C069 Certification Report

MarkLogic Server 8.0-4

File name: ISCB-5-RPT-C069-CR-v1
Version: v1
Date of document: 22 December 2015
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
(726930-U)
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999
Corporate Office
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
www.cybersecurity.my

C069 Certification Report
MarkLogic Server 8.0-4

22 December 2015

ISCB Department

CyberSecurity Malaysia

Level 5, Sapura@Mines,
No 7 Jalan Tasik,The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 □Fax: +603 8992 6841
http://www.cybersecurity.my

Copyright Statement

Registered office:

Level 5, Sapura@Mines

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 22 December 2015, and the Security Target (Ref [20]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [18]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 4 (Ref [17]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (Ref [16]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	3 December 2015	All	Initial draft of certification report
v1	22 December 2015	All	Final version of certification report

Executive Summary

MarkLogic Server 8.0-4 is the Target of Evaluation (TOE) for the Evaluation Assurance Level 2 Augmented with ALC_FLR.3 Evaluation.

The TOE is MarkLogic Server 8.0-4, hereinafter referred to as MarkLogic Server. The TOE is an enterprise-class database that provides a set of services used to build content and search applications which query, manipulate and render Extensible MarkUp Language (XML) content.

The scope of evaluation covers major security features as follows:

a) Security Audit: The TOE generates audit records that include date and time of the event, subject identity and outcome for security events.

b) Cryptographic Support: The Transport Layer Security (TLS) protocol is used to provide protection of the communications surrounding the remote administrative sessions from disclosure and from undetected modification.

c) User Data Protection: The TOE enforces a Discretionary Access Control (DAC) policy which restricts access to TOE-controlled object(s). Users of the TOE are identified and authenticated by the TOE before any access to the system is granted.

d) Identification & 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 TOE-controlled objects based on role membership.

e) Security Management: The security functions of the TOE are managed by authorized administrators via the web-based Admin Interface, or application written using the Admin API, Security API, PKI API, and built-in admin functions.

f) 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.

g) 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 scope of the evaluation is defined by the Security Target (Ref[20]), which identifies assumptions made during the evaluation, the intended environment for the TOE, the security function requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2) Augmented with ALC_FLR.3. This report confirms that the evaluation was conducted in accordance with the relevant criteria and

the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [18]).

The evaluation was performed by BAE Systems Applied Intelligence MySEF (Malaysia Security Evaluation Facility) and completed on 13 November 2015.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that MarkLogic Server 8.0-4 meet their requirements. It is recommended that a potential user of MarkLogic Server 8.0-4 refer to the Security Target (Ref [20]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

1 Target of Evaluation

1.1 TOE Description

1 The 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 and XML is accepted in an 'as is' form, while content in other formats can be converted to an XML representation or stored as is (in binary or text formats) when loaded into the TOE. As an XML database, 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).

2 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. It provides developers with the functionality and programmability, using XQuery as its query language, to build content-centric applications. Developers build applications using XQuery both to search the content and as a programming language in which to develop applications. It is possible to create entire applications using only MarkLogic Server, and programmed entirely in XQuery. Applications can also be created using Java or other programming languages that access MarkLogic Server.

3 The details of the TOE functions can be found starting in section 2.1 of the Security Target (Ref [20]).

4 There are seven security functionalities covered under the scope of the evaluation which are:

Security Function	Description
Security Audit	The TOE generates audit records that include date and time of the event, subject identity and outcome for security events.
Cryptographic Support	The Transport Layer Security (TLS) protocol is used to provide protection of the communications surrounding the remote administrative sessions from disclosure and from undetected modification.
User Data Protection	The TOE enforces a Discretionary Access Control (DAC) policy which restricts access to TOE-controlled object(s). Users of the TOE are identified and authenticated by the TOE before any access to the system is granted.
Identification & 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 TOE-controlled objects based on role membership.
Security Management	The security functions of the TOE are managed by authorized administrators via the web-based Admin Interface, or application written using the Admin API, Security API, PKI API, and built-in admin functions.

