JRC TECHNICAL REPORTS

DSRC CAN INTERFACE SPECIFICATION for the Smart Tachograph application

Version 1.5

Gianmarco Baldini, Michel Chiaramello

JRC129396

Contact information
Name: Michel Chiaramello
Address: Via Enrico Fermi 2749, 21027, Ispra (VA)
Email: Michel.Chiaramello@ec.europa.eu
Tel.: +39 0332 78 5781

EU Science Hub
https://ec.europa.eu/jrc

JRC129396

How to cite this report: Gianmarco Baldini, Michel Chiaramello, DSRC CAN Interface Specification for the Smart Tachograph application – Version 1.5, JRC129396.

Printed in Italy

Contents

Acknowledgements

This technical report is based on the technical specification details an implementation of the DSRC-CAN interface and communication protocol based on the SAE J1939 standard between the Vehicle Unit and a CAN based DSRC module in a Smart Tachograph System. The technical specification has been defined by the tachograph manufacturers Stoneridge, Continental and Intellic with the technical support of the Joint Research Centre of the European Commission and the vehicle manufactures via the HDEI (Heavy Truck Electronic Interface) working group. This document has been revised by the tachograph manufacturers following the publication of the regulation (EU) 2020/1228.

Gianmarco Baldini and Michel Chiaramello from EC JRC have only inserted the content from the technical specification in the format of a JRC Technical report to complement the Smart Tachograph regulation: European Commission, Commission implementing regulation (EU) 2016/799 of 18 march 2016 implementing regulation (eu) no 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components, 2016.

Authors

Gianmarco Baldini, Michel Chiaramello (on behalf of the HDEI working group)

1 Executive Summary

This document defines the protocol between the Vehicle Unit (VU) and the DSRC-VU module in the Smart Tachograph application defined in the Commission implementing regulation (EU) 2016/799 of 18 march 2016 implementing regulation (EU) no 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components.

The high level definition of the protocol (application layer) between the VU and the DSRC-VU module in the Smart Tachograph application is provided in Appendix 14 of regulation (EU) 2016/799. In Appendix 14, different options are possible for the choice of the lower layers of the protocol (e.g., transport layer) to be adopted.

This document describes the specific implementation of the protocol on the basis of the standard SAE J1939 standard between the VU and a CAN based DSRC module. SAE J1939 defines five layers in the seven-layer OSI network model, and this includes the Controller Area Network (CAN) ISO 11898 specification (using only the 29-bit/"extended" identifier) for the physical and data-link layers.

In this context, this document complements regulation (EU) 2016/799 for the specific implementation of the VU to DSRC-VU protocol on the basis of SAE J1939.

2 Document Scope

This document specifies the CAN protocol based on the [SAE J1939] standard between a Smart Tachograph and a DSRC-VU module, implementing the suggested Application Protocol defined in Annex 1C Appendix 14, and the reading by the Smart Tachograph of the DSRC-VU serial number.

3 Relevant Documents

Reference Id	Title
[Annex1C]	Commission implementing regulation (EU) 2016/799 of 18 march 2016 implementing regulation (EU) no 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components, 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX: 32016R0799
[Annex1C Amendment]	Commission Implementing Regulation (EU) 2018/502 of 28 February 2018 amending Implementing Regulation (EU) 2016/799 laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX: 32018R0502.
[Annex1C Amendment]	Commission Implementing Regulation (EU) 2021/1228 of 16 July 2021 amending Implementing Regulation (EU) 2016/799 as regards the requirements for the construction, testing, installation, operation and repair of smart tachographs and their components https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R1228
[Annex1C Appendix 1]	Appendix 1. Data Dictionary of [Annex1C].
[Annex1C Appendix 11]	Appendix 11. Common Security Mechanisms of [Annex1C].
[Annex1C Appendix 14]	Appendix 14. Remote Communication Function of [Annex1C].
[ISO 16844-4]	ISO 16844-4:2015 Road vehicles – Tachograph systems – Part 4 : CAN Interface
[ISO 8825-2]	ISO/IEC 8825-2:2015 Information technology - ASN.1 encoding rules – Part 2: Specification of Packed Encoding Rules (PER). 2015.
[ISO 8825-7]	ISO/IEC 8825-7:2015 Information technology - ASN.1 encoding rules – Part 7: Specification of Octet Encoding Rules (OER). 2015.
[SAE J1939]	Recommended Practice for a Serial Control and Communications Vehicle Network
[SAE J1939-21]	SAE J1939-21:MAR2016, Data Link Layer

4 Document Revision History

1 Rev: 0.1 Date of issue: 2020-04-28 Issued by EC D G JRC on the basis of the document prepared by Smart Tachograph stakeholders and coordinated by Stoneridge (coordinator: Lars Bodin)
Version for review.

