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

6. DATA DOWNLOAD DIGITAL SIGNATURE MECHANISMS

The intelligent dedicated equipment (IDE) stores data received from an equipment (VU or card) during one download session within one physical data file. This file must contain the certificates MS_i.C and EQT.C. The file contains digital signatures of data blocks as specified in Appendix 7 Data Downloading Protocols.

Digital signatures of downloaded data shall use a digital signature scheme with appendix such, that downloaded data may be read without any decipherment if desired.

6.1. Signature generation

Data signature generation by the equipment shall follow the signature scheme with appendix defined in reference (PKCS1) with the SHA-1 hash function:

Signature = EQT.SK[′00′ || ′01′ || *PS* || ′00′ || DER(SHA-1(Data))]

PS = Padding string of octets with value ′FF′ such that length is 128.

DER(SHA-1(*M*)) is the encoding of the algorithm ID for the hash function and the hash value into an ASN.1 value of type *DigestInfo* (distinguished encoding rules):

′30′||′21′||′30′||′09′||′06′||′05′||′2B′||′0E′||′03′||′02′||′1A′||′05′||′00′||′04′||′14′|| Hash Value.

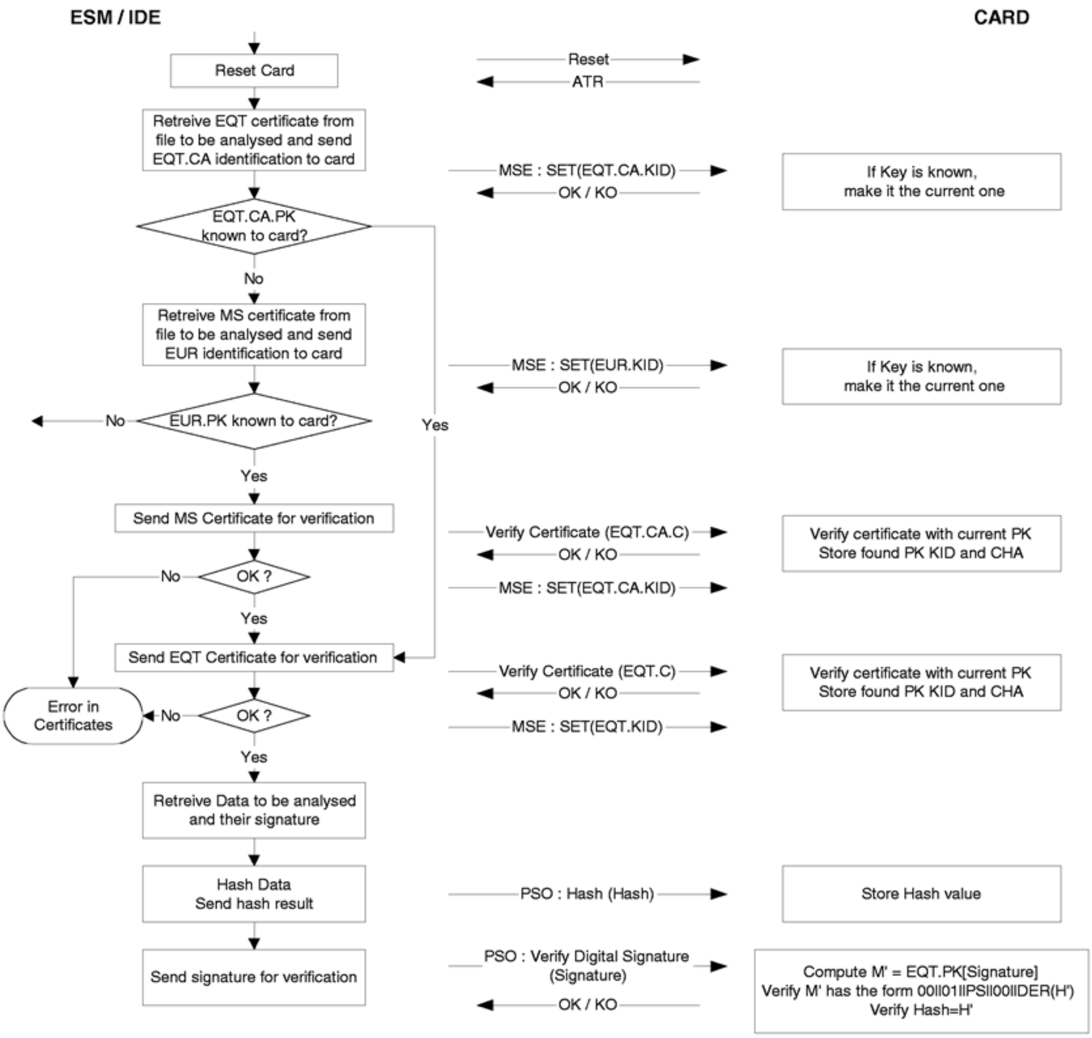
6.2. Signature verification

Data signature verification on downloaded data shall follow the signature scheme with appendix defined in reference (PKCS1) with the SHA-1 hash function.

The European public key EUR.PK needs to be known independently (and trusted) by the verifier.

The following table illustrates the protocol an IDE carrying a Control card can follow to verify the integrity of data downloaded and stored on the ESM (external storage media). The control card is used to perform the decipherement of digital signatures. This function may in this case not be implemented in the IDE.

The equipment that has downloaded and signed the data to be analysed is denoted EQT.


ESM / IDE
CARD
Reset Card
Reset
ATR
Retreive EQT certificate from file to be analysed and send EQT.CA identification to card
MSE : SET(EQT.CA.KID)
OK / KO
If Key is known, make it the current one
EQT.CA.PK known to card?
No
Yes
Retreive MS certificate from file to be analysed and send EUR identification to card
MSE : SET(EUR.KID)
OK / KO
If Key is known, make it the current one
No
EUR.PK known to card?
Yes
Send MS Certificate for verification
Verify Certificate (EQT.CA.C)
OK / KO
MSE : SET(EQT.CA.KID)
Verify certificate with current PK Store found PK KID and CHA
No
OK ?
Yes
Send EQT Certificate for verification
Verify Certificate (EQT.C)
OK / KO
MSE : SET(EQT.KID)
Verify certificate with current PK Store found PK KID and CHA
Error in Certificates
No
OK ?
Yes
Retreive Data to be analysed and their signature
Hash Data Send hash result
PSO : Hash (Hash)
Store Hash value
Send signature for verification
PSO : Verify Digital Signature (Signature)
OK / KO
Compute M' = EQT.PK[Signature] Verify M' has the form 00||01||PS||00||DER(H') Verify Hash=H'

]]

Changes to legislation:
There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85, Division 6..