National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

MarkLogic Server Enterprise Edition Version 4.0

Report Number: CCEVS-VR-VID10306-2010
Dated: 15 July 2010
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 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
Ken Eggers

Common Criteria Testing Laboratory

Terrie Diaz, Lead Evaluator
Science Applications International Corporation (SAIC)
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the MarkLogic Server Enterprise Edition Version 4.0.

The Validation Report presents the evaluation results, their 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.

The evaluation of MarkLogic Server Enterprise Edition Version 4.0 was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed on 7 July 2010.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and Team Test Report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 3 augmented with ALC_FLR.3. In addition, the ST is compliant with the U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2, July 25, 2007 (DBMS PP). All security functional requirements are derived from the DBMS PP and Part 2 of the Common Criteria.

The assurance requirements in the DBMS PP are the CC v3.1 Part 3 requirements for EAL 2 augmented with ALC_FLR.2. The assurance requirements in the ST are the CC v3.1, Release 2, Part 3 EAL 3 requirements augmented with ALC_FLR.3. The assurance requirements in the ST are conformant to the DBMS PP, in that they meet or exceed those requirements.

MarkLogic pursued a more rigorous assurance level because the TOE is a commercial product whose users require a moderate to high level of independently assured security. The TOE is targeted at a relatively benign environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have little attack potential. As such, EAL3 is appropriate to provide the assurance necessary to counter the limited potential for attack.

The TOE is MarkLogic Server Enterprise Edition Version 4.0 provided by Mark Logic Corporation. MarkLogic Server Enterprise Edition Version 4.0 is an enterprise-class database or “contentbase” that provides a set of services used to build both content and search applications which query, manipulate and render XML content.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

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

2 Identification

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

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

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

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant; and
- 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:	MarkLogic Server Enterprise Edition Version 4.0
Protection Profile	U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2, July 25, 2007
ST:	MarkLogic Server Enterprise Edition Version 4.0 Security Target, Version 1.0, June 29, 2010
Evaluation Technical Report	Evaluation Technical Report for MarkLogic Server Enterprise Edition Version 4.0, Part 1 (Non-Proprietary), Version 2.0, 29 June 2010, Part 2 (Proprietary), Version 3.0, 24 June 2010.

Item	Identifier
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007
Conformance Result	CC Part 2 extended and Part 3 conformant, EAL 3 augmented with ALC_FLR.3
Sponsor	Mark Logic Corporation
Developer	Mark Logic Corporation
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation (SAIC), Columbia, MD
CCEVS Validators	Kenneth Eggers, Orion Security Solutions, Inc. Paul Bicknell, The MITRE Corporation

3 TOE Overview

The MarkLogic Server TOE is built with a blend of search engine and database architecture approaches specifically designed to index and retrieve XML content. The TOE's native data format is XML, which is accepted directly, while content in other formats can be converted to an XML representation or stored in their original binary or text formats when loaded into the server. As an XML content server, the TOE manages its own content repository and is accessed using the W3C standard XQuery language, just as a relational database is a specialized server that manages its own repository and is accessed through Structured Query Language (SQL).

The TOE is fully transactional, runs in a distributed environment and can scale to terabytes of indexed content. It is schema independent and all loaded documents can be immediately queried without normalizing the data in advance. Like a relational database, it provides developers with the functionality and programmability to build content-centric applications using XQuery as its query language. Developers use XQuery both to search the content and to develop applications. It is possible to create entire applications programmed entirely in XQuery using only MarkLogic Server.

The security management functions of the TOE are performed via the Admin Interface, which is a web based browser GUI implemented as a MarkLogic Server web application. This interface allows authorized administrators to manage audit events, user accounts, access control and TOE sessions. It also provides the ability to control the creation, management, and configuration of databases, forests, servers, and hosts. Documents are stored in forests. The term "forest" comes from the fact that XML documents are tree structures and a collection of trees is a forest. A database is a collection of one or more forests. Databases are logical units against which you can assign HTTP and XDBC servers

and set various runtime configuration options. A host is a single instance of MarkLogic Server running on a single machine. Databases exist as a logical abstraction because in a distributed environment it can be useful to have a single logical database spread across multiple hosts, such as one host with two forests and another with three forests.

4 Assumptions, Threats, and Organizational Security Policies

The statement of TOE security environment describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be employed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product and defines the threats that the product is designed to counter.

The assumptions, threats and organizational security policies are taken directly from the DBMS PP. With the exception of two additional threats, T.PRIV and T.OPS, and two additional assumptions, A.ADMIN and A.AUTH, there are no modifications to the security environment of the PP.

