

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

CHAPTER I

Principles and scope

- Article 1 Recording equipment within the meaning of this Regulation shall, as...
- Article 2 For the purpose of this Regulation the definitions set out...
- Article 3 (1) Recording equipment shall be installed and used in vehicles...

CHAPTER II

Type approval

- Article 4 For the purposes of this Chapter, the words ‘ recording...
- Article 5 A Member State shall grant EC component type-approval to any...
- Article 6 Member States shall issue to the applicant an EEC approval...
- Article 7 The competent authorities of the Member State to which the...
- Article 8 (1) If a Member State which has granted EEC type...
- Article 9 (1) An applicant for EEC type approval of a model...
- Article 10 No Member State may refuse to register any vehicle fitted...
- Article 11 All decisions pursuant to this Regulation refusing or withdrawing approval...

CHAPTER III

Installation and inspection

- Article 12 (1) Recording equipment may be installed or repaired only by...

CHAPTER IV

Use of equipment

- Article 13 The employer and drivers shall ensure the correct functioning and...
- Article 14 (1) The employer shall issue a sufficient number of record...
- Article 15 (1) Drivers shall not use dirty or damaged record sheets...
- Article 16 (1) In the event of breakdown or faulty operation of...

CHAPTER V

Final provisions

- Article 17 (1) The amendments required to adjust the annexes to technical...
- Article 18 (1) The Commission shall be assisted by a Committee.

Article 19	(1) Member States shall, in good time and after consulting...
Article 20	Regulation (EEC) No 1463/70 shall be repealed. However, Article 3...
Article 20a	This Regulation shall not apply until 1 January 1991 to...
Article 21	This Regulation shall enter into force on 29 September 1986....
	Signature

ANNEX I

REQUIREMENTS FOR CONSTRUCTION, TESTING, INSTALLATION AND INSPECTION

- I. DEFINITIONS
- II. GENERAL CHARACTERISTICS AND FUNCTIONS OF RECORDING EQUIPMENT
- III. CONSTRUCTION REQUIREMENTS FOR RECORDING EQUIPMENT
 - (a) General points
 - 1. Recording equipment shall include the following:
 - 1.1. Visual instruments showing:
 - 1.2. Recording instruments comprising:
 - 1.3. A means of marking showing on the record sheet individually:...
 - 2. Any inclusion in the equipment of devices additional to those...
 - 3. Materials
 - 3.1. All the constituent parts of the recording equipment must be...
 - 3.2. Any modification in a constituent part of the equipment or...
 - 4. Measurement of distance travelled
 - 5. Measurement of speed
 - 5.1. The range of speed measurement shall be as stated in...
 - 5.2. The natural frequency and the damping of the measuring device...
 - 6. Measurement of time (clock)
 - 6.1. The control of the mechanism for resetting the clock must...
 - 6.2. If the forward movement mechanism of the record sheet is...
 - 7. Lighting and Protection
 - 7.1. The visual instruments of the equipment must be provided with...
 - 7.2. For normal conditions of use, all the internal parts of...
 - (b) Visual instruments
 - 1. Distance travelled indicator (distance recorder)
 - 1.1. The value of the smallest grading on the instrument showing...
 - 1.2. The figures on the distance recorder must be clearly legible...
 - 1.3. The distance recorder must be capable of reading up to...
 - 2. Speed indicators (speedometer)
 - 2.1. Within the range of measurement, the speed scale must be...
 - 2.2. The range indicated beyond that measured need not be marked...
 - 2.3. The length of each space on the scale representing a...

Changes to legislation: There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85. (See end of Document for details)

