SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*
SERTIT er en del av Nasjonal sikkerhetsmyndighet *SERTIT is a part of Norwegian National Security Authority*

SERTIT-119 CR Certification Report

Issue 1.0 12 December 2019

Expiry date 12 December 2024

Thinklogical TLX1280 Matrix Switch

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE ST 009E VERSION 2.5 15.05.2018

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

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 components up to EAL 2 with 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 TLX1280 Matrix Switch is a fiber optic switch that uses multi-mode fiber optics to transmit and receive a digital video pulse stream without alteration or interpretation of the original signal. Embedded keyboard, mouse, USE 1.1, USB 2.0 (high speed up to 480 Mbps), and audio signals are also transmitted.

Thinklogical TLX1280 Matrix Switch version:

- TLX1280 Matrix Switch Chassis (TLX-MSC-001280 Rev A);
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, SFP+, Multi-Mode (TLX-MSD-M00032 Rev A), Single Mode (TLX-MSD-S00032 Rev A);
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, 6G+, SFP+, Multi-Mode (TLX-MSD-MV0032 Rev A), Single-Mode (TLX-MSD-SV0032 Rev A);
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, SFP+, Multi-Mode (TLX-MSD-M00032 Rev B), Single Mode (TLX-MSD-S00032 Rev B);
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, 6G+, SFP+, Multi-Mode (TLX-MSD-MV0032 Rev B), Single-Mode (TLX-MSD-SV0032 Rev B).

has been evaluated under the terms of the Norwegian Certification Authority 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.

There is currently no Protection Profile directly applicable to the type of technology provided by the TOE, unless where there is a single set of peripherals locally managing multiple computers. It is the aim to stay close to the requirements of the PSSPP generalizing them for the case of multiple sets of peripherals and remote connectivity.

Certification team	Lars Borgos, Øystein Hole.
Date approved	12 December 2019
Expiry date	12 December 2024

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
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
PP	Protection Profile
SERTIT	Norwegian Certification Authority for IT Security
SOGIS MRA	SOGIS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

3 References

[1] CCRA (2014), *Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security*, CCRA, July 2nd 2014.

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

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

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

[5] CCRA (2017), *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, CCMB-2017-04-004, Version 3.1 R5, CCRA, April 2017.

[6] *Evaluation Technical Report Common Criteria EAL4 Evaluation of Thinklogical Router KVM Matrix Switch*, Thinklogical TLX1280, Issue 1.0, 2019-10-27.

[7] Information Assurance Directorate (IAD) (2010), *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, version 2.1, IAD, 7 September 2010.

[8] SERTIT (2018), *The Norwegian Certification Scheme*, SD001E, Version 10.4, SERTIT, 20 February 2018.

[9] SOGIS Management Committee (2010), *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, Version 3.0, SOGIS MC, January 8th 2010.

[10] Thinklogical (2019), *TLX1280 Matrix Switch Security Target*, Thinklogical, version 1.4, Oct 2019.

Annex A: List of guidance documents

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Thinklogical TLX1280 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 ST[10] which specifies the functional, environmental and assurance evaluation components.

4.2 Evaluated Product

The product evaluated was Thinklogical TLX1280 Matrix Switch comprising:

- TLX1280 Matrix Switch Chassis (TLX-MSC-001280 Rev A);
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, SFP+, Multi-Mode (TLX-MSD-M00032 Rev A), Single Mode (TLX-MSD-S00032 Rev A);
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, 6G+, SFP+, Multi-Mode (TLX-MSD-MV0032 Rev A), Single-Mode (TLX-MSD-SV0032 Rev A);
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, SFP+, Multi-Mode (TLX-MSD-M00032 Rev B), Single Mode (TLX-MSD-S00032 Rev B);
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, 6G+, SFP+, Multi-Mode (TLX-MSD-MV0032 Rev B), Single-Mode (TLX-MSD-SV0032 Rev B).

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

Annex A gives details of the evaluated configuration, including the TOE’s supporting guidance documentation.

TOE does not require any other hardware equipment in order to maintain the Security Functional Requirements (SFRs). However, the KVM Matrix Switch is used with the 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 ST[10], section 2.

4.4 Protection Profile Conformance

The ST[10] did not claim conformance to any Protection Profile.