4.1 Assumptions

Following are the assumptions identified in the Security Target:

- It is assumed the Admin Interface application runs on Port 8001 behind a firewall which is configured to block egress and ingress of traffic over Port 8001.
- It is assumed passwords are encrypted during the authentication process.
- It is assumed Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
- It is assumed there are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration and support of the DBMS.
- It is assumed the underlying OS has been validated against an NSA sponsored OS PP of at least Basic Robustness.
- It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

4.2 Threats

Following are the threats levied against the TOE and its environment as identified in the Security Target. The threats that are identified are mitigated by the TOE and its environment. All of the threats identified in the ST are addressed.

- An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

- A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
- An unauthorized process or application may gain access to the TOE security functions and data, inappropriately changing the configuration data for the TOE security functions.
- Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
- Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
- Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being discovered thereby causing potential security vulnerabilities.
- An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data, inappropriately changing the configuration data for TOE security functions.
- A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
- A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted).
- A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.
- Failure of the authorized administrator to identify and act upon unauthorized actions may occur.

4.3 Organizational Security Policies

In addition to the threats, the following organizational security policies are identified in the Security Target.

- The authorized users of the TOE shall be held accountable for their actions within the TOE.
- The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

5 Clarification of Scope

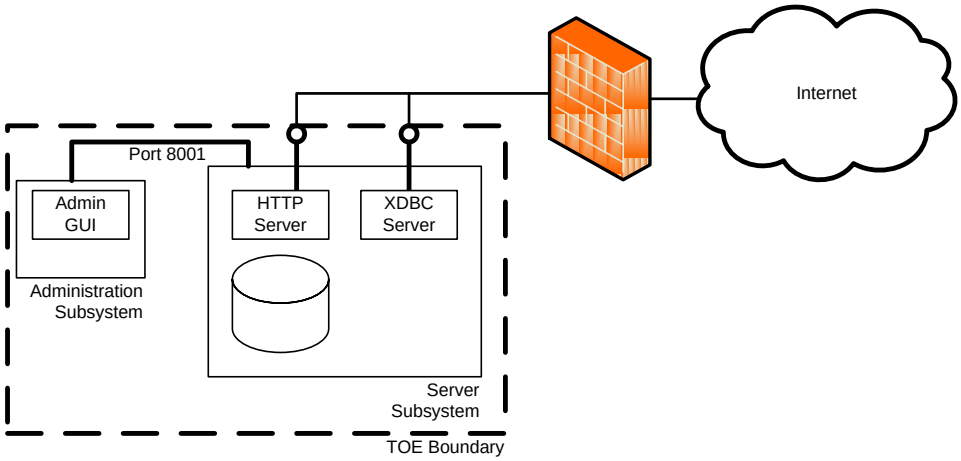
All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 3 extended in this case).
- As with all EAL 3 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.
- Cryptographic protection of passwords is used by the TOE; however, the cryptography used in this product was not analyzed or tested to conform to cryptographic standards during this evaluation.

6 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target.

The TOE consists of two subsystems, the Administration subsystem and the Server subsystem, as shown in the TOE Architecture diagram below.



TOE Architecture

6.1 Administration Subsystem

The Administration subsystem provides the Admin Interface to the Server subsystem. The Admin Interface application manages all features of the Server subsystem. It is composed of XQuery programs that are evaluated inside of an HTTP server. The HTTP server evaluates each request and sends a response back as a web page to the requester. The Admin Interface runs on Port 8001 behind a firewall that is configured to block egress and ingress of traffic over Port 8001.

6.2 Server Subsystem

The Server subsystem provides the software applications, network/application programming interfaces (APIs) and a database or contentbase.

The network/programmatic interfaces (HTTP and XDBC) are used by developers in a system that requires access to a backend XML content store.

The TOE can be set up as a single instance of MarkLogic Server on a single machine or it can support large scale high-performance architectures through multi-host distributed architectures. The following terminology has been defined for consideration in a TOE distributed environment:

