# [F1[F2ANNEX I B

## REQUIREMENTS FOR CONSTRUCTION, TESTING, INSTALLATION AND INSPECTION

**Textual Amendments**

**F1** Inserted by Council Regulation (EC) No 2135/98 of 24 September 1998 amending Regulation (EEC) No 3821/85 on recording equipment in road transport and Directive 88/599/EEC concerning the application of Regulations (EEC) No 3820/85 and (EEC) No 3821/85.

**F2** Substituted by Commission Regulation (EC) No 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport (Text with EEA relevance).

## Appendix 10

## GENERIC SECURITY TARGETS

### TACHOGRAPH CARD GENERIC SECURITY TARGET

4. Security enforcing functions

This paragraph refines some of the permitted operations such as assignment or selection of (ES PP) and provides additional SEF functional requirements.

4.1. Compliance to protection profiles

The TOE shall comply with (IC PP).

The TOE shall comply with (ES PP) as refined further.

4.2. User identification and authentication

The card must identify the entity in which it is inserted and know whether it is an authenticated vehicle unit or not. The card may export any user data whatever the entity it is connected to, except the control **[**[F3]and the company card**]** which may export card holder identification data to authenticated vehicle units only (such that a controller is ensured that the vehicle unit is not a fake one by seeing his name on display or printouts).

**Textual Amendments**

**F3** Inserted by Commission Regulation (EC) No 432/2004 of 5 March 2004 adapting for the eighth time to technical progress Council Regulation (EEC) No 3821/85 of 20 December 1985 on recording equipment in road transport (Text with EEA relevance).

4.2.1. User identification

**Assignment** (FIA_UID.1.1) *List of TSF mediated actions*: none.

**[**[X1]**Assignment** (FIA_ATD.1.1) *List of security attributes*:

**Editorial Information**

**X1** Substituted by Corrigendum to Commission Regulation (EC) No 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport (Official Journal of the European Communities L 207 of 5 August 2002).

USER_GROUP : VEHICLE_UNIT, NON_VEHICLE_UNIT,
USER_ID : Vehicle Registration Number (VRN) and registering Member State code (USER_ID is known for USER_GROUP = VEHICLE_UNIT only).**]**

4.2.2. User authentication

**Assignment** (FIA_UAU.1.1) *List of TSF mediated actions*:

— Driver and Workshop cards: export user data with security attributes (card data download function),

— Control card: export user data without security attributes except cardholder identification data.

Authentication of a vehicle unit shall be performed by means of proving that it possesses security data that only the system could distribute.

**Selection** (FIA_UAU.3.1 and FIA_UAU.3.2): prevent.

**Assignment** (FIA_UAU.4.1) *Identified authentication mechanism(s)*: any authentication mechanism.

The Workshop card shall provide an additional authentication mechanism by checking a PIN code (This mechanism is intended for the vehicle unit to ensure the identity of the card holder, it is not intended to protect workshop card content).

4.2.3. Authentication failures

**[**[F4]Additionally the following assignments describe the card reaction for each single user authentication failure.

**Textual Amendments**

**F4** Substituted by Commission Regulation (EC) No 432/2004 of 5 March 2004 adapting for the eighth time to technical progress Council Regulation (EEC) No 3821/85 of 20 December 1985 on recording equipment in road transport (Text with EEA relevance).

**Assignment** (FIA_AFL.1.1) *Number*: 1, *list of authentication events*: authentication of a card interface device.

**Assignment** (FIA_AFL.1.2) *List of actions*:
— warn the entity connected,
— assume the user as NON_VEHICLE_UNIT.

Additionally the following assignments**]** describe the card reaction in the case of failure of the additional authentication mechanism required in UIA_302.

**Assignment** (FIA_AFL.1.1) *Number*: 5, *list of authentication events*: PIN checks (workshop card).

**Assignment** (FIA_AFL.1.2) *List of actions*:
— warn the entity connected,
— block the PIN check procedure such that any subsequent PIN check attempt will fail,
— be able to indicate to subsequent users the reason of the blocking.