- 2.4. On an indicator with a needle, the distance between the...
 3. Time indicator (clock)
 - (c) Recording instruments
 1. General points
 - 1.1. All equipment, whatever the form of the record sheet (strip...
 - 1.2. The mechanism moving the record sheet must be such as...
 - 1.3. For record sheets in disc form, the forward movement device...
 - 1.4. Recording of the distance travelled, of the speed of the...
 2. Recording distance travelled
 - 2.1. Every kilometre of distance travelled must be represented on the...
 - 2.2. Even at speeds reaching the upper limit of the range...
 3. Recording speed
 - 3.1. Whatever the form of the record sheet, the speed recording...
 - 3.2. Each variation in speed of 10 kilometres per hour must...
 4. Recording time
 - 4.1. Recording equipment must be so constructed that the period of...
 - 4.2. It must be possible, from the characteristics of the traces,...
 - 4.3. In the case of vehicles with a crew consisting of...
 - (d) Closing device
 1. The case containing the record sheet or sheets and the...
 2. Each opening of the case containing the record sheet or...
 - (e) Markings
 1. The following markings must appear on the instrument face of...
 2. The descriptive plaque must be built into the equipment and...
 - (f) Maximum tolerances (visual and recording instruments)
 1. On the test bench before installation:
 2. On installation:
 3. In use:
 4. The maximum tolerances set out in points 1, 2 and...
 5. Measurement of the maximum tolerances set out in points 2...
- IV. RECORD SHEETS
 - (a) General points
 1. The record sheets must be such that they do not...
 2. The minimum recording capacity of the sheets, whatever their form,...
 - (b) Recording areas and their graduation
 1. The record sheets shall include the following recording areas:
 2. The area for recording speed must be scaled off in...
 3. The area for recording distance travelled must be set out...
 4. The area or areas reserved for recording the periods referred...
 - (c) Information to be printed on the record sheets
 - (d) Free space for hand written insertions
- V. INSTALLATION OF RECORDING EQUIPMENT
 1. Recording equipment must be positioned in the vehicle in such...
 2. It must be possible to adapt the constant of the...
 3. After the equipment has been checked on installation, an installation...
 4. Sealing
 5. The cables connecting the recording equipment to the transmitter must...
- VI. CHECKS AND INSPECTIONS

1. Certification of new or repaired instruments
2. Installation
3. Periodic inspections
4. Measurement of errors

ANNEX I B

REQUIREMENTS FOR CONSTRUCTION, TESTING, INSTALLATION AND INSPECTION

- I. DEFINITIONS
- II. GENERAL CHARACTERISTICS AND FUNCTIONS OF THE RECORDING EQUIPMENT
 1. General characteristics
 2. Functions
 3. Modes of operation
 4. Security
- III. CONSTRUCTION AND FUNCTIONAL REQUIREMENTS FOR RECORDING EQUIPMENT
 1. Monitoring cards insertion and withdrawal
 2. Speed and distance measurement
 - 2.1. Measurement of distance travelled
 - 2.2. Measurement of speed
 3. Time measurement
 4. Monitoring driver activities
 5. Monitoring driving status
 6. Drivers manual entries
 - 6.1. Entry of places where daily work periods begin and/or end...
 - 6.2. Manual entry of driver activities
 - 6.3. Entry of specific conditions
 7. Company locks management
 8. Monitoring control activities
 9. Detection of events and/or faults
 - 9.1. Insertion of a non-valid card ‘ ‘ event
 - 9.2. ‘ Card conflict ’ event
 - 9.3. ‘ Time overlap ’ event
 - 9.4. ‘ Driving without an appropriate card ’ event
 - 9.5. ‘ Card insertion while driving ’ event
 - 9.6. ‘ Last card session not correctly closed ’ event
 - 9.7. ‘ Over speeding ’ event
 - 9.8. ‘ Power supply interruption ’ event
 - 9.9. ‘ Motion data error ’ event
 - 9.9 bis. ‘ Vehicle Motion Conflict ’ event
 - 9.10. ‘ Security breach attempt ’ event
 - 9.11. ‘ Card ’ fault
 - 9.12. ‘ Recording equipment ’ fault
 10. Built-in and self tests
 11. Reading from data memory
 12. Recording and storing in the data memory
 - 12.1. Equipment identification data

Changes to legislation: There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85. (See end of Document for details)

- 12.1.1. Vehicle unit identification data
- 12.1.2. Motion sensor identification data
- 12.2. Security elements
- 12.3. Driver card insertion and withdrawal data
- 12.4. Driver activity data
- 12.5. Places where daily work periods start and/or end
- 12.6. Odometer data
- 12.7. Detailed speed data
- 12.8. Events data
- 12.9. Faults data
- 12.10. Calibration data
- 12.11. Time adjustment data
- 12.12. Control activity data
- 12.13. Company locks data
- 12.14. Download activity data
- 12.15. Specific conditions data
- 13. Reading from tachograph cards
- 14. Recording and storing on tachograph cards
- 15. Displaying
 - 15.1. Default display
 - 15.2. Warning display
 - 15.3. Menu access
 - 15.4. Other displays
- 16. Printing
- 17. Warnings
- 18. Data downloading to external media
- 19. Output data to additional external devices
- 20. Calibration
- 21. Time adjustment
- 22. Performance characteristics
- 23. Materials
- 24. Markings