2 Rev: 1.0 Date of issue: 2020-05-12 Issued by EC D G JRC on the basis of the review provided by stakeholders.
Final Version for publication.

3 Rev: 1.5 Date of issue: 2022-05-02 Issued by EC D G JRC on the basis of the review provided by stakeholders, following approbation of amendment (EU) 2021/1228.
Version for publication

5 General

[Annex 1C Appendix 14] defines the communication between a VU-RTM unit inside a Smart Tachograph (SM) and a Remote Early Detection Communication Reader (REDCR) as described in Figure 1.

One potential solution to this purpose is to use an external DSRC module (DSRC-VU) connected by a CAN bus using a communication protocol based on SAE J1939 defined in [SAE J1939-21]. A suggested application protocol and data transfer between VU-RTM and DSRC-VU is defined in [Annex 1C Appendix 14].

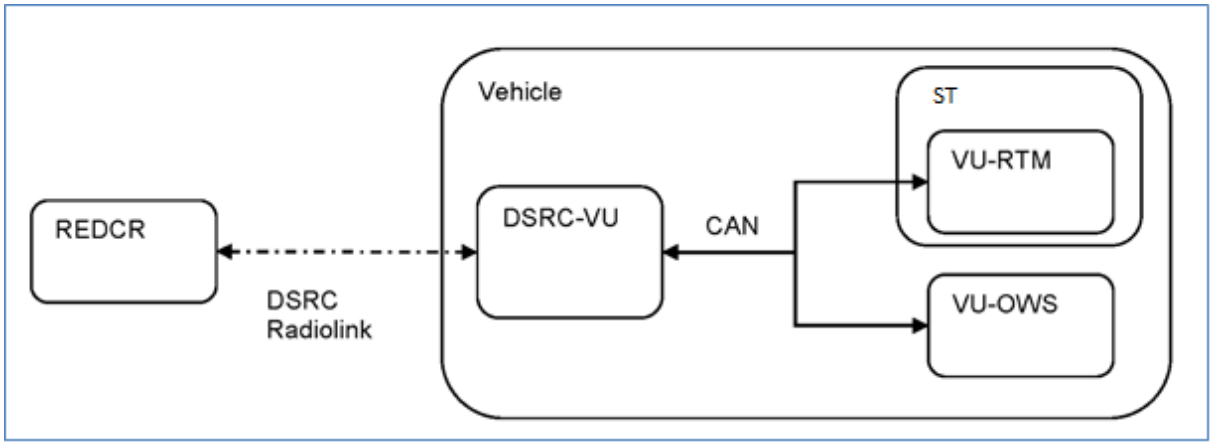

Figure 1 Communication between a VU-RTM unit inside a Smart Tachograph (ST) and a Remote Early Detection Communication Reader (REDCR)

Note: The implementation of a connection between the DSRC-VU and the VU-OWS is dependent on the future implementation of Directive (EU) 2017/719 and it is not addressed in this document.

This document specifies the CAN interface for the communication between Smart Tachographs and DSRC modules (DSRC-VU), including the attributes needed to implement the Parameter Group (PG) content. The application protocol and the physical layer are only referenced in the corresponding standards. The referenced standards for each layer are listed in the following Table 1.

Layer	Referenced Standard	Main Chapter
Application Layer	[Annex1C Appendix 11]	13 Security for Remote Communication over DSRC
	[Annex1C Appendix 14]	5.6.2 Application Protocol
	[ISO 8825-2]	All
Transport Layer	[SAE J1939-21]	5.10 Transport Protocol Function
Data Link Layer	[ISO 16844-4]	6 Data link layer application requirements
Physical Layer	[ISO 16844-4]	5 Physical layer application requirements

Table 1 Layers and referenced standards in DSRC communication.

6 Physical Layer

The physical layer for the DSRC CAN communication is defined in ISO 16844-4 Road vehicles- Tachograph systems- Part 4: CAN Interface [ISO 16844-4].

