Certification Report

EAL 4+ (ALC_FLR.1) Evaluation of

TR7 SİBER SAVUNMA A.Ş.
TR7 Application Security Platform Software v1.8

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03.0.00.00//TSE-CCCS-98

TABLE OF CONTENTS

Document Information

Date of Issue	**10.10.2025**
Approval Date	**13.10.2025**
Certification Report Number	**21.0.03/25-004**
Sponsor and Developer	**TR7 SİBER SAVUNMA A.Ş.**
Evaluation Facility	**BEAM TEKNOLOJİ A.Ş.**
TOE Name	**TR7 Application Security Platform Software v1.8**
Pages	**16**

Prepared by *Common Criteria Inspection Expert*	**Mehmet Kürşad ÜNAL**
Common Criteria Inspection Expert	**Yavuz AVCI**
Reviewer (Approver)	**Mert LENGERLİOĞLU**

The experts whose names and signatures are shown as above prepared and reviewed this report.

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
1.0	10.10.2025	All	First Release

DISCLAIMER

This certification report and the IT product/PP 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 Turkish 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 BEAM TEKNOLOJİ A.Ş., 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/PP 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 TR7 Application Security Platform Software v1.8 whose evaluation was completed on May 20th 2025 and whose evaluation technical report was drawn up by BEAM TEKNOLOJİ A.Ş. (as CCTL), and with the Security Target document with version no 1.27 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the Products List at 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

Developer of the IT product: TR7 SİBER SAVUNMA A.Ş.

Evaluated IT product: TR7 Application Security Platform Software v1.8

IT Product Version: 1.8

Name of IT Security Evaluation Facility: BEAM TEKNOLOJİ A.Ş.

Completion date of evaluation: 20.05.2025

Assurance Package: EAL 4+ (ALC_FLR.1)

1.1. Brief Description

TR7 Application Security Platform (ASP) Software (hereinafter TOE) is a security software which provides load balancing (LB), web application firewall (WAF) services. With such services, the TOE provides comprehensive network traffic management and multilayer security of web applications. TR7 ASP software can be located as a hardware or virtual appliance. However, TR7 ASP software cannot be offered as a Software as a Service (SaaS) appliance on cloud. It is deployed into the infrastructure of the customers and can be used by those customers only.

1.2. Major Basic Security and Functional Attributes

The following features are the major security functionality of the TOE;

- **Security Audit**
- **Trusted Path**
- **Data Protection**
- **User Identification and Authentication**
- **TOE Access**
- **Role Based Access Control**
- **Session Management**
- **TOE Trusted Recovery**

1.3. Threats

Agents whose name ends with "**Client**", are unauthorized agents who are not authenticated by the TOE, i.e these agents can harm the TOE without being logged in. "**User**" agents are agents who are either successfully authenticated by the TOE or bypassed the authentication mechanisms. Threat agents (starting with TA) and threats (starting with T) are:

