

Protection Profile

Digital Tachograph – Vehicle Unit (VU PP)

Version 1.0

BSI-CC-PP-0057-2010



Dipl.-Phys. Osman Kocar
Certification
Federal Office for Information Security (BSI), Germany

Topics of VU-PP CC 3.1 R3

- ❑ **Overview**
- ❑ **Security Concept of the Digital Tachograph**
- ❑ **Security Objectives for the TOE (VU PP, CC 3.1 R3)**
- ❑ **Security Objectives for the Operational Environment (VU PP, CC 3.1 R3)**
- ❑ **Primary Assets to be protected (VU PP, CC 3.1 R3)**
- ❑ **Secondary Assets to be protected (VU PP, CC 3.1 R3)**
- ❑ **Security Functional Requirements (VU PP, CC 3.1 R3)**
- ❑ **Security Assurance Requirements (VU PP, CC 3.1 R3)**
- ❑ **Outlook**

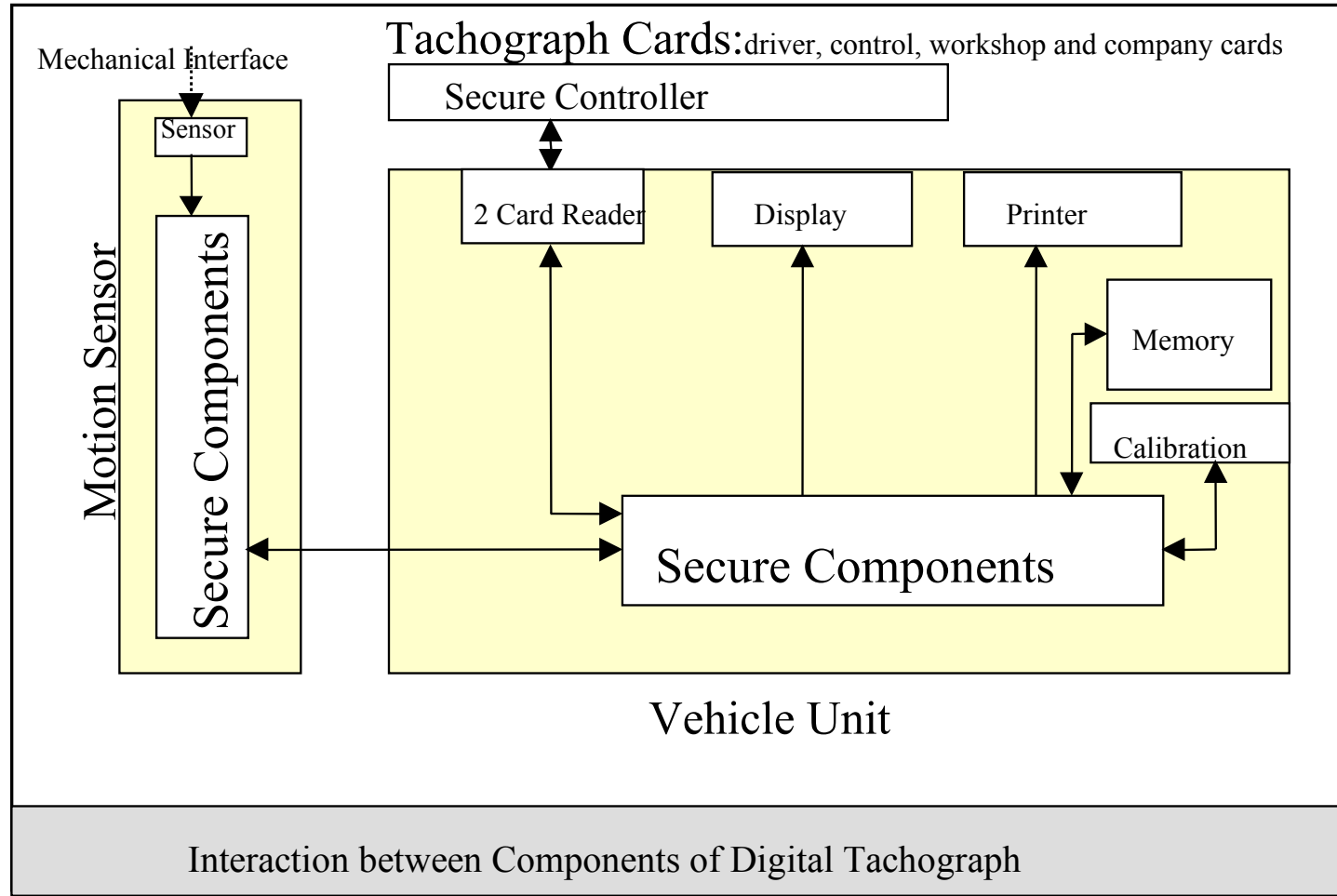
Overview

- ❑ The Digital Tachograph Systems consists of Vehicle Unit, Motion Sensor and Tachograph Cards.
- ❑ The System with different components will be installed in road transport vehicles (e.g. truck over 3.5T, bus 9 Persons)
- ❑ The Security of the technical components of the Digital Tachograph System (e.g. vehicle unit) expressed in the European Commission Regulation 1360/2002, Annex I B, Appendix 10 (Generic Security Target written according to ITSEC)
- ❑ Generic Security Target is issued by the European Commission (basis for the VU PP)
- ❑ Joint Interpretation Library (JIL), Version 1.12, Security Evaluation and Certification of Digital Tachographs, interpretation of the Security Certification according to Commission Regulation (Annex IB)

Overview

- ❑ This new Protection Profile should reflect the content of the Generic Security Target (GST) in Appendix 10 of Annex IB (issued by the EC) and
- ❑ Joint Interpretation Library (JIL, Digital Tachographs), V1.12
- ❑ The intention is the coverage of the requirements in Appendix 10 by the security functional requirements of the current PP and the JIL document
- ❑ GST (ITSEC:E3, high) ==> CC EAL4+
- ❑ Draft developments of the PP for VU have been commented by the European Schemes and manufacturers

Security Concept of the Digital Tachograph



Security Objectives for the TOE

(VU PP, CC 3.1 R3)

O.Access	The TOE must control user access to functions and data.
O.Accountability	The TOE must collect accurate accountability data.
O.Audit	The TOE must audit attempts to undermine system security and should trace them to associated users.
O.Authentication	The TOE should authenticate users and connected entities (when a trusted path needs to be established between entities).
O.Integrity	The TOE must maintain stored data integrity.

Security Objectives for the TOE

(VU PP, CC 3.1 R3)

O.Output	The TOE must ensure that data output reflects accurately data measured or stored.
O.Processing	The TOE must ensure that processing of inputs to derive user data is accurate.
O.Reliability	The TOE must provide a reliable service.
O.Secured_Data_Exchange	The TOE must secure data exchanges with the motion sensor and with tachograph cards.
