Certification Report

EAL 4+ (AVA_VAN.5, ATE_DPT.2) Evaluation of

ASELSAN Inc.
Aselsan Digital Tachograph Vehicle Unit
STC-8250 A version 1.0.0

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-35

TABLE OF CONTENTS

DOCUMENT INFORMATION

Date of Issue	11.08.2016
Approval Date	11.08.2016
Certification Report Number	21.0.03/16-004
Sponsor and Developer	ASELSAN Inc.
Evaluation Facility	Epoche & Espri S.L.U.
TOE	Aselsan Digital Tachograph Vehicle Unit version 1.0.0
Pages	23

Prepared by	Cem ERDİVAN
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	11.08.2016	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 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 (CCCS) 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 Epoche & Espri S.L.U, 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 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 Digital Tachograph Vehicle Unit version 1.0.0 whose evaluation was completed on 11.08.2016 and whose evaluation technical report was drawn up by Epoche & Espri S.L.U (as CCTL), and with the Security Target document with version no 1.6 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 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 Digital Tachograph Vehicle Unit
IT Product version: v1.0.0
Developer's Name: ASELSAN Inc.
Name of CCTL: Epoche & Espri S.L.U
Assurance Package: EAL4+ (ATE_DPT.2, AVA_VAN.5)
Completion date of evaluation: 11.08.2016

The Target of Evaluation (TOE) addressed by the current Security Target is a vehicle unit (VU) in the sense of Annex I B [6] intended to be installed in road transport vehicles. Its purpose is 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.

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.

The block diagram of the TOE is depicted in Figure 1 (it is noted that although the printer mechanism is part of the TOE, the paper document once produced is not).

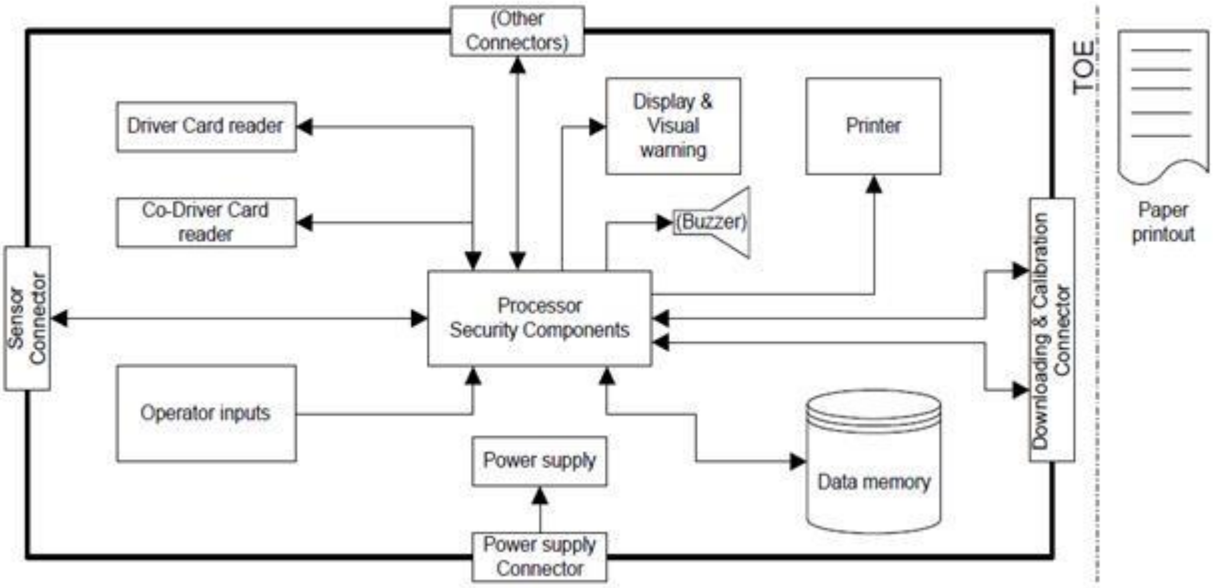

Figure 1: Block Diagram of the TOE

1.1 TOE Major Security Features for Operational Use

The main security feature of the TOE is as specified in [7]: The data to be measured (the physical data measurement is performed by the motion sensor and the motion sensor is not part of the current TOE) 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. It concretely means that security of the VU aims to protect:

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, and
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, and tachograph cards,
b) Access control to functions and stored data,
c) Accountability of users,
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),
i) Secure software upgrade.

