Certification Report

EAL4+ (ATE_DPT.2, AVA_VAN.5) Evaluation of

ASELSAN Inc.

ASELSAN STC-8255 V1.0

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-74

Doküman Kodu: BTBD-03-01-FR-01   Yayın Tarihi: 04.08.2015   Revizyon Tarih/No: 06.03.2019/6

Bu dokümanın güncelliği, elektronik ortamda TSE Doküman Yönetim Sisteminden takip edilmelidir.   Sayfa 1 / 19

TABLE OF CONTENTS

Doküman Kodu: BTBD-03-01-FR-01   Yayın Tarihi: 04.08.2015   Revizyon Tarih/No: 06.03.2019/6

Bu dokümanın güncelliği, elektronik ortamda TSE Doküman Yönetim Sisteminden takip edilmelidir.   Sayfa 2 / 19

Document Information

Date of Issue	*20.05.2021*
Approval Date	*21.05.2021*
Certification Report Number	*21.0.03/21-006*
Sponsor and Developer	*ASELSAN ELEKTRONİK SANAYİ VE TİC.A.Ş.*
Evaluation Facility	*TÜBİTAK OKTEM*
TOE	*ASELSAN STC-8255 V1.0*
Pages	19

Prepared by	*Halime Eda BİTLİSLİ 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	*20.05.2021*	*All*	*First Release*

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 conformant 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 (CCCS) provides an evaluation and certification service to ensure the reliability of Information Security 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, TÜBİTAK OKTEM 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 *ASELSAN STC-8255 V1.0* whose evaluation was completed on *03.05.2021* and whose evaluation technical report was drawn up by *03.05.2021* (as CCTL), and with the Security Target document with version no 0.12 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 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: ASELSAN STC-8255

IT Product version: 1.0

Developer's Name: Aselsan Inc.

Name of CCTL: TÜBİTAK OKTEM

Assurance Package: EAL4+ (ATE_DPT.2, AVA_VAN.5)

Completion date of evaluation: 03.05.2021

1.1. Brief Description

The Target of Evaluation (TOE) is a vehicle unit (VU) in the sense of Annex 1B[1] intended to be installed in road transport vehicles to record, store, display, print and output data related to driver activities.

The VU records and stores user activities data in its internal data memory, it also records user activities data in tachograph cards. The VU outputs data to display, printer and external devices. It is connected to a motion sensor with which it exchanges vehicle's motion data. Users identify themselves to the VU using tachograph cards. Moreover, an internal GNSS module with its antenna connector is optionally offered as an independent source of motion.

The TOE receives motion data from the motion sensor and activity data via the facilities for entry of user's. It stores all these user data internally and can export them to the tachograph cards inserted, to the display, to the printer, and to electrical interfaces.

