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 11

COMMON SECURITY MECHANISMS

5. VU-CARDS DATA TRANSFER CONFIDENTIALITY, INTEGRITY AND AUTHENTICATION MECHANISMS

5.1. Secure messaging

VU-cards data transfers integrity shall be protected through Secure Messaging in accordance with references (ISO/IEC 7816-4) and (ISO/IEC 7816-8).

When data need to be protected during transfer, a cryptographic checksum data object shall be appended to the data objects sent within the command or the response. The cryptographic checksum shall be verified by the receiver.

The cryptographic checksum of data sent within a command shall integrate the command header, and all data objects sent (= > CLA = ′0C′, and all data objects shall be encapsulated with tags in which b1 = 1).

The response status-information bytes shall be protected by a cryptographic checksum when the response contains no data field.

Cryptographic checksums shall be four bytes long.

The structure of commands and responses when using secure messaging is therefore the following:

The DOs used are a partial set of the Secure Messaging DOs described in ISO/IEC 7816-4:

Tag	**Mnemonic**	**Meaning**
′81′	T_{PV}	Plain Value not BER-TLV coded data (to be protected by CC)
′97′	T_{LE}	Value of Le in the unsecured command (to be protected by CC)
′99′	T_{SW}	Status-Info (to be protected by CC)
′8E′	T_{CC}	Cryptographic Checksum
′87′	$T_{PI\ CG}$	Padding Indicator Byte || Cryptogram (Plain Value not coded in BER-TLV)

Given an unsecured command response pair:

Command header	**Command body**
CLA INS P1 P2	(L_c-field) (Data field) (L_e-field)
four bytes	L bytes, denoted as B_1 to B_L

Response body	**Response trailer**	
(Data field)	SW1	SW2
L_r data bytes	two bytes	

The corresponding secured command response pair is:

Secured command:

Command header (CH)	**Command body**										
CLA INS P1 P2	(New L_c field)	(New Data field)									(New L_e field)
′OC′	Length of new data field	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	′00′
		′81′	L_c	Data field	′97′	′01′	L_e	′8E′	′04′	CC	

Data to be integrated in checksum = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} L_e || PB

[[X1]PB = padding bytes (80.. 00) in accordance with ISO-IEC 7816-4 and ISO 9797 method 2**]**

DOs PV and LE are present only when there is some corresponding data in the unsecured command.

Secured response:

1. Case where response data field is not empty and needs not to be protected for confidentiality:

Response body						**Response trailer**
(New data field)						new SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
′81′	L_r	Data field	′8E′	′04′	CC	

Data to be integrated in checksum = T_{PV} || L_{PV} || PV || PB

2. Case where response data field is not empty and needs to be protected for confidentiality:

Response body	**Response trailer**

(New data field)						new SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Data to be carried by CG: non BER-TLV coded data and padding bytes.

Data to be integrated in checksum = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG PB

3. Case where response data field is empty:

Response body						**Response trailer**
(New data field)						new SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	New SW1 SW2	'8E'	'04'	CC	

Data to be integrated in checksum = T_{SW} || L_{SW} || SW || PB

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).

5.2. Treatment of secure messaging errors

When the tachograph card recognises an SM error while interpreting a command, then the status bytes must be returned without SM. In accordance with ISO/IEC 7816-4, the following status bytes are defined to indicate SM errors:

'66 88' : verification of cryptographic checksum failed,
'69 87' : expected SM data objects missing,
'69 88' : SM data objects incorrect.

When the tachograph card returns status bytes without SM DOs or with an erroneous SM DO, the session must be aborted by the VU.

5.3. Algorithm to compute cryptographic checksums

Cryptographic checksums are built using a retail MACs in accordance with ANSI X9.19 with DES:

— initial stage: the initial check block y0 is E(Ka, SSC).
— sequential stage: the check blocks y1, …, yn are calculated using Ka.

— final stage: the cryptographic checksum is calculated from the last check block yn as follows: E(Ka, D(Kb, yn)).