1.2 Threats

Threat	Description
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).
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 (through calibration data modification, or through organizational weaknesses).
T.Clock	Users could try to modify internal clock.
T.Design	Users could try to gain illicit knowledge of design 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, mechanical, etc.).
T.Fake_Devices	Users could try to connect fake devices (motion sensor, smart cards) to the TOE.
T.Hardware	Users could try to modify TOE hardware.
T.Identification	Users could try to use several identifications or no identification.
T.Motion_Data	Users could try to modify the vehicle’s motion data (addition, modification, deletion, replay of signal).
T.Power_Supply	Users could try to defeat the TOE security objectives by modifying (cutting, reducing, increasing) its power supply.
T.Security_Data	Users could try to gain illicit knowledge of security data during security data generation or transport or storage in the equipment.
T.Software	Users could try to modify TOE software.
T.Stored_Data	Users could try to modify stored data (security or user data).
T.Tests	The use of non-invalidated test modes or of existing back doors could compromise the TOE security.
T.Non_Activated	Users could use non-activated equipment.

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-35
TOE Name and Version	Aselsan Digital Tachograph Vehicle Unit v1.0.0
Security Target Document Title	Aselsan Digital Tachograph Vehicle Unit v1.0.0 Security Target
Security Target Document Version	1.6
Security Target Document Date	08.08.2016
Assurance Level	EAL4+ (ATE_DPT.2, AVA_VAN.5)
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 • JIL-Minimum-site-security-requirements v.1.1
Protection Profile Conformance	Protection Profile Digital Tachograph-Vehicle Unit (VU-PP), BSI-CC-PP-0057, Version 1.0, 13th July 2010
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	ASELSAN Inc.
Evaluation Facility	Epoche & Espri S.L.U
Certification Scheme	TSE CCCS

2.2 Security Policy

TOE Security Function	***Description***
Security Audit	The TOE records security breach attempts (motion sensor authentication failure, tachograph card authentication failure, unauthorised change of motion sensor, card data input integrity error, stored user data integrity error, internal data transfer error, hardware sabotage), last card session not correctly closed error, motion data error event, power supply interruption event and the TOE internal fault which affect the security of the TOE. The TOE enforces audit records storage rules and also stores audit records generated by the motion sensor in its data memory. The audit records can be reviewed on TOE display, printed by the TOE printer and downloaded to an external media.
Cryptographic Support	The TOE performs cryptographic operations and supports functions for the generation, distribution, access and destruction of cryptographic keys.
User Data Protection	The TOE manages and checks access control rights to functions and to data. It enforces mode of operation selection rules. After the TOE activation, only in calibration mode, may calibration and time adjustment functions be accessed. The TOE checks user data in the data memory for integrity errors. Tachograph cards can not be released before relevant data stored to them. The TOE verifies the integrity and authenticity of data imported from the tachograph cards. The TOE exports data to tachograph cards and to external media with associated security attributes such that the card or the external media is able to verify its integrity and authenticity.
Identification & Authentication of Motion Sensor and Tachograph Cards	The TOE enforces identification and authentication of the motion sensor and the tachograph cards.The TOE requires workshops to be authenticated through a PIN check. Before allowing any interaction, the TOE authenticates the management device.
Security Management	All commands, actions or test points, specific to the testing needs of the manufacturing phase is disabled and removed before the TOE activation. It is not possible to restore them for later use. There is no way to analyze or debug the software in the field after the TOE activation. All processors are protected by a hardware implementation, and any attempt to reach them is detected as hardware sabotage. Moreover, all inputs from external sources are not accepted as executable code. Only the program upgrade is accepted to upgrade the software after checking its signature.
Protection of the TSF	The TSF preserves a secure state upon detection of an internal fault during self test. The VU detects deviations from the specified values of the power supply, including cut-off. In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset conditions, the VU resets cleanly.
Communication	An evidence of origin is generated for data downloaded to external media. The TOE provides a capability to verify the evidence of origin of downloaded data to the recipient by relating the TOE identity of the information and the data to be downloaded to external media to which the evidence applies. Data signature is generated for the verification of the evidence of origin of information to the recipient by following PKCS1.

TOE Security Function	*Description*
Privacy	TOE is designed so that its users are unable to observe the cryptographic operations using any TOE external interface in order to gain the values of cryptographic keys being to keep secret.
Resource utilization	TOE is designed so as to ensure that its resources required for the functions and data covered by the SFRs is obtained when required and that resources are not requested nor retained unnecessarily.