There is currently no Protection Profile directly applicable to the type of technology provided by the TOE, unless where there is a single set of peripherals locally managing multiple computers. The ST[10] states it is the aim to stay close to the requirements of the PSSPP [7] generalizing them for the case of multiple sets of peripherals and remote connectivity.

US Government Peripheral Sharing Switch (PSS) For Human Interface Devices Protection Profile Version 1.2.

4.5 Assurance Level

The ST[10] 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[1].

4.6 Security Policy

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

4.7 Security Claims

The ST[10] fully specifies the TOE’s security objectives, the threats which these objectives are to 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 ST[10], 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 ST[10], 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 ST[10], section 3.1.

4.12 IT Security Objectives

The Security Objectives for the TOE that apply to this TOE are described in the ST[10], section 4.1.

4.13 Non-IT Security Objectives

The security objectives for the environment that apply to this TOE are described in the ST[10], section 4.2.

4.14 Security Functional Requirements

The following security functional requirements apply to this TOE, as also described in the ST[10], section 5.1.

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

Table 1 TOE Security Functional Components

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[8]. 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 both the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, CCRA[1], and the Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, SOGIS MRA[6]. The evaluation was conducted in accordance with the terms of the before mentioned Arrangement and Agreement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its ST[10], which prospective consumers are advised to read. To ensure that the ST[10] 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)[5].

SERTIT monitored the evaluation in accordance with SD001E[8], which was carried out by the Commercial Evaluation Facility (EVIT) named Norconsult AS. The evaluation was completed when the EVIT submitted the final ETR[6] to SERTIT on 27.10.2019. SERTIT then produced this Certification Report.

4.16 General Points

The evaluation addressed the security functionality claimed in the ST[10] with reference to the assumed operating environment specified by the ST[10]. 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

The evaluators examined the following assurance classes and components taken from CC Part 3[4]. These classes comprise the EAL 4 assurance package.

Assurance class	Assurance components	
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_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 assessment	AVA_VAN.3	Focused vulnerability analysis

Table 2 TOE Assurance Classes and Components

5.1 Introduction

The evaluation addressed the requirements specified in the ST[10]. The results of this work were reported in the ETR[6] 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[10] can be found in the guidance documents as listed in Annex A.

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.

Annex A holds a list of all evaluated guidance documents.

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 August 2019.

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 August 2019.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[6], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Thinklogical TLX1280 Matrix Switch version:

- TLX1280 Matrix Switch Chassis (TLX-MSC-001280 Rev A);
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, SFP+, Multi-Mode (TLX-MSD-M00032 Rev A), Single Mode (TLX-MSD-S00032 Rev A);
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, 6G+, SFP+, Multi-Mode (TLX-MSD-MV0032 Rev A), Single-Mode (TLX-MSD-SV0032 Rev A)
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, SFP+, Multi-Mode (TLX-MSD-M00032 Rev B), Single Mode (TLX-MSD-S00032 Rev B);
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, 6G+, SFP+, Multi-Mode (TLX-MSD-MV0032 Rev B), Single-Mode (TLX-MSD-SV0032 Rev B).

meets the specified 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 TLX1280 Matrix Switch should understand the specific scope of the certification by reading this report in conjunction with the ST[10]. The TOE should be used in accordance with a number of environmental considerations as specified in the ST[10].

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, see Annex A.

One assumption for the TOE stated in the ST[10] 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:

- TLX1280 Matrix Switch Chassis (TLX-MSC-001280 Rev A 1.4);
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, SFP+, Multi-Mode (TLX-MSD-M000032 Rev A), Single Mode (TLX-MSD-S00032 Rev A);
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, 6G+, SFP+, Multi-Mode (TLX-MSD-MV0032 Rev A), Single-Mode (TLX-MSD-SV0032 Rev A)
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, SFP+, Multi-Mode (TLX-MSD-M00032 Rev B), Single Mode (TLX-MSD-S00032 Rev B);
- TLX1280 Matrix Switch Data Input / Output Card, 32 Ports, 6G+, SFP+, Multi-Mode (TLX-MSD-MV0032 Rev B), Single-Mode (TLX-MSD-SV0032 Rev B).