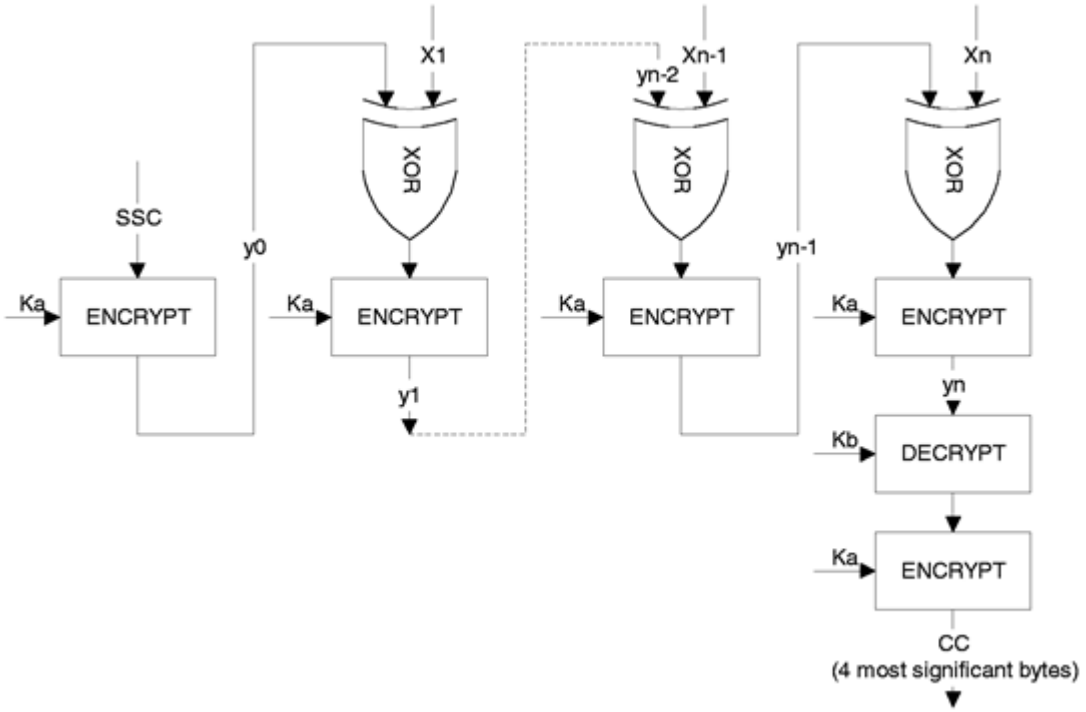
where E() means encryption with DES, and D() means decryption with DES.

The four most significant bytes of the cryptographic checksum are transferred

The send sequence counter (SSC) shall be initiated during key agreement procedure to:
Initial SSC: Rnd3 (4 least significant bytes) || Rnd1 (4 least significant bytes).

The send sequence counter shall be increased by 1 each time before a MAC is calculated (i.e. the SSC for the first command is Initial SSC + 1, the SSC for the first response is Initial SSC + 2).

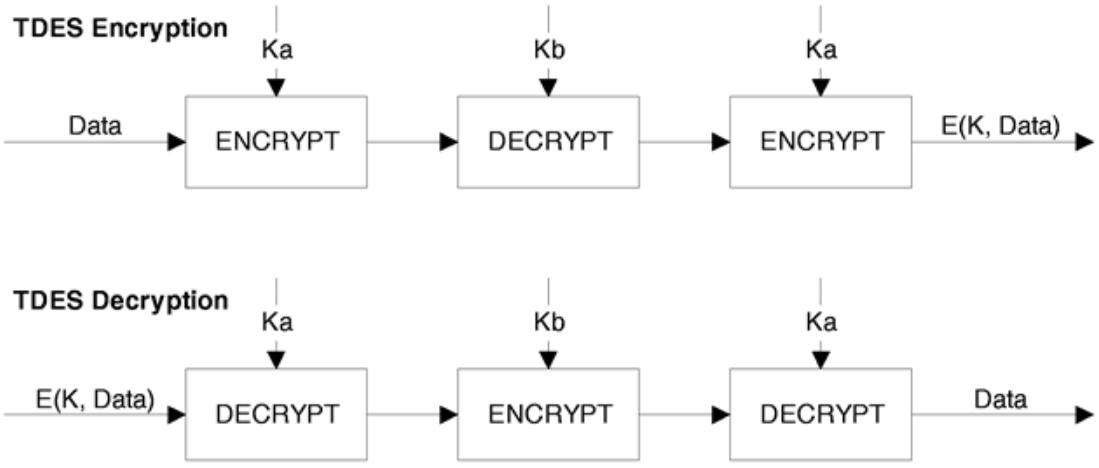
The following figure shows the calculation of the retail MAC:



5.4. Algorithm to compute cryptograms for confidentiality DOs

Cryptograms are computed using TDEA in TCBC mode of operation in accordance with references (TDES) and (TDES-OP) and with the Null vector as Initial Value block.

The following figure shows the application of keys in TDES:



]]

Changes to legislation:
There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85, Division 5..