2.3 Assumptions and Clarification of Scope

Organizational Security Policy	*Description*
OSP.Accountability	The TOE must collect accurate accountability data.
OSP.Audit	The TOE must audit attempts to undermine system security and should trace them to associated users.
OSP.Processing	The TOE must ensure that processing of inputs to derive user data is accurate.
OSP.Test_Points	All commands, actions or test points, specific to the testing needs of the manufacturing phase of the TOE must be disabled or removed before the TOE activation during the manufacturing process.
OSP.Type_Approved_MS	The TOE only operates together with a motion sensor being type approved according to Annex IB [6].
OSP.PKI	The European Authority establishes a PKI according to [8] sec. 3.1.1 (starting with ERCA). This PKI is used for device authentication (TOE <-> Tachograph Cards) and for digital signing the user data to be downloaded. The European Authority properly operates the ERCA steering other levels (the Member State and the equipment levels) of the PKI. The ERCA securely generates its own key pair (EUR.PK and EUR.SK) and Member State certificates (MSi.C) over the public keys of the MSCAs. The ERCA ensures that it issues MSi.C certificates only for the rightful MSCAs. The ERCA issues the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules. MSCAs securely generates their own key pairs (Msi.PK and Msi.SK) and equipment certificates (EQTj.C) over the public keys of the equipment. MSCAs ensures that they issue EQTj.C certificates only for the rightful equipment.
OSP.MS_Keys	The European Authority establishes a special key infrastructure for management of the motion sensor keys according to [9] (starting with ERCA). This key infrastructure is used for device authentication (TOE <-> MS). The European Authority properly operates the ERCA steering other levels (the Member State and the equipment levels) of this key infrastructure. The ERCA securely generates both parts (K_{mVU} and K_{mWC}) of the master key (K_m). The ERCA ensures that it securely convey this key material only to the rightful MSCAs. The ERCA issues the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules. MSCAs securely calculates the motion sensor identification key (K_{ID}) and the motion sensor's credentials: MS individual serial number encrypted with the identification key ($Enc(K_{ID}\|N_S)$) and MS individual pairing key encrypted with the master key ($Enc(K_M\|K_P)$). MSCAs ensures that they issue these MS credentials, K_{mVU} and K_{mWC} only to the rightful equipment.
OSP.Management_Device	The Management Device supports the appropriate communication interface with the VU and secures the relevant secrets inside the MD as appropriate.

Assumption	*Description*
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

Below figure is a block diagram of the main components and the interfaces of the TOE:

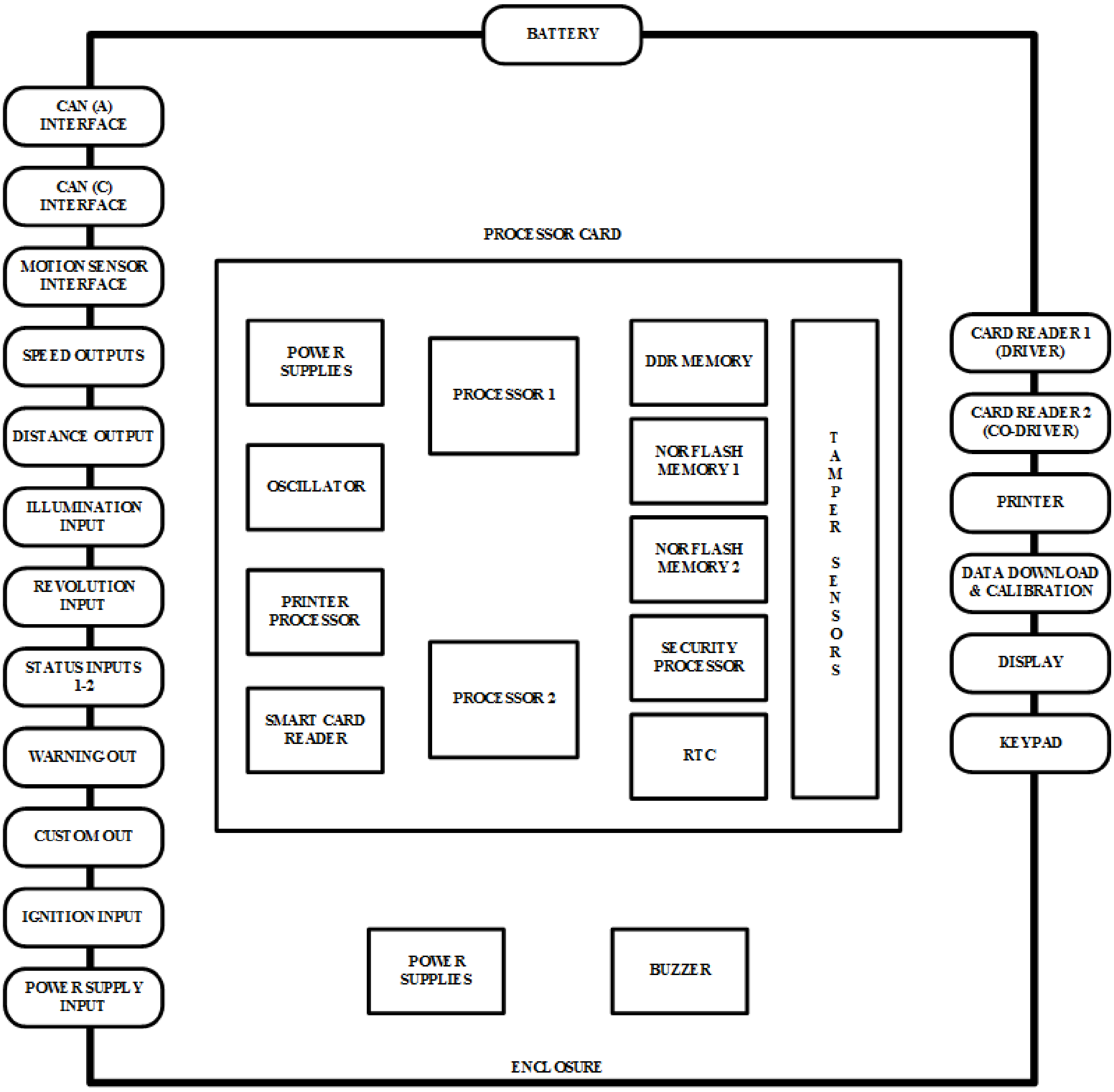

Figure 2 : Aselsan Digital Tachograph Vehicle Unit

- **Processor Card** is the main processing unit of the TOE. All processors and the peripheral units are on this card. Processor Card is used as the system main controller. Main Processor on this card has System On Chip (SOC) architecture.
- **Processor1** executes general TOE control and interfacing functions.
- **Processor2** supports the Security Processor.
- **Security Processor** executes tamper detection functions.
- **RTC (Real Time Clock)** keeps the time information as the reference time source for the operation of the TOE.
- **Tamper Sensors** are the detectors. These electronic circuits are connected to the Security Processor.
- **Oscillator** supplies the clock signal for the operation of the Processors.
- **Power Supplies** on the Processor Card generates local voltages necessary for the operation of the electronics.

- **DDR Memory** is the storage medium for the Processor1.
- **NOR Flash Memory1** is used for the code storage.
- **NOR Flash Memory2** is used as the mass storage medium.
- **Printer Processor** serves as a slave to the Processor1. Any data that will be printed is transferred to the Printer Processor which controls the printer interface and the illumination input.
- **Battery** supplies energy for the operation. Battery is replacable and placed in a slot on the enclosure of the VU.
- **Smart Card Reader** is an integrated circuit providing electrical interface between Processor1 and card readers (Card Reader 1 and Card Reader 2).
- **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 a pulse width modulated format.
- **Distance Output** is the pulse output to indicate the distance of the vehicle to external cluster displays.
- **Illumination Input** is for acquiring the cabin illumination level.
- **Revolution Input** supplies revolution information of the vehicle to the TOE.
- **Status Input 1 and 2** are for the determination of the level for the external contacts.
- **Warning Output** is for sharing any warning with the external equipments.
- **Custom Out** is a serial output line for communicating with the external equipments.
- **Ignition Input** is for the detection of vehicle ignition status.
- **Power Supply Input** provides the voltage for the operation of the TOE.
- **Power Supplies** generate various level of internal voltages for the correct operation of the TOE.
- **Card Reader 1 (Driver)** is the first connection port for the tachograph cards.
- **Card Reader 2 (Co-Driver)** is the second connection port for the tachograph cards.
- **Printer** is the interface to print reports.
- **Data Download & Calibration** is the interface for calibration and data downloading.
- **Display** is a built in visual output indicator for the user interaction.
- **Keypad** is the input interface for the user interaction.
- **Buzzer** is the sound source to warn user about the situational changes and the events.
- **Enclosure** provides casing to the TOE.