TOE Documentation

The supporting guidance documents evaluated were:

[a] Operational User Guidance Rev. F

[b] TLX1280 10G Matrix Switch Product Manual Rev. C

[c] System Management Portfolio Rev. A

[d] TLX Matrix Switch ASCII API V5 Rev. I

[e] TLX Matrix Switch Interfaces Rev. H

[f] QUICK-START GUIDE TLX1280 10G Fiber-Optic MATRIX Switch As used with Thinklogical’s Q-Series & TLX Video Extension Systems

[g] How To Change A TLX Matrix Switch's IP Address Rev. D

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 TLX1280 Router KVM Matrix Switch in an evaluated configuration.

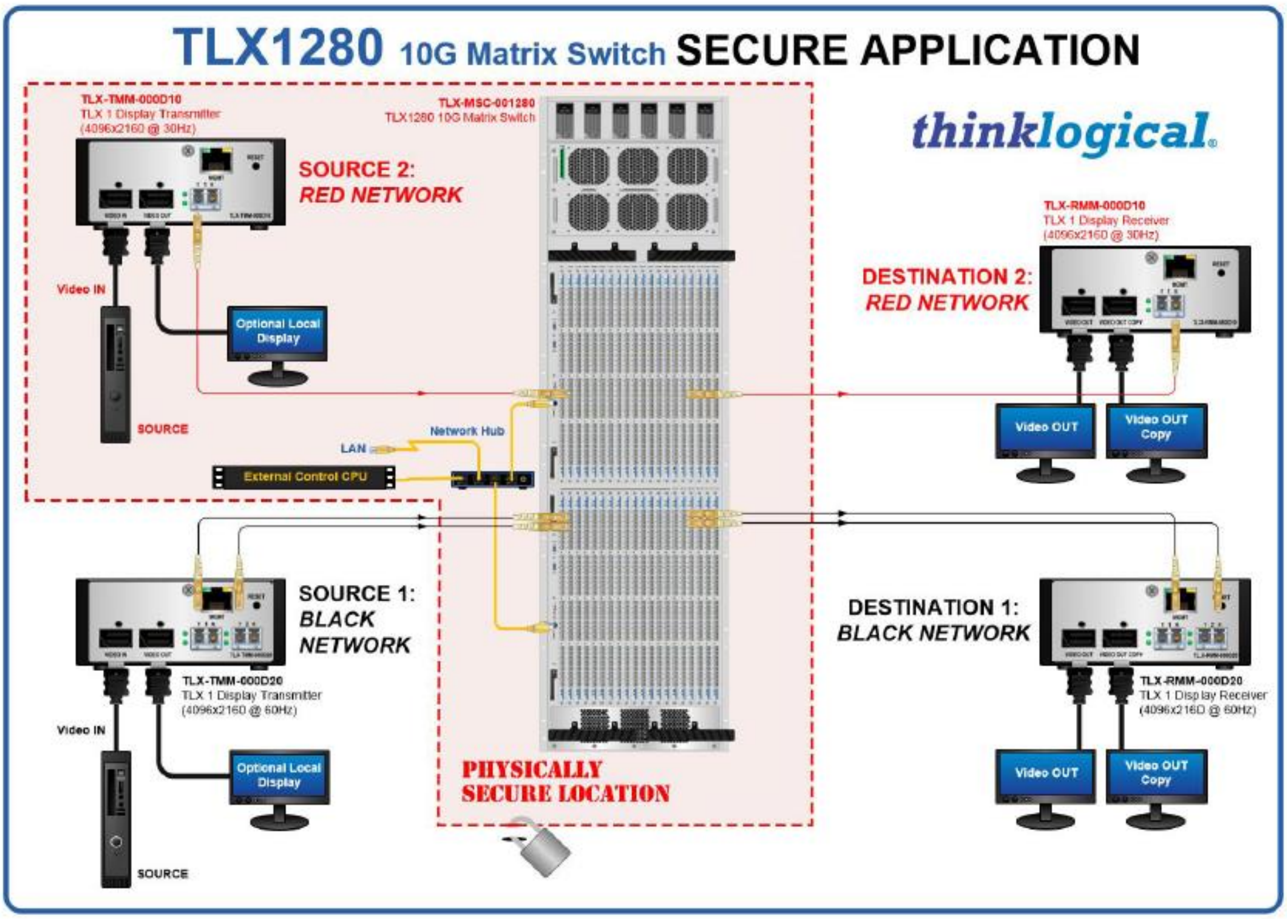

Figure 3 TLX1280 Router KVM Matrix Awitch in an evaluated configuration.