IV. CONSTRUCTION AND FUNCTIONAL REQUIREMENTS FOR TACHOGRAPH CARDS

- 1. Visible data
- 2. Security
- 3. Standards
- 4. Environmental and electrical specifications
- 5. Data storage
 - 5.1. Card identification and security data
 - 5.1.1. Application identification
 - 5.1.2. Chip identification
 - 5.1.3. IC card identification
 - 5.1.4. Security elements
 - 5.2. Driver card
 - 5.2.1. Card identification
 - 5.2.2. Card holder identification
 - 5.2.3. Driving licence information
 - 5.2.4. Vehicles used data
 - 5.2.5. Driver activity data
 - 5.2.6. Places where daily work periods start and/or end
 - 5.2.7. Events data

- 5.2.8. Faults data
 - 5.2.9. Control activity data
 - 5.2.10. Card session data
 - 5.2.11. Specific conditions data
 - 5.3. Workshop card
 - 5.3.1. Security elements
 - 5.3.2. Card identification
 - 5.3.3. Card holder identification
 - 5.3.4. Vehicles used data
 - 5.3.5. Driver activity data
 - 5.3.6. Daily work periods start and/or end data
 - 5.3.7. Events and faults data
 - 5.3.8. Control activity data
 - 5.3.9. Calibration and time adjustment data
 - 5.3.10. Specific conditions data
 - 5.4. Control card
 - 5.4.1. Card identification
 - 5.4.2. Card holder identification
 - 5.4.3. Control activity data
 - 5.5. Company card
 - 5.5.1. Card identification
 - 5.5.2. Card holder identification
 - 5.5.3. Company activity data
- V. INSTALLATION OF RECORDING EQUIPMENT
- 1. Installation
 - 2. Installation plaque
 - 3. Sealing
- VI. CHECKS, INSPECTIONS AND REPAIRS
- 1. Approval of fitters or workshops
 - 2. Check of new or repaired instruments
 - 3. Installation inspection
 - 4. Periodic inspections
 - 5. Measurement of errors
 - 6. Repairs
- VII. CARD ISSUING
- VIII. TYPE APPROVAL OF RECORDING EQUIPMENT AND TACHOGRAPH CARDS
- 1. General points
 - 2. Security certificate
 - 3. Functional certificate
 - 4. Interoperability certificate
 - 5. Type approval certificate
 - 6. Exceptional procedure: first interoperability certificates

Appendix 1

DATA DICTIONARY

1. INTRODUCTION

Changes to legislation: There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85. (See end of Document for details)

- 1.1. Approach for definitions of data types
- 1.2. References
2. DATA TYPE DEFINITIONS
 - 2.1. ActivityChangeInfo
Note for the case ‘ card withdrawal ’ :
 - 2.2. Address
 - 2.3. BCString
 - 2.4. CalibrationPurpose
 - 2.5. CardActivityDailyRecord
 - 2.6. CardActivityLengthRange
 - 2.7. CardApprovalNumber
 - 2.8. CardCertificate
 - 2.9. CardChipIdentification
 - 2.10. CardConsecutiveIndex
 - 2.11. CardControlActivityDataRecord
 - 2.12. CardCurrentUse
 - 2.13. CardDriverActivity
 - 2.14. CardDrivingLicenceInformation
 - 2.15. CardEventData
 - 2.16. CardEventRecord
 - 2.17. CardFaultData
 - 2.18. CardFaultRecord
 - 2.19. CardIccIdentification
 - 2.20. CardIdentification
 - 2.21. CardNumber
 - 2.22. CardPlaceDailyWorkPeriod
 - 2.23. CardPrivateKey
 - 2.24. CardPublicKey
 - 2.25. CardRenewalIndex
 - 2.26. CardReplacementIndex
 - 2.27. CardSlotNumber
 - 2.28. CardSlotsStatus
 - 2.29. CardStructureVersion
 - 2.30. CardVehicleRecord
 - 2.31. CardVehiclesUsed
 - 2.32. Certificate
 - 2.33. CertificateContent
 - 2.34. CertificateHolderAuthorisation
 - 2.35. CertificateRequestID
 - 2.36. CertificationAuthorityKID
 - 2.37. CompanyActivityData
 - 2.38. CompanyActivityType
 - 2.39. CompanyCardApplicationIdentification
 - 2.40. CompanyCardHolderIdentification
 - 2.41. ControlCardApplicationIdentification
 - 2.42. ControlCardControlActivityData
 - 2.43. ControlCardHolderIdentification
 - 2.44. ControlType
 - 2.45. CurrentDateTime
 - 2.46. DailyPresenceCounter
 - 2.47. Datef
 - 2.48. Distance

