

HBT-CC-8255-DT-01

Rev 0.13

May 2021

Aselsan STC-8255 v1.0
Digital Tachograph
Vehicle Unit

Security Target Lite
(DTVU-ST-Lite)

ASELSAN A.Ş.

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

Contents

1. OVERVIEW	5
1.1 Abstract	5
1.2 Document Organization	6
1.3 Document Formatting Conventions.....	6
1.4 List Acronyms and Glossary of Terms	7
1.4.1 Acronyms	7
1.4.2 Glossary of terms.....	8
2 ST INTRODUCTION	13
2.1 ST Reference and TOE Reference	13
2.2 TOE Overview	14
2.2.1 TOE Definition and Operational Usage.....	14
2.2.2 TOE Major Security Features for Operational Use	14
2.2.3 TOE Type	15
2.2.4 Non-TOE hardware/software/firmware	17
2.3 TOE Description	18
2.3.1 Physical Scope.....	18
2.3.2 Logical Scope	22
3 CONFORMANCE CLAIMS.....	24
3.1 CC Conformance Claim	24
3.2 PP and Package Claim.....	24
3.2.1 Protection Profile (PP) Claim	24
3.2.2 Package Claim	24
3.3 Conformance Rationale.....	24
4 SECURITY PROBLEM DEFINITION	25
4.1 Assets	25
4.1.1 Primary Assets.....	25
4.1.2 Secondary Assets	26
4.2 Subjects and External Entities	27
4.3 Subjects, objects, and access rights	29
4.3.1 Subjects.....	29
4.3.2 Objects.....	29
4.3.3 Access Rights	30
4.4 Threats.....	34
4.5 Organizational Security Policies	35
4.5.1 OSPs related to the TOE.....	35
4.5.2 OSPs related to the TOE and its operational environment	36
4.5.3 OSPs related to the TOE's operational environment	36
4.6 Assumptions	37
5 SECURITY OBJECTIVES	38
5.1 Security Objectives for the TOE	38
5.2 Security Objectives for the Operational Environment.....	38
5.2.1 Design environment (cf. the life cycle diagram in above).....	39
5.2.2 Manufacturing environment	39
5.2.3 Workshops environment.....	40
5.2.4 End-user environment.....	40
5.3 Security Objective Rationale	40
5.3.1 Rationale for Threats	45
5.3.2 Rationale for Organizational Security Policies	47
6 EXTENDED COMPONENTS DEFINITION	49
7 SECURITY REQUIREMENTS.....	50
7.1 Security Functional Requirements	50

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

7.1.1	Overview	51
7.1.2	Class FAU Security Audit	56
7.1.3	Class FCO Communication	58
7.1.4	Class FCS Cryptographic Support	58
7.1.5	Class FDP User Data Protection	63
7.1.6	Class FIA Identification and Authentication	79
7.1.7	Class FPR Privacy	83
7.1.8	Class FPT Protection of the TSF	83
7.1.9	Class FRU Resource Utilisation	86
7.1.10	Class FMT Security Management	86
7.2	Security Assurance Requirements	89
7.3	Security Requirements Rationale	90
7.3.1	Security Functional Requirements Rationale	90
7.3.2	Rationale for SFR's Dependencies	101
7.3.3	Security Assurance Requirements Rationale	101
8	TOE SUMMARY SPECIFICATIONS	103
9	BIBLIOGRAPHY	112
10	ANNEX-A: COVERAGE OF THE REQUIREMENTS OF APPENDIX 10.....	113

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

List of Figures

Figure 1: Block Diagram of the TOE	14
Figure 2: TOE Life Cycle.....	16
Figure 3: TOE Operational Environment	17
Figure 4: Aselsan Digital Tachograph Vehicle Unit	19

List of Tables

Table 1: Logical scope	22
Table 2: Primary assets.....	25
Table 3: Secondary assets.....	26
Table 4: Subjects and external entities	27
Table 5: Access rights	30
Table 6: Security objective rationale.....	42
Table 7: Security functional groups vs. SFRs.	51
Table 8: Security assurance requirements	89
Table 9: Coverage of security objectives for the TOE by SFR	90
Table 10: Suitability of the SFRs	93
Table 11: SAR Dependencies.....	102
Table 12: TOE Summary	103
Table 13: Requirement coverage.....	113

1. Overview

1.1 Abstract

This document provides the basis for an evaluation of a specific target of evaluation (TOE), Aselsan Digital Tachograph Vehicle Unit (STC-8255 v1.0). This security target (ST) defines a set of assumptions about the operational environment, a list of threats that the product intends to counter, a set of security objective, a set of security requirements and the IT security functions provided by the TOE, which meet the security objectives.

1.2 Document Organization

Section 1	Overview	General document formatting conventions, glossary of terms, tables
Section 2	ST Introduction	Includes an overview and description of the TOE, the hardware and software that make up the TOE, as well as the physical and logical boundaries of the TOE
Section 3	Conformance Claims	Lists evaluation conformance to Common Criteria versions and applicable Protection Profile and Package.
Section 4	Security Problem Definition	Specifies the assets, threats, assumptions and organizational security policies that effect the TOE.
Section 5	Security Objectives	Defines the security objectives for the TOE and operational environment and rationale illustrating that the security objectives mitigate the threats.
Section 6	Extended Components Definition	Details any extended components used in this evaluation.
Section 7	Security Requirements	Describes the functional and assurance requirements for this TOE
Section 8	TOE Summary Specification	Identifies the IT security functions provided by the TOE and how the assurance requirements are satisfied.

1.3 Document Formatting Conventions


In this Security Target some notations and conventions, which are taken from the Common Criteria v3.1R5 have been used in order to guide the reader. The conventions used for the specification of the functional requirements under the Section 5 are defined in the Section 7.

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

1.4 List Acronyms and Glossary of Terms

1.4.1 Acronyms

AETR	Accord Européen sur les Transports Routiers
CA	Certification Authority
CAN	Controller Area Network
CBC	Cipher Block Chaining
CC	Common Criteria
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ECB	Electronic Code Book
EQTj.C	Equipment Certificate
EQTj.PK	Equipment Public Key
EQTj.SK	Equipment Private Key
ERCA	European Root Certification Authority
GST	Generic Security Target
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
MSi.C	Member State Certificate
OSP	Organizational Security Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
REQ_{xxx}	A requirement from [6]
SAR	Security Assurance Requirements
SFR	Security Functional Requirement
ST	Security Target
TC	Tachograph Card
TDES	Triple-DES
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policies
VU	Vehicle Unit
RSA	Rivest Shamir-Adleman

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

1.4.2 Glossary of terms

The following terminology is used in this Security Target (ST).

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 license.
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 organizations, 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.

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

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 [12] 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.

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

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://dte.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 organization 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 organization 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
European Commission - 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: $K_{m_{wc}}$ and $K_{m_{vu}}$. The first partial key $K_{m_{wc}}$ is intended to be stored in each

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

workshop tachograph card; the second partial key $K_{m_{vu}}$ is inserted into each vehicle unit. The final master key K_m results from XOR (exclusive OR) operation between $K_{m_{wc}}$ and $K_{m_{vu}}$.

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:

Each Member State of the European Union establishes its own national

Authority (MSA):

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 personalization 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 $K_{m_{wc}}$, $K_{m_{vu}}$, motion sensor identification (Ns) 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 $K_{m_{wc}}$, $K_{m_{vu}}$, encrypting motion sensor identification (Ns) and authentication data (K_P) with K_{ID} and K_m , respectively,

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

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 ($\text{Enc}(K_{ID}|N_S)$) together with pairing key encrypted with the master key ($\text{Enc}(K_M|K_P)$).

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.

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

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 organization 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. [9], 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 [2]).
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.

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

2 ST Introduction

This document contains a description of the TOE (ASELSAN STC-8255 v1.0), the threats; it must be able to counteract and the security objectives; it must achieve. It specifies the security requirements. It states the claimed minimum resistance against attacks of security functional requirements and the required level of assurance for the development and the evaluation.

For clarity of reading, duplication sometimes arises between Annex 1B [6] main body requirements and security target requirements. In case of ambiguity between a security target requirement and the Annex 1B [6] main body requirement referred by this security target requirement, the Annex 1B main body requirement shall prevail.

Annex 1B [6] main body requirements not referred by this security target are not the subject of security certification.

The VU general characteristics, functions and mode of operations are described in Chapter II of Annex 1B [6]. The VU functional requirements are specified in Chapter III of Annex 1B [6].

2.1 ST Reference and TOE Reference

ST Title:	Aselsan STC-8255 v1.0 Digital Tachograph Vehicle Unit Security Target Lite
ST Version:	v0.13
ST Release Date:	18.05.2021
ST TOE Developer:	Aselsan Inc.
TOE Identification:	ASELSAN STC-8255 v1.0
TOE Version:	v1.0
TOE Software Version:	v1.0
CC Identification:	Common Criteria for Information Technology Security Evaluations, Version 3.1R5
Keywords:	Digital Tachograph, Vehicle Unit, Transport Vehicle, Security Target

TOE Variants: Final TOE product variants will have 5820-8255-1xxxxy, type Aselsan stock numbers. Remaining digits ‘xxx’ (starting from 111 to 999) and ‘y’ (starting from A to Z) are used for the TOE’s variants with different options. The letter ‘xxx’ defines the hardware options which are LCD backlight color, CAN-Bus termination resistance options, GNSS and I/O options. On the other hand, the letter ‘y’ defines the OEM configuration options (such as OEM logo on front panel and labelling differences). One major variant (5820-8255-1417A) which includes all the options and covering the remaining variants in terms of hardware and software configuration items is used as a reference TOE in the scope of CC security evaluation. In terms of tachograph security functions, all variants are identical to reference TOE.

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

2.2 TOE Overview

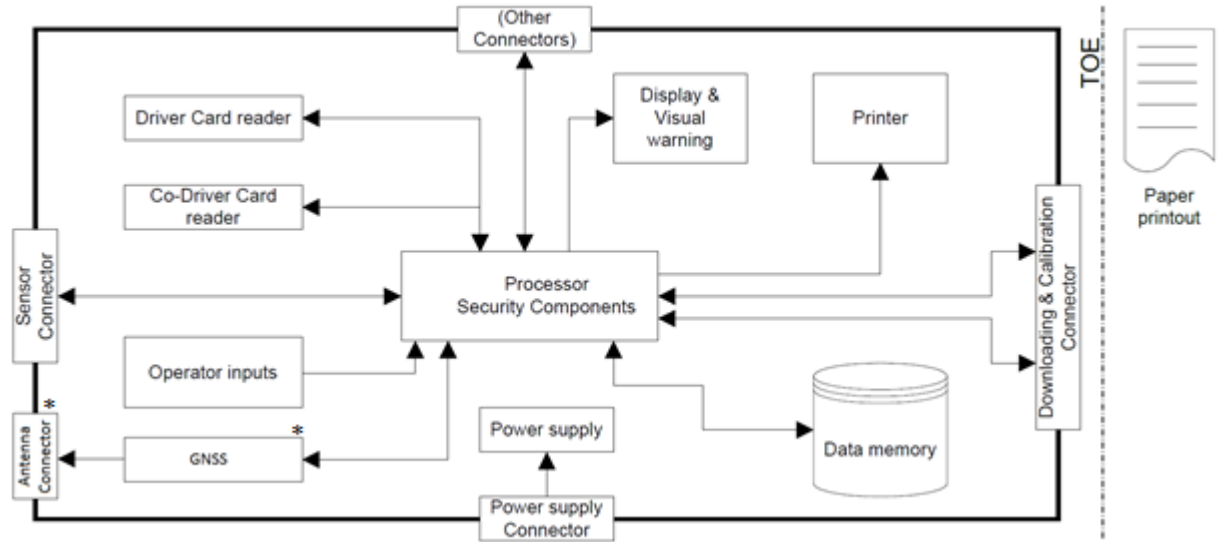
2.2.1 TOE Definition and Operational Usage

The Target of Evaluation (TOE) addressed by the current Security Target is a vehicle unit (VU) in the sense of Annex 1B [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. 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.

The block diagram of the TOE is depicted in *: optional

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



*: optional

Figure 1: Block Diagram of the TOE

2.2.2 TOE Major Security Features for Operational Use

The main security feature of the TOE is as specified in [7]¹: The data to be measured² 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.

¹ O.VU_Main

² in the sense 'collected'; the physical data measurement is performed by the motion sensor and the motion sensor is not part of the current TOE.

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

- 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 (Refer to [9], chap.4)

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

Application Note 1: At least two services listed above – “Identification and authentication” as well as “data exchange” require cryptographic support according to [10], section 4.9.

2.2.3 TOE Type

The TOE type “ASELSAN STC-8255 v1.0” is a Vehicle Unit (VU) in the sense of Annex 1B [6].

The life cycle of the TOE is described in the following figure:

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

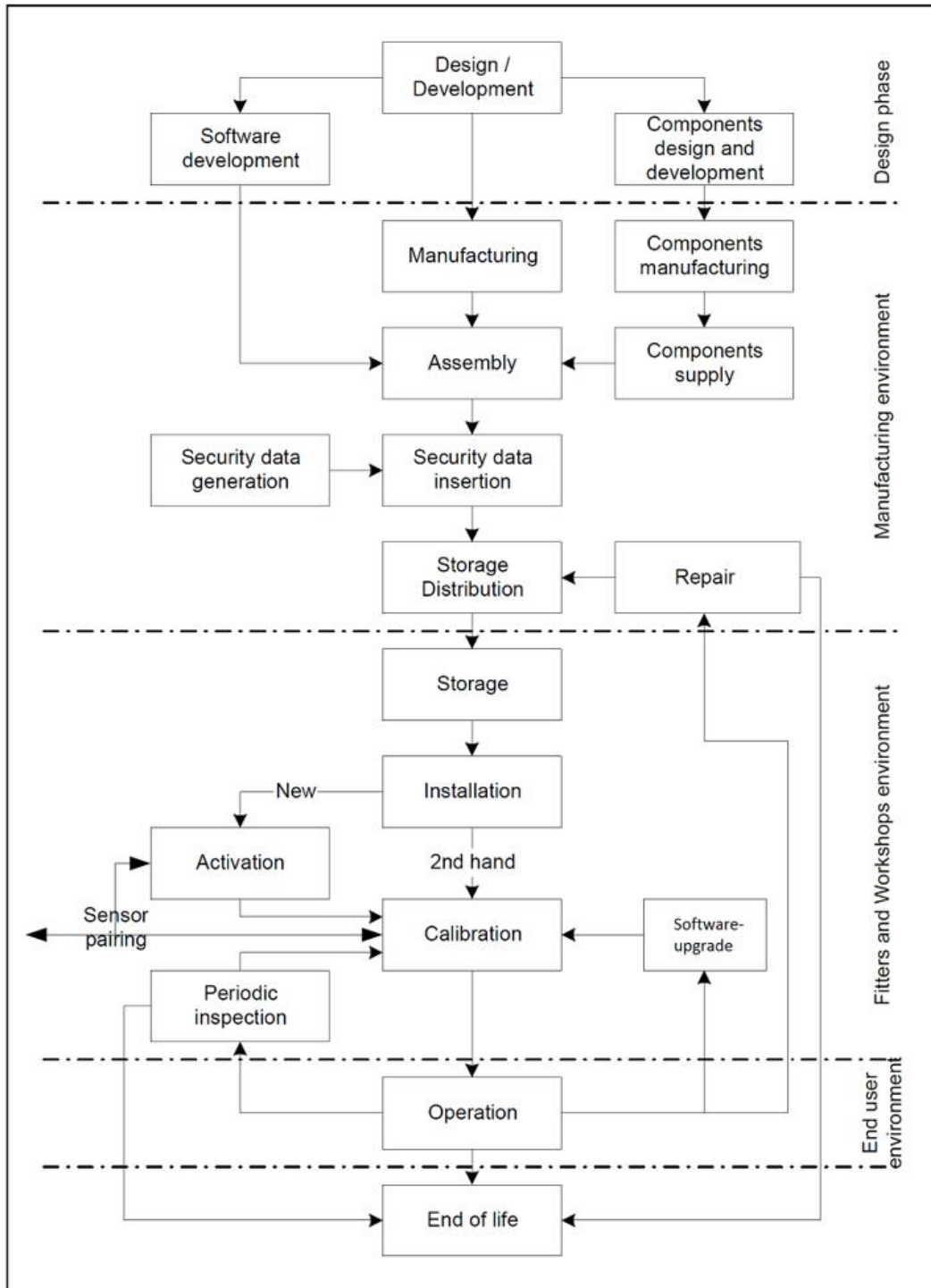


Figure 2: TOE Life Cycle

Application Note 2: The security requirements in sec. 4 of [7] limit the scope of the security examination of the TOE to the *operational phase* in the end user environment. Therefore, the security policy defined by the current ST also focuses on the operational phase of the VU in the

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

end user environment. Some single properties of the *calibration phase*³ being significant for the security of the TOE in its *operational phase* are also considered by the current ST as required by [7]. The TOE distinguishes between its calibration and operational phases by modes of operation as defined in [5], REQ007 and REQ010: operational, control and company modes presume the operational phase, whereby the calibration mode presumes the calibration phase of the VU.

A security evaluation/certification involves all life phases into consideration to the extent as required by the assurance package chosen here for the TOE (see chap. 3.2.2 ‘Package Claim’ below). The TOE delivery from its manufacturer to the first customer (approved workshops) exactly happens at the transition from the manufacturing to the calibration phase.

There is no plan for repairing or changing components of the TOE in the fitters or the workshops. The only exceptions that can be executed in the workshops are;

- printer drawer replacement,
- approved software upgrade

for the TOE.

2.2.4 Non-TOE hardware/software/firmware

The vehicle unit’s operational environment while installed in a vehicle is shown in the following figure:

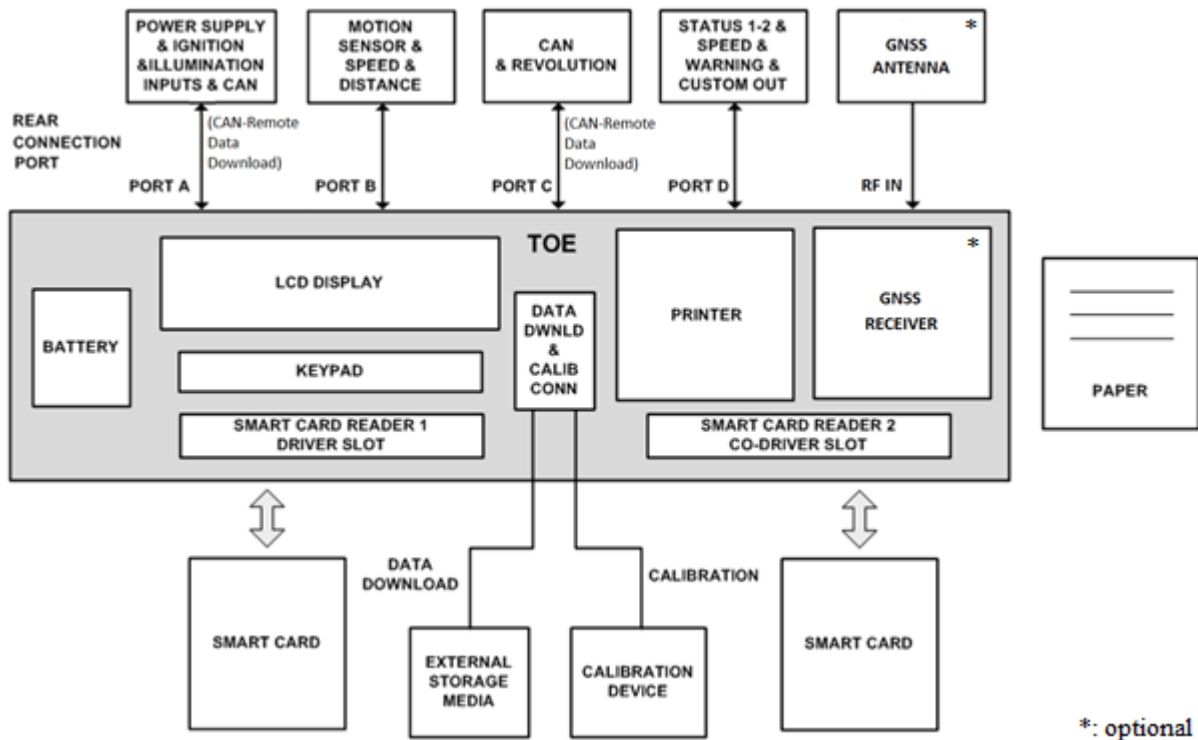


Figure 3: TOE Operational Environment

The following TOE-external components are

³ *calibration phase* comprises all operations within the fitters and workshops environment

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

- a) mandatory for a proper TOE operation:
- power supply e.g. from the vehicle, where the TOE is installed,
 - motion sensor.
- b) functionally necessary for an Annex 1B [6] compliant operation:
- calibration device (fitters and workshops environment only),
 - tachograph cards (four different types of them; driver card, workshop card, company card, control card),
 - printer paper,
 - external storage media for data download.
- c) helpful for a convenient TOE operation:
- connection to the vehicle network e.g. CAN-connection,
 - access to GNSS signals (optional),
 - revolution input,
 - status 1-2 inputs.

Application Note 3: While operating, the TOE will verify, whether the motion sensor and tachograph cards, which are connected, possess appropriate credentials showing their belongings to the digital tachograph system. A security certification according to [9] is a prerequisite for the type approval of a motion sensor and tachograph cards.

2.3 TOE Description

2.3.1 Physical Scope

The physical scope of the TOE is Aselsan Digital Tachograph Vehicle Unit (Aselsan STC-8255 v1.0) which is a device to be installed in a vehicle. The TOE consists of a hardware box, which includes processing units, a program memory, a data memory, a real time clock, two smart card interface devices (driver and co-driver), a printer, a display, a calibration/downloading connector, facilities for entry of user's inputs, an optional GNSS module, embedded software and of related manuals.

The TOE must be connected to a motion sensor (MS) and to a power supply unit; it can temporarily be connected with other devices used for calibration, data export, software upgrade and diagnostics.

The TOE is delivered to authorized Digital Tachograph workshops and Vehicle Manufacturers together with related manuals according to delivery procedures described in Delivery Procedures Document of the TOE. The manuals include a Quick User Guide, a Preparation Manual and an Operation Manual for users, workshops and vehicle manufacturers.

TOE Software

STC-8255 software v1.0 is to be embedded into the delivered TOE.

Quick User Guide

Aselsan STC-8255 v1.0 Quick User Guide v0.1 is the printed (hardcopy) document describing summary usage information for all users of the TOE. It is included in the delivery package of the TOE.

Preparation Manual

Aselsan STC-8255 v1.0 Preparation Manual v0.7 is the electronic document (pdf format) describing the TOE installation details for workshops.

