Certification Report

EAL 4+ (ALC_FLR.1) Evaluation of

ICTERRA Bilgi ve İletişim Teknolojileri San. Ve Tic. A.Ş.

ATES v1.0 Intelligent Intrusion Detection System

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-45

TABLE OF CONTENTS

DOCUMENT INFORMATION

Date of Issue	August 18, 2017
Approval Date	August 18, 2017
Certification Report Number	21.0.03/17-009
Sponsor and Developer	ICTERRA Bilgi ve İletişim Teknolojileri San. Ve Tic. A.Ş.
Evaluation Facility	Beam Technology
TOE	ATES v1.0 Intelligent Intrusion Detection System
Pages	17

Prepared by	Cem ERDİVAN
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***
1.0	August 18, 2017	All	First Release

DISCLAIMER

This certification report and the IT product 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 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. 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 Beam Technology Testing Facility, 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 ATES v1.0 whose evaluation was completed on August 15, 2017 and whose evaluation technical report was drawn up by Beam Technology (as CCTL), and with the Security Target document with version no 2.9 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

1.1 TOE Overview

TOE is application layer software of an Intrusion Detection System, called ATES.

ATES is a next generation network security system which helps secure institutions' networks from external threats. ATES consists of two major components: ATES agent and ATES Control Center, and ATES is a web based application.

ATES agents are Intrusion Detection Systems. Agents listen to traffic flowing in the corporate network. Neither the ATES Control Center nor the ATES agents make or execute any decision to pass/drop network datagrams. ATES components do not generate any traffic to intervene user sessions either. Their sole transmission on network is for communicaton among TOE components.

ATES components are intelligent network monitoring and intrusion detection tools. ATES uses both signature and anomaly based IDS signature databases to detect cyber attacks. ATES also uses well-known IP reputation algorithms as well as its own IP reputation algorithm to further detect IP domains generating abnormal traffic.

ATES agents can sniff all user traffic received by their network interface cards. ATES agents analyze this traffic by comparing IP addresses, port numbers or other parts of datagrams to predefined patterns, called attack signatures. ATES can also investigate some time dependent patterns, called "anomalies" in the monitored network traffic. Attack patterns are both defined locally by TOE and obtained from several external sources. Anomaly detection algorithms are developed by TOE designers. ATES Agents can create customizable reports indicating the findings and statistics generated according to the patterns that are being sought within the monitored traffic.

ATES has a control center where all agents of the TOE can be monitored and controlled remotely. TOE security function interfaces are on the ATES Control Center as well.

ATES agents do not have an IP address connected to the network interface card that is used to sniff network traffic. Agents have an IP address connected to a second network interface card, which is used to communicate with the Control Center.

1.2 Threats

Threats	Definition
T.NO_AUTH	An unauthorized user may gain access to the TOE and alter the TOE configuration.
T.NO_PRIV	An authorized user of the TOE exceeds his/her assigned security privileges resulting in unauthorized modification of the TOE configuration and/or data.
T.DELETE_LOG	An authorised administrator, using his/her privileges, may purposefully delete the audit logs to cover his/her malicious activities.

Table 1: Threats

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-45
TOE Name and Version	ATES v1.0
Security Target Title	ATES v1.0 Security Target
Security Target Version	v2.9
Security Target Date	August 18, 2017
Assurance Level	EAL4+ (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 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
Protection Profile Conformance	None
Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012, extended • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012, conformant
Sponsor and Developer	ICTERRA Bilgi ve İletişim Teknolojileri San. Ve Tic. A.Ş.
Evaluation Facility	Beam Technology
Certification Scheme	TSE CCCS

2.2 Security Policy

TOE controls access to security management functions through user roles called Product_Admin, Administrator, Auditor and Operator. Product_Admin role is held by the TOE developer to create the initial Administrator and Auditor accounts. Then, the management of TOE is passed on to the customer.

All authorized users are forced to verify their user identities and passwords through session initiation.

Execution of security management functions such as user creation or deletion are subject to audit logging.

“Segregation of duties” principle is implemented through separation of Administrator and Auditor roles. Administrators are not allowed to delete the audit logs generated through their actions and Auditors are not allowed to execute the tasks subject to audit logging.

Operating systems of platforms running TOE components and Administrators of these operating systems (which will be called “Operating System Administrator” in the rest of that document) are outside the scope of TOE.