- Cluster – A cluster is a set of one or more instances (see hosts, below) of MarkLogic Server (i.e., the TOE's Server subsystem) that will work together as a unified whole to provide content services. Security management functions of the TOE are performed from the Administration subsystem by connecting to any cluster host.
- Host – A host is a single instance of MarkLogic Server running on a single machine. Even though each host in a cluster can be configured to perform a different task, the full MarkLogic Server software (Server subsystem) runs on each host. MarkLogic Server Standard Edition can only be configured to run in a single-host configuration. MarkLogic Server Enterprise Edition enables multi-host configurations.
- Cluster Management Group – A cluster management group is a set of hosts with uniform HTTP and XDBC server configurations (but not necessarily uniform forest configurations). Cluster Management Groups are used to simplify cluster management.
- Forest – A forest is a repository for documents. Each forest is managed by a single host. The mapping of which forest is managed by which host is transparent to queries, as queries are processed against databases, not forests.
- Database – A database is a set of one or more forests that appears as a single contiguous set of content for query purposes. Each forest in a database must be configured consistently. HTTP and XDBC servers evaluate queries against a single database. In addition to databases created by the administrator for user content, MarkLogic Server maintains databases for administrative purposes: security databases, which contain user authentication and permissions information; schema databases, which are used to store schemas used by the system; modules databases, which are used to store executable XQuery code; last-login databases, which are used to store session history and data and triggers databases, used to store trigger definitions.

7 Security Policy

The TOE logically supports the following security functions:

- Security Audit
- Identification and Authentication
- Security Management
- User Data Protection
- Protection of the TSF
- TOE Access

7.1 Security audit

The TOE generates audit records that include date and time of the event, subject identity and outcome for security events. The TOE provides authorized administrators with the ability to include and exclude auditable events based on group identity, event type, object identity and success and failure of auditable security events. When appropriate, the TOE also associates audit events with the identity of the user that caused the event. The IT environment stores the audit records and also provides the system clock information that is used by the TOE to timestamp each audit record.

7.2 User data protection

The TOE enforces a Discretionary Access Control (DAC) policy that restricts access to DBMS-controlled object(s). Users of the TOE are identified and authenticated by the TOE before any access to the system is granted. Once access to the system is granted, authorization provides the mechanism to control what functions a user is allowed to perform based on the user's group membership. Access to all DBMS-controlled objects is denied unless access, based on group membership, is explicitly allowed. The authorized administrator role shall be able to bypass the DAC policy. The TOE also provides amplifications or "amps" which temporarily grant roles to a user only for the execution of a specific function. Therefore, the DAC policy can also be bypassed by a user who is temporarily granted the authorized administrator role in order to perform a specific "amped" function. The TOE also ensures that any previous information content of a resource is made unavailable upon the allocation of the resource to an object. Memory or disk space is only allocated when the size of the new data is first known, so that all previous data is overwritten by the new data.

7.3 Identification and authentication

The TOE requires users to provide unique identification and authentication data before any access to the system is granted and further restricts access to DBMS-controlled objects based on group membership. The TOE maintains the following security attributes belonging to individual users: group membership, security-relevant database role and password. The TOE uses these attributes to determine access.

7.4 Security management

The security functions of the TOE are managed by authorized administrators via the web based Admin Interface. The TOE defines the security role of 'authorized administrator.' Authorized administrators perform all security functions of the TOE including managing audit events, user accounts, access control and TOE sessions.

7.5 Protection of the TSF

The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate and have the appropriate permissions before any administrative operations or access to TOE data and resources can be performed on the system. The TOE also maintains a security domain that protects it from interference and tampering by untrusted subjects within the TOE scope of control. Additionally, the TOE ensures that TSF data is consistent between parts of the TOE with a mechanism that brings inconsistent data into a consistent state.

7.6 TOE access

The TOE restricts the maximum number of concurrent sessions that belong to the same user by enforcing an administrator configurable number of sessions per user. The TOE also denies session establishment based on attributes that can be set explicitly by authorized administrators including group identity, time of day and day of week. Upon successful session establishment, the TOE stores and retrieves the date and time of the last successful session establishment to the user. It also stores and retrieves the date and time of the last unsuccessful session establishment and the number of unsuccessful attempts since the last successful session establishment.

8 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

8.1 Design documentation

Document	Version	Date
MarkLogic Server Enterprise Edition 4.0 Security Architecture	ARC_0.5	August 2009
MarkLogic Server Enterprise Edition 4.0 Functional Specification	FSP_0.8	October 2009
MarkLogic Server Enterprise Edition 4.0 Technical Design Document	TDS_0.3	August 2008

8.2 Guidance documentation

Document	Version	Date
MarkLogic Server Administrator's Guide	Release 4	September 2008
MarkLogic Server Understanding And Using Security	Release 4.0	September 2008

MarkLogic Server Developer's Guide	Release 4.0	September 2008
MarkLogic Common Criteria Evaluated Configuration Guide Last Revised: 4.0-8, April, 2010	Release 4.0	September 2009