2.5 Documentation

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

Document Name	*Version*	*Release Date*
ASELSAN Digital Tachograph Vehicle Unit Security Target	1.6	08.08.2016
STC-8250 A Digital Tachograph Operation Manual	0.4	08.08.2016
STC-8250 A Digital Tachograph Preparation Manual	0.4	08.08.2016

2.6 IT Product Testing

The evaluator has performed an analysis of the coverage and depth of the tests performed during the independent testing plan. The main goal of this analysis is demonstrate that, at least, all the SFR enforcing and supporting TSFIs, subsystems and modules have been tested in the independent testing plan.

To perform this analysis the evaluator has taken into account the information provided in the security target, functional specification and the design documentation.

Evaluator has performed 72 functional tests. Evaluator has performed a sample of tests using the developer testing efforts. Later, the evaluator has planned independent tests and performed the tests.

Evaluator has performed 22 penetration tests. TOE is tested against:

- Tampering,
- Bypass,
- Overrun,
- Protocol attacks.

2.7 Evaluated Configuration

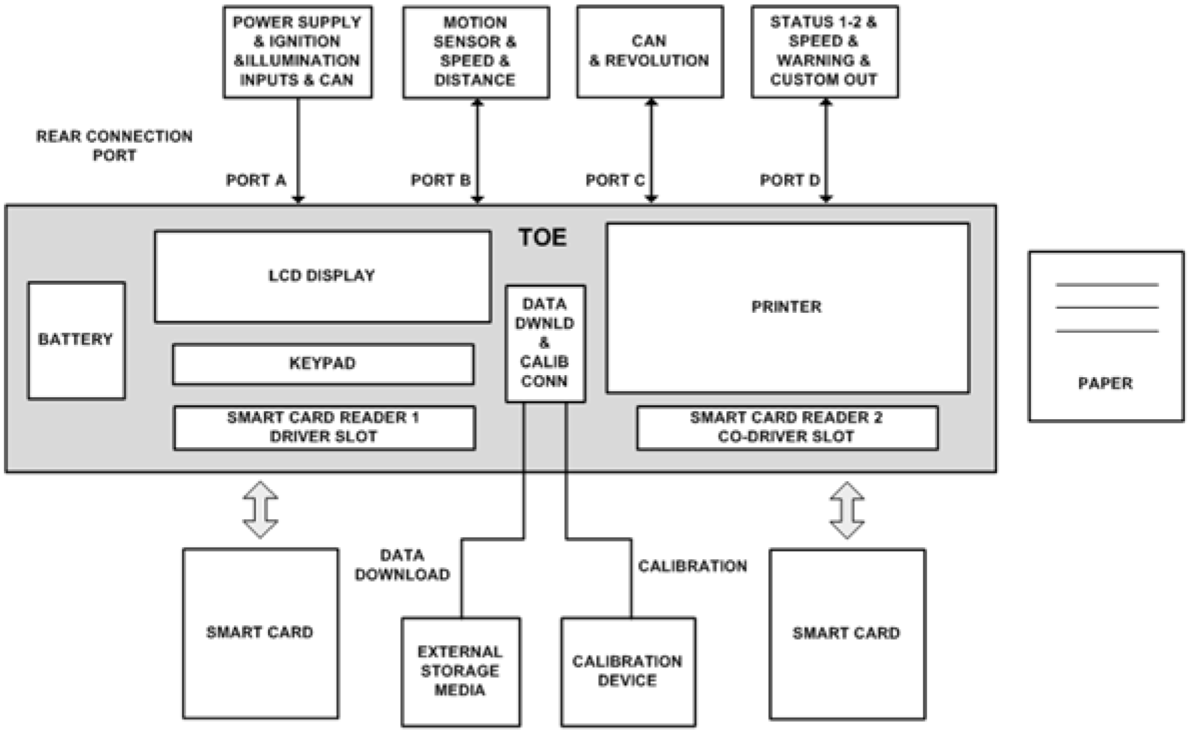

Figure 3 : TOE Operational Environment

The following TOE versions have been used:

- SW Version 0.7.9
- HW Version 1.0.0

2.8 Results of the Evaluation

The verdict for the CC Part 3 assurance components (according to EAL4+ (ATE_DPT.2, AVA_VAN.5) and the security target evaluation) is summarized in the following table:

Assurance Class	Component ID	Component Title	Verdict
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
Guidance documents	AGD_OPE.1	Operational user guidance	PASS
	AGD_PRE.1	Preparative procedures	PASS
Life-cycle 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_TAT.1	Well-defined development tools	PASS
	ALC_LCD.1	Life Cycle Definition	PASS
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	Security requirements	PASS
	ASE_SPD.1	Security problem definition	PASS
	ASE_TSS.1	TOE summary specification	PASS
Tests	ATE_COV.2	Analysis of coverage	PASS
	ATE_DPT.2	Testing: security enforcing modules	PASS
	ATE_FUN.1	Functional testing	PASS
	ATE_IND.2	Independent testing - sample	PASS
Vulnerability assessment	AVA_VAN.5	Advanced methodical 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 “ASELSAN DIGITAL TACHOGRAPH VEHICLE UNIT v1.0.0” 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 DIGITAL TACHOGRAPH VEHICLE UNIT v1.0.0 Security Target
Version: 1.6
Date of Document: 08.08.2016

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

4.1 Acronyms

AETR	Accord Europeen sur les Transports
CA	Certification Authority
CAN	Controller Area Network
CBC	Cipher Block Chaining (an operation mode of a block cipher; here of TDES)
CC	Common Criteria
DES	Data Encryption Standard (see FIPS PUB 46-3)
EAL	Evaluation Assurance Level (a pre-defined package in CC)
ECB	Electronic Code Book (an operation mode of a block cipher; here of TDES)
EQTj.C	Equipment Certificate
EQTj.PK	Equipment Public Key
EQTj.SK	Equipment Private Key
ERCA	European Root Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
K_{ID}	Identification key, manages the pairing between a motion sensor and the vehicle unit
K_{m}	Master key, manages the pairing between a motion sensor and the vehicle unit
K_{mVU}	Part of the Master key stored in the VU, manages the pairing between a motion sensor and the vehicle unit
K_{mWC}	Part of the Master key stored in the workshop card, manages the pairing between a motion sensor and the vehicle unit
K_{P}	Pairing key, manages the pairing between a motion sensor and the vehicle unit
K_{SM}	Session key between motion sensor and vehicle unit
K_{ST}	Session key between tachograph cards and vehicle unit
MD	Management Device
MS	Motion Sensor
MSA	Member State Authority
MSCA	Member State Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
MSi.C	Member State Certificate
OSP	Organizational Security Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
REQxxx	A requirement from [6], whereby ‘xxx’ represents the requirement number.
SAR	Security Assurance Requirements
SFR	Security Functional Requirement
ST	Security Target
TC	Tachograph Card
TDES	Triple-DES (see FIPS PUB 46-3)
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policies
VU	Vehicle Unit

4.2 Glossary

Activity data: Activity data include user activities data, events and faults data and control activity data.
Activity data are part of User Data.

Application note: Optional informative part of the PP containing sensible supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.

Approved Workshops: Fitters and workshops installing, calibrating and (optionally) repairing VU and being under such agreement with a VU manufacturer, so that the assumption A.Approved_Workshops is fulfilled.

Authenticity: Ability to confirm that an entity itself and the data elements stored in were issued by the entity issuer.

Certificate chain: Hierarchical sequence of Equipment Certificate (lowest level), Member State Certificate and European Public Key (highest level), where the certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.

Certification authority: A natural or legal person who certifies the assignment of public keys (for example PK.EQT) to serial number of equipment and to this end holds the licence.

Digital Signature: A digital signature is a seal affixed to digital data which is generated by the private signature key of an entity (a private signature key) and establishes the owner of the signature key (the entity) and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority.

Digital Tachograph: Recording equipment including a vehicle unit and a motion sensor connected to it.

Digital Tachograph System: Equipment, people or organisations, involved in any way with the recording equipment and tachograph cards.

