National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

MetaMatrix Enterprise Release 5.5.3

Report Number: CCEVS-VR-VID10199-2009
Dated: August 18, 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

Paul Bicknell
Jean J. Hung
The MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

Mr. Dragua Zenelaj
CygnaCom Solutions
McLean, Virginia

Much of the material in this report 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 were extracted from the MetaMatrix Enterprise Release 5.5.3 Security Target.

Table of Contents

List of Figures

List of Tables

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product MetaMatrix Enterprise Release 5.5.3 (with patch r553_090507_0021**)**.

The Validation Report presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

MetaMatrix Enterprise Release 5.5.3 (MetaMatrix) is an enterprise information integration (EII) system. EII is based on the premise that enterprises have a variety of information sources and information types, distributed geographically, and owned by different parts of the enterprise. A basic tenet of EII is that information should be capable of integration regardless of its native physical storage characteristics.

MetaMatrix manages and describes information that is spread across disparate enterprise information systems. Using MetaMatrix these enterprise information systems can be integrated into a single, complete data access solution. It provides a way to define the characteristics of information and how information is related, and manage this "data about data", or "Metadata". MetaMatrix users can issue queries to any data source, process and integrate the results derived from multiple sources.

MetaMatrix protects the distributed data and Metadata through an access control policy, user identification and authentication, role-based management functions and auditing of security relevant events.

The MetaMatrix is intended for use in computing environments where there is a low level threat of malicious attacks.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in July 2009. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 3.1 R2 [CC] Part 2 and Part 3 conformant, and meets the assurance requirements of EAL 2 extended from the Common Methodology for Information Technology Security Evaluation, Version 3.1 R2, [CEM]. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific security objectives.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org. The Security Target (ST) is contained within the document "MetaMatrix Enterprise Release 5.5.3 Security Target, Version 1.5", dated July 10, 2009.

During this validation, the Validators determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validators conclude that the CygnaCom findings are accurate, the conclusions justified, and the conformance claims correct.

2. Identification

Target of Evaluation:	MetaMatrix Enterprise Release 5.5.3
Security Target:	MetaMatrix Enterprise Release 5.5.3 Security Target, Version 1.5, July 10, 2009.
Evaluated Software:	MetaMatrix Enterprise Release 5.5.3 The following patch must be applied to the MetaMatrix server system: • r553_090507_0021.jar
Sponsor:	Red Hat, Inc 77 Westport Plaza, Suite 160 St. Louis, Missouri 63146
Developer:	Red Hat, Inc 77 Westport Plaza, Suite 160 St. Louis, Missouri 63146
CCTL:	CygnaCom Solutions 7925 Jones Branch Dr, Suite 5200 McLean, VA 22102-3321
Evaluators:	Dragua Zenelaj
Validation Scheme:	NIAP Common Criteria Evaluation and Validation Scheme
Validators:	Paul Bicknell Jean Hung
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1 R2, September 2007
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 R2, September 2007

3. Organization Security Policy

The TOE's security policy is expressed in the security functional requirements identified in the section 6.1 in the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements. A description of the principle security policies is as follows:

3.1. Security Audit

MetaMatrix's auditing capabilities include recording information about system processing and users' access to the TOE. Subject identity (user login name) and outcome are recorded for each event audited. The audit records generated by MetaMatrix are protected by the TSF interfaces working in conjunction with the protection mechanisms of the IT Environment.

The audit function requires the following support from the TOE's IT environment:

- The third-party RDBMS that stores the audit records to protect the audit records from unauthorized access (unauthorized deletion and modification)
- The OS of the TOE component host platforms to protect the audit records stored in logfiles to ensure it's protected from unauthorized deletion and modification.
- The platform to provide reliable time when required to ensure the audit records have meaningful timestamps.

3.2. Data Protection

MetaMatrix provides its own access control separate from the IT Environment between subjects and objects covered by the MetaMatrix Access Control SFP. MetaMatrix provides facilities to define and manage permissions (authorizations) to control a user's access to both Data from the EISs and Metadata stored in the MMR.

Authorization controls the privileges of users to access information. This is also referred to as "Entitlements". Entitlements represent named sets of access rights. Entitlements control which data constructs, such as tables or columns, a user account can create, read, update, and / or delete. MetaMatrix provides facilities to define, manage, and use Entitlements for both data access, and for controlling access to information Metadata.

