# Certification Report

## TLX48 2RU Matrix Switch Chassis (TLX-MSC-020048)

| | |
|---|---|
| Sponsor and developer: | ***Thinklogical LLC***<br>**100 Washington Street**<br>**Milford, Connecticut, 06460**<br>**USA** |
| Evaluation facility: | ***SGS Brightsight B.V.***<br>**Brassersplein 2**<br>**2612 CT Delft**<br>**The Netherlands** |
| Report number: | **NSCIB-CC-0612764-CR** |
| Report version: | **1** |
| Project number: | **0612764** |
| Author(s): | **Kjartan Jæger Kvassnes** |
| Date: | **04 July 2023** |
| Number of pages: | **11** |
| Number of appendices: | **0** |





Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

# CONTENTS

# Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, 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 or site satisfies the security requirements stated in the (site) security target.

# Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

## International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

## European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

# 1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the TLX48 2RU Matrix Switch Chassis (TLX-MSC-020048). The developer of the TLX48 2RU Matrix Switch Chassis (TLX-MSC-020048) is Thinklogical LLC located in Milford, USA and they also act as the sponsor of the evaluation and certification A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE 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. Embedded keyboard, mouse, USB 1.1, USB 2.0 (high speed up to 480 Mbps), and audio signals are also transmitted. The TLX48 2RU provides reliability and signal integrity with high performance 6.25Gbps and 10.3125Gbps capability. Scalable up to 48 x 48 bi-directional ports, this highly robust KVM Matrix Switch is used with ThinklogicalTM Velocity extender series and the ThinklogicalTM TLX extender series. The Switch includes pluggable cards which allow changing the number of supported ports in groups of 24.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 4 July 2023 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the TLX48 2RU Matrix Switch Chassis (TLX-MSC-020048), the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the TLX48 2RU Matrix Switch Chassis (TLX-MSC-020048) are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw reporting procedures).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

# 2 Certification Results

## 2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the TLX48 2RU Matrix Switch Chassis (TLX-MSC-020048) from Thinklogical LLC located in Milford, USA.

The TOE is comprised of the following main components:

| Delivery item type | Identifier | Version |
|---|---|---|
| Hardware | TLX48 2RU Matrix Switch Chassis (TLX-MSC-020048) | Rev. B |
| | TLX48 2RU Matrix Switch Data Input/Output Card, 24 Ports, SFP+, 10G Multi-Mode (TLX-MSD-M00024) | Rev. A |
| | TLX48 2RU Matrix Switch Data Input/Output Card, 24 Ports, SFP+, 10G SingleMode (TLX-MSD-S00024) | Rev A |
| | TLX48 2RU Matrix Switch Data Input/Output Card, 24 Ports, SFP+, 6G Multi-Mode (TLX-MSD-MV0024) | Rev A |
| | TLX48 2RU Matrix Switch Data Input/Output Card, 24 Ports, SFP+, 6G Single-Mode (TLX-MSD-SV0024) | Rev A |
| Software | TLX48 2RU Firmware (SFT-TLX248-01) | 5.09.01 |

To ensure secure usage a set of guidance documents is provided, together with the TLX48 2RU Matrix Switch Chassis (TLX-MSC-020048). For details, see section 2.5 “Documentation” of this report.

## 2.2 Security Policy

The TOE has the following features:

- User Data Protection (enforces Data Separation SFP)

  Data shall flow between Transmitter Port group A and Receiver Port group B if and only if a deliberate logical connection has been established to connect A to B. There shall be no data flow between Transmitter Port Groups or Receiver Port Groups and any other physical port on the Switch.

  The use of a restrict or partition table in the system overrides any deliberate logical connection established between Transmitter Port A and Receiver Port B since the restrict policy disallows connection of a higher priority input to a lower priority output and the partition policy disallows connection of an input from one partition going to the output of another partition.

