TÜVRheinland®
Precisely Right.

Certification Report

ZTE 5G-RAN Solution V3.00.30.20P10

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

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

Report number:	**NSCIB-CC-0132539-CR**
Report version:	**1**
Project number:	**0132539**
Author(s):	**Brian Smithson**
Date:	**07 April 2021**
Number of pages:	**13**
Number of appendices:	**0**

Headoffice:
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 Dutch Chamber of Commerce 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 license 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, in order 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

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the ZTE 5G-RAN Solution V3.00.30.20P10. The developer of the ZTE 5G-RAN Solution V3.00.30.20P10 is ZTE Corporation located in Shenzhen, P.R. China 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 New Generation Radio Access Network (NG-RAN) system solution for NR (new radio) network plus an UME. The solution interfaces with User Equipment (UE) and implements such functions as radio resource management, data stream IP header compression and encryption, attach progress selection, user plane data routing, data scheduling and transmission, and mobility management. The UME is used to manage the system via web interface.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 30 March 2021 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 5G-RAN Solution V3.00.30.20P10, 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 5G-RAN Solution V3.00.30.20P10 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 provides 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 and *[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. It should be noted that the certification results only apply 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 releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the ZTE 5G-RAN Solution V3.00.30.20P10 from ZTE Corporation located in Shenzhen, P.R. China.

The TOE is comprised of the following main components:

BBU Hardware and Software Components

Delivery item type	Identifier	Version
Hardware	BBU	V9200
Software	BBU	NR: V3.00.30.20P10

RRU Hardware and Software Components

Delivery item type	Identifier	Version
Hardware	RRU	R9105 R9212 R8998 R8894 R8854 R9222 R9214 R8862 R8852
Software	RRU	V3.00.30.20P10

AAU Hardware and Software Components

Delivery item type	Identifier	Version
Hardware	AAU	A9611 A9815 A9631 A9622
Software	AAU	V3.00.30.20P10

UME Software Components

Delivery item type	Identifier	Version
Software	UME Server version ElasticNet UME	V16.20.30
	SSH Server (Apache SSHD)	V2.1.0
	SFTP Server (Apache-sshd-core)	V2.2.0
	LDAP server (ApacheDS)	V2.0.0-M24

To ensure secure usage a set of guidance documents is provided together with the ZTE 5G-RAN Solution V3.00.30.20P10. Details can be found in section 2.5 of this report.

2.2 Security Policy

The major security features of the ZTE 5G-RAN Solution V3.00.30.20P10 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 user data and/or management commands cannot be read or modified in between; and,
- Logging and auditing of user actions.

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 3.4 of the *[ST]*.

2.3.2 Clarification of scope

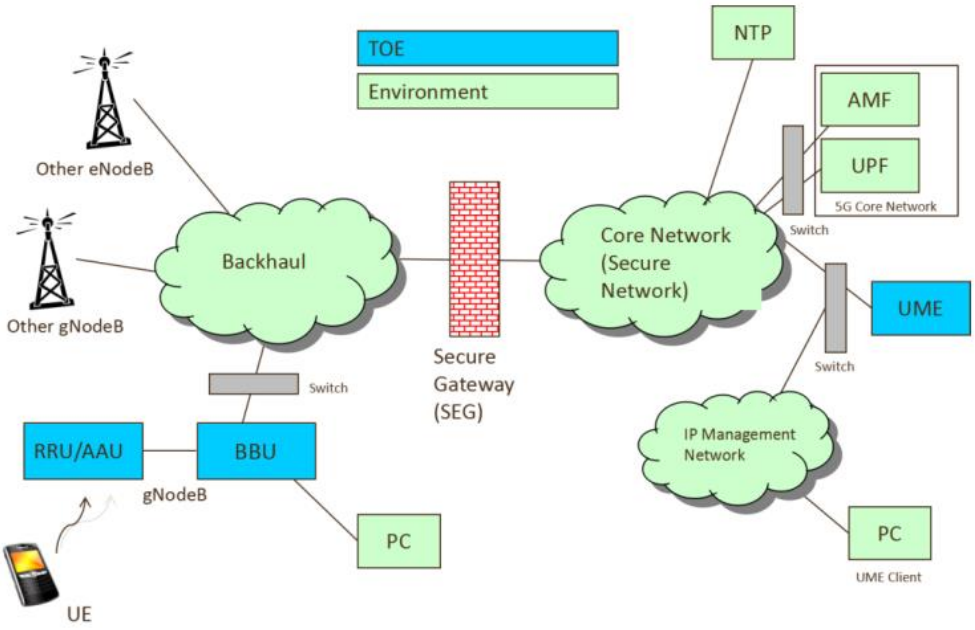
The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The TOE consists of three parts: a Baseband Unit (BBU), a Remote RF unit (RRU) or Active Antenna Unit (AAU), and a Unified Management Expert (UME).