3.3. Identification and Authentication

Each user must be successfully identified and authenticated with a username and password by the TSF or by an authentication service invoked by the TSF before access is allowed to MetaMatrix. There are two ways that users can be authenticated to the MetaMatrix system in the evaluated configuration. The first is through username and password. The second is through authentication by a third-party Membership Domain Provider. The TSF maintains security attributes for each individual TOE user for the duration of the user's login session.

3.4. Security Management

MetaMatrix provides role-based security management functions through the use of the Console. Through the enforcement of the MetaMatrix Access Control SFP, the ability to manage various security attributes, system parameters and all TSF data is controlled and limited to those users who have been assigned the appropriate administrative role.

4. Assumptions and Policies

4.1. Environmental Assumptions

The following assumptions apply to the security environment in which the TOE operates:

- It is assumed that there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- It is assumed that there will be no untrusted users and no untrusted software on the TOE server host.
- It is assumed that appropriate physical security is provided to protect the hardware and software critical to the security policy enforcement from unauthorized modification.
- It is assumed that the environment provides a secure channel to protect communications between the TOE components and between the TOE components and the remote users.
- Users will protect their authentication data
- User applications that access the MMR data have been developed, installed and maintained in a secure manner

4.2. Policies

The following organizational security policies are levied against the TOE and its environment as identified in the Security Target:

- The authorized users of the TOE shall be held accountable for their actions within the TOE.
- The TOE users will select secure passwords that meet the Password Policy defined in the user guidance documentation.

5. Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 extended in this case).
2. As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
3. The TOE depends on the IT environment to provide the capability to read the audit records, protect audit information, provide reliable time stamps, conduct user identification and authentication via third-party Membership Domain Provider before any action (option), TOE also provide protections against interference and logical tampering..
4. The following product capabilities were not covered by the evaluation:
    - Product components not used during normal operation (runtime) of the TOE:
        - MetaMatrix Enterprise Designer
        - MetaMatrix Query Builder
        - Connector Developer Kit
        - Command Line Interface utilities used during the initial installation and configuration of product
        - MMAdmin CLI (programming, migration and testing tools)
    - Depreciated product components
        - MetaMatrix Dimension Designer
        - MetaMatrix Reporter
        - adminshell (precursor to MMAdmin CLI)
5. Only out of the box capabilities were tested. No custom connectors, applications were included in the evaluation.
6. Cryptographic protection of communications with the TOE is not provided by the TOE, however a security objective on the IT Environment requires that the "IT Environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote users." This places the entire responsibility for protecting TOE communications on the buyers and necessitates careful network design and configurations. The evaluation team did verify that communication between these

components is encrypted. Testing confirmed the presence of encrypted communication. However, the cryptography used in this product was not analyzed or tested to conform to cryptographic standards during this evaluation.

The ST provides additional information on the assumptions made and the threats countered.

6. Architectural Information

The evaluated configuration of the TOE (MetaMatrix Enterprise) consists of the software components listed below. In the evaluated configuration, some components either do not provide any security functions, were/are being deprecated, and are used to customize connectors and applications and are therefore outside the scope of some assurance evaluation activities. Below is a detailed list of the components that are in and out of scope.

MetaMatrix Enterprise Release 5.5.3 (MetaMatrix) is a software-only product whose components are shown in the figure below.

