Certification Report

EAL 4+ (ALC_FLR.2) Evaluation of

Labris Teknoloji Bil. Çöz. A.Ş.
Labris v2.2.1

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-37

TABLE OF CONTENTS

Document Information

Date of Issue	07.11.2016
Approval Date	08.11.2016
Certification Report Number	21.0.03/16-006
Sponsor and Developer	Labris Teknoloji Bil. Çöz. A.Ş.
Evaluation Facility	BEAM Teknoloji A.Ş.
TOE	Labris v2.2.1
Pages	16

Prepared by	İbrahim Halil KIRMIZI
Reviewed by	Zümrüt MÜFTÜOĞLU

This report has been prepared by the Certification Expert and reviewed by the Technical Responsible of which signatures are above.

Document Change Log

Release	*Date*	*Pages Affected*	*Remarks/Change Reference*
1	07.11.2016	*ALL*	First Release

DISCLAIMER

This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformant to Common Criteria for IT Security Evaluation, version 3.1,revision 3, using Common Methodology for IT Products Evaluation, version 3.1, revision 3. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related *with a Common Criteria evaluation which is made under the ITCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.*

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL = Common Criteria Testing Laboratory) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by BEAM Teknoloji A.Ş., which is a public CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for Labris version 2.2.1 whose evaluation was completed on 27.10.2016 and whose evaluation technical report was drawn up by BEAM Teknoloji A.Ş. (as CCTL), and with the Security Target document with version no 36 of the relevant product.

The certification report, certificate of product and security target document are posted on the ITCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org

1 - EXECUTIVE SUMMARY

This report constitutes the certification results by the certification body on the evaluation results applied with requirements of the Common Criteria for Information Security Evaluation.

Evaluated IT product name: Labris

IT Product version: 2.2.1

Developer's Name: Labris Teknoloji A.Ş.

Name of CCTL: BEAM Teknoloji A.Ş.

Assurance Package: EAL 4+ (ALC_FLR.2)

Completion date of evaluation: 27.10.2016

1.1 Brief Description

TOE is a firewall management software that provides mechanisms for management and monitoring of packet filtering, IP routing, network address translation, port address translation and audit records generation. TOE is composed of two parts, which are LABRİS Management Console (LMC) Software and LABRİS Management Console Server (LMCS) software.

Labris Management Console Software is used by TOE administrators to first authenticate them to TOE and then administer it in same secure environment. They can change access rules, packet-filtering policies, routing configuration and network interface configuration. At the same time, they can review audit logs of TOE from the Labris Management Console Software. LMCCP is the network protocol between LMC Software and LMCS Software and is implemented in both TOE parts. It is an xml-based protocol. It is used with SSL sockets, which are provided by client and server operating systems. LMCCP provides reliable and secure remote connection.

1.2 TOE Security Functions

As described in the Security Target document, TOE Security Functions are;

- Information Flow
- Access Control
- Logging

1.3 Threats

Possible threat agents considered for TOE are unauthorized persons or external IT entities, which are not authorized to use TOE. Threat agents are considered independent entities with a low level of attack sophistication, which are not able to perform organized attacks on TOE.

- **T.REPEAT**: An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
- **T.AUDFUL**: An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
- **T.NOAUTH**: An unauthorized person may attempt to bypass the security of the TOE so as to access and use security function and/or non-security functions provided by the TOE.
- **T.AUDACC**: An unauthorized person may not be accountable for the TOE attack actions, because the audit records are not reviewed, thus allowing an attacker to escape detection.
- **T.SELPRO**: An unauthorized person may read, modify, or destroy security critical TOE configuration data.

1.4 Organizational Security Policies

The following security policies shall be applied by the organization hosting the TOE.

- **P.GENPUR**: There shall be no use of general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on platforms where TOE runs.
- **P.PUBLIC**: The platforms where TOE runs shall not host public data. Databases or other company related information that may be accessed from internal or external network, which is publicly available to remote applications, shall not be stored on platforms where TOE runs.
- **P.SINGEN**: Network infrastructure shall be configured such that all the information between internal networks, external networks and DMZ pass through the gateway configured by the TOE.