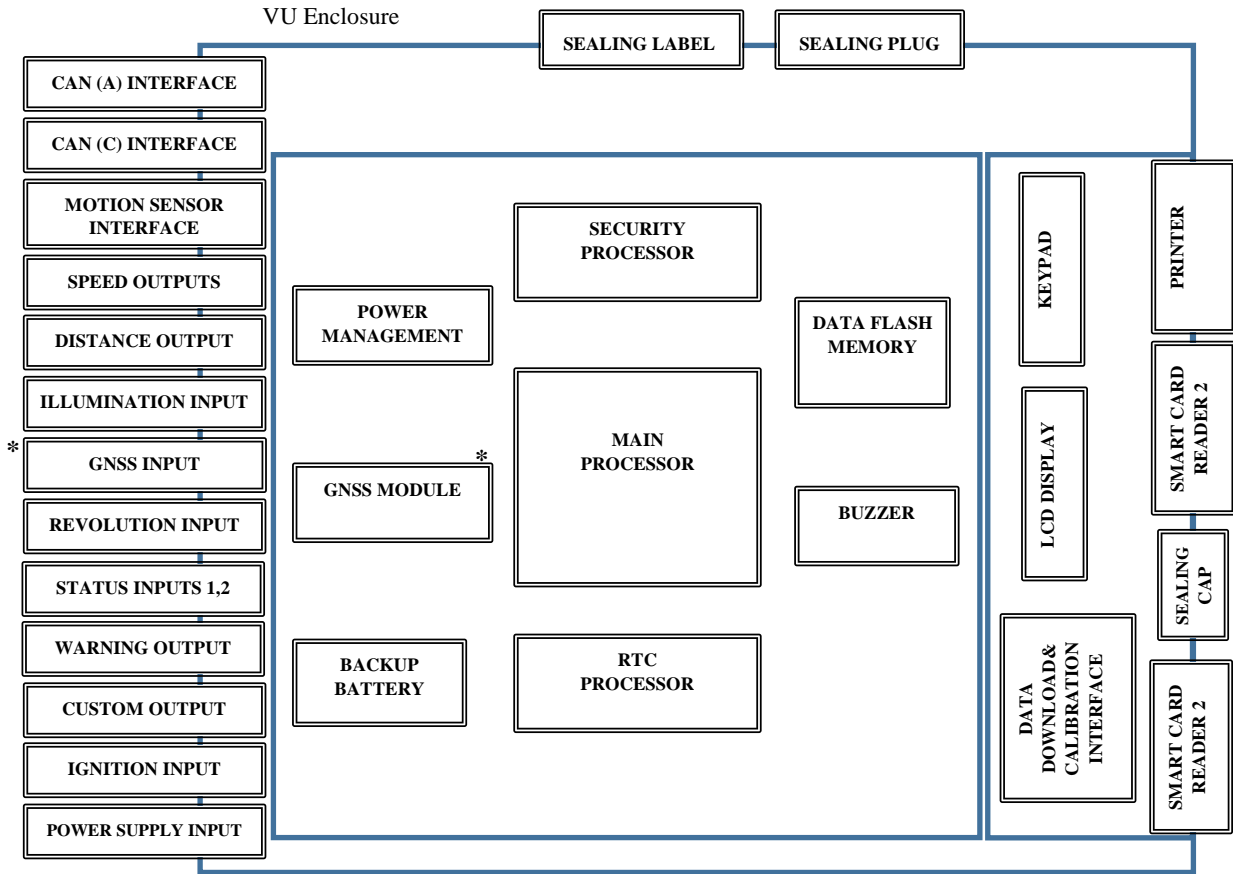
Aselsan STC-8255 v1.0 Digital Tachograph Vehicle Unit Security Target Lite

Operation Manual

Aselsan STC-8255 v1.0 Operation Manual v0.7 is the electronic document (pdf format) describing the TOE operation for users, workshops and vehicle manufacturers.

Preparation and Operation Manuals can be downloaded on <https://www.aselsan.com.tr/en/capabilities/public-safety-communication-systems/digital-tachograph-systems>.

A block diagram which consists of the main components and the interfaces of the TOE is given in Figure 4.



*: optional

Figure 4: 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.

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

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.

	<i>Communication and Information Technologies Sector Common Criteria Document</i>	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

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.

2.3.2 Logical Scope

Table 1: Logical scope

TOE Security Function	Description
Security Audit	The TOE records security breach attempts (motion sensor authentication failure, tachograph card authentication failure, unauthorized 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, calibration and time adjustment functions may 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, Tachograph Cards and Management Device	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 or 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. Not all inputs from external sources are accepted as executable code. Only a valid software, which possesses appropriate credentials, is accepted as an executable code.
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 and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

TOE Security Function	Description
Communication	For data downloaded to external media, an evidence of origin is generated. 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.
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.

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

3 Conformance Claims

3.1 CC Conformance Claim

This Security Target and TOE claim conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017 [3]

as follows;

- Part 2 conformant,
- Part 3 conformant,
- The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017 [4] has to be taken into account.

3.2 PP and Package Claim

3.2.1 Protection Profile (PP) Claim

This Security Target claims strictly conformance to ‘Protection Profile Digital Tachograph-Vehicle Unit (VU-PP), BSI-CC-PP-0057, Version 1.0, 13th July 2010, Bundesamt für Sicherheit in der Informationstechnik [11].

Application Note 4: This vehicle unit ST covers all requirements of the vehicle unit generic ITSEC ST as contained in [7]. The coverage of the requirements of [7] by the security functional requirements of the current ST is stated in Annex A, chapter 11 of this security target.

3.2.2 Package Claim

This Security Target is conformant to the following security requirements package:

- Assurance package E3hCC31_AP as defined in section 7.3.3.

This assurance package is commensurate with JIL [9] defining an assurance package called E3hAP. This assurance package declares assurance equivalence between the assurance level E3 of an ITSEC certification and the assurance level of the package E3hAP within a Common Criteria (ver. 2.1) certification (in conjunction with the Digital Tachograph System).

The assurance package E3hCC31_AP represents the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5 (see sec. 7.3.3).

3.3 Conformance Rationale

The type of TOE defined in this ST is a Vehicle Unit in the sense of Annex 1B [5] and strictly compliant with the TOE type defined in the PP [11] which is claimed in the section 3.2.1.

4 Security Problem Definition

4.1 Assets

4.1.1 Primary Assets

Table 2: Primary assets

Object No	Asset	Definition	Generic Security Property to be Maintained by the Current Security Policy
1	User Data (recorded or stored in the TOE)	Any data, other than security data (sec. III.12.2 of [5]) and authentication data, recorded or stored by the TOE, required by Chapter III.12 of the Commission Regulation [5]).	Integrity Authenticity
2	User Data transferred between the TOE and an external device connected	All user data being transferred from or to the TOE. A TOE communication partner can be: - a motion sensor, - a tachograph card, or - an external medium for data download. Motion data are part of this asset. User data can be received and sent (exchange ↔ {receive, send}).	Confidentiality ⁴ Integrity Authenticity ⁵

All these primary assets represent User Data in the sense of the CC.

⁴ Not each data element being transferred represents a secret. Whose data confidentiality shall be protected while transferring them (i) between the TOE and a MS, is specified in [10], sec. 7.6 (instruction #11); (ii) between the TOE and a tachograph card – in [6], chap. 4 (access condition = PRO SM). Confidentiality of data to be downloaded to an external medium is not required to be protected.

⁵ Not each data element being transferred shall be protected for its integrity and authenticity. Whose data integrity and authenticity shall be protected while transferring them (i) between the TOE and a MS, is specified in [10], sec. 7.5 (instruction #80); (ii) between the TOE and a tachograph card – in [6], chap. 4 (access condition = AUT). Integrity and authenticity of data to be downloaded to an external medium shall always be protected.

4.1.2 Secondary Assets

Table 3: Secondary assets

Object No	Secondary Asset	Definition	Generic Security Property to be Maintained by the Current Security Policy
3	Accessibility to the TOE functions and data only for authorised subjects	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only.	Availability
4	Genuineness of the TOE	Property of the TOE to be authentic in order to provide the claimed security functionality in a proper way.	Availability
5	TOE immanent secret security data	<p>Secret security elements used by the TOE in order to enforce its security functionality.</p> <p>These are the following security elements of this category:</p> <ul style="list-style-type: none"> -equipment private key (EQT.SK), see [5], sec.III.12.2, -vehicle unit part of the symmetric master key for communication with MS (K_{mVU}), see [8], sec.3.1.3, -session key between motion sensor and vehicle unit K_{SM} (see [10], sec. 7.4.5 (instruction 42)), -session key between tachograph cards and vehicle unit K_{ST} (see [8], sec 3.2), - SW-Upgrade encryption key: SK_SWU - Secure boot private keys: PRIV_BOOT, SK_AP, SK_RTP, - Data storage key: SK_DATA, - Stored data integrity key: SK_HMAC. 	Confidentiality Integrity
6	TOE immanent non-secret security data	<p>Non-secret security elements used by the TOE in order to enforce its security functionality.</p> <p>There are the following security elements of this category:</p> <ul style="list-style-type: none"> -European public key (EUR.PK) -Member State certificate (MS.C) 	Integrity Authenticity

Object No	Secondary Asset	Definition	Generic Security Property to be Maintained by the Current Security Policy
		-equipment certificate (EQT.C) see [5], sec. III.12.2 -SW-Upgrade verification key: PUB_SWU -Secure boot public key: PUB_BOOT	
7	Application Processor Software	Upgradable software components	Confidentiality Integrity Authenticity
8	Security Processor Software	Upgradable software components	Confidentiality Integrity Authenticity
9	RTC Processor Software	Upgradable software components	Confidentiality Integrity Authenticity

Application Note 5: The workshop tachograph card requires an additional human user authentication by presenting a correct PIN value to the card. The vehicle unit (i) transmits the PIN verification value input by the user to the card and (ii) receives the card response to this verification attempt. A workshop tachograph card can only be used within the fitters and workshops environment (see A.Card_Availability below), which is presumed to be trustworthy (see A.Approved_Workshops below). Hence, no threat agent is presumed while using a workshop tachograph card. In this context, the VU is not required to secure a PIN verification value and any card response to a verification attempt, cf. [8], chapter 4.

The secondary assets represent TSF and TSF-data in the sense of the CC.

4.2 Subjects and External Entities

This security target considers the following subjects:

Table 4: Subjects and external entities

External Entity No	Subject No	Role	Definition
1	1	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.

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

External Entity No	Subject No	Role	Definition
			<p>There can also be Unknown User of the TOE and malicious user of the TOE – an attacker.</p> <p>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’.</p> <p>An attacker is a threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current ST, especially to change properties of the assets having to be maintained.</p> <p>The attacker is assumed to possess an <i>high</i> attack potential. Please note that the attacker might ‘capture’ any subject role recognised by the TOE.</p> <p>Due to constraints and definitions in [7], an attacker is an <u>attribute</u> of the role ‘User’ in the context of the current ST. Being a legal user is also an attribute of the role User.</p>
2	2	Unknown User	not authenticated user.
3	3	Motion Sensor	<p>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.</p> <p>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))</p>
4	-	Tachograph Card	<p>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:</p> <ul style="list-style-type: none"> Driver card, Control card, Workshop card, Company card. <p>A tachograph card possesses valid credentials for its authentication and their validity is verifiable.</p> <p>Valid credentials are a certified key pair for authentication being verifiable up to EUR.PK.</p>
5	4	Unknown Equipment	<p>A technical device not possessing valid credentials for its authentication or validity of its credentials is not verifiable.</p> <p>Valid credentials can be either a certified key pair for authentication of a device or MS serial number encrypted with</p>

External Entity No	Subject No	Role	Definition
			the identification key (Enc(K _{ID} N _S)) together with pairing key encrypted with the master key (Enc(K _m K _P))
6	-	Attacker	see item User above.

Application Note 6: This table defines the subjects in the sense of [1] which can be recognized by the TOE independent of their nature (human or technical user). As result of an appropriate identification and authentication process, the TOE creates – for each of the respective external entity – an ‘image’ inside and ‘works’ then with this TOE internal image (also called subject in [1]). From this point of view, the TOE itself does not differ between ‘subjects’ and ‘external entities’. There is no dedicated subject with the role ‘attacker’ within the current security policy, whereby an attacker might ‘capture’ any subject role recognised by the TOE.

4.3 Subjects, objects, and access rights

In this section access rights of TOE users and its external entities on the objects described for TOE are summarised below.

4.3.1 Subjects

S1 entities:

- S1.1 tachograph cards
- S1.2 downloading equipment
- S1.3 calibration device
- S1.4 motion sensor
- S1.5 management device

S2 users:

- S2.1 drivers and co-drivers
- S2.2 workshop staff, fitters and staff of vehicle manufacturers
- S2.3 control officers from national control authorities
- S2.4 staff of the respective haulage company
- S2.5 unknown

4.3.2 Objects

1. VU identification
2. Currently paired motion sensor ID
3. Driver card insertion and withdrawal data
4. Driver activity data
5. Places where daily work periods start and/or end
6. Odometer data
7. Detailed speed data
8. Events data
9. Faults data
10. Calibration data
11. Time adjustment data
12. Control activity data
13. Company locks data

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

14. Download activity data
15. Specific conditions data
16. PIN from workshop card
17. European public key EUR.PK
18. Member state certificate $MSi.C$
19. Equipment certificate $EQTj.C$ includes equipment public key $EQTj.PK$
20. Equipment private key $EQTj.SK$
21. Part of the Master key Km_{vu}
22. Software upgrade keys SK_SWU and PUB_SWU
23. Session key between motion sensor and vehicle unit K_{sm}
24. Session key between tachograph cards and vehicle unit K_{st}
25. Secure boot keys PUB_BOOT, PRIV_BOOT
26. Session key between AP and SP SK_AP
27. Session key between AP and RTP SK_RTP
28. Data storage key SK_DATA
29. HASH_AP and HASH_RTP
30. Part of the master key read out from the workshop card Km_{wc}
31. K_m : temporarily reconstructed from part of the master key Km_{VU}
32. K_{ID} : motion sensor identification key, temporarily reconstructed from the master key K_m
33. K_P : Temporarily reconstructed from $Enc(K_m|K_P)$

4.3.3 Access Rights

Table 5: Access rights

Record Name(Objects)	Subjects									
	Entities					Users				
	S1.1	S1.2	S1.3	S1.4	S1.5	S2.1	S2.2	S2.3	S2.4	S2.5
VU identification					W(once)	R	R	R	R	R
Currently paired motion sensor ID						R	R	R	R	R
Driver card insertion and withdrawal data						R/W	R/W	R/W	R/W	
Driver activity data	R					R/W	R/W	R	R	R/W
Places where daily work periods start and/or end	R					R/W	R/W	R	R	R/W
Odometer data						R/W	R/W	R/W	R/W	R/W
Detailed speed data						R/W	R/W	R/W	R/W	W
Events data	R					R/W	R/W	R/W	R/W	R/W

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

Record Name(Objects)	Subjects									
	Entities					Users				
	S1.1	S1.2	S1.3	S1.4	S1.5	S2.1	S2.2	S2.3	S2.4	S2.5
Faults data	R					R/W	R/W	R/W	R/W	R/W
Calibration data	R		R/W			R	R/W	R	R	R
Time adjustment data	R		R/W			R	R/W	R	R	R
Control activity data	R					R	R	R/W	R	R
Company locks data	R					R	R	R	R/W	R
Download activity data	R	R				R	R/W	R/W	R/W	R
Specific conditions data	R					R/W	R/W	R/W	R/W	R/W
PIN from workshop card	W						W			
European public key EUR.PK					W(once)	U	U	U	U	
Member state certificate MSi.C					W(once)	U	U	U	U	
Equipment certificate EQT _j .C includes equipment public key EQT _j .PK					W(once)	U	U	U	U	
Equipment private key EQT _j .SK					W(once)	U	U	U	U	
Part of the Master key K _{mvu}					W(once)	U	U	U	U	
Software upgrade keys PUB_SWU and SK_SWU					W(once)		U			

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

Record Name(Objects)	Subjects									
	Entities					Users				
	S1.1	S1.2	S1.3	S1.4	S1.5	S2.1	S2.2	S2.3	S2.4	S2.5
Session key between motion sensor and vehicle unit K_{sm}				G/U		G/U	G/U	G/U	G/U	
Session key between tachograph cards and vehicle unit K_{st}	G/U					G/U	G/U	G/U	G/U	
Secure boot keys PUB_BOOT, PRIV_BOOT					W(once)					
Session key between AP and SP SK_AP										
Session key between AP and RTP SK_RTP										
Data storage key SK_DATA						U	G/U	U	U	
HASH_AP and HASH_RTP					W					
Part of the master key read out from the workshop card K_{mwc}							U			
K_m : temporarily reconstructed from part of the master key K_{mvu}							U			
K_{ID} : motion sensor identification							U			

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

Record Name(Objects)	Subjects									
	Entities					Users				
	S1.1	S1.2	S1.3	S1.4	S1.5	S2.1	S2.2	S2.3	S2.4	S2.5
key, temporarily reconstructed from the master key K_m										
K_P : Temporarily reconstructed from $Enc(K_m K_P)$							U			

R = read; W = write; G = generate, U = use

4.4 Threats

This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the assets protected by the TOE and the method of TOE's use in the operational environment. The threats are identical to those given in [7] chapter 3.3.

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 ⁶ .
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 ⁶ not allowed to them (e.g. drivers gaining access to calibration function).
T.Calibration_Parameters	Users could try to use miscalibrated equipment ⁶ (through calibration data modification, or through organisational weaknesses).
T.Clock	Users could try to modify internal clock ⁶ .
T.Design	Users could try to gain illicit knowledge of design ⁶ either from manufacturer's material (through theft, bribery, etc.) or from reverse engineering.
T.Environment	Users could compromise the TOE security ⁶ 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 ⁷ .
T.Hardware	Users could try to modify TOE hardware ⁶ .
T.Identification	Users could try to use several identifications or no identification ⁸ .

⁶ The terms 'miscalibrated equipment', 'TOE security', 'TOE security objectives', 'data output', 'not allowed functions', 'TOE in a well defined state', 'TOE design', 'correctness of the internal clock', 'integrity of the TOE hardware', 'integrity of the TOE software', 'full activated security functionality of the TOE' correspond with [7] and are covered by the assets 'Accessibility to the TOE functions and data only for authorised subjects' and 'Genuineness of the TOE'.

⁷ Communication with genuine/known equipment is a prerequisite for a secure data exchange and, hence, represents a partial aspect of the asset 'user data transferred between the TOE and an external device connected'.

⁸ Identification data are part of the asset 'User data', see Glossary.

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

T.Motion_Data	Users could try to modify the vehicle's motion data (addition, modification, deletion, replay of signal) ⁹ .
T.Power_Supply	Users could try to defeat the TOE security objectives ⁶ by modifying (cutting, reducing, increasing) its power supply.
T.Security_Data	Users could try to gain illicit knowledge of security data ⁹ during security data generation or transport or storage in the equipment.
T.Software	Users could try to modify TOE software ⁶ .
T.Stored_Data	Users could try to modify stored data (security ¹⁰ or user data).
T.Tests	The use of non invalidated test modes or of existing back doors could compromise the TOE security ⁶ .

Application Note 7: Threat T.Faults represents a 'natural' flaw not induced by an attacker; hence, no threat agent can be stated here.

The threat agent for T.Tests is User. It can be deduced from the semantic content of T.Tests.

Threats averted solely by the TOE's operational environment:

T.Non_Activated	Users could use non-activated equipment ⁶ .
-----------------	--

4.5 Organizational Security Policies

The TOE and/or its environment must comply with the following Organisational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation upon its operations. They are defined here to reflect those security objectives from [7] for which there is no threat directly and fully associated.


4.5.1 OSPs related to the TOE

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.

⁹ Motion data transmitted are part of the asset 'user data transferred between the TOE and an external device connected'.

⁹ 'security data' are covered by the assets 'TOE immanent secret security data' and 'TOE immanent non-secret security data'

¹⁰ it means 'TOE immanent secret security data' and 'TOE immanent non-secret security data'

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

4.5.2 OSPs related to the TOE and its operational environment

OSP.Type_Approved_MS¹¹ The TOE only operates together with a motion sensor being type approved according to Annex 1B [5].

OSP.Management_Device The Management Device (MD) supports the appropriate communication interface with the VU and secures the relevant secrets inside the MD as appropriate.

4.5.3 OSPs related to the TOE's operational environment

OSP.PKI

- 1) 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.
- 2) 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.
- 3) The ERCA ensures that it issues Msi.C certificates only for the rightful MSCAs.
- 4) The ERCA issues the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules.
- 5) MSCAs securely generates their own key pairs (Msi.PK and Msi.SK) and equipment certificates (EQTj.C) over the public keys of the equipment.
- 6) MSCAs ensures that they issue EQTj.C certificates only for the rightful equipment.

OSP.MS_Keys

- 1) The European Authority establishes a special key infrastructure for management of the motion sensor keys according to [10] (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.
- 2) The ERCA securely generates both parts (K_{mVU} and K_{mWC}) of the master key (K_m).
- 3) The ERCA ensures that it securely convey this key material only to the rightful MSCAs.
- 4) The ERCA issues the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules.

¹¹ The identity data of the motion sensor (serial number N_S) will be sent to the VU on request by the MS itself (see instruction #40 in [12]). The 'certificate' $Enc(K_{ID}|N_S)$ stored in the motion sensor is merely used by it for VU authentication, but not for verifying N_S by the VU (see instruction #41 in [12]). Therefore, the VU accepts this data (serial number N_S) as it is. Hence, the structure of the motion sensor Identification Data is the matter of the IT environment (here: MS), but not of the VU itself. A correct structure of the MS identity is guaranteed by the fact that the MS is type approved.

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

- 5) 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 ($Enc(K_M|K_P)$).
- 6) MSCAs shall ensure that they issue these MS credentials¹², K_{mVU} ¹³ and K_{mWC} ¹⁴ only to the rightful equipment.

4.6 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

The GST in [7] does not define any dedicated assumption, but measures; these measures will be reflected in the current ST in form of the security objectives for the TOE environment below. Hence, it is to define some assumptions in the current ST being sensible and necessary from the formal point of view (to reflect those environmental measures from [7]).

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.) ¹⁵
A.Regular_Inspections	Recording equipment will be periodically inspected and calibrated. Inspection personal is educated about the security check points of the TOE.

¹² to the motion sensors

¹³ to the vehicle units

¹⁴ to the workshop cards

¹⁵ The assumption A.Faithful_Drivers taken from the Generic Security Target [7] seems not to be realistic and enforceable (from security point of view), because the driver is the person, who has to be controlled and surveyed (see the Commission Regulation [5]). This assumption is made in the current ST only for the sake of compatibility with the GST [7] and is necessary from functional point of view.

5 Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment.

5.1 Security Objectives for the TOE

The following TOE security objectives address the protection provided by the TOE independent of the TOE environment.

They are derived from the security objectives as defined in GST [7], sec. 3.5.

O.Access	The TOE controls user access to functions and data.
O.Accountability	The TOE collects accurate accountability data.
O.Audit	The TOE audits attempts to undermine system security and should trace them to associated users.
O.Authentication	The TOE authenticates users and connected entities (when a trusted path needs to be established between entities).
O.Integrity	The TOE maintains stored data integrity.
O.Output	The TOE ensures that data output reflects accurately data measured or stored.
O.Processing	The TOE ensures that processing of inputs to derive user data is accurate.
O.Reliability	The TOE provides a reliable service.
O.Secured_Data_Exchange	The TOE secures data exchanges with the motion sensor and with tachograph cards.
O.Software_Analysis ¹⁶	There is no way to analyse or debug software ¹⁷ in the field after the TOE activation.
O.Software_Upgrade	The TOE must ensure authenticity, integrity and confidentiality of the software to be installed during a software upgrade.


5.2 Security Objectives for the Operational Environment

The following security objectives for the TOE's operational environment address the protection provided by the TOE environment independent of the TOE itself.

They are derived from the security objectives as defined in GST [7], sec. 3.6, where they are represented as security measures.

¹⁶ This objective is added for the sake of a more clear description of the security policy: In the GST [7], this aspect is part of O.Reliability, what might be not self-evident. The special concern here is RLB_204 in [7].

¹⁷ It is a matter of the decision by the certification body and the evaluation facility involved in a concrete certification process on a classification of the TOE (hard- and software) into security relevant and irrelevant parts.

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

5.2.1 Design environment (cf. the life cycle diagram in above)

OE.Development The TOE developers ensure that the assignment of responsibilities during development is done in a manner which maintains IT security.

5.2.2 Manufacturing environment

OE.Manufacturing The TOE manufacturer ensures that the assignment of responsibilities during manufacturing is done in a manner which maintains IT security and that during the manufacturing process the TOE is protected from physical attacks which might compromise IT security.

OE.Sec_Data_Generation Security data generation algorithms are accessible to authorised and trusted persons only.

OE.Sec_Data_Transport Security data is generated, transported, and inserted into the TOE, in such a way to preserve its appropriate confidentiality and integrity.

OE.Delivery The TOE manufacturer, vehicle manufacturers and fitters or workshops ensure that handling of the TOE is done in a manner which maintains IT security.

OE.Software_Upgrade Software revisions are granted security certification before they can be implemented in the TOE.

OE.Sec_Data_Strong¹⁸ Security data inserted into the TOE is as cryptographically strong as required by [8].

OE.Test_Points¹⁹ All commands, actions or test points, specific to the testing needs of the manufacturing phase of the TOE are disabled or removed before the TOE activation by the manufacturer during the manufacturing process.

OE.Management_Device The TOE is personalized by the Management Device (MD). MD signs and encrypts the personalization file before being loaded into the VU.