- **TA.PHYSICAL_CLIENT:** Physical clients have access to the TOE console via the VGA or serial port of the device. In virtual environments, such clients have access to the virtualization environment GUI.
- **TA.INTRANET_CLIENT:** Intranet clients are the clients who are in the same local network as the TOE. Such clients have web GUI and SSH access to the TOE.
- **TA.INTERNET_CLIENT:** This threat agent can be anybody in the internet. Even though the TOE is not accessible over the internet unless configured by the admin users, such threat agents can have access to the TOE as a result of misconfiguration.
- **TA.CONSOLE_USER:** Console users are the users who are authenticated through the physical console interface or SSH of the TOE.
- **TA.MANAGER_USER:** These are the TOE users with the "Manager" role who were authenticated in the web GUI. Such users can manage configurations and can manipulate access to the TOE. Admin role and this role are the only roles that can manage access to the TOE.
- **TA.USER_USER:** These are the TOE users with the "User" role who were authenticated in the web GUI. Such users cannot manage configurations, but can view information on the TOE.
- **T.DDOS:** This threat refers to denial of service (DoS) or distributed denial of service (DDoS) attacks. Such attacks can disable access to the web GUI and can be executed by TA.INTRANET_CLIENT or TA.INTERNET_CLIENT threat agents.
- **T.BRUTEFORCE:** Bruteforce attacks can be executed against the TOE. As a result of such attacks, non-TOE users can be granted access to the TOE as being authenticated as a TOE user. Can be executed by TA.INTRANET_CLIENT, TA.PHYSICAL_CLIENT or TA.INTERNET_CLIENT.
- **T.MISCONFIG:** After being authenticated as a TOE user, threat agents might change the access configurations of the TOE. TA.MANAGER_USER threat agents can manipulate access configurations. As a result of this threat, access to the TOE can be affected.
- **T.EAVESDROP:** HTTP/HTTPS/SSH traffic between the TOE and clients can be intercepted by threat agents. Data transfer between the TOE and clients may carry sensitive information in plain text depending on the access configurations of the TOE. Login credentials of TOE users can be acquired as a result of sniffing. Can be executed by TA.INTRANET_CLIENT or TA.INTERNET_CLIENT threat agents.
- **T.PRIVILEDGE_ESCALATION:** Malicious TOE users can gain further priviledges determined by their role groups through the exploitation of the TOE's vulnerabilities. Can be executed by TA.CONSOLE_USER or TA.MANAGER_USER threat agents.
- **T.LOG_DISCLOSURE:** Audit logs kept on the TOE can be reached by unauthorized users. A user can see logs he/she should not have access to, or an unauthorized user can reach the audit logs. Can be executed by TA.INTRANET_CLIENT, TA.PHYSICAL_CLIENT, TA.CONSOLE_USER, TA.MANAGER_USER, TA.USER_USER or TA.INTERNET_CLIENT.
- **T.LOG_STORAGE:** Audit log storage of the TOE can get full after a while. This may result in service discontinuity and/or disfunctionalities. This threat can be executed by anyone who can take actions on the TOE GUI: TA.INTRANET_CLIENT, TA.PHYSICAL_CLIENT,

TA.MANAGER_USER, TA.CONSOLE_USER, TA.USER_USER or TA.INTERNET_CLIENT.

1.4. Organizational Security Policies (OSPs)

OSPs for the TOE are:

- **P.PASSWORD_POLICY:** Users of TOE shall use passwords that obey TR7's password policy ,that is defined in FIA_SOS.1 ,in order to ensure the security of TOE.

1.5. Assumptions

Assumptions for the TOE are:

- **A.NO_GENERAL_PURPOSE** It is assumed that there are no general-purpose computing capabilities (e.g.,compilers or user applications) available on the TOE, other than those installed initially during the setup of the TOE.
- **A.PHYSICAL** Physical security is assumed to be provided by the environment such that the device cannot be physically harmed.
- **A.TRUSTED_ADMIN** TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- **A.TIME_SERVER** It is assumed that a trustworthy computing platform is provided for the TOE and that the trusted time server provides reliable time information.
- **A.BACKUP_SAFETY** It is assumed that the backups of the TOE are stored in a safe environment.
- **A.LOG_SAFETY** It is assumed that the logged audit trail of the TOE is stored in a safe environment, and that enough storage is present to accommodate for the stored logs of the TOE. It is also assumed that the log storage is increased when necessary.
- **A.STRICT_BRUTEFORCE_CONFIG** It is assumed that anti-bruteforce settings "Max. failed login per IP" and "Max. failed login per IP & username" are not intentionally configured above 15 by the admin users to allow bruteforce attacks.

2 -CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03.0.00.00//TSE-CCCS-98
TOE Name and Version	TR7 Application Security Platform Software v1.8
Security Target Title	TR7 ASP Software - Application Security Platform Software Security Target
Security Target Version	1.27
Security Target Date	10.04.2025
Assurance Level	EAL 4+ (ALC_FLR.1)
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	None

Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, conformant • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, conformant
Sponsor and Developer	TR7 SİBER SAVUNMA A.Ş.
Evaluation Facility	BEAM TEKNOLOJİ A.Ş.
Certification Scheme	TSE CCCS

2.2 Security Policy

Security policies for the TOE are:

- **P.PASSWORD_POLICY:** Users of TOE shall use passwords that obey TR7's password policy ,that is defined in FIA_SOS.1 ,in order to ensure the security of TOE.