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.
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.

1.2 TOE Identification

5 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C069
TOE Name	MarkLogic Server
TOE Version	8.0-4
Security Target Title	MarkLogic Essential Enterprise 8 and MarkLogic Global Enterprise 8 Security Target
Security Target Version	0.5
Security Target Date	9 October 2015
Assurance Level	Evaluation Assurance Level 2 Augmented with ALC_FLR.3
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [16])
Methodology	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [17])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL 2 Augmented (ALC_FLR.3
Sponsor and Developer	MarkLogic Corporation 999 Skyway Road Suite 200 San Carlos, CA 94070
Evaluation Facility	BAE Systems Applied Intelligence MySEF

1.3 Security Policy

6 There are no organisational security policies that have been defined regarding the use of the TOE.

1.4 TOE Architecture

7 The TOE includes both logical and physical boundaries, which are described in Section 2.2 of the Security Target (Ref [20]).

8 The TOE consists of two subsystems, the Administration subsystem and the Server 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 which 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 is accessed through HTTPS only (i.e., HTTP over TLS).

9 The following figure 1 shows the evaluated configuration that comprise the TOE:

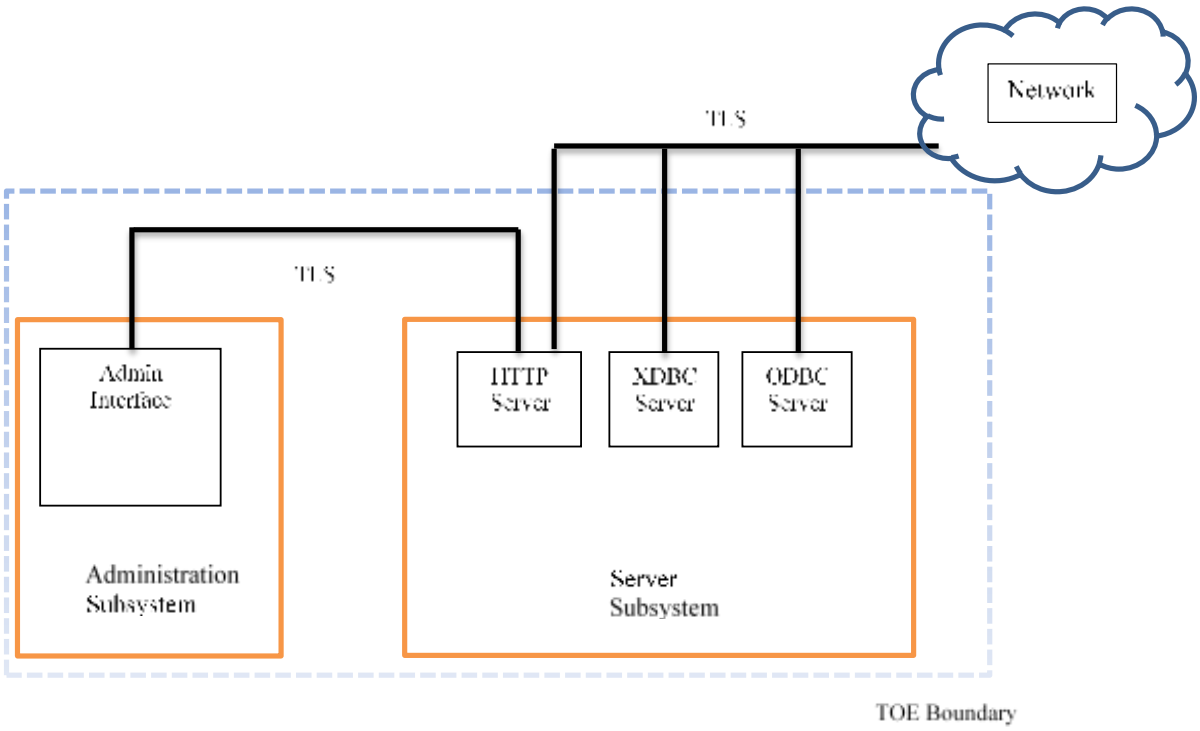

Figure 1 – TOE Architecture

10 The TOE supports three interfaces that are available through a network. An HTTP server offers connectivity for the administrative interface and for customer applications with the Server subsystem. The communication pathways to and from the Server subsystem are depicted in Figure 1 by the lines labelled as “TLS”. Two additional programmatic interfaces are provided by XDBC and ODBC protocols that can also use TLS to protect the session. Developers write client applications to use