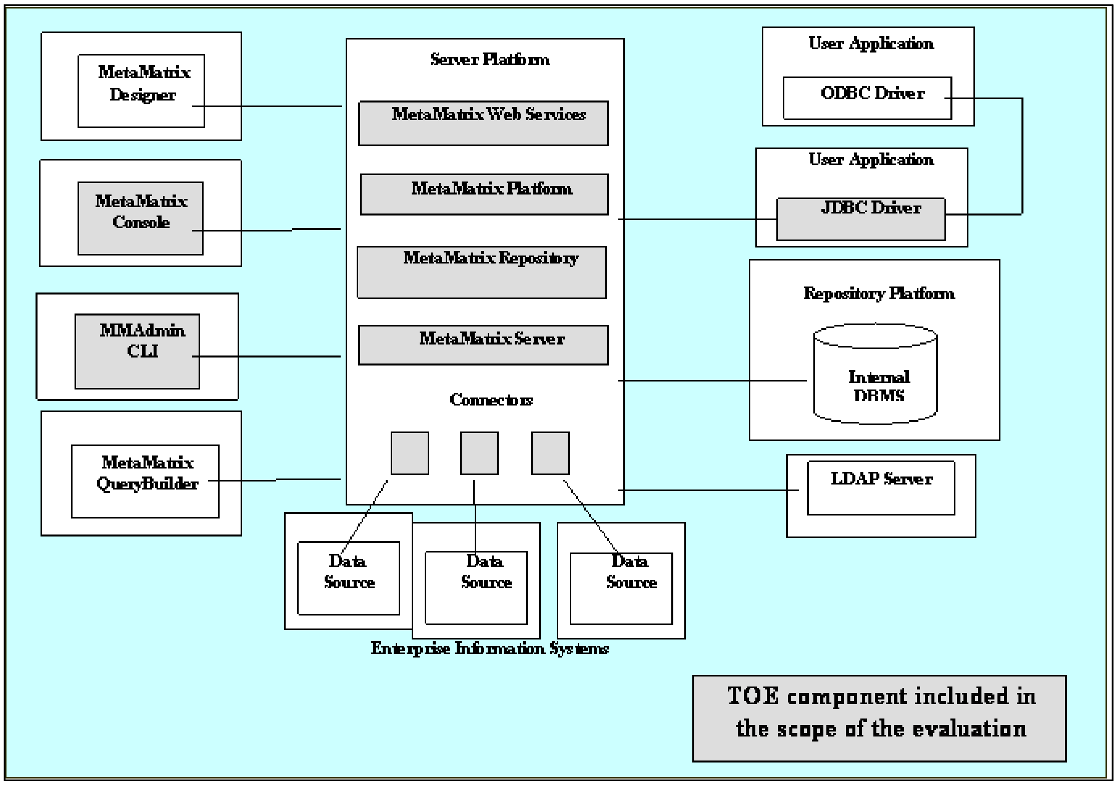

Figure 1. MetaMatrix components and TOE Boundary

MetaMatrix is an enterprise information integration (EII) system that manages and describes information across disparate enterprise information systems (EISs).

MetaMatrix has a federated data system that provides uniform access to all enterprise data sources using a variety of APIs. Information is accessed through the same standard APIs, regardless of whether the information is obtained from a single source or is consolidated from many sources, and regardless of whether the sources natively support the APIs. MetaMatrix provides access to information via SQL (or XQuery for XML), over JDBC, ODBC, SOAP/HTTP, or SOAP/JMS.

MetaMatrix enables end user applications to process queries that select (and update) data from one or more enterprise information sources, regardless of the native physical data storage method used by each enterprise information system. This means that a single query can access, reference, and return results from multiple integrated data sources.

Within MetaMatrix, the design-time components (including the MetaMatrix Enterprise Designer, and the MetaMatrix Repository), enable users to create and manage Metadata Models: representations describing the nature and content of enterprise information systems.

Once captured, this Metadata can be searched, analyzed, and applied by applications throughout the enterprise.

These Metadata Models can be deployed to the MetaMatrix Server (Server). The Server can then use the Metadata at runtime to:

- Process queries posed by a user application
- Retrieve data from information sources
- Return the integrated results in a useful information format

The MetaMatrix Server parses queries based upon the Metadata information and distributes the sub-queries to the appropriate EIS(s) through Connectors. These Connectors are Java classes that translate queries into the EIS's native application programming interface (API). Once the various EISs return the data results, the MetaMatrix Server reassembles and returns those results to the client application.

