec.txt
    b. 6.1.0_config_spec_BYNET.txt
    c. 6.1.0_config_spec_PDE.txt
    d. 6.1.0_source.txt

[1] This documentation list is based on the list provided in the Evaluation Technical Report, Part 1, developed by SAIC.

e. 6.1.0_source_BYNET.txt
f. 6.1.0_source_PDE.txt

4. Web TRP Quick Reference, 541-0002801
5. Information Engineering Development and Delivery Process, 541-0002721
6. DARTS Quick Reference, 541-0005154
7. Sample DARTS Report: DR Report - V2R6.1.0.xls

6.2 Delivery and Operation

1. Teradata V2R6.1 Delivery Process, 541-0004
2. Customer Procedures for NCR, W. Columbia, Pegasus Logistics Group
3. Teradata Database Release Summary, Release V2R6.1.0, B035-1098-115A
4. Teradata Database Base System Release Definition, Release V2R6.1.0, B035-1725-115K
5. Teradata Database for Microsoft Windows Server 2003 (32-bit) Installation Guide, Release 6.1, B035-5219-115K
6. NCR 540S Node for Microsoft Windows Server 2003 (32-bit) Software Installation Guide, Release 6.1, B035-5218-115K
7. Parallel Upgrade Tool (PUT) for Microsoft Windows User Guide, Release 3.04.02, B035-5710-115K
8. Teradata Database Security Administration, Release V2R6.1.0, B035-1100-115A

6.3 Design Documentation

1. Teradata Server EAL4 CC Evaluation Functional Specification, 541-0004655
2. Teradata Server EAL4 CC Evaluation High Level Design, 541-0004656
3. Teradata Server EAL4 CC Evaluation Low Level Design - AMP Subsystem, 541-0005919
4. Teradata Server EAL4 CC Evaluation Low Level Design - PDE Subsystem, 541-0005920
5. Teradata Server EAL4 CC Evaluation Low Level Design - Gateway Subsystem, 541-0005921
6. Teradata Server EAL4 CC Evaluation Low Level Design - Session Control Subsystem, 541-0005922
7. Teradata Server EAL4 CC Evaluation Low Level Design - Parser Subsystem, 541-0005923
8. Teradata Database EAL4 CC Evaluation Representation Correspondence, 541-0004678
9. Teradata Server EAL4 CC Evaluation Security Policy Model, 541-0006147
10. Teradata Database V2R6.1 Source Code
11. Teradata Database Database Administration, Release V2R6.1, B035-1093-115A
12. Teradata Database Security Administration, Release V2R6.1, B035-1100-115A
13. Teradata Database Data Dictionary, Release V2R6.1, B035-1092-115A
14. Teradata Database SQL Reference – Fundamentals, Release V2R6.1, B035-1141-115A
15. Teradata Database SQL Reference - Data Definition Statements, Release V2R6.1, B035-1144-115A
16. Teradata Database Utilities – Volume 1 A-F, B035-1102-115A
17. Teradata Database Utilities – Volume 2 G-S, B035-1102-115A
18. Teradata Database Utilities – Volume 3 T-Z, B035-1102-115A
19. Teradata Database Messages, Release V2R6.1 & Teradata Tools and Utilities 08.01.00, B035-1096-115A
20. Teradata Database Graphical User Interfaces: Database Window and Teradata MultiTool, Release V2R6.1, B035-1095-115A
21. Teradata Database Performance Management, Release V2R6.1, B035-1097-115A
22. Teradata Manager User Guide, Release 07.01.00, B035-2428-115A
23. Teradata Call-Level Interface Version 2 Reference for Network-Attached Systems, Release 04.08.01, B035-2418-115A
24. Teradata FastLoad Reference, Release 07.07.00, B035-2411-115A
25. Teradata MultiLoad Reference, Release 07.08.00, B035-2409-115A
26. Teradata FastExport Reference, Release 07.08.00, B035-2410-115A

6.4 Guidance Documentation

1. Teradata Database Database Administration, Release V2R6.1, B035-1093-115A
2. Teradata Database Security Administration, Release V2R6.1, B035-1100-115A
3. Teradata Database Data Dictionary, Release V2R6.1, B035-1092-115A
4. Teradata Database SQL Reference – Fundamentals, Release V2R6.1, B035-1141-115A
5. Teradata Database SQL Reference - Data Definition Statements, Release V2R6.1, B035-1144-115A
6. Teradata Database Utilities – Volume 1 A-F, B035-1102-115A
7. Teradata Database Utilities – Volume 2 G-S, B035-1102-115A
8. Teradata Database Utilities – Volume 3 T-Z, B035-1102-115A
9. Teradata Database Messages, Release V2R6.1 & Teradata Tools and Utilities 08.01.00, B035-1096-115A
10. Teradata Database Graphical User Interfaces: Database Window and Teradata MultiTool, Release V2R6.1, B035-1095-115A
11. Teradata Database Performance Management, Release V2R6.1, B035-1097-115A
12. Teradata Manager User Guide, Release 07.01.00, B035-2428-115A
13. Teradata Call-Level Interface Version 2 Reference for Network-Attached Systems, Release 04.08.01, B035-2418-115A
14. Teradata FastLoad Reference, Release 07.07.00, B035-2411-115A
15. Teradata MultiLoad Reference, Release 07.08.00, B035-2409-115A
16. Teradata FastExport Reference, Release 07.08.00, B035-2410-115A