these interfaces in a system that requires access to a backend XML database. In particular, the HTTP and XDBC servers each provide the Admin API, Security API, and PKI API, which are collections of XQuery functions. The API functions are evaluated inside the HTTP and XDBC servers. Consequently, the servers enforce TOE security policy (for example, authentication, security management restrictions, access control, and auditing). The ODBC server provides read-only access to SQL views that are defined in the context database for that App Server, and is authenticated and authorized based on DAC policy.

11 The TOE includes REST APIs, a Java Client API, and XCC libraries. These libraries are for application development. They do not provide any security functionality. The REST APIs are implemented as XQuery programs that run on an HTTP server. The Java Client API is implemented in Java, and calls the REST APIs, which in turn run on an HTTP server. The HTTP server is an interface to the TOE that honors DAC policy. The XCC libraries run against an XDBC server, which is also an interface to the TOE that honors DAC policy.

1.4.1 Logical Boundaries

12 The scope of the evaluation was limited to those claims made in the Security Target (Ref [20]) and includes only the following evaluated security functionality:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification & Authentication
- Security Management
- Protection of the TSF
- TOE Access

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 user identity, role, 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 TOE relies on the operational environment for secure storage of the audit records and for system clock information that is used by the TOE to timestamp each audit record.

Cryptographic Support: The Transport Layer Security (TLS) protocol is used to provide protection of the communications surrounding the remote administrative sessions from disclosure and from undetected modification. The TOE supports TLS v1.0, v1.1, and v1.2. For communication between a customer application on a network and the HTTP server, XDBC server, or ODBC server of the TOE, the TOE offers the use of a TLS session to protect these communications. Finally, the TOE uses a TLS protected channel to distribute TSF data when it is transmitted between distributed parts of the TOE (that is, hosts within a cluster).

The TOE uses OpenSSL object module version 2.0 which has undergone a FIPS 140-2 certification (certificate #1747). The TOE includes an OpenSSL object module built without

modification from the source code of the OpenSSL FIPS certification. All references to "the TOE" performing cryptographic operations in this security target are indicating that the TOE is performing the operation through its use of the OpenSSL object module.

User Data Protection: The TOE enforces a Discretionary Access Control (DAC) policy which restricts access to TOE-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 role. Access to all TOE-controlled objects is denied unless access, based on role, is explicitly allowed. The authorized administrator role shall be able to access any object regardless of the object's permissions. 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 extended by a user who is temporarily granted the privileged 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.

Identification & 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 TOE-controlled objects based on role membership. The TOE maintains the following security attributes belonging to individual users: identities; role membership; and password. The TOE uses these attributes to determine access.

The TOE provides a password plug-in functionality that allows administrators to write custom code to require passwords to conform to specific rules (e.g., the number of characters, special characters, last change date).

Security Management: The security functions of the TOE are managed by authorized administrators via the web-based Admin Interface, or application written using the Admin API, Security API, PKI API, and built-in admin functions. The ST 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.

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.

Communication with remote administrators is protected by TLS, which protects against the disclosure and undetected modification of data exchanged between the TOE and the administrator. Communication with remote customer applications can also utilize TLS to protect against the disclosure and undetected modification of data exchanged between the TOE and the customer application. Customer applications must determine whether the use of TLS is necessary for that specific customer application's data.