2.3 Assumptions and Clarification of Scope

Policy	Definition
P.ACCESS	None of the authorized users (users associated to Product_Admin, Administrator, Auditor and Operator roles) shall have access to TOE through Internet. Authorized users shall not have direct access to the agents either. Authorized users shall access the agents only through the Control Center. Figure 2 gives a general overview of TOE and the corporate network.
P.AUDIT	Personnel and procedures shall be in place to monitor and manage the audit logs generated by ATES components.
P.SEGREGATION	Personnel and procedures shall be in place to segregate the “Auditor” and “Administrator” roles.

Table 2: Organizational Security Policies

Assumption	Definition
A.MANAGE	Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.
A.NOEVIL	Operating system administrators of platforms where TOE components are running and users accessing the local area network are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.HARDENING	Operating system and virtualization software executing on platforms where TOE components are running are hardened according to industry standards.
A.LOCATE	The platforms on which the TOE resides are assumed to be located within a facility that provides controlled access.
A.TIMESOURCE	The system where TOE is located has, or allows access to, an NTP server.
A.PHYSEC	The TOE is physically secure. Only authorized personnel has physical access to the system which hosts the TOE.

Table 3: Assumptions

2.4 Architectural Information

2.4.1 Logical Scope

TSF	Description
Security Management	Administrators can configure the TOE, accessing the Control Center interface via a web browser.
Security Audit	The TOE generates audit logs of management functions as well as several system events. Audit logs may be reviewed on the ATES Control Center interface.
User Data Protection	The TOE enforces discretionary access rules using an access control list with user attributes. Some user attributes may be refined during initialization or modified later at the ATES Control Center interface by authorized administrators.
Identification and Authentication	Legitimate users defined by Administrators are forced to authentication at the Control Center interface via declaration of user attributes (user name and password).

2.4.2 Physical Scope

The TOE is a software and consists of the following components:

- ATES Control Center Application
- ATES IDS Agents Application

Applications execute on (at least) two separate computers; The Control Center computer and (at least) one Agent computer(s).

ATES Control Center Application is a web application. Hence, a third computer, a “terminal computer” is required to access the services provided by the Control Center. Terminal Computer is outside the scope of TOE.

Control Center Application deals with management and monitoring of agents. Security features are initiated through the Control Center application as well.

Agent Application listens to network traffic, conducts the analysis requested by the Control Center and returns the results to the Control Center.

Like most application software, TOE components depend on the services provided by the operating system as well as other software to execute their functions. Figure 1 given below briefly summarizes the software organization of the platforms hosting TOE components: The Control Center computer and the Agent computer. TOE components, operating systems and the other third party software the TOE components depend on are observable on Figure 1. Hence Figure 1 presents both the TOE components and their operational environment.