Equipment Level: At the equipment level, one single key pair (EQTj.SK and EQTj.PK) is generated and inserted in each equipment (vehicle unit or tachograph card). Equipment public keys are certified by a Member State Certification Authority (EQTj.C). This key pair is used for (i) authentication between vehicle units and tachograph cards, (ii) enciphering services: transport of session keys between vehicle units and tachograph cards, and (iii) digital signature of data downloaded from vehicle units or tachograph cards to external media.
The final master key K_m and the identification key K_{ID} are used for authentication between the vehicle unit and the motion sensor as well as for an encrypted transfer of the motion sensor individual pairing key K_P from the motion sensor to the vehicle unit. The master key K_m, the pairing key K_P and the identification key K_{ID} are used merely during the pairing of a motion sensor with a vehicle unit (see ISO 16844-3 [9] for further details). K_m and K_{ID} are permanently stored neither in the motion sensor nor in the vehicle unit; K_P is permanently stored in the motion sensor and temporarily – in the vehicle unit.

ERCA policy: The ERCA policy is not a part of the Commission Regulation 1360/2002 and represents an important additional contribution. It was approved by the European Authority on 9 July 2004. The ERCA policy is available from the web site http://dtc.jrc.ec.europa.eu.
Confidentiality, integrity and authenticity of the entities to be transferred between the different levels of the hierarchy within the tachograph system are subject to the ERCA and MSA policies.

European Authority: An organisation being responsible for the European Root Certification Authority policy. It is represented by
European Commission
Directorate General for Mobility and Transport
B – 1049 Brussels.
The entire Digital Tachograph System is operated in the frame and on the base of the Digital Tachograph System European Root Policy (Administrative Agreement TREN-E1-08-M-ST-SI2.503224) defining the general conditions for the PKI concerned and contains accordingly more detailed information.

European Root Certification Authority (ERCA): An organisation being responsible for implementation of the ERCA policy and for the provision of key certification services to the Member States. It is represented by
Digital Tachograph Root Certification Authority
- Joint Research Centre,
Institute for the Protection and Security of the Citizen,
Digital Citizen Security Unit,
Ispra Establishment (TP.360)
Via E. Fermi, 1
I-21020 Ispra (VA)

At the European level, ERCA generates a single European key pair (EUR.SK and EUR.PK). It uses the European private key to certify the Member States` public keys and keeps the records of all certified keys. A change of the European (root) key pair is currently not intended.

ERCA also generates two symmetric partial master keys for the motion sensor: Km_{wc} and Km_{vu}. The first partial key Km_{wc} is intended to be stored in each workshop tachograph card; the second partial key Km_{vu} is inserted into each vehicle unit. The final master key K_m results from XOR (exclusive OR) operation between Km_{wc} and Km_{vu}.

Identification data: Identification data include VU identification data.
Identification data are part of User data.

Manufacturer: The generic term for a VU Manufacturer producing and completing the VU to the TOE. The Manufacturer is the default user of the TOE during the manufacturing life phase. The manufacturer of the VU within this Security Target is ASELSAN and unless it is explicitly stated the term manufacturer means “ASELSAN”.

Member State Authority (MSA): Each Member State of the European Union establishes its own national Member State Authority (MSA) usually represented by a state authority, e.g. Ministry of Transport. The national MSA runs some services, among others the Member State Certification Authority (MSCA).

The MSA has to define an appropriate Member State Policy (MSA policy) being compliant with the ERCA policy.

MSA (MSA component personalisation service) is responsible for issuing of equipment keys, wherever these keys are generated: by equipment manufacturers, equipment personalisers or MSA itself.

MSA is also responsible for inserting data containing Km_{wc}, Km_{vu}, motion sensor identification (N_S) and authentication data (K_P) encrypted with K_{ID} and K_m, resp., into respective equipment (workshop card, vehicle unit and motion sensor).

Confidentiality, integrity and authenticity of the entities to be transferred between the different levels of the hierarchy within the tachograph system are subject to the ERCA and MSA policies.

Turkey implements the Digital Tachograph System as a non-EU AETR Contracting Party according to Digital Tachograph System Turkish Authority Policy (TR-A Policy) approved by ERCA. TR-A Policy is available from the web site http://staum.tobb.org.tr. AETR is European Agreement Concerning the Work of Crews of Vehicles Engaged in International Road Transport concluded at Geneva on 1 July 1970. The term Member State is used to refer to non-EU AETR Contracting Party along this document while the MSA policy refers to the TR-A Policy.

Member State Certification Authority (MSCA): At the Member State level, each MSCA generates a Member State key pair (MSi.SK and MSi.PK). Member States' public keys are certified by the ERCA (MSi.C).

MSCAs use their Member State private key to certify public keys to be inserted in equipment (vehicle unit or tachograph card) and keep the records of all certified public keys with the identification of the equipment concerned. MSCA is allowed to change its Member State key pair.

MSCA also calculates an additional identification key K_{id} as XOR of the master key K_m with a constant control vector CV.

MSCA is responsible for managing Km_{wc}, Km_{vu}, encrypting motion sensor identification (N_S) and authentication data (K_P) with K_{ID} and K_m, respectively, and distributing them to the respective MSA component personalisation services.

Motion data: The data exchanged with the VU, representative of speed and distance travelled.

Motion Sensor: Part of the recording equipment, providing a signal representative of vehicle speed and/or distance travelled.
A MS possesses valid credentials for its authentication and their validity is verifiable.
Valid credentials are MS serial number encrypted with the identification key (Enc(K_{ID}|N_S)) together with pairing key encrypted with the master key (Enc(K_M|K_P)).

Personal Identification Number (PIN): A short secret password being only known to the approved workshops.

Personalisation: The process by which the equipment-individual data (like identification data and authentication key pairs for VU and TC or serial numbers and pairing keys for MS) are stored in and unambiguously, inseparably associated with the related equipment.

Reference data: Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.

Secure messaging in combined mode: Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4.

Security data: The specific data needed to support security enforcing functions (e.g. cryptographic keys).
Security data are part of sensitive data.

Sensitive data: Data stored by the recording equipment and by the tachograph cards that need to be protected for integrity, unauthorised modification and confidentiality (where applicable for security data).
Sensitive data includes security data and user data.

Tachograph cards: Smart cards intended for use with the recording equipment. Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage. A tachograph card may be of the following types:
driver card,
control card,
workshop card,
company card.
A tachograph card possesses valid credentials for its authentication and their validity is verifiable.
Valid credentials are a certified key pair for authentication being verifiable up to EUR.PK.

TSF data: Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]).

Unknown equipment: A technical device not possessing valid credentials for its authentication or validity of its credentials is not verifiable.
Valid credentials can be either a certified key pair for authentication of a device or MS serial number encrypted with the identification key (Enc(K_{ID}|N_S)) together with pairing key encrypted with the master key (Enc(K_M|K_P)).

Unknown User: Not authenticated user.

Update issuer: An organisation issuing the completed update data of the tachograph application.

User: Users are to be understood as legal human user of the TOE. The legal users of the VU comprise drivers, controllers, workshops and companies. User authentication is performed by possession of a valid tachograph card.
There can also be Unknown User of the TOE and malicious user of the TOE – an attacker.
User identity is kept by the VU in form of a concatenation of User group and User ID, cf. [7], UIA_208 representing security attributes of the role 'User'.

User Data: Any data, other than security data and authentication data, recorded or stored by the VU, required by Chapter III.12 of the Commission Regulation [6]. User data are part of sensitive data.

User data include identification data and activity data.
CC give the following generic definitions for user data:
Data created by and for the user that does NOT affect the operation of the TSF (CC part 1 [1]. Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [1]).

Vehicle Unit: The recording equipment excluding the motion sensor and the cables connecting the motion sensor. The vehicle unit may either be a single unit or be several units distributed in the vehicle, as long as it complies with the security requirements of this regulation.

Verification Data: Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

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 v3.0 of ASELSAN Digital Tachograph Unit v1.0.0, Rel. Date: 11.08.2016.

[5] ASELSAN Digital Tachograph Unit v1.0.0 Security Target v1.6 [ST], Rel. Date: 08.08.2016.

[6] Annex I B of Commission Regulation (EC) No. 1360/2002 'Requirements for construction, testing, installation and inspection', adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport Official Journal of the European Communities L 77/71-86, 13.03.2004 amended by,

- Council Regulation (EC) No 1791/2006 of 20 November 2006.
- Commission Regulation (EC) No 68/2009 of 23 January 2009.
- Commission Regulation (EU) No 1266/2009 of 16 December 2009.

[7] Appendix 10 of Annex I B of Commission Regulation (EEC) No. 1360/2002 – Generic Security Targets.

[8] Appendix 11 of Annex I B of Commission Regulation (EEC) No. 1360/2002 – Common Security Mechanisms.

[9] ISO 16844-3:2004, First Edition, 2004-11-01 with Technical Corrigendum 1:2006, 2006-03-01, Road Vehicles – Tachograph Systems – Part 3: Motion Sensor Interface.