7 Transport Layer

The transport layer defined for the communication between DSRC-VU and VU-RTM or VU-OWS is the 'Transport Protocol Function', defined in [SAE J1939-21], for Parameter Groups which have 9 or more data bytes to transfer. The 'Transport Protocol Function' has the capability to communicate the data itself in a series of CAN Data Frames (packets) containing the packetized data. Additionally, the Transport Protocol Function provides flow control and handshaking capabilities for destination specific transfers.

A Parameter Group defined as multi-packet capable, having fewer than 9 data bytes to transfer in a specific instance, shall be sent in a single CAN Data Frame with the DLC set to 8.

7.1 SAE J1939 Transport Protocol Function

The 'Transport Protocol Function', between precisely two ECUs, allows a transmission of messages of arbitrary length up to 1785 bytes. The data flow for one PG can be bidirectional and is controlled by a handshake between sender and receiver ECU. The handshake consists of four dedicated message identifiers RTS, CTS, EndOfMsgACK and Conn_Abort, which is sent in connection management (TP.CM) messages. In case of error, the handshake mechanism allows a retransmission of communication subsequence without a complete repetition of the whole PG. In addition, the reception of a PG is confirmed by the receiving ECU.

The protocol is partly defined in [ISO 16844-4] and in any detail in [SAE J1939-21].

Note: the "ProprietaryA" PGN number (61184) will be used.

7.2 CAN node address

The CAN node address of a Smart Tachograph is defined as 0xEEh (238dec) in [ISO 16844-4]. The fixed address for the DSRC-VU module will be configurable to support different manufacturer needs.

ECU	Address	Comment
Smart Tachograph	0xEEh	
DSRC-VU	0xXXh	Shall be configurable in DSRC-VU and VU

Table 2 CAN node address

7.3 DSRC CAN Parameter Group Number – DSRC Communication

Name	Value	Comment
DSRC_Communication	61184 (00EF00h)	The Parameter Group Number (PGN) is from J1939-21.

Table 3 DSRC_Communication Parameter Group Number

DSRC_Communication will be used for sending DSRC command identity, application link identity and possibly including additional data related to the specific command (e.g. RCDT Data in SendData command).

Attribute	Value
Transmission Repetition Rate	On request
Data Length	Variable, 2 to 1785 bytes
Extended Data Page	0
Data Page	0
PDU Format	239
PDU Specific	Destination Address (DA)
Default Priority	6
PGN	61184_{10}/$00EF00_{16}$

Table 4 DSRC_Communication attribute specification

8 Application Layer

The application layer, for the DSRC_Communication PG, consists of three pairs of commands for initializing an application link, cyclic exchange of RTM/OWS data and for termination of the application link.

For application management the two command pairs “Initialization Request/Response” and “Termination Request/Response” are used. The “SendData” and “Acknowledgement of data” is used for cyclic transmission of application data for RTM and OWS. The application data in the “SendData” command is encrypted and signed before transmission according to chapter 13. “Security for Remote Communication over DSRC” of [Annex 1C Appendix 11].

Command	Direction	Payload defined in[Annex 1C Appendix 14]
Initialization Request	VU->DSRC-VU	RCDT-Communication Link Initialization - Request
Initialization Response	VU<-DSRC-VU	RCDT-Communication Link Initialization - Response
Send Data	VU->DSRC-VU	RCDT- Send Data (for RTM or OWS)
Acknowledgment of the data	VU<-DSRC-VU	RCDT Data Acknowledgment
Termination Request	VU->DSRC-VU	RCDT-Communication Link Termination - Request
Termination Response	VU<-DSRC-VU	RCDT-Communication Link Termination - Response

Table 5 Application Commands

8.1 DSRC_Communication Parameter Group

The content of the DSRC_Communication PG is divided in two parts. The first part defines the command header and the second part contains a variable length of bytes depending on type of command, i.e. either the answer in a response command or the payload of the RTM or OWS data, in a send data request:

4 Header
5 Answer or RTM / OWS Payload

8.1.1 DSRC_Communication CAN Header

The Header consists of two parts. The DSRC command transmitted in the message and an identifier specifying the application used in the message. Possible choices are RTM, OWS or further applications defined in the future.

