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

[^{F1}]^{F2}ANNEX 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).

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

Appendix 10

GENERIC SECURITY TARGETS

VEHICLE UNIT GENERIC SECURITY TARGET

- 4. Security enforcing functions
 - 4.1. Identification and authentication
 - 4.1.1. Motion sensor identification and authentication

The VU shall be able to establish, for every interaction, the identity of the motion sensor it is connected to.

The identity of the motion sensor shall consist of the sensor approval number and the sensor serial number.

The VU shall authenticate the motion sensor it is connected to:

- at motion sensor connection,
- at each calibration of the recording equipment,
- at power supply recovery.

Authentication shall be mutual and triggered by the VU.

The VU shall periodically (period TBD by manufacturer and more frequently than once per hour) re-identify and re-authenticate the motion sensor it is connected to, and ensure that the motion sensor identified during the last calibration of the recording equipment has not been changed.

The VU shall detect and prevent use of authentication data that has been copied and replayed.

After (TBD by manufacturer and not more than 20) 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 SEF 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.

- 4.1.2. User identification and authentication

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.

The user identity shall consist of:

- a user group:
 - DRIVER (driver card),
 - CONTROLLER (control card),
 - WORKSHOP (workshop card),
 - COMPANY (company card),
 - UNKNOWN (no card inserted),
- a user ID, composed of:
 - the card issuing Member State code and of the card number,

— UNKNOWN if user group is UNKNOWN.

UNKNOWN identities may be implicitly or explicitly known.

The VU shall authenticate its users at card insertion.

The VU shall re-authenticate its users:

- at power supply recovery,
- periodically or after occurrence of specific events (TBD by manufacturers and more frequently than once per day).

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.

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.

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.

The VU shall detect and prevent use of authentication data that has been copied and replayed.

After 5 consecutive unsuccessful authentication attempts have been detected, the SEF shall:

- 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).

4.1.3. Remotely connected company identification and authentication

Company remote connection capability is optional. This paragraph therefore applies only if this feature is implemented.

For every interaction with a remotely connected company, the VU shall be able to establish the company's identity.

The remotely connected company's identity shall consist of its company card issuing Member State code and of its company card number.

The VU shall successfully authenticate the remotely connected company before allowing any data export to it.

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.

The VU shall detect and prevent use of authentication data that has been copied and replayed.

After 5 consecutive unsuccessful authentication attempts have been detected, the VU shall:

- warn the remotely connected company.

4.1.4. Management device identification and authentication

VU manufacturers may foresee dedicated devices for additional VU management functions (e.g. Software upgrading, security data reloading, ...). This paragraph therefore applies only if this feature is implemented.

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

For every interaction with a management device, the VU shall be able to establish the device identity.

Before allowing any further interaction, the VU shall successfully authenticate the management device.

The VU shall detect and prevent use of authentication data that has been copied and replayed.

4.2. Access control

Access controls ensure that information is read from, created in, or modified into the TOE only by those authorised to do so.

It must be noted that the user data recorded by the VU, although presenting privacy or commercial sensitivity aspects, are not of a confidential nature. Therefore, the functional requirement related to data read access rights (requirement 011) is not the subject of a security enforcing function.

4.2.1. Access control policy

The VU shall manage and check access control rights to functions and to data.

4.2.2. Access rights to functions

The VU shall enforce the mode of operation selection rules (requirements 006 to 009).

The VU shall use the mode of operation to enforce the functions access control rules (requirement 010).

4.2.3. Access rights to data

The VU shall enforce the VU identification data write access rules (requirement 076)

The VU shall enforce the paired motion sensor identification data write access rules (requirements 079 and 155)

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).

After the VU activation, the VU shall enforce calibration data write and delete access rules (requirement 097).

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).

After the VU activation, the VU shall enforce time adjustment data write and delete access rules (requirement 100).

The VU shall enforce appropriate read and write access rights to security data (requirement 080).

4.2.4. File structure and access conditions

Application and data files structure and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion.

4.3. Accountability

The VU shall ensure that drivers are accountable for their activities (requirements 081, 084, 087, 105a, 105b, 109 and 109a).

The VU shall hold permanent identification data (requirement 075).

The VU shall ensure that workshops are accountable for their activities (requirements 098, 101 and 109).

The VU shall ensure that controllers are accountable for their activities (requirements 102, 103 and 109).