The MetaMatrix Enterprise Release 5.5.3 Product is comprised of the following software components:

- Design-Time Components:
    - MetaMatrix Repository
    - MetaMatrix Enterprise Designer
- Run-Time Components:
    - MetaMatrix Server
    - Connectors
    - MetaMatrix QueryBuilder
- Supporting Software Components:
    - MetaMatrix Platform
    - MetaMatrix Web Services
    - MetaMatrix ODBC and JDBC Drivers
- Management Components:
    - MetaMatrix Enterprise Console
    - MMAdmin Scripting Environment

The TOE relies on the following IT environment components to support the evaluated security functions:

- Server running Red Hat Enterprise Linux 5 to host the following product components:
  - MetaMatrix Server
  - MetaMatrix Metadata Repository
  - MetaMatrix Platform
  - MetaMatrix Web Services
  - Connectors
- Workstation running Windows XP to host the following product components:
  - MetaMatrix Enterprise Designer
  - MetaMatrix Enterprise Console
  - MetaMatrix QueryBuilder (running inside Internet Explorer)
- SSL Implementation (MetaMatrix uses the JSSE implementation in the Java Runtime Environment provided by the product installer, which is the Sun JRE version 1.5.0.11)
- Tomcat/Apache Web Services (version 5.0.25 is installed by the MetaMatrix product installer)
- Relational Database to implement MetaMatrix Metadata Repository:
  - Oracle 11g;
- JDBC Database Drivers
  - DataDirect Connect for JDBC version 3.7
- LDAP Server
  - Red Hat Directory Server 8
- Databases and applications used as data sources for testing

7. Documentation

CC Evaluation Evidence:

Note: Bolded documents are available for MetaMatrix customers.

Table 1. Evaluation Documentation and Evidence

Acronym	Document Title
FSP	MetaMatrix Enterprise Release 5.5.3 Common Criteria EAL 2 Functional Specification v 0.2, April 24, 2009
ARC	MetaMatrix Enterprise Release 5.5.3 TOE Security Architecture Version 0.1, April 10, 2009
TDS	MetaMatrix Enterprise Release 5.5.3 TOE Design Version 0.2, April 24, 2009
AGD (OPE)	**MetaMatrix Enterprise Administration Guide, MetaMatrix Products, Release 5.5.3, October 2008** **MetaMatrix Enterprise Installation Guide, MetaMatrix Products, Release 5.5.3, October 2008** **MetaMatrix Enterprise Designer User's Guide, MetaMatrix Products, Release 5.5.3, October 2008** **MetaMatrix Enterprise Console User's Guide, MetaMatrix Products, Release 5.5.3, October 2008** **MetaMatrix Enterprise QueryBuilder User's Guide, MetaMatrix Products, Release 5.5.3, October 2008** **MetaMatrix Enterprise SSL Guide, MetaMatrix Products, Release 5.5.3, Rev A. May 2009**
AGD (PRE)	MetaMatrix Enterprise Release 5.5.3 Preparative Procedures Version 1.0, April 23, 2009 **MetaMatrix Enterprise Release 5.5.3 Common Criteria Supplement to the Administrative Guidance Version 1.0, May 8, 2009**
CMC	MetaMatrix Enterprise Release 5.5.3 Configuration Management Procedures Version 0.2, May 21, 2009
CMS	MetaMatrix 5.5.3 Files Under Version Control (CVS and SVN)
DEL	MetaMatrix Enterprise Release 5.5.3 Delivery Procedures Version 0.2, April 17, 2009
COV	MetaMatrix Enterprise Release 5.5.3 Common Criteria EAL 2 Functional Specification, Version 0.3, 22 May, 2009 MetaMatrix Enterprise Release 5.5.3 Common Criteria EAL 2 Evidence of Test Coverage supporting doc, Version 0.3, 22 May, 2009
FUN	ATE_FUN_MM-Testing_23-03-2009.zip
IND	Evaluation Team Plan for MetaMatrix Enterprise Release 5.5.3, V.0.2B Test Report for MetaMatrix Enterprise Release 5.5.3, V.1.2

Acronym	Document Title
VAN	Searching for publicly known vulnerabilities applicable on MetaMatrix Enterprise Release 5.5.3, V.1 Evaluation Team Plan for MetaMatrix Enterprise Release 5.5.3, V.0.2B Test Report for MetaMatrix Enterprise Release 5.5.3, V.1.2
Other Documents	
	MetaMatrix Administration Shell Users Guide, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix Connector Developer's Guide, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix Custom Scalar Functions Tutorial, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix Enterprise 5.5.3 – README, MetaMatrix Enterprise Server, Release 5.5.3, Build 3126, October 15, 2008
	MetaMatrix Enterprise Client Developer's Guide, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix Enterprise Data Caching, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix Enterprise Server Tuning Guide, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix Enterprise XQuery Guide, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix Feature Overview and Value Proposition, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix Guide to the Design Time Catalog, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix JDBC Connector Integration Guide, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix Known Issues, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix Membership Domain Guide, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix Metadata Repository User Guide, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix Oracle Spatial Connector Integration Guide, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix Release Notes, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix Server Security, User Authentication, and Authorization, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix Text File Connector Integration Guide, MetaMatrix Products, Release 5.5.3, October 2008

