[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).

Appendix 2

TACHOGRAPH CARDS SPECIFICATION

3. HARDWARE AND COMMUNICATION

3.6. Commands description

3.6.3. Update Binary

This command is compliant with ISO/IEC 7816-4, but has a restricted usage compared to the command defined in the norm.

The UPDATE BINARY command message initiates the update (erase + write) of the bits already present in an EF binary with the bits given in the command APDU.

The command can be performed only if the security status satisfies the security attributes defined for the EF for the UPDATE function (If the access control of the UPDATE function includes PRO SM, a secure messaging must be added in the command).

3.6.3.1. Command without secure messaging

This command enables the IFD to write data into the EF currently selected, without the card verifying the integrity of data received. This plain mode is allowed only if the related file is not marked as ‘Encrypted’.

COMMAND MESSAGE

Byte	Length	Value	Description
CLA	1	′00h′	No secure messaging asked
INS	1	′D6h′	
P1	1	′XXh′	Offset in bytes from the beginning of the file: most significant byte
P2	1	′XXh′	Offset in bytes from the beginning of the file: least significant byte
Lc	1	′NNh′	Lc length of data to Update. Number of bytes to be written
#6-#(5+NN)	NN	′XX..XXh′	Data to be written

Note: bit 8 of P1 must be set to 0.

RESPONSE MESSAGE

Byte	Length	Value	Description

SW	2	'XXXXh'	Status words (SW1, SW2)

— If the command is successful, the card returns '9000',
— if no EF is selected, the processing state returned is '6986',
— if the Access Control of the selected file are not satisfied, the command is interrupted with '6982',
— if the Offset is not compatible with the size of the EF (Offset > EF size), the processing state returned is '6B00',
— if the size of the data to be written is not compatible with the size of the EF **[**[F3](Offset + Lc > EF size)**]** the processing state returned is '6700',
— if an integrity error is detected within the file attributes, the card shall consider the file as corrupted and unrecoverable, the processing state returned is '6400' or '6500',
— if writing is unsuccessful, the processing state returned is '6581'.

Textual Amendments

F3 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).

3.6.3.2. Command with secure messaging

This command enables the IFD to write data into the EF currently selected, with the card verifying the integrity of data received. As no confidentiality is required, the data are not encrypted.

COMMAND MESSAGE

Byte	Length	Value	Description
CLA	1	'0Ch'	Secure messaging. Asked
INS	1	'D6h'	INS
P1	1	'XXh'	Offset in bytes from the beginning of the file: most significant byte
P2	1	'XXh'	Offset in bytes from the beginning of the file: least significant byte
Lc	1	'XXh'	Length of the secured data field
#6	1	'81h'	T_{PV}: tag for plain value data
#7	L	'NNh' or '81 NNh'	L_{PV}: length of transmitted data

			L is 2 bytes if L_{PV}> 127 bytes
#(7+L)-#(6+L+NN)	NN	′XX..XXh′	Plain data value (data to be written)
#(7+L+NN)	1	′8Eh′	T_{CC}: tag for cryptographic checksum
#(8+L+NN)	1	′04h′	L_{CC}: Length of following cryptographic checksum
#(9+L+NN)-#(12+L+NN)	4	′XX..XXh′	Cryptographic checksum (4 most significant bytes)
Le	1	′00h′	As specified in ISO/IEC 7816-4

RESPONSE MESSAGE IF CORRECT SECURE MESSAGING INPUT FORMAT

Byte	**Length**	**Value**	**Description**
#1	1	′99h′	T_{SW}: tag for status words (to be protected by CC)
#2	1	′02h′	L_{SW}: length of returned status words
#3-#4	2	′XXXXh′	Status words (SW1, SW2)
#5	1	′8Eh′	T_{CC}: tag for cryptographic checksum
#6	1	′04h′	L_{CC}: Length of following cryptographic checksum
#7-#10	4	′XX..XXh′	Cryptographic checksum (4 most significant bytes)
SW	2	′XXXXh′	Status words (SW1, SW2)

The ‘regular’ processing states, described for the UPDATE BINARY command with no secure messaging (see point 3.6.3.1), can be returned using the response message structure described above.

Additionally, some errors specifically related to secure messaging can happen. In that case, the processing state is simply returned, with no secure messaging structure involved:

RESPONSE MESSAGE IF ERROR IN SECURE MESSAGING

Byte	Length	Value	Description
SW	2	′XXXXh′	Status Words (SW1, SW2)

— If no current session key is available, the processing state ′6A88′ is returned,

— if some expected data objects (as specified above) are missing in the secure messaging format, the processing state ′6987′ is returned: this error happens if an expected tag is missing or if the command body is not properly constructed,

— if some data objects are incorrect, the processing state returned is ′6988′: this error happens if all the required tags are present but some lengths are different from the ones expected,

— if the verification of the cryptographic checksum fails, the processing state returned is ′6688′.**]]**

Changes to legislation:
There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85, Division 3.6.3..