6.5 Life Cycle

1. Corporate Management Policy Manual - Protecting Information within NCR, Policy No. 1402
2. Information Protection Standard - Information Protection Baseline Requirements, Policy No. 102
3. Securitas Security Services, Facility Entry and Exit Control, No. 105
4. DARTS Quick Reference, 541-0005154
5. Teradata Database Engineering Software DR Process Using DARTS, 541-0001057
6. Teradata Global Support Center Service Delivery Process Support Center Practices 2.0, 950003
7. Teradata Global Support Center Incident Management Process Support Center Practices 2.0, 950000
8. Teradata Global Support Center Tech Alert Process, 950012
9. Teradata Research & Development PRP Quick Reference, 541-0000017
10. Teradata Research & Development Alternate Development Models, 541-0001900
11. Master Integration Plan for Teradata Database Version 2 Release 6.1, 541-0004943
12. Microsoft Visual Studio, Microsoft Corp., Online Reference Manual, http://msdn2.microsoft.com/en-us/library/ms269115.aspx

6.6 Testing

1. Teradata Server EAL4 CC Evaluation System Test Overview, 541-0004842
2. Teradata Server EAL4 CC Evaluation - Test Suite 1, 541-0004843
3. Teradata Server EAL4 CC Evaluation - Test Suite 2, 541-0004844
4. Teradata Server EAL4 CC Evaluation - Test Suite 3, 541-00048453
5. Teradata Server EAL4 CC Evaluation - Test Suite 4, 541-0004846
6. Teradata Server EAL4 CC Evaluation - Test Suite 5, 541-0004847
7. Teradata Server EAL4 CC Evaluation - Test Suite 6, 541-0006329
8. Test code

6.7 Vulnerability Assessment

1. Teradata Database EAL4 CC Evaluation - Guidance Analysis, 541-0006423

2. Teradata Database EAL4 CC Evaluation - Strength of Function Analysis, 541-0004942
3. Teradata Database EAL4 CC Evaluation - Vulnerability Analysis, 541-0004834

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Plan for the Teradata Database Product, Version 1.0, December 19, 2006.

7.1 Developer Testing

- At EAL4, testing must demonstrate correspondence between the tests and the functional specification and high level design. The vendor testing was extensive and covered all of the security functions identified in the ST and interfaces in the design. The following table summarizes the security functions and functional classes tested, with a brief summary of the test cases.

Security Function	Functional Classes Tested	Summary of Test Cases
Identification and Authentication And TOE Access	FIA FTA	• Test multiple logons with invalid passwords. Determine the action taken by the system based on system settings for password characteristics. • Define profiles with different password characteristics and create users with these profiles. • Create new users with various password characteristics • Logon with an invalid user identifier. • Logon with an invalid password and submit SQL statements prior to logon. • Logon with an expired password. • Create roles and associate users with those roles. • Test session establishment using the Grant/Revoke Logon statements • Test expired passwords at logon • Test reuse of previously used passwords
User Data Protection	FDP	1. Actions by the owner of the object • Interactive operations by the owner of the object • Application programmed operations by the owner of the object • Archive/restore operations by the owner of the object 2. Operations with explicitly granted privileges • Interactive operations with privileges explicitly granted to an individual • Application programmed operations with privileges explicitly granted to an individual • Archive/restore operations with privileges explicitly granted to an individual 3. Operations through roles • Interactive operations with privileges explicitly granted to a role • Application programmed operations with privileges explicitly granted to a role • Archive/restore operations with privileges explicitly granted to a role.

Security Management	FMT	Tests the ability: • to restrict to the administrator the right to enable and modify the behavior of the threshold for unsuccessful authentication attempts and the actions to be taken in the event of an authentication failure. • to restrict to the administrator the right to create users, profiles and roles and to assign to users the quotas of disk space and cpu usage necessary . • of users to revoke selected privileges they either own or have granted and the subsequent enforcement of that revocation.
Security Audit	FAU	• Initiate logging of access checks using the begin/end logging statements • Execute server actions which will cause audit entries to be generated • Execute SQL statements to display the logged entries. • Demonstrate that access checks cannot be bypassed and that generated log entries cannot be modified or deleted
Protection of the TSF	FPT FRU	• Test the servers ability to limit quotas. • Test the servers ability to reject use of PDE functions by a non-server executable.

