Certification Report

EAL 3 Evaluation of

MAY SİBER TEKNOLOJİ A.Ş.

>scopNET v7

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-57

TABLE OF CONTENTS

Document Information

Date of Issue	11.03.2019
Approval Date	11.03.2019
Certification Report Number	21.0.03/19-003
Sponsor and Developer	MAY SİBER TEKNOLOJİ A.Ş.
Evaluation Facility	BEAM TEKNOLOJİ A.Ş.
TOE	>scopNET v7
Pages	19

Prepared by	İbrahim Halil KIRMIZI	
Reviewed by	Zümrüt MÜFTÜOĞLU	

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
1.0	07.03.2019	All	First Release
2.0	11.03.2019	16	ST-Lite information added

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.

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.

CCTL 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 CCTL 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 BEAM TEKNOLOJİ A.Ş., which is a public CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target that has been approved by the CCCS. The Security Target 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 >scopNET v7 whose evaluation was completed on 04.03.2019 and whose evaluation technical report was drawn up by BEAM TEKNOLOJİ A.Ş. (as CCTL), and with the Security Target with version no 1.15 of the relevant product.

The certification report, certificate of product evaluation and security target are posted on the ITCD Certified Products List at bilisim.tse.org.tr 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 EAL2. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org

1. EXECUTIVE SUMMARY

This report constitutes the certification results by the certification body on the evaluation results applied with requirements of the Common Criteria for Information Security Evaluation.

Evaluated IT product name: >scopNET

IT Product version: v7

Developer's Name: MAY SİBER TEKNOLOJİ A.Ş.

Name of CCTL: BEAM TEKNOLOJİ A.Ş.

Assurance Package: EAL 3

Completion date of evaluation: 04.03.2019

1.1.Brief Description

The TOE is a network access control system that provides detection, authentication and authorization of devices attempting to access a network. These devices may be Guest Computers, Mobile Devices, PDA, Smart Phones or Tablets. >scopNET controls the device compliance to the company policy and authenticates this device. Compliance policies are defined by the company and introduced to >scopNET during setup and configuration processes.

1.2. Major Security Features

The TOE is a software-only product and consists of the >scopNET software components: >scopNET GUI, >scopNET Server, >scopNET Detector, >scopNET Captive Portal GUI & Engine, >scopNET Agent.

>scopNET have the following security functions;

- **Security Audit** by generating audit records for security events. Only the Root User role is allowed to view the audit trail.
- **Cryptographic Support**
- **User Data Protection** by specifying requirements for TOE security functions and TOE security function policies related to protecting user data.
- **Identification and Authentication**
- **Security Management**
- **Protection of the TSF** by maintaining the secure state in the event of certain types of failures.
- **Resource Utilisation**
- **TOE Access**
- **Trusted Path/Channels** to provide confidence that a user is communicating directly with the TSF whenever it is invoked.

1.3. Threats

The threats addressed by the TOE are;

- **T.ACC_AUD:** An attacker from the internal network could try to modify the Configuration and device data store in the Database1, audit data and user information data stored in Database4 and Database2. If the audits are not controlled regularly or the audit control could be bypassed, this action may not be noticed. Thus, the attacker succeeds without being detected.

- **T.DOS:** An attacker could execute commands, send data, or perform other operations that make resources on the internal network unavailable to system users.

- **T.FUL_AUD:** An attacker from the internal network could take actions resulting in low importance audits so as to exhaust audit storage capacity. If the audit storage capacity is exhausted, future audits are lost since no further audit could be recorded.

- **T.INFLUX:** An attacker may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
- **T.DATALOSS/MODIFY:** An attacker from the outside or internal network may attempt to remove, destroy or modify configuration, device and user information data stored in the Database1, Database2 and Database3.
- **T.MASQ:** An attacker may masquerade as another entity in order to gain access to data or TOE resources.
- **T.MEDIAT:** An attacker from the outside network may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
- **T.NOAUTH:** An attacker from internal network may attempt to bypass the security services of the TOE so as to access and use resources on the internal network. Attempts by user to gain unauthorized access to the TOE, thus limiting the Root User's ability to identify and take action against a possible security breach.
- **T.UNSECCONF:** An attacker from internal network may cause attack surface by using unsecure configurations.