- 2.49. DriverCardApplicationIdentification
- 2.50. DriverCardHolderIdentification
- 2.51. EntryTypeDailyWorkPeriod
- 2.52. EquipmentType
- 2.53. EuropeanPublicKey
- 2.54. EventFaultType
- 2.55. EventFaultRecordPurpose
- 2.56. ExtendedSerialNumber
- 2.57. FullCardNumber
- 2.58. HighResOdometer
- 2.59. HighResTripDistance
- 2.60. HolderName
- 2.61. K-ConstantOfRecordingEquipment
- 2.62. KeyIdentifier
- 2.63. L-TyreCircumference
- 2.64. Language
- 2.65. LastCardDownload
- 2.66. ManualInputFlag
- 2.67. ManufacturerCode
- 2.68. MemberStateCertificate
- 2.69. MemberStatePublicKey
- 2.70. Name
- 2.71. NationAlpha
- 2.72. NationNumeric
- 2.73. NoOfCalibrationRecords
- 2.74. NoOfCalibrationsSinceDownload
- 2.75. NoOfCardPlaceRecords
- 2.76. NoOfCardVehicleRecords
- 2.77. NoOfCompanyActivityRecords
- 2.78. NoOfControlActivityRecords
- 2.79. NoOfEventsPerType
- 2.80. NoOfFaultsPerType
- 2.81. OdometerValueMidnight
- 2.82. OdometerShort
- 2.83. OverspeedNumber
- 2.84. PlaceRecord
- 2.85. PreviousVehicleInfo
- 2.86. PublicKey
- 2.87. RegionAlpha
- 2.88. RegionNumeric
- 2.89. RSAKeyModulus
- 2.90. RSAKeyPrivateExponent
- 2.91. RSAKeyPublicExponent
- 2.92. SensorApprovalNumber
- 2.93. SensorIdentification
- 2.94. SensorInstallation
- 2.95. SensorInstallationSecData
- 2.96. SensorOSIdentifier
- 2.97. SensorPaired
- 2.98. SensorPairingDate
- 2.99. SensorSerialNumber
- 2.100. SensorSCIdentifier
- 2.101. Signature

Changes to legislation: There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85. (See end of Document for details)

- 2.102. SimilarEventsNumber
- 2.103. SpecificConditionType
- 2.104. SpecificConditionRecord
- 2.105. Speed
- 2.106. SpeedAuthorised
- 2.107. SpeedAverage
- 2.108. SpeedMax
- 2.109. TDesSessionKey
- 2.110. TimeReal
- 2.111. TyreSize
- 2.112. VehicleIdentificationNumber
- 2.113. VehicleRegistrationIdentification
- 2.114. VehicleRegistrationNumber
- 2.115. VuActivityDailyData
- 2.116. VuApprovalNumber
- 2.117. VuCalibrationData
- 2.118. VuCalibrationRecord
- 2.119. VuCardIWData
- 2.120. VuCardIWRecord
- 2.121. VuCertificate
- 2.122. VuCompanyLocksData
- 2.123. VuCompanyLocksRecord
- 2.124. VuControlActivityData
- 2.125. VuControlActivityRecord
- 2.126. VuDataBlockCounter
- 2.127. VuDetailedSpeedBlock
- 2.128. VuDetailedSpeedData
- 2.129. VuDownloadablePeriod
- 2.130. VuDownloadActivityData
- 2.131. VuEventData
- 2.132. VuEventRecord
- 2.133. VuFaultData
- 2.134. VuFaultRecord
- 2.135. VuIdentification
- 2.136. VuManufacturerAddress
- 2.137. VuManufacturerName
- 2.138. VuManufacturingDate
- 2.139. VuOverSpeedingControlData
- 2.140. VuOverSpeedingEventData
- 2.141. VuOverSpeedingEventRecord
- 2.142. VuPartNumber
- 2.143. VuPlaceDailyWorkPeriodData
- 2.144. VuPlaceDailyWorkPeriodRecord
- 2.145. VuPrivateKey
- 2.146. VuPublicKey
- 2.147. VuSerialNumber
- 2.148. VuSoftInstallationDate
- 2.149. VuSoftwareIdentification
- 2.150. VuSoftwareVersion
- 2.151. VuSpecificConditionData
- 2.152. VuTimeAdjustmentData
- 2.153. VuTimeAdjustmentRecord
- 2.154. W-VehicleCharacteristicConstant

- 2.155. WorkshopCardApplicationIdentification
 - 2.156. WorkshopCardCalibrationData
 - 2.157. WorkshopCardCalibrationRecord
 - 2.158. WorkshopCardHolderIdentification
 - 2.159. WorkshopCardPIN
- 3. VALUE AND SIZE RANGE DEFINITIONS
 - 3.1. Definitions for the Driver Card:
 - 3.2. Definitions for the Workshop Card:
 - 3.3. Definitions for the Control Card:
 - 3.4. Definitions for the Company Card:
 - 4. CHARACTER SETS
 - 5. ENCODING

