Council Regulation (EEC) No 3821/85 of 20 December 1985 on recording equipment in road transport

[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 7

DATA DOWNLOADING PROTOCOLS

3. TACHOGRAPH CARDS DOWNLOADING PROTOCOL

3.1. Scope

This paragraph describes the direct card data downloading of a tachograph card to an IDE. The IDE is not part of the secure environment; therefore no authentication between the card and the IDE is performed.

3.2. Definitions

Download session : Each time a download of the ICC data is performed. The session covers the complete procedure from the reset of the ICC by an IFD until the deactivation of the ICC (withdraw of the card or next reset).

Signed data file : A file from the ICC. The file is transferred to the IFD in plain text. On the ICC the file is hashed and signed and the signature is transferred to the IFD.

3.3. Card downloading

The download of a tachograph card includes the following steps:

- download the common information of the card in the EFs *ICC* and *IC*. This information is optional and is not secured with a digital signature,
- Download the EFs Card_Certificate and CA_Certificate. This information is not secured with a digital signature,

  It is mandatory to download these files for each download session.
- download the other application data EFs (within Tachograph DF) except EF Card_Download. This information is secured with a digital signature,
  - it is mandatory to download at least the EFs Application_Identification and ID for each download session,
  - when downloading a driver card it is also mandatory to download the following EFs:
    - Events_Data,
    - Faults_Data,
    - Driver_Activity_Data,
    - Vehicles_Used,
    - Places,
    - Control_Activity_Data,
    - Specific_Conditions.
- When downloading a driver card, update the LastCardDownload date in EF Card_Download,
- When downloading a workshop card, reset the calibration counter in EF Card_Download.

3.3.1. Initialisation sequence

The IDE shall initiate the sequence as follows:

Card	Direction	IDE/IFD	Meaning/Remarks
	⇦	Hardware reset	
ATR	⇨		

It is optional to use PPS to switch to a higher baudrate as long as the ICC supports it.

3.3.2. Sequence for unsigned data files

The sequence to download the *ICC*, *IC*, *Card_Certificate* and *CA_Certificate* is as follows:

Card	Direction	IDE/IFD	Meaning/Remarks
	⇦	Select file	Select file select by file identifiers
OK	⇨		
	⇦	Read Binary	If the file contains more data than the buffer size of the reader or the card the command has to be repeated until the complete file is read.
File data OK	⇨	Store data to ESM	according to 3.4, (Data storage format)

Note: Before selecting the *Card_Certificate* EF, the Tachograph Application must be selected (selection by AID).

3.3.3. Sequence for signed data files

The following sequence shall be used for each of the following files that has to be downloaded with their signature:

Card	Direction	IDE/IFD	Meaning/Remarks
	⇦	Select File	
OK	⇨		
	⇦	Perform hash of File	Calculates the hash value over the data content of the selected file using the prescribed hash algorithm in accordance with Appendix 11. This

			command is not an ISO-Command.
Calculate hash of file and store hash value temporarily			
OK	⇨		
	⇦	Read Binary	If the file contains more data than the buffer of the reader or the card can hold, the command has to be repeated until the complete file is read.
File Data OK	⇨	Store received data to ESM	according to 3.4, (Data storage format)
	⇦	PSO: Compute digital signature	
Perform security operation ‘compute digital signature’ using the temporarily stored hash value			
Signature OK	⇨	Append data to the previous stored data on the ESM	according to 3.4, (Data storage format)

3.3.4. Sequence for resetting the calibration counter

The sequence to reset the *NoOfCalibrationsSinceDownload* counter in the EF *Card_Download* in a workshop card is the following:

Card	**Direction**	**IDE/IFD**	**Meaning/Remarks**
	⇦	Select File EF *Card_Download*	Select by file identifiers
OK	⇨		
	⇦	Update Binary *NoOfCalibrationsSinceDownload* = ′00 00′	
Resets card download number			
OK	⇨		

3.4. Data storage format

3.4.1. Introduction

The downloaded data has to be stored according to the following conditions:

— the data shall be stored transparent. This means that the order of the bytes as well as the order of the bits inside the byte that are transferred from the card has to be preserved during storage,

— all files of the card downloaded within a download session are stored in one file on the ESM.

3.4.2. File format

The file format is a concatenation of several TLV objects.

The tag for an EF shall be the FID plus the appendix ‘00’.

The tag of an EF's signature shall be the FID of the file plus the appendix ‘01’.

The length is a two byte value. The value defines the number of bytes in the value field. The value ‘FF FF’ in the length field is reserved for future use.

When a file is not downloaded nothing related to the file shall be stored (no tag and no zero length).

A signature shall be stored as the next TLV object directly after the TLV object that contains the data of the file.

Definition	**Meaning**	**Length**
FID (2 Bytes) || ‘00’	Tag for EF (FID)	3 Bytes
FID (2 Bytes) || ‘01’	Tag for Signature of EF(FID)	3 Bytes
xx xx	Length of value field	2 Bytes

Example of data in a download file on an ESM:

Tag	**Length**	**Value**
00 02 00	*00 11*	Data of EF *ICC*
C1 00 00	*00 C2*	Data of EF *Card_Certificate*
		…
05 05 00	*0A 2E*	Data of EF *Vehicles_Used*
05 05 01	*00 80*	Signature of EF *Vehicles_Used**]]***

Changes to legislation:
There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85, Division 3..