Certification Report

ZTE IPN Solution v1.2

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-2300138-01-CR**
Report version:	**1**
Project number:	**NSCIB-2300138-01**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**17 April 2024**
Number of pages:	**19**
Number of appendices:	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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, TrustCB 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 TrustCB 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 TrustCB 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, TrustCB 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.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

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 IPN Solution v1.2. The developer of the ZTE IPN Solution v1.2 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 focused on the requirements of core Internet nodes, backbone tandem nodes, core egress nodes of large MANs, and data centre gateways. 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

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 17 April 2024 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 IPN Solution v1.2, 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 IPN Solution v1.2 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).

TrustCB 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 IPN Solution v1.2 from ZTE Corporation located in Shenzhen, P.R.C..

The TOE is comprised of the following main components:

	Name		Version
Hardware	ZXCTN 9000-E Series Routers	ZXCTN 9000-3EA	N/A[2]
		ZXCTN 9000-8EA	
		ZXCTN 9000-18EA	
	ZXR10 5960M Series Switches	ZXR10 5960M-56QU-HI	
		ZXR10 5960M-4M-HI	
		ZXR10 5960M-8M-HI	
	ZXR10 5960X Series Switches	ZXR10 5960X-56QU-HF	
		ZXR10 5960X-54DU-HF	
		ZXR10 5960X-24U-HF	
		ZXR10 5960X-56QU-HG	
		ZXR10 5960X-54DU-HG	
	ZXR10 9900X Series Switches	ZXR10 9904X	
		ZXR10 9908X	
		ZXR10 9916X	
	ZXR10 M6000-2S Series Routers	ZXR10 M6000-2S6	
		ZXR10 M6000-2S16	
	ZXR10 M6000-S Series Routers	M6000-18S	
		M6000-8S	
		M6000-8S Plus	
		M6000-5S	
		M6000-3S	
		M6000-3S Plus	
	ZXR10 M6000-SE Series Routers	M6000-16SE	
		M6000-8SE	
		M6000-4SE	
Software	ZXCTN 9000-E series	9000E_5.00.10.72_rel.set	CTN9000-E V5.00.10.72

[2] TOE hardware model name is the hardware unique identifier and served as the version of the hardware

	Name		Version
	ZXR10 5960M Series	5960M_61P64.set patchname：V7.00.00.61P64_HP_348390.pat	5960 V7.00.00.61P64 patch version：ZXR10 5960V7.00.00.61P64_HP_348390
	ZXR10 5960X Series	5960X_LS2088A.set patch name：V6.00.03.92P02_HP_348390.pat	5900 V6.00.03.92P02 patch version：ZXR10 5960X V6.00.03.92P02_HP_348390
	ZXR10 9900X Series	base.set patch name: Patch-V1.00.30.01P26_HP_965767.pat	V1.00.30.01P26 patch version:V1.00.30.01P26_HP_965767
	ZXR10 M6000-2S Series Routers	ZXCTNM600090002E8A_V5.10.10.30B34.set	M6000V5.10.10.30
	ZXR10 M6000-S Series Routers	M6000-S_5.00.10.72_rel.set	M6000-S V5.00.10.72
	ZXR10 M6000-SE Series Routers	M6000-SE_V6.00.10.10_rel.set	M6000-SE V6.00.10.10

To ensure secure usage a set of guidance documents is provided, together with the ZTE IPN Solution v1.2. 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