The VU shall record odometer data (requirement 090) and detailed speed data (requirement 093).

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.

The VU shall ensure that it does not modify data already stored in a tachograph card (requirements 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.

4.4. Audit

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 to security.

The VU shall, for events impairing the security of the VU, record those events with associated data (requirements 094, 096 and 109).

The events affecting the security of the VU are the following:

- Security breach attempts,
 - motion sensor authentication failure,
 - tachograph card authentication failure,
 - unauthorised change of motion sensor,
 - card data input integrity error,
 - stored user data integrity error,
 - internal data transfer error,
 - unauthorised case opening,
 - hardware sabotage,
- last card session not correctly closed,
- motion data error event,
- power supply interruption event,
- VU internal fault.

The VU shall enforce audit records storage rules (requirement 094 and 096).

The VU shall store audit records generated by the motion sensor in its data memory.

It shall be possible to print, display and download audit records.

4.5. Object re-use

The VU shall ensure that temporary storage objects can be re-used without this involving inadmissible information flow.

4.6. Accuracy

4.6.1. Information flow control policy

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

The VU shall ensure that user data related to requirements 081, 084, 087, 090, 093, 102, 104, 105, 105a and 109 may only be processed from the right input sources:

- vehicle motion data,
- VU's real time clock,
- recording equipment calibration parameters,
- tachograph cards,
- user's inputs.

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).

4.6.2. Internal data transfers

The requirements of this paragraph apply only if the VU makes use of physically separated parts.

If data are transferred between physically separated parts of the VU, the data shall be protected from modification.

Upon detection of a data transfer error during an internal transfer, transmission shall be repeated and the SEF shall generate an audit record of the event.

4.6.3. Stored data integrity

The VU shall check user data stored in the data memory for integrity errors.

Upon detection of a stored user data integrity error, the SEF shall generate an audit record.

4.7. Reliability of service

4.7.1. Tests

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. It shall not be possible to restore them for later use.

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).

Upon detection of an internal fault during self test, the SEF shall:

- generate an audit record (except in calibration mode) (VU internal fault),
- Preserve the stored data integrity.

4.7.2. Software

There shall be no way to analyse or debug software in the field after the VU activation.

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

4.7.3. Physical protection

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 six months. In such a case, the SEF shall generate an audit record (It is acceptable that the audit record is generated and stored after power supply reconnection).

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).

After its activation, the VU shall detect specified (TBD by manufacturer) hardware sabotage.

In the case described above, the SEF shall generate an audit record and the VU shall: (TBD by manufacturer).

4.7.4. Power supply interruptions

The VU shall detect deviations from the specified values of the power supply, including cut-off.

In the case described above, the SEF shall:

- 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.

4.7.5. Reset conditions

In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset conditions, the VU shall be reset cleanly.

4.7.6. Data availability

The VU shall ensure that access to resources is obtained when required and that resources are not requested nor retained unnecessarily.

The VU must ensure that cards cannot be released before relevant data have been stored to them (requirements 015 and 016)

In the case described above, the SEF shall generate an audit record of the event.

4.7.7. Multiple applications

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.

4.8. Data exchange

This paragraph addresses data exchange between the VU and connected devices.

4.8.1. Data exchange with motion sensor

The VU shall verify the integrity and authenticity of motion data imported from the motion sensor

Upon detection of a motion data integrity or authenticity error, the SEF shall:

- generate an audit record,
- continue to use imported data.

4.8.2. Data exchange with tachograph cards

The VU shall verify the integrity and authenticity of data imported from tachograph cards.

Upon detection of card data integrity or authenticity error, the VU shall:

- generate an audit record,
- not use the data.

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

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.

4.8.3. Data exchange with external storage media (downloading function)

The VU shall generate an evidence of origin for data downloaded to external media.

The VU shall provide a capability to verify the evidence of origin of downloaded data to the recipient.

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

4.9. Cryptographic support

The requirements of this paragraph are applicable only where needed, depending upon security mechanisms used and upon the manufacturer's solutions.

Any cryptographic operation performed by the VU shall be in accordance with a specified algorithm and a specified key size.

If the VU generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes.

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

If the VU accesses cryptographic keys, it shall be in accordance with specified cryptographic keys access methods.

If the VU destroys cryptographic keys, it shall be in accordance with specified cryptographic keys destruction methods.]]

Changes to legislation:

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