2. CERTIFICATION RESULTS

2.1. Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-57
TOE Name and Version	>scopNET v7
Security Target Title	>scopNET Security Target
Security Target Version	1.15
Security Target Date	22.06.2018
Assurance Level	EAL 3
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, September 2017 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-001, Version 3.1, Revision 5, September 2017 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-001, Version 3.1, Revision 5, September 2017
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, September 2017

Protection Profile Conformance	None
Sponsor and Developer	MAY SİBER TEKNOLOJİ A.Ş.
Evaluation Facility	BEAM TEKNOLOJİ A.Ş.
Certification Scheme	TSE CCCS

2.2. Security Policy

The only Organizational Security Policy defined at Security Target is;

- **OSP.SECURE TRANSFER:** The policy is about operational environment which provides a secure channel so that credentials are protected between the >scopNET users (Root User and >scopNET Admin) and >scopNET GUI application server. SSL (Secure Socket Layer) which is a cryptographic protocol designed to provide communication's security over a computer network, is used for communication between >scopNET Users and >scopNET GUI. It provides "HTTPS" connection.

2.3. Assumptions and Clarification of Scope

Assumptions for the operational environment of the composite TOE are;

- **A.ACCDATA:** The TOE has access to all the IT System data it needs to perform its functions.
- **A.NOEVIL:** Root User, who manages the TOE is a non-hostile user, configures and maintains the TOE and follows all guidance.
- **A.EDUCUSER:** Root User and end users are educated so as to use the >scopNET system suitably and correctly. Root User will install and configure the TOE according to the management guide.

- **A.PYHPROT:** The TOE resides in a physically controlled access facility that prevents unauthorized physical access. Therefore, the physical hardware and software in which the TOE is deployed will be protected from unauthorized physical modification.

- **A.SECENV:** The Operating Systems, Database, Application and Web Server, on which the TOE is running are, fixed against all security bugs and protected against all threats.

- **A.TRUST:** Creation of architecture, coding and administrative functions are done by trusted persons. The designer, programmer (coder) and Root User are responsible for these operations respectively.

2.4. Architectural Information

The TOE composed of multiple software modules that run as a complete IT product on required host computers. The host computers must run with an operating system platform on which the TOE executes; >scopNET consists of the following components:

- **>scopNET GUI :** Graphical User Interface of >scopNET provides management and configuration functions of all >scopNET System. (Network and Attack Configurations, Logs, Reports)
- **>scopNET Server:** This component manages the system. It is responsible for managing network devices (VLAN & ACL Management), agentless enumeration and applying policies.
- **>scopNET Detector:** This component performs ARP sniffing & ARP Blocking.
- **>scopNET Captive Portal GUI & Engine:** This component is a portal for user registration of requesters. It can be a gateway in the guest VLAN or used by wireless controllers for authentication.
- **>scopNET Agent:** Performs inventory collection on computers. This component is installed to the target devices in case of customer's request (customer decides whether to install Agent or not).

2.5. Documentation

Documents below are provided to the customer by the developer alongside the TOE;

Name of Document	Version Number	Date
>scopNET Security Target	1.15	22.06.2018
>scopNET Administration Guide v7	1.5	22.06.2018
>scopNET Getting Started Guide	1.4	22.06.2018
>scopNET Install and Upgrade Guide	1.4	22.06.2018

2.6. IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developers. All the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families Common Criteria and Common Methodology; so the connections between the assurance families and the evaluation evidences has been established. The evaluation results are available in the final Evaluation Technical Report (ETR) of >scopNET v7.

It is concluded that the TOE supports EAL 3. There are 22 assurance families which are all evaluated with the methods detailed in the ETR.

2.6.1. Developer Testing

Developer has prepared TOE Test Document according to the TOE Functional Specification documentation, TOE Design documentation which includes TSF subsystems and its interactions. All SFR-Enforcing TSFIs have been tested by developer. Developer has conducted 98 functional tests in total.