---
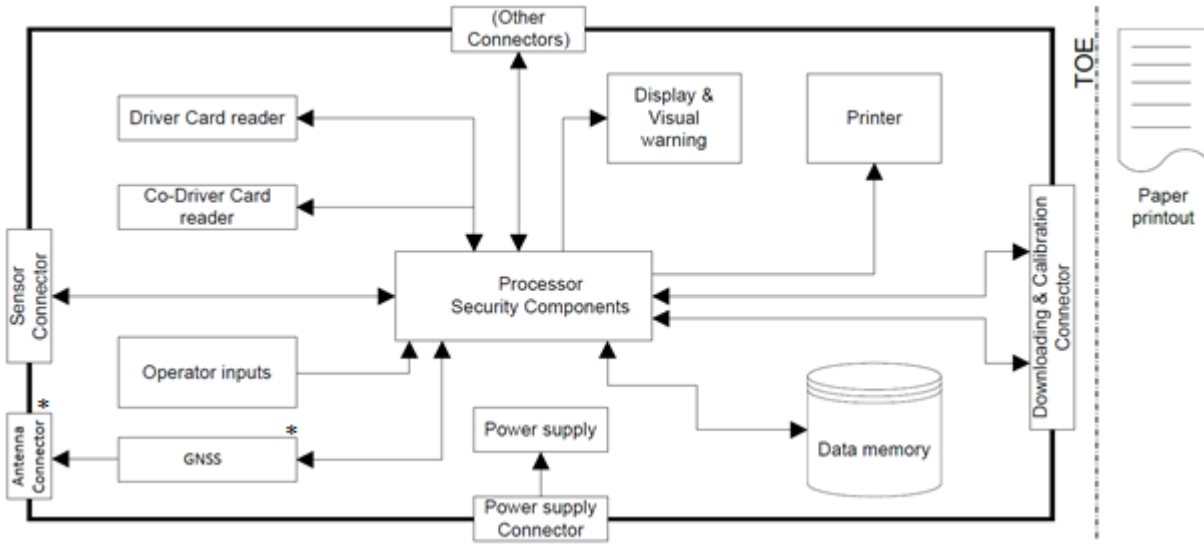
*: optional

Figure 1: Block Diagram of the TOE

1.2.   *Major Security Features*

The data to be measured and recorded and then to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed.

The main security feature of the TOE is:

a)   The data recorded and stored in such a way as to prevent unauthorized access to and manipulation of the data and detecting any such attempts,

b)   The integrity and authenticity of data exchanged between the motion sensor and the vehicle unit,

c) The integrity and authenticity of data exchanged between the recording equipment and the tachograph cards,

d) The integrity and authenticity of data downloaded,

e) Integrity, authenticity and confidentiality of software upgrade.

The main security feature stated above is provided by the following major security services

a) Identification and authentication of motion sensor, tachograph cards and **management device**,

b) Access control to functions and stored data,

c) Accountability of users,

Doküman Kodu: BTBD-03-01-FR-01   Yayın Tarihi: 04.08.2015   Revizyon Tarih/No: 06.03.2019/6

Bu dokümanın güncelliği, elektronik ortamda TSE Doküman Yönetim Sisteminden takip edilmelidir.   Sayfa 7 / 19

d) Audit of events and faults,

e) Object reuse for secret data,

f) Accuracy of recorded and stored data,

g) Reliability of services,

h) Data exchange with motion sensor, tachograph cards and external media (download function).

1.3. Threats

Threats averted solely by the TOE:

T.Card_Data_Exchange   Users could try to modify user data while exchanged between TOE and tachograph cards (addition, modification, deletion, replay of signal).

T.Faults   Faults in hardware, software, communication procedures could place the TOE in unforeseen conditions compromising its security.

T.Output_Data   Users could try to modify data output (print, display or download).

Threats averted by the TOE and its operational environment:

T.Access   Users could try to access functions not allowed to them (e.g. drivers gaining access to calibration function).

T.Calibration_Parameters   Users could try to use miscalibrated equipment[1] (through calibration data modification, or through organisational weaknesses).

T.Clock   Users could try to modify internal clock.

T.Design   Users could try to gain illicit knowledge of design[1] either from manufacturer's material (through theft, bribery, etc.) or from reverse engineering.

T.Environment   Users could compromise the TOE security through environmental attacks (thermal, electromagnetic, optical, chemical, and mechanical, etc.).

T.Fake_Devices   Users could try to connect fake devices (motion sensor, smart cards) to the VU .

T.Hardware   Users could try to modify TOE hardware.

T.Identification   Users could try to use several identifications or no identification.

2. CERTIFICATION RESULTS

2.1. *Identification of Target of Evaluation*

Certificate Number	*21.0.03/TSE-CCCS-74*
TOE Name and Version	*Aselsan STC-8255 v1.0*
Security Target Title	Aselsan STC-8255 v1.0 Digital Tachograph Vehicle Unit Security Target
Security Target Version	*0.12*
Security Target Date	*27.04.2021*
Assurance Level	*EAL4+ (ATE_DPT.2, AVA_VAN.5)*
Criteria	• *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017* • *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017* • *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017*
Methodology	*Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017*
Protection Profile Conformance	*Protection Profile Digital Tachograph-Vehicle Unit (VU-PP), BSI-CC-PP-0057, Version 1.0, 13th July 2010, Bundesamt für Sicherheit in der Informationstechnik*
Sponsor and Developer	*ASELSAN ELEKTRONİK SANAYİ VE TİC.A.Ş.*
Evaluation Facility	*TÜBİTAK OKTEM*
Certification Scheme	*TSE CCCS*

2.2. Security Policy

The TOE and/or its environment must comply with the Organisational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.