Appendix 2

TACHOGRAPH CARDS SPECIFICATION

- 1. INTRODUCTION
 - 1.1. Abbreviations
 - 1.2. References
- 2. ELECTRICAL AND PHYSICAL CHARACTERISTICS
 - 2.1. Supply voltage and current consumption
 - 2.2. Programming voltage V_{pp}
 - 2.3. Clock generation and frequency
 - 2.4. I/O contact
 - 2.5. States of the card
- 3. HARDWARE AND COMMUNICATION
 - 3.1. Introduction
 - 3.2. Transmission protocol
 - 3.2.1. Protocols
 - 3.2.2. ATR
 - 3.2.3. PTS
 - 3.3. Access conditions (AC)
 - 3.4. Data encryption
 - 3.5. Commands and error codes overview
 - 3.6. Commands description
 - 3.6.1. Select file
 - 3.6.1.1. Selection by name (AID)
 - 3.6.1.2. Selection of an elementary file using its file identifier
 - 3.6.2. Read Binary
 - 3.6.2.1. Command without secure messaging
 - 3.6.2.2. Command with secure messaging
 - 3.6.3. Update Binary
 - 3.6.3.1. Command without secure messaging
 - 3.6.3.2. Command with secure messaging
 - 3.6.4. Get challenge
 - 3.6.5. Verify

Changes to legislation: There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85. (See end of Document for details)

- 3.6.6. Get response
 - 3.6.7. PSO: verify certificate
 - 3.6.8. Internal authenticate
 - 3.6.9. External authenticate
 - 3.6.10. Manage security environment
 - 3.6.11. PSO: hash
 - 3.6.12. Perform hash of file
 - 3.6.13. PSO: compute digital signature
 - 3.6.14. PSO: verify digital signature
4. TACHOGRAPH CARDS STRUCTURE
- 4.1. Driver card structure
 - 4.2. Workshop card structure
 - 4.3. Control card structure
 - 4.4. Company card structure

Appendix 3 PICTOGRAMS

The recording equipment may optionally use the following pictograms and...
BASIC PICTOGRAMS People Actions Modes of operation
Company Company mode...

Appendix 4 PRINTOUTS

- 1. GENERALITIES
- 2. DATA BLOCKS SPECIFICATION
- 3. PRINTOUT SPECIFICATIONS
 - 3.1. Driver Activities from Card Daily Printout
 - 3.2. Driver Activities from daily VU printout
 - 3.3. Events and faults from card printout
 - 3.4. Events and faults from VU printout
 - 3.5. Technical data printout
 - 3.6. Over speeding printout

Appendix 5 DISPLAY

In this appendix the following format notation conventions have been...
characters printed in bold denote plain text to be displayed...
The recording equipment shall display data using the following formats:...

Appendix 6

EXTERNAL INTERFACES

1. HARDWARE
 - 1.1. Connector
 - 1.2. Contact allocation
 - 1.3. Block diagram
2. DOWNLOADING INTERFACE
3. CALIBRATION INTERFACE

Appendix 7

DATA DOWNLOADING PROTOCOLS

1. INTRODUCTION
 - 1.1. Scope
 - 1.2. Acronyms and notations
2. VU DATA DOWNLOADING
 - 2.1. Download procedure
 - 2.2. Data download protocol
 - 2.2.1. Message structure
 - 2.2.2. Message types
 - 2.2.2.1. Start communication request (SID 81)
 - 2.2.2.2. Positive response start communication (SID C1)
 - 2.2.2.3. Start diagnostic session request (SID 10)
 - 2.2.2.4. Positive response start diagnostic (SID 50)
 - 2.2.2.5. Link control service (SID 87)
 - 2.2.2.6. Link control positive response (SID C7)
 - 2.2.2.7. Request upload (SID 35)
 - 2.2.2.8. Positive response request upload (SID 75)
 - 2.2.2.9. Transfer data request (SID 36)
 - 2.2.2.10. Positive response transfer data (SID 76)
 - 2.2.2.11. Request transfer exit (SID 37)
 - 2.2.2.12. Positive response request transfer exit (SID 77)
 - 2.2.2.13. Stop communication request (SID 82)
 - 2.2.2.14. Positive response stop communication (SID C2)
 - 2.2.2.15. Acknowledge submessage (SID 83)
 - 2.2.2.16. Negative Response (SID 7F)
 - 2.2.3. Message flow
 - 2.2.4. Timing
 - 2.2.5. Error handling
 - 2.2.5.1. Start communication phase
 - 2.2.5.2. Communication phase
 - 2.2.6. Response message content
 - 2.2.6.1. Positive response transfer data overview
 - 2.2.6.2. Positive response transfer data activities
 - 2.2.6.3. Positive response transfer data events and faults
 - 2.2.6.4. Positive response transfer data detailed speed
 - 2.2.6.5. Positive response transfer data technical data