2.6.2. Evaluator Testing

- Independent Testing: Evaluator has chosen 49 developer tests to conduct by itself. Additionally, evaluator has prepared 14 independent tests. TOE has passed all 63 functional tests to demonstrate that its security functions work as it is defined in the ST.
- Penetration Testing: TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, 24 penetration tests have been conducted.

2.7. Evaluated Configuration

The evaluated TOE configuration is composed of;

- >scopNET GUI,
- >scopNET Server,
- >scopNET Detector,
- >scopNET Captive Portal GUI & Engine,
- >scopNET Agent
- Guidance documents

During the evaluation; following documents of the developer were used;

Name of Document	**Version Number**	**Publication Date**
>scopNET Security Target	1.15	22.06.2018
>scopNET Fonksiyonel Özellikler Dokümanı	1.11	16.07.2018
>scopNET Mimari Tasarım Dokümanı	1.12	16.07.2018
>scopNET Güvenli Mimari Dokümanı	1.3	15.03.2018
>scopNET Getting Started Guide	1.4	22.06.2018
>scopNET Install and Upgrade Guide	1.4	22.06.2018
>scopNET Administration Guide	1.5	22.06.2018

NAC_Configuration Management Plan	1.17	31.01.2019
>scopNET Konfigürasyon Yönetimi Dokümanı	1.18	31.01.2019
>scopNET Kurulum ve Teslim Dokümanı	1.3	17.04.2019
>scopNET Geliştirme Ortamı Güvenliği Dokümanı	1.4	31.01.2019
>scopNET Yazılım Yaşam Döngüsü Dokümanı	1.5	31.01.2019
>scopNET Test Kapsam ve Derinlik Dokümanı	1.8	24.09.2018

2.8. Results of the Evaluation

Table below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 4 (EAL 3) components as specified in Part 3 of the Common Criteria.

Assurance Class	**Component**	**Component Title**
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life-Cycle Support	ALC_CMC.3	Authorisation Controls
	ALC_CMS.3	Implementation Representation CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
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

Security Target Evaluation	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing
Vulnerability Analysis	AVA_VAN.2	Vulnerability analysis

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 3 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer about the issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. So for TOE “>scopNET v7”, the results of the assessment of all evaluation tasks are “Pass”.

2.9. Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of “>scopNET v7” 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: >scopNET v7 Security Target

Version: 1.15

Date of Document: 22.06.2018

A public version has been created and verified according to ST-Santizing:

Title: >scopNET v7 Security Target Lite

Version: v.1.1

Date of Document: 11.03.2019

4. GLOSSARY

ADV : Assurance of Development

AGD : Assurance of Guidance Documents

ALC : Assurance of Life Cycle

ASE : Assurance of Security Target Evaluation

ATE : Assurance of Tests Evaluation

AVA : Assurance of Vulnerability Analysis

CC : Common Criteria (Ortak Kriterler)

CCCS : Common Criteria Certification Scheme (TSE)

CCMB: Common Criteria Maintenance Board

CCRA : Common Criteria Recognition Arrangement

CCTL : Common Criteria Test Laboratory

CEM :Common Evaluation Methodology

CMC : Configuration Management Capability

CMS : Configuration Management Scope

DEL : Delivery

DVS : Development Security

EAL : Evaluation Assurance Level

GUI: Graphical User Interface

OPE : Opretaional User Guidance

OSP : Organisational Security Policy

PP : Protection Profile

PRE : Preperative Procedures

PP : Protection Profile

SAR : Security Assurance Requirements

SFR : Security Functional Requirements

ST : Security Target

TOE : Target of Evaluation

TSF : TOE Secırity Functionality

TSFI : TSF Interface

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] BTBD-03-01-TL-01 Certification Report Preparation Instructions, Rel.Date: February 8th 2016

[4] BTTM-CCE-009 DTR v.3.2 BTTM Değerlendirme Teknik Raporu

6. ANNEXES

There is no additional information which is inappropriate for reference in other sections