The detail of these policies is documented in the Security Target, section 4.5.

2.3. Assumptions and Clarification of Scope

Assumptions for the operational environment of the TOE are;

A.Activation	Vehicle manufacturers and fitters or workshops activate the TOE after its installation before the vehicle leaves the premises where installation took place.
A.Approved_Workshops	The Member States approve, regularly control and certify trusted fitters and workshops to carry out installations, calibrations, checks, inspections, repairs.
A.Card_Availability	Tachograph cards are available to the TOE users and delivered by Member State authorities to authorised persons only.
A.Card_Traceability	Card delivery is traceable (white lists, black lists), and black lists are used during security audits.
A.Controls	Law enforcement controls will be performed regularly and randomly, and must include security audits (as well as visual inspection of the equipment).
A.Driver_Card_Uniqueness	Drivers possess, at one time, one valid driver card only.
A.Faithful_Calibration	Approved fitters and workshops enter proper vehicle parameters in recording equipment during calibration.
A.Faithful_Drivers	Drivers play by the rules and act responsibly (e.g. use their driver cards, properly select their activity for those that are manually selected, etc.)
A.Regular_Inspections	Recording equipment will be periodically inspected and calibrated. Inspection personal is educated about the security check points of the TOE.

2.4. Architectural Information

A block diagram which consists of the main components and the interfaces of the TOE is given in Figure below.
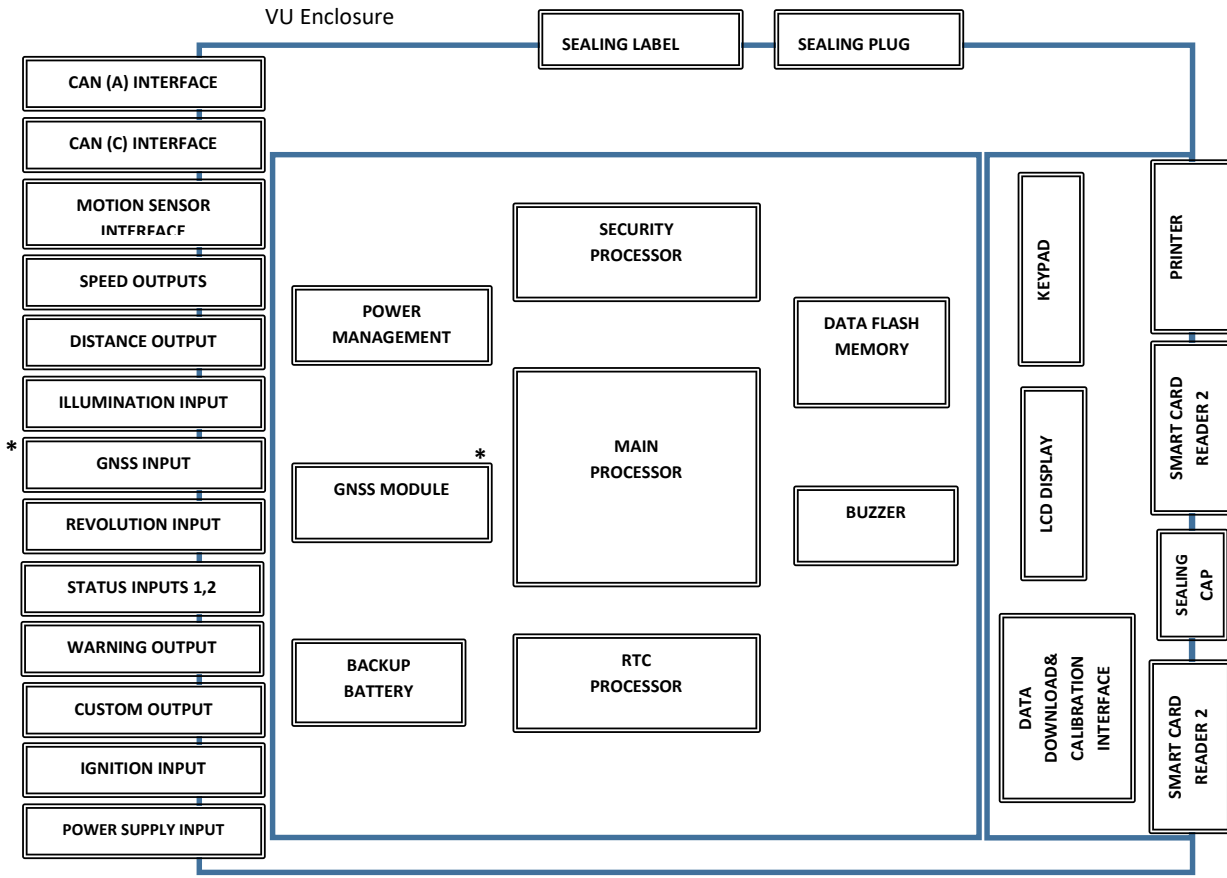
*: optional