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-37
TOE Name and Version	Labris version 2.2.1
Security Target Title	Labris v2.2.1 Security Target
Security Target Version	36
Security Target Date	20.10.2016
Assurance Level	EAL 4+ (ALC_FLR.2)
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009, • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1 Revision 3, July 2009, • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2009-07-003, Version 3.1 Revision 3, July 2009
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009
Protection Profile Conformance	None
Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1 Revision 3, July 2009, extended • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2009-07-003, Version 3.1 Revision 3, July 2009, augmented

2.2 Security Policy

The following security policies shall be applied by the organization hosting the TOE.

- **P.GENPUR**: There shall be no use of general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on platforms where TOE runs.
- **P.PUBLIC**: The platforms where TOE runs shall not host public data. Databases or other company related information that may be accessed from internal or external network, which is publicly available to remote applications, shall not be stored on platforms where TOE runs.
- **P.SINGEN**: Network infrastructure shall be configured such that all the information between internal networks, external networks and DMZ pass through the gateway configured by the TOE.

2.3 Assumptions and Clarification of Scope

The following conditions are assumed to exist in the operational environment.

- **A.CORRECT**: The platform, where management console runs, correctly transmits the information to the server by direct link, and receives the information correctly, which is sent to it by the server from the same direct link.
- **A.NOEVIL**: Authorized root administrator and authorized administrators are non-hostile
- **A.FOLLOW:** Authorized administrators and Authorized Root Administrators follow all administrator guidance; however, they are capable of error.
- **A.PHYSEC**: TOE is physically secure. It is assumed that there are no physical attacks on platforms where LMC server and LMC client is running. TOE shall only be accessed and managed from a Secure Environment using Management Console monitor, keyboard and mouse. A securely configured Management Console shall be directly connected to the LMC Server via dedicated link entirely within a secure environment.

2.4 Architectural Information

Labris v2.2.1 is a client-server application. It has two main components; LMC and LMCS. LMCS is the server component and runs on a dedicated host, which may be Labris hardware or any equivalent server hardware. LMC is the client component and it runs on PC. This two components communicate through a secure line via LMCCP protocol. Since this two components have different execution environments their execution environments are described in the following seperate sections.

- **Labris Management Console:** LMC is a multi-platform Java application used to control LMCS remotely. Currently there are distribution packages of LMC for Windows and Linux platforms. These packages also includes the platform specific, redistributable, Java(TM) 2 Runtime Environment, Standard Edition Version 6. LMC runs on the Java Virtual Machine of the JRE. For software and hardware requirements of JRE.
- **Labris Management Console Server:** LMCS is a system, which is a collection of C++ main application, C++ loadable modules and BASH scripts. LMCS designed to run on Linux i686 platform. LMCS runs specifically on minimal installation of CentOS Release 5 with unnecessary packets removed. See Appendix 6.1 for list of the removed packets from standard minimal CentOS Release 5.

The Security Functions are enforced by the following subsystems;

- Client Base Subsystem,
- Client Firewall Subsystem,
- Client System Subsystem,
- Client IP Route,
- Server Base,
- Server Firewall,
- Server System,
- Server IP Route

2.5 Documentation

These documents listed below are provided to customer by the developer alongside the TOE:

Document	Version	Release Date
Labris v2.2.1 Security Target	36	20.10.2016
Labris Güvenlik Duvarı v2.2.1 Kullanım Kılavuzu	23	21.02.2014
Labris v2.2.1 Kurulum Kılavuzu	27	21.02.2014
Labris v2.2.1 Güvenlik İyileştirme Kılavuzu	17	21.02.2014
Labris IP Yönlendirme Kılavuzu	14	21.02.2014
Labris v2.2.1 Lisans Kullanım Kılavuzu	15	21.02.2014
Labris v2.2.1 Sistem Kullanım Kılavuzu	19	21.02.2014
Labris Security Architecture Documentation	01	27.12.2013
Labris v2.2.1 Functional Specification	24	10.03.2014
Labris High Level Design Description	18	10.03.2014
Labris Low Level Design Description	20	27.12.2013
Configuration Management Document	25	20.10.2016
Labris_DEL Kurulum Kılavuzu	27	22.11.2013
Labris Development Security Documentation	10	22.11.2013
Labris Flaw Remediation Procedures	12	22.11.2013
Labris Life Cycle Definition	11	22.11.2013
Labris Development Tools and Techniques	13	22.11.2013
Labris v2.2.1 Açıklık Bildirimi ve Güncelleme Kılavuzu	04	22.11.2013
Labris Test Documentation	18	09.05.2014

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developers. All the delivered evaluation evidences which include software, hardware documents, etc. are mapped to the assurance families Common Criteria and Common Methodology; so the connections between the assurance families and the evaluation evidences has been established. The evaluation results are available in the final Evaluation Technical Report (ETR) of Labris v2.2.1.