O.Software_Analysis	There shall be no way to analyse or debug software in the field after the TOE activation.

Security Objectives for the Operational Environment (VU PP, CC 3.1 R3)

- Design environment
- Manufacturing environment
- Workshops environment
- End-user environment

Security Objectives for the Operational Environment (VU PP, CC 3.1 R3)

OE.Activation	Vehicle manufacturers and fitters or workshops shall 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 shall be carried by trusted and approved fitters or workshops.
OE.Faithful_Calibration	Approved fitters and workshops shall enter proper vehicle parameters in recording equipment during calibration.

Primary Assets to be protected (VU PP, CC 3.1 R3)

Object No.	Asset	Definition	Generic security
1	user data (recorded or stored in the TOE)	Any data, other than security data and authentication data, recorded or stored by the VU, required by Commission Regulation	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: <ul style="list-style-type: none"> - a motion sensor, - a tachograph card, or - an external medium for data download. 	Confidentiality Integrity Authenticity

Secondary Assets to be protected (VU PP, CC 3.1 R3)

Object No.	Asset	Definition	Generic Security
1	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 subjects only.	Availability
2	Genuineness of the TOE	Property of the TOE to be authentic in order to provide the claimed security functionality in a proper way.	Availability
3	TOE immanent secret security data	Secret security elements: All Keys used (e.g. symmetric master key, session keys)	Confidentiality Integrity

- ❑ Identification and authentication of motion sensor and tachograph cards,
- ❑ Access control to functions and stored data,
- ❑ Accountability of users,
- ❑ Audit of events and faults,
- ❑ Prevention of object reuse for secret data,
- ❑ Accuracy of recorded and stored data,
- ❑ Reliability of services,
- ❑ Secure data exchange (e.g. MS or Tach. Cards).

Security Assurance Requirements (VU PP, CC 3.1 R3)

- ❑ Common Criteria Part 3 conformant
- ❑ EAL 4 augmented by ATE_DPT.2 and AVA_VAN.5
- ❑ ID: BSI-CC-PP-0057-2010
- ❑ Why ATE_DPT.2 ?

Outlook

- ❑ The advantages of this CC VU PP:
 - ❑ Easy creation of the Security Target for manufacturer
 - ❑ Applying the new evaluation technique according to CC improvement
 - ❑ Applying the latest CEM after harmonization with different schemes
 - ❑ Using the latest CC interpretation during certification
 - ❑ Comparability of the certification results between schemes
 - ❑ CC has more acceptance than ITSEC in the world

- ❑ Next steps: PPs for Tachograph Cards and Motion Sensors

Contact

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Referat 322 - Zertifizierung
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)228-99-9582-111

zertifizierung@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de