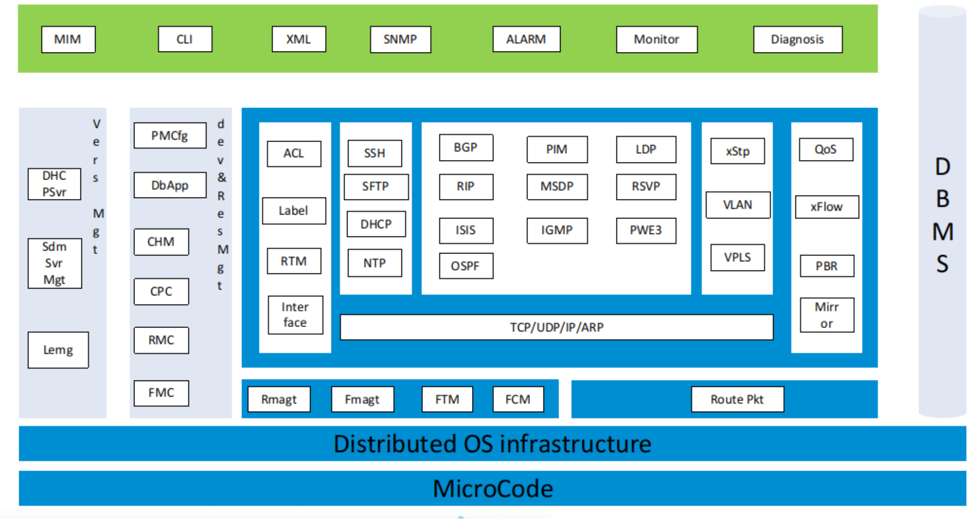
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

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 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:

Reference	Name	Version	Date
[UG CONF]	ZTE IPN Common Criteria Security Evaluation - Certified Configuration.pdf	R1.4,	2024-03-14
ZXCTN 9000-E Series Routers guidance	SJ-20230404101353-001-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform Safety Precautions.pdf	R1.0,	2023-04-18
	SJ-20230404101353-002-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform Product Description.pdf	R1.0,	2023-04-18
	SJ-20230404101353-003-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform Hardware Description.pdf	R1.0,	2023-04-18
	SJ-20230404101353-004-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform Feature Description.pdf	R1.0,	2023-04-18
	SJ-20230404101353-005-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform Security Description.pdf	R1.0,	2023-04-18
	SJ-20230404101353-006-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform Hardware Installation Guide.pdf	R1.0,	2023-04-18

Reference	Name	Version	Date
	SJ-20230404101353-007-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform License Operation Guide.pdf	R1.0,	2023-04-18
	SJ-20230404101353-008-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform Initial Configuration Guide_R1.1.pdf	R1.1,	2023-05-31
	SJ-20230404101353-009-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform Configuration Guide.pdf	R1.0,	2023-04-18
	SJ-20230404101353-010-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform Backup and Recovery.pdf	R1.0,	2023-04-18
	SJ-20230404101353-011-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform Routine Maintenance.pdf	R1.0,	2023-04-18
	SJ-20230404101353-012-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform Parts Replacement Guide.pdf	R1.0,	2023-04-18
	SJ-20230404101353-013-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform Troubleshooting.pdf	R1.0,	2023-04-18
	SJ-20230404101353-014-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform Emergency Maintenance.pdf	R1.0,	2023-04-18
	SJ-20230404101353-015-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform Alarm Handling.pdf	R1.0,	2023-04-18
	SJ-20230404101353-016-ZXCTN 9000-EA (V5.00.10.72) Carrier-Class Multi-Service Packet-Based Platform Command Reference.chm	R1.0,	2023-04-18
	SJ-20230404101353-017-ZXCTN 9000-EA (V5.00.10.72) Carrier Class Multi-Service Packet-Based Platform Security Hardening.pdf	R1.0,	2023-05-31
ZXR10 5960M Series Switches Guidance	SJ-20230817094310-001-ZXR10 5960M Series (V7.00.00.61) Data Center Switch Product Description.pdf	R1.0,	2023-08-30