- 2.3. ESM File storage
- 3. TACHOGRAPH CARDS DOWNLOADING PROTOCOL
 - 3.1. Scope
 - 3.2. Definitions
 - 3.3. Card downloading
 - 3.3.1. Initialisation sequence
 - 3.3.2. Sequence for unsigned data files
 - 3.3.3. Sequence for signed data files
 - 3.3.4. Sequence for resetting the calibration counter
 - 3.4. Data storage format
 - 3.4.1. Introduction
 - 3.4.2. File format
- 4. DOWNLOADING A TACHOGRAPH CARD VIA A VEHICLE UNIT

Appendix 8

CALIBRATION PROTOCOL

- 1. INTRODUCTION
- 2. TERMS, DEFINITIONS AND REFERENCES
- 3. OVERVIEW OF SERVICES
 - 3.1. Services available
 - 3.2. Response codes
- 4. COMMUNICATION SERVICES
 - 4.1. StartCommunication Service
 - 4.2. StopCommunication service
 - 4.2.1. Message description
 - 4.2.2. Message format
 - 4.2.3. Parameter definition
 - 4.3. TesterPresent service
 - 4.3.1. Message description
 - 4.3.2. Message format
- 5. MANAGEMENT SERVICES
 - 5.1. StartDiagnosticSession service
 - 5.1.1. Message description
 - 5.1.2. Message format
 - 5.1.3. Parameter definition
 - 5.2. SecurityAccess service
 - 5.2.1. Message description
 - 5.2.2. Message format — SecurityAccess — requestSeed
 - 5.2.3. Message format — SecurityAccess — sendKey
- 6. DATA TRANSMISSION SERVICES
 - 6.1. ReadDataByIdentifier service
 - 6.1.1. Message description
 - 6.1.2. Message format

- 6.1.3. Parameter definition
- 6.2. WriteDataByIdentifier service
 - 6.2.1. Message description
 - 6.2.2. Message format
 - 6.2.3. Parameter definition
- 7. CONTROL OF TEST PULSES — INPUT/OUTPUT CONTROL FUNCTIONAL UNIT
 - 7.1. Message description
 - 7.1.1. Message description
 - 7.1.2. Message format
 - 7.1.3. Parameter definition
- 8. DATARECORDS FORMATS
 - 8.1. Transmitted parameter ranges
 - 8.2. dataRecords formats

Appendix 9

TYPE APPROVAL — LIST OF MINIMUM REQUIRED TESTS

- 1. INTRODUCTION
 - 1.1. Type approval
 - 1.2. References
- 2. VEHICLE UNIT FUNCTIONAL TESTS
- 3. MOTION SENSOR FUNCTIONAL TESTS
- 4. TACHOGRAPH CARDS FUNCTIONAL TESTS
- 5. INTEROPERABILITY TESTS

Appendix 10

GENERIC SECURITY TARGETS

MOTION SENSOR GENERIC SECURITY TARGET

- 1. Introduction
- 2. Abbreviations, definitions and references
 - 2.1. Abbreviations
 - 2.2. Definitions
 - 2.3. References
- 3. Product rationale
 - 3.1. Motion sensor description and method of use
 - 3.2. Motion sensor life cycle
 - 3.3. Threats
 - 3.3.1. Threats to access control policies
 - 3.3.2. Design related threats
 - 3.3.3. Operation oriented threats
 - 3.4. Security objectives

Changes to legislation: There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85. (See end of Document for details)

- 3.5. Information technology security objectives
- 3.6. Physical, personnel or procedural means
 - 3.6.1. Equipment design
 - 3.6.2. Equipment delivery
 - 3.6.3. Security data generation and delivery
 - 3.6.4. Recording equipment installation, calibration, and inspection
 - 3.6.5. Law enforcement control
 - 3.6.6. Software upgrades
- 4. Security enforcing functions
 - 4.1. Identification and authentication
 - 4.2. Access control
 - 4.2.1. Access control policy
 - 4.2.2. Data access rights
 - 4.2.3. File structure and access conditions
 - 4.3. Accountability
 - 4.4. Audit
 - 4.5. Accuracy
 - 4.5.1. Information flow control policy
 - 4.5.2. Internal data transfers
 - 4.5.3. Stored data integrity
 - 4.6. Reliability of service
 - 4.6.1. Tests
 - 4.6.2. Software
 - 4.6.3. Physical protection
 - 4.6.4. Power supply interruptions
 - 4.6.5. Reset conditions
 - 4.6.6. Data availability
 - 4.6.7. Multiple applications
 - 4.7. Data exchange
 - 4.8. Cryptographic support
- 5. Definition of security mechanisms
- 6. Minimum strength of security mechanisms
- 7. Level of assurance
- 8. Rationale