Acronym	Document Title
	MetaMatrix Web Services Guide, MetaMatrix Products, Release 5.5.3, October 2008
	MetaMatrix XML-Relational Connectors Reference Guide, MetaMatrix Products, Release 5.5.3, October 2008
	SQL Query Web Service User's Guide, MetaMatrix Products, Release 5.5.3, October 2008

8. IT Product Testing

This section describes the testing efforts of the vendor and the evaluation team.

8.1. Developer Testing

The test approach consisted of manual tests that were grouped together under the TOE component being tested. The tests were designed to cover all of the security functions as described in the SFR and TSS section of the ST.

The test plan and procedures did not cover every possible combination of parameters for a given interface or every possible combination of parameters for a given security function. However, the test plan and procedures did stimulate every external interface and all of the security functions.

The individual tests were performed and the results were collected and verified by the developer. The results were archived, recorded, and sent to the evaluator for review.

The vendor's testing purposefully intended to cover all the security functions of Security Audit, Data Protection, Identification and Authentication, Security Management as defined in Section 6 of the ST.

The evaluator determined that the developer's approach to testing the TSFs was adequate for an EAL2 evaluation.

8.2. Evaluator Independent Testing

The test approach consisted of providing full coverage of all the TOE's security functions between the developer tests and team-defined functional tests as required under EAL 2. The tests reran a subset of the of the vendor's tests. In addition, the evaluation team developed a set of independent team tests to address areas of the ST that did not seem completely addressed by the vendor's test suite, or areas where the ST did not seem completely clear. All were run as manual tests and completed successfully.

Test Hardware

MetaMatrix provided the test setup for CygnaCom testing. The test setup was consistent with the available MetaMatrix test facilities.

Hardware consists of two workstations with Intel P4 CPU, 2.66 GHz, 2 GB internal RAM, 2 disk drives (20 GB & 40 GB) to install the MM server and the client.

An addition attacking computer (CygnaCom) is been used during the testing for the penetration tests.

Software

The following software testing tools were used for testing the TOE:

Software on the **Server machine:**

- Operating System
    - RHEL 5.1,
- Tomcat/Apache Web Services (version 5.0.25 is installed by the MetaMatrix product installer)
- Relational Database to implement MetaMatrix Metadata Repository:
    - Oracle 11g;
- JDBC Database Drivers
    - DataDirect Connect for JDBC version 3.7
- LDAP Server
    - Red Hat Directory Server 8
- MetaMatrix Metadata Repository
- MetaMatrix Supporting Software
    - MetaMatrix Platform
    - MetaMatrix Web Services
    - MetaMatrix ODBC and JDBC Drivers
- 2-way SSL implementation in the server side (MetaMatrix uses the JSSE implementation in the Java Runtime Environment provided by the product installer, which is the Sun JRE version 1.5.0.11)

Software on the **client machine:**

- OS -Windows XP SP3 with a all the updates (up the testing date)
- 2-way SSL implementation in the client side
- MetaMatrix product components:
    - MetaMatrix Enterprise Designer
    - MetaMatrix Enterprise Console
    - MetaMatrix QueryBuilder (running inside Internet Explorer)

Software tools used for testing:

- Internet Explorer
- Nmap
- Nessus

All tools were available at MetaMatrix facility.

8.3. Strategy for Devising Test Subset (Developer and Team Defined Tests)

The tests were manual using mmadmin (in server and client) and console (in the client side) interfaces. For each tests a unique test name was used and for every tests several screenshots were taken showing the options selected during the test and its results.

Mmadmin was tested using BeanShell scripts (scripting shell for Java). These scripts were provided to the evaluator and archived with the evaluation evidence.