Reference	Name	Version	Date
	SJ-20230817094310-002-ZXR10 5960M Series (V7.00.00.61) Data Center Switch Hardware Description.pdf	R1.0,	2023-08-30
	SJ-20230817094310-005-ZXR10 5960M Series (V7.00.00.61) Data Center Switch Hardware Installation Guide.pdf	R1.0,	2023-08-30
	SJ-20230817094310-008-ZXR10 5960M Series (V7.00.00.61) Data Center Switch Configuration Guide.pdf	R1.0,	2023-09-30
	SJ-20230817094310-009-ZXR10 5960M Series (V7.00.00.61) Data Center Switch Routine Maintenance.pdf	R1.0,	2023-09-30
	SJ-20230817094310-010-ZXR10 5960M Series (V7.00.00.61) Data Center Switch Troubleshooting.pdf	R1.0,	2023-09-30
	SJ-20230817094310-011-ZXR10 5960M Series (V7.00.00.61) Data Center Switch Alarm Handling.pdf	R1.0,	2023-09-30
ZXR10 5960X Series Switches Guidance	SJ-20230524100811-001-ZXR10 5960X Series (V6.00.03.92) Data Center Core Switch Product Description.pdf	R1.0,	2023-07-30
	SJ-20230524100811-002-ZXR10 5960X Series (V6.00.03.92) Data Center Core Switch Hardware Description.pdf	R1.0,	2023-07-30
	SJ-20230524100811-003-ZXR10 5960X Series (V6.00.03.92) Data Center Core Switch Hardware Installation Guide.pdf	R1.0,	2023-07-30
	SJ-20230524100811-004-ZXR10 5960X Series (V6.00.03.92) Data Center Core Switch Initial Configuration Guide.pdf	R1.0,	2023-06-30
	SJ-20230524100811-005-ZXR10 5960X Series (V6.00.03.92) Data Center Core Switch Security Hardening.pdf	R1.0,	2023-06-30
	SJ-20230524100811-006-ZXR10 5960X Series (V6.00.03.92) Data Center Core Switch Configuration Guide.pdf	R1.0,	2023-07-20
	SJ-20230524100811-007-ZXR10 5960X Series (V6.00.03.92) Data Center Core Switch Routine Maintenance.pdf	R1.0,	2023-06-30
	SJ-20230524100811-008-ZXR10 5960X Series (V6.00.03.92) Data Center Core Switch Troubleshooting.pdf	R1.0,	2023-07-15
	SJ-20230524100811-009-ZXR10 5960X Series (V6.00.03.92) Data Center Core Switch Alarm Handling.pdf	R1.0,	2023-07-15

Reference	Name	Version	Date
	SJ-20230524100811-011-ZXR10 5960X Series (V6.00.03.92) Data Center Core Switch Feature Description.pdf	R1.0,	2023-07-15
ZXR10 9900X Series Switches Guidance	SJ-20230210102038-002-ZXR10 9900X Series (V1.00.30) Data Center Core Switch Product Description.pdf	R1.0	2023-06-30
	SJ-20230210102038-003-ZXR10 9900X Series (V1.00.30) Data Center Core Switch Hardware Description.pdf	R1.0	2023-06-30
	SJ-20230210102038-005-ZXR10 9900X Series (V1.00.30) Data Center Core Switch Hardware Installation Guide.pdf	R1.0	2023-06-30
	SJ-20230210102038-007-ZXR10 9900X Series (V1.00.30) Data Center Core Switch Routine Maintenance.pdf	R1.0	2023-06-30
	SJ-20230210102038-008-ZXR10 9900X Series (V1.00.30) Data Center Core Switch Parts Replacement Guide.pdf	R1.0	2023-06-30
	SJ-20230210102038-009-ZXR10 9900X Series (V1.00.30) Data Center Core Switch Troubleshooting.pdf	R1.0	2023-06-30
	SJ-20230210102038-013-ZXR10 9900X Series (V1.00.30) Data Center Core Switch Initial Configuration Guide.pdf	R1.0	2023-06-30
	SJ-20230210102038-014-ZXR10 9900X Series (V1.00.30) Data Center Core Switch Security Hardening.pdf	R1.0	2023-06-30
ZXR10 M6000-2S Series Routers Guidance	SJ-20230202173055-001-ZXR10 M6000-2S (V5.10.10.30) Safety Precautions.pdf	R1.0	2023-02-28
	SJ-20230202173055-002-ZXR10 M6000-2S (V5.10.10.30) Security Description.pdf	R1.0	2023-02-28
	SJ-20230202173055-003-ZXR10 M6000-2S (V5.10.10.30) Commissioning Guide.pdf	R1.0	2023-01-30
	SJ-20230202173055-004-ZXR10 M6000-2S (V5.10.10.30) Initial Configuration Guide.pdf	R1.0	2023-01-30
	SJ-20230202173055-005-ZXR10 M6000-2S (V5.10.10.30) Configuration Guide (System Management).pdf	R1.0	2023-03-30
	SJ-20230202173055-006-ZXR10 M6000-2S (V5.10.10.30) Configuration Guide (Interface Management).pdf	R1.0	2023-03-30
	SJ-20230202173055-007-ZXR10 M6000-2S (V5.10.10.30) Configuration Guide (IP Service).pdf	R1.0	2023-01-30