The TOE ensures that TSF data is encrypted and remains consistent when transmitted between parts of the TOE. The TOE provides consistency of TSF data between distributed parts of the TOE by regularly monitoring the configuration file and security database for changes and distributing the updated configuration file or security database to all parts of the cluster. The TOE utilizes a TLS protected channel to distribute TSF data among a cluster.

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 role 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. This information is collected by the TOE Access security function, because the information pertains to user's attempts to access the TOE. The information gathered by the TOE pertains to historical session establishment actions by a user.

1.4.2 Physical Boundaries

13 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 using a supported browser, Firefox, Internet Explorer, or Chrome. The Server subsystem applications and network interfaces execute on a Linux operating system. The TOE requires the following hardware and OS platforms in its operational environment:

Memory, Disk Space, and Swap Space Requirements
The host system must meet the following minimum requirements:

- 512 MB of system memory, minimum. 2 GB or more recommended, depending on database size.
- 1.5 times the disk space of the total forest size. More specifically, each forest on a filesystem requires its filesystem to have at least 1.5 times the forest size in disk space (or, for each forest less than 32GB, 3 times the forest size).
- Swap space equal to the amount of physical memory on the machine.

Supported Platforms – Server Subsystem

The evaluated configuration of the TOE is supported on Red Hat Enterprise Linux 7 (x64). Note, the deadline I/O scheduler is required on Red Hat Linux platforms. The deadline scheduler is optimized to ensure efficient disk I/O for multi-threaded processes, and the TOE can have many simultaneous threads. In addition, the redhat-lsb, glibc (both the 32-bit and the 64-bit packages) and gdb packages are required.

Supported Platforms – Administration Subsystem

The Administration subsystem is supported on the following browsers in the evaluated configuration:

- Firefox on Windows and Mac OS
- Internet Explorer on Windows
- Chrome on Windows and Mac OS.

Other browser/platform combinations may work but are not as thoroughly tested by MarkLogic.

14 As noted previously, the TOE can be deployed on a single machine or in a distributed environment across multiple machines. In a distributed environment, the TOE is a

cluster of hosts as defined above. The hosts communicate using TLS to protect transmitted data from disclosure or undetected modification.

15 A customer application on the network can also communicate with the TOE's App Servers (HTTP, XDBC or ODBC). The TOE supports the use of TLS versions 1.0, 1.1 and 1.2. The TOE requires applications that use the Admin API, Security API, and PKI API to communicate with the HTTP App Server and XDBC App Server using TLS. Customer client applications are not part of the TOE.

1.5 Clarification of Scope

16 The TOE relies on the hosting OS to protect its applications, processes, and any locally stored data. The TOE itself maintains a security domain that protects it from interference and tampering by untrusted subjects within the TOE scope of control. Web browsers in the environment are used to access the Admin Interface and the HTTP server through its HTTPS interface, and to terminate a session. The Admin Interface prompts the user to authenticate with a valid username and password in order to log in for a session. As is standard in browser-based applications, the browser caches and automatically re-issues the login credentials for each request throughout the browser session. These credentials are valid until the browser is closed, which terminates the session. When the browser is restarted, the user will once again be prompted to authenticate with a valid username and password.

17 Section 1.4 of this document described the scope of the evaluation which was limited to those claims made in the Security Target (Ref [20]).

18 Potential consumers of the TOE are advised that some functions and services of the overall product have not have been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

19 This section summarises the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments that are required for secure operation of the TOE, which is defined in the Security Target (Ref [20]) section 3.1.

1.6.1 Usage assumptions

20 Assumption for the TOE usage as listed in Security Target :

a) TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

b) The web browsers used to access the Admin Interface perform correctly such that when the browser is closed, the active Admin session is terminated. Client applications used to access the Admin API, Security API, and PKI API will perform correctly and when the application is closed, the active Admin session will be terminated.

