EUCC Certification Report

ZTE IPN Solution v1.2

Sponsor and developer:	***ZTE Corporation*** **ZTE Plaza, Keji Road South, Hi-Tech Industrial Park,** **Nanshan District, Shenzhen,** **Guangdong** **P.R China**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**EUCC-3110-2026-2500103-01 Certification Report**
Report version:	**1.0**
Project number:	**EUCC-2500103-01**
Author(s):	**Haico Haak, TrustCB B.V.** **contact: eucc@trustcb.com**
Date:	**04 July 2026**
Number of pages:	**22**
Number of appendices:	**0**

CONTENTS

Foreword

The Common Criteria-based European Cybersecurity Certification Scheme (EUCC) is a certification scheme created under the Cybersecurity Act (CSA), Regulation (EU) 2019/881 of 17 April 2019.

The EUCC is described by Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

The Dutch implementation of the CSA is regulated in Dutch law in the 'Uitvoeringswet cyberbeveiligingsverordening' (UITVW). In this law the role of NCCA is assigned to the Dutch Authority for Digital Infrastructure (RDI), which is part of the Ministry of Economic Affairs.

TrustCB B.V. has been licensed by the RDI as a Certification Body (CB) for the task of ISO/IEC 17065 Certification Activities up to and including CSA assurance level high for ICT security products, as well as for protection profiles. Part of the procedure is the technical examination (evaluation) of the product, protection profile according to the NP002 EUCC processes published by the Dutch NCCA.

Evaluations of ICT products are performed by an IT Security Evaluation Facility (ITSEF) licensed by the Dutch NCCA as a CAB for ISO/IEC 17025 Evaluation Activities, with scope aligning to the requested Evaluation Assurance Level of the Object for the evaluation, referred to as the Target of Evaluation (TOE) in this report.

By awarding an EUCC certificate as a Common Criteria certificate, TrustCB B.V. asserts that the ICT product complies with the security requirements specified in the associated 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 security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the ICT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the ICT product satisfies the security requirements stated in the security target.

International recognition of the certificate

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of published 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.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the ZTE IPN Solution v1.2, identified in this document as either the ICT Product or as the Target of Evaluation (TOE).

The developer of the ICT Product is ZTE Corporation located in Shenzhen, P.R. China and they also act as the sponsor of the evaluation and certification.

This Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the ICT 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.

A certification procedure was conducted on the TOE by TrustCB B.V., in accordance with the provisions of the EUCC as described in Commission implementing regulation (EU) 2024/482 of 31 January 2024, amended by (EU) 2024/3144 of 18 December 2024 and (EU) 2025/2462 of 8 December 2025.

The successful completion of the certification procedure resulted in TrustCB issuing an EUCC certificate, The certificate identifier is **EUCC-3110-2026-2500103-01**, dated 04-07-2026 and with a 5-year validity.

The evaluation of the TOE was performed by SGS Brightsight located in Delft, the Netherlands. The evaluation was completed on 29-06-2026 with the issuance of the evaluation technical report *[ETR]*. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CC:2022, R1 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 R1 *[CC]* (Parts 1, 2, 3, 4, 5).

The scope of the evaluation was defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the ICT Product, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements.

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 AVA_VAN level applied during the evaluation was AVA_VAN.2. This assurance level is recognised by article 52 of [CSA] as ‘substantial’.

Consumers of this ICT Product 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.

TrustCB B.V., as Certification Assessment Body licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC high certification activities, declares that the product will be listed on the ENISA EU Cybersecurity Certificates list and that the evaluation meets all the conditions for international recognition of Common Criteria Certificates.

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 ICT Product details

2.1 Identification of the ICT Product

The Target of Evaluation (TOE) for this evaluation is ICT product ZTE IPN Solution v1.2 from ZTE Corporation located in Shenzhen, P.R. China.

The TOE is comprised of the following main components:

Delivery item type	Identifier		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
	ZXR10 5960M Series	5960M_61P64.set Patchname :	5960 V7.00.00.61P64 patch version : ZXR10 5960V7.00.00.61P64_H

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

Delivery item type	Identifier		Version
		V7.00.00.61P64_HP_348390.pat	P_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

Additional requirements for the operational environment of the certified ICT product are described in section 4.2 of the *[ST]*.

To ensure secure usage a set of guidance documents is provided with the TOE. For details, see section 2.6 of this report, “Supplementary Cybersecurity Information.

