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

3. KEYS AND CERTIFICATES

3.1. Keys generation and distribution

3.1.1. RSA keys generation and distribution

RSA keys shall be generated through three functional hierarchical levels:

— European level,

— Member State level,

— Equipment level.

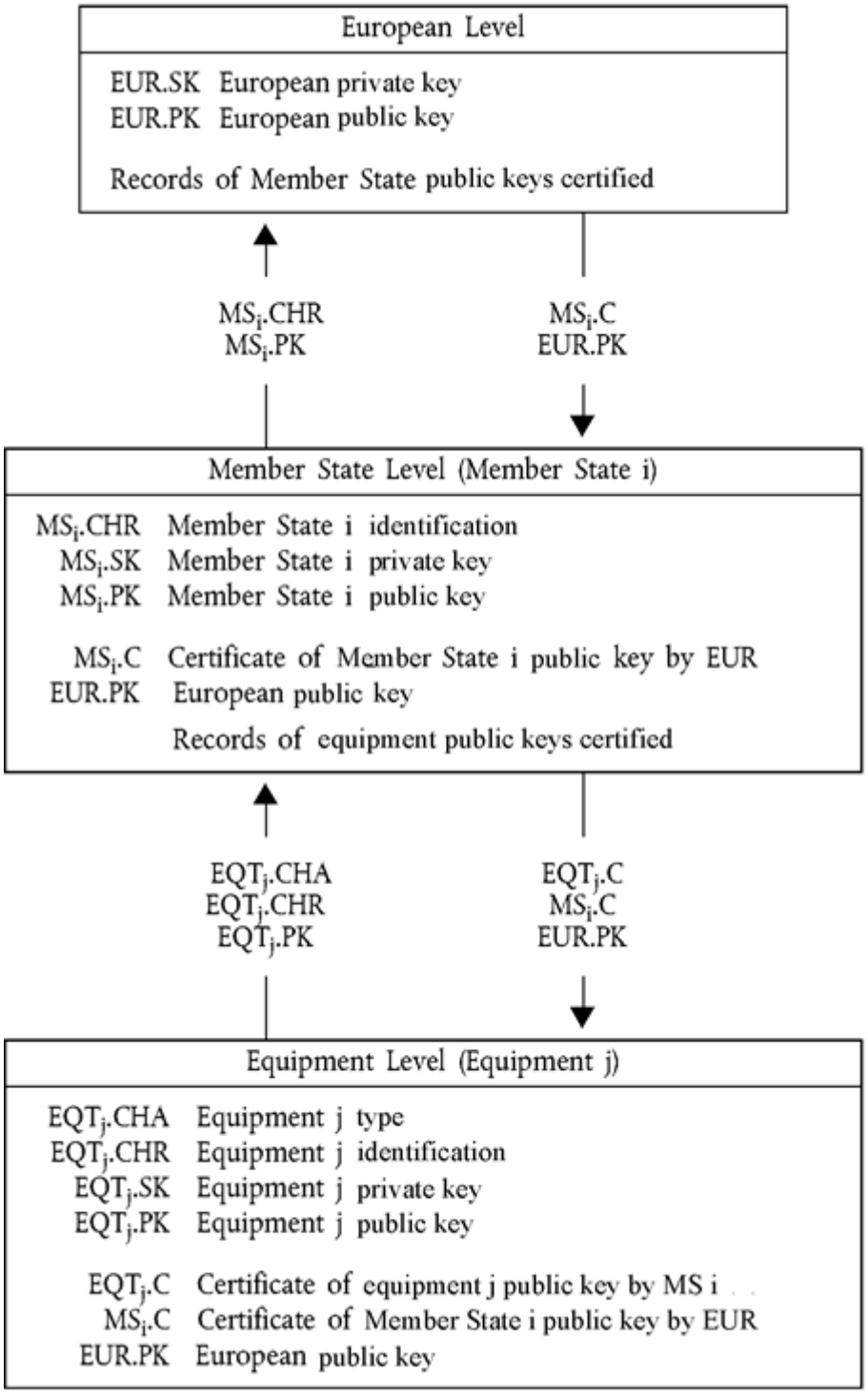
At European level, a single European key pair (EUR.SK and EUR.PK) shall be generated. The European private key shall be used to certify the Member States public keys. Records of all certified keys shall be kept. These tasks shall be handled by a European certification authority, under the authority and responsibility of the European Commission.

