SERTIT-104 CR Certification Report

Issue 1.0 8 May 2018

Thinklogical TLX80 Matrix Switch
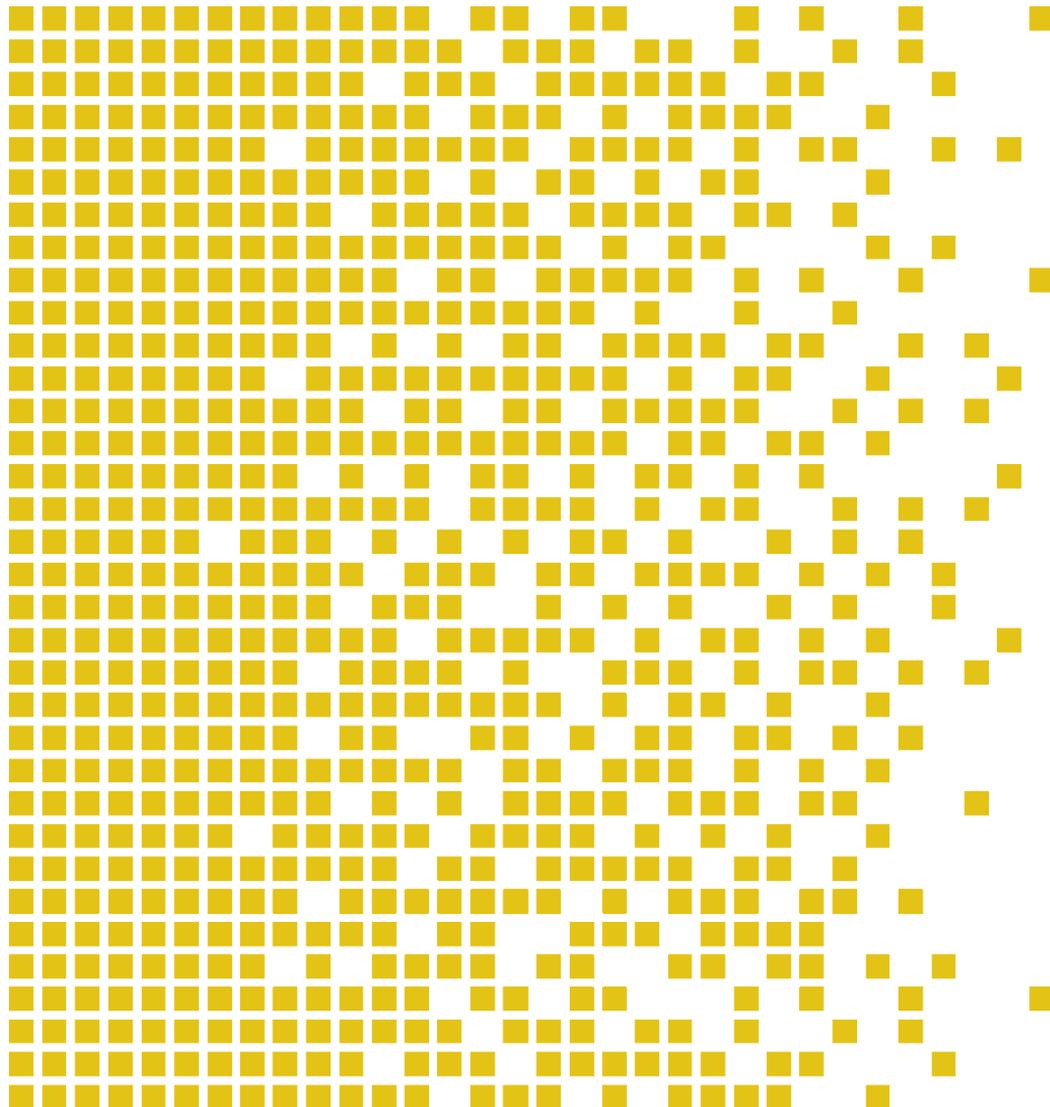
CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009E VERSION 1.1 01.07.2015

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The recognition under CCRA is limited to cPP related assurance packages or EAL 2 and ALC_FLR CC part 3 components.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Mutual recognition under SOGIS MRA applies to components up to EAL 4.

⠿⠇⠿⠒⠒⠿⠿⠶⠿⠿⠿⠿⠿⠶⠶⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿⠿

Contents

⠟⠁⠇⠕⠗⠑⠀⠃⠗⠁⠊⠇⠇⠑⠀⠞⠑⠭⠞⠀⠏⠇⠁⠉⠑⠓⠕⠇⠙⠑⠗

1   Certification Statement

Thinklogical TLX80 Matrix Switch is a fiber optic switch that uses multi-mode or single-mode fiber optics to transmit and receive a digital video pulse stream without alteration or interpretation of the original signal.