Reference	Name	Version	Date
	SJ-20230202173055-008-ZXR10 M6000-2S (V5.10.10.30) Configuration Guide (IP Routing).pdf	R1.0	2023-03-30
	SJ-20230202173055-009-ZXR10 M6000-2S (V5.10.10.30) Configuration Guide (IP Multicast).pdf	R1.0	2023-03-30
	SJ-20230202173055-010-ZXR10 M6000-2S (V5.10.10.30) Configuration Guide (MPLS).pdf	R1.0	2023-03-30
	SJ-20230202173055-011-ZXR10 M6000-2S (V5.10.10.30) Configuration Guide (VPN).pdf	R1.0	2023-01-30
	SJ-20230202173055-012-ZXR10 M6000-2S (V5.10.10.30) Configuration Guide (QoS).pdf	R1.0	2023-01-30
	SJ-20230202173055-013-ZXR10 M6000-2S (V5.10.10.30) Configuration Guide (Security).pdf	R1.0	2023-03-30
	SJ-20230202173055-014-ZXR10 M6000-2S (V5.10.10.30) Configuration Guide (Reliability).pdf	R1.0	2023-03-30
	SJ-20230202173055-015-ZXR10 M6000-2S (V5.10.10.30) Configuration Guide (SR).pdf	R1.0	2023-03-30
	SJ-20230202173055-016-ZXR10 M6000-2S (V5.10.10.30) Configuration Guide (SRv6).pdf	R1.0	2023-03-30
	SJ-20230202173055-017-ZXR10 M6000-2S (V5.10.10.30) Backup and Recovery.pdf	R1.0	2023-03-30
	SJ-20230202173055-018-ZXR10 M6000-2S (V5.10.10.30) Routine Maintenance.pdf	R1.0	2023-03-30
	SJ-20230202173055-019-ZXR10 M6000-2S (V5.10.10.30) Fault Management Overview.pdf	R1.0	2023-02-28
	SJ-20230202173055-020-ZXR10 M6000-2S (V5.10.10.30) Emergency Handling.pdf	R1.0	2023-02-28
	SJ-20230202173055-021-ZXR10 M6000-2S (V5.10.10.30) Alarm Handling.pdf	R1.0	2023-02-28
	SJ-20230202173055-022-ZXR10 M6000-2S (V5.10.10.30) Troubleshooting.pdf	R1.0	2023-02-28
	SJ-20230202173055-023-ZXR10 M6000-2S (V5.10.10.30) Fault Information Collecting.pdf	R1.0	2023-03-30
	SJ-20230202173055-024-ZXR10 M6000-2S (V5.10.10.30) Performance Reference.pdf	R1.0	2023-03-31

Reference	Name	Version	Date
	SJ-20230202173055-025-ZXR10 M6000-2S (V5.10.10.30) Command Reference.chm	R1.1	2023-06-30
ZXR10 M6000-S Series Routers Guidance	SJ-20230220175532-001-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Safety Precautions.pdf	R1.0	2023-02-28
	SJ-20230220175532-002-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Product Description.pdf	R1.0	2023-02-28
	SJ-20230220175532-003-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Hardware Description.pdf	R1.0	2023-02-28
	SJ-20230220175532-004-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Feature Description.pdf	R1.0	2023-02-28
	SJ-20230220175532-005-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Security Description.pdf	R1.0	2023-02-28
	SJ-20230220175532-006-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Hardware Installation Guide.pdf	R1.0	2023-02-28
	SJ-20230220175532-007-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router License Operation Guide.pdf	R1.0	2023-02-28
	SJ-20230220175532-008-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Initial Configuration Guide_R1.1.pdf	R1.1	2023-05-31
	SJ-20230220175532-009-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Configuration Guide.pdf	R1.0	2023-02-28
	SJ-20230220175532-010-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Backup and Recovery.pdf	R1.0	2023-02-28
	SJ-20230220175532-011-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Routine Maintenance.pdf	R1.0	2023-02-28
	SJ-20230220175532-012-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Parts Replacement Guide.pdf	R1.0	2023-02-28
	SJ-20230220175532-013-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Troubleshooting.pdf	R1.0	2023-02-28
	SJ-20230220175532-014-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Emergency Maintenance.pdf	R1.0	2023-02-28