2.3 Assumptions and Clarification of Scope

Assumptions for the TOE are:

- **A.NO_GENERAL_PURPOSE** It is assumed that there are no general-purpose computing capabilities (e.g.,compilers or user applications) available on the TOE, other than those installed initially during the setup of the TOE.
- **A.PHYSICAL** Physical security is assumed to be provided by the environment such that the device cannot be physically harmed.
- **A.TRUSTED_ADMIN** TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- **A.TIME_SERVER** It is assumed that a trustworthy computing platform is provided for the TOE and that the trusted time server provides reliable time information.
- **A.BACKUP_SAFETY** It is assumed that the backups of the TOE are stored in a safe environment.
- **A.LOG_SAFETY** It is assumed that the logged audit trail of the TOE is stored in a safe environment, and that enough storage is present to accommodate for the stored logs of the TOE. It is also assumed that the log storage is increased when necessary.
- **A.STRICT_BRUTEFORCE_CONFIG** It is assumed that anti-bruteforce settings "Max. failed login per IP" and "Max. failed login per IP & username" are not intentionally configured above 15 by the admin users to allow bruteforce attacks.

For further clarification of scope, see related ST.

2.4 Architectural Information

The Physical Scope of the TOE is the blue area in the figure below. The TOE is limited to the software that provides the Load Balancing and Web Application Firewall functionality. The hardware and the operating system that the TOE runs on is excluded in the scope of the TOE. In addition, backend services and other network elements that can communicate with the TOE are also excluded from the scope.

The TOE is delivered to the customer as a single ISO file that contains the virtual image of the TOE. This ISO file delivered to the customer environment by TR7 Support Team. Hence, only delivered part of the TOE includes TR7 Application Secuirty Platform Software in the format ".iso".

"TR7 ASP Software- AGD - User Guide" and "TR7 ASP Software - AGD – Kurulum" documents are presented to the customers when the support team visit the customers face to face.

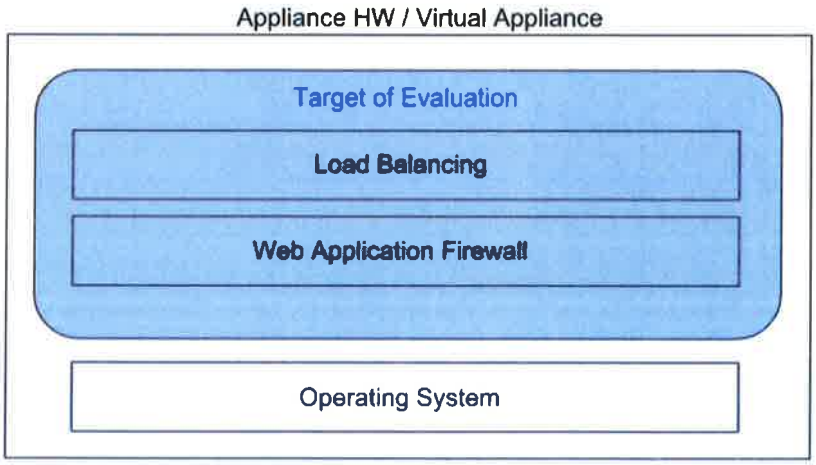

Figure 1: Typical Software/Firmware Environment of TOE

2.5 Documentation

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

Document Name	Version	Release Date
TR7 ASP – Application Security Platform Software Security Target Lite	Version 1.0	09.10.2025

TR7 ASP – Application Security Platform Software User Guide	Version 1.8	15.04.2025
TR7 Application Security Platform® (ASP) Software Kurulum Dokümanı	Version 1.8	15.04.2025

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developer. All the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families and the evaluation evidences has been established. The evaluation results are available at the final Evaluation Technical Report (ETR) of TR7 Application Security Platform Software v1.8. It is concluded that the TOE supports EAL 4 augmented with ALC_FLR.1. There exist 25 assurance families which are all evaluated with the methods detailed in the ETR.