Application Note 10: Please note that the design and the manufacturing environments are not the intended usage environments for the TOE (cf. the Application Note 2 above). The security objectives for these environments being due to the current security policy (OE.Development, OE.Manufacturing, OE.Test_Points, OE.Delivery) are the subject to the assurance class ALC. Hence, the related security objectives for the design and the manufacturing environments do not address any potential TOE user and, therefore, cannot be reflected in the documents of the assurance class AGD. The remaining security

¹⁸ The security objective OE.Sec_Data_Strong is defined in addition to [7] in order to reflect an aim of establishing the PKI and the symmetric key infrastructure (OSP.PKI and OSP.MS_Keys)

¹⁹ This objective is added for the sake of a more clear description of the security policy: In the GST [7], this aspect is part of O.Reliability, what might be not self-evident: A TOE cannot achieve an objective depending on action of its manufacturer. The special concern here is RLB_201 in [7] .

objectives for the manufacturing environment (OE.Sec_Data_Generation, OE.Sec_Data_Transport, OE.Sec_Data_Strong and OE.Software_Upgrade) are subject to the ERCA and MSA Policies and, therefore, are not specific for the TOE.

5.2.3 Workshops environment

OE.Activation	Vehicle manufacturers and fitters or workshops activate the TOE after its installation before the vehicle leaves the premises where installation took place.
OE.Approved_Workshops	Installation, calibration and repair of recording equipment carry by trusted and approved fitters or workshops.
OE.Faithful_Calibration	Approved fitters and workshops enter proper vehicle parameters in recording equipment during calibration.

5.2.4 End-user environment

OE.Card_Availability	Tachograph cards are available to TOE users and delivered by Member State Authorities to authorized persons only.
OE.Card_Traceability	Card delivery is traceable (white lists, black lists), and black lists are used during security audits.
OE.Controls	Law enforcement controls is performed regularly and randomly, and includes security audits.
OE.Driver_Card_Uniqueness	Drivers possess, at one time, one valid driver card only.
OE.Faithful_Drivers ²⁰	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.).
OE.Regular_Inspections	Recording equipment is periodically inspected and calibrated.
OE.Type_Approved_MS ²¹	The Motion Sensor of the recording equipment connected to the TOE is type approved according to Annex-1B [5].

5.3 Security Objective Rationale

The following table provides an overview for security objectives coverage (TOE and its environment) also giving an evidence for *sufficiency* and *necessity* of the security objectives defined. It shows that all threats

²⁰ The objective OE.Faithful_Drivers taken from the Generic Security Target [7] seems not to be realistic and enforceable (from security point of view), because the driver is the person, who has to be controlled and surveyed (see the Council Regulation [5]). This objective is claimed in the current PP only for the sake of compatibility with the GST [7] and is necessary from functional point of view, see also A.Faithful_Drivers.

²¹ The identity data of the motion sensor (serial number N_S) will be sent to the VU on request by the MS itself (see instruction #40 in [10]). The ‘certificate’ Enc(K_{ID} | N_S) stored in the motion sensor is merely used by it for VU authentication, but not for verifying N S by the VU (see instruction #41 in [10]). Therefore, the VU accepts this data (serial number N_S) as it is. Hence, the structure of the motion sensor Identification Data is the matter of the IT environment (here: MS), but not of the VU itself. A correct structure of the MS identity is guaranteed by the fact that the MS is type approved (-> UIA_202).

	<i>Communication and Information Technologies Sector Common Criteria Document</i>	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

and OSPs are addressed by the security objectives. It also shows that all assumptions are addressed by the security objectives for the TOE environment.

This rationale covers the rationale part in GST [7], chapter 8 and in [5].

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

Table 6: Security objective rationale

	Threats																OSPs							Assumptions														
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	OSP_Accountability	OSP_Audit	OSP_Processing	OSP_Test_Points	OSP_Type_Approved_MS	OSP_PKI	OSP_MS_Keys	OSP_Management_Device	A.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Fatihful_Calibration	A.Fatihful_Drivers	A.Regular_Inspections			
O.Access	X					X	X		X						X		X																					
O.Accountability		X																X																				
O.Audit	X	X				X			X	X	X		X	X		X	X		X																			
O.Authentication	X	X				X	X		X		X											X																
O.Integrity						X											X																					
O.Output					X					X			X			X	X																					
O.Processing						X	X	X	X	X					X	X				X																		
O.Reliability			X	X	X		X	X	X	X	X			X	X	X	X				X																	
O.Secured_Data_Exchange						X			X		X				X																							
O.Software_Analysis					X																																	
O.Software_Upgrade																X																						



**Communication and Information Technologies Sector
Common Criteria Document**

REV: 0.13 Number: **HBT-CC-8255-DT-01**


Language: 10 Date: **18.05.2021**

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

	Threats																OSPs							Assumptions														
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	OSP.Accountability	OSP.Audit	OSP.Processing	OSP_Test_Points	OSP_Type_Approved_MS	OSP.PKI	OSP_MS_Keys	OSP.Management_Device	A.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Faithful_Calibration	A.Faithful_Drivers	A.Regular_Inspections			
OE.Development					X											X																						
OE.Manufacturing				X	X																																	
OE.Sec_Data_Generation																X								X	X													
OE.Sec_Data_Transport																X								X	X													
OE.Delivery													X																									
OE.Software_Upgrade																X	X	X																				
OE.Sec_Data_Strong																X									X	X												
OE.Test_Points																						X																
OE.Management_Device																											X											
OE.Activation	X												X															X										
OE.Approved_Workshops						X	X					X																X								X		

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

	Threats															OSPs								Assumptions												
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	OSP.Accountability	OSP.Audit	OSP.Processing	OSP_Test_Points	OSP_Type_Approved_MS	OSP.PKI	OSP_MS_Keys	OSP.Management_Device	A.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Faithful_Calibration	A.Faithful_Drivers	A.Regular_Inspections	
OE.Faithful_Calibration						X	X																											X		
OE.Card_Availability		X																												X						
OE.Card_Traceability		X																													X					
OE.Controls						X	X	X	X	X		X		X	X	X	X	X														X				
OE.Driver_Card_Uniqueness		X																														X				
OE.Faithful_Drivers																																		X		
OE.Regular_Inspections						X	X		X	X	X	X		X		X																				X
OE.Type_Approved_MS									X		X											X														

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

The rationales for the mapping in the above table are given below.

5.3.1 Rationale for Threats

T.Access is addressed by O.Authentication to ensure the identification of the user, O.Access to control access of the user to functions, O.Audit to trace attempts of unauthorised accesses, OE.Activation to ensure access of the relevant users to relevant functions of the TOE.

T.Identification is addressed by O.Authentication to ensure the identification of the user, O.Audit to trace attempts of unauthorised accesses. O.Accountability contributes to address this threat by storing all activities carried (even without an identification) with the TOE. The OE.Driver_Card_Uniqueness, OE.Card_Availability and OE.Card_Traceability objectives, also required from Member States by law, help addressing the threat.

T.Faults is addressed by O.Reliability for fault tolerance. Indeed, if the TOE provides a reliable service as required by O.Reliability, the TOE cannot experience uncontrollable internal states. Hence, also each possible fault of the TOE will be controllable, i.e. the TOE will be in a well-known state at any time. Therefore, threats grounding in faults of the TOE will be eliminated.

T.Tests is addressed by O.Reliability and OE.Manufacturing. Indeed, if the TOE provides a reliable service as required by O.Reliability and its security cannot be compromised during the manufacturing process (OE.Manufacturing), the TOE can neither enter any invalidated test mode nor have any back door. Hence, the related threat will be eliminated.

T.Design is addressed by OE.Development and OE.Manufacturing before activation, and after activation by O.Software_Analysis to prevent reverse engineering and by O.Output to ensure that data output reflects accurately data measured or stored. Also the security objective O.Reliability makes it difficult for the user to gain information about the design of the TOE by reverse engineering.

T.Calibration_Parameters is addressed by O.Access to ensure that the calibration function is accessible to workshops only, O.Authentication to ensure the identification of the workshop, O.Processing to ensure that processing of inputs made by the workshop to derive calibration data is accurate, O.Integrity to maintain the integrity of calibration parameters stored. Workshops are approved by Member States authorities and are therefore trusted to calibrate properly the equipment (OE.Approved_Workshops, OE.Faithful_Calibration). Periodic inspections and calibration of the equipment, as required by law (OE.Regular_Inspections), contribute to address the threat. Finally, OE.Controls includes controls by law enforcement officers of calibration data records held in the TOE, which helps addressing the threat as well.

T.Card_Data_Exchange is countered by the combination of the security objectives O.Audit, O.Secured_Data_Exchange and O.Reliability. The security objective O.Secured_Data_Exchange secures the data exchange between the TOE and the tachograph card, such that modifications of the data are detected, in which case by the security objective O.Audit modifications of exchanged data are audited by the TOE. With O.Reliability data are exchanged by reliable services.

T.Clock is addressed by the security objectives; O.Access, O.Authentication, O.Processing, OE.Approved_Workshops, OE.Regular_Inspections, OE.Faithful_Calibration and OE.Controls. O.Access ensures that the full time adjustment function is accessible to workshops only, O.Authentication ensures the identification of the workshop, and O.Processing ensures that processing of inputs made by the workshop to derive time adjustment data is accurate. Workshops are approved by Member State authorities and are therefore trusted to properly set the clock (OE.Approved_Workshops). Periodic inspections and calibration of the equipment, as required by law (OE.Regular_Inspections,

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

OE.Faithful_Calibration), contribute to address the threat. Finally, OE.Controls includes controls by law enforcement officers of time adjustment data records held in the TOE, which helps addressing the threat.

T.Environment is addressed by O.Processing to ensure that processing of inputs to derive user data is accurate, O.Reliability to ensure that physical attacks are countered. OE.Controls includes controls by law enforcement officers of time adjustment data records held in the TOE, which helps addressing the threat.

T.Fake_Devices is addressed by O.Access, O.Authentication, O.Audit, O.Processing, O.Reliability, and O.Secured_Data_Exchange. OE.Type_Approved_MS ensures that only motion sensors with correct identification data have the credentials required to successfully authenticate themselves. OE.Controls and OE.Regular_Inspections help addressing the threat through visual inspection of the whole installation.

T.Hardware is addressed by O.Reliability, O.Output and O.Processing. O.Audit also contributes to address the threat by recording events related to hardware manipulation. The OE.Controls and OE.Regular_Inspections help addressing the threat through visual inspection of the installation.

T.Motion_Data is addressed by O.Authentication, O.Reliability, O.Secured_Data_Exchange, OE.Regular_Inspections and OE.Type_Approved_MS. O.Audit contributes to address the threat by recording events related to motion data exchange integrity or authenticity errors.

T.Non_Activated is addressed by the OE.Activation and OE.Delivery. Workshops are approved by Member States authorities and are therefore trusted to activate properly the equipment (OE.Approved_Workshops). Periodic inspections and calibration of the equipment, as required by law (OE.Regular_Inspections, OE.Controls), also contribute to address the threat.

T.Output_Data is addressed by O.Output. O.Audit contributes to address the threat by recording events related to data display, print and download.

T.Power_Supply is mainly addressed by O.Reliability to ensure appropriate behaviour of the VU against the attack. O.Audit contributes to address the threat by keeping records of attempts to tamper with power supply. OE.Controls includes controls by law enforcement officers of power supply interruption records held in the VU, which helps addressing the threat. OE.Regular_Inspections also helps addressing the threat through installations, calibrations, checks, inspections and repairs carried out by trusted fitters and workshops.

T.Security_Data is addressed by OE.Sec_Data_Generation, OE.Sec_Data_Strong, OE.Sec_Data_Transport, OE.Software_Upgrade and OE.Controls. It is also addressed by the O.Access, O.Processing, and O.Secured_Data_Exchange to ensure appropriate protection while stored in the VU. O.Reliability is relevant here as well.

T.Software is addressed in the user environment by O.Output, O.Processing, O.Reliability and O.Software_Upgrade to ensure the integrity of the code. O.Audit contributes to address the threat by recording events related to integrity errors. During design and manufacturing, the threat is addressed by the OE.Development. OE.Controls, OE.Regular_Inspections (checking for the audit records related).

T.Stored_Data is addressed mainly by O.Integrity, O.Access, O.Output and O.Reliability to ensure that no illicit access to data is possible. The O.Audit contributes to address the threat by recording data integrity errors. OE.Software_Upgrade included that software revisions must be security certified before they can be implemented in the TOE to prevent to alter or delete any stored driver activity data. OE.Controls includes controls by law enforcement officers of integrity error records held in the VU helping in addressing the threat.

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

5.3.2 Rationale for Organizational Security Policies

OSP.Accountability is addressed by O.Accountability by collecting accurate accountability data.

OSP.Audit is addressed by O.Audit by auditing attempts to undermine system security and tracing them to associated users.

OSP.Processing is addressed by O.Processing by ensuring that data output reflects accurately data measured or stored.

OSP.Test_Points is addressed by O.Reliability and OE.Test_Points by providing reliable service and disabling all test points before the TOE leaves the manufacturer site.

OSP.Type_Approved_MS is addressed by O.Authentication by ensuring the identity of the user and OE.Type_Approved_MS by accepting inputs only from the type approved motion sensor.

OSP.PKI is addressed by OE.Sec_Data_Generation by allowing only the authorized and trusted persons to access to the security data, OE.Sec_Data_Strong by using cryptographically secure algorithms, and OE.Sec_Data_Transport by ensuring the confidentiality and the integrity of the transported data.

OSP.MS_Keys is addressed by OE.Sec_Data_Generation by allowing only the authorized and trusted persons to access to the security data, OE.Sec_Data_Strong by using cryptographically secure algorithms, and OE.Sec_Data_Transport by ensuring the confidentiality and the integrity of the transported data.

OSP.Management_Device is addressed by O.Software_Upgrade by ensuring the confidentiality, integrity and authenticity of the software to be loaded and OE.Management_Device by providing a secure channel between the TOE and MD.

5.3.3. Rationale for Assumptions

A.Activation is upheld by OE.Activation by activating the TOE by approved workshops after its installation before the vehicle leaves the premises.

A.Approved_Workshops is upheld by OE.Approved_Workshops by carrying installation, calibration and repair by trusted and approved workshops.

A.Card_Availability is upheld by OE.Card_Availability by delivering the tachograph cards to the authorized persons only by Member State Authorities.

A.Card_Traceability is upheld by OE.Card_Traceability by tracing the card delivery and using these traces during security audits.

A.Controls is upheld by OE.Controls by performing controls regularly and randomly including security audits by the law enforcement.

A.Driver_Card_Uniqueness is upheld by OE.Driver_Card_Uniqueness by providing only one valid driver card at one time to each driver by the card issuing authority.

A.Faithful_Calibration is upheld by OE.Faithful_Calibration and OE.Approved_Workshops by carrying installation, calibration and repair of the TOE and entering proper vehicle parameters during calibration by trusted and approved workshops.

A.Faithful_Drivers is upheld by OE.Faithful_Drivers by obeying the rules and acting responsibly by drivers.

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

A.Regular_Inspections is upheld by OE.Regular_Inspections by periodically inspecting and calibrating the TOE by approved workshops.

6 Extended Components Definition

This Security Target does not use any components defined as extensions to CC part 2.

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

7 Security Requirements

This Security Target clarifies and adapts the security requirements as given in the Digital Tachograph-Vehicle Unit Protection Profile, BSI-CC-PP-0057, Version 1.0, 13th July 2010 [11].

This part of the Security Target defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE.

The CC allows several operations to be performed on security requirements (on the component level); *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 8.1 of Part 1 [1] of the CC. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and, thus, further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and changed words are ~~crossed out~~.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicised*.

Selections having been made by the ST author are denoted as *italic*.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicised*. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus, this text is underlined and italicised like *this*.

Assignments having been made by the ST author are denoted by showing as *italic and bold underlined text*.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash “/”, and the iteration indicator after the component identifier. In order to trace elements belonging to a component, the same slash “/” with iteration indicator is used behind the elements of a component.

For the sake of a better readability, the author uses an additional notation in order to indicate belonging of some SFRs to same functional cluster, namely a double slash “//” with the related functional group indicator after the component identifier. In order to trace elements belonging to a component, the same double slash “//” with functional cluster indicator is used behind the elements of a component

7.1 Security Functional Requirements

The security functional requirements are as derived in the PP [11] which covers the SFRs from the generic security target from [7].

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

In the following the necessary assignments as foreseen by the PP for the SFRs in the protection profile and the necessary enhancements for software-update functionality are processed. For the software-update functionality, some new SFRs are included.

Each of the below SFRs includes in curly braces {...} a list of SFRs related. This not only explains why the given SFR has been chosen, but moreover is used to state further detail of the SFR without verbose repetition of the original text of the corresponding SFR(s) from [7]. The main advantage of this approach is avoiding redundancy, and, more important, any unambiguity.

The complete coverage of the SFR(s) from [7] is documented in Annex A, sec. 10 below.

7.1.1 Overview

Table 7: Security functional groups vs. SFRs.

Security Functional Groups	Security Functional Requirements concerned
<p>Identification and authentication of motion sensor, tachograph cards and management device (according to [7], sec. 4.1)</p>	<ul style="list-style-type: none"> – FIA_UID.2/MS: Identification of the motion sensor – FIA_UID.2/TC: Identification of the tachograph cards – FIA_UID.2/MD: Identification of the Management Device – (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor – (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards – FIA_UAU.1/MD, FIA_UAU.3/MD: Authentication of the Management Device – FIA_UAU.1/PIN: additional PIN authentication for the workshop card – FIA_AFL.1/MS: Authentication failure: motion sensor – FIA_AFL.1/TC: Authentication failure: tachograph cards – (FIA_ATD.1//TC, FMT_SMR.1//TC): User groups to be maintained by the TOE Supported by: – FCS_COP.1/TDES: for the motion sensor – FCS_COP.1/RSA: for the tachograph cards – FCS_COP.1/ECDSA: for signature verification of the software update data – (FCS_CKM.1/TDES, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management – FAU_GEN.1: Audit records: Generation – (FMT_MSA.1, FMT_SMF.1) – FIA_AFL.1/Remote: remote TC authentication failure handling

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

Security Functional Groups	Security Functional Requirements concerned
<p>Access control to functions and stored data (according to [7], sec. 4.2)</p>	<ul style="list-style-type: none"> – (FDP_ACC.1/FIL, FDP_ACF.1/FIL): file structures – (FDP_ACC.1/FUN, FDP_ACF.1/FUN): functions – (FDP_ACC.1/DAT, FDP_ACF.1/DAT): stored data – (FDP_ACC.1/UDE, FDP_ACF.1/UDE): user data export – (FDP_ACC.1/IS, FDP_ACF.1/IS): input sources – FDP_ACC.1/SW-Upgrade: authenticate the software upgrades – FDP_ACF.1/SW-Upgrade: capability to control access to the TSF software upgrade function <p>Supported by:</p> <ul style="list-style-type: none"> – (FIA_UAU.2//MS, FIA_UAU.3//MS, FIA_UAU.6//MS): Authentication of the motion sensor – (FIA_UAU.1//TC, FIA_UAU.3//TC, FIA_UAU.5//TC, FIA_UAU.6//TC): Authentication of the tachograph cards – FIA_UAU.1//PIN: additional PIN authentication for the workshop card – FIA_UAU.1//MD, FIA_UAU.3//MD: Authentication of the Management Device – FMT_MSA.3/FIL – FMT_MSA.3/FUN – FMT_MSA.3/DAT – FMT_MSA.3/UDE – FMT_MSA.3/IS – (FMT_MSA.1, FMT_SMF.1, FMT_SMR.1//TC)

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

Security Functional Groups	Security Functional Requirements concerned
<p>Accountability of users (according to [7], sec. 4.3)</p>	<ul style="list-style-type: none"> – FAU_GEN.1: Audit records: Generation – FAU_STG.1: Audit records: Protection against modification – FAU_STG.4: Audit records: Prevention of loss – FDP_ETC.2: Export of user data with security attributes <p>Supported by:</p> <ul style="list-style-type: none"> – (FDP_ACC.1/DAT, FDP_ACF.1/DAT): VU identification data – (FDP_ACC.1/UDE, FDP_ACF.1/UDE): Data update on the TC – FPT_STM.1: time stamps – FCS_COP.1/TDES: for the motion sensor and the tachograph cards
<p>Audit of events and faults (according to [7], sec. 4.4)</p>	<ul style="list-style-type: none"> – FAU_GEN.1: Audit records: Generation – FAU_SAR.1: Audit records: Capability of reviewing <p>Supported by:</p> <ul style="list-style-type: none"> – (FDP_ACC.1/DAT, FDP_ACF.1/DAT): Storing motion sensor's audit records – FDP_ETC.2 Export of user data with security attributes: Related audit records to the TC.
<p>Object reuse for secret data (according to [7], sec. 4.5)</p>	<ul style="list-style-type: none"> – FDP_RIP.1 Subset residual information protection <p>Supported by:</p> <ul style="list-style-type: none"> – FCS_CKM.4: Cryptographic key destruction

Security Functional Groups	Security Functional Requirements concerned
<p>Accuracy of recorded and stored data</p>	<ul style="list-style-type: none"> – FDP_ITC.1: right input sources without sec. attributes (keyboard, calibration data, RTC)

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

Security Functional Groups	Security Functional Requirements concerned
(according to [7], sec. 4.6)	<ul style="list-style-type: none"> – FDP_ITC.2//IS: right input sources with sec. attributes (MS and TC) – FDP_ITC.2//SW-Upgrade: import of user data with security attributes – FPT_TDC.1//IS: Inter-TSF basic TSF data consistency (MS and TC) – FDP_SDI.2: Stored data integrity – FPT_TDC.1//SW-Upgrade: capability to ensure the consistency of data for the update – FCS_COP.1/AES: for decryption of the software update data and encryption / decryption of the data transferred between the security processor and the application processor – FCS_COP.1/ECDSA: for sign verification of the software update data <p>Supported by:</p> <ul style="list-style-type: none"> – FCS_CKM.1/AES: Cryptographic key generation – (FDP_ACC.1//IS, FDP_ACF.1//IS): right input sources – (FDP_ACC.1//FUN, FDP_ACF.1//FUN): limited manual entry – FAU_GEN.1: Audit records: Generation – FPT_STM.1: Reliable time stamps – (FIA_UAU.2//MS, FIA_UAU.3//MS, FIA_UAU.6//MS): Authentication of the motion sensor – (FIA_UAU.1//TC, FIA_UAU.3//TC, FIA_UAU.5//TC, FIA_UAU.6//TC): Authentication of the tachograph cards – FIA_UAU.1//MD, FIA_UAU.3//MD: Authentication of the Management Device

Security Functional Groups	Security Functional Requirements concerned
Reliability of services	– FDP_ITC.2//IS: no executable code from external sources

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

Security Functional Groups	Security Functional Requirements concerned
(according to [7], sec. 4.7)	<ul style="list-style-type: none"> – FDP_ITC.2//SW-Upgrade: definition of conditions for update acceptance – FPR_UNO.1: Unobservability of leaked data – FPT_FLS.1: Failure with preservation of secure state – FPT_PHP.2//Power_Deviation: Notification of physical attack – FPT_PHP.2// HW_sabotage: Notification of physical attack – FPT_PHP.3: Resistance to physical attack: stored data – FPT_TST.1: TSF testing – FRU_PRS.1: Availability of services Supported by: – FAU_GEN.1: Audit records: Generation – (FDP_ACC.1/IS, FDP_ACF.1/IS): no executable code from external sources – (FDP_ACC.1/FUN, FDP_ACF.1/FUN): Tachograph Card withdrawal – FMT_MOF.1: No test entry points

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

Security Functional Groups	Security Functional Requirements concerned
<p>Data exchange with motion sensor, tachograph cards and external media (download function) (according to [7], sec. 4.8)</p>	<p>– FCO_NRO.1: Selective proof of origin for data to be downloaded to external media</p> <p>– FDP_ETC.2 Export of user data with security attributes: to the TC and to external media</p> <p>– FDP_ITC.2//IS Import of user data with security attributes: from the MS and the TC</p> <p>Supported by:</p> <p>– FCS_COP.1/TDES: for the motion sensor and the tachograph cards (secure messaging)</p> <p>– FCS_COP.1/RSA: for data downloading to external media (signing)</p> <p>– (FCS_CKM.1/TDES, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management</p> <p>– (FDP_ACC.1/UDE, FDP_ACF.1/UDE): User data export to the TC and to external media</p> <p>– (FDP_ACC.1/IS, FDP_ACF.1/IS): User data import from the MS and the TC</p> <p>– FAU_GEN.1: Audit records: Generation</p>
<p>Management of and access to TSF and TSF-data</p>	<p>– The entire class FMT.</p> <p>Supported by:</p> <p>– the entire class FIA: user identification/authentication</p>

7.1.2 Class FAU Security Audit

7.1.2.1 FAU_GEN Security audit data generation

FAU_GEN.1 Audit data generation {UIA_206, UIA_214, ACT_201, ACT_203, ACT_204, ACT_205, AUD_201, AUD_202, AUD_203, ACR_205, RLB_203, RLB_206, **RLB_208**, RLB_210, RLB_214, DEX_202, DEX_204}

Hierarchical to: -

Dependencies: FPT_STM.1 Reliable time stamps: is fulfilled by FPT_STM.1.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the *not specified* level of audit; and

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

- c) the activities and auditable events specified in REQ 081, 084, 087, 090, 093, 094, 096, 098, 101, 102, 103, and 105a²² and {UIA 206, UIA 214, AUD 202, ACR 205, RLB 203, RLB 206, RLB 210, RLB 214²³, DEX 202, DEX 204}; RLB 208.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, the information specified in {REQ 081, 084, 087, 090, 093, 094, 096, 098, 101, 102, 103, 105a²⁴}; none.