At Member State level, a Member State key pair (MS.SK and MS.PK) shall be generated. Member States public keys shall be certified by the European Certification Authority. The Member State private key shall be used to certify public keys to be inserted in equipment (vehicle unit or tachograph card). Records of all certified public keys shall be kept with the identification of the equipment to which it is intended. These tasks shall be handled by a Member State certification authority. A Member State may regularly change its key pair.

At equipment level, one single key pair (EQT.SK and EQT.PK) shall be generated and inserted in each equipment. Equipment public keys shall be certified by a Member State certification authority. These tasks may be handled by equipment manufacturers, equipment personalisers or Member State authorities. This key pair is used for authentication, digital signature and encipherement services

Private keys confidentiality shall be maintained during generation, transport (if any) and storage.

The following picture summarises the data flow of this process:



3.1.2. RSA test keys

For the purpose of equipment testing (including interoperability tests) the European certification authority shall generate a different single European test key pair and at least two Member State test key pairs, the public keys of which shall be certified with the European private test key. Manufacturers shall insert, in equipment undergoing type approval tests, test keys certified by one of these Member State test keys.

3.1.3. Motion sensor keys

The confidentiality of the three TDES keys described below shall be appropriately maintained during generation, transport (if any) and storage.

In order to support recording equipment compliant with ISO 16844, the European certification authority and the Member State certification authorities shall, in addition, ensure the following:

The European certification authority shall generate Km_{VU} and Km_{WC}, two independent and unique Triple DES keys, and generate Km as:

$$Km = Km_{VU} \text{ XOR } Km_{WC}$$

The European certification authority shall forward these keys, under appropriately secured procedures, to Member States certification authorities at their request.

Member States certification authorities shall:

— use Km to encrypt motion sensor data requested by motion sensor manufacturers (data to be encrypted with Km is defined in ISO 16844-3),

— forward Km_{VU} to vehicle unit manufacturers, under appropriately secured procedures, for insertion in vehicle units,

— ensure that Km_{WC} will be inserted in all workshop cards (*SensorInstallationSecData* in *Sensor_Installation_Data* elementary file) during card personalisation.

3.1.4. T-DES session keys generation and distribution

Vehicle units and tachograph cards shall, as a part of the mutual authentication process, generate and exchange necessary data to elaborate a common Triple DES session key. This exchange of data shall be protected for confidentiality through an RSA crypt-mechanism.

This key shall be used for all subsequent cryptographic operations using secure messaging. Its validity shall expire at the end of the session (withdrawal of the card or reset of the card) and/or after 240 use (one use of the key = one command using secure messaging sent to the card and associated response).

3.2. Keys

RSA keys shall have (whatever the level) the following lengths: modulus *n* 1024 bits, public exponent *e* 64 bits maximum, private exponent *d* 1024 bits.

Triple DES keys shall have the form (K_a, K_b, K_a) where K_a and K_b are independent 64 bits long keys. No parity error detecting bits shall be set.

3.3. Certificates

RSA Public key certificates shall be ‘non self-descriptive’‘Card Verifiable’ certificates (Ref.: ISO/IEC 7816-8)

3.3.1. Certificates content

RSA Public key certificates are built with the following data in the following order:

Data	Format	Bytes	Obs
CPI	INTEGER	1	Certificate profile identifier (′01′ for this version)
CAR	OCTET STRING	8	Certification authority reference
CHA	OCTET STRING	7	Certificate holder authorisation
EOV	TimeReal	4	Certificate end of validity. Optional, ′FF ′ padded if not used
CHR	OCTET STRING	8	Certificate holder reference
n	OCTET STRING	128	Public key (modulus)
e	OCTET STRING	8	Public key (public exponent)
		164	

Notes:

1. The ‘Certificate Profile Identifier’ (CPI) delineates the exact structure of an authentication certificate. It can be used as an equipment internal identifier of a relevant headerlist which describes the concatenation of Data Elements within the certificate.

The headerlist associated with this certificate content is as follows:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Extended headerlist Tag	Length of header list	CPI Tag	CPI Length	CAR Tag	CAR Length	CHA Tag	CHA Length	EOV Tag	EOV Length	CHR Tag	CHR Length	Public key Tag (constructed)	Length of subsequent DOs	modulus Tag	modulus length	public exponent Tag	public exponent length

2. The ‘Certification Authority Reference’ (CAR) has the purpose of identifying the certificate issuing CA, in such a way that the data element can be used at the same time as an authority key identifier to reference the public key of the certification authority (for coding, see Key Identifier below).