- **Developer Testing:** Developer has prepared TOE Test Document according to the TOE Functional Specification documentation, TOE design documentation which includes TSF subsystems and their iteractions. All SFR-Enforcing TSFIs have been tested by developer. Developer has conducted 43 functional tests in total.
- **Evaluator Testing:** Evaluator has conducted 17 developer tests. Additionally, evaluator has prepared 5 independent tests. TOE has passed all functional 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, 23 penetration tests have been conducted. TOE proved that it is resistant to "Attacker with Enhanced-Basic Attack Potential". In addition, the developer carries out penetration tests regularly. These tests involve simulating real-world attacks to uncover security weaknesses and assess the application's resilience against various attack vectors. No other external penetration test services are used.

2.7 Evaluated Configuration

Evaluated TOE configuration is composed of:

- TR7 Application Security Platform Software v1.8

Also as consistent with the minimum Hardware/Software/OS requirements for the TOE, the test environment presented at the ETR is composed of software and hardware.

Hardware	Software
Processor (Minimum 4 64-bit Cores with 2 GHz +)	TOE
RAM (4096 MB+)	Debian GNU/Linux 10 (buster)
Disk Space 130 GB+	Linux Kernel
	Docker Engine version 20.10.17
	JSON Database (in-memory)

Table 1: *Minimum Software and Hardware Requirements of Test Environment*

2.8 Results of the Evaluation

The table below provides a complete list of the Security Assurance Requirements for the TOE. These requirements consist of the Evaluation Assurance Level 4 (EAL 4) components augmented with ALC_FLR.1 as specified in Part 3 of the Common Criteria.

Class Heading	Class Family	Description	Result
ADV: Development	ADV_ARC.1	Security architecture description	PASS
	ADV_FSP.4	Complete functional specification	PASS
	ADV_IMP.1	Implementation representation	PASS
	ADV_TDS.3	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.4	Production support, acceptance procedures and automation	PASS
	ALC_CMS.4	Problem tracking CM coverage	PASS
	ALC_DEL.1	Delivery procedures	PASS
	ALC_DVS.1	Identification of security measures	PASS
	ALC_FLR.1	Basic flaw remediation	PASS
	ALC_LCD.1	Developer-defined life-cycle model	PASS

Class Heading	Class Family	Description	Result
	ALC_TAT.1	Well-defined development tools	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.2	Analysis of coverage	PASS
	ATE_DPT.1	Testing: basic design	PASS
	ATE_FUN.1	Functional testing	PASS
	ATE_IND.2	Independent testing - sample	PASS
AVA: Vulnerability Analysis	AVA_VAN.3	Focused vulnerability analysis	PASS

2.9 Evaluator Comments / Recommendations

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable with the stated security objectives for the operational environment and it can be suitably addressed.

3 SECURITY TARGET

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

Title: TR7 ASP Software - Application Security Platform Software Security Target

Version: v1.27

Date of Document: April 10, 2025

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

Title: TR7 ASP Software – Application Security Platform Software Security Target Lite

Version: 1.0

Date of Document: 09.10.2025

4 GLOSSARY

CCCS: Common Criteria Certification Scheme

CCMB: Common Criteria Management Board

CCRA: Common Criteria Recognition Arrangement

EAL: Evaluation Assurance Level

FTP: Function of Trusted Path

IoT: Internet of Things

ITC: Inter TSF Confidentiality

MSA: Management of Security Attributes

OSP: Organisational Security Policy

SAR: Security Assurance Requirements

SFR: Security Functional Requirements

SHA: Secure Hash Algorithm

SMF: Specification of Management Functions

ST: Security Target

TLS: Transport Layer Security

TOE: Target of Evaluation

TDC: TSF Data Consistency

TSF: TOE Security 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] BTTM-CCE-074 DTR v.1.2 BTTM Evaluation Technical Report, Version 1.2, Rel. Date: May 28, 2025.

[4] TR7 ASP – Application Security Platform Software Security Target, Version 1.27, Rel. Date: April 10, 2025.

[5] TR7 ASP – Application Security Platform Software Security Target Lite, Version 1.0, Rel. Date: October 9, 2025.

6 ANNEXES

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