7.1.2.2 FAU_SAR Security audit review

FAU_SAR.1 Audit review {AUD_205}

Hierarchical to: -

Dependencies: FAU_GEN.1 Audit data generation: is fulfilled by FAU_GEN.1.

FAU_SAR.1.1 The TSF shall provide everybody with the capability to read the recorded information according to REQ011 from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

7.1.2.3 FAU_STG Security audit event storage

FAU_STG.1 Protected audit trail storage {ACT_206}²⁵

Hierarchical to: -

Dependencies: FAU_GEN.1 Audit data generation: is fulfilled by FAU_GEN.1.

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to *detect* unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss {ACT_206}²⁶

Hierarchical to: FAU_STG.3

Dependencies: FAU_STG.1 Protected audit trail storage: is fulfilled by FAU_STG.1.

FAU_STG.4.1 The TSF shall overwrite the oldest stored audit records and behaves according to REQ 083, 086, 089, 092 and 105b, if the audit trail is full.

²² all these REQ are referred to in {ACT_201, ACT_203, ACT_204, ACT_205, AUD_201, AUD_203}

²³ Last card session not correctly closed

²⁴ all these REQ are referred to in {ACT_201, ACT_203, ACT_204, ACT_205, AUD_203}

²⁵ REQ081 to 093 and REQ102 to 105a

²⁶ REQ 083, 086, 089, 092, 105b; REQ105b is completely covered by ACT_206.

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

Application Note 17: The data memory is able to hold ‘driver card insertion and withdrawal data’ (REQ082), ‘driver activity data’ (REQ085) and ‘places where daily work periods start and/or end’ (REQ088) for at least 365 days. Since these requirements are not subject to GST [9]²⁷, they are also not included in the formal content of FAU_STG.4.

For same reason, the respective part of requirement for ‘specific conditions data’ (REQ105b, at least 365 days) is also out of scope of the formal content of FAU_STG.4.

7.1.3 Class FCO Communication

7.1.3.1 FCO_NRO Non-repudiation of origin

FCO_NRO.1 Selective proof of origin {DEX_206, DEX_207}

Hierarchical to: -

Dependencies: FIA_UID.1 Timing of identification: not fulfilled, but **justified**.

The components FIA_UID.2/MS, FIA_UID.2/TC being present in the ST do not fulfil this dependency, because they are not affine to DEX_206, DEX_207 (data download).

The sense of the current dependency would be to attach the VU identity (ACT_202) to the data to be downloaded; the VU identification data are permanently stored in the VU, so that the VU always ‘knows’ its own identity.

Application Note 17a: The dependency is justified as the vehicle unit identification data can be downloaded if the technical data from the VU is requested by the Intelligent Dedicated Equipment (IDE) according to DDP_011 [14]. Moreover, according to DDP_054 [14] it is mandatory for the IDE to request the overview data transfer during a download session as this only will ensure that the VU certificates are recorded within the downloaded file (and allow for verification of digital signature). Certificate Holder Reference (CHR) field of the VU certificate includes the serial number of the VU according to CSM_017 [10]. This serial number is part of the permanent identification data as referred to in (ACT_202) and it can be used to trace between technical data and overview data. Hence the dependency of the SFR is interpreted as the fact that the VU always knows its own identity which can be downloaded in the technical data if requested by the download equipment (IDE).

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted data to be downloaded to external media at the request of the originator.

FCO_NRO.1.2 The TSF shall be able to relate the VU identity of the originator of the information, and the data to be downloaded to external media of the information to which the evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to the recipient given – according to specification [8], sec. 6.1, limited to the scope as required in {DEX_207} and {DEX_208}.

7.1.4 Class FCS Cryptographic Support

7.1.4.1 FCS_CKM Cryptographic key management

FCSC_CKM.1/TDES Cryptographic key generation {CSP_202}

²⁷ ACT_206 does not require keeping data for at least 365 days

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

Hierarchical to: -

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: is fulfilled by FCS_CKM.2;
FCS_CKM.4 Cryptographic key destruction: is fulfilled by FCS_CKM.4

FCS_CKM.1.1/TDES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm cryptographic key derivation algorithms (for the session keys K_{SM} and K_{ST} as well as for the temporarily stored keys K_m , K_P and K_{ID}) and specified cryptographic key sizes 112 bits that meet the following: list of standards:

- a) K_m , K_P , K_{ID} and K_{SM} : two-keys TDES as specified in [10];
- b) K_{ST} : two-keys TDES as specified in [8].

FCS_CKM.1/AES Cryptographic key generation {CSP_202}

Hierarchical to: -

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: is fulfilled by FCS_COP.1/AES;

FCS_CKM.1.1/AES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Using the Output of a Random Bit Generator (for session keys SK_{AP} and SK_{RTP} , for data stored inside AP temporarily SK_{DATA}) and specified cryptographic key sizes 128 bits that meet the following: list of standards:

- a) SK_{AP} key generation algorithm are not made according to any standard;
- b) SK_{RTP} key generation algorithm are not made according to any standard;
- c) SK_{DATA} key generation algorithm are not made according to any standard.

FCS_CKM.2 Cryptographic key distribution {CSP_203}

Hierarchical to: -

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/TDES or FCS_CKM.1/AES]: is fulfilled by FCS_CKM.1/TDES or FCS_CKM.1/AES
FCS_CKM.4: is fulfilled by FCS_CKM.4

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method as specified in the list below that meets the following list of standards:

- a) K_{SM} : as specified in [12], sec. 7.4.5;
- b) K_{ST} : as specified in [10], CSM_020;
- c) SK_{AP} : not made according to any standard;
- d) SK_{RTP} : not made according to any standard.

FCS_CKM.3 Cryptographic key access {CSP_204}

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

Hierarchical to: -

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/TDES or FCS_CKM.1/AES]:

- a) fulfilled by FCS_CKM.1/TDES for the session keys K_{SM} and K_{ST} as well as for the temporarily stored keys K_m , K_P and K_{ID} ; **and fulfilled by FCS_CKM.1/AES for session keys SK_AP, SK_RTP and SK_DATA;**
- b) fulfilled by FDP_ITC.2//IS for the temporarily stored key $K_{m_{wc}}$ (entry DEX_203);
- c) not fulfilled, but **justified** for EUR.PK, EQT.SK, $K_{m_{vu}}$, **PUB_BOOT, PRIV_BOOT, PUB_SWU, SK_SWU, SK_HMAC**: The persistently stored keys (EUR.PK, EQTj.SK, $K_{m_{vu}}$, **PUB_BOOT, PRIV_BOOT, PUB_SWU, SK_SWU, SK_HMAC**) will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx.

[FCS_CKM.4]: is fulfilled by FCS_CKM.4

FCS_CKM.3.1

The TSF shall perform cryptographic key access and storage in accordance with a specified cryptographic key access method as specified below that meets the following list of standards:

- a) $K_{m_{wc}}$: part of the Master key read out from the workshop card and temporarily stored in the TOE (calibration phase);
- b) K_m : temporarily reconstructed from part of the Master key $K_{m_{vu}}$ and part of the Master key $K_{m_{wc}}$ as specified in [12], sec. 7.2 and in [10], sec. 3.1.3, CSM 036, CSM 037 (calibration phase);
- c) K_{ID} : temporarily reconstructed from the Master key K_m as specified in [12], sec. 7.2, 7.4.3 (calibration phase);
- d) K_P : temporarily reconstructed from $Enc(K_m K_P)$ as specified in [12], sec. 7.2, 7.4.3 (calibration phase);
- e) K_{SM} : internally generated and temporarily stored during a session between the TOE and the motion sensor connected (calibration and operational phases);
- f) K_{ST} : internally generated and temporarily stored during a session between the TOE and the tachograph card connected (calibration and operational phases);
- g) EUR.PK: stored during manufacturing of the TOE (calibration and operational phases);
- h) EQTj.SK: stored during manufacturing of the TOE (calibration and operational phases);
- i) part of the Master key $K_{m_{vu}}$: stored during manufacturing of the TOE (calibration and operational phases);
- j) Software upgrade keys – SK_SWU and PUB_SWU: stored during manufacturing of the TOE;
- k) Secure boot keys – PUB_BOOT and PRIV_BOOT: stored during manufacturing of the TOE;
- l) SK AP: internally generated and temporarily stored during a session between AP and SP;

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

- m) SK RTP: internally generated and temporarily stored during a session between AP and RTP;
- n) SK DATA: internally generated and temporarily stored during a session between the TOE and the motion sensor connected (calibration and operational phases);
- o) SK HMAC: stored during manufacturing of the TOE.

FCS_CKM.4 Cryptographic key destruction {CSP_205}

Hierarchical to: -

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/TDES or FCS_CKM.1/AES]:
see explanation for FCS_CKM.3 above

FCS_CKM.4.1 The TSF shall destroy cryptographic key in accordance with a specified cryptographic key destruction method as specified below that meets the following list of standards:

- a) K_{mwc}: delete after use (at most by the end of the calibration phase);
- b) K_m: delete after use (at most by the end of the calibration phase);
- c) K_{ID}: delete after use (at most by the end of the calibration phase);
- d) K_P: delete after use (at most by the end of the calibration phase);
- e) K_{SM}: delete by replacement (by closing a motion sensor communication session during the next pairing process);
- f) K_{ST}: delete by replacement (by closing a card communication session);
- g) EUR.PK: this public key does not represent any secret and, hence, needn't to be deleted;
- h) EQT_j.SK: will be loaded into the TOE outside of its operational phase, cf. also OE.Sec Data xx and must not be destroyed as long as the TOE is operational;
- i) part of the Master key K_{m_{vu}}: will be loaded into the TOE outside of its operational phase, cf. also OE.Sec Data xx and must not be destroyed as long as the TOE is operational;
- j) Software upgrade keys – SK SWU and PUB SWU: will be loaded into the TOE outside of its operational phase, cf. also OE.Sec Data xx, and must not be destroyed as long as the TOE is operational;
- k) Secure boot keys – PUB BOOT and PRIV BOOT: will be loaded into the TOE outside of its operational phase, cf. also OE.Sec Data xx and must not be destroyed as long as the TOE is operational;
- l) SK AP: delete by replacement (by closing a communication session between AP and SP);
- m) SK RTP: delete by replacement (by closing a communication session between AP and RTP);
- n) SK DATA: delete by replacement (by closing a motion sensor communication session during the next pairing process);

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

- o) SK HMAC: will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx, and must not be destroyed as long as the TOE is operational.

Application Note 18: The component FCS_CKM.4 relates to any instantiation of cryptographic keys independent of whether it is of temporary or permanent nature. In contrast, the component FDP_RIP.1 concerns in this ST only the temporarily stored instantiations of objects in question. The permanently stored instantiations of EQT_j.SK and of the part of the Master key Km_{vu} must not be destroyed as long as the TOE is operational. Making the permanently stored instantiations of EQT_j.SK and of the part of the Master key Km_{vu} unavailable at decommissioning the TOE is a matter of the related organizational policy.

7.1.4.2 FCS_COP Cryptographic operation

FCS_COP.1/TDES Cryptographic operation {CSP_201}

Hierarchical to: -

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/TDES]: is fulfilled by FCS_CKM.1/TDES
FCS_CKM.4: is fulfilled by FCS_CKM.4.

FCS_COP.1.1/TDES The TSF shall perform the cryptographic operations (encryption, decryption, Retail-MAC) in accordance with a specified cryptographic algorithm Triple DES in CBC and ECB modes and cryptographic key size 112 bits that meet the following: [10] for the Motion Sensor and [8] for the Tachograph Cards.

FCS_COP.1/RSA Cryptographic operation {CSP_201}

Hierarchical to: -

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]: not fulfilled, but **justified**.
It is a matter of RSA decrypting and verifying in the context of CSM_020 (VU<->TC authentication) and of RSA signing according to CSM_034 using static keys imported outside of the VU's operational phase (OE.Sec_Data_xx).
FCS_CKM.4: is fulfilled by FCS_CKM.4.
[FCS_CKM.1/RSA]: is fulfilled by FCS_CKM.1/RSA.

FCS_COP.1.1/RSA The TSF shall perform the cryptographic operations (decryption, verifying for the Tachograph Cards authentication and signing for downloading to external media) in accordance with a specified cryptographic algorithm RSA and cryptographic key size 1024 bits that meet the following: [8], CSM_020 for the Tachograph Cards authentication and [8], CSM_034 for downloading to external media, respectively.

FCS_COP.1.2/RSA The TSF shall perform the cryptographic operations (encryption and decryption of the secure boot data) in accordance with a specified cryptographic algorithm RSA and cryptographic key size 1024 bits that meet the following: none.

FCS_COP.1/AES Cryptographic operation

Hierarchical to: -

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

Dependencies: [FDP_ITC.2 or FCS_CKM.1/AES]: not fulfilled, but justified for SK_SWU: The persistently stored key SK_SWU will be loaded into the TOE during personalization at the end of the manufacturing of the TOE outside of its operational phase, cf. also OE.Sec_Data_xx.

FCS_CKM.4: is fulfilled by FCS_CKM.4.

[FCS_CKM.1/AES]: is fulfilled by FCS_CKM.1/AES for SK_AP, SK_RTP and SK_DATA.

FCS_COP.1.1/AES The TSF shall perform the cryptographic operations (encryption and decryption) in accordance with a specified cryptographic algorithm AES in ECB and OFB mode and cryptographic key size 128 bits that meet the following: [AES].

FCS_COP.1.2/AES The TSF shall perform the cryptographic operations (encryption and decryption) in accordance with a specified cryptographic algorithm AES in OFB mode and cryptographic key size 256 bits that meet the following: [AES].

FCS_COP.1/ECDSA Cryptographic operation

Hierarchical to: -

Dependencies: [FDP_ITC.2 or FCS_CKM.1]: not fulfilled, but justified for PUB_SWU: The persistently stored key PUB_SWU will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx.

[FCS_CKM.3 or FCS_CKM.4]: is fulfilled by FCS_CKM.3 or FCS_CKM.4.

FCS_COP.1.1/ECDSA The TSF shall perform the cryptographic operations (signature verification) in accordance with a specified cryptographic algorithm ECDSA using SHA-256 and cryptographic key size 521 bits (NIST Curve P-521) that meet the following: [ECDSA], [SHA-256].

FCS_COP.1/HMAC Cryptographic operation

Hierarchical to: -

Dependencies: [FCS_CKM.1]: not fulfilled, but justified for SK_HMAC: The persistently stored key SK_HMAC will be loaded into the TOE outside of its operational phase, cf. also OE.Sec_Data_xx.

[FCS_CKM.3 or FCS_CKM.4]: is fulfilled by FCS_CKM.4.

FCS_COP.1.1/HMAC The TSF shall perform the cryptographic operations (user data integrity and authenticity verification) in accordance with a specified cryptographic algorithm HMAC using SHA-1 and cryptographic key size 32 bytes that meet the following: none.

7.1.5 Class FDP User Data Protection

7.1.5.1 FDP_ACC Access control policy

FDP_ACC.1/FIL Subset access control {ACC_211}

Hierarchical to: -

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

Dependencies: FDP_ACF.1: is fulfilled by FDP_ACF.1/FIL.

FDP_ACC.1.1/FIL The TSF shall enforce the File Structure SFP on

- subjects:

- User.

- Motion Sensor.

- objects:

- application and data files structure as required by ACC 211

- operations:

- as defined in FDP_ACF.1.2/FIL.

Application Note 19: The current assignment shall cover tachograph application and data files structure as required by ACC_211.

FDP_ACC.1/FUN Subset access control {ACC_201}

Hierarchical to: -

Dependencies: FDP_ACF.1: is fulfilled by FDP_ACF.1/FUN.

FDP_ACC.1.1/FUN The TSF shall enforce the SFP FUNCTION on

- subjects:

- User.

- Unknown User.

- Motion Sensor.

- objects:

- Vehicle unit identification data (REQ075, REQ076)

- currently paired motion sensor identification data (REQ079, REQ 155)

- Driver card insertion and withdrawal data (REQ081)

- Driver activity data (REQ084)

- Places where daily work periods start / end (REQ087)

- Odometer data(REQ090)

- Detailed speed data (REQ093)

- Events data (REQ094, REQ095)

- Faults data (REQ096)

- calibration data (REQ097, REQ098)

- time adjustment data (REQ100, REQ101)

- Control activity data (REQ102, REQ103)

- Company locks data (REQ104)

- Download activity data (REQ105)

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

- Specific conditions data (REO105a)

- operations:

- as defined in FDP ACF.1.2/FUN.

Application Note 20: The current assignment shall cover subjects, objects, and operations as referred to in:

- operational modes {ACC_202} and the related restrictions on access rights {ACC_203},
- calibration functions {ACC_206} and time adjustment {ACC_208},
- limited manual entry {ACR_201a},
- Tachograph Card withdrawal {RLB_213}

as required by ACC_201.

FDP_ACC.1/DAT Subset access control {ACC_201}

Hierarchical to: -

Dependencies: FDP_ACF.1: is fulfilled by FDP_ACF.1/DAT

FDP_ACC.1.1/DAT The TSF shall enforce the SFP DATA on

- subjects:

- User.

- Motion Sensor.

- objects:

- VU identification data (REQ075, REQ076)

- MS identification data (REQ079, REQ 155)

- calibration data (REQ097, REQ098)

- time adjustment data (REQ100, REQ101)

- security data (REQ080)

- MS Audit Records {AUD 204}

- operations:

- as defined in FDP ACF.1.2/DAT

Application Note 21: The current assignment shall cover subjects, objects, and operations as referred to in:

- VU identification data: REQ075 (structure) {ACT_202} and REQ076 (once recorded) {ACC_204},
- MS identification data: REQ079 (Manufacturing-ID) and REQ155 (pairing) {ACC_205},
- Calibration Mode Data: REQ097 {ACC_207} and REQ100 {ACC_209},
- Security Data: REQ080 {ACC_210},
- MS Audit Records: {AUD_204}²⁸

as required by ACC_201.

²⁸ These data are generated not by the TOE, but by the Motion Sensor. Hence, they represent - from the point of view of the TOE - just a kind of data to be stored.

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

FDP_ACC.1/UDE Subset access control {ACT_201, ACT_203, ACT_204}; REQ 109 and 109a

Hierarchical to: -

Dependencies: FDP_ACF.1: is fulfilled by FDP_ACF.1/UDE

FDP_ACC.1.1/UDE The TSF shall enforce the SFP User Data Export on

- subjects:

- User.

- objects:

- Vehicles used data (REO197, REO217)

- Driver activity data (REO199, REO219)

- Places where daily work periods start / end (REO202, REO221)

- Events data (REO204, REO205, REO223)

- Faults data (REO207, REO208, REO223)

- Control activity data (REO210, REO225)

- Card session data (REO212)

- Specific conditions data (REO212a, REO230a)

- Calibration and time adjustment data (REO226, REO227)

- Control activity data (REO233)

- operations:

- as defined in FDP_ACF.1.2/UDE

Application Note 22: The current assignment shall cover subjects, objects, and operations as required by REQ 109 and 109a.

FDP_ACC.1/IS Subset access control {ACR_201, RLB_205}

Hierarchical to: -

Dependencies: FDP_ACF.1: is fulfilled by FDP_ACF.1/IS

FDP_ACC.1.1/IS The TSF shall enforce the SFP Input Sources on

- subjects:

- User.

- Motion Sensor.

- objects:

- Data stored on VU memory:

- Driver card insertion and withdrawal data (REO081)

- Driver activity data (REO084)

- Places where daily work periods start / end (REO087)

- Odometer data (REO090)

- Detailed speed data (REO093)

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

- Control activity data (REO102, REO103)
- Company locks data (REO104)
- Download activity data (REO105)
- Specific conditions data (REO105a)
- Data stored on Tachograph cards (REO109, REO109a)
- Vehicles used data (REO197, REO217)
- Driver activity data (REO199, REO219)
- Places daily work periods start/end(REO202, REO221)
- Events data (REO204, REO205, REO223)
- Faults data (REO207, REO208, REO223)
- Control activity data (REO210, REO225)
- Card session data (REO212)
- Specific conditions data (REO212a, REO230a)
- Calibration and time adjustment data (REO226, REO227)
- Control activity data (REO233)
- SW Upgrade patch

-operations:

- as defined in FDP_ACF.1.2/IS

Application Note 23: The current assignment shall cover subjects, objects, and operations as required by ACR_201 (right input sources) and RLB_205 (no external executable code).

FDP_ACC.1/SW-Upgrade Subset access control {ACC_201}

Hierarchical to:

-

Dependencies:

FDP_ACF.1: is fulfilled by FDP_ACF.1/SW-Upgrade

FDP_ACC.1.1/SW-Upgrade

The TSF shall enforce the SFP SW-Upgrade on updateable software components (Application Processor Software, Security Processor Software and RTC Processor Software) and User with identity WORKSHOP for upgrades in the Workshop.

7.1.5.2 FDP_ACF Access control functions

FDP_ACF.1/FIL Security attribute based access control {ACC_211}

Hierarchical to:

-

Dependencies:

FDP_ACC.1: is fulfilled by FDP_ACC.1/FIL

FMT_MSA.3: is fulfilled by FMT_MSA.3/FIL

FDP_ACF.1.1/FIL

The TSF shall enforce the File Structure SFP to objects based on the following:

- subjects:

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

- User.

- Motion Sensor.

- security attributes for subject:

- User:

- USER GROUP

— DRIVER (driver card)

— CONTROLLER (control card)

— WORKSHOP (workshop card)

— COMPANY (company card)

— UNKNOWN (no card inserted)

- USER ID, composed of:

— card issuing Member State code and of the card number

— UNKNOWN if user group is UNKNOWN

- Motion Sensor:

- serial number

- approval number

- objects:

- application and data files structure as required by ACC 211

- security attributes for objects:

- VU identification data (REO075)

- Security elements (REO080)

FDP_ACF.1.2/FIL The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: none.

FDP_ACF.1.3/FIL The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4/FIL The TSF shall explicitly deny access of subjects to objects based on the following additional rules as required by {ACC 211}.

Application Note 24: The current assignment in FDP_ACF.1.1 shall cover the entire files structure of the TOE-application as required by ACC_211.

FDP_ACF.1/FUN Security attribute based access control {ACC_202, ACC_203, ACC_206, ACC_208, ACR_201a, RLB_213}

Hierarchical to: -

Dependencies: FDP_ACC.1: is fulfilled by FDP_ACC.1/FUN
FMT_MSA.3: is fulfilled by FMT_MSA.3/FUN

FDP_ACF.1.1/FUN The TSF shall enforce the SFP FUNCTION to objects based on the following:

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

- subjects:

- User.

- Unknown User.

- Motion Sensor.