The Logfiles that were generated from running the tests, were used for verification and validation of the tests.

Tests were designed to stimulate the Console, MMAdmin, Client, and Webserver TSFIs.

8.4. Coverage Provided by Devised Test Subset

The evaluator ensured that the test sample sufficient tests such that:

- All Security Functions were tested
- All External interfaces were exercised
- All Security Functional Requirements were tested.

The environment and configuration for the team-defined testing has been previously described. A distributed environment was selected to be able to test all of the functionality as described in the ST. This product can be installed in a number of configurations, including all on one machine.

The independent testing purposefully (directly) covered all of the security functions of, Audit, Data Protection, Identification and Authentication, Security Management as defined in Section 6 of the ST.

The evaluation team executed a set of the developer tests, all the additional team tests and penetration tests described in the test plan. The **MetaMatrix Enterprise Release 5.5.3** successfully passed security testing. However, as a result of testing updates to the code, CC Supplement Guide, ST, and SSL Guide were made. No obvious vulnerabilities were found.

9. Evaluated Configuration

The Evaluated Configuration (consistent with the ST):

- MetaMatrix Enterprise Release 5.5.3. The r553_090507_0021.jar patch must be applied to the MetaMatrix server system.
- Hardware consists of two workstations with Intel P4 CPU, 2.66 GHz, 2 GB internal RAM, 2 disk drives (20 GB & 40 GB) to install the MM server and the client.

10. Results of Evaluation

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 version 3.1 R2 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL.

Below lists the assurance requirements the TOE was required to be evaluated and pass at Evaluation Assurance Level 2. The following components are taken from CC part 3. The components in the following section have no dependencies unless otherwise noted.

- ADV_ARC.1 Security architecture description
- ADV_FSP.2 Security-enforcing functional specification
- ADV_TDS.1 Basic design
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ALC_CMC.2 Use of a CM system
- ALC_CMS.2 Parts of the TOE CM coverage
- ALC_DEL.1 Delivery procedures
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.2 Security objectives
- ASE_REQ.2 Derived security requirements
- ASE_SPD.1 Security problem definition
- ASE_TSS.1 TOE summary specification
- ATE_COV.1 Evidence of coverage
- ATE_FUN.1 Functional testing
- ATE_IND.2 Independent testing – sample
- AVA_VAN.2 Vulnerability analysis

The evaluators concluded that the overall evaluation result for the target of evaluation is Pass. The evaluation team reached pass verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

- The TOE is CC Part 2 Extended
- The TOE is CC Part 3 Conformant.

The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

11. Validators Comments/Recommendations

The validation team observed that the evaluation was performed in accordance with the CC, the CEM, and CCEVS practices. The Validation team agrees that the CCTL presented appropriate rationales to support the Results presented in Section 4 ETR Volume 1 (ST) and Section 5 ETR Volume 2 (TOE).

The validation team, therefore, recommends that the evaluation and Pass result for the identified TOE be accepted.

12. Security Target

The Security Target is identified as MetaMatrix Enterprise Release 5.5.3 Security Target, Version 1.5, July 10, 2009

13. Glossary

The following is an acronym list used within this validation report other evaluation evidence such as the ST.

ACI	Access Control Item
API	Application Programming Interface
CC	Common Criteria [for IT Security Evaluation]
CDK	Connector Development Kit
CLI	Command Line Interface
DBMS	Data Base Management System
EAL	Evaluation Assurance Level
EII	Enterprise Information Integration
EIS	Enterprise Information Systems
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
IT	Information Technology
JDBC	Java Database Connectivity
MMR	MetaMatrix Metadata Repository
ODBC	Open Database Connectivity
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
UML	Unified Modeling Language
VDB	Virtual Database
XA	eXtended Architecture
XML	Extensible Markup Language

14. Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).
- CygnaCom Solutions CCTL (http://www.cygnacom.com).
- MetaMatrix Inc. (http://www.redhat.com/metamatrix).

CCEVS Documents

- [CC] Common Criteria for Information Technology Security Evaluation, Version 3.1 R2, September 2007.
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 R2, September 2007.
- Other Documents
- [ST] MetaMatrix Enterprise Release 5.5.3 Security Target, Version 1.5, July 10, 2009.