4.3. Access control

4.3.1. Access control policy

During end-usage phase of its life cycle, the tachograph card is the subject of one single access control security function policy (SFP) named AC_SFP.

**Assignment** (FDP_ACC.2.1) *Access control SFP*: AC_SFP.

4.3.2. Access control functions

**Assignment** (FDP_ACF.1.1) *Access control SFP*: AC_SFP.

**Assignment** (FDP_ACF.1.1) *Named group of security attributes*: USER_GROUP.

**Assignment** (FDP_ACF.1.2) *Rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*:

**[**[F4]GENERAL_READ : User data may be read from the TOE by any user, except cardholder identification data which may be read from control cards and company cards by VEHICLE_UNIT only.**]**

IDENTIF_WRITE : Identification data may only be written once and before the end of phase 6 of card's life-cycle. No user may write or modify identification data during end-usage phase of card's life-cycle.

ACTIVITY_WRITE: Activity data may be written to the TOE by VEHICLE_UNIT only.

SOFT_UPGRADE : No user may upgrade TOE's software.

FILE_STRUCTURE: Files structure and access conditions shall be created before end of phase 6 of TOE's life-cycle and then locked from any future modification or deletion by any user.

4.4. Accountability

The TOE shall hold permanent identification data.

There shall be an indication of the time and date of the TOE's personalisation. This indication shall remain unalterable.

4.5. Audit

The TOE must monitor events that indicate a potential violation of its security.

**Assignment** (FAU_SAA.1.2) Subset of defined auditable events:

— cardholder authentication failure (5 consecutive unsuccessful PIN checks),
— self test error,
— stored data integrity error,
— activity data input integrity error.

4.6. Accuracy

4.6.1. Stored data integrity

**Assignment** (FDP_SDI.2.2) *Actions to be taken*: warn the entity connected,

4.6.2. Basic data authentication

**Assignment** (FDP_DAU.1.1) *List of objects or information types*: activity data.

**Assignment** (FDP_DAU.1.2) *List of subjects*: any.

4.7. Reliability of service

4.7.1. Tests

**Selection** (FPT_TST.1.1): during initial start-up, periodically during normal operation.

Note: during initial start-up means before code is executed (and not necessarily during Answer To Reset procedure).

The TOE's self tests shall include the verification of the integrity of any software code not stored in ROM.

Upon detection of a self test error the TSF shall warn the entity connected.

After OS testing is completed, all testing-specific commands and actions shall be disabled or removed. It shall not be possible to override these controls and restore them for use. Command associated exclusively with one life cycle state shall never be accessed during another state.

4.7.2. Software

There shall be no way to analyse, debug or modify TOE's software in the field.

Inputs from external sources shall not be accepted as executable code.

4.7.3. Power supply

The TOE shall preserve a secure state during power supply cut-off or variations.

4.7.4. Reset conditions

If power is cut (or if power variations occur) from the TOE, or if a transaction is stopped before completion, or on any other reset conditions, the TOE shall be reset cleanly.

4.8. Data exchange

4.8.1. Data exchange with a vehicle unit

The TOE shall verify the integrity and authenticity of data imported from a vehicle unit.

Upon detection of an imported data integrity error, the TOE shall:
— warn the entity sending the data,
— not use the data.

The TOE shall export user data to the vehicle unit with associated security attributes, such that the vehicle unit will be able to verify the integrity and authenticity of data received.

4.8.2. Export of data to a non-vehicle unit (download function)

The TOE shall be able to generate an evidence of origin for data downloaded to external media.

The TOE shall be able to provide a capability to verify the evidence of origin of downloaded data to the recipient.

The TOE shall be able to download data to external storage media with associated security attributes such that downloaded data integrity can be verified.

4.9. Cryptographic support

If the TSF generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes. Generated cryptographic session keys shall have a limited (TBD by manufacturer and not more than 240) number of possible use.

If the TSF distributes cryptographic keys, it shall be in accordance with specified cryptographic key distribution methods.**]]**

**Changes to legislation:**
There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85, Division 4..