- security attributes for subject:

- User:

- USER GROUP

— DRIVER (driver card)

— CONTROLLER (control card)

— WORKSHOP (workshop card)

— COMPANY (company card)

— UNKNOWN (no card inserted)

- USER ID, composed of:

— card issuing Member State code and of the card number

— UNKNOWN if user group is UNKNOWN

- Motion Sensor:

- serial number

- approval number

- objects:

- Vehicle unit identification data (REQ075, REQ076)

- MS identification data (REQ079, REQ 155)

- Driver card insertion and withdrawal data (REQ081)

- Driver activity data (REQ084)

- Places where daily work periods start / end (REQ087)

- Odometer data(REQ090)

- Detailed speed data (REQ093)

- Events data (REQ094, REQ095)

- Faults data (REQ096)

- calibration data (REQ097, REQ098)

- time adjustment data (REQ100, REQ101)

- Control activity data (REQ102, REQ103)

- Company locks data (REQ104)

- Download activity data (REQ105)

- Specific conditions data (REQ105a)

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

- security attributes for objects: mode of operation (REO006, REO007, REO008) and the VU activation status.

FDP_ACF.1.2/FUN The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: rules in {ACC_202, ACC_203, ACC_206, ACC_208, ACR_201a, RLB_213}.

FDP_ACF.1.3/FUN The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4/FUN The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.

Application Note 25: The current assignment in FDP_ACF.1.1 shall cover subjects, objects, and their attributes as referred to in:

- operational modes {ACC_202} and the related restrictions on access rights {ACC_203},
- calibration functions {ACC_206} and time adjustment {ACC_208},
- limited manual entry {ACR_201a}, and
- Tachograph Card withdrawal {RLB_213}.

FDP_ACF.1/DAT Security attribute based access control {ACC_204, ACC_205, ACC_207, ACC_209, ACC_210, ACT_202, AUD_204}

Hierarchical to: -

Dependencies: FDP_ACC.1: is fulfilled by FDP_ACC.1/DAT
FMT_MSA.3: is fulfilled by FMT_MSA.3/DAT

FDP_ACF.1.1/DAT The TSF shall enforce the SFP DATA to objects based on the following:

- subjects:

- User.

- Motion Sensor.

- security attributes for subject:

- User:

- USER GROUP

— DRIVER (driver card)

— CONTROLLER (control card)

— WORKSHOP (workshop card)

— COMPANY (company card)

— UNKNOWN (no card inserted)

- USER ID. composed of:

— card issuing Member State code and of the card number

— UNKNOWN if user group is UNKNOWN

- Motion Sensor:

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

- serial number
- approval number
- objects:
 - VU identification data (REQ075, REQ076)
 - MS identification data (REQ079, REQ 155)
 - Calibration data (REQ097, REQ098)
 - Time adjustment data (REQ100, REQ101)
 - Security data (REQ080)
 - MS Audit Records {AUD 204}
- security attributes for objects:
 - VU identification data (REQ076)
 - MS identification data:
 - serial number
 - approval number
 - first pairing date
 - Calibration data: CALIBRATION mode of operation
 - Time adjustment data: CALIBRATION mode of operation
 - Security data (REQ080): Software upgrade keys SK SWU and PUB SWU are used to decrypt and verify the security data (REQ080) which is signed and encrypted before insertion into the VU during the manufacturing phase.
 - MS Audit Records: Audit records from MS is sent to the VU in an encrypted form with session key K_{SM} [I2]

FDP_ACF.1.2/DAT The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: the access rules as required by {ACC 204, ACC 205, ACC 207, ACC 209, ACC 210, ACT 202, AUD 204}.

FDP_ACF.1.3/DAT The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4/DAT The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.

Application Note 26: The current assignment shall cover subjects, objects, and their attributes as referred to in:

- VU identification data: REQ075 (structure) {ACT_202} and REQ076 (once recorded) {ACC_204},
- MS identification data: REQ079 (Manufacturing-ID) and REQ155 (pairing) {ACC_205},
- Calibration Mode Data: REQ097 {ACC_207} and REQ100 {ACC_209},
- Security Data: REQ080 {ACC_210},

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

- MS Audit Records: {AUD_204}²⁹.

FDP_ACF.1/UDE Security attribute based access control {ACT_201, ACT_203, ACT_204} (REQ109 and 109a)

Hierarchical to: -

Dependencies: FDP_ACC.1: is fulfilled by FDP_ACC.1/UDE
FMT_MSA.3: is fulfilled by FMT_MSA.3/UDE

FDP_ACF.1.1/UDE The TSF shall enforce the SFP User Data Export to objects based on the following:

- subjects:

- User.

- security attributes for subject:

- USER GROUP

- DRIVER

- CONTROLLER

- WORKSHOP

- USER ID, composed of:

- Member State code

- Card number.

- objects:

- Vehicles used data (REQ197, REQ217)

- Driver activity data (REQ199, REQ219)

- Places daily work periods start / end (REQ202, REQ221)

- Events data (REQ204, REQ205, REQ223)

- Faults data (REQ207, REQ208, REQ223)

- Control activity data (REQ210, REQ225)

- Card session data (REQ212)

- Specific conditions data (REQ212a, REQ230a)

- Calibration and time adjustment data (REQ226, REQ227)

- Control activity data (REQ233)

- security attributes for objects: Mutual authentication between the VU and the Tachograph card must have been performed (PRO SM / AUT) in order to satisfy the access condition required for the VU to update on the tachograph cards as described in TCS 400, TCS 405 and TCS 410.

²⁹ These data are generated not by the TOE, but by the Motion Sensor. Hence, they represent - from the point of view of the TOE - just a kind of data to be stored.

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

- FDP_ACF.1.2/UDE The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: rules in REQ109 and 109a.
- FDP_ACF.1.3/UDE The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
- FDP_ACF.1.4/UDE The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.

Application Note 27: The current assignment shall cover subjects, objects, and as their attributes required by REQ 109 and 109a.

FDP_ACF.1/IS Security attribute based access control {ACR_201, RLB_205}

Hierarchical to: -

Dependencies: FDP_ACC.1: is fulfilled by FDP_ACC.1/IS
FMT_MSA.3: is fulfilled by FMT_MSA.3/IS

FDP_ACF.1.1/IS The TSF shall enforce the SFP Input Sources to objects based on the following:

- subjects:

- User.

- Motion Sensor.

- security attributes for subject:

- User:

- USER GROUP

— DRIVER (driver card)

— CONTROLLER (control card)

— WORKSHOP (workshop card)

— COMPANY (company card)

— UNKNOWN (no card inserted)

- USER ID, composed of:

— card issuing Member State code and of the card number

— UNKNOWN if user group is UNKNOWN

- Motion Sensor:

- serial number

- approval number

- objects:

- Data stored on VU memory:

- Driver card insertion and withdrawal data (REQ081)

- Driver activity data (REQ084)

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

- Places where daily work periods start / end (REO087)
- Odometer data(REO090)
- Detailed speed data (REO093)
- Control activity data (REO102, REO103)
- Company locks data (REO104)
- Download activity data (REO105)
- Specific conditions data (REO105a)
- Data stored on Tachograph cards (REO109, REO109a)
 - Vehicles used data (REO197, REO217)
 - Driver activity data (REO199, REO219)
 - Places daily work periods start/end(REO202, REO221)
 - Events data (REO204, REO205, REO223)
 - Faults data (REO207, REO208, REO223)
 - Control activity data (REO210, REO225)
 - Card session data (REO212)
 - Specific conditions data (REO212a, REO230a)
 - Calibration and time adjustment data (REO226, REO227)
 - Control activity data (REO233)
- SW Upgrade patch
- security attributes for objects:
 - Data stored on VU memory: mode of operation
 - vehicle motion data : pulse counter value.
 - recording equipment calibration parameters:
 - CALIBRATION mode of operation
 - user's inputs : time of events entered manually
 - Data stored on Tachograph cards:
 - Mutual authentication between the VU and the Tachograph card must have been performed (PRO SM / AUT) in order to satisfy the access condition required for the VU to update on the tachograph cards as described in TCS 400, TCS 405 and TCS 410.
- SW Upgrade patch:
 - CALIBRATION mode of operation
 - Software upgrade keys PUB SWU and SK SWU

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

FDP_ACF.1.2/IS	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: <u>rules in {ACR_201³⁰}</u> .
FDP_ACF.1.3/IS	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: <u>none</u> .
FDP_ACF.1.4/IS	The TSF shall explicitly deny access of subjects to objects based on the following additional rules <u>as required by {RLB_205}</u> .

Application Note 28: The current assignment shall cover subjects, objects, and their attributes as required by ACR_201 (right input sources) and RLB_205 (no external executable code).

FDP_ACF.1/SW-Upgrade Security attribute based access control {RLB_205}

Hierarchical to:	-
Dependencies:	FDP_ACC.1: is fulfilled by FDP_ACC.1/SW-Upgrade FMT_MSA.3: is fulfilled by FMT_MSA.3/SW-Upgrade
FDP_ACF.1.1/SW-Upgrade	The TSF shall enforce SFP SW-Upgrade to objects based on the following: updateable software components (Application Processor software, Security Processor software and RTP Processor software) may be exchanged if the confidentiality, integrity and the authenticity of the patch data is confirmed with help of the update credentials.
FDP_ACF.1.2/SW-Upgrade	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: - software upgrade at the workshop is only possible after workshop card authentication, - software upgrade is only possible if the confidentiality, integrity and the authenticity of the patch data is confirmed with help of the update credentials.
FDP_ACF.1.3/SW-Upgrade	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/SW-Upgrade	The TSF shall explicitly deny access of subjects to objects based on the following additional rule: none.

7.1.5.3 FDP_ETC Export from the TOE

FDP_ETC.2 Export of user data with security attributes {ACT_201, ACT_203, ACT_204, ACT_207, AUD_201, DEX_205, DEX_208} (REQ109 and 109a)

Hierarchical to:	-
Dependencies:	[FDP_ACC.1 or FDP_IFC.1]: is fulfilled by FDP_ACC.1/UDE
FDP_ETC.2.1	The TSF shall enforce the <u>SFP User Data Export</u> when exporting user data, controlled under the SFP(s), outside of the TOE.

³⁰ Especially for MS and TC

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

- FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.
- FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
- FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: REQ110, DEX_205, DEX_208.

7.1.5.4 FDP_ITC Import from outside of the TOE

FDP_ITC.1 Import of user data without security attributes {ACR_201}

Hierarchical to: -

Dependencies: [FDP_ACC.1 or FDP_IFC.1]: is fulfilled by FDP_ACC.1/IS
FMT_MSA.3: is fulfilled by FMT_MSA.3/IS

FDP_ITC.1.1 The TSF shall enforce the SFP Input Sources when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: as required by {ACR_201} for recording equipment calibration parameters and user's inputs.
Moreover, GNSS data shall only be processed from the right input sources.

FDP_ITC.2//IS Import of user data with security attributes {ACR_201, RLB_205, DEX_201, DEX_202, DEX_203, DEX_204}

Hierarchical to: -

Dependencies: [FDP_ACC.1 or FDP_IFC.1]: is fulfilled by FDP_ACC.1/IS
[FTP_ITC.1 or FTP_TRP.1]: not fulfilled, but **justified**:
Indeed, trusted channels VU<->MS and VU<->TC will be established. Since the component FTP_ITC.1 represents just a higher abstraction level integrative description of this property and does not define any additional properties comparing to {FDP_ITC.2//IS + FDP_ETC.2 + FIA_UAU.1/TC (and /MS)}, it can be dispensed with this dependency in the current context of the PP.

FPT_TDC.1: is fulfilled by FPT_TDC.1//IS

FDP_ITC.2.1//IS The TSF shall enforce the SFP Input Sources when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2//IS The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3//IS The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

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

FDP_ITC.2.4//IS The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5//IS The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE as required by:

- [12] for the Motion Sensor {ACR_201, DEX_201},
- DEX_202 (audit record and continue to use imported data),
- [10] for the Tachograph Cards {ACR_201, DEX_203},
- DEX_204 (audit record and not using of the data),
- RLB_205 (no executable code from external sources).

FDP_ITC.2//SW-Upgrade Import of user data with security attributes {RLB_205}

Hierarchical to: -

Dependencies: **[FDP_ACC.1 or FDP_IFC.1]: is fulfilled by FDP_ACC.1/SW-Upgrade [FTP_ITC.1 or FTP_TRP.1]: not fulfilled, but justified:**

The new TOE software to replace the current TOE software, the new TOE software is accepted by the TOE only together with the corresponding credentials, which contain all information needed for verification. That is, the TOE needs first to decrypt and then verify the signature on the new TOE software before allowing it to replace the current TOE software. So, it is not necessary to establish trusted channel or trusted path.

FPT_TDC.1: is fulfilled by FPT_TDC.1//SW-Upgrade

FDP_ITC.2.1//SW-Upgrade The TSF shall enforce the SFP SW-Upgrade when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2//SW-Upgrade The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3//SW-Upgrade The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4//SW-Upgrade The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5//SW-Upgrade The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: update of the TOE software is allowed only if the integrity and the authenticity of the new TOE software patch is confirmed with the help of the update credentials.

7.1.5.5 FDP_RIP Residual information protection

FDP_RIP.1 Subset residual information protection {REU_201}

Hierarchical to: -

Dependencies: -

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

FDP_RIP.1.1

The TSF shall ensure that any previous information content of a **temporarily stored** resource is made unavailable upon the *deallocation of the resource* from the following objects:

- a) K_{wc}: workshop card part of the motion sensor master key (at most by the end of the calibration phase);
- b) K_m: motion sensor master key (at most by the end of the calibration phase);
- c) K_{ID}: motion sensor identification key (at most by the end of the calibration phase);
- d) K_p: motion sensor pairing key (at most by the end of the calibration phase);
- e) K_{SM}: session key between motion sensor and vehicle unit (when its temporarily stored value shall not be used any more);
- f) K_{ST}: session key between tachograph cards and vehicle unit (by closing a card communication session);
- g) EQT_j.SK: equipment private key (when its temporarily stored value shall not be used any more);
- h) K_{m_{vu}}: VU part of the motion sensor master key (when its temporarily stored value shall not be used any more);
- i) PIN: the verification value of the workshop card PIN temporarily stored in the TOE during its calibration (at most by the end of the calibration phase);
- j) Software upgrade keys – PUB SWU and SK SWU (at most by the end of the software update);
- k) Secure boot keys – PUB BOOT and PRIV BOOT (at most by the end of secure boot);
- l) SK AP: session key between AP and SP (when its temporarily stored value shall not be used anymore);
- m) SK RTP: session key between AP and RTP (when its temporarily stored value shall not be used anymore);
- n) SK DATA: data storage key (when its temporarily stored value shall not be used any more);
- o) SK HMAC: user data integrity key used for HMAC of stored data in data memory.

Application Note 29: The component FDP_RIP.1 concerns in this ST only the temporarily stored (e.g. in RAM) instantiations of objects in question. In contrast, the component FCS_CKM.4 relates to any instantiation of cryptographic keys independent of whether it is of temporary or permanent nature. Making the permanently stored instantiations of EQT_j.SK and of the part of the Master key K_{m_{vu}} unavailable at decommissioning the TOE is a matter of the related organizational policy.

Application Note 30: The functional family FDP_RIP possesses such a general character, so that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMSEC. Applied to cryptographic keys, FDP_RIP.1 requires a certain quality metric ('any previous information content of a resource is made unavailable') for key's destruction in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard.

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

7.1.5.6 FDP_SDI Stored data integrity

FDP_SDI.2 Stored data integrity {ACR_204, ACR_205}

Hierarchical to: -

Dependencies: -

FDP_SDI.2.1 The TSF shall monitor user data stored in **the TOE's data memory containers controlled by the TSF for integrity errors on all objects, based on the following attributes: [assignment: user data attributes].**

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall generate an audit record.

Application Note 31: The context for the current SFR is built by the related requirements ACR_204, ACR_205 (sec. 4.6.3 of [9] 'Stored data integrity'). This context gives a clue for interpretation that it is not a matter of temporarily, but of permanently stored user data (see definition in glossary).

7.1.6 Class FIA Identification and Authentication.

7.1.6.1 FIA_AFL Authentication failures

FIA_AFL.1/MS Authentication failure handling {UIA_206}

Hierarchical to: -

Dependencies: FIA_UAU.1: is fulfilled by FIA_UAU.2/MS

FIA_AFL.1.1/MS The TSF shall detect when 2 unsuccessful authentication attempts occur related to motion sensor authentication.

FIA_AFL.1.2/MS When the defined number of unsuccessful authentication attempts has been surpassed, the TSF shall

- generate an audit record of the event,
- warn the user,
- continue to accept and use non secured motion data sent by the motion sensor.

Application Note 32: The positive integer number expected above shall be ≤ 20 , cf. UIA_206 in [7].

FIA_AFL.1/TC Authentication failure handling {UIA_214}


Hierarchical to: -

Dependencies: FIA_UAU.1: is fulfilled by FIA_UAU.1/TC

FIA_AFL.1.1/TC The TSF shall detect when 5 unsuccessful authentication attempts occur related to tachograph card authentication.

FIA_AFL.1.2/TC When the defined number of unsuccessful authentication attempts has been surpassed, the TSF shall

- generate an audit record of the event,
- warn the user,

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

- assume the user as Unknown User and the card as non valid (is commensurate with 'Unknown equipment' in the current ST) (definition (z) and REQ007).

FIA_AFL.1/Remote: Remote TC Authentication failure handling {UIA_220}

Hierarchical to: -

Dependencies: **FIA_UAU.1: is fulfilled by FIA_UAU.1/TC**

FIA_AFL.1.1/Remote **The TSF shall detect when 5 unsuccessful authentication attempts occur related to tachograph card authentication.**

FIA_AFL.1.2/Remote **When the defined number of unsuccessful authentication attempts has been surpassed, the TSF shall**
- warn the remotely connected company.

7.1.6.2 FIA_ATD User attribute definition

FIA_ATD.1//TC User attribute definition {UIA_208, UIA_216}

Hierarchical to: -

Dependencies: -

FIA_ATD.1.1//TC The TSF shall maintain the following list of security attributes belonging to individual users: as defined in {UIA_208, UIA_216}.

7.1.6.3 FIA_UAU User authentication

FIA_UAU.1/TC Timing of authentication {UIA_209, UIA_217}

Hierarchical to: -

Dependencies: FIA_UID.1: is fulfilled by FIA_UID.2/TC

FIA_UAU.1.1/TC The TSF shall allow (i) TC identification as required by FIA_UID.2.1/TC and (ii) reading out audit records as required by FAU_SAR.1 on behalf of the user to be performed before the user is authenticated³¹.

FIA_UAU.1.2/TC The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1/PIN Timing of authentication {UIA_212}

Hierarchical to: -

Dependencies: FIA_UID.1: is fulfilled by FIA_UID.2/TC³²

FIA_UAU.1.1/PIN The TSF shall allow (i) TC (Workshop Card) identification as required by FIA_UID.2.1/TC and (ii) reading out audit records as required by

³¹ According to CSM_20 in [10] the TC identification (certificate exchange) is to perform strictly before the mutual authentication between the VU and the TC.

³² The PIN-based authentication is applicable for the workshop cards, whose identification is ruled by FIA_UID.2/TC.ş

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

FAU_SAR.1 on behalf of the user to be performed before the user is authenticated³³.

FIA_UAU.1.2/PIN The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1/MD Timing of authentication {UIA_222}

Hierarchical to: -

Dependencies: **FIA_UID.1: is fulfilled by FIA_UID.2/MD**

FIA_UAU.1.1/MD **The TSF shall allow MD identification as required by FIA_UID.2.1/MD on behalf of the user to be performed before the user is authenticated.**

FIA_UAU.1.2/MD **The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.**

FIA_UAU.2//MS User authentication before any action {UIA_203}³⁴.

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1: is fulfilled by FIA_UID.2/MS

FIA_UAU.2.1//MS The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.3/MS Unforgeable authentication {UIA_205}.

Hierarchical to: -

Dependencies: -

FIA_UAU.3.1/MS The TSF shall detect and prevent use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2/MS The TSF shall detect and prevent use of authentication data that has been copied from any other user of the TSF.

FIA_UAU.3/TC Unforgeable authentication {UIA_213, UIA_219}.

Hierarchical to: -

Dependencies: -

FIA_UAU.3.1/TC The TSF shall detect and prevent use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2/TC The TSF shall detect and prevent use of authentication data that has been copied from any other user of the TSF.

FIA_UAU.3/MD Unforgeable authentication {UIA_223}

³³ According to CSM_20 in [10] the TC identification (certificate exchange) is to perform strictly before the PIN authentication of the Workshop Card.

³⁴ Though MS identification happens before the MS authentication, they will be done within same command (80 or 11); hence, it is also plausible to choose here the functional component FIA_UAU.2.

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

Hierarchical to: -

Dependencies: -

FIA_UAU.3.1/MD **The TSF shall detect and prevent use of authentication data that has been forged by any user of the TSF.**

FIA_UAU.3.2/MD **The TSF shall detect and prevent use of authentication data that has been copied from any other user of the TSF.**

FIA_UAU.5//TC Multiple authentication mechanisms {UIA_211, UIA_218}.

Hierarchical to: -

Dependencies: -

FIA_UAU.5.1//TC The TSF shall provide multiple authentication mechanisms according to CSM_20 in [8] to support user authentication.

FIA_UAU.5.2//TC The TSF shall authenticate any user's claimed identity according to the CSM_20 in [8].

FIA_UAU.6/MS Re-authenticating {UIA_204}.

Hierarchical to: -

Dependencies: -

FIA_UAU.6.1/MS The TSF shall re-authenticate the user under the conditions every 10 seconds.

Application Note 37: The condition under which re-authentication is required expected above shall be more frequently than once per hour, cf. UIA_204 in [7].

FIA_UAU.6/TC Re-authenticating {UIA_210}.

Hierarchical to: -

Dependencies: -

FIA_UAU.6.1/TC The TSF shall re-authenticate the user under the conditions:

- after power supply recovery.
- periodically with a period of 12 hours.
- when session counter is expired (the maximum number is 240).
- when the inserted tachograph card returns an error code.
- If re-authentication is not performed in any cases listed above, a flag is set indicating a pending re-authentication. The pending re-authentication is performed in 10 minutes, after the flag is set. In case of tachograph card data needs to be updated while the flag is set, re-authentication is performed immediately before the update.

Application Note 38: The condition under which re-authentication is required expected above shall be more frequently than once per day, cf. UIA_210 in [7].

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

7.1.6.4 FIA_UID user identification

FIA_UID.2/MS User identification before any action {UIA_201}

Hierarchical to: FIA_UID.1

Dependencies: -

FIA_UID.2.1/MS The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2/TC User identification before any action {UIA_207, **UIA_215**}

Hierarchical to: FIA_UID.1

Dependencies: -

FIA_UID.2.1/TC The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2/MD User identification before any action {UIA_221}

Hierarchical to: FIA_UID.1

Dependencies: -

FIA_UID.2.1/MD The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

7.1.7 Class FPR Privacy

7.1.7.1 FPR_UNO Unobservability

FPR_UNO.1 Unobservability {RLB_204 for leaked data}

Hierarchical to: -

Dependencies: -

FPR_UNO.1.1 The TSF shall ensure that all users are unable to observe the **cryptographic** operations as required by FCS COP.1/TDES and FCS COP.1/RSA, FCS COP.1/ECDSA, FCS COP.1/AES, on cryptographic keys being to keep secret (as listed in FCS CKM.3 excepting EUR.PK, PUB_SW, PUB_BOOT) by the TSF ~~{assignment: list of protected users and/or subjects}~~.

Application Note 40: ‘To observe the cryptographic operations’ means here ‘using any TOE external interface in order to gain the values of cryptographic keys being to keep secret’.

7.1.8 Class FPT Protection of the TSF

7.1.8.1 FPT_FLS Fail secure

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: -

Dependencies: -

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: as specified in {RLB_203, RLB_210, RLB_211}.

Aselsan STC-8255 v1.0 Digital Tachograph Vehicle Unit Security Target Lite**7.1.8.2 FPT_PHP TSF physical protection**

FPT_PHP.2//Power_Deviation Notification of physical attack {RLB_209}

Hierarchical to: FPT_PHP.1

Dependencies: FMT_MOF.1: not fulfilled, but **justified**:

It is a matter of RLB_209: this function (detection of deviation) must not be deactivated by anybody. But FMT_MOF.1 is formulated in a not applicable way for RLB_209.

