



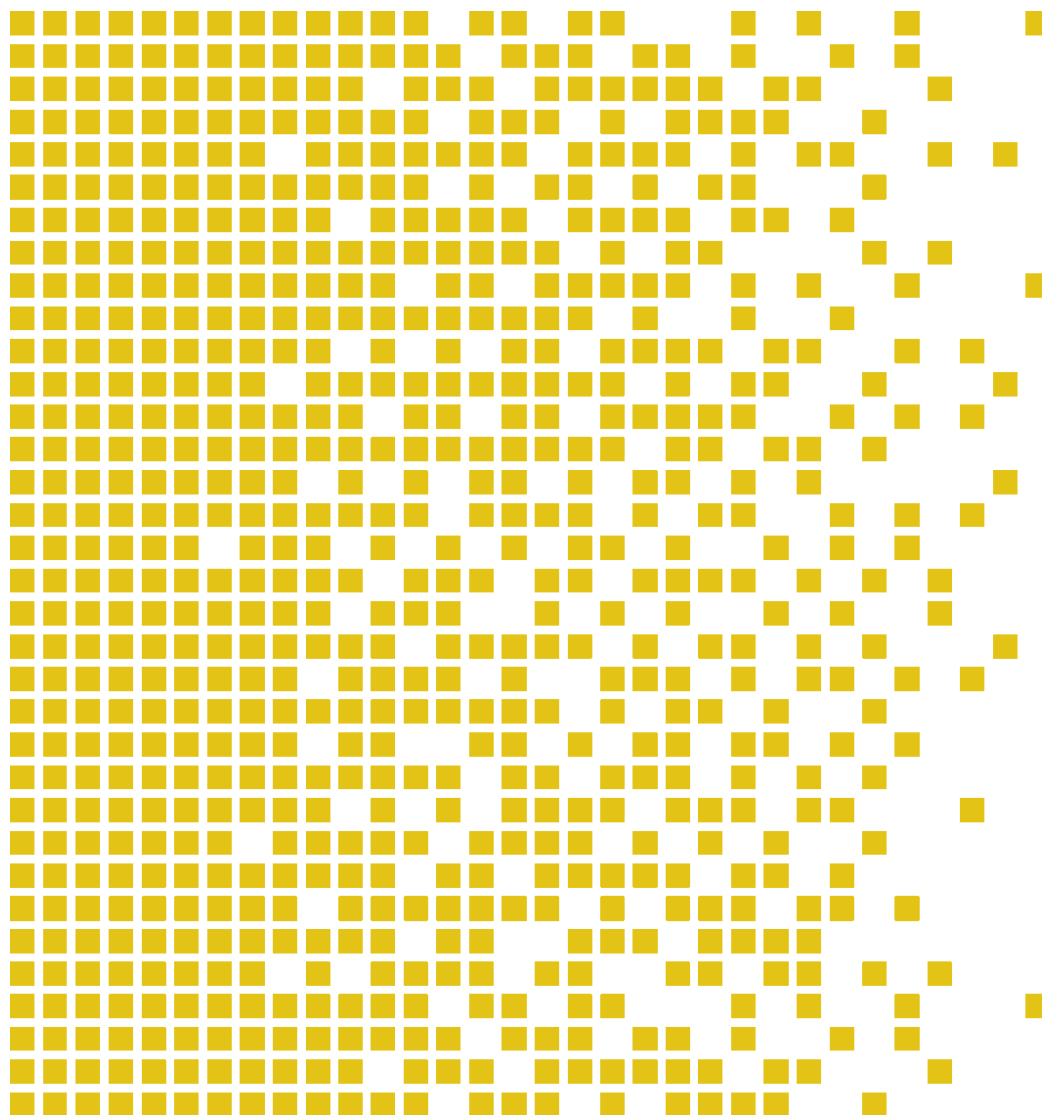
SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet Norwegian Certification Authority for IT Security

SERTIT-37 CR Certification Report

Issue 1.0 17 August 2012

ZTE Access System Series - ZXMSG5200 V3.2P03T2, C300M V2.1T5, C350M V2.1T5, ZXMSG 5208 V1.0.1, FSAP 9800 V1.0.6P9, FSAP 9800 V3.2P3, ZXDSL 9806H V1.2P20, ZXDSL 9806H V2.1P5, ZXDSL 9816 V2.0.0 and ZXDSL 9836 V1.0.0P1



CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.1 11.11.2011

**ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN
THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

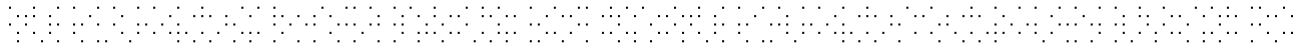
The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. [*]

* Mutual Recognition under the CC recognition arrangement applies to EAL 2 but not to ALC_FLR.2.