Thinklogical TLX80 Matrix Switch has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant components of Evaluation Assurance Level EAL 4 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality in the specified environment when running on the platforms specified in Annex A.

Author	Arne Høye Rage
	Certifier
Quality Assurance	Kjartan Jæger Kvassnes
	Quality Assurance
Approved	Kristian Bae
	Head of SERTIT
Date approved	8 May 2018

2   Abbreviations

CC	Common Criteria for Information Technology Security Evaluation(ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
POC	Point of Contact
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SOGIS MRA	SOGIS Mutual Recognition Agreement
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

⠿⠿⠿

3   References

[1]   Thinklogical TLX80 Matrix Switch Security Target Document Version 1.2.

[2]   Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2017-04-001, Version 3.1 R5, April 2017.

[3]   Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CCMB-2017-04-002, Version 3.1 R5, April 2017.

[4]   Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CCMB-2017-04-003, Version 3.1 R5, April 2017.

[5]   The Norwegian Certification Scheme, SD001E, Version 10.4, 02 February 2018.

[6]   Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 R5, April 2017.

[7]   Evaluation Technical Report Common Criteria EAL4 Evaluation of Thinklogical Router KVM Matrix Switches 2018-03-15, Issue 1.0.

[8]   SOGIS MRA, Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3.0, January 8th 2010.

A list of guidance documents can be found in Annex A

⠿⠀⠿

4   Executive Summary

4.1   Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Thinklogical TLX80 Matrix Switch to the developer, Thinklogical, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation components.

4.2   Evaluated Product

The product evaluated was Thinklogical TLX80 Matrix Switch consisting of:

- TLX80 Matrix Switch Chassis (TLX-MSC-000080 Rev A)
- TLX80 Matrix Switch Data Input and Output Card, 10 Ports, SFP+, 10G Multi-Mode (TLX-MSD-M00005 Rev B), Single Mode (TLX-MSD-S00005 Rev B)
- TLX80 Matrix Switch Data Input and Output Card, 10 Ports, SFP+, 6G
- Multi-Mode (TLX-MSD-MV0005 Rev B), Single Mode (TLX-MSD-SV0005 Rev B)

This product is also described in this report as the Target of Evaluation (TOE). The developer was Thinklogical.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

TOE does not require any other hardware equipment in order to maintain the Security Function Requirements (SFRs). However, the KVM Matrix Switch is used with Thinklogical Velocity extender series and the Thinklogical TLX extender series. The extenders are not part of the TOE.

4.3   TOE scope

The TOE scope is described in the Security Target[1] section 2.

4.4   Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5   Assurance Level

The Security Target[1] specified the assurance components for the evaluation. Predefined evaluation assurance level EAL 4 was used. Common

Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

There are no Organizational Security Policies or rules with which the TOE must comply.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats which these objectives meet and security functional components and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

All threats that are countered are described in the Security Target [1], section 3.2.

4.9 Threats Countered by the TOE's environment

All threats that are countered by the TOE's environment are described in the Security Target [1], section 3.2.

4.10 Threats and Attacks not Countered

No threats or attacks are described that are not countered.

4.11 Environmental Assumptions and Dependencies

The assumptions that apply to this TOE are described in the Security Target [1], section 3.1.

4.12 IT Security Objectives

The security objectives for the TOE that apply to this TOE are described in the Security Target[1] section 4.1.

4.13 Non-IT Security Objectives

The security objectives for the environment that apply to this TOE are described in the Security Target[1] section 4.2

⠠⠃⠗⠁⠊⠇⠇⠑ ⠞⠑⠭⠞

4.14 Security Functional Components

The security functional requirements that apply to this TOE are described in the Security Target[1] section 5.1.

Security Functional Components	
FDP_ETC.1	Export of User Data Without Security Attributes
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_ITC.1	Import of User Data Without Security Attributes

4.15 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Norconsult AS Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR)[7] to SERTIT in 3 May 2018. SERTIT then produced this Certification Report.

4.16 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their

identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

⠿⠿⠒⠶⠿⠶⠶⠿⠒⠶⠿⠿⠒⠶⠿⠶⠶⠿⠒⠶⠿⠿⠒⠶⠿⠶⠶⠿⠒⠶⠿⠿⠒⠶⠿⠶⠶⠿

5   Evaluation Findings

5.1   Introduction

The evaluation addressed the requirements specified in the Security
Target[1]. The results of this work were reported in the ETR[7] under the CC
Part 3[4] headings. The following sections note considerations that are of
particular relevance to either consumers or those involved with subsequent
assurance maintenance and re-evaluation of the TOE.