## 2.3 Assumptions and Clarification of Scope

### 2.3.1 Assumptions

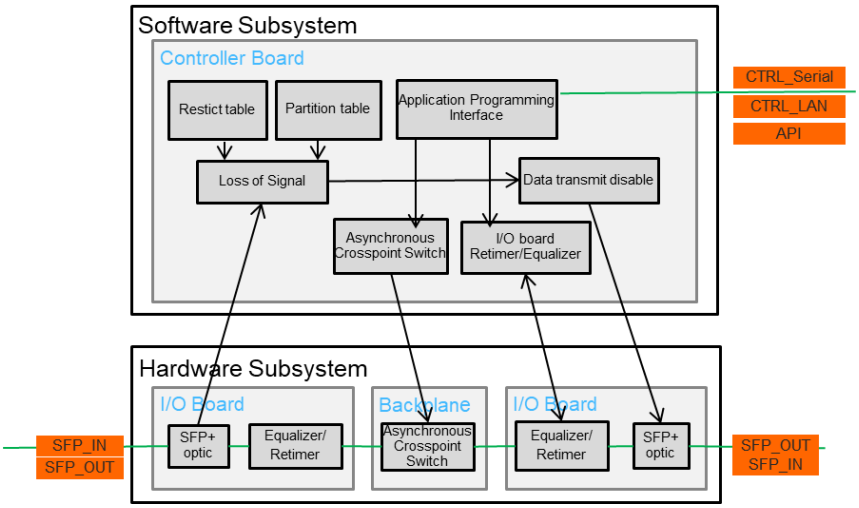
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

### 2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

## 2.4 Architectural Information

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:




## 2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

| Identifier | Version |
|---|---|
| TLX48 2RU Product Manual, May 2023 | Rev. E |
| TLX48 2RU Quick Start Guide | Rev. A |

## 2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

### 2.6.1 Testing approach and depth

The developer performed extensive testing on functional specification, subsystem and module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

The evaluator created additional test cases test to confirm verification of the version of the TOE / to supplement coverage of SFRs and/or TSFI / to further exercise the behaviour of critical functionality.

### 2.6.2 Independent penetration testing

Because the TOE is located in a physically protected environment where only trusted authorized administrator can access it and make any change (physical and logical) to it. The system user has very limited interaction with the TOE (switch the ports based on the restrictions, send hot key to make pre-defined connection, send key/mouse signal passing the TOE to the source, receive response from the source). Therefore, there is very limited attack surface and attack path to the TOE.

Due to the very limited attack path, the vulnerability analysis is performed in only three parts

- SFR Design Analysis: Based on the information obtained in the evaluation evidence, the SFR implementation details were examined. The aspects described in CEM annex B were considered. During this examination several potential vulnerabilities were identified.

- CWE Vulnerability focus: When the implementation of the SFR was understood, a coverage check were performed on the relevant aspects of all SFRs. This expanded the list of potential vulnerabilities.
- Public domain analysis: The evaluator performed public domain vulnerability search based on the TOE name, TOE type, and identified 3rd party security relevant libraries and/or services. Several additional potential vulnerabilities were identified during a search in the public domain.
- The potential vulnerabilities identified were analyzed, and some of the potential vulnerabilities were concluded not exploitable within in the Enhanced-Basic attack potential, or covered by guidance. For remaining potential vulnerabilities, penetration tests were devised.

The total test effort expended by the evaluators was 64 man hours. During that test campaign, 100% of the total time was spent on logical tests.

### 2.6.3 Test configuration

The TOE was tested in the following configuration:

- TLX Matrix Switch Chassis TLX-MSC-020048 REV B , quantity 1
- TLX Matrix Switch Controller Card TLX-MSM-C20048 REV A, quantity 2
- TLX Matrix Switch 48 Data I/O Card TLX-MSD-M00024 REV A, quantity 2

SFT-TLX248-01 v5.09.01

### 2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

## *2.7 Reused Evaluation Results*

There is no reuse of evaluation results in this certification.

## *2.8 Evaluated Configuration*

The TOE is defined uniquely by its name and version number TLX48 2RU Matrix Switch Chassis (TLX-MSC-020048).

## *2.9 Evaluation Results*

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Report(s) for the site(s) *[STAR]* [2].

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the TLX48 2RU Matrix Switch Chassis (TLX-MSC-020048), to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

## *2.10 Comments/Recommendations*

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

# 3 Security Target

The Thinklogical TLX48 2RU Matrix Switch Security Target, version 1.7, May 2023 *[ST]* is included here by reference.

# 4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

| | |
|---|---|
| IT | Information Technology |
| ITSEF | IT Security Evaluation Facility |
| JIL | Joint Interpretation Library |
| NSCIB | Netherlands Scheme for Certification in the area of IT Security |
| PP | Protection Profile |
| TOE | Target of Evaluation |

# 5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.


| | |
|---|---|
| [CC] | Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017 |
| [CEM] | Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017 |
| [ETR] | Evaluation Technical Report “ThinkLogical TLX48 2RU” – EAL4+, 22-RPT-998, Version 2.0, 02 June 2023 |
| [NSCIB] | Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019 |
| [ST] | Thinklogical TLX48 2RU Matrix Switch Security Target, version 1.7, May 2023 |
| [STAR] | Site Technical Audit Report - ThinkLogical Milford Development and Production site, 23-RPT-551, Version 2.0, dated 02 June 2023 |


(This is the end of this report.)