Developer tests had a significant degree of automation, with custom applications written to execute scripts that were developed by the vendor. The scripts are commented so that it is possible to understand their intended purpose.

7.2 Evaluation Team Independent Testing

The evaluation team verified that the TOE was installed as is specified in the secure installation procedures, reran all developer tests and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

Evaluation team tests were performed in the following areas:

- Independent Tests
  - Confirming that the user's role information is stored in audit logs.
  - Testing the ability to revoke a user's ability to create or access objects.
  - Following the steps in the administrative guidance to ensure that the expected results followed.
  - Confirming the password selection rules are enforced.
  - Confirming that the resource utilization constraints are properly enforced.
- Vulnerability Tests
  - Confirming that the database authentication procedures could not be subverted with Windows domain authentication.

- Port scanning of the TOE in the evaluated configuration to ensure that no ports are open other than those required by the product.
- Testing of the operating system's discretionary access control settings was performed, and it was determined that the Security Target required an update to ensure that non-administrative personnel were not granted logical access to the system as a result
- Deliberately sending malformed packets over the client server interface to ensure that the server drops the invalid messages.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Teradata Database Version 2 Release 6.1.0 (V2R6.1.0) running on Windows Server 2003. The product comes preinstalled in its evaluated configuration as identified in the following manual - Teradata Database Security Administration, Release V2R6.1, B035-1100-115A.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL4 augmented with ALC_FLR.3 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.3 and CEM version 1.0 [5], [6]. The evaluation determined the NCR Teradata TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.3 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

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

9.2 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. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from NCR and performed a CM audit.

9.3 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. The evaluation team followed the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

9.4 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.

9.5 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. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 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.

In addition to the EAL 4 ALC CEM work units, the evaluation team applied the ALC_FLR.3 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

9.7 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 enforces the TOE security functional requirements. 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.

9.8 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.

9.9 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.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

As with any server product, the administrators of the TOE should take steps to harden the operating system prior to installing the product, including but not limited to, removing any unnecessary user accounts and software products. The raw database contents are not protected by the operating system discretionary access control, so it is very important that non-administrators be denied logical access to the system.

While there are no security claims in the security target pertaining to cryptography, if the software's cryptographic features are used, it is recommended that FIPS 140-2 approved

algorithms be selected[2], for example the GLOBAL_QOP_1 Quality of Protection configuration shown in the Security Administration document uses approved algorithms.

During the vulnerability analysis, it was determined that the TOE does not mitigate the risk inherent in the lack of segregation of duties between database administration and security management. As a result, it is possible that privileged users could perform improper actions and perform security management activities to attempt to cover their tracks. While the ST assumes that administrators are well trained and trustworthy, good security practices include additional checks and balances. If separation of duties among administrators is required, one way to mitigate this risk is to install the TOE in a controlled location and provide logical access only via a console in the room and then use two person physical controls (e.g., dual locks) to ensure separation of duties.

11 Security Target

The Security Target is identified as *Teradata Database Version 2 Release 6.1.0 (V2R6.1.0) Security Target,* Version 2.0, February 2007.

12 Glossary

The following definitions are used throughout this document:

- **Attribute.** A characteristic or trait of an entity that describes the entity; for example, the telephone number of an employee is one of that employee's attributes. An attribute may have a type, which indicates the range of information given by the attribute, and a value, which is within that range.
- **Audit Trail.** Data, in the form of a logical path that links a sequence of events, used for tracing the transactions that affected the contents of a record.
- **Authentication.** Verification of the identity of a user or the user's eligibility to access an object.
- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

[2] A list of those algorithms may be found at http://csrc.nist.gov/cryptval/.

- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 2.3, August 2005.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 2.3, August 2005.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 2.3, August 2005.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.

[5] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 1.0, August 1999.

[6] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[7] Science Applications International Corporation. *Evaluation Technical Report for the Teradata Database, Part 1 (Non-Proprietary)*, Version 1.0, December 19, 2006.

[8] Science Applications International Corporation. *Evaluation Technical Report for the Teradata Database Part 2 (Proprietary)*, Version 1.6, February 2, 2007.

[9] Science Applications International Corporation. *Evaluation Team Test Plan for the Teradata Database Product, ETR Part 2 Supplement (SAIC and NCR Proprietary)*, Version 1.0, December 19, 2006.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] *Teradata Database Version 2 Release 6.1.0 (V2R6.1.0) Security Target, Version 2.0, February 2007*