VEHICLE UNIT GENERIC SECURITY TARGET

- 1. Introduction
- 2. Abbreviations, definitions and references
 - 2.1. Abbreviations
 - 2.2. Definitions
 - 2.3. References
- 3. Product rationale
 - 3.1. Vehicle unit description and method of use
 - 3.2. Vehicle unit life cycle
 - 3.3. Threats
 - 3.3.1. Threats to identification and access control policies
 - 3.3.2. Design related threats
 - 3.3.3. Operation oriented threats
 - 3.4. Security objectives
 - 3.5. Information technology security objectives
 - 3.6. Physical, personnel or procedural means
 - 3.6.1. Equipment design
 - 3.6.2. Equipment delivery and activation

- 3.6.3. Security data generation and delivery
- 3.6.4. Cards delivery
- 3.6.5. Recording equipment installation, calibration, and inspection
- 3.6.6. Equipment operation
- 3.6.7. Law enforcement control
- 3.6.8. Software upgrades
- 4. Security enforcing functions
 - 4.1. Identification and authentication
 - 4.1.1. Motion sensor identification and authentication
 - 4.1.2. User identification and authentication
 - 4.1.3. Remotely connected company identification and authentication
 - 4.1.4. Management device identification and authentication
 - 4.2. Access control
 - 4.2.1. Access control policy
 - 4.2.2. Access rights to functions
 - 4.2.3. Access rights to data
 - 4.2.4. File structure and access conditions
 - 4.3. Accountability
 - 4.4. Audit
 - 4.5. Object re-use
 - 4.6. Accuracy
 - 4.6.1. Information flow control policy
 - 4.6.2. Internal data transfers
 - 4.6.3. Stored data integrity
 - 4.7. Reliability of service
 - 4.7.1. Tests
 - 4.7.2. Software
 - 4.7.3. Physical protection
 - 4.7.4. Power supply interruptions
 - 4.7.5. Reset conditions
 - 4.7.6. Data availability
 - 4.7.7. Multiple applications
 - 4.8. Data exchange
 - 4.8.1. Data exchange with motion sensor
 - 4.8.2. Data exchange with tachograph cards
 - 4.8.3. Data exchange with external storage media (downloading function)
 - 4.9. Cryptographic support
- 5. Definition of security mechanisms
- 6. Minimum strength of security mechanisms
- 7. Level of assurance
- 8. Rationale

TACHOGRAPH CARD GENERIC SECURITY TARGET

- 1. Introduction
- 2. Abbreviations, definitions and references
 - 2.1. Abbreviations
 - 2.2. Definitions
 - 2.3. References
- 3. Product Rationale
 - 3.1. Tachograph card description and method of use
 - 3.2. Tachograph card life cycle

Changes to legislation: There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85. (See end of Document for details)

- 3.3. Threats
 - 3.3.1. Final aims
 - 3.3.2. Attack paths
- 3.4. Security Objectives
- 3.5. Information technology security objectives
- 3.6. Physical, personnel or procedural means
- 4. Security enforcing functions
 - 4.1. Compliance to protection profiles
 - 4.2. User identification and authentication
 - 4.2.1. User identification
 - 4.2.2. User authentication
 - 4.2.3. Authentication failures
 - 4.3. Access control
 - 4.3.1. Access control policy
 - 4.3.2. Access control functions
 - 4.4. Accountability
 - 4.5. Audit
 - 4.6. Accuracy
 - 4.6.1. Stored data integrity
 - 4.6.2. Basic data authentication
 - 4.7. Reliability of service
 - 4.7.1. Tests
 - 4.7.2. Software
 - 4.7.3. Power supply
 - 4.7.4. Reset conditions
 - 4.8. Data exchange
 - 4.8.1. Data exchange with a vehicle unit
 - 4.8.2. Export of data to a non-vehicle unit (download function)
 - 4.9. Cryptographic support
- 5. Definition of security mechanisms
- 6. Claimed minimum strength of mechanisms
- 7. Level of Assurance
- 8. Rationale

