TÜVRheinland®
Precisely Right.

Certification Report

ZTE OTN Solution v1.10

Sponsor and developer: ***ZTE Corporation***
R&D Building 1, ZTE Industrial Plaza LiuXian Avenue Xili
Nanshan District, Shenzhen
P.R.C

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-0648132-CR**

Report version: **1**

Project number: **0648132**

Author(s): **Kjartan Jæger Kvassnes**

Date: **19 April 2023**

Number of pages: **12**

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

TÜVRheinland®
Precisely Right.

CONTENTS

TÜVRheinland®
Precisely Right.

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 ZTE OTN Solution v1.10. The developer of the ZTE OTN Solution v1.10 is ZTE Corporation located in Shenzhen, P.R.C. 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 the ZTE OTN solution aimed to build broadband and intelligent full connection for the ICT field in the 5G era. Based on cloud datacenters (DCs), ZTE OTN solution establishes large-capacity interconnection pipes between DCs and between DCs and services, to implement unified transport of fixed/wireless networks and vertical industries

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 27 June 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 ZTE OTN Solution v1.10, 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 ZTE OTN Solution v1.10 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 EAL3 augmented (EAL3+) 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 ZTE OTN Solution v1.10 from ZTE Corporation located in Shenzhen, P.R.C..

The TOE is comprised of the following main components:

Delivery item type	Identifier	Software version
Hardware models	ZXONE 9700 S3K ZXONE 9700 G2K ZXONE 9700 NX41 ZXONE 9700 OX42 ZXONE 9700 NXG0 ZXONE 9700 NXG1	ZXONE19700V1.10.010.002B500, including the following patches: ZXONE19700V1.10.010.002B500CP001 ZXONE19700V1.10.010.002B500CP002 ZXONE19700V1.10.010.002B500CP003
Hardware models	ZXONE 7000 C2	ZXONE7000V2.00R5B111, including the following patches: ZXONE7000V2.00R5B111_C01 ZXONE7000V2.00R5B111_C02
Hardware models	ZXMP M721 CX66A(E) ZXMP M721 CX63A(E) ZXMP M721 DX63(E)	ZXMPM721V5.10.070.001B100, including the following patches: ZXMPM721V5.10.070.001B100CP001 ZXMPM721V5.10.070.001B100CP002

To ensure secure usage a set of guidance documents is provided, together with the ZTE OTN Solution v1.10. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The major security features of the TOE are:

- Secure management and usage of the TOE, to ensure that only properly authorized staff can manage and/or use the TOE
- Secure interaction between various parts of the TOE and between the TOE and various machines in the environment, so that the management data and commands cannot be read or modified in-between
- Logging and auditing of user actions
- Information flow control for management traffic.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

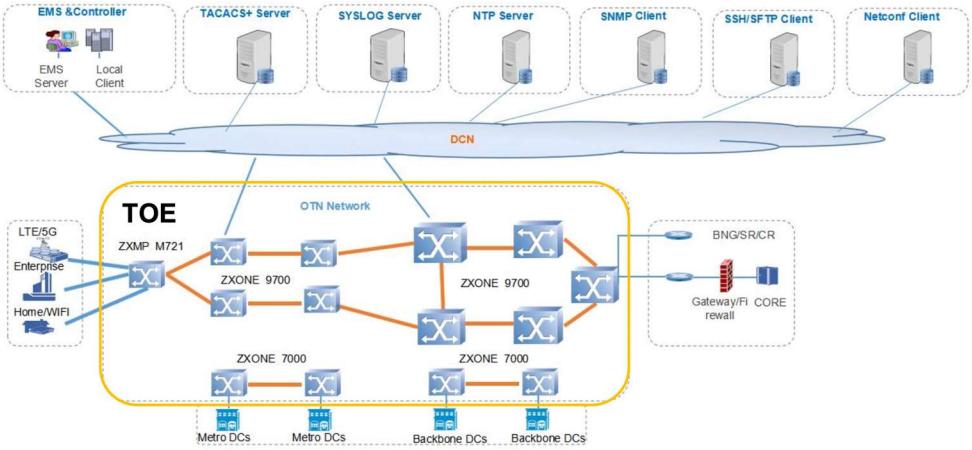
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

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 TOE is the ZTE OTN solution aimed to build broadband and intelligent full connection for the ICT field in the 5G era. Based on cloud datacentres (DCs), ZTE OTN solution establishes large-capacity interconnection pipes between DCs and between DCs and services, to implement unified transport of fixed/wireless networks and vertical industries.



The TOE is widely used in metro network (including core layer, aggregation layer, and access layer) and backbone network. They provide transmission solutions with various capacities, transmission distances, and intelligent service applications.