It is concluded that the TOE supports EAL 4+ (ALC_FLR.2). There are 25 assurance families which are all evaluated with the methods detailed in the ETR.

IT Product Testing is mainly realized in two parts:

2.6.1 Developer Testing:

- TOE Test Coverage: Developer has prepared TOE Test Documentation according to the TOE Functional Specification documentation.
- TOE Test Depth: Developer has prepared TOE Test Documentation according to the TOE Design documentation which include TSF subsystems and its interactions.
- TOE Functional Testing: Developer has made functional tests according to the test documentation. Test plans, test scenarios, expected test results and actual test results are in the test documentation.

2.6.2 Evaluator Testing:

The tests were performed with the product Labris v2.2.1.

- Independent Testing: Evaluator has done a total of 14 sample independent tests. All of them are related to TOE security functions.
- Penetration Testing: Evaluator has done 7 penetration tests to find out if TOE`s vulnerabilities can be used for malicious purposes. The potential vulnerabilities and the penetration tests are in "beam_labris_van_report v1.2" which is in Annex-E of the ETR and the penetration tests and their results are available in detail in the ETR document as well.

2.7 Evaluated Configuration

The evaluated configuration consists of the Labris v2.2.1 components which are configured as specified in "Labris Güvenlik Duvarı v2.2.1 Kullanım Kılavuzu v23, 21.02.2014" document.

2.8 Results of the Evaluation

Table below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with ALC_FLR.2.

Assurance Class	Component	Component Title
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.4	Complete Functional Specification
	ADV_IMP.1	Implementation Representation of the TSF
	ADV_TDS.3	Basic Modular Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life-Cycle Support	ALC_CMC.4	Production Support, Acceptance Procedures and Automation
	ALC_CMS.4	Problem Tracking CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Identification of Security Measures
	ALC_FLR.2	Flaw Remediation Procedures
	ALC_LCD.1	Developer Defined Life-Cycle Model
	ALC_TAT.1	Well-defined Development Tools
Security Target Evaluation	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
Tests	ATE_COV.2	Analysis of Coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing -sample

Vulnerability Analysis	AVA_VAN.3	Focused Vulnerability Analysis

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer about the 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. So for TOE "Labris v2.2.1" the results of the assessment of all evaluation tasks are "Pass".

The result of AVA_VAN.3 evaluation is given below:
It is determined that TOE, in its operational environment, is resistant to an attacker possessing **"Enhanced-Basic"** attack potential.

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of "Labris v2.2.1" product, result of the evaluation, or the ETR.

3 SECURITY TARGET

The Security Target associated with this Certification Report is identified by the following terminology:
Title: Labris v2.2.1 Security Target
Version: 36
Date of Document: 20.10.2016

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale.

4 GLOSSARY

ADV : Assurance of Development

AGD : Assurance of Guidance Documents

ALC : Assurance of Life Cycle

ASE : Assurance of Security Target Evaluation

ATE : Assurance of Tests Evaluation

AVA : Assurance of Vulnerability Analysis

CC : Common Criteria (Ortak Kriterler)

CCCS : Common Criteria Certification Scheme (TSE)

CCRA : Common Criteria Recognition Arrangement

CCTL : Common Criteria Test Laboratory (OKTEM)

CEM :Common Evaluation Methodology

CMC : Configuration Management Capability

CMS : Configuration Management Scope

DEL : Delivery

EAL : Evaluation Assurance Level

OPE : Opretaional User Guidance

OSP : Organisational Security Policy

PP : Protection Profile

PRE : Preperative Procedures

SAR : Security Assurance Requirements

SFR : Security Functional Requirements

ST : Security Target

TOE : Target of Evaluation

TSF : TOE Secırity Functionality

TSFI : TSF Interface

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009,

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009 ,

[3] BTBD-01-01-TL-01 Certification Report Preparation Instructions, Rel.Date: 08.02.2016

[4] BTTM-CCE-001 Labris v2.2.1 Değerlendirme Teknik Raporu v1.2, 27.10.2016

6 ANNEXES

There is no additional information which is inappropriate for reference in other sections