Appendix 11

COMMON SECURITY MECHANISMS

- 1. GENERALITIES
 - 1.1. References
 - 1.2. Notations and abbreviated terms
- 2. CRYPTOGRAPHIC SYSTEMS AND ALGORITHMS
 - 2.1. Cryptographic systems
 - 2.2. Cryptographic algorithms
 - 2.2.1. RSA algorithm
 - 2.2.2. Hash algorithm
 - 2.2.3. Data encryption algorithm
- 3. KEYS AND CERTIFICATES
 - 3.1. Keys generation and distribution
 - 3.1.1. RSA keys generation and distribution

- 3.1.2. RSA test keys
- 3.1.3. Motion sensor keys
- 3.1.4. T-DES session keys generation and distribution
- 3.2. Keys
- 3.3. Certificates
 - 3.3.1. Certificates content
 - Notes:
 1. The ‘ Certificate Profile Identifier ’ (CPI) delineates the exact...
 2. The ‘ Certification Authority Reference ’ (CAR) has the purpose...
 3. The ‘ Certificate Holder Authorisation ’ ((CHA) is used to...
 4. ‘ Certificate Holder Reference ’ (CHR) has the purpose of...
 5. Key Identifiers uniquely identify certificate holder or certification authorities. They...
 6. Certificate verifiers shall implicitly know that the public key certified...
 - 3.3.2. Certificates issued
 - Notes:
 1. This certificate is 194 bytes long.
 2. CAR, being hidden by the signature, is also appended to...
 3. The certificate verifier shall implicitly know the algorithm used by...
 4. The headerlist associated with this issued certificate is as follows:...
 - 3.3.3. Certificate verification and unwrapping
- 4. MUTUAL AUTHENTICATION MECHANISM
- 5. VU-CARDS DATA TRANSFER CONFIDENTIALITY, INTEGRITY AND AUTHENTICATION MECHANISMS
 - 5.1. Secure messaging
 - 5.2. Treatment of secure messaging errors
 - 5.3. Algorithm to compute cryptographic checksums
 - 5.4. Algorithm to compute cryptograms for confidentiality DOs
- 6. DATA DOWNLOAD DIGITAL SIGNATURE MECHANISMS
 - 6.1. Signature generation
 - 6.2. Signature verification

Appendix 12

ADAPTOR FOR M 1 AND N1 CATEGORY VEHICLES

- 1. ABBREVIATIONS AND REFERENCE DOCUMENTS
 - 1.1. Abbreviations
 - 1.2. Reference standards
- 2. GENERAL CHARACTERISTICS AND FUNCTIONS OF THE ADAPTOR

Changes to legislation: There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85. (See end of Document for details)

- 2.1. Adaptor general description
- 2.2. Functions
- 2.3. Security
3. REQUIREMENTS FOR THE RECORDING EQUIPMENT WHEN AN ADAPTOR IS INSTALLED...
4. CONSTRUCTION AND FUNCTIONAL REQUIREMENTS FOR THE ADAPTOR
 - 4.1. Interfacing and adapting incoming speed pulses
 - 4.2. Inducing the incoming pulses to the embedded motion sensor
 - 4.3. Embedded motion sensor
 - 4.4. Security requirements
 - 4.5. Performance characteristics
 - 4.6. Materials
 - 4.7. Markings
5. INSTALLATION OF THE RECORDING EQUIPMENT WHEN AN ADAPTOR IS USED...
 - 5.1. Installation
 - 5.2. Sealing
6. CHECKS, INSPECTIONS AND REPAIRS
 - 6.1. Periodic inspections
7. TYPE APPROVAL OF RECORDING EQUIPMENT WHEN AN ADAPTOR IS USED...
 - 7.1. General points
 - 7.2. Functional certificate

ANNEX II

APPROVAL MARK AND CERTIFICATE

- I. APPROVAL MARK
 1. The approval mark shall be made up of:
 2. The approval mark shall be shown on the descriptive plaque...
 3. The dimensions of the approval mark drawn below are expressed...
- II. APPROVAL CERTIFICATE FOR PRODUCTS COMPLIANT WITH ANNEX I
- III. APPROVAL CERTIFICATE FOR PRODUCTS COMPLIANT WITH ANNEX I B

Changes to legislation: There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85. (See end of Document for details)

- (1) OJ No C 100, 12. 4. 1984, p. 3, and OJ No C 223, 3. 9. 1985, p. 5.
- (2) OJ No C 122, 20. 5. 1985, p. 168.
- (3) OJ No C 104, 25. 4. 1985, p. 4, and OJ No C 303, 25. 11. 1985, p. 29.
- (4) OJ No L 164, 27. 7. 1970, p. 1.
- (5) OJ No L 334, 24. 12. 1977, p. 11.
- (6) See page 1 of this Official Journal.

Changes to legislation:

There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85.