5.2   Delivery

On receipt of the TOE, the consumer is recommended to check that the
evaluated version has been supplied, and to check that the security of the
TOE has not been compromised in delivery.

The developer has procedures for standard commercial delivery services
supplemented with methods for tamper proof delivery of the TOE.

5.3   Installation and Guidance Documentation

A description of the secure installation of the TOE and the secure
preparation of the operational environment in accordance with the security
objectives in the ST[1] can be found in the guidance documents.

The guidance documentation also describes the security functionality and
interfaces provided by the TOE. It provides instructions and guidelines for
the secure use of the TOE, it addresses secure procedures for all modes of
operation, facilitates prevention and detection of insecure TOE states.

A list of all guidance documents evaluated can be found in Annex A.

5.4   Misuse

There is always a risk of intentional and unintentional misconfigurations that
could possibly compromise confidential information. The user should always
follow the guidance for the TOE in order to ensure that the TOE operates in a
secure manner.

The guidance documents adequately describe the mode of operation of the
TOE, all assumptions about the intended environment and all requirements
for external security. Sufficient guidance is provided for the consumer to
effectively use the TOE's security functions

5.5   Vulnerability Analysis

The evaluators' vulnerability analysis was based on both public domain
sources and the visibility of the TOE given by the evaluation process and
evaluation process of previous versions of the TOE. The vulnerability
analysis took into consideration the Enhanced-Basic attack potential

The evaluators have devised a set of tests to test potential vulnerabilities to the TOE. The tests were performed at the developer's site in Milford, Connecticut in October 2017 / March 2018.

The result of the vulnerability analysis is that the TOE in its evaluated configuration and in its intended environment has no exploitable vulnerabilities.

5.6 Developer's Tests

The evaluators' assessment of the developer´s tests shows that the developer´s tests cover all the TSFIs and all SFRs.

The evaluators have confirmed the developer have correctly performed and documented the tests according to the test documentation.

5.7 Evaluators' Tests

The evaluators have independently tested a sample of the developer´s tests and verified that the TOE behaves as specified. Confidence in the developer's test results is gained by performing a sample of the developer's tests.

The evaluators tests were conducted at the developer's site in Milford, Connecticut in October 2017 / March 2018.

6   Evaluation Outcome

6.1   Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Thinklogical TLX80 Matrix Switch meet the Common Criteria Part 3 conformant components of Evaluation Assurance Level EAL 4 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

6.2   Recommendations

Prospective consumers of Thinklogical TLX80 Matrix Switch should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Section 4.3 "TOE Scope" and Section 5 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

One assumption for the TOE stated in the ST [1] is that the switch, the transmitters, the receivers, the optical connections from the Switch to the transmitters and receivers and the wired network connections from the Switch to the administrators are physically secure.The product manuals states that the TOE must be physically protected in accordance with the requirements of the highest classification. This assumption is important to take into consideration especially for larger operational environments.

The above "Evaluation Findings" include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