Byte pos	Bit pos	Parameter	Remarks
1		Command_ID	See Table 7
2		Link_ID	See Table 8

Table 6 DSRC_Communication header specification

Attribute	Value
Data length	1 byte
Resolution	1/bit
Operating range	0 – LinkInitializationRequest 1 – LinkInitializationResponse 2 – SendData 3 – AcknowledgeData 4 – LinkTerminationRequest 5 – LinkTerminationResponse 6 to 255 reserved for further usage

Table 7 Command_ID specification

Attribute	Value
Data length	1 byte
Resolution	1/bit
Operating range	0 – RemoteTachographMonitoring 1 – OnboardWeighingSystem 2 – RemoteTachographMonitoring V2 3 to 255 reserved for further usage

Table 8 Link_ID specification

8.1.2 DSRC_Communication Payload

The payload for the DSRC_Communication PG varies in size according to the application and command specified in the header. Size and content are defined in Annex 2 of this document.

The plain text DSRC payload is either the RTM or the OWS data. The OWS data is supported for future use only. The plain text TachographPayload (and OwsPayload) shall be encoded using OER (Octet Encoding Rules) defined in ISO/IEC 8825-7, Rec. ITU-T X.696 (according to update of DSC_43 in Annex 1C Amendment, see [Annex1C Amendment]). See ASN.1 specification and examples of encoding of the plain text TachographPayload in Annex 2.

All other data, including the RCDTData, in the DSRC-REDCR transactions shall be encoded using UPER (Unaligned Packet Encoding Rules). See examples of RCDTData encoding in Annex 2 (chapter 2.4).

8.2 Application protocol

For ASN.1 definition of the application protocol, see Annex 2 chapter 2.1.

8.2.1 Initialization of the communication link – Request

The initialization of the requested application link shall be done at the start of the engine/when VU is switched on (IGNITION_ON), after the VU has been activated and calibrated. The Link_ID attribute is used in all further messages until the communication is terminated or the communication is restarted after IGNITION ON. If the given application link is already used by another ongoing communication, the DSRC-VU shall answer with a negative acknowledgement in the LinkInitializationResponse message.

The initialization request should be successfully finished with a positive acknowledgement before the cyclic communication starts. In case of no response from the DSRC-VU, the request shall be restarted after a 10 seconds timeout.

Byte pos	Parameter	Value	Type
1	Command_ID	0x00	INTEGER (0..255)
2	Link_ID	See Table 8	INTEGER (0..255)

Table 9 LinkInitializationRequest specification

8.2.2 Initialization of the communication link – Response

LinkInitializationResponse command is used by the DSRC-VU to provide the response of the request to initialize the application link. The command shall be sent by the DSRC-VU to the VU. The command

provides the result of the initialization. If a Link_ID is already in use by a VU, the DSRC-VU shall answer negatively to any other VU trying to use this Link_ID.

Byte pos	Parameter	Value	Type
1	Command_ID	0x01	INTEGER (0..255)
2	Link_ID	See Table 8	INTEGER (0..255)
3	Answer	0x01 (Success) 0x00 (Failure)	INTEGER (0..255)

Table 10 LinkInitializationResponse specification

8.2.3 Send Data

SendData command is used by the VU to send the signed RCDTData (i.e., the remote communication Data) to the DSRC-VU. The data shall be sent every 60 seconds. The Link_ID is used to ensure that the appropriate application link is used. Any message with a false Link_ID or without a previous link established should be rejected by a negative Acknowledgement. Only one ongoing transaction is allowed per each specific application link (Link_ID). If the VU has not received an Acknowledgement within 15 seconds, it shall abort the current transmission.

Byte pos	Parameter	Value	Type
1	Command_ID	0x02	INTEGER (0..255)
2	Link_ID	See Table 8	INTEGER (0..255)
3 to 1785 (variable)	RCDTData	See Annex 2	See Annex 2

Table 11 SendData specification

8.2.4 Acknowledgment of the data

AcknowledgeData is sent by the DSRC-VU to provide the feedback to the VU on the reception of the data from a SendData command. The DSRC-VU shall acknowledge within 10 seconds from received SendData. If a VU receives more than three subsequent answers equal to 0 or if the VU does not receive an AcknowledgeData, the VU shall generate and record an event (‘62’H Remote Communication Facility communication fault). The VU should then terminate and re-initialize the specific link before sending data again. If a Link_ID is already in use by a VU, the DSRC-VU shall answer with negative acknowledgement to any other VU trying to use this Link_ID.

Byte pos	Parameter	Value	Type
1	Command_ID	0x03	INTEGER (0..255)
2	Link_ID	See Table 8	INTEGER (0..255)
3	Answer	0x01(Success) 0x00 (Failure)	INTEGER (0..255)

Table 12 AcknowledgeData specification

8.2.5 Termination of the communication link – Request

LinkTerminationRequest shall be sent by the VU to DSRC-VU to terminate a link for a specific application link (Link_ID). The DSRC-VU shall positively confirm the termination, regardless if the

specific link is initialized or not. In case of no response from the DSRC-VU within 10 seconds, the VU shall regard the link as successfully terminated.

Byte pos	Parameter	Value	Type
1	Command_ID	0x04	INTEGER (0..255)
2	Link_ID	See Table 8	INTEGER (0..255)

Table 13 LinkTerminationRequest specification

8.2.6 Termination of the communication link – Response

Byte pos	Parameter	Value	Type
1	Command_ID	0x05	INTEGER (0..255)
2	Link_ID	See Table 8	INTEGER (0..255)
3	Answer	0x01(Success) 0x00 (Failure)	INTEGER (0..255)

Table 14 LinkTerminationResponse specification

9 Reading of the DSRC-VU serial number

Below are the CAN messages needed to request the DSRC-VU Extended Serial Number from the DSRC-VU. This is the method accepted by the market/OEMs today.

I.e. the tachograph sends a J1939 Request message, to request the DSRC to respond with the DSRC_ExtendedSerialNumber message, which then includes the DSRC Extended Serial Number.

9.1 Request

The request message, identified by the PGN, shall be used to request information from the DSRC_VU. Only information that is not broadcast periodically shall be requested. Table 15 specifies the PG attributes. Table 16 specifies the PG content.

Attribute	Value
Transmission Repetition Rate	On request
Data Length	3 bytes
Extended Data Page	0
Data Page	0
PDU Format	234
PDU Specific	Destination Address (DA)
Default Priority	6
PGN	59904_{10}/$00EA00_{16}$

Table 15 Request attribute specification

Byte pos	Parameter
1-3	PGN being requested (byte 1 is LSB, byte 3 is MSB)

Table 16 Request parameter specification

9.2 DSRC_ExtendedSerialNumber

DSRC_ExtendedSerialNumber PG shall be transmitted by the DSRC_VU on a specific request from any device on the network. Table 17 specifies the PG attributes. Table 18 specifies the PG content. The ExtendedSerialNumber data bytes shall be sent with MSB first.

Attribute	Value
Transmission Repetition Rate	On request
Data Length	8 bytes
Extended Data Page	0
Data Page	0
PDU Format	255
PDU Specific	16 (Default, configurable)
Default Priority	6
PGN	65296_{10}/$00FF10_{16}$ (Default, configurable)

Table 17 DSRC_ExtendedSerialNumber attribute specification

Byte pos	Parameter	Remarks
1-8	DSRC Serial number+ month_year+equipment_type+ manufacturer_code (8 bytes)	According to [Annex1C Appendix 1], chapter 2.72

Table 18 DSRC_ExtendedSerialNumber parameter specification

10 List of Abbreviations

CAN	Controller Area network
Conn_Abort	Connection Abort. See [SAE J1939-21] CTS
DSRC	Dedicated Short Range Communications
ECU	Electronic Control Unit
EndOfMsgACK	End Of Message Acknowledgement. See [SAE J1939-21]
HDEI	Heavy Truck Electronic Interface
OER	Octet Encoding Rules
OWS	On-board Weighing System
PER	Packed Encoding Rules
PG	Parameters Group
PGN	Parameter Group Number
REDCR	Remote Early Detection Communication Reader
RCDT	Remote Communication Digital Tachograph
RTM	Remote Tachograph Monitoring
RTS	Request To Send. See [SAE J1939-21] SAE
SM	Smart Tachograph
VU	Vehicle Unit
VU-OWS	Vehicle Unit – Onboard Weighing System

11 List of Figures

12 List of Tables

Annexes

Annex 1 Example of CAN Sequence

Assumptions:

Tacho Source Address=0xEE DSRC

Source Address=0x7E

DSRC_Communication PGN = 0x00EF00

DSRC← →Tacho

At ignition ON:

←REQUEST:	DSRC_Com	PGN: 0x18EF7EEE len:8 data: 00 00 FF FF FF FF FF FF
		(LinkInitializationRequest, RTM)
→RESPONSE:	DSRC_Com	PGN: 0x18EFEE7E len:8 data: 01 00 01 FF FF FF FF FF
		(LinkInitializationResponse, RTM, ok)

Each 60 seconds:

←COMMAND:	TP.CM_RTS	PGN: 0x18EC7EEE len:8 data: 10 LL LL PP FF 00 EF 00
		(RTS, LLLL bytes, #PP, PGN=00EF00)
→RESPONSE:	TP.CM_CTS	PGN: 0x18ECEE7E len:8 data: 11 PP 01 FF FF 00 EF 00
		(CTS, packet sup PP, next 01)
←COMMAND:	TP.DT	PGN: 0x18EB7EEE len:8 data: 01 02 00 TT TT TT TT TT
		(SeqN=01, SendData, RTM, RCDT=TT)
←COMMAND:	TP.DT	PGN: 0x18EB7EEE len:8 data: 02 TT TT TT TT TT TT TT
		(SeqN=02, RCDT=TT)
…		
←COMMAND:	TP.DT	PGN: 0x18EB7EEE len:8 data: PP TT TT TT TT TT TT TT
		(SeqN=PP, RCDT=TT (fill with 0xFF))
→RESPONSE:	TP.CM_EOMA	PGN: 0x18ECEE7E len:8 data: 13 LL LL PP FF 00 EF 00
		(EndOfMsgACK, LLLL bytes, packets PP)
→RESPONSE:	DSRC_Com	PGN: 0x18EFEE7E len:8 data: 03 00 01 FF FF FF FF FF
		(AcknowledgeData, RTM, ok)

At restart:

←REQUEST:	DSRC_Com	PGN: 0x18EF7EEE len:8 data: 04 00 FF FF FF FF FF FF
		(LinkTerminationRequest, RTM)
→RESPONSE:	DSRC_Com	PGN: 0x18EFEE7E len:8 data: 05 00 01 FF FF FF FF FF
		(LinkTerminationResponse, RTM, ok)

Annex 2 ASN.1 Definitions and Data Examples

2.1 Remote-Communication-DT-Protocol Definition

```
-- Annex 1C DSC_73

-- The value range of link Identifier is limited to 0..255 in this proposed document while it is specified as full INTEGER in [Annex1C] (Appendix 14 DSC_73). The proposal in this document should not be considered to be in conflict with [Annex1C], but it is a recommendation.


Remote-Communication-DT-Protocol DEFINITIONS ::= BEGIN


RCDT-Command ::= SEQUENCE

{

unused INTEGER(0..31), -- waste 5 bit payload RCDT-Payload

}


RCDT-Payload ::= CHOICE

{

link-Initialization-Request [0] RCDT-Communication-Link-Initialization-Request,

link-Initialization-Response [1] RCDT-Communication-Link-Initialization-Response,

send-Data [2] RCDT-Send-Data,

data-Acknowledgment [3] RCDT-Data-Acknowledgment,

link-Termination-Request [4] RCDT-Communication-Link-Termination-Request,

link-Termination-Response [5] RCDT-Communication-Link-Termination-Response

}


RCDT-Communication-Link-Initialization-Request ::= SEQUENCE

{

linkIdentifier INTEGER(0..255) -- 0x00 = RTM, 0x01 = OWS, 0x02 = RTM V2, 0x03..0xFF reserved for future use

}


RCDT-Communication-Link-Initialization-Response ::= SEQUENCE

{

linkIdentifier INTEGER(0..255), -- 0x00 = RTM, 0x01 = OWS, 0x02 = RTM V2, 0x03..0xFF reserved for future use

answer INTEGER(0..255) -- Link initialization accepted: 1 (Success), 0 (Failure)

}


RCDT-Send-Data ::= SEQUENCE

{

linkIdentifier INTEGER(0..255), -- 0x00 = RTM, 0x01 = OWS, 0x02 = RTM V2, 0x03..0xFF reserved for future use

rCDTData SignedTachographPayload

}


RCDT-Data-Acknowledgment ::= SEQUENCE

{

linkIdentifier INTEGER(0..255), -- 0x00 = RTM, 0x01 = OWS, 0x02 = RTM V2, 0x03..0xFF reserved for future use

answer INTEGER(0..255) -- rCDTