Certification Report

EAL 2 + ALC_FLR.2 Evaluation of

FiberHome Telecommunication Technologies Co., Ltd.

FiberHome Enhanced Optical Transport Equipment Manager including UNM2000 EMS Server version V3R2, UNM2000 EMS Client version V3R2, FONST 5000 COTP version RP0100, FONST 5000 U10E version RP0101, FONST 5000 U20E version RP0101, FONST 1000 D2 version RP0100, FONST 5000 N32 version RP0101

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-77

TABLE OF CONTENTS

Document Information

Date of Issue	02.11.2021
Approval Date	02.11.2021
Certification Report Number	21.0.03/21-009
Sponsor and Developer	Fiberhome Telecommunication Technologies Co., Ltd.
Evaluation Facility	DEKRA Testing and Certification S.A.U.
TOE Name	FiberHome Enhanced Optical Transport Equipment Manager including UNM2000 EMS Server version V3R2, UNM2000 EMS Client version V3R2, FONST 5000 COTP version RP0100, FONST 5000 U10E version RP0101, FONST 5000 U20E version RP0101, FONST 1000 D2 version RP0100, FONST 5000 N32 version RP0101
Pages	13

Prepared by	Mert LENGERLİOĞLU
Reviewed by	İbrahim Halil KIRMIZI

This report has been prepared by the Certification Expert and reviewed by the Technical Responsible of which signatures are above.

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
V1.0	02.11.2021	All	None

DISCLAIMER

This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1 revision 5 using Common Methodology for IT Products Evaluation, version 3.1, revision 5 This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any

other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the ITCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL = Common Criteria Testing Laboratory) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by DEKRA Testing and Certification S.A.U. which is a commercial CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for FiberHome Enhanced Optical Transport Equipment Manager including UNM2000 EMS Server version V3R2, UNM2000 EMS Client version V3R2, FONST 5000 COTP version RP0100, FONST 5000 U10E version RP0101, FONST 5000 U20E version RP0101, FONST 1000 D2 version RP0100, FONST 5000

N32 version RP0101whose evaluation was completed on 21.10.2021 and whose evaluation technical report was drawn up by DEKRA Testing and Certification S.A.U. (as CCTL), and with the Security Target document with version no 1.9 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the ITCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

This Certification Report comprises the outcome of Common Criteria security evaluation of the aforementioned Target of Evaluation (TOE) and potential users of the TOE are advised to read this document along with the referred Security Target (ST) document.

TOE is a distributed solution for the management of Optical Transport Equipments (models FONST1000 D2, FONST 5000 COTP, FONST 5000 U10E, FONST 5000 U20E, and FONST 5000 N32). The TOE encompasses the software running on the UNM2000 EMS Server and the UNM2000 EMS Client along with the firmware running on the OTEs. For versioning reference of TOE, see section 1.2 of ST document.

Two critical points worth mentioning regarding the scope of this evaluation are as follows;

- the security functionality of the TOE relies on software and firmware only and thus the hardware is out of scope,
- although the databases that contain the user credential and the logs are located in the UNM2000 EMS server, this database has no direct interface associated and its protection is ensured by the TOE environment.

The major security features of the TOE can be summarized as;

- Authentication: the TOE implements mechanisms for users authentication,
- Authorization: the TOE implements a role-based access control policy for users,
- Access Control: the TOE control the access to the OTEs,
- Audit: the TOE generates audit records,
- Management: the TOE include management functionality.

For any other relevant information regarding the evaluation such as assurance package, threats, assumptions, etc. please see the other sections of this report or ST document.

2 -CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-77
TOE Name and Version	FiberHome Enhanced Optical Transport Equipment Manager including UNM2000 EMS Server version V3R2SP1, UNM2000 EMS Client version V3R2SP1, FONST 5000 COTP version RP0100, FONST 5000 U10E version RP0101, FONST 5000 U20E version RP0101, FONST 1000 D2 version RP0100, FONST 5000 N32 version RP0101
Security Target Title	FiberHome Enhanced Optical Transport Equipment Manager Security Target
Security Target Version	V1.9
Security Target Date	2021/09/27
Assurance Level	EAL 2 augmented by ALC_FLR.2
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 5, April 2017
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017
Protection Profile Conformance	NA
Sponsor and Developer	FiberHome Telecommunication Technologies Co., Ltd.
Evaluation Facility	DEKRA Testing and Certification S.A.U.
Certification Scheme	TSE CCCS

2.2 Security Policy

There is only one policy to be fulfilled by the TOE which is defined as;

P.FLEXIBLE_MANAGEMENT The TOE must be able to support a role-based authorization framework with predefined and customizable roles, to manage the TOE itself, manage authentication framework, allowing the TOE to accept/reject users based on username/password and a configurable subset of IP-address and time of login. Review logging and auditing of events regularly.

2.3 Assumptions and Clarification of Scope

Assumptions for the IT and non-IT environment and intended usage are defined as below:

A.TRUSTED_NETWORK It is assumed that the intranet connecting UNM 2000 EMS Server, and EMS Client is trusted and managed with firewall policy. On the other hand the connection between UNM 2000 EMS Server and the OTEs is considered secure and trustful since the WDM/OTN/POTN/DCI protocols are used.

A.TIME_SYNC It is also assumed that the UNM2000 EMS server underlying Windows Server 2012, which supply time sources are trusted and will not be used to attack the TOE.

A.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g. compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

Users are as usual, advised to make sure to follow guidance and installation procedures provided by the vendor and set up their networks properly.

2.4 Architectural Information

TOE is distributed in three physically separate parts; Optical Transport Equipment, UNM2000 EMS Server and UNM2000 EMS client. For details regarding this distribution can be found in part 1.4.2 of the Security Target Document. Figure below is given for better understanding of the distribution.

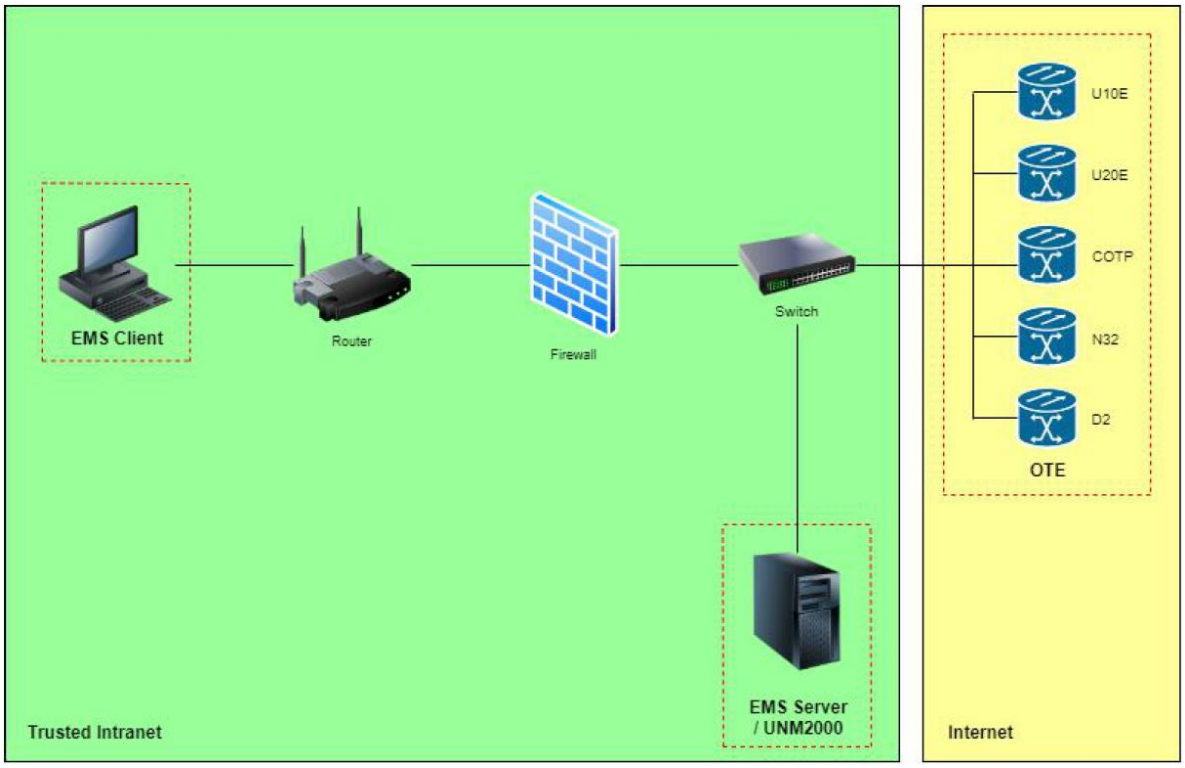

Figure 1 – TOE demarcation

The TOE supports a flexible authentication framework, allowing the TOE to accept/reject users from UNM2000 EMS client based on: username/password and a configurable subset of IP address and time of login.Also a flexible role-based authorization framework is supported with predefined and customizableroles for management.

These roles can use the UNM2000 EMS server to manage OTEs. OTE transport data of WDM/OTN/POTN/DCI connecting status, in such a way that only the intended recipients from UNM2000 EMS server are able to read OTE signal. Nobody can modify the signals of OTE, which was monitored by UNM2000 EMS server. UNM2000 EMS server supports flexible logging and auditing of events. The TOE manages traffic rules, authentication, authorization, user accounts and sessions.

2.5 Documentation

These documents listed below are provided to customer by the developer alongside the TOE:

Document Name	Version	Release Date
FIBERHOME Enhanced Optical Transport Equipment Manager Preparative Procedures and User Operational Guidance	Version 1.5	27.09.2021
UNM2000_Network Convergence Management System V3R2_Installation Guide	Version A	April 2020
UNM2000_Network Convergence Management System_Troubleshooting Guide	Version A	April 2019
UNM2000_Network Convergence Management System V3R2_Operation Guide	Version A	April 2020

2.6 IT Product Testing

- **Developer Testing:** TSFIs and subsystem/module behaviors have been tested by developer. Developer has conducted 9 functional tests in total.
- **Evaluator Testing:** Evaluator has conducted a set of tests for all SFRs and taking into account the developer test rigor and results along with other criteria regarding the selection of TSFIs and a sampling methodology is used. A total of 25 independent tests have been conducted. TOE has passed all tests to demonstrate that its security functions work as it is defined in the ST.
- **Penetration Tests:** TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, 18 penetration tests have been conducted. TOE proved that it is resistant to “Attacker with Basic Attack Potential”.

2.7 Evaluated Configuration

UNM2000 EMS Server

A Server suitable to run the Windows Server 2012 R2 (Supply time sources)

Suggested Hardware: CPU 4 E5-2667V2-8 core Processors, RAM Memory 128GB, 6 x 600 GB physical hard disk, 2 x 200G SSD + 30T disk array

Software: Windows Server 2012 R2, TOE – UNM2000 EMS Server V3R2SP1

UNM2000 EMS Client

A Workstation suitable to run Windows 10 (10.0.10240)

Suggested Hardware: CPU Intel XeonE5-2637V2 (4-core) 3.5GHz, RAM Memory 16GB, 1 x 2TB physical hard disk

Software: Windows 10 (10.0.10240), TOE – UNM2000 EMS Client V3R2SP1

OTEs

FONST1000 D2, FONST 5000 COTP, FONST 5000 U10E, FONST 5000 U20E, and FONST

5000 N32

2.8 Results of the Evaluation

The verdict for the CC Part 3 assurance components (according to EAL2+ (ALC_FLR.2) and the security target evaluation) is summarized in the following table:

Class Heading	Class Family	Description	Result
ADV: Development	ADV_ARC.1	Security-enforcing functional specification	PASS
	ADV_FSP.2	Basic design	PASS
	ADV_TDS.1	Basic modular design	PASS
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance	PASS
	AGD_PRE.1	Preparative procedures	PASS
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM system	PASS
	ALC_CMS.2	Parts of the TOE CM coverage	PASS
	ALC_DEL.1	Delivery procedures	PASS
	ALC_FLR.2	Flaw reporting procedures	PASS
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims	PASS
	ASE_ECD.1	Extended components definition	PASS
	ASE_INT.1	ST introduction	PASS
	ASE_OBJ.2	Security objectives	PASS
	ASE_REQ.2	Derived security requirements	PASS
	ASE_SPD.1	Security problem definition	PASS
	ASE_TSS.1	TOE summary specification	PASS
ATE: Tests	ATE_COV.1	Evidence of coverage	PASS
	ATE_FUN.1	Functional testing	PASS
	ATE_IND.2	Independent testing - sample	PASS
AVA: Vulnerability Analysis	AVA_VAN.2	Vulnerability analysis	PASS

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of "EGA Application Firmware v1.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III" product, result of the evaluation, or the ETR.

3 SECURITY TARGET

The security target associated with this Certification Report is identified by the following terminology:

Title: FiberHome Enhanced Optical Transport Equipment Manager Security Target

Version: v1.9

Date of Document: September 2021

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale

4 GLOSSARY

CCCS: Common Criteria Certification Scheme

CCMB: Common Criteria Management Board

ITCD: Information Techologies Test And Certification Department

EAL: Evaluation Assurance Level

OSP: Organisational Security Policy

SAR: Security Assurance Requirements

SFR: Security Functional Requirements

ST: Security Target

TOE: Target of Evaluation

TSF: TOE Security Funcationality

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017

[3] ETR v1.2 of EGA Application Firmware v2.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III, Rel. Date: October 21, 2021

[4] EGA Application Firmware v2.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III Security Target, Version 1.2.0, Rel. Date: May 05, 2021.

6 ANNEXES

There is no additional information or reference.