2.5 Documentation

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

Reference	Name	Version	Date
[UG CONF]	ZXONE 9700 ZXONE 7000 ZXMP M721 Common Criteria Security Evaluation - Certified Configuration	v3.0	2023-03-27
[UG CLI]	OTN Product CLI User Manual.en-US	V1.5,	2023-01-04
[UG QX]	OTN Product QX Interface Specification.en-US	V1.2,	2022-10-19
[UG-RTN]	ZXONE 9700 ZXONE 7000 ZXMP M721 Interface Specification Return Value.en-US	V1.0	N/A
[UG NETCONF]	ZXONE 7000 NETCONF Interface Specification.en-US	V1.3,	2023-01-04
[UG 9700]	ZXONE 9700 Quick Installation Guide	R1.7,	2019-07-18
	Unitrans ZXONE 9700 Packet OTN Equipment Routine Maintenance(V4.20)	R1.1,	2022-02-28
	Unitrans ZXONE 9700 Packet OTN Equipment Alarm Handling(V4.20)	R1.0,	2021-06-15
	Unitrans ZXONE 9700 Packet OTN Equipment Performance Reference(V4.20)	R1.0,	2021-06-15
	Unitrans ZXONE 9700 Packet OTN Equipment Security Description(V4.20)	R1.0,	2021-06-25

Reference	Name	Version	Date
	Unitrans ZXONE 9700 Packet OTN Equipment Hardware Description(V4.20)	R1.1,	2022-03-30
[UG 7000]	ZXONE 7000 Quick Installation Guide	R1.1,	2018-01-23
	Unitrans ZXONE 7000 Cloud OTN Equipment Routine Maintenance Guide(V2.00)	R1.0,	2019-07-03
	Unitrans ZXONE 7000 Cloud OTN Equipment Alarm Handling (V2.00)	R1.0,	2022-06-10
	Unitrans ZXONE 7000 Cloud OTN Equipment Performance Reference (V2.00)	R1.0,	2022-06-10
	Unitrans ZXONE 7000 Cloud OTN Equipment Security Description (V2.00)	R1.0,	2022-06-10
	Unitrans ZXONE 7000 Cloud OTN Equipment Hardware Description(V2.00)	R1.2,	2021-12-26
[UG M721]	ZXMP M721 Quick Installation Guide	R2.0,	2022-04-30
	Unitrans ZXMP M721 Metro-Edge OTN Equipment Routine Maintenance (V5.10)	R1.0,	2021-04-25
	Unitrans ZXMP M721 Metro-Edge OTN Equipment Alarm Handling (ZENIC ONE R22)(V5.10)	R1.0,	2021-06-30
	Unitrans ZXMP M721 Metro-Edge OTN Equipment Performance Reference (ZENIC ONE R22)(V5.10)	R1.0,	2021-06-30
	Unitrans ZXMP M721 Metro-Edge OTN Equipment Security Description(V5.10)	R1.0,	2021-06-10
	Unitrans ZXMP M721 Metro-Edge OTN Equipment Hardware Description(V5.10)	R1.4,	2022-08-27

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 based the functional test plan on the security function requirements defined in the ST and developer documents. These tests cover the security related aspects of the TOE functions. In total 30 test cases are defined in test plan which covers the SSH, QX and NETCONF interfaces consisting of 30 test cases. These test cases were then divided into four categories based on the security relevant subsystems.

The developer has performed all the test on all the TOE hardware models with the corresponding software packages specified in chapter 2.1.

The evaluator created additional test cases test to confirm verification of the version of the TOE to further exercise the behaviour of critical functionality.

2.6.2 Independent penetration testing

To identify potential vulnerabilities the evaluator performed the following activities:

- SFR design analysis: SFR implementation details were examined in the SFR design analysis. During this examination potential vulnerabilities were identified.
- CWE vulnerability focus: Using the CWE weaknesses collection, the evaluator collected a list of security questions and related answers. This approach ensured that the evaluator was forced to think in terms of vulnerabilities from all different angles and improved completeness in the vulnerability analysis. Also during this examination several potential vulnerabilities were identified.
- Use of Scanning tools: The evaluator runs vulnerability scanning tools to identify potential vulnerabilities.
- Public vulnerability search: Several additional potential vulnerabilities were identified during a search in the public domain.

The total test effort expended by the evaluators was 40 hours. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The evaluator has performed the tests on the following hardware models:

- ZXONE 9700 NXG1 running ZXONE 19700 V1.10.010.002B500 (with patches)
- ZXONE 7000 C2 running ZXONE 7000 V2.00R5B111 (with patches)
- ZXMP M721 DX63(E) running ZXMPM721 v5.10.070.001B100 (with patches)

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.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

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 ZTE OTN Solution v1.10.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

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

Based on the above evaluation results the evaluation lab concluded the ZTE OTN Solution v1.10, to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 3 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 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 ZTE OTN Solution Security Target v1.1, 18 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:

ACL	Access Control List
AES	Advanced Encryption Standard
BAC	Basic Access Control
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LAN	Local Area Network
MAC	Message Authentication Code
NSCIB	Netherlands Scheme for Certification in the area of IT Security
OTE	Optical Transmission Equipment
OTN	Optical Transmission Network
PP	Protection Profile
SSH	Secure Shell
TACACS+	Terminal Access Controller Access-Control System Plus
TOE	Target of Evaluation
VLAN	Virtual LAN

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 “ZTE OTN Solution v1.10” – EAL3+, 22-RPT-1377, Version 3.0, 19 May 2023
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	ZTE OTN Solution Security Target v1.1, 18 May 2023

(This is the end of this report.)