FPT_PHP.2.1//Power_Deviation The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.2.2//Power_Deviation The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3//Power_Deviation For the devices/elements for which active detection is required in {RLB_209}, the TSF shall monitor the devices and elements and notify the user and audit record generation when physical tampering with the TSF's devices or TSF's elements has occurred.**FPT_PHP.2//HW_sabotage Notification of physical attack {RLB_207, RLB_208}****Hierarchical to: FPT_PHP.1****Dependencies: FMT_MOF.1: not fulfilled, but justified:**

It is a matter of RLB_207 and RLB_208: this function (detection of removal of the smart card placed in any slot outside the control of the TOE) must not be deactivated by anybody. But FMT_MOF.1 is formulated in a not applicable way for RLB_207 and RLB_208.

FPT_PHP.2.1//HW_sabotage The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.2.2//HW_sabotage The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3// HW_sabotage **For the smart card interfaces of the TOE, the TSF shall monitor the devices and elements and notify any user except WORKSHOP and audit record generation when physical tampering, by removal of the smart card placed in any slot outside the control of the TOE, with the TSF's devices or TSF's elements has occurred.****FPT_PHP.3 Resistance to physical attack {RLB_204 for stored data, RLB_206}**

Hierarchical to: -

Dependencies: -

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

FPT_PHP.3.1 The TSF shall resist physical tampering attacks to the TOE security enforcing part of the software in the field after the TOE activation by responding automatically such that the SFRs are always enforced.

7.1.8.3 FPT_STM time stamps

FPT_STM.1 Reliable time stamps {ACR_201}

Hierarchical to: -

Dependencies: -

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application Note 41: This requirement is the matter of the VU's real time clock. According to ACC_208 and REQ157 small time adjustments are allowed and therefore, are out of the scope of this requirement.

7.1.8.4 FPT_TDC Inter-TSF TSF Data Consistency

FPT_TDC.1//IS Inter-TSF basic TSF data consistency {ACR_201}

Hierarchical to: -

Dependencies: -

FPT_TDC.1.1//IS The TSF shall provide the capability to consistently interpret secure messaging attributes as defined by [10] for the Motion Sensor and by [8] for the Tachograph Cards when shared between the TSF and another trusted IT product.

FPT_TDC.1.2//IS The TSF shall use the interpretation rules (communication protocols) as defined by [10] for the Motion Sensor and by [8] for the Tachograph Cards when interpreting the TSF data from another trusted IT product.

FPT_TDC.1//SW-Upgrade Inter-TSF basic TSF data consistency {RLB_205}

Hierarchical to: -

Dependencies: -

FPT_TDC.1.1//SW-Upgrade The TSF shall provide the capability to consistently interpret SW upgrade patch data and update credentials when shared between the TSF and another trusted IT product.

FPT_TDC.1.2//SW-Upgrade The TSF shall use the credentials which belong to software component and particular VU when interpreting the TSF data from another trusted IT product.

7.1.8.5 FPT_TST TSF self test

FPT_TST.1 TSF testing {RLB_202}

Hierarchical to: -

Dependencies: -

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

- FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up, periodically during normal operation to demonstrate **the integrity of security data and the integrity of stored executable code (if not in ROM)** ~~the correct operation of [selection: [assignment: parts of TSF], the TSF].~~
- FPT_TST.1.2 The TSF shall ~~provide authorised users with the capability to~~ verify the integrity of security data.
- FPT_TST.1.3 The TSF shall ~~provide authorised users with the capability to~~ verify the integrity of stored TSF executable code.

7.1.9 Class FRU Resource Utilisation

7.1.9.1 FRU_PRS Priority of service

FRU_PRS.1 Limited priority of service {RLB_212}

Hierarchical to: -

Dependencies: -

FRU_PRS.1.1 The TSF shall assign a priority to each subject in the TSF.

FRU_PRS.1.2 The TSF shall ensure that each access to functions and data covered by the current set of SFRs shall be mediated on the basis of the subjects assigned priority.

Application Note 42: The current assignment is to consider in the context of RLB_212 (sec. 4.7.6 of [7] ‘Data availability’). Controlled resources in this context may be ‘functions and data covered by the current set of SFRs’.

7.1.10 Class FMT Security Management

7.1.10.1 FMT_MSA Management of security attributes

FMT_MSA.1 Management of security attributes {UIA_208}

Hierarchical to: -

Dependencies: [FDP_ACC.1 or FDP_IFC.1]: is fulfilled by FDP_ACC.1/FUN

FMT_SMR.1: is fulfilled by FMT_SMR.1//TC

FMT_SMF.1: is fulfilled by FMT_SMF.1

FMT_MSA.1.1 The TSF shall enforce the SFP FUNCTION to restrict the ability to change default the security attributes User Group, User ID³⁵ to nobody.

FMT_MSA.3/FUN Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: is fulfilled by FMT_MSA.1

FMT_SMR.1: is fulfilled by FMT_SMR.1//TC

³⁵ see the definition of the role “User” in Table 3 above

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

FMT_MSA.3.1/FUN The TSF shall enforce the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/FUN The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/FIL Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: is fulfilled by FMT_MSA.1
FMT_SMR.1: is fulfilled by FMT_SMR.1//TC

FMT_MSA.3.1/FIL The TSF shall enforce the File Structure SFP to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/FIL The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/DAT Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: is fulfilled by FMT_MSA.1
FMT_SMR.1: is fulfilled by FMT_SMR.1//TC

FMT_MSA.3.1/DAT The TSF shall enforce the SFP DATA to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/DAT The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/UDE Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: is fulfilled by FMT_MSA.1
FMT_SMR.1: is fulfilled by FMT_SMR.1//TC

FMT_MSA.3.1/UDE The TSF shall enforce the SFP User Data Export to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/UDE The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/IS Static attribute initialisation

Hierarchical to: -

Dependencies: FMT_MSA.1: is fulfilled by FMT_MSA.1
FMT_SMR.1: is fulfilled by FMT_SMR.1//TC

FMT_MSA.3.1/IS The TSF shall enforce the SFP Input Sources to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/IS The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.

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

FMT_MSA.3/SW-Upgrade Static attribute initialization

Hierarchical to: -

Dependencies: **FMT_MSA.1: is fulfilled by FMT_MSA.1**
 FMT_SMR.1: is fulfilled by FMT_SMR.1//TC

FMT_MSA.3.1/SW-Upgrade **The TSF shall enforce the SFP SW-Upgrade to provide restrictive default values for security attributes that are used to enforce the SFP.**

FMT_MSA.3.2/SW-Upgrade **The TSF shall allow nobody to specify alternative initial values to override the default values when an object or information is created.**

7.1.10.2 FMT_MOF Management of functions in TSF

FMT_MOF.1 Management of security functions behaviour {RLB_201}

Hierarchical to: -

Dependencies: FMT_SMR.1: is fulfilled by FMT_SMR.1//TC
 FMT_SMF.1: is fulfilled by FMT_SMF.1

FMT_MOF.1.1 The TSF shall restrict the ability to enable the functions specified in {RLB_201} to nobody.

7.1.10.3 FMT_SMF Specification of Management Functions

FMT_SMF.1 Specification of Management Functions {UIA_208}

Hierarchical to: -

Dependencies: -

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: all operations being allowed only in the calibration mode as specified in REQ010.

7.1.10.4 FMT_SMR Security management roles

FMT_SMR.1//TC Security roles {UIA_208}

Hierarchical to: -

Dependencies: FIA_UID.1: is fulfilled by FIA_UID.2//TC

FMT_SMR.1.1//TC The TSF shall maintain the roles as defined in {UIA_208} as User Groups:

- DRIVER (driver card),
- CONTROLLER (control card),
- WORKSHOP (workshop card),
- COMPANY (company card),
- UNKNOWN (no card inserted),
- Motion Sensor,
- Unknown equipment.

FMT_SMR.1.2//TC The TSF shall be able to associate users with roles.

7.2 Security Assurance Requirements

The security assurance requirements for the TOE are as derived in the PP [11], which are the requirements for the Evaluation Assurance Level 4 augmented with ATE_DPT.2 and AVA_VAN.5. The security assurance requirements are listed in the table below.

Table 8: Security assurance requirements

Assurance Classes	Assurance Components
ADV: 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
AGD: Guidance Documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DVS.1 Identification of security measures
	ALC_TAT.1 Well-defined development tools
	ALC_DEL.1 Delivery procedures
	ALC_LCD.1 Developer defined life-cycle model
ASE: Security Target Evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.2 Testing: security enforcing modules
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability Assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

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

7.3 Security Requirements Rationale

7.3.1 Security Functional Requirements Rationale

The following table provides an overview for security functional requirements coverage also giving an evidence for sufficiency and necessity of the SFRs chosen.

Table 9: Coverage of security objectives for the TOE by SFR

		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	O.Software_Analysis	O.Software_Upgrade
FAU_GEN.1	Audit data generation		X	X								
FAU_SAR.1	Audit review		X	X								
FAU_STG.1	Protected audit trail storage		X	X		X						
FAU_STG.4	Prevention of audit data loss		X	X								
FCO_NRO.1	Selective proof of origin						X			X		
FCS_CKM.1/TDES	Cryptographic key generation									X		
FCS_CKM.1/AES	Cryptographic key generation											X
FCS_CKM.2	Cryptographic key distribution									X		
FCS_CKM.3	Cryptographic key access									X		X
FCS_CKM.4	Cryptographic key destruction									X		X
FCS_COP.1/TDES	Cryptographic operation									X		
FCS_COP.1/RSA	Cryptographic operation									X		
FCS_COP.1/AES	Cryptographic operation											X
FCS_COP.1/ECDSA	Cryptographic operation											X
FCS_COP.1/HMAC	Cryptographic operation					X						
FDP_ACC.1/FIL	Subset access control	X										
FDP_ACC.1/FUN	Subset access control	X						X	X	X	X	
FDP_ACC.1/DAT	Subset access control	X										
FDP_ACC.1/UDE	Subset access control	X										
FDP_ACC.1/IS	Subset access control	X						X	X			
FDP_ACC.1/SW-Upgrade	Subset access control											X
FDP_ACF.1/FIL	Security attribute based access control	X										
FDP_ACF.1/FUN	Security attribute based access control	X						X	X	X	X	
FDP_ACF.1/DAT	Security attribute based access control	X										
FDP_ACF.1/UDE	Security attribute based access control	X										

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

		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	O.Software_Analysis	O.Software_Upgrade
FDP_ACF.1/IS	Security attribute based access control	X						X	X			
FDP_ACF.1/SW-Upgrade	Security attribute based access control											X
FDP_ETC.2	Export of user data with security attributes		X			X	X			X		
FDP_ITC.1	Import of user data without security attributes							X	X			
FDP_ITC.2//IS	Import of user data with security attributes							X	X	X		
FDP_ITC.2//SW-Upgrade	Import of user data with security attributes											X
FDP_RIP.1	Subset residual information protection	X						X	X			
FDP_SDI.2	Stored data integrity monitoring and action			X		X	X		X			
FIA_AFL.1/MS	Authentication failure handling			X	X				X			
FIA_AFL.1/TC	Authentication failure handling			X	X				X			
FIA_AFL.1/Remote	Authentication failure handling			X	X							
FIA_ATD.1//TC	User attribute definition			X						X		
FIA_UAU.1/TC	Timing of authentication				X					X		
FIA_UAU.1/PIN	Timing of authentication				X							
FIA_UAU.1/MD	Timing of authentication				X							
FIA_UAU.2//MS	User authentication before any action				X					X		
FIA_UAU.3/MS	Unforgeable authentication				X							
FIA_UAU.3/TC	Unforgeable authentication				X							
FIA_UAU.3/MD	Unforgeable authentication				X							
FIA_UAU.5//TC	Multiple authentication mechanisms	X			X					X		
FIA_UAU.6/MS	Re-authenticating				X					X		
FIA_UAU.6/TC	Re-authenticating				X					X		
FIA_UID.2/MS	User identification before any action	X	X	X	X					X		
FIA_UID.2/TC	User identification before any action	X	X	X	X					X		

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

		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	O.Software_Analysis	O.Software_Upgrade
FIA_UID.2/MD	User identification before any action	X	X	X	X							
FMT_MSA.1	Management of security attributes	X								X		
FMT_MSA.3/FUN	Static attribute initialization	X						X	X	X	X	
FMT_MSA.3/FIL	Static attribute initialization	X										
FMT_MSA.3/DAT	Static attribute initialization	X										
FMT_MSA.3/IS	Static attribute initialization	X						X	X			
FMT_MSA.3/UDE	Static attribute initialization	X										
FMT_MSA.3/SW-Upgrade	Static attribute initialization											X
FMT_MOF.1	Management of security functions	X							X			
FMT_SMF.1	Specification of Management Functions	X								X		
FMT_SMR.1//TC	Security roles	X								X		
FPR_UNO.1	Unobservability						X	X	X		X	
FPT_FLS.1	Failure with preservation of secure state.			X					X			
FPT_PHP.2//Power_Deviation	Notification of physical attack								X			
FPT_PHP.2//HW_sabotage	Notification of physical attack								X			
FPT_PHP.3	Resistance to physical attack						X	X	X		X	
FPT_STM.1	Reliable time stamps		X	X				X	X			
FPT_TDC.1//IS	Inter-TSF basic TSF data consistency							X	X			
FPT_TDC.1//SW-Upgrade	Inter-TSF basic TSF data consistency											X
FPT_TST.1	TSF testing			X					X			
FRU_PRS.1	Limited priority of service								X			

Note: FCS_CKM.1/TDES corresponds to FCS_CKM.1 in the protection profile [11].

A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given in the table below.

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

Table 10: Suitability of the SFRs

Security Objectives	Security Functional Requirements
O.Access	<p>FDP_ACC.1/FIL File structure SFP on application and data files structure</p> <p>FDP_ACC.1/FUN SFP FUNCTION on the functions of the TOE</p> <p>FDP_ACC.1/DAT SFP DATA on user data of the TOE</p> <p>FDP_ACC.1/UDE SFP User_Data_Export for the export of user data</p> <p>FDP_ACC.1/IS SFP Input Sources to ensure the right input sources</p> <p>FDP_ACC.1/SW-Upgrade SFP SW-Upgrade for the upgrade of the software in the TOE</p> <p>FDP_ACF.1/FIL Entire files structure of the TOE-application</p> <p>FDP_ACF.1/FUN Defines security attributes for SFP FUNCTION according to the modes of operation</p> <p>FDP_ACF.1/DAT Defines security attributes for SFP DATA on user</p> <p>FDP_ACF.1/UDE Defines security attributes for SFP User_Data_Export</p> <p>FDP_ACF.1/IS Defines security attributes for SFP Input Sources</p> <p>FDP_ACF.1/SW-Upgrade Defines security attributes for SFP SW-Upgrade</p> <p>FDP_RIP.1 Any previous information content of a resource is made unavailable upon allocation or deallocation of resource</p> <p>FIA_UAU.5//TC Multiple authentication mechanisms according to CSM_20 in [8] to support user authentication.</p> <p>FIA_UID.2/MS A motion sensor is successfully identified before allowing any other action</p> <p>FIA_UID.2/TC A tachograph card is successfully identified before allowing any other action</p> <p>FIA_UID.2/MD A management device is successfully identified before allowing any other action</p> <p>FMT_MSA.1 Provides the SFP FUNCTION to restrict the ability to change_default the security attributes User Group, User ID to nobody.</p> <p>FMT_MSA.3/FUN Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p>FMT_MSA.3/FIL Provides the File_Structure SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p>FMT_MSA.3/DAT Provides the SFP DATA to provide restrictive default values for security attributes that are used to enforce the SFP and</p>

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

Security Objectives	Security Functional Requirements
	<p>allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p>FMT_MSA.3/IS Provides the SFP Input_Sources to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p>FMT_MSA.3/UDE Provides the SFP User Data Export to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p>FMT_MSA.3/SW-Upgrade Provides the SFP SW-Upgrade to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p>FMT_MOF.1 Restricts the ability to enable the test functions as specified in {RLB_201} to nobody and, thus, prevents an unintended access to data in the operational phase.</p> <p>FMT_SMF.1 Performing all operations being allowed only in the calibration mode.</p> <p>FMT_SMR.1//TC Maintain the roles as defined in {UIA_208} as User Groups.</p>
O.Accountability	<p>FAU_GEN.1 Generates correct audit records</p> <p>FAU_SAR.1 Allows users to read accountability audit records</p> <p>FAU_STG.1 Protect the stored audit records from unauthorised deletion</p> <p>FAU_STG.4 Prevent loss of audit data loss (overwrite the oldest stored audit records and behave according to REQ 105b if the audit trail is full.)</p> <p>FDP_ETC.2 Provides export of user data with security attributes using the SFP User_Data_Export</p> <p>FIA_UID.2/MS A motion sensor is successfully identified before allowing any other action</p> <p>FIA_UID.2/TC A tachograph card is successfully identified before allowing any other action</p> <p>FIA_UID.2/MD A management device is successfully identified before allowing any other action</p> <p>FPT_STM.1 Provides accurate time</p>
O.Audit	<p>FAU_GEN.1 Generates correct audit records</p> <p>FAU_SAR.1 Allows users to read accountability audit records</p> <p>FAU_STG.1 Protect the stored audit records from unauthorized deletion.</p> <p>FAU_STG.4 Prevent loss of audit data loss (overwrite the oldest stored audit records and behave according to REQ 105b if the audit trail is full.)</p>

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

Security Objectives	Security Functional Requirements
	<p>FDP_SDI.2 monitors user data stored for integrity error</p> <p>FIA_AFL.1/MS Detects and records authentication failure events for the motion sensor</p> <p>FIA_AFL.1/TC Detects and records authentication failure events for the tachograph cards</p> <p>FIA_AFL.1/Remote Detects authentication failure events in case of remote company access</p> <p>FIA_ATD.1//TC Defines user attributes for tachograph cards</p> <p>FIA_UID.2/MS A motion sensor is successfully identified before allowing any other action</p> <p>FIA_UID.2/TC A tachograph card is successfully identified before allowing any other action</p> <p>FIA_UID.2/MD A management device is successfully identified before allowing any other action</p> <p>FPT_FLS.1 Preserves a secure state when the following types of failures occur: as specified in {RLB_203, RLB_210, RLB_211}</p> <p>FPT_STM.1 Provides accurate time</p> <p>FPT_TST.1 Detects integrity failure events for security data and stored executable code</p>
O.Authentication	<p>FIA_AFL.1/MS Detects and records authentication failure events for the motion sensor</p> <p>FIA_AFL.1/TC Detects and records authentication failure events for the tachograph cards</p> <p>FIA_UAU.1/TC Allows TC identification before authentication</p> <p>FIA_UAU.1/PIN Allows TC (Workshop Card) identification before authentication</p> <p>FIA_UAU.1/MD Allows MD identification before authentication</p> <p>FIA_UAU.2//MS Motion sensor has to be successfully authenticated before allowing any action</p> <p>FIA_UAU.3/MS Provides unforgeable authentication for the motion sensor</p> <p>FIA_UAU.3/TC Provides unforgeable authentication for the tachograph cards</p> <p>FIA_UAU.3/MD Provides unforgeable authentication for the management device</p> <p>FIA_UAU.5//TC Multiple authentication mechanisms according to CSM_20 in [8] to support user authentication.</p> <p>FIA_UAU.6/MS Periodically re-authenticate the motion sensor</p> <p>FIA_UAU.6/TC Periodically re-authenticate the tachograph cards</p>

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

Security Objectives	Security Functional Requirements
	<p>FIA_UID.2/MS A motion sensor is successfully identified before allowing any other action</p> <p>FIA_UID.2/TC A tachograph card is successfully identified before allowing any other action</p> <p>FIA_UID.2/MD A management device is successfully identified before allowing any other action</p>
O.Integrity	<p>FAU_STG.1 Protect the stored audit records from unauthorised deletion</p> <p>FDP_ETC.2 Provides export of user data with security attributes using the SFP User_Data_Export</p> <p>FDP_SDI.2 monitors user data stored for integrity error</p>
O.Output	<p>FCO_NRO.1 Generates an evidence of origin for the data to be downloaded to external media.</p> <p>FDP_ETC.2 Provides export of user data with security attributes using the SFP User_Data_Export</p> <p>FDP_SDI.2 monitors user data stored for integrity error</p> <p>FPR_UNO.1 Ensures unobservability of secrets</p> <p>FPT_PHP.3 Ensures resistance to physical attack to the TOE software in the field after the TOE activation</p> <p>FPT_TDC.1//SW-Upgrade Provides the capability to consistently interpret secure attributes as defined by the proprietary specification for the SW-Upgrade by the AVU developer</p>
O.Processing	<p>FDP_ACC.1/FUN Defines security attributes for SFP FUNCTION according to the modes of operation</p> <p>FDP_ACC.1/IS SFP Input Sources to ensure the right input sources</p> <p>FDP_ACC.1/SW-Upgrade Defines security attributes for SFP SW-Upgrade</p> <p>FDP_ACF.1/FUN Defines security attributes for SFP FUNCTION according to the modes of operation</p> <p>FDP_ACF.1/IS Defines security attributes for SFP User_Data_Export</p> <p>FDP_ACF.1/SW-Upgrade Defines security attributes for SFP SW-Upgrade</p> <p>FDP_ITC.1 Provides import of user data from outside of the TOE using the SFP Input Sources</p> <p>FDP_ITC.2//IS Provides import of user data from outside of the TOE, using the security attributes associated with the imported user data for the Motion Sensor and for the Tachograph Cards</p> <p>FDP_ITC.2//SW-Upgrade Provides import of user data, from outside of the TOE using the SFP SW-Upgrade. Only user data recognized as an</p>

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

Security Objectives	Security Functional Requirements
	<p>authentic SW-Upgrade are allowed to be accepted as executable code; else they are rejected.</p> <p>FDP_RIP.1 Any previous information content of a resource is made unavailable upon allocation or deallocation of resource</p> <p>FMT_MSA.3/FUN Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p>FMT_MSA.3/IS Provides the SFP Input_Sources to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p>FMT_MSA.3/SW-Upgrade Provides the SFP SW-Upgrade to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p>FPR_UNO.1 Ensures unobservability of secrets</p> <p>FPT_PHP.3 Ensures Resistance to physical attack to the TOE software in the field after the TOE activation</p> <p>FPT_STM.1 Provides accurate time</p> <p>FPT_TDC.1//IS Provides the capability to consistently interpret secure messaging attributes as defined by [10] for the Motion Sensor and by [8] for the Tachograph Cards</p> <p>FPT_TDC.1//SW-Upgrade Provides the capability to consistently interpret secure attributes as defined by the proprietary specification for the SW-Upgrade by the AVU developer</p>
O.Reliability	<p>FDP_ACC.1/FUN Defines security attributes for SFP FUNCTION according to the modes of operation</p> <p>FDP_ACC.1/IS SFP Input Sources to ensure the right input sources</p> <p>FDP_ACC.1/SW-Upgrade Defines security attributes for SFP SW-Upgrade</p> <p>FDP_ACF.1/FUN Defines security attributes for SFP FUNCTION according to the modes of operation</p> <p>FDP_ACF.1/IS Defines security attributes for SFP User_Data_Export</p> <p>FDP_ACF.1/SW-Upgrade Defines security attributes for SFP SW-Upgrade</p> <p>FDP_ITC.1 Provides import of user data from outside of the TOE using the SFP Input Sources</p> <p>FDP_ITC.2//IS Provides import of user data from outside of the TOE, using the security attributes associated with the imported user data for the Motion Sensor and for the Tachograph Cards</p>

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

Security Objectives	Security Functional Requirements
	<p>FDP_ITC.2//SW-Upgrade Provides import of user data, from outside of the TOE using the SFP SW-Upgrade. Only user data recognized as an authentic SW-Upgrade are allowed to be accepted as executable code; else they are rejected.</p> <p>FDP_RIP.1 Any previous information content of a resource is made unavailable upon allocation or deallocation of resource</p> <p>FDP_SDI.2 monitors user data stored for integrity error</p> <p>FIA_AFL.1/MS Detects and records authentication failure events for the motion sensor</p> <p>FIA_AFL.1/TC Detects and records authentication failure events for the tachograph cards</p> <p>FMT_MOF.1 Restricts the ability to enable the test functions as specified in {RLB_201} to nobody and, thus, increases TOE reliability in the operational phase.</p> <p>FMT_MSA.3/FUN Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p>FMT_MSA.3/IS Provides the SFP Input_Sources to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p>FMT_MSA.3/SW-Upgrade Provides the SFP SW-Upgrade to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p>FPR_UNO.1 Ensures unobservability of secrets</p> <p>FPT_FLS.1 Preserves a secure state when the following types of failures occur: as specified in {RLB_203, RLB_210, RLB_211}</p> <p>FPT_PHP.2//Power_Deviation Detection of physical tampering (Power_Deviation) and generation of an audit record</p> <p>FPT_PHP.2/HW_sabotage Detection of physical tampering (Removal of the smart card placed in any slot outside the control of the TOE) and generation of an audit record</p> <p>FPT_PHP.3 Ensures Resistance to physical attack to the TOE software in the field after the TOE activation</p> <p>FPT_STM.1 Provides accurate time</p> <p>FPT_TDC.1//IS Provides the capability to consistently interpret secure messaging attributes as defined by [10] for the Motion Sensor and by [8] for the Tachograph Cards.</p>