Figure 2: Aselsan Digital Tachograph Vehicle Unit

The following components are in the physical scope of the TOE;

Application Processor (AP) provides main functionality and executes TOE control and interfacing functions. Application processor directly manages the functions of peripheral units of the TOE.

Security Processor (SP) executes security related functions and keeps main secure assets. It conforms to common criteria assurance level of EAL5 augmented by ALC.DVS_2 and AVA_VAN.5. It has security features to help to protect against advanced form of attacks.

RTC Processor (RTP) has discrete functions of keeping the time information with its internal RTC.

Power Management consists of various switching power up or down converters, which provides necessary voltage levels of internal integrated and other lumped circuits.

Data Flash Memory is serial access type nonvolatile memory.

Backup Battery is the alternative power supply unit of RTC Processor (RTP). In case of main power supply interruption, it powers this processor and keeps RTC running.

Smart Card Reader is the connection port for smart card (Smart Card1 and Smart Card2).

CAN A Interface is for the interconnection of the TOE to a CAN bus in the vehicle.

CAN C Interface is for the interconnection of the TOE to another CAN bus in the vehicle.

Motion Sensor Interface is the connection port for the Motion Sensor to detect vehicle speed.

Speed Outputs are the indicators of vehicle speed in an electrical pulse width modulated format.

Distance Output is the electrical pulse output to indicate the distance of the vehicle to external instrument clusters.

Illumination Input is for acquiring the cabin illumination level in terms of an electrical value.

Revolution Input is for acquiring the revolution speed data of vehicle revolution sensor.

Status Input 1 and 2 are for the determination of the logic level for the external contacts.

Warning Output is for sharing any warning with the external equipment.

Custom Out is an asynchronous serial output line in order to communicate with the external equipment.

Ignition Input is for the detection of vehicle ignition status.

Power Supply Input provides the voltage for the operation of the TOE.

Printer is the interface to print reports.

Data Download & Calibration is the interface for data downloading and calibration.

LCD Display is a built in visual output indicator for the user.

Keypad is the input interface for the user interaction.

Buzzer is the sound source to warn-out user about the status changes and the events.

VU Enclosure provides casing to the TOE.

Sealing Label is tamper-evident label carrying a unique serial number which is also embedded into the VU software.

Sealing Plug is a tamper-evident breakable mechanical part covering the locking joint of VU enclosure.

Sealing Cap is tamper-evident mechanical part covering a joint screw.

GNSS Module with **GNSS Input** is optionally offered as an independent source of motion interface.

Doküman Kodu: BTBD-03-01-FR-01   Yayın Tarihi: 04.08.2015   Revizyon Tarih/No: 06.03.2019/6

Bu dokümanın güncelliği, elektronik ortamda TSE Doküman Yönetim Sisteminden takip edilmelidir.   Sayfa 12 / 19

2.5. Documentation

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

Name of Document	Version Number	Date
Aselsan STC-8255 v1.0 Digital Tachograph Vehicle Unit Operation Manual	*0.7*	*27.04.2021*
Aselsan STC-8255 v1.0 Digital Tachograph Vehicle Unit Security Target Lite	*0.13*	*14.10.2020*
Aselsan STC-8255 v1.0 Digital Tachograph Vehicle Unit Preparation Manual	*0.7*	*27.04.2021*

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 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 Aselsan STC-8255 v1.0.

It is concluded that TOE supports EAL4+ (ATE_DPT.2, AVA_VAN.5). IT Product Testing is composed of two parts:

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. Developer has conducted 11 functional tests in total.