**Contents**

1	Certification Statement	5
2	Abbreviations	6
3	References	10
4	Executive Summary	11
4.1	Introduction	11
4.2	Evaluated Product	11
4.3	TOE scope	11
4.4	Protection Profile Conformance	11
4.5	Assurance Level	11
4.6	Security Policy	11
4.7	Security Claims	12
4.8	Threats Countered	12
4.9	Threats Countered by the TOE's environment	12
4.10	Threats and Attacks not Countered	12
4.11	Environmental Assumptions and Dependencies	12
4.12	IT Security Objectives	13
4.13	Non-IT Security Objectives	13
4.14	Security Functional Requirements	14
4.15	Security Function Policy	14
4.16	Evaluation Conduct	15
4.17	General Points	15
5	Evaluation Findings	15
5.1	Introduction	16
5.2	Delivery	16
5.3	Installation and Guidance Documentation	17
5.4	Misuse	17
5.5	Vulnerability Analysis	17
5.6	Developer's Tests	17
5.7	Evaluators' Tests	17
6	Evaluation Outcome	18
6.1	Certification Result	18
6.2	Recommendations	18
	Annex A: Evaluated Configuration	19
	TOE Identification	19
	TOE Documentation	19
	TOE Configuration	22



1 Certification Statement

ZTE Corporation ZTE Access System Series is an Access System, which regulates the access between networks, like a provider IP network or the PSTN or subscribers, who wish to access these networks.

ZTE Access System Series version ZXMSG5200 V3.2P03T2, C300M V2.1T5, C350M V2.1T5, ZXMSG 5208 V1.0.1, FSAP 9800 V1.0.6P9, FSAP 9800 V3.2P3, ZXDSL 9806H V1.2P20, ZXDSL 9806H V2.1P5, ZXDSL 9816 V2.0.0 and ZXDSL 9836 V1.0.0P1 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality in the specified environment when running on the platforms specified in Annex A.

Author	Kvassnes, Kjartan Jæger
Certifier	
Quality Assurance	Arne Høye Røge
Quality Assurance	
Approved	Kjeil W. Bergan
Head of SERTIT	
Date approved	17 August 2012



2 Abbreviations

ADSL	Asymmetric DSL
AGCF	Access Gateway Control Function
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BRI	Basic Rate Interface
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
E&M	Earth & Magneto
EAL	Evaluation Assurance Level
EMS	Element Management System
EOR	Evaluation Observation Report
EPNI	EPON Network Interface
EPON	Ethernet PON
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
FE	Fast Ethernet
FTP	File Transfer Protocol
GE	Gigabit Ethernet
GPNI	GPON Network Interface
GPON	Gigabit PON
IGMP	Internet Group Management Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol

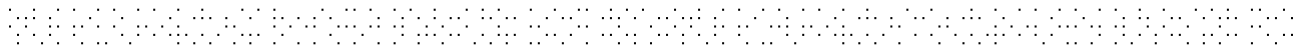


IPTV	IP Television
ISDN	Integrated Services Data Network
ISIS	Intermediate System to Intermediate System
IUA	ISDN User Adaptation
LE	Local Exchange
NGN	Next Generation Network
NTP	Network Time Protocol
OLT	Optical Line Terminal
OSPF	Open Shortest Path First
P-CSCF	Proxy Call Session Control Function
PIM	Protocol Independent Multicast
PIM-DM	PIM Dense Media
PIM-SM	PIM Sparse Media
POC	Point of Contact
PON	Passive Optical Network
POTS	Plain Old Telephony Service
PPP	Point to Point Protocol
PPPoE	PPP over Ethernet
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
PWE3	Pseudo Wire Emulation Edge - Edge
QP	Qualified Participant
RADIUS	Remote Authentication Dial In User Service
RCTP	Real Time Control Protocol
RIP	Routing Information Protocol
RTP	Real Time Protocol
SCP	Session Control Protocol
SERTIT	Norwegian Certification Authority for IT Security
SHDSL	Single Rate High Speed DSL
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol



SoF	Strength of Function
SPM	Security Policy Model
SSH	Secure Shell
ST	Security Target
TACACS	Terminal Access Controller Access Control System
TFTP	Trivial FTP
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VDSL	Very High Bit Rate DSL
VF	Voice Frequency
xPON	EPON or GPON





3 References

- [1] ZTE Access System Series Security Target, v 1.0, 25 April 2012.
- [2] Common Criteria Part 1, CCMB-2009-07-001, Version 3.1 R3, July 2009.
- [3] Common Criteria Part 2, CCMB-2009-07-002, Version 3.1 R3, July 2009.
- [4] Common Criteria Part 3, CCMB-2009-07-003, Version 3.1 R3, July 2009.
- [5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.
- [6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1 R3, July 2009.
- [7] Evaluation Technical Report Common Criteria EAL2+ Evaluation of ZTE Access System Series, v 1.1, 23 April 2012.
- [8] ZXMSG 5200(V3.2) Configuration Manual (CLI)
- [9] ZXMSG 5200(V3.2) Configuration Manual (NetNumen) Volume I
- [10] ZXMSG 5200(V3.2) Configuration Manual (NetNumen) Volume II
- [11] ZXA10 C300M(V2.1) Multi-service Access Equipment Configuration Manual (CLI)
- [12] ZXA10 C300M(V2.1) Multi-Service Access Equipment Configuration Manual (NetNumen)
- [13] ZXA10 C350M(V2.1) Multi-Service Access Equipment Configuration Manual (CLI)
- [14] ZXA10 C350M(V2.1) Multi-Service Access Equipment Configuration Manual (NetNumen)
- [15] ZXMSG 5208(V1.0) Configuration Manual (NetNumen)
- [16] FSAP 9800 (V3.2) Full Service Access Platform Operation Manual (CLI)
- [17] FSAP 9800 (V3.2) Full Service Access Platform Operation Manual (NetNumen)
- [18] ZXDSL 9806H (V2.1) ZTE Broadband Universal Access System Configuration Manual(CLI)
- [19] ZXDSL 9806H (V2.1) ZTE Broadband Universal Access System Configuration Manual(NetNumen)
- [20] ZXDSL 9816(V2.0) Configuration Manual (CLI)
- [21] ZXDSL 9816(V2.0) Configuration Manual (NetNumen).



4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of ZTE Access System Series version ZXMSG5200 V3.2P03T2, C300M V2.1T5, C350M V2.1T5, ZXMSG 5208 V1.0.1, FSAP 9800 V1.0.6P9, FSAP 9800 V3.2P3, ZXDSL 9806H V1.2P20, ZXDSL 9806H V2.1P5, ZXDSL 9816 V2.0.0 and ZXDSL 9836 V1.0.0P1 to the Sponsor, ZTE Corporation, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The versions of the product evaluated was ZTE Access System Series - ZXMSG5200 V3.2P03T2, C300M V2.1T5, C350M V2.1T5, ZXMSG 5208 V1.0.1, FSAP 9800 V1.0.6P9, FSAP 9800 V3.2P3, ZXDSL 9806H V1.2P20, ZXDSL 9806H V2.1P5, ZXDSL 9816 V2.0.0 and ZXDSL 9836 V1.0.0P1.

This product is also described in this report as the Target of Evaluation (TOE). The developer was ZTE Corporation.

The TOE regulates the access between networks, like a provider IP network or the PSTN or subscribers, who wish to access these networks.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The TOE scope is described in the ST[1], chapter 1.3.

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The assurance incorporated predefined evaluation assurance level EAL 2, augmented by ALC_FLR.2. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

There are no Organizational Security Policies or rules with which the TOE must comply.



4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats which these objectives meet and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

- T.UNAUTHORISED_ADMIN¹
TA.NETWORK or TA.SUBSCRIBER gains access to the management functionality of the TOE.
- T.UNAUTHORISED_ACCESS
TA.SUBSCRIBER gains access to a service on a Network that he is not authorized to access
- T.PHYSICAL_ATTACK
TA.PHYSICAL gains physical access to the TOE and is able to perform actions on the TOE.
- T.CONFIDENTIALITY
TA.SUBSCRIBER is able to read traffic from/to another subscriber
- T.INTEGRITY
TA.SUBSCRIBER is able to modify traffic from/to another subscriber

4.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE's environment.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described

4.11 Environmental Assumptions and Dependencies

The Security Target describes one assumption:

For FSAP 9800 V1.0.6P9

It is assumed that the Network(s) (including the Management Network) are trusted, such that they will not interfere with subscriber and/or management traffic. It is also assumed that the EMS, RADIUS and TACACS+ servers will not be used to attack the TOE.

¹ As TA.NETWORK does not exist for the FSAP 9800 V1.06P9: for this TOE only TA.SUBSCRIBER is relevant.



For all other TOEs

It is assumed that the Network(s) (except the Management Network) are trusted, such that they will not interfere with subscriber traffic. It is also assumed that the EMS, RADIUS and TACACS+ servers will not be used to attack the TOE.

4.12 IT Security Objectives

- O.ACCESS

The TOE shall ensure that subscribers have only access to the services on the networks that they are entitled to.

- O.MANAGE_ACCESS

The TOE shall offer administrators the possibility to modify the access that subscribers have to networks.

- O.AUTHENTICATE_ADMIN

The TOE shall identify and authenticate administrators before allowing them access to administrative functions.

- O.ENCRYPTED_MANAGEMENT (not relevant for FSAP 9800 V1.0.6P9)

The TOE shall offer an encrypted channel for administrative actions, preventing disclosure, insertion and/or modification of administrative commands.

- O.SEPARATION_OF_PORTS

The TOE shall offer physical ports, and be able to separate traffic between different ports, such that:

- It is not possible to listen in on traffic from one port on a different port
- It is not possible to modify traffic on one port from another port
- O.xPON (only on TOEs offering xPON)

THE TOE shall offer physical xPON ports to subscribers, such that:

- It is not possible for one subscriber on a xPON port to listen in on traffic from/to other subscribers on that xPON port
- It is not possible for one subscriber on a XPON port to modify traffic from/to other subscribers on that xPON port

4.13 Non-IT Security Objectives

- OE.PHYSICAL_SECURITY

The operator shall ensure that the TOE shall be protected from physical attacks.

- OE.MULTIPLE_SUBSCRIBERS

Where multiple subscribers are connected to a single non-xPON port, and it is desired that the confidentiality and/or integrity of traffic from/to a subscriber shall be protected from other subscribers, this must be arranged by the environment.

- OE.TRUSTED_NETWORK (for FSAP 9800 V1.0.6P9)

The environment shall ensure that the Network(s) are trusted (including the Management Network), such that they will not interfere with subscriber and/or management traffic and that the EMS, RADIUS and TACACS+ servers will not be used to attack the TOE.

- OE.TRUSTED_NETWORK (for all other TOEs)

The environment shall ensure that the Network(s) are trusted (except the Management Network), such that they will not interfere with subscriber traffic and that the EMS, RADIUS and TACACS+ servers will not be used to attack the TOE.

4.14 Security Functional Requirements

The following Security Functional requirements were used:

- FMT_SMR.1 Security roles
- FIA_UID.2 User identification before any action
- FIA_UAU.2 User authentication before any action
- FMT_SMF.1 Specification of Management Functions
- FTP_ITC.1 Inter-TSF trusted channel (not relevant for FSAP 9800 V1.0.6P9)
- FDP_IFC.1 Subset information flow control
- FDP_IFF.1 Simple security attributes

Details on the usage of these requirements are described in the ST[1], chapter 5.3

4.15 Security Function Policy

The TOE has the following general functionalities:

- Provide access of subscribers to networks (and vice versa)
- Convert the protocols used by the subscribers to protocols suitable for the networks (and vice versa)
- Allow management of itself through a Management Network

The TOE

- provides secure management of itself, to ensure that only properly authorized staff can manage the TOE
- ensures that subscribers have only access to the networks and functionalities/entities on those networks that they are entitled to



- ensures that subscribers cannot read traffic from/to other subscribers
- ensures that subscribers cannot modify traffic from/to other subscribers.

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Brightsight B.V. Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR)[7] to SERTIT in 23 April 2012. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3. These classes comprise the EAL 2 assurance package augmented with ALC_FLR.2



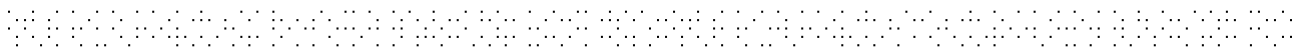
Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.



5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance in the Operational User Guidance documents provided by the developer.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Developers should follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents[8]to[21] adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

The evaluators assessed all possible vulnerabilities found during evaluation of the classes except those tests from [ATE IND AVA].

BrightSight tested the remaining potential vulnerabilities on the final version of the TOE at the premises of ZTE, Shanghai, China on 27th and 29th March. SERTIT witnessed all these test with two certifiers.

5.6 Developer's Tests

The developer test effort is considered already fairly complete. Any major missing features reported by the evaluators such as user management, STP and LACP tests have been added to the developer test set. And the developer integrated tests for similar functionality into bigger test case. Nevertheless the evaluator has modified 13 additional tests as the evaluator's independent tests.

BrightSight performed these tests based on the final version of the TOE at the premises of ZTE, Shanghai, China on 27th and 29th of March. SERTIT witnessed all these tests with two certifiers.

5.7 Evaluators' Tests

For independent testing, the evaluator has repeated 9 out of the 11 developer's tests and added 12 tests (21 evaluator's ATE_IND.2 tests in total). For each of the TSFI available at least one test is performed. BrightSight performed these tests based on the final version of the TOE at the premises of ZTE, Shanghai, China on 27th and 29th of March. SERTIT witnessed all these tests with two certifiers.



6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that ZTE Access System Series version ZXMSG5200 V3.2P03T2, C300M V2.1T5, C350M V2.1T5, ZXMSG 5208 V1.0.1, FSAP 9800 V1.0.6P9, FSAP 9800 V3.2P3, ZXDSL 9806H V1.2P20, ZXDSL 9806H V2.1P5, ZXDSL 9816 V2.0.0 and ZXDSL 9836 V1.0.0P1 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 2 + ALC_FLR.2 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of ZTE Access System Series should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 4.3 "TOE Scope" and Section 5 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

There is no special hardware requirement. Since the TOE already includes the hardware components. The configuration of the hardware is listed below:

TYPE	TOE NAME	VERSION
Hardware	ZXMSG 5200 V3.2P03T2	ZXMSG 5200
	ZXA10 C300M V2.1T5	ZXA10 C300M
	ZXA10 C350M V2.1T5	ZXA10 C350M
	ZXMSG 5208 V1.0.1	ZXMSG 5208
	FSAP 9800 V3.2P3	FSAP 9800
	FSAP 9800 V1.0.6P9	FSAP 9800
	ZXDSL 9806H V1.2P20	ZXDSL 9806H
	ZXDSL 9806H V2.1P5	ZXDSL 9806H
	ZXDSL 9816 V2.0.0	ZXDSL 9816
	ZXDSL 9836 V1.0.0P1	ZXDSL 9836

TOE Documentation

The supporting guidance documents evaluated were:

- [a] Access Gateways, Version 0.4, 14 March 2012
- [b] FSAP9800 physical functional specification v0.99, 13 September 2011
- [c] ZXA10 C300M physical functional specification v0.99, 13 September 2011
- [d] ZXA10 C350M physical functional specification v0.99, 13 September 2011
- [e] ZXDSL 98x6 Series MDU Running ZXMAP_v1.0, 06 September 2011
- [f] ZXMSG 5200 physical functional specification v0.99, 13 September 2011
- [g] ZXMSG 5208 physical functional specification v0.99, 13 September 2011
- [h] ALC_DEL.1, ALC_CMC.2, ALC_CMS.2, ALC_FLR.2 documentation for ZTE eNodeB, Version: 0.2, 13 February 2012
- [i] CC Test Specification ZTE 20120322, Version: 1.7, 22 March 2012
- [j] ZXMSG 5200 General Test Specification, v1.2, 25 March 2010
- [k] Test case SFR mapping for each device v5, 26 March 2012
- [l] 9800V1.0.6---CC Self-Test Report ZTE 20120324 V1.0

- [m] 9800V3.2---CC Self-Test Report ZTE 20120324 V1.0
- [n] 9806HV1.2---CC Self-Test Report ZTE 20120324 V1.0
- [o] 9806HV2.1---CC Self-Test Report ZTE 20120324 V1.0
- [p] 9816V2---CC Self-Test Report ZTE 20120324 V1.0
- [q] 9836V1---CC Self-Test Report ZTE 20120324 V1.0
- [r] C300MV2.1---CC Self-Test Report ZTE 20120324 V1.0
- [s] C350MV2.1---CC Self-Test Report ZTE 20120324 V1.0
- [t] MSG5200V3.2---CC Self-Test Report ZTE 20120324 V1.0
- [u] MSG5208V1---CC Self-Test Report ZTE 20120324 V1.0
- [v] ZXMSG 5200(V3.2) Configuration Manual (CLI)
- [w] ZXMSG 5200(V3.2) Maintenance Manual
- [x] ZXMSG 5200(V3.2) Configuration Manual (NetNumen) Volume I
- [y] ZXMSG 5200(V3.2) Configuration Manual (NetNumen) Volume II
- [z] ZXMSG 5200 (V3.2) Security Issues
- [aa] ZXA10 C300M(V2.1) Multi-service Access Equipment Configuration Manual (CLI)
- [bb] ZXA10 C300M(V2.1) Multi-Service Access Equipment Configuration Manual (NetNumen)
- [cc] ZXA10 C300M(V2.1) Multi-service Access Equipment Maintenance Manual
- [dd] ZXA10 C300M(V2.1) Security Issues
- [ee] ZXA10 C350M(V2.1) Multi-Service Access Equipment Configuration Manual (CLI)
- [ff] ZXA10 C350M(V2.1) Multi-Service Access Equipment Configuration Manual (NetNumen)
- [gg] ZXA10 C350M(V2.1) Multi-Service Access Equipment Routine Maintenance Manual
- [hh] ZXA10 C350M(V2.1) Security Issues
- [ii] ZXMSG 5208(V1.0) Feature Guide
- [jj] ZXMSG 5208(V1.0) Configuration Manual (NetNumen)
- [kk] ZXMSG 5208(V1.0) Command Reference (Volume I)
- [ll] ZXMSG 5208(V1.0) Command Reference (Volume II)
- [mm] ZXMSG 5208(V1.0) Command Reference (Volume III)
- [nn] ZXMSG 5208(V1.0) Security Issues



- [oo] FSAP 9800 (V1.0.6) Full Service Access Platform Operation Manual (CLI)
- [pp] FSAP 9800 (V1.0.6) Full Service Access Platform Operation Manual (NetNumen)
- [qq] FSAP 9800 (V1.06) Full Service Access Platform Maintenance Manual
- [rr] FSAP 9800 (V1.06) Security Issues
- [ss] FSAP 9800 (V3.2) Full Service Access Platform Maintenance Manual.pdf
- [tt] FSAP 9800 (V3.2) Full Service Access Platform Operation Manual (CLI)
- [uu] FSAP 9800 (V3.2) Full Service Access Platform Operation Manual (NetNumen)
- [vv] FSAP 9800 (V3.2) Security Issues
- [ww] ZXDSL 9806H (V1.2) ZTE Broadband Universal Access System User Manual (Volume I)
- [xx] ZXDSL 9806H (V1.2) ZTE Broadband Universal Access System User Manual (Volume II)
- [yy] ZXDSL 9806H (V1.2) Security Issues
- [zz] ZXDSL 9806H (V2.1) ZTE Broadband Universal Access System Configuration Manual(CLI)
- [aaa] ZXDSL 9806H (V2.1) ZTE Broadband Universal Access System Configuration Manual(NetNumen)
- [bbb] ZXDSL 9806H (V2.1) ZTE Broadband Universal Access System Maintenance Manual
- [ccc] ZXDSL 9806H (V2.1) Security Issues
- [ddd] ZXDSL 9816(V2.0) Configuration Manual (CLI)
- [eee] ZXDSL 9816(V2.0) Configuration Manual (NetNumen)
- [fff] ZXDSL 9816(V2.0) Security Issues
- [ggg] ZXDSL 9836(V1.0) Command Reference (Volume I).pdf
- [hhh] ZXDSL 9836(V1.0) Command Reference (Volume II).pdf
- [iii] ZXDSL 9836(V1.0) Command Reference (Volume III).pdf
- [jjj] ZXDSL 9836(V1.0) Hardware Description.pdf
- [kkk] ZXDSL 9836(V1.0) Maintenance Manual.pdf
- [lll] ZXDSL 9836(V1.0) Product Description.pdf
- [mmm] ZXDSL 9836(V1.0) Security Issues

Further discussion of the supporting guidance material is given in Section 5.3 "Installation and Guidance Documentation".