1.6.2 Environment assumptions

21 Assumptions for the TOE environment listed in Security Target are:

a) The OS in the environment shall be able to provide reliable time stamps for use by the TOE.

b) Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

1.7 Evaluated Configuration

22 The evaluated configuration is described in details (see Figure 1) as described in Section 2.3 of the Security Target (Ref [20]).

1.8 Delivery Procedures

23 The delivery process for the TOE is provided in Section 4.0 of Delivery documentation (Ref [11])

1.9 Documentation

24 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage of the product.

25 The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product:

[1] MarkLogic Essential Enterprise 8 and MarkLogic Global Enterprise 8 Security Target, Version 0.5, 9 October 2015

[2] MarkLogic Server 8 Security Architecture (ADV_ARC), Version 0.1, 21 August 2015

[3] MarkLogic Server 8 Functional Specification (ADV_FSP), Version 0.2, 2 November 2015

[4] MarkLogic Server 8 Basic Design (ADV_TDS), Version 0.2, 2 November 2015

[5] MarkLogic Server 8 Security Architecture (ADV_ARC), Version 0.1, 21 August 2015

[6] MarkLogic Server Administrator's Guide, February 2015, Last Revised: 8.0-3, June 2015

[7] MarkLogic Server Understanding and Using Security, February 2015, Last Revised: 8.0-1, February 2015

[8] MarkLogic Common Criteria Evaluated Configuration Guide, October 2015, Last Revised: 8.0-4, October 2015

[9] MarkLogic Server Installation Guide for All Platforms, February 2015, Last Revised: 8.0-3, June 2015

[10] MarkLogic Server 8 Configuration Management, Version 0.5, 3 November 2015

[11] MarkLogic Server 8 Delivery Procedures, Version 0.2, 11 September 2015

[12] MarkLogic Server 8 Flaw Remediation Procedures, Version 0.2, 11 September 2015

[13] MarkLogic Server 8 Functional Test Plan, Version 1.0, 28 September 2015

[14] MarkLogic Server 8.0 Test Design, Version 1.0, 28 September 2015

2 Evaluation

26 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [16]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [17]). The evaluation was conducted at Evaluation Assurance Level 2+ (EAL2+) Augmented ALC_FLR.3. The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [18]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [19]).

2.1 Evaluation Analysis Activities

27 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

2.1.1.1 Configuration Management Capability:

a) The evaluators confirmed that the TOE provided for evaluation is labelled with its reference.

b) The evaluators confirmed that the TOE references used are consistent.

c) The evaluators examined the method of identifying configuration items and determined that it describes how configuration items are uniquely identified.

d) The evaluators examined the configuration items in the configuration item list and determined that they are identified in a way that is consistent with the CM documentation. The application of the CM systems was examined during the site visits at MarkLogic Corporation HQ (999 Skyway Road, Suite 200 San Carlos, CA, 94070, United States of America) and the evaluators confirmed that the CI List was consistent with the provided evidence.

2.1.1.2 Configuration Management Scope:

The evaluators confirmed that the configuration list includes the following set of items:

a) the TOE itself;

b) the parts that comprise the TOE;

c) the TOE implementation representation; and

d) the evaluation evidence required by the SARs in the ST.

The evaluators confirmed that the configuration list uniquely identifies each configuration item.

The evaluators confirmed that the configuration list indicates the developer of each TSF relevant configuration item.

2.1.2 Development

28 The evaluators examined the security architecture description and determined that the information provided in the evidence is presented at a level of detail

commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

29 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities.

30 The evaluators examined the TOE design (Ref. [4]) and determined that the structure of the entire TOE is described in terms of subsystems. The evaluators also determined that all subsystems of the TSF are identified. The evaluators determined that interactions between the subsystems of the TSF were described.

31 The evaluators examined the TOE and determined that each SFR-non interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is SFR-non interfering.

32 The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

33 The evaluators examined the TOE design and determined that it provided a complete and accurate high-level description of the SFR-supporting and SFR-non interfering behaviour of the SFR-enforcing subsystems. The evaluators determined that the TOE design provided a complete and accurate high-level description of the behaviour of the SFR-supporting subsystems.