Reference	Name	Version	Date
	SJ-20230220175532-015-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Alarm Handling.pdf	R1.0	2023-02-28
	SJ-20230220175532-016-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Command Reference.chm	R1.0	2023-02-28
	SJ-20230220175532-017-ZXR10 M6000-S (V5.00.10.72) Carrier-Class Router Security Hardening.pdf	R1.0	2023-05-31
ZXR10 M6000-SE Series Routers Guidance	SJ-20230727183755-001-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router Safety Precautions.pdf	R1.0	2023-10-20
	SJ-20230727183755-002-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router Product Description.pdf	R1.0	2023-10-20
	SJ-20230727183755-003-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router Hardware Description.pdf	R1.0	2023-10-20
	SJ-20230727183755-004-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router Feature Description.pdf	R1.0	2023-10-20
	SJ-20230727183755-005-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router Security Description.pdf	R1.0	2023-10-20
	SJ-20230727183755-006-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router Hardware Installation Guide.pdf	R1.0	2023-10-20
	SJ-20230727183755-007-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router Initial Configuration Guide.pdf	R1.0	2023-03-06
	SJ-20230727183755-008-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router License Operation Guide.pdf	R1.0	2023-10-20
	SJ-20230727183755-009-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router Configuration Guide.pdf	R1.0	2023-10-20
	SJ-20230727183755-010-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router Security Hardening.pdf	R1.0	2023-10-20
	SJ-20230727183755-011-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router Parts Replacement Guide.pdf	R1.0	2023-10-20
	SJ-20230727183755-012-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router Routine Maintenance.pdf	R1.0	2023-10-20

Reference	Name	Versio n	Date
	SJ-20230727183755-013-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router Backup and Recovery.pdf	R1.0	2023-10-20
	SJ-20230727183755-014-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router Emergency Maintenance.pdf	R1.0	2023-10-20
	SJ-20230727183755-015-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router Alarm Handling.chm	R1.0	2023-10-20
	SJ-20230727183755-016-ZXR10 M6000-SE (V6.00.10.10) Carrier-Class Router Troubleshooting.pdf	R1.0	2023-10-20

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 and 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 3.5 weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The evaluator performed the tests on the following hardware models and software versions:

Series	Hardware Model	Software Version
ZXCTN 9000-E	ZXCTN 9000-8EA	CTN9000-E V5.00.10.72
ZXR10 5960M	ZXR10 5960M-4M-HI	ZXR10 5960 V7.00.00.61P64 with patch ZXR10 5960 V7.00.00.61P64_HP_348390
ZXR10 5960X	ZXR10 5960X-56-QU-HF	5900 V6.00.03.92P02 with patch ZXR 10 5960X V6.00.03.92P02_HP_348390
ZXR10 9900X	ZXR10 9904X	V1.00.30.01P26 with patch V1.00.30.01P26_HP_965767
ZXR10 M6000-2S	ZXR10 M6000-2S16	M6000 V5.10.10.30
ZXR10 M6000S	ZXR10 M6000-3S	M6000-S V5.00.10.72
ZXR10 M6000SE	ZXR10 M600016SE	M6000-SE V6.00.10.10

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 has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 4 Site Audit Reports.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number ZTE IPN Solution v1.2.

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 IPN Solution v1.2, 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.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: <none>.

3 Security Target

The ZTE IPN Solution Security Target, Version 1.1, Dated 14 March 2024 *[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 “ZTE IPN Solution v1.2” – EAL3, 23-RPT-1253, Version 3.0, Dated 15 March 2024

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022

[ST] ZTE IPN Solution Security Target, Version 1.1, Dated 14 March 2024

(This is the end of this report.)