8.3 Lifecycle documentation

Document	Version	Date
MarkLogic Server Enterprise Edition 4.0 Configuration Management	ALC-0.3	June 2009
MarkLogic Server Enterprise Edition 4.0 Life Cycle Document	LCD_0.2	June 2009
MarkLogic Server Enterprise Edition 4.0 Lifecycle Management: Development Security	ALC_DVS-0.2	June 2009
MarkLogic Enterprise Edition 4.0 Delivery Procedures	DP_0.4	January 2010
MarkLogic Enterprise Edition 4.0 Flaw Remediation Procedures	FLR_0.6	January 2010

8.4 Test documentation

Document	Version	Date
MarkLogic Server Enterprise Edition 4.0 Test Design	ATE-0.1	December 2008
MarkLogic Server Enterprise Edition 4.0 Functional Test Plan	ATE_FUN-0.69	May 2010

Actual results in the form of list files, key files, XML files, text files, and JAVA files

8.5 Security Target

Document	Version	Date
MarkLogic Server Enterprise Edition 4.0 Security Target	Version 1.0	June 29, 2010

9 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

9.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function, more specifically to the security functional requirements tested. The scope of the developer tests included all the TSFI. The testing covered the security functional requirements in the ST including: Security Audit, Identification and Authentication, Security Management, User Data Protection, Protection of the TSF, and TOE Access. All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

9.2 Evaluation Team Independent Testing

The evaluation team exercised the entire automated test suite and a subset of the vendor's manual test suite. The following describes the testing environment of the TOE diagramed below:

- All the computing resources are behind a firewall so only authorized and authenticated machines have access to the HTTP, XDBC, or the Admin interfaces of the TOE.
- MarkLogic Server is installed on either a Red Hat or Solaris server.
- The HTTP and XDBC interfaces are part of the MarkLogic Server binary and are available when MarkLogic Server is started.
- The QA Harness runs on the same Red Hat or Solaris server as MarkLogic Server.
- During testing, the QA Harness creates XDBC and HTTP application servers on the MarkLogic Server during testing.
- The Admin interface also runs on MarkLogic Server and is accessible through HTTP.
- The Windows XP workstation accesses the Admin interface through the web browser.

The evaluators generated keys using the putty Key generator. The public key was provided to the MarkLogic developer who installed the key on the server (TOE). The evaluators accessed the servers (TOE) remotely using getty secure connection (SSH Tunnel).

In addition to developer testing, the evaluation team conducted its own suite of tests, which were developed independently of the sponsor. These also completed successfully.

9.3 Vulnerability Testing

The evaluators developed vulnerability tests to address the Protection of the TSF security function, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

10 Evaluated Configuration

The TOE consists of the software applications and network protocol interfaces (described and shown in the diagram above). The Administration subsystem, which provides the Admin Interface, runs on Windows XP SP2 using Internet Explorer v.6.0 or higher. The Server subsystem applications and network interfaces execute either on Sun Solaris or Linux operating systems. The TOE requires the following hardware and operating system (OS) platforms in the IT environment:

Memory, Disk Space, and Swap Space Requirements
Before installing the software, the system must meet the following minimum requirements:

- 512 MB of system memory, minimum.
- Three times the disk space of the source content to be loaded.
- Swap space at least equal to the amount of physical memory on the machine.

Supported Platforms – Server Subsystem
The MarkLogic Server server subsystem is supported on the following platforms for the evaluated configuration:

- Sun Solaris 10 (64-bit SPARC)
- Sun Solaris 10 (x64)
- Red Hat Enterprise Linux 5.0 (x64)

Supported Platforms – Administration Subsystem
The MarkLogic Server administration subsystem is supported on the following platforms for the evaluated configuration:

- Microsoft Windows XP SP2.

The TOE relies on the hosting OS to protect its applications, processes, and any locally stored data. Web browsers in the IT environment are utilized to access the Admin Interface and the HTTP server. As noted previously, the TOE can be deployed on a single machine or in a distributed environment across multiple machines.

For specific configuration settings required in the evaluated configuration see MarkLogic Server Installation Guide for All Platforms, MarkLogic Server Administrator's Guide, MarkLogic Server Understanding and Using Security, and MarkLogic Common Criteria Evaluated Configuration Guide.

11 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 3.1, Revision 2, September 2007; the Common Evaluation Methodology (CEM), Version 3.1, Revision 2, September 2007; and all applicable International Interpretations in effect on February 2008. The evaluation confirmed that MarkLogic Server Enterprise Edition Version 4.0 product is compliant with the Common Criteria Version 3.1 Revision 2, functional requirements (Part 2), Part 2 extended, assurance requirements (Part 3) conformant for EAL3 augmented with ACL_FLR.3, and conformant with the U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2, July 25, 2007. The details of the evaluation are recorded in the CCTL's evaluation technical report; Final Evaluation Technical Report for the MarkLogic Server Enterprise Edition Version 4.0, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the MarkLogic Server Enterprise Edition Version 4.0 Security Target, Version 1.0, June 29, 2010.