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

Security Objectives	Security Functional Requirements
	<p>FPT_TDC.1//SW-Upgrade Provides the capability to consistently interpret secure attributes as defined by the proprietary specification for the SW-Upgrade by the AVU developer.</p> <p>FPT_TST.1 Detects integrity failure events for security data and stored executable code</p> <p>FRU_PRS.1 Ensures that resources will be available when needed</p>
O.Secured_Data_Exchange	<p>FCO_NRO.1 Generates an evidence of origin for the data to be downloaded to external media.</p> <p>FCS_CKM.1/TDES Generates of session keys for the motion sensor and the tachograph cards</p> <p>FCS_CKM.2 Controls distribution of cryptographic keys in accordance with a specified cryptographic key distribution method as specified in the table below that meets the following list of standards.</p> <p>FCS_CKM.3 Controls cryptographic key access and storage in the TOE</p> <p>FCS_CKM.4 Destroys cryptographic keys in the TOE</p> <p>FCS_COP.1/TDES Provides the cryptographic operation TDES</p> <p>FCS_COP.1/RSA Provides the cryptographic operation RSA</p> <p>FDP_ACC.1/FUN Defines security attributes for SFP FUNCTION according to the modes of operation</p> <p>FDP_ACF.1/FUN Defines security attributes for SFP FUNCTION according to the modes of operation</p> <p>FDP_ETC.2 Provides export of user data with security attributes using the SFP User_Data_Export</p> <p>FDP_ITC.2//IS Provides import of user data from outside of the TOE, using the security attributes associated with the imported user data for the Motion Sensor and for the Tachograph Cards</p> <p>FIA_ATD.1//TC Defines user attributes for tachograph cards</p> <p>FIA_UAU.1/TC Allows TC identification before authentication</p> <p>FIA_UAU.2//MS Motion sensor has to be successfully authenticated before allowing any action</p> <p>FIA_UAU.5//TC Multiple authentication mechanisms according to CSM_20 in [8] to support user authentication.</p> <p>FIA_UAU.6/MS Periodically re-authenticate the motion sensor</p> <p>FIA_UAU.6/TC Periodically re-authenticate the tachograph cards</p> <p>FIA_UID.2/MS A motion sensor is successfully identified before allowing any other action</p> <p>FIA_UID.2/TC A tachograph card is successfully identified before allowing any other action</p>

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

Security Objectives	Security Functional Requirements
	<p>FMT_MSA.1 Provides the SFP FUNCTION to restrict the ability to change_default the security attributes User Group, User ID to nobody</p> <p>FMT_MSA.3/FUN Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p>FMT_SMF.1 Performing all operations being allowed only in the calibration mode</p> <p>FMT_SMR.1//TC Maintain the roles as defined in {UIA_208} as User Groups</p>
O.Software_Analysis	<p>FPT_PHP.3 Ensures resistance to physical attack to the TOE software in the field after the TOE activation</p> <p>FPR_UNO.1 Ensures unobservability of secrets</p> <p>FDP_ACC.1/FUN Defines security attributes for SFP FUNCTION according to the modes of operation</p> <p>FDP_ACF.1/FUN Defines security attributes for SFP FUNCTION according to the modes of operation</p> <p>FMT_MSA.3/FUN Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p>
O.Software_Upgrade	<p>FCS_COP.1/AES Provides the cryptographic operation AES.</p> <p>FCS_COP.1/ECDSA Provides the cryptographic operation ECDSA</p> <p>FCS_CKM.1/AES Generates secure boot keys</p> <p>FCS_CKM.3 Controls cryptographic key access and storage in the TOE</p> <p>FCS_CKM.4 Destroys cryptographic keys in the TOE</p> <p>FDP_ACC.1/ SW-Upgrade SFP SW-Upgrade for the upgrade of the software in the TOE</p> <p>FDP_ACF.1/SW-Upgrade Defines security attributes for SFP SW-Upgrade</p> <p>FDP_ITC.2//SW-Upgrade Provides import of user data, from outside of the TOE using the SFP SW-Upgrade. : Only user data recognized as an authentic SW-Upgrade are allowed to be accepted as executable code; else they are rejected</p> <p>FMT_MSA.3/SW-Upgrade Provides the SFP SW_Upgrade to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p>

Security Objectives	Security Functional Requirements
	FPT_TDC.1//SW-Upgrade Provides the capability to consistently interpret secure attributes as defined by the proprietary specification for the SW-Upgrade by the AVU developer

7.3.2 Rationale for SFR's Dependencies

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-dissolved dependencies are appropriately explained.

The dependency analysis has directly been made within the description of each SFR in sec. 7.1 above. All dependencies being expected by CC part 2 are either fulfilled or their non-fulfilment is justified.

7.3.3 Security Assurance Requirements Rationale

The current Security Target is claimed to be conformant with the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5.

The current assurance package was chosen based on the pre-defined assurance package EAL4. This package permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level, at which it is likely to retrofit to an existing product line in an economically feasible way. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs.

The selection of the component ATE_DPT.2 provides a higher assurance than the pre-defined EAL4 package due to requiring the functional testing of SFR-enforcing modules.

The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This decision represents a part of the conscious security policy for the recording equipment required by the legislative [5] and reflected by the current ST.

The set of assurance requirements being part of EAL4 fulfils all dependencies a priori.

The augmentation of EAL4 chosen comprises the following assurance components:

- ATE_DPT.2 and
- AVA_VAN.5.

For these additional assurance component, all dependencies are met or exceeded in the EAL4 assurance package:

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

Table 11: SAR Dependencies

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependency fulfilled by
TOE security assurance requirements (only additional to EAL4)		
ATE_DPT.2	ADV_ARC.1	ADV_ARC.1
	ADV_TDS.3	ADV_TDS.3
	ATE_FUN.1	ATE_FUN.1
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1
	ADV_FSP.4	ADV_FSP.4
	ADV_TDS.3	ADV_TDS.3
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.2

8 TOE Summary Specifications

Table 12: TOE Summary

Security Service	Security Functional Requirements concerned
<p>Identification and authentication of motion sensor, tachograph cards and management device:</p> <p>It describes the identification and authentication of motion sensor, user (by using tachograph cards), and management device. It is defined in [7] and summarized in Annex-A: Coverage of the requirements of Appendix 10 (UIA_201 to UIA_206 for motion sensor, UIA_207 to UIA_214 for user, UIA_215 to UIA_220 for remotely connected company, UIA_221 to UIA_223 for management device).</p> <p>The TOE authenticates the motion sensor it is connected to; at motion sensor connection, at each calibration of the recording equipment, at power supply recovery. Authentication is mutual and triggered by the TOE before allowing any other TSF-mediated actions in accordance with FIA_UAU.2//MS. TSF detects and prevents use of authentication data that has been copied and replayed (FIA_UAU.3/MS) and supports enforcing the SFP FUNCTION and SFP Input Sources to avoid value changes of security attributes (FMT_MSA.1, FMT_MSA.3/FUN and FMT_MSA.3/IS).</p> <p>The TOE identifies and authenticates its users at card insertion before allowing any further TSF-mediated actions in accordance with FIA_UID.2/TC, FIA_UAU.1/TC and FIA_UAU.5//TC as well as FIA_UAU.1/PIN. The authentication is mutual and triggered by the TOE. TSF detects and prevents use of authentication data that has been copied and replayed (FIA_UAU.3/TC), maintains the list of security attributes belonging to individual users as required by FIA_ATD.1//TC and prevents value changes of security attributes (FMT_MSA.1). Authentication is performed by means of proving that the card inserted is a valid tachograph card, possessing security data that only the system could distribute.</p> <p>The TOE identifies and authenticates the remotely connected company for every interactions before allowing any data to export it. Similar to the FIA_UAU.3/TC, the TOE detects and prevents use of authentication data that has been copied and replayed. After 5 consecutive unsuccessful authentication</p>	<ul style="list-style-type: none"> – FIA_UID.2/MS: Identification of the motion sensor – FIA_UID.2/TC: Identification of the tachograph cards – FIA_UID.2/MD: Identification of the Management Device – (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor – (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards – FIA_UAU.1/MD, FIA_UAU.3/MD: Authentication of the Management Device – FIA_UAU.1/PIN: additional PIN authentication for the workshop card – FIA_AFL.1/MS: Authentication failure: motion sensor – FIA_AFL.1/TC: Authentication failure: tachograph cards – FIA_AFL.1/Remote – (FIA_ATD.1//TC, FMT_SMR.1//TC): User groups to be maintained by the TOE – FMT_MSA.3/FUN – FDP_ACC.1/FUN functions <p>Supported by:</p> <ul style="list-style-type: none"> – FCS_COP.1/TDES: for the motion sensor – FCS_COP.1/RSA: for the tachograph cards – FCS_COP.1/ECDSA: for signature verification of the software update data

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

Security Service	Security Functional Requirements concerned
<p>attempts have been detected, the TOE warns the remotely connected company and close the current session.</p> <p>The TOE identifies and authenticates the management device (MD).</p>	<ul style="list-style-type: none"> – (FCS_CKM.1/TDES, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management – FAU_GEN.1: Audit records: Generation – (FMT_MSA.1, FMT_SMF.1)
<p>Access control to functions and stored data:</p> <p>It ensures that the access to read, create or modify any information into the TOE is granted to only by those authorized. It is defined in [7] and summarized in Annex-A: Coverage of the requirements of Appendix 10 (ACC_201 for general access control, ACC_202-ACC_203 for functions, ACC_204 to ACC_210 for data, ACC_211 for file structure).</p> <p>TSF controls the access to the data and functions and enforces the File Structure SFP, SFP FUNCTION, SFP DATA, SFP User Data Export, SFP Input Sources, SFP SW-Upgrade as required by FDP_ACC.1/*, FDP_ACF.1/* and FMT_MSA.3/FUN, FMT_MSA.3/FIL, FMT_MSA.3/DAT, FMT_MSA.3/IS, FMT_MSA.3/UDE, FMT_MSA.3/SW-Upgrade.</p> <p>TSF implements the File Structure SFP for tachograph application and data files structure as required by ACC_211 (FDP_ACC.1/FIL, FDP_ACF.1/FIL) and enforces the SFP FUNCTION, SFP DATA, SFP User Data Export on subjects, objects, and operations as required in [5] and described in Class FDP User Data Protection (FDP_ACC.1/DAT, FDP_ACF.1/DAT, FDP_ACC.1/UDE, FDP_ACF.1/UDE).</p> <p>TSF ensures that user data (entered manually) related to requirement 109a in [5] may only be entered for the period last card withdrawal — current insertion (requirement 050a) in accordance with the requirements FDP_ACC.1/UDE, FDP_ACF.1/UDE.</p> <p>Software update of the security and non-security relevant software components is only possible after the corresponding authentication and verification with help of credentials as required in FDP_ACC.1/SW-Upgrade and FDP_ACF.1/SW-Upgrade.</p> <p>Nobody may change the public/private keys and the Km_{VU} after their insertion during the personalization.</p>	<ul style="list-style-type: none"> – (FDP_ACC.1/FIL, FDP_ACF.1/FIL): file structures – (FDP_ACC.1/FUN, FDP_ACF.1/FUN): functions – (FDP_ACC.1/DAT, FDP_ACF.1/DAT): stored data – (FDP_ACC.1/UDE, FDP_ACF.1/UDE): user data export – (FDP_ACC.1/IS, FDP_ACF.1/IS): input sources – FDP_ACC.1/SW-Upgrade: authenticate the software upgrades – FDP_ACF.1/SW-Upgrade: capability to control access to the TSF software upgrade function <p>Supported by:</p> <ul style="list-style-type: none"> – (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor – (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards – FIA_UAU.1/PIN: additional PIN authentication for the workshop card – FIA_UAU.1/MD, FIA_UAU.3/MD: Authentication of the Management Device – FMT_MSA.3/FIL – FMT_MSA.3/FUN – FMT_MSA.3/DAT – FMT_MSA.3/UDE

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

Security Service	Security Functional Requirements concerned
<p>Nobody may read the private keys and the Km_{VU} after their insertion during the personalization process in full compliance with FMT_MSA.1, MT_MSA.3/FUN, FMT_MSA.3/FIL, FMT_MSA.3/DAT, FMT_MSA.3/IS, FMT_MSA.3/UDE.</p>	<ul style="list-style-type: none"> - FMT_MSA.3/IS - FMT_MSA.3/SW-Upgrade. - FMT_MSA.1, FMT_SMF.1, FMT_SMR.1//TC
<p>Accountability of users:</p> <p>It defines the accountability for each user. It is defined in [7] and summarized in Annex-A: Coverage of the requirements of Appendix 10 (ACT_201 to ACT_207).</p> <p>The audit function will be started up as soon as the TOE has external power supply after activation and shut down, when the external power supply is interrupted. In this case TSF records within each audit record at least the information date and time of begin and end of the event and the type of event.</p> <p>TSF, for events impairing the security of the TOE, records those events with associated data ([5] (requirements 094, 096 and 109) as required in FAU_GEN.1.</p> <p>TSF enforces audit records storage rules [5] (requirement 094) and (requirement 096) in a way as required in FDP_ETC.2, furthermore, it preserves the audit trail as required by FAU_STG.1</p> <p>TSF stores audit records generated by the motion sensor in its data memory as required by FAU_GEN.1 and the transfer of the record from the motion sensor to the TOE is encrypted according to FCS_COP.1/TDES.</p> <p>Audit capabilities are required only for events that may indicate a manipulation or a security breach attempt. It is not required for the normal exercising of rights even if relevant for security.</p> <p>TSF is also able to provide reliable time stamps based on the RTC time information (as required in FPT_STM.1) for its own use.</p> <p>TSF writes the relevant audit records on tachograph cards in a way as required by FDP_ACC.1/DAT and FDP_ACF.1/DAT and update binary with secure messaging is used [8] (FCS_COP.1/TDES). TSF overwrites the oldest stored audit records and behaves according to [5] requirements 083, 086, 089, 092 and 105b, if the audit trail is full as required in FAU_STG.4.</p>	<ul style="list-style-type: none"> - FAU_GEN.1: Audit records: Generation - FAU_STG.1: Audit records: Protection against modification - FAU_STG.4: Audit records: Prevention of loss - FDP_ETC.2: Export of user data with security attributes <p>Supported by:</p> <ul style="list-style-type: none"> - (FDP_ACC.1/DAT, FDP_ACF.1/DAT): VU identification data - (FDP_ACC.1/UDE, FDP_ACF.1/UDE): Data update on the TC - FPT_STM.1: time stamps - FCS_COP.1/TDES: for the motion sensor and the tachograph cards

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

Security Service	Security Functional Requirements concerned
<p>Audit of events and faults:</p> <p>It defines the audit capabilities. It is required only for events that may indicate a manipulation or a security breach attempt. It is defined in [7] and summarized in Annex-A: Coverage of the requirements of Appendix 10 (AUD_201 to AUD_205).</p> <p>TSF, for events impairing the security of the TOE, records those events with associated data as required in FAU_GEN.1 and makes it possible to print, display and download audit records except for the events listed in REQ 011 as required by FAU_SAR.1.</p>	<p>– FAU_GEN.1: Audit records: Generation</p> <p>– FAU_SAR.1: Audit records: Capability of reviewing</p> <p>Supported by:</p> <p>– (FDP_ACC.1/DAT, FDP_ACF.1/DAT): Storing motion sensor’s audit records</p> <p>– FDP_ETC.2 Export of user data with security attributes: Related audit records to the TC.</p>
<p>Object reuse for secret data:</p> <p>It provides residual information protection by deallocating the resource. It is defined in [7] and summarized in Annex-A: Coverage of the requirements of Appendix 10 (REU_201)</p> <p>TSF ensures that any previous information content of a resource used for operations in which security relevant material is involved in volatile memory in the TOE, is erased upon the allocation of a new resource as required in FDP_RIP.1. Furthermore temporarily active keys are destroyed in accordance with FCS_CKM.4. Other temporary storage objects can be re-used without implying inadmissible information flow.</p>	<p>– FDP_RIP.1 Subset residual information protection</p> <p>Supported by:</p> <p>– FCS_CKM.4: Cryptographic key destruction</p>
<p>Accuracy of recorded and stored data:</p> <p>It provides accuracy services by controlling the information flow, checking the internal data transfers, and checking the stored data integrity. It is defined in [7] and summarized in Annex-A: Coverage of the requirements of Appendix 10 (ACR_201-ACR_201a for information flow, ACR_202-ACR_203 for internal data transfers, ACR_204-ACR_205 for stored data integrity).</p> <p>TSF ensures that user data related to requirements 081, 084, 087, 090, 093, 102, 104, 105, 105a and 109 [5] may only be processed from the right input sources:</p> <ul style="list-style-type: none"> • vehicle motion data, as required by FPT_TDC.1//IS • VU’s real time clock, as required in FPT_STM.1 	<p>– FDP_ITC.1: right input sources without sec. attributes (keyboard, calibration data, RTC)</p> <p>– FDP_ITC.2//IS: right input sources with sec. attributes (MS and TC)</p> <p>– FDP_ITC.2//SW-Upgrade: import of user data with security attributes</p> <p>– FPT_TDC.1//IS: Inter-TSF basic TSF data consistency (MS and TC)</p> <p>– (FDP_ACC.1/UDE, FDP_ACF.1/UDE): User data export to the TC and to external media</p> <p>– FDP_SDI.2: Stored data integrity</p>

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

Security Service	Security Functional Requirements concerned
<ul style="list-style-type: none"> • recording equipment calibration parameters, as required in FDP_ITC.1 • tachograph cards, as required by FPT_TDC.1//IS, supported by users' inputs <p>in accordance with the requirements FDP_ACC.1//IS, FDP_ACF.1//IS, FPT_STM.1, FDP_ITC.1, FDP_ITC.2//IS, FPT_TDC.1//IS.</p> <p>TSF ensures that user data related to requirement 109a [5], may only be entered for the period last card withdrawal — current insertion (requirement 050a) in accordance with the requirements FDP_ACC.1//UDE and FDP_ACF.1//UDE.</p> <p>TSF protects the user data stored in the TOE by SHA-1 hash values which are calculated about the data and stored in the TOE together with the data. The integrity of the user data is checked regularly fulfilling the requirement FDP_SDI.2. Upon detection of a stored user data integrity error, TSF generates an audit record in accordance with FAU_GEN.1.</p> <p>Software update is only possible after the corresponding authentication as required in FIA_UAU.1//MD, FIA_UAU.3//MD. SW-Upgrade is performed only if the integrity and the authenticity of the patch data is confirmed by means of update credentials (FPT_TDC.1//SW-Upgrade and FDP_ITC.2//SW-Upgrade) which are used by FCS_COP.1//AES and FCS_COP.1//ECDSA.</p>	<p>– FPT_TDC.1//SW-Upgrade: capability to ensure the consistency of data for the update</p> <p>Supported by:</p> <p>– FCS_COP.1//AES: for decryption of the software update data and encryption / decryption of the data transferred between the security processor and the main processor</p> <p>– FCS_COP.1//ECDSA: for signature verification of the software update data</p> <p>– FCS_CKM.1//AES: Cryptographic key generation</p> <p>– (FDP_ACC.1//IS, FDP_ACF.1//IS): right input sources</p> <p>– (FDP_ACC.1//FUN, FDP_ACF.1//FUN): limited manual entry</p> <p>– FAU_GEN.1: Audit records: Generation</p> <p>– FPT_STM.1: Reliable time stamps</p> <p>– (FIA_UAU.2//MS, FIA_UAU.3//MS, FIA_UAU.6//MS): Authentication of the motion sensor</p> <p>– (FIA_UAU.1//TC, FIA_UAU.3//TC, FIA_UAU.5//TC, FIA_UAU.6//TC): Authentication of the tachograph cards</p> <p>– FIA_UAU.1//MD, FIA_UAU.3//MD: Authentication of the Management Device</p>
<p>Reliability of services:</p> <p>It provides reliability services related to test, software, physical protection, power supply interruptions, reset conditions, data availability and multiple applications. It is defined in [7] and summarized in Annex-A: Coverage of the requirements of Appendix 10 (RLB_201 to RLB_203 for tests, RLB_204-RLB_205 for software, RLB_206 to RLB_208 for physical protection, RLB_209-RLB_210 for power supply interruptions, RLB_211 for reset conditions, RLB_212 to RLB_214</p>	<p>– FDP_ITC.2//IS: no executable code from external sources</p> <p>– FDP_ITC.2//SW-Upgrade: definition of conditions for update acceptance</p> <p>– FPR_UNO.1: Unobservability of leaked data</p> <p>– FPT_FLS.1: Failure with preservation of secure state</p>

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

Security Service	Security Functional Requirements concerned
<p>for data availability, RLB_215 for multiple applications).</p> <p>Inputs from external sources are not accepted as executable code (as required in FDP_ITC.2//IS, FDP_ACC.1//IS, FDP_ACF.1//IS). SW-Upgrade of the TOE is accepted only if the update patch can be decrypted and the digital signature on it can be verified (FDP_ITC.2//SW-Upgrade) with the help of credentials as required in FDP_ACC.1//SW-Upgrade, FDP_ACF.1//SW-Upgrade and FPT_TDC.1//SW-Upgrade. The cryptographic keys necessary for decryption and digital signature verification are securely loaded to the TOE during the manufacturing before the personalization (FMT_MSA.3//SW-Upgrade).</p> <p>TSF controls the access to the data and functions of the TOE and prevents analysis or debug of TOE's software (including the cryptographic material) in the field after the TOE activation (FPR_UNO.1). This includes that TSF allows the calibration functions only in calibration mode (REQ 010) in accordance with FMT_SMF.1.</p> <p>TSF ensures that cards cannot be released before relevant data have been stored to them (FDP_ACC.1//FUN, FDP_ACF.1//FUN).</p> <p>TSF preserves a secure state when deviation from specified values of the power supply, including cut-off is detected. In that case TSF, in compliance with FPT_FLS.1,</p> <ul style="list-style-type: none"> • generates an audit record (except when in calibration mode) compliant with FAU_GEN.1, • preserves the secure state of the TOE, • maintains the security functions, related to components or processes still operational, • preserves the stored data integrity <p>In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset condition, TSF resets the TOE clearly as required by FPT_FLS.1 and an audit record is generated and stored after power supply reconnection as required by FAU_GEN.1.</p> <p>TSF deletes security sensitive information in the flash memory of the security processor when electrical or</p>	<p>– FPT_PHP.2//Power_Deviation: Notification of physical attack</p> <p>– FPT_PHP.2//HW_sabotage : Notification of physical attack</p> <p>– FPT_PHP.3: Resistance to physical attack: stored data</p> <p>– FPT_TST.1: TSF testing</p> <p>– FRU_PRS.1: Availability of services</p> <p>– FDP_ACC.1//SW-Upgrade</p> <p>– FDP_ACF.1//SW-Upgrade</p> <p>– FPT_TDC.1//SW-Upgrade</p> <p>– FMT_MSA.3//SW-Upgrade</p> <p>Supported by:</p> <p>– FAU_GEN.1: Audit records: Generation</p> <p>– (FDP_ACC.1//IS, FDP_ACF.1//IS): no executable code from external sources</p> <p>– (FDP_ACC.1//FUN, FDP_ACF.1//FUN): Tachograph Card withdrawal</p> <p>– FMT_MOF.1: No test entry points</p>