3. The ‘Certificate Holder Authorisation’ ((CHA) is used to identify the rights of the certificate holder. It consists of the Tachograph Application ID and of the type of equipment to which the certificate is intended (according to EquipmentType data element, ‘00’ for a Member State).

4. ‘Certificate Holder Reference’ (CHR) has the purpose of identifying uniquely the certificate holder, in such a way that the Data Element can be used at the same time as a Subject Key Identifier to reference the Public Key of the certificate holder.

5. Key Identifiers uniquely identify certificate holder or certification authorities. They are coded as follows:

5.1. Equipment (VU or Card):

Data	**Equipment serial number**	**Date**	**Type**	**Manufacturer**
Length	4 Bytes	2 Bytes	1 Byte	1 Byte
Value	Integer	mm yy BCD coding	Manufacturer specific	Manufacturer code

In the case of a VU, the manufacturer, when requesting certificates, may or may not know the identification of the equipment in which the keys will be inserted.

In the first case, the manufacturer will send the equipment identification with the public key to its Member State authority for certification. The certificate will then contain the equipment identification, and the manufacturer must ensure that keys and certificate are inserted in the intended equipment. The Key identifier has the form shown above.

In the later case, the manufacturer must uniquely identify each certificate request and send this identification with the public key to its Member State authority for certification. The certificate will contain the request identification. The manufacturer must feed back its Member State authority with the assignment of key to equipment (i.e. certificate request identification, equipment identification) after key installation in the equipment. The key identifier has the following form:

Data	**Certificate request serial number**	**Date**	**Type**	**Manufacturer**
Length	4 Bytes	2 Bytes	1 Byte	1 Byte
Value	**[**[F3]Integer**]**	**[**[X1]mm yy BCD coding**]**	′FF′	Manufacturer code

5.2. Certification Authority:

Data	**Authority identification**	**Key serial number**	**Additional info**	**Identifier**
Length	4 Bytes	1 Byte	2 Bytes	1 Byte

Value	1 Byte nation numerical code	Integer	additional coding (CA specific)	′01′
	3 Bytes nation alphanumerical code		′FF FF′ if not used	

The key serial number is used to distinguish the different keys of a Member State, in the case the key is changed.

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).

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).

6. Certificate verifiers shall implicitly know that the public key certified is an RSA key relevant to authentication, digital signature verification and encipherement for confidentiality services (the certificate contains no Object Identifier to specify it).

3.3.2. Certificates issued

The certificate issued is a digital signature with partial recovery of the certificate content in accordance with ISO/IEC 9796-2 **[**[F4]except for its Annex A.4**]**, with the ‘Certification Authority Reference’ appended.

Textual Amendments

F4 Inserted 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).

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, Hash(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

With certificate content

$$= Cc = \underbrace{C_r}_{106\ Bytes} \,||\, \underbrace{C_n}_{58\ Bytes}$$

Notes:

1. This certificate is 194 bytes long.

2. CAR, being hidden by the signature, is also appended to the signature, such that the public key of the certification authority may be selected for the verification of the certificate.

3. The certificate verifier shall implicitly know the algorithm used by the certification authority to sign the certificate.

4. The headerlist associated with this issued certificate is as follows:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
CV Certificate Tag (Constructed)	Length of subsequent DOs	Signature Tag	Signature length	Remainder Tag	Remainder length	CAR Tag	CAR length

3.3.3. Certificate verification and unwrapping

Certificate verification and unwrapping consists in verifying the signature in accordance with ISO/IEC 9796-2, retrieving the certificate content and the public key contained: X.PK = X.CA.PK$_o$X.C, and verifying the validity of the certificate.

It involves the following steps:

verify signature and retrieve content:

— from X.C retrieve Sign, C_n' and CAR′:

— from CAR′ select appropriate Certification Authority Public Key (if not done before through other means)

— open Sign with CA Public Key: Sr′ = X.CA.PK [Sign],

— check Sr′ starts with ′6A′ and ends with ′BC′

— compute Cr′ and H′ from:

— Recover certificate content C′ = C_r' || C_n',

— check *Hash*(C′) = H′

If the checks are OK the certificate is a genuine one, its content is C′.

Verify validity. From C′:

— if applicable, check End of validity date,

Retrieve and store public key, Key Identifier, Certificate Holder Authorisation and Certificate End of Validity from C′:

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV.]]

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