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

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 sample of the suite of the vendor test, the evaluation team's independent tests and the vulnerability test, also demonstrated the accuracy of the claims in the ST.

12 Validator Comments/Recommendations

All Validator concerns with respect to the evaluation have been addressed. No issues are outstanding.

13 Security Target

The Security Target is identified MarkLogic Server Enterprise Edition 4.0 Security Target, Version 1.0, June 29, 2010. The document identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 3 augmented with ALC_FLR.3.

14 Glossary

The following definitions are used throughout this document:

API	Application Programming Interface
CC	Common Criteria

CEM	Common Evaluation Methodology
CCEVS	Common Criteria Evaluation and Validation Scheme
CIM	Consistency Instruction Manual for Development of U.S. Government Protection Profiles for use in Basic Robustness Environments
DAC	Discretionary Access Control
DBMS	Database Management System
DBMS PP	U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2, July, 25, 2007
DoD	Department of Defense
DoS	Denial of Service
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HLD	High-level Design
IA	Initial Assessment
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
PP	Protection Profile
SAIC	Science Applications International Corporation
SFP	Security Function Policy
SOF	Strength of Function
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
URI	Uniform Resource Identifier

US	United States
W3C	World Wide Web Consortium
XML	Extensible Markup Language

15 Glossary of Terms

The terminology below is described in order to clarify and distinguish the terms used in the Protection Profile, the ST and those used in the TOE product documentation.

Group - The DBMS PP specifies that the discretionary access control policy (DAC) is based on a user's identity and/or group membership. The term "group" as used in the DBMS PP is equivalent to the concept of "role" which is the terminology used by Mark Logic. Therefore, for purposes of this ST and consistency with DBMS PP terminology, the terms "group(s)" is used, but refers to the concept of "role" that is described in other TOE documentation and is defined below.

Role - In the DBMS PP, the term "role" is used to refer to the security relevant database roles that are defined for the TOE. For the MarkLogic TOE, one security relevant role, authorized administrator, has been identified. The MarkLogic TOE actually implements and enforces other user roles; however, these translate into "groups" and are discussed as such for purposes of this ST and consistency with the DBMS terminology. A role (i.e., group) is a named entity that provides authorization privileges and permissions to other roles (i.e., groups) or to users. Users, privileges, document permissions and other roles (i.e., groups) are all assigned to roles which are "groups" in this ST.

Note: Apart from the authorized administrator role defined in this ST, MarkLogic TOE user roles, shall, henceforth be referred to as groups.

Amps - Amps are security objects that temporarily grant group membership to unprivileged users only for the execution of a given function. While executing an "amped" function, the user is temporarily part of the amped group which in turn temporarily grants the user the additional privileges and permissions given by the groups configured in the amp. Amps enable the effect of the additional permissions and privileges to be limited to a particular function.

Permissions - Permissions provide a group with the ability to perform certain capabilities (i.e., read, insert, update, execute) on documents. Permissions are assigned to documents. Users gain the authority to perform these capabilities on a document if they are members of a group to which a permission is associated.

Capabilities - Permissions are a combination of group and a capability. Capabilities are: Read, Update, Insert or Execute.

Execute Privileges - Execute privileges allow developers to control authorization for the execution of an XQuery function. These privileges are assigned to a user through a group.

URI Privileges - Uniform Resource Identifier privileges are used to control the creation of documents with a given URI prefix. In order to create a document with a prefix that has a URI privilege associated with it, a user must be part of a group to which the needed URI privilege is assigned.

Application Server Privileges - Application Server Privileges are Execute Privileges that can be configured to control access to each application server (i.e., HTTP or XDBC server). If such a privilege is specified, any users that access the server must possess the specified privilege.

16 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 1, September 2006

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 2, September 2007

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 2, September 2007

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 2, September 2007.

[5] MarkLogic Server Enterprise Edition 4.0, Final Non-Proprietary ETR – Part 1, Version 2.0, 29 June 2010.

[6] MarkLogic Server Enterprise Edition 4.0, Final Proprietary ETR – Part 2, Version 3.0 dated 24 June 2010 and Supplemental Team Test Report, Version 3.0, 26 March 2010.

[7] MarkLogic Server Enterprise Edition 4.0 Security Target, Version 1.0, June 29, 2010.

[8] NIAP Common Criteria Evaluation and Validation Scheme Publication #4, Guidance to CCEVS Common Criteria Testing Laboratories, Version 2.0, September 8, 2008.