- BBU is the device processing the analogue to digital conversion of the signal.
- RRU is the remote radio unit transceiver.
- AAU is a radio frequency processing module and antenna.
- UME is a unified intelligent operation and maintenance system for RAN. UME provides the intelligent operation and maintenance management of network and the on-demand deployment and the gray-scale based upgrade of system.

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



The TOE has the following features:

- 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 user data and/or management commands cannot be read or modified in between; and,
- Logging and auditing of user actions.

2.5 Documentation

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

Reference	Name	Version	Date
[UG-BBU-ACP]	UG-BBU-ACP Acceptance procedure	0.4	2021/02/03
[UG-BBU-CONF]	RAN Configuration Management	1.3	2020/09/23
[UG-BBU-HW-DES]	ZXRAN V9200 Radio Access Network Product Description	2.0	2019/10/08
[UG-BBU-HW-INS]	ZXRAN V9200 Radio Access Network Hardware Installation	2.0	2019/10/08
[UG-BBU-OPE]	RAN Element Management	1.0	2020/07/26
[UG-BBU-SW-INS]	ZXRAN Base Station Commissioning Guide (Image Burning)	1.2	2020/04/28
[UG-UME-ACP]	UG-UME-ACP Acceptance procedure	0.3	2021/02/03
[UG-UME-INS]	UME Installation and Deployment Guide	1.3	2020/09/11
[UG-UME-LE]	Security Log Events	1.0	NA
[UG-UME-MML]	UME Command List	1.0	NA
[UG-UME-OPE-LOG]	ElasticNet UME Log Management Operation Guide	R1.0	2020/07/22
[UG-UME-OPE-OAOG]	ElasticNet UME Open API Service Operation Guide	R1.0	2020/07/30
[UG-UME-OPE-SMOG]	ElasticNet UME Security Management Operation Guide	R1.0	2020/07/22
[UG-UME-PRE]	UME Software Integrity Protection Evidence description	1.0	NA
[UG-UME-SPM]	Security Parameter Manual	1.0	NA
[UG-UME-UPG]	UME Upgrade Guide	1.12	2020/08/11
[UG-A9622E-INST]	ZXRAN A9622E S35 5G Hardware Installation	1.0	2019/12/24
[UG-A9631-AAU-INST]	ZXRAN A9631 S26 5G Active Antenna Unit Hardware Installation Guide	1.0	2019/12/25
[UG-A9815-AAU-INST]	ZXRAN A9815 5G Active Antenna Unit Hardware Installation	1.0	2018/03/30
[UG-A9611-AAU-INST]	ZXRAN A9611 S35 5G Active Antenna Unit Hardware Installation	1.0	2018/01/25
[UG-R9105-S26-RRU-INST]	ZXRAN R9105 S26 5G Remote Radio Unit Hardware Installation	1.0	2019/06/20

Reference	Name	Version	Date
[UG-R9105-S35-RRU-INST]	ZXRAN R9105 S35 5G Remote Radio Unit Hardware Installation	1.0	2019/08/20
[UG-R9212E-RRU-INST]	ZXRAN R9212E Macro Radio Remote Unit Hardware Installation Guide	1.0	2019/07/30
[UG-R9214E-RRU-INST]	ZXRAN R9214E Macro Radio Remote Unit Hardware Installation	1.0	2019/10/22
[UG-R9222-RRU-INST]	ZXRAN R9222 Macro Radio Remote Unit Hardware Installation Guide	1.0	2019/10/24
[UG-R8862A-RRU-INST]	ZXSDR R8862A Macro Remote Radio Unit Hardware Installation	1.0	2018/06/20
[UG-R8998E-S2600-RRU-INST]	ZXSDR R8998E S2600 TDD Multi-Path Remote Radio Unit Hardware Installation	1.0	2018/12/10
[UG-R8998E-S3700-RRU-INST]	ZXSDR R8998E S3700 TDD Multi-Path Remote Radio Unit Hardware Installation	1.0	2018/12/18
[UG-R8852E-RRU-INST]	ZXSDR R8852E Macro Remote Radio Unit Hardware Installation	1.0	2018/09/30
[UG-R8854E-RRU-INST]	ZXSDR R8854E Macro Radio Remote Unit Hardware Installation	1.0	2018/09/30
[UG-R8894-RRU-INST]	ZXSDR R8894E Macro Radio Remote Unit Hardware Installation	1.0	2019/11/30