TOE Configuration

The following configuration was used for testing:

TOE	ITEM	IDENTIFIER	VERSION
ZXMSG5200 V3.2P03T2	Hardware	ZXMSG 5200	
	Software	MSG5200 ZXIAP ZXROS Vxworks	V3.2P03T2 v1.2 04.08.01 5.5.1
	Guidance	ZXMSG 5200(V3.2) Configuration Manual (CLI) ZXMSG 5200(V3.2) Maintenance Manual ZXMSG 5200(V3.2) Configuration Manual (NetNumen) Volume I ZXMSG 5200(V3.2) Configuration Manual (NetNumen) Volume II ZXMSG 5200 (V3.2) Security Issues	R1.0
C300M V2.1T5	Hardware	ZXA10 C300M	
	Software	MSG_6000 ZXIAP ZXROS Vxworks	V2.1T5 v1.2 04.08.01 5.5.1
	Guidance	ZXA10 C300M(V2.1) Multi-service Access Equipment Configuration Manual (CLI) ZXA10 C300M(V2.1) Multi-Service Access Equipment Configuration Manual (NetNumen) ZXA10 C300M(V2.1) Multi-service Access Equipment Maintenance Manual ZXA10 C300M(V2.1) Security Issues	R1.0
C350M V2.1T5	Hardware	ZXA10 C350M	
	Software	MSG_6000 ZXIAP ZXROS Vxworks	V2.1T5 v1.2 04.08.01 (5.5.1)
	Guidance	ZXA10 C350M(V2.1) Multi-Service Access Equipment Configuration Manual (CLI) ZXA10 C350M(V2.1) Multi-Service Access Equipment Configuration Manual (NetNumen) ZXA10 C350M(V2.1) Multi-Service Access Equipment Routine Maintenance Manual ZXA10 C350M(V2.1) Security Issues	R1.0
ZXMSG 5208 V1.0.1	Hardware	ZXMSG 5208	
	Software	ZXMSG 5208 ZXMAP Linux	V1.0.1 2.0 2.6.21.7
	Guidance	ZXMSG 5208(V1.0) Feature Guide ZXMSG 5208(V1.0) Configuration Manual (NetNumen) ZXMSG 5208(V1.0) Command Reference (Volume I) ZXMSG 5208(V1.0) Command Reference (Volume II) ZXMSG 5208(V1.0) Command Reference (Volume III) ZXMSG 5208(V1.0) Security Issues	R1.0
FSAP 9800 V1.0.6P9	Hardware	FSAP 9800	
	Software	9800 Vxworks	V1.0.6P9 V5.4

	Guidance	FSAP 9800 (V1.0.6) Full Service Access Platform Operation Manual (CLI) FSAP 9800 (V1.0.6) Full Service Access Platform Operation Manual (NetNumen) FSAP 9800 (V1.06) Full Service Access Platform Maintenance Manual FSAP 9800 (V1.06) Security Issues	R1.0
FSAP 9800 V3.2P3	Hardware	FSAP 9800	
	Software	9800 ZXIAP ZXROS Vxworks	V3.2P3 v1.2 04.08.01 5.5.1
	Guidance	FSAP 9800 (V3.2) Full Service Access Platform Maintenance Manual.pdf FSAP 9800 (V3.2) Full Service Access Platform Operation Manual (CLI) FSAP 9800 (V3.2) Full Service Access Platform Operation Manual (NetNumen) FSAP 9800 (V3.2) Security Issues	R1.0
ZXDSL 9806H V1.2P20	Hardware	ZXDSL 9806H	
	Software	ZXDSL 9806H ZXMAP Linux	V1.2P20 2.0 2.6.21.7
	Guidance	ZXDSL 9806H (V1.2) ZTE Broadband Universal Access System User Manual (Volume I) ZXDSL 9806H (V1.2) ZTE Broadband Universal Access System User Manual (Volume II) ZXDSL 9806H (V1.2) Security Issues	R1.0
ZXDSL 9806H V2.1P5	Hardware	ZXDSL 9806H	
	Software	ZXDSL 9806H ZXMAP Linux	V2.1P5 2.0 2.6.21.7
	Guidance	ZXDSL 9806H (V2.1) ZTE Broadband Universal Access System Configuration Manual(CLI) ZXDSL 9806H (V2.1) ZTE Broadband Universal Access System Configuration Manual(NetNumen) ZXDSL 9806H (V2.1) ZTE Broadband Universal Access System Maintenance Manual ZXDSL 9806H (V2.1) Security Issues	R1.0
ZXDSL 9816 V2.0.0	Hardware	ZXDSL 9816	
	Software	ZXDSL 9816 ZXMAP Linux	v2.0.0 2.0 2.6.21.7
	Guidance	ZXDSL 9816(V2.0) Configuration Manual (CLI) ZXDSL 9816(V2.0) Configuration Manual (NetNumen) ZXDSL 9816(V2.0) Security Issues	
ZXDSL 9836 V1.0.0P1	Hardware	ZXDSL 9836	
	Software	ZXDSL 9836 ZXMAP Linux	v1.0.0P1 2.0 2.6.21.7