2.2 Contact information related to the evaluation of the ICT Product

Holder of the EUCC Certificate

Organisation name:	ZTE Corporation
Address:	ZTE Plaza, Keji Road South, Hi-Tech, Industrial Park, Nanshan District, Shenzhen, Guangdong, P.R. China
Certified product contact details	GCTC@zte.com.cn

Developer of the certified ICT Product

ICT product developer	ZTE Corporation

Identification of CAB

The Certification Assessment Body for this ICT Product is TrustCB B.V. TrustCB is licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC certification activities up to and including EUCC High.

TrustCB point of contact: EUCC@trustcb.com

Identification of ITSEF

Evaluation and testing for this ICT Product was performed by following ITSEF:

SGS Brightsight in Delft, the Netherlands

2.3 Security services and policies

2.3.1 Security services

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.

2.3.2 Vulnerability management

The following vulnerability policy has been identified as applicable to the ZTE IPN Solution v1.2

Document reference: ZTE Vulnerability Management and Disclosure Policy V2.0, 20 October 2025

2.3.3 Assurance Continuity policies

This is a new product certification. An assurance continuity policy was not provided.

2.3.4 Lifecycle management processes and production facilities

Not applicable to this evaluation.

2.3.5 Patch management process

Not applicable to this evaluation.

2.4 Assumptions and Clarification of Scope

2.4.1 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]*.

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE and its configuration in the environment to fulfil all Assumptions described in the *[ST]*.

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.

2.4.2 Clarification of scope

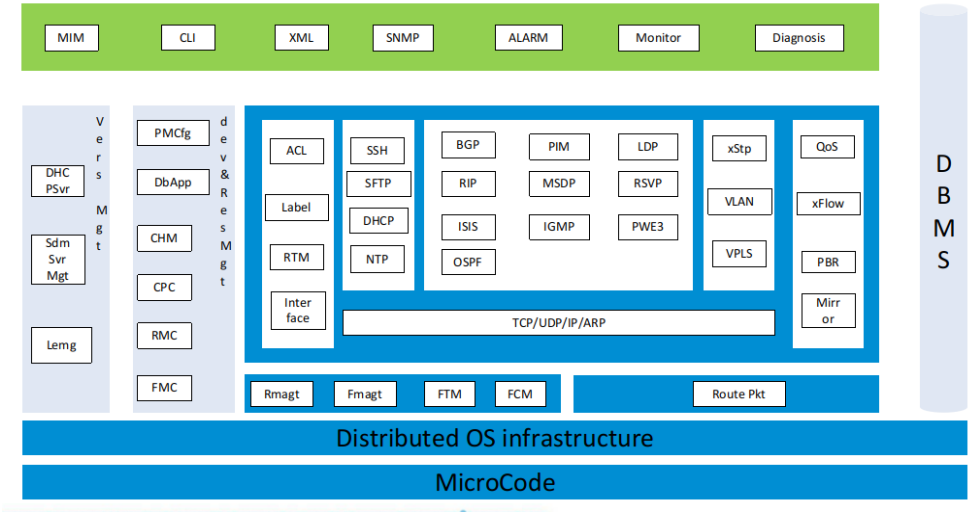
Considering all Assumptions above, the evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

Threats addressed by the TOE are presented in Section 4.1 of *[ST]*. The assumed level of expertise of the attacker for all identified threats is Basic.

No Organizational Security Polices (OSPs) have been defined for this TOE.

2.5 Architectural Information

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



2.6 Supplementary Cybersecurity Information

The following website link was provided for the ZTE IPN Solution v1.2 for the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881:

https://www.zte.com.cn/global/about/trust-center/ipn_products.html

This link provides further details and links on:

- Guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ZTE IPN Solution v1.2.
- The period during which the ZTE IPN Solution v1.2 security support will be offered to end users, in particular as regards the availability of cybersecurity related updates, is stated as 5 years aligned with the validity of the issued EUCC certificate.
- Contact information and accepted method for receiving vulnerability information from end users and security researchers for the ZTE IPN Solution v1.2. (https://www.zte.com.cn/global/about/trust-center/ztepsirt.html)
- the online repository listing publicly disclosed vulnerabilities related to the ZTE IPN Solution v1.2 and to any relevant cybersecurity advisories. (https://support.zte.com.cn/zte-iccp-isupport-webui/support/bulletin/security?code=bulletin%E2%8C%A9=en_US&t=0.5982917545557167)

Note: The following documentation, guidance and recommendations, is provided with the product by the developer to the customer to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ZTE IPN Solution v1.2:

Reference	Name	Version	Date
[UG CONF]	ZTE IPN Common Criteria Security Evaluation - Certified Configuration.pdf	R1.6,	2025-12-09
[UG CLI]	ZTE IPN Product CLI User Manual	R1.5,	2024-03-14
[UG NETCONF]	ZTE IPN NETCONF Interface Specification	R1.1,	2024-03-08
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

Reference	Name	Version	Date
	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
	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

Reference	Name	Version	Date
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
	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	R1.1,	2023-08-15
	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
	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

Reference	Name	Version	Date
	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
	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	R1.0	2023-02-28

Reference	Name	Version	Date
	Description.pdf		
	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
	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	R1.0	2023-10-20

Reference	Name	Version	Date
	Description.pdf		
	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
	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

3 Evaluation summary

3.1 Identification of used assurance components

The assurance components used in the product testing were:

- **EAL 3 augmented with ALC_FLR.2**

as defined by, and detailed in, *[CC]* and *[CEM]*.

3.2 EUCC State of the Art documents and Protection Profiles

Not applicable to this evaluation.

3.3 ICT 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.

3.3.1 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.

3.3.2 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.

3.3.3 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

Testing of these hardware models was considered representative of all the hardware models in each Series.

3.3.4 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.

3.4 ICT Product evaluation

3.4.1 Reused evaluation results

This was a new certification under EUCC.

3.4.2 Evaluated configuration

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

3.4.3 Assessment against each assurance requirement

ASE

ASE	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1
Security objectives	ASE_OBJ.2
Extended components definition	ASE_ECD.1
Security requirements	ASE.REQ.2
TOE summary specification	ASE.TSS.1

The findings are well-documented and internally consistent, demonstrating a thorough understanding of the Security Target *[ST]* and its components. The TOE introduction, conformance claim, security problems, security objectives, security requirements, TOE summary specification are appropriately addressed, and the TOE description is accurate and adequate for the evaluation level. Consequently, the ASE activities fulfil the assurance requirements EAL3 augmented with ALC_FLR.2. No issues or deviations were identified.

ADV

ADV	
Security architecture	ADV_ARC.1
Functional specification	ADV_FSP.3
TOE design	ADV_TDS.2

The evaluation has demonstrated that the developer's evidence meets ADV specified requirements. The TOE model is complete, clearly showing all interfaces (TSFI/non-TSFI), user roles, and relations, with explanations on completeness and tracing requirements met. The subsystem level model is sensible, useful, and shows TSFIs and subsystem decomposition. The behaviour of each subsystem and its interaction with other subsystems is explained. The security architecture is thoroughly explained, design compliance rationale is complete and coherent, and necessary evidence is extracted per alternative approach. The evaluation presents for each SFR, how the TSFIs, subsystems provide this SFR, using the TOE, diagrams, screenshots, etc. The evaluation describes the roles of the TSFIs and subsystems in meeting these SFRs. Accordingly, the ADV activities meet the assurance requirements for EAL3 augmented with ALC_FLR.2, with no issues or deviations identified.

AGD

AGD	
Operational user guidance	AGD_OPE.1
Preparative procedures	AGD_PRE.1

The evaluation has demonstrated that the guidance documentation is clear, complete, and sufficient to support the secure acceptance, installation, configuration, and operation of the TOE within its intended environment by its user roles. The guidance effectively helps prevent common misconfigurations and promotes correct usage. Therefore, the AGD activities fulfil the assurance requirements for EAL3 augmented with ALC_FLR.2, with no issues or deviations identified.

ALC

ALC	
CM capabilities	ALC_CMC.3
CM Scope	ALC_CMS.3
Delivery	ALC_DEL.1
Development security	ALC_DVS.1
Life cycle definition	ALC_LCD.1
Flaw remediation	ALC_FLR.2

The evaluation has demonstrated that the developer's evidence meets ALC specified. The CI-list was comprehensive and uniquely identified all configuration items, with clear identification of the developer. The CM documentation effectively described unique identification methods, a CM plan for development, procedures for accepting modified or new CIs, and the CM system was operated in accordance with the CM plan to maintain all configuration items by automated means. The CM System allows authorized changes only. Delivery procedures were well-documented, ensuring security during TOE distribution. Flaw remediation procedures were comprehensive, including methods for receiving reports, tracking flaws, providing corrective actions, and updating users. Accordingly, the ALC activities satisfy the assurance requirements for EAL3 augmented with ALC_FLR.2, with no issues or deviations identified.