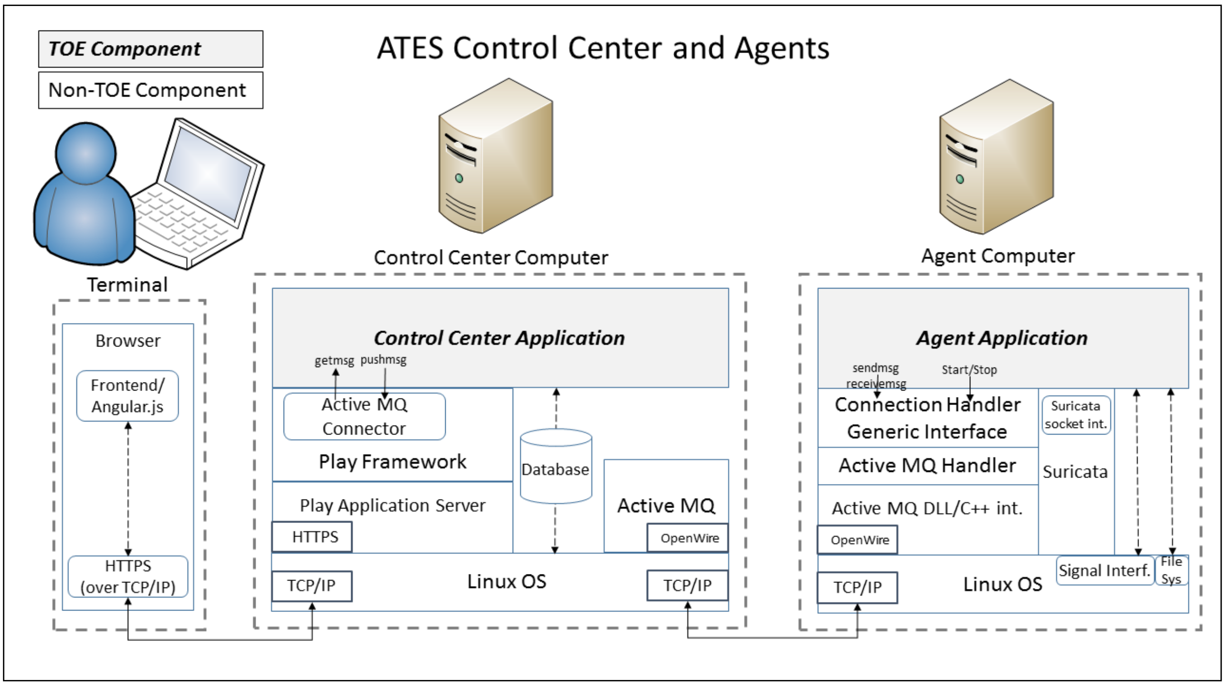

Figure-1 TOE Boundary

2.4.3 Software environment of TOE

The TOE components run with the following software:

Software	Version/Model Number
Operating System	CentOS 7 64-bit
Other Software	Apache ActiveMQ 5.14.0 Play Framework 2.4.3 MySQL 5.7.x Google AngularJS 1.4
WEB browser (running on terminal)	Google Chrome 49.0.x (min.)

Table 4 – ATES Control Center software requirements

Software	Version/Model Number
Operating System	CentOS 7 64-bit
Other Software	Apache ActiveMQ 5.12.0 Suricata 3.1.2 MySQL 5.7.x

Table 5 – ATES IDS Agent software requirements

2.4.4 Hardware Environment of TOE

Minimum hardware requirements of ATES components are listed below:

Aspect	Minimum Requirements
CPU	64-bit
RAM	8 Giga Byte
Hard Disk	20 Tera Bytes of free space
Network Interface Card	CentOS 7 64-bit compatible

Table 6 – Hardware requirements of ATES Control Center

Aspect	Minimum Requirements
CPU	64-bit, dual core
RAM	8 Giga Byte
Hard Disk	20 Tera Bytes of free space
Network Interface Card	CentOS 7 64-bit compatible

Table 7 – Hardware requirements of ATES IDS agents

2.5 Documentation

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

Document Name	Version	Release Date
ATES v1.0 Security Target	v2.9	August 18, 2017
ATES v1.0 Guidance Document	v1.4	April, 2017

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 v3.2 of ATES v1.0. It is concluded that the TOE supports EAL 4+ (ALC_FLR.1).

IT Product Testing is mainly realized in two parts:

1-Developer Testing: (195 Tests)

- **TOE Test Coverage:** Developer has prepared TOE Test Document according to the TOE Functional Specification documentation.

- **TOE Functional Testing:** Developer has made functional tests according to the test documentation. Test plans, test scenarios, expected test results and actual test results are in the test documentation.

2- Evaluator Testing:

Independent Testing: The evaluator conducted testing using 100 of developer tests found in the developer's test plan and procedures (actual total number is 40 since evaluator merged some of the developer tests into one test). Additionally, the evaluator conducted 36 independent tests prepared by the evaluators themselves. All off these tests have ensured that TOE is capable of demonstrating the functional requirements stated in security document. TOE has successfully passed all tests.

Penetration Testing: Evaluator has done 22 penetration tests to find out if TOE`s vulnerabilities can be used for malicious purposes. During devising the tests, a flaw hypothesis was prepared considering:

- SFRs in security target,
- Architectural elements in architecture document,
- Guidance documents,
- Internet search for publicly known vulnerabilities of TOE and tools used to create TOE etc.

TOE has successfully passed all tests.

2.7 Evaluated Configuration

Evaluated configuration for the TOE is as follows:

- ATES Control Center 1.0
- ATES IDS Agent 1.0

2.8 Results of the Evaluation

The verdict for the CC Part 3 assurance components (according to EAL4+ (ALC_FLR.1) and the security target evaluation) is summarized in the following table:

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 of the TSF	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
	ALC_TAT.1	Well-defined development tools	PASS

Class Heading	Class Family	Description	Result
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: security enforcing modules	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

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of “ATES v1.0” 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: ATES v1.0 Security Target
Version: v2.9
Date of Document: August 18, 2017

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 ACRONYMS

ATES:	**A**kıllı **TE**hdit izleme **S**istemi – Intelligent Intrusion Detection System
CC:	Common Criteria version 3.1 (ISO/IEC 15408)
EAL:	Evaluation Assurance Level
IDS:	Intrusion Detection System
SFR:	Security Functional Requirement
SMF:	Security Management Function
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Function

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012

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

[4] ETR v3.2 of ATES v1.0, Rel. Date: August 15, 2017

[5] ATES v1.0 Security Target, Version 2.9, Rel. Date: August 18, 2017