	Guidance	ZXDSL 9836(V1.0) Command Reference (Volume I).pdf ZXDSL 9836(V1.0) Command Reference (Volume II).pdf ZXDSL 9836(V1.0) Command Reference (Volume III).pdf ZXDSL 9836(V1.0) Hardware Description.pdf ZXDSL 9836(V1.0) Maintenance Manual.pdf ZXDSL 9836(V1.0) Product Description.pdf ZXDSL 9836(V1.0) Security Issues	
Development Evidence		[ST] Access Gateways ST [ADV] Access Gateways [FSP] FSAP9800 physical functional specification [FSP] ZXA10 C300M physical functional specification [FSP] ZXA10 C350M physical functional specification [FSP] ZXDSL 98x6 Series MDU Running ZXMAP [FSP] ZXMSG 5200 physical functional specification [FSP] ZXMSG 5208 physical functional specification [SFR MAP] Test case SFR mapping for each device [ATE 5200] ZXMSG 5200 General Test Specification [ATE] CC Test Specification ZTE [ALC] ALC_DEL.1, ALC_CMC.2, ALC_CMS.2, ALC_FLR.2 for Access System Series	V0.9 V0.4 v0.99 v0.99 v0.99 v1.0 v0.99 v0.99 v4 V1.1 V1.7 v0.1

Certificate

The IT product identified in this certificate has been evaluated at the Norwegian evaluation facility described on this certificate using Common Methodology for IT Security Evaluation, according to the version number described on this certificate, for conformance to the Common Criteria for IT Security Evaluation according to the version number described on this certificate. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of The Norwegian Certification Authority for IT Security (SERTIT) and the conclusions of the evaluation technical report are consistent with the evidence adduced. Certification does not guarantee that the IT product is free from security vulnerabilities. This certificate only reflects the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown of this certificate. This certificate is not an endorsement of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

Product Manufacturer: ZTE Corporation

Product Name: ZTE Access System Series

Type of Product: Telecommunication Access System

Version and Release Numbers: ZXMSG5200 V3.2P03T2, C300M V2.1T5, C350M V2.1T5, ZXMSG 5208 V1.0.1, FSAP 9800 V1.0.6P9, FSAP 9800 V3.2P3, ZXDSL 9806H V1.2P20, ZXDSL 9806H V2.1P5, ZXDSL 9816 V2.0.0 and ZXDSL 9836 V1.0.0P1

Assurance Package: EAL 2 augmented with ALC_FLR.2

Evaluation Criteria: Common Criteria version 3.1R3 (ISO/IEC 15408)

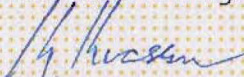
Name of IT Security Evaluation Facility: Brightsight B.V.

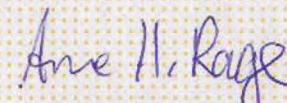
Name of Certification Body: SERTIT

Certification Report Identifier: SERTIT-037 CR, issue 1.0, 17 August 2012

Certificate Identifier: SERTIT-037 C

Date Issued: 17 August 2012


Kjartan Jæger Kvassnes
Certifier


Arne Høye Røge
Quality Assurance


Kjell Werner Bergan
Head of SERTIT



SERTIT

Norwegian Certification Authority for IT Security