- TLX80 Matrix Switch Chassis (TLX-MSC-000080 Rev A)
- TLX80 Matrix Switch Data Input and Output Card, 10 Ports, SFP+, 10G Multi-Mode (TLX-MSD-M00005 Rev B), Single Mode (TLX-MSD-S00005 Rev B)
- TLX80 Matrix Switch Data Input and Output Card, 10 Ports, SFP+, 6G
- Multi-Mode (TLX-MSD-MV0005 Rev B), Single Mode (TLX-MSD-SV0005 Rev B)
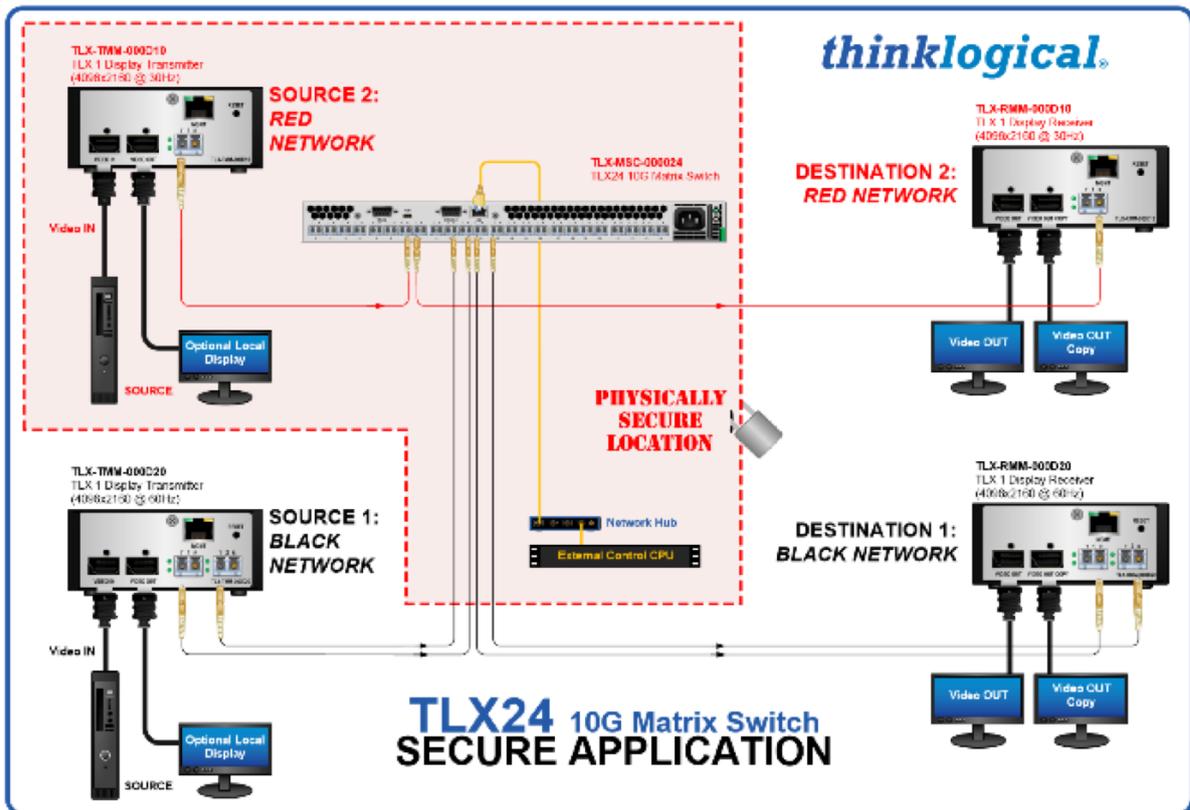
TOE Documentation

The supporting guidance documents evaluated were:

[a]   Operational User Guidance Rev. E

[b]   TLX12 10G Matrix Switch Product Manual Rev. B

[c]   TLX24 10G Matrix Switch Product Manual Rev. F

[d]   TLX80 10G Matrix Switch Product Manual Rev. C

[e]   TLX160 10G Matrix Switch Product Manual Rev. C

[f]   System Management Portfolio Rev. A

[g]   TLX Matrix Switch ASCII API V5 Rev. H

[h]   TLX Matrix Switch Interfaces Rev. F

[i]   QUICK-START GUIDE TLX12 10G Fiber-Optic MATRIX Switch As used with Thinklogical's Q-Series & TLX Video Extension Systems

[j]   QUICK-START GUIDE TLX24 10G MATRIX Switch As used with Thinklogical's Q-Series & TLX Video Extension Systems

[k]   QUICK--START GUIDE TLX80 10G Fiber-Optic MATRIX Switch As used with Thinklogical's TLX KVM Extension Systems

[l]   QUICK--START GUIDE TLX160 10G Fiber-Optic MATRIX Switch As used with Thinklogical's TLX KVM Extension Systems

[m]   How To Change A TLX Matrix Switch's IP Address Rev. B

Environmental Configuration

For use in an evaluated configuration, the Router KVM Matrix Switches must be located in a physically secure environment to which only authorized administrators has access. Similarly, the server used to manage the Router KVM Matrix Switches must be physically protected and have suitable

identification/authentication mechanism to ensure that only trusted administrators have access.

The figure below shows the TLX24 Router KVM Matrix Switch in an evaluated configuration. An equivalent layout is the evaluated configuration for the TLX80 Router KVM Matrix Switch.

Certificate

Product Manufacturer: Thinklogical

Product Name: TLX80 Matrix Switch

Type of Product: KVM Matrix Switch

Version and Release Numbers: Versions are detailed in the Certification Report

Assurance Package: EAL 4

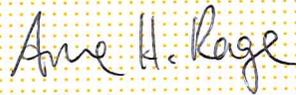Evaluation Criteria: Common Criteria v. 3.1 R5

Name of IT Security Evaluation Facility: Norconsult AS

Name of Certification Body: SERTIT

Certification Report Identifier: SERTIT-104 CR Issue 1.0, 8. May 2018

Certificate Identifier: SERTIT-104 C

Date Issued: 8. May 2018

Arne Høye Rage
Certifier

Kjartan Jæger Kvassnes
Quality Assurance

Kristian Steinfeld Bae
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security

CCRA recognition for components up EAL 2 and ALC_FLR only.

SOGIS MRA recognition for components up to EAL 4.