34 The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

35 The evaluators determined that all Security Target SFRs were covered by the TOE design, and concluded that the TOE design was an accurate instantiation of all SFRs.

2.1.3 Guidance documents

2.1.3.1 Operating Guidance:

36 The evaluators examined the operational user guidance and determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

37 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

38 The evaluators examined the operational user guidance (in conjunction with other evaluation evidence) and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

39 The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

40 The evaluators found that the operational user guidance is clear and reasonable.

2.1.3.2 Preparation Guidance:

41 The evaluators examined the provided delivery acceptance and determined that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

42 The evaluators determined that the provided installation procedures describe the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST.

43 The evaluators performed all user procedures necessary to prepare the TOE during testing and determined that the TOE and its operational environment can be prepared securely using only the supplied preparative user guidance.

2.1.4 IT Product Testing

44 Testing at EAL2+ Augmented ALC_FLR.3 consists of assessing developer tests, perform independent function test, and perform penetration tests. The TOE testing was conducted by evaluators from BAE Systems Applied Intelligence MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Assessment of Developer Tests

45 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [21]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

46 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

47 At EAL2+ Augmented ALC_FLR.3, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing sample of the developer's test plan, and creating test cases that augmented developer tests.

48 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The evaluators confirmed that the developer supplied test documentation includes test plans, expected test results and actual test results. The result of the independent functional tests were developed and performed by the evaluators are consistent with the expected test results in the test documentation.

Identifier	Security Function	Descriptions
F001	FIA_UAU.2, FIA_UAU.5, FIA_ATD.1, FIA_UID.2, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FTA_TAH_EXT.1, FAU_GEN.1, FAU_GEN.2, FAU_SEL.1	1. To test that the user shall be authenticated and identified before allowing any other TSF-mediated actions on behalf of that user. 2. To test the TOE shall require a correct form of identification to support user authentication (password). 3. To test that the TOE shall store information regarding the user for authentication purposes. 4. To test that the TOE restricts the ability to manage or specify alternative values and override defaults values as well as security attributes to Authorized Administrators and certain database users as allowed by the Discretionary Access Policy (DAC). 5. To test that the TOE shall store information regarding the last successful session establishment to the user. 6. To test that the TOE could perform the following management function: a. Configure Auditing functionality b. Manage user accounts
F002	FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FTP_TRP.1, FMT_SMF.1, FPT_ITT.1	1. To test that the TOE must be able to generate and destroy cryptographic keys in accordance with the specified cryptographic key generation algorithm. 2. To test that the TOE provides a secure communication path between itself and the user
F003	FMT_MSA.3, FMT_MTD.1, FMT_SMR.1, FDP_ACF.1, FDP_ACC.1, FMT_REV.1	1. To test that the TOE enforces Discretionary Access Policy (DAC) and provide default values to security attributes that enforce Security Functionality. 2. To test that the TOE restricts access to TOE Security Functions data except to Authorized Administrators. 3. To test that the TOE shall have a role called “Admin” which are an Authorized Administrators and associate it with certain approved users. 4. To test that the TOE enforces the DAC policy based on the following criteria: - Subject (User Identity & Role) - Object (Object Identity, Permissions, Protected Collections)