ATE

ATE	
Coverage	ATE_COV.2
Depth	ATE_DPT.1
Functional tests	ATE_FUN.1
Independent testing	ATE_IND.2

The evaluation has demonstrated that the developer's evidence for ATE requirements meets all specified requirements. The testing approach used by the developer effectively covered the TSFIs. The developer's rationale for testing all TSFIs was presented and verified. The developer test results show that for all tests the results were pass. For the evaluator's independent testing, the overall approach for test selection, goals for the witnessing session, and independent test plan were clearly outlined. The evaluator's testing results showed that all sampled tests were passed. Accordingly, the ATE activities satisfy the assurance requirements for EAL3 augmented with ALC_FLR.2, with no issues or deviations identified.

AVA

AVA	
Vulnerability analysis	AVA_VAN.2

The penetration tests were defined and performed. The overall conclusion is that the TOE is protected against attackers possessing a basic attack potential, under the condition that the TOE user guidance is followed. Consequently, the AVA activities were performed in full compliance with the assurance requirements EAL3 augmented with ALC_FLR.2, providing a substantial level of confidence in the TOE's resistance to exploitation.

3.5 Results of the evaluation

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

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

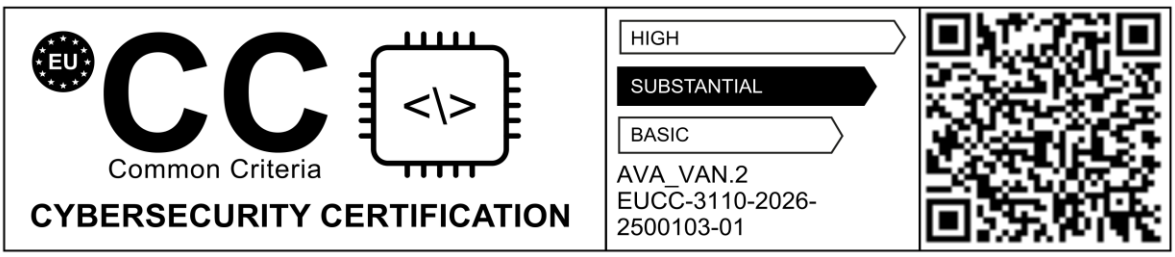
Based on the evaluation results the evaluation lab concluded the ZTE IPN Solution v1.2, to be **CC:2022 R1 1 Part 2 conformant, CC:2022 R1 Part 3 conformant**, at an assurance level recognised by article 52 of [CSA] as '**Substantial**' with **AVA_VAN 2** and to meet the requirements of **EAL 3 augmented with ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

3.6 Certificate information and scheme label

A Certificate has been issued recognising this evaluation result as follows:

Unique identifier: EUCC-3110-2026-2500103-01

Date of issuance: 04-07-2026 and with a validity period of **5 years**.



3.7 Comments and Recommendations

The user guidance as outlined in section 2.6 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.

4 Security Target

The certification references the following security target:

ZTE IPN Solution Security Target, Version 1.5, Dated 09 December 2025 *[ST]*.

5 Glossary

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

CM	Configuration Management
DCN	Data Communications Network
EMS	Equipment Management System
IP	Internet Protocol
IT	Information and communication technologies product as defined by [EUCC]
ITSEF	IT Security Evaluation Facility
MAC	Media Access Control
NMS	Network Management System
NNI	Network-to-network Interface
NTP	Network Time Protocol
IPN	Internet Protocol Network
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transmission Control Protocol
TRNG	True Random Number Generator
TOE	Target of Evaluation; the object of the certification activity described by this report
VLAN	Virtual LAN

6 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, CC:2022 Parts 1, 2, 3, 4 and 5, R1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 R1, November 2022
[CCMB-2024-002]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1
[DEV_DOCS]	ZTE IPN Common Criteria Security Evaluation - Certified Configuration.pdf, R1.6, 2025-12-09
	ZTE IPN Product CLI User Manual, R1.5, 2024-03-14
	ZTE IPN NETCONF Interface Specification, R1.1, 2024-03-08
	The specific user guidance for each series are listed in section 2.6 of this document, Supplementary Cybersecurity Information
	IPN Configuration Management Scope, Version 1.3
[ETR]	Evaluation Technical Report “ZTE IPN Solution v1.2” – EAL3 augmented, 25-RPT-1621, Version 2.0, Dated 29 June 2026
[EU-CSA]	REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[EU-EUCC]	COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
[EU-EUCC-amdt.1]	Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
[EU-EUCC-amdt.2]	Commission Implementing Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art documents
[ST]	ZTE IPN Solution Security Target, Version 1.5, Dated 09 December 2025

(This is the end of this report.)