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 provided evidence, that is mapped to the TOE TSFIs, which represents a subset of the entire developer functional testing. Evaluators validated the correctness of the mapping and the correspondence of the testing to the TSFIs expected behavior. Evaluators validated the appropriateness of the test cases definition (prerequisites, test procedure, expected results) for testing the expected TSFIs behavior.

The developer created its functional test plan directly from the test cases described in the 3gpp standards *[TS.33.511]* for BBU, and *[TS.33.117]* for BBU and UME, as required by NESAS for 5G products.

The developer provided the evaluator with access to TOE samples.

For the BBU the evaluators performed 100% sampling of the delevoper testing.

For the UME, evaluators repeated all developer tests on an earlier version of the UME software. The evaluators then repeated a sample of developer tests that covered all UME subsystems and relevant TSFIs on the version of UME software included in the TOE.

2.6.2 Independent Penetration Testing

To identify potential vulnerabilities the evaluator performed the following activities:

- Analyzed public vulnerabilities sources and internal vulnerability sources and assess the applicability and execute or define a new penetration test if required.

- Performed network and web scanning tools on the UME and BBU interfaces so identify vulnerabilities, discover unexpected ports, and check cipher suites.

During the evaluation of all performed assurance classes the evaluator labeled the identified potential vulnerabilities, if any. No potential vulnerabilities were identified during the evaluation activities for ASE, AGD, or ALC. Potential vulnerabilities were identified during the evaluation activities for ADV and ATE. Only software attacks category is taken into account since it is assumed that the TOE physical access is protected. The penetration tests that were devised and executed were:

- Communication channel attack
- Web attack
- OS attack
- Data protection of logs and other information

2.6.3 Test Configuration

The configuration of the sample was the same as described in the ZTE RAN Solution Security Target, v0.22, 4 February 2021:The sampled BBU and UME are listed, below (RRU/AAU units are essentially passive radio transceivers in these tests). The Developer and Independent tests were performed on the same TOE model and version.

TOE component	Version number
BBU	ZXRAN V9200
UME	V16.20.30

Tests were conducted with test clients/tools communicating with the BBU and UME through a router and, when required, also directly to the BBU through its debug port.

2.6.4 Testing 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 Re-used evaluation results

There is no re-use of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number ZTE 5G-RAN Solution V3.00.30.20P10. Details of the verification process for both hardware and software components is provided in acceptance procedures *[UG-BBU-ACP]* for BBU and *[UG-UME-ACP]* for UME.

2.9 Results of the Evaluation

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 5G-RAN Solution V3.00.30.20P10, to be **CC Part 2 extended, 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 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 with respect to 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 need to 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. In order for the evolution of attack methods and techniques to be covered, he 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 RAN Solution Security Target, v0.22, 4 February 2021*[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

3GPP	3rd Generation Partnership Project
5G	Fifth generation technology standard for broadband cellular networks
AAU	Active Antenna Unit
BBU	Baseband Unit
gNodeB	5G base station employing New Radio technology
GSMA	GSM Association
IT	Information Technology
ITSEF	IT Security Evaluation Facility
NESAS	Network Equipment Security Assurance Scheme (GSMA/3GPP)
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
RAN	Radio Access Network
RRU	remote RF unit
TOE	Target of Evaluation
UME	Unified Management Expert

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 RAN V3.00.30.20P10 – EAL3+, 20-RPT-1144, v4.0, 26 March 2021.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[ST]	ZTE RAN Solution Security Target, v0.22, 4 February 2021.
[TS.33.117]	TS.33.117: Catalogue of general security assurance requirements, Release 16.6.0, 16 December 2020.
[TS.33.511]	TS.33.511: Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class, Release 16.5.0, 25 September 2020.
[UG-BBU-ACP]	UG-BBU-ACP Acceptance procedure, v0.4, 3 February 2021.
[UG-UME-ACP]	UG-UME-ACP Acceptance procedure, v0.3, 3 February 2021.

(This is the end of this report).