2.6.2. Evaluator Testing

- Independent Testing: Evaluator has conducted 11 tests of developer and also has prepared 10 independent tests. TOE has passed all functional tests to demonstrate that its security functions work as it is defined in the ST.

- Penetration Testing: Evaluator has conducted 10 penetration tests to find out TOE's vulnerabilities that can be used for malicious purposes.

2.7. Evaluated Configuration

The evaluator has performed an installation and configuration of the TOE using the information provided in the preparation manual and the operational manual. Also evaluator satisfied the security objectives for the operational environment described in the security target.

The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to security target.

The evaluated TOE configuration is composed of;

The software version of the product for which the evaluation is completed is 1.0. The 1.0 software package (STC8255-release-v1_0) contains software of 3 different processors.

For AP processor: avu-app-release-v1_0_652-20210427.bin

For RTP processor: avu-rtp-release-v1_0_101-20210427.bin

For SP processor: avu-sp-release-v0_43_81-20210408.bin
These three software are combined with a software specific to Aselsan and then signed.

A single software package and the signed one: STC8255-release-v1_0.fup is deployed into the device.

The product hardware evaluated is 5820-8255-1417A. This hardware includes all optional features.

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 4) components as specified in Part 3 of the Common Criteria, augmented with ATE_DPT.2, AVA_VAN.5.

Assurance Class	Component	Component Title
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic Modular Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life-Cycle Support	ALC_CMC.4	Production Support, Acceptance Procedures and automation
	ALC_CMS.4	Problem Tracking CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Sufficiency of Security Measures
	ALC_LCD.1	Developer Defined Life-Cycle Model
	ALC_TAT.1	Well-Defined Development Tools
Security Target	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives

Doküman Kodu: BTBD-03-01-FR-01   Yayın Tarihi: 04.08.2015   Revizyon Tarih/No: 06.03.2019/6

Bu dokümanın güncelliği, elektronik ortamda TSE Doküman Yönetim Sisteminden takip edilmelidir.   Sayfa 15 / 19

Evaluation	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: security enforcing modules
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing
Vulnerability Analysis	AVA_VAN.5	Advanced methodical vulnerability analysis

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4+ (ATE_DPT.2, AVA_VAN.5) 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 "Aselsan STC-8255 v1.0", the results of the assessment of all evaluation tasks are "Pass".

2.9.   Evaluator Comments / Recommendations

No recommendations have been communicated to CCCS by the evaluators related to the evaluation process of "Aselsan STC-8255 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: Aselsan STC-8255 v1.0 Digital Tachograph Vehicle Unit Security Target

Doküman Kodu: BTBD-03-01-FR-01   Yayın Tarihi: 04.08.2015   Revizyon Tarih/No: 06.03.2019/6

Bu dokümanın güncelliği, elektronik ortamda TSE Doküman Yönetim Sisteminden takip edilmelidir.   Sayfa 16 / 19

Version: v0.12

Date of Document: 27.04.2021

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

Title: *Aselsan STC-8255 v1.0 Digital Tachograph Vehicle Unit Security Target Lite*

Version: *0.13*

Date of Document: *18.05.2021*

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)

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

OPE : Opretaional User Guidance

OSP : Organisational Security Policy

PP : Protection Profile

SAR : Security Assurance Requirements
SF :   Security Function

SFP :   Security Function Policy

SFR : Security Functional Requirements

TOE : Target of Evaluation

TSF : TOE Secırity Functionality

TSFI : TSF Interface

5. BIBLIOGRAPHY

[1]: Appendix 2 of Annex-1B of Council Regulation (EEC) No 3821/85 – Tachograph Cards Specification

[2]: Council Regulation (EEC) No 3821/85 on recording equipment in road transport, Official Journal of the European Communities

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

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

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

Doküman Kodu: BTBD-03-01-FR-01   Yayın Tarihi: 04.08.2015   Revizyon Tarih/No: 06.03.2019/6

Bu dokümanın güncelliği, elektronik ortamda TSE Doküman Yönetim Sisteminden takip edilmelidir.   Sayfa 18 / 19

6. ANNEXES

There is no additional information to this report.