Identifier	Security Function	Descriptions
		5. To test that the TOE determines if an operation among controlled objects are allowed based on a number of factors supplied by the Authorized Administrators. 6. To test that the TOE grants full access to all documents and folders to Authorized Administrators regardless of permissions
F004	FTA_MCS.1, FMT_SMF.1, FTA_TAH_EXT.1	1. To test that the TOE could perform the following management function: - Manage Access Controls - Manage TOE Sessions 2. To test that the TOE could restrict the maximum number of concurrent sessions belonging to the same user connected to the TOE, and by default impose them on the users.
F005	FPT_ITT.1, FPT_TRC_EXT.1, FDP_RIP.1	1. To test that the data transmitted between separate parts of the TOE (if any) are protected. 2. To test that data between separate parts of the TOE (if any) are consistent with one another.
F006	FAU_GEN.1, FAU_GEN.2, FAU_SEL.1	1. To test that the TOE should be able to generate audit record of selected auditable events. 2. To test that the auditable events shall contain information regarding the event as well as information of the user that initiates it. 3. To test those auditable events could be modified by the authorized administrator.
D001	FMT_MSA.1, FDP_ACF.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1, FMT_SMF.1, FMT_SMR.1, FTA_TSE.1, FAU_GEN.1, FAU_GEN.2, FAU_SEL.1, FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FDP_RIP.1, FTA_TAH_EXT.1	1. This test aims to test a myriad of Security Functional Interface and how the TOE reacts to these functions and queries. The Test Harness is used to execute test suites which contain a number of XML files to be loaded in the TOE. The test harness then extracts the results of these tests into XML files and stored it in a directory. These XML files then can be opened for further examination. These are the test suite: - 45adminapi - installodbc - mlsql - password-plugin

Identifier	Security Function	Descriptions
		- 46audit - 0390-audit - ssl - 30 - compartment-security - fips - 51extsec - httptest
D002	FMT_MSA.1, FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FPT_ITT.1	1. This test aims to focus on administrative actions using API's (Admin API, Security API, PKI API, and built-in admin functions). This is the test suite: - 000config-admin-rest-apis
D003	FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1, FMT_SMF.1, FMT_SMR.1	1. This test aims to exercise the Admin Interface and ensure that the Security Management functions are behaving to specification. This is the test suite: - cc-all-admin-gui

2.1.4.3 Penetration Testing

49 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, and security architecture description.

50 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapse time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other requirement for exploitation.

51 The penetration tests focused on:

a) SQL Injections

b) Cross Site Scripting

c) Cross-Site Request Forgery (CSRF)

d) Security Misconfiguration

e) Failure to restrict URL Access

f) Information Disclosure

g) Directory Traversal

h) Buffer Overflow

52 The results of the penetration testing note that there is no residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment as specified in the Security Target (Ref [20]).

2.1.4.4 Testing Results

53 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target (Ref[20]) and its functional specification. In addition, the documentation supplied as evidence for the EAL2+ ALC_FLR.3 Common Criteria evaluation of the TOE was analysed to identify possible vulnerabilities.

3 Result of the Evaluation

54 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [21]), the Malaysian Common Criteria Certification Body certifies the evaluation of MarkLogic Server 8.0-4 performed by BAE Systems Applied Intelligence MySEF.

55 BAE Systems Applied Intelligence MySEF, found that MarkLogic Server 8.0-4 upholds the claims made in the Security Target (Ref [20]) and supporting documentations, and has met the requirements of the Common Criteria (CC) assurance level 2 Augmented with ALC_FLR.3 (EAL2+ ALC_FLR.3).

56 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

57 EAL2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

58 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to an attacker possessing a -Basic attack potential.

59 EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

60 The following recommendations are made:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.
b) The users should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.
c) The users must maintain the confidentiality, integrity and availability of security relevant data for TOE initialisation, start-up and operation if stored or handled outside the TOE
d) System Auditor should review the audit trail generated and exported by the TOE periodically
e) The users must ensure appropriate network protection is maintained, the network on which the TOE is installed must be both physically and logically protected, commensurate with the sensitivity of the TOE keys

Annex A References

A.1 References

[15] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

[16] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[17] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[18] MyCC Scheme Policy (MyCC_P1), v1c, CyberSecurity Malaysia, December 2015.

[19] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1b, December 2015.

[20] MarkLogic Server 8 ST v0.5 Security Target, Version 0.5, 9 October 2015

[21] Evaluation Technical Report, EAU000291-S030-ETR v1.0, Version 1.0, 24 November 2015

A.2 Terminology

A.2.1 Acronyms

Table 2: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 3: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.

Term	Definition and Source
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---