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

Security Service	Security Functional Requirements concerned
<p>environmental attack on the TOE security module is detected (FPT_PHP.3). All other physical tampering attempts can be detected by visual inspection.</p> <p>After its activation, the TOE detects removal of the smart card placed in any slot outside the control of the TOE as required by FPT_PHP.2/HW_sabotage and generates an audit record as required by FAU_GEN.1.</p> <p>TSF executes self tests during initial start-up, and during normal operation to verify its correct operation (FPT_TST.1). The TOE self tests include the verification of the integrity of security data and the verification of stored executable code. TSF ensures that access to resources is obtained when required and that resources are neither requested nor retained unnecessarily as required by FRU_PRS.1. All commands, actions or test points, specific to the testing needs of the manufacturing phase of the TOE are disabled during the personalization in accordance with FMT_MOF.1. It is not possible to restore them for later use.</p>	
<p>Cryptographic support:</p> <p>It provides support for security mechanism when needed. It is defined in [7] and summarized in Annex-A: Coverage of the requirements of Appendix 10 (CSP_201 to CSP_205).</p> <p>TOE performs all cryptographic operations with algorithms and a specific key size defined in [8]. Moreover, TOE generates, distributes, accesses and destroys all cryptographic keys in accordance with specified methods in [8].</p>	<ul style="list-style-type: none"> – FCS_COP.1/TDES: for the motion sensor and the tachograph cards (secure messaging) – FCS_COP.1/RSA: for data downloading to external media (signing), for encryption/decryption during the mutual authentication mechanism with tachograph cards and for encryption/decryption during the secure boot mechanism. – FCS_COP.1/AES: for decrypting the personalization file and the deployment software loaded to the TOE during the personalization. For decrypting the deployment software loaded to the TOE during the software upgrade. For encryption/decryption operations during the communication between AP-SP and AP-RTP. – FCS_COP.1/ECDSA: for verifying the digital signature on the personalization file and deployment software when loaded on the TOE

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

Security Service	Security Functional Requirements concerned
	– (FCS_CKM.1/TDES, FCS_CKM.1/AES, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management
<p>Data exchange with motion sensor, tachograph cards and external media (download function):</p> <p>It provides the data exchange service between the TOE and motion sensor, tachograph cards and external media. It is defined in [7] and summarized in Annex-A: Coverage of the requirements of Appendix 10 (DEX_201-DEX202 for motion sensor, DEX_203 to DEX_205 for tachograph cards, DEX_206 to DEX_208 for external media).</p> <p>TSF protects the authenticity and integrity of data being exchanged between the TOE and the external subjects (tachograph card, motion sensor, downloading equipment). The data transfer between the TOE and tachograph cards is secured according to ISO/IEC 7816-4 to the extent as defined in [8] CSM_021 – Retail-MAC as required in FCS_COP.1/TDES. TSF verifies the integrity and authenticity of data imported from tachograph cards. Upon detection of card data integrity or authenticity error, TSF generates an audit record compliant with FAU_GEN.1 and does not use the data as required in FDP_ITC.2//IS.</p> <p>TSF exports data to tachograph smart cards with associated security attributes such that the card will be able to verify its integrity and authenticity as required in FDP_ETC.2.</p> <p>The data transfer between the TOE and the motion sensor is secured according to [10] and as required in FCS_COP.1/TDES and after proper authentication as required in FIA_UAU.2//MS, FIA_UAU.6/MS, FIA_UID.2/MS. TSF verifies the integrity and authenticity of motion data imported from the motion sensor. Upon detection of a motion data integrity or authenticity error, TSF generates an audit record and continues to use imported data as required in FDP_ITC.2//IS.</p> <p>The data transfer between the TOE and downloading equipment are secured according to PKCS#1 v2.0 and with hash algorithm SHA-1 as required in FCS_COP.1/RSA. The TOE identification, its</p>	– FCO_NRO.1: Selective proof of origin for data to be downloaded to external media. Appendix 7 of the regulation [6] describes the data structures to be downloaded to external media. – FDP_ETC.2 Export of user data with security attributes: to the TC and to external media – FDP_ITC.2//IS Import of user data with security attributes: from the MS and the TC Supported by: – FCS_COP.1/TDES: for the motion sensor and the tachograph cards (secure messaging) – FCS_COP.1/RSA: for data downloading to external media (signing) – (FCS_CKM.1/TDES, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management – (FDP_ACC.1/UDE, FDP_ACF.1/UDE): User data export to the TC and to external media – (FDP_ACC.1/IS, FDP_ACF.1/IS): User data import from the MS and the TC – FAU_GEN.1: Audit records: Generation

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

Security Service	Security Functional Requirements concerned
equipment key certificate and the member state certificate are also downloaded (FCO_NRO.1). The verifier of the data must possess European public key to verify the certificate chain.	

	Communication and Information Technologies Sector Common Criteria Document	REV: 0.13 Number: HBT-CC-8255-DT-01 Language: 10 Date: 18.05.2021
---	---	--

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

9 Bibliography

Common Criteria

- [1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
- [2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
- [3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012
- [4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

Digital Tachograph: Directives and Standards

- [5] Council Regulation (EEC) No 3821/85 on recording equipment in road transport, Official Journal of the European Communities
- [6] Appendix 2 of Annex-1B of Council Regulation (EEC) No 3821/85 – Tachograph Cards Specification
- [7] Appendix 10 of Annex-1B of Council Regulation (EEC) No 3821/85 – Generic Security Targets
- [8] Appendix 11 of Annex-1B of Council Regulation (EEC) No 3821/85 – Common Security Mechanisms
- [9] Joint Interpretation Library (JIL): Security Evaluation and Certification of Digital Tachographs, JIL interpretation of the Security Certification according to Commission Regulation (EC) 1360/2002, Annex-1B, Version 1.12, June 2003
- [10] 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
- [11] Digital Tachograph-Vehicle Unit Common Criteria Protection Profile, BSI-CC-PP-0057, Version 1.0, 13th July 2010, Bundesamt für Sicherheit in der Informationstechnik
- [12] Appendix 7 of Annex-1B of Council Regulation (EEC) No 3821/85 – Data Downloading Protocols

Other Reference Documents

- [ECDSA] FIPS 186-2 Digital Signature Standard (ECDSA).
- [SHA-256] FIPS 180-2 Secure Hash Standard (SHA-256).
- [AES] Advanced Encryption Standard (AES) (FIPS PUB 197) and NIST Special Publication 800-38A 2001 Edition.
- [NIST] Special Publication 800-133 Recommendation for Cryptographic Key Generation, Dec. 2012

10 Annex-A: Coverage of the requirements of Appendix 10

The following table demonstrates the coverage of the requirements of [7], chapter 4 by the security functional requirements chosen from [1], [2], [3] and specified in section 7.1 “Security Functional Requirements” above.

Table 13: Requirement coverage

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
	Identification & Authentication	
UIA_201	The VU shall be able to establish, for every interaction, the identity of the motion sensor it is connected to.	FIA_UID.2/MS
UIA_202	The identity of the motion sensor shall consist of the sensor approval number and the sensor serial number.	OSP.Type_Approved_MS
UIA_203	The VU shall authenticate the motion sensor it is connected to: <ul style="list-style-type: none"> - at motion sensor connection, - at each calibration of the recording equipment, - at power supply recovery. Authentication shall be mutual and triggered by the VU.	FIA_UAU.2//MS
UIA_204	The VU shall periodically (<i>every 60 seconds, in power save mode up to 30 minutes</i>) re-identify and reauthenticates the motion sensor it is connected to, and ensures that the motion sensor identified during the last calibration of the recording equipment has not been changed.	FIA_UAU.6/MS
UIA_205	The VU shall detect and prevent use of authentication data that has been copied and replayed.	FIA_UAU.3/MS
UIA_206	After 3 consecutive unsuccessful authentication attempts have been detected, and/or after detecting that the identity of the motion sensor has changed while not authorised (i.e. while not during a calibration of the recording equipment), the SFR shall: <ul style="list-style-type: none"> - generate an audit record of the event, - warn the user, - continue to accept and use non secured motion data sent by the motion sensor. 	FIA_AFL.1/MS, FAU_GEN.1
UIA_207	The VU shall permanently and selectively track the identity of two users, by monitoring the tachograph cards inserted in respectively the driver slot and the co-driver slot of the equipment.	FIA_UID.2/TC

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

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
UIA_208	<p>The user identity shall consist of:</p> <ul style="list-style-type: none"> - a user group: <ul style="list-style-type: none"> - DRIVER (driver card), - CONTROLLER (control card), - WORKSHOP (workshop card), - COMPANY (company card), - UNKNOWN (no card inserted), - a user ID, composed of : <ul style="list-style-type: none"> - the card issuing Member State code and of the card number, - UNKNOWN if user group is UNKNOWN. <p>UNKNOWN identities may be implicitly or explicitly.</p>	<p>FIA_ATD.1//TC for User Identity</p> <p>FMT_MSA.3/FUN for the default value UNKNOWN (no valid card)</p> <p>FDP_ACC.1/FUN for functions (for UNKNOWN)</p> <p>FMT_MSA.1</p> <p>FMT_MSA.3/FUN</p> <p>FMT_SMF.1</p> <p>FMT_SMR.1//TC for five different User Groups</p>
UIA_209	The VU shall authenticate its users at card insertion.	FIA_UAU.1/TC
UIA_210	<p>The VU shall re-authenticate its users:</p> <ul style="list-style-type: none"> - at power supply recovery, - periodically or after occurrence of specific events (TBD by manufacturers and more frequently than once per day). 	FIA_UAU.6/TC
UIA_211	Authentication shall be performed by means of proving that the card inserted is a valid tachograph card, possessing security data that only the system could distribute. Authentication shall be mutual and triggered by the VU.	FIA_UAU.5//TC
UIA_212	<p>In addition to the above, workshops shall be required to be successfully authenticated through a PIN check. PINs shall be at least 4 characters long.</p> <p>Note: In the case the PIN is transferred to the VU from an outside equipment located in the vicinity of the VU, PIN confidentiality need not be protected during the transfer.</p>	FIA_UAU.1/PIN
UIA_213	The VU shall detect and prevent use of authentication data that has been copied and replayed.	FIA_UAU.3/TC
UIA_214	<p>After <u>5</u> consecutive unsuccessful authentication attempts have been detected, the SFR shall:</p> <ul style="list-style-type: none"> - generate an audit record of the event, - warn the user, - assume the user as UNKNOWN, and the card as non valid (definition (z) and requirement 007). 	<p>FIA_AFL.1/TC,</p> <p>FAU_GEN.1</p>

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

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
UIA_215	For every interaction with a remotely connected company, the VU shall be able to establish the company's identity.	FIA_UID.2/TC
UIA_216	The remotely connected company's identity shall consist of its company card issuing Member State code and of its company card number.	FIA_ATD.1/TC
UIA_217	The VU shall successfully authenticate the remotely connected company before allowing any data export to it.	FIA_UAU.1/TC
UIA_218	Authentication shall be performed by means of proving that the company owns a valid company card, possessing security data that only the system could distribute.	FIA_UAU.5/TC
UIA_219	The VU shall detect and prevent use of authentication data that has been copied and replayed.	FIA_UAU.3/TC
UIA_220	After 5 consecutive unsuccessful authentication attempts have been detected, the VU shall: warn the remotely connected company.	FIA_AFL.1/Remote
UIA_221	For every interaction with a management device, the VU shall be able to establish the device identity.	FIA_UID.2/MD
UIA_222	Before allowing any further interaction, the VU successfully authenticates the management device.	FIA_UAU.1/MD
UIA_223	The VU shall detect and prevent use of authentication data that has been copied and replayed.	FIA_UAU.3/MD FMT_MSA.3/IS
Access Control		
ACC_201	The VU shall manage and check access control rights to functions and to data.	FDP_ACC.1/FUN for functions FMT_MSA.3/FUN FDP_ACC.1/DAT for data FMT_MSA.3/DAT
ACC_202	The VU shall enforce the mode of operation selection rules (requirements 006 to 009).	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for choosing an operation mode according to REQ006 to 009.
ACC_203	The VU shall use the mode of operation to enforce the functions access control rules (requirement 010).	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for accessible

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

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
		functions in each mode of operation (REQ010)
ACC_204	The VU shall enforce the VU identification data write access rules (requirement 076)	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for REQ076 FMT_MSA.3/DAT
ACC_205	The VU shall enforce the paired motion sensor identification data write access rules (requirements 079 and 155)	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for REQ079 and 155 FMT_MSA.3/DAT
ACC_206	After the VU activation, the VU shall ensure that only in calibration mode, may calibration data be input into the VU and stored into its data memory (requirements 154 and 156).	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for REQ154 and 156.
ACC_207	After the VU activation, the VU shall enforce calibration data write and delete access rules (requirement 097).	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for REQ097 FMT_MSA.3/DAT
ACC_208	After the VU activation, the VU shall ensure that only in calibration mode, may time adjustment data be input into the VU and stored into its data memory (This requirement does not apply to small time adjustments allowed by requirements 157 and 158).	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for ACC_208
ACC_209	After the VU activation, the VU shall enforce time adjustment data write and delete access rules (requirement 100).	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for ACC_209 FMT_MSA.3/DAT
ACC_210	The VU shall enforce appropriate read and write access rights to security data (requirement 080).	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for REQ080 FMT_MSA.3/DAT
ACC_211	Application and data files structure and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion.	FDP_ACC.1/FIL and FDP_ACF.1/FIL with only one rule as stated in ACC_211 for file structure FMT_MSA.3/FIL

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

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
	Accountability	
ACT_201	The VU shall ensure that drivers are accountable for their activities (requirements 081, 084, 087, 105a, 105b, 109 and 109a).	FAU_GEN.1 with an entry for REQ081, 084, 087,105a REQ105b is completely covered by ACT_206 FDP_ACC.1/UDE FDP_ACF.1/UDE FDP_ETC.2 for REQ109, 109a FMT_MSA.3/UDE
ACT_202	The VU shall hold permanent identification data (requirement 075).	FDP_ACC.1/DAT, FDP_ACF.1/DAT FMT_MSA.3/DAT
ACT_203	The VU shall ensure that workshops are accountable for their activities (requirements 098, 101 and 109).	FAU_GEN.1 with an entry for REQ098, 101 FDP_ACC.1/UDE FDP_ACF.1/UDE FDP_ETC.2 for REQ109 FMT_MSA.3/UDE
ACT_204	The VU shall ensure that controllers are accountable for their activities (requirements 102, 103 and 109).	FAU_GEN.1 with an entry for REQ102, 103 FDP_ACC.1/UDE FDP_ACF.1/UDE FDP_ETC.2 for REQ109 FMT_MSA.3/UDE
ACT_205	The VU shall record odometer data (requirement 090) and detailed speed data (requirement 093).	FAU_GEN.1 with an entry for REQ 090, 093
ACT_206	The VU shall ensure that user data related to requirements 081 to 093 and 102 to 105b inclusive are not modified once recorded, except when becoming oldest stored data to be replaced by new data.	FAU_STG.1 with <i>detection</i> for 081 to 093 and 102 to 105a FAU_STG.4 for REQ083, 086, 089, 092, 105b (replacing oldest data)
ACT_207	The VU shall ensure that it does not modify data already stored in a tachograph card (requirement 109 and 109a) except for replacing oldest data by new data (requirement 110) or in the case described in Appendix 1 Paragraph 2.1.Note.	FDP_ETC.2 for REQ109, 109a and 110

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

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
	Audit	
AUD_201	The VU shall, for events impairing the security of the VU, record those events with associated data (requirements 094, 096 and 109).	FAU_GEN.1 for REQ094, 096 FDP_ETC.2
AUD_202	The events affecting the security of the VU are the following: <ul style="list-style-type: none"> - Security breach attempts: <ul style="list-style-type: none"> - 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, - unauthorised case opening, - hardware sabotage, - Last card session not correctly closed, - Motion data error event, - Power supply interruption event, - VU internal fault. 	FAU_GEN.1 for AUD_202
AUD_203	The VU shall enforce audit records storage rules (requirement 094 and 096).	FAU_GEN.1
AUD_204	The VU shall store audit records generated by the motion sensor in its data memory.	FDP_ACC.1/DAT FDP_ACF.1/DAT FMT_MSA.3/DAT
AUD_205	It shall be possible to print, display and download audit records.	FAU_SAR.1
	Object Reuse	
REU_201	The VU shall ensure that temporary storage objects can be reused without this invoking inadmissible information flow.	FDP_RIP.1
	Accuracy	

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

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
ACR_201	The VU shall ensure that user data related to requirements 081, 084, 087, 090, 093, 102, 104, 105, 105a, 109 may only be processed from the right input sources: <ul style="list-style-type: none"> - Vehicle motion data, - VU's real time clock, - Recording equipment calibration parameters, - Tachograph cards, - User's inputs. 	FDP_ACC.1/IS FDP_ACF.1/IS FPT_STM.1 for VU's real time clock, FDP_ITC.1 for recording equipment calibration parameters, User's inputs; FDP_ITC.2/IS for vehicle motion data; tachograph cards. FPT_TDC.1/IS
ACR_201a	The VU shall ensure that user data related to requirement 109a may only be entered for the period last card withdrawal – current insertion (requirement 050a).	FDP_ACC.1/FUN FDP_ACF.1/FUN
ACR_202	If data are transferred between physically separated parts of the VU, the data shall be protected from modification.	Not applicable, the TOE does not have physically separated parts.
ACR_203	Upon detection of a data transfer error during an internal transfer, transmission shall be repeated and the SFR shall generate an audit record of the event.	Not applicable, the TOE does not have physically separated parts.
ACR_204	The VU shall check user data stored in the data memory for integrity errors.	FDP_SDI.2
ACR_205	Upon detection of a stored user data integrity error, the SFR shall generate an audit record.	FDP_SDI.2, FAU_GEN.1
	Reliability	
RLB_201	a) Organisational part by manufacturer All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU shall be disabled or removed before the VU activation. b) VU cares: It is not possible to restore them for later use.	The property a) is formulated as OSP.Test_Points FMT_MOF.1 for the property b)
RLB_202	The VU shall run self tests, during initial start-up, and during normal operation to verify its correct operation. The VU self tests shall include a verification of the integrity of security data and a verification of the integrity of stored executable code (if not in ROM).	FPT_TST.1
RLB_203	Upon detection of an internal fault during self test, the SFR shall:	FAU_GEN.1 for an audit record

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

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
	<ul style="list-style-type: none"> - generates an audit record (except in calibration mode), - preserves the stored data integrity. 	FPT_FLS.1 for preserving the stored data integrity
RLB_204	There shall be no way to analyse or debug software in the field after the VU activation.	FPT_PHP.3 and ADV_ARC (self protection for stored data) FPR_UNO.1 (no successful analysis of leaked data)
RLB_205	Inputs from external sources shall not be accepted as executable code.	FDP_ITC.2//IS with FDP_ACC.1/IS, FDP_ACF.1/IS FDP_ITC.2//SW-Upgrade FPT_TDC.1//SW-Upgrade FDP_ACC.1/SW-Upgrade FDP_ACF.1/SW-Upgrade FMT_MSA.3/SW-Upgrade
RLB_206	<p>If the VU is designed so that it can be opened, the VU shall detect any case opening, except in calibration mode, even without external power supply for a minimum of 6 months.</p> <p>In such a case, the SFR shall generate an audit record (It is acceptable that the audit record is generated and stored after power supply reconnection).</p> <p>If the VU is designed so that it cannot be opened, it shall be designed such that physical tampering attempts can be easily detected (e.g. through visual inspection).</p>	FPT_PHP.3
RLB_207	After its activation, the VU shall detect specified (Removal of the smart card placed in any slot outside the control of the TOE) hardware sabotage:	see Application Note 15 (an additional FPT_PHP.2/HW_sabotage may be suitable)
RLB_208	In the case described above, the SFR shall generate an audit record and the VU: (shall warn the user).	This requirement depends on RLB_207; see Application Note 15 (an additional FPT_PHP.2/HW_sabotage and RLB_208 in FAU_GEN.1 may be suitable)
RLB_209	The VU shall detect deviations from the specified values of the power supply, including cut-off.	FPT_PHP.2//Power_Deviation for detection

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

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
RLB_210	In the case described above, the SFR shall: <ul style="list-style-type: none"> - generate an audit record (except in calibration mode), - preserve the secure state of the VU, - maintain the security functions, related to components or processes still operational, - preserve the stored data integrity. 	FAU_GEN.1 for Auditing FPT_FLS.1 for preserving a secure state incl. the stored data integrity and/or a clean reset (cf. also RLB_203 and RLB_211)
RLB_211	In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset conditions, the VU shall reset cleanly.	FPT_FLS.1 for preserving a secure state incl. the stored data integrity and/or a clean reset
RLB_212	The VU shall ensure that access to resources is obtained when required and that resources are not requested nor retained unnecessarily.	FRU_PRS.1
RLB_213	The VU shall ensure that cards cannot be released before relevant data have been stored to them (requirements 015 and 016).	FDP_ACC.1/FUN FDP_ACF.1/FUN with a rule for REQ015 and 016
RLB_214	In the case described above, the SFR shall generate an audit record of the event.	FAU_GEN.1 (Last card session not correctly closed)
RLB_215	If the VU provides applications other than the tachograph application, all applications shall be physically and/or logically separated from each other. These applications shall not share security data. Only one task shall be active at a time.	Not applicable. (TOE does not provide applications other than the tachograph application.)
Data Exchange		
DEX_201	The VU shall verify the integrity and authenticity of motion data imported from the motion sensor.	FDP_ITC.2//IS for – vehicle motion data
DEX_202	Upon detection of a motion data integrity or authenticity error, the SFR shall: <ul style="list-style-type: none"> - generate an audit record, - continue to use imported data. 	FAU_GEN.1. FDP_ITC.2//IS for – vehicle motion data
DEX_203	The VU shall verify the integrity and authenticity of data imported from tachograph cards.	FDP_ITC.2//IS for – tachograph cards.
DEX_204	Upon detection of a card data integrity or authenticity error, the SFR shall: <ul style="list-style-type: none"> - generate an audit record, - not use the data. 	FAU_GEN.1 FDP_ITC.2//IS for – tachograph cards

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

Requirement Appendix 10	Requirement Description	Related SFR used in the current ST
DEX_205	The VU shall export data to tachograph smart cards with associated security attributes such that the card will be able to verify its integrity and authenticity.	FDP_ETC.2
DEX_206	The VU shall generate an evidence of origin for data downloaded to external media.	FCO_NRO.1
DEX_207	The VU shall provide a capability to verify the evidence of origin of downloaded data to the recipient.	FCO_NRO.1
DEX_208	The VU shall download data to external storage media with associated security attributes such that downloaded data integrity and authenticity can be verified.	FDP_ETC.2
	Cryptographic Support	
CSP_201	Any cryptographic operation performed by the VU shall be in accordance with a specified algorithm and a specified key size.	FCS_COP.1/TDES FCS_COP.1/RSA FCS_COP.1/AES FCS_COP.1/ECDSA
CSP_202	If the VU generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes	FCS_CKM.1/TDES FCS_CKM.1/AES
CSP_203	If the VU distributes cryptographic keys, it shall be in accordance with specified key distribution methods.	FCS_CKM.2
CSP_204	If the VU accesses cryptographic keys, it shall be in accordance with specified cryptographic keys access methods.	FCS_CKM.3
CSP_205	If the VU destroys cryptographic keys, it shall be in accordance with specified cryptographic keys destruction methods.	FCS_CKM.4

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

Revision History

<u>Revision No</u>	<u>Revision Reason</u>	<u>Date of Revision</u>
0.1	First Publication	29.05.2019
0.2	New cryptographic keys are added and the rest of the document is changed accordingly.	18.09.2020
0.3	FPT_PHP.3 is changed. Sealing label, sealing plug, and sealing cap are changed to SFR enforcing. Figure 4 is also changed accordingly.	09.10.2020
0.4	Revised according to 83-GR_01-ASE.	27.10.2020
0.5	TOE software version info is added.	04.11.2020
0.6	FCS_COP.1/HMAC is added to Table 9.	30.11.2020
0.7	Revised according to 83-GR_05-ASE.	25.12.2020
0.8	TOE software version is updated to v0.9	18.01.2021
0.9	TOE software version is updated to v0.10	05.03.2021
0.10	TOE software version is updated to v0.11.	26.03.2021
0.11	TOE software version is updated to v0.12.	12.04.2021
0.12	TOE software version is updated to v1.0.	27.04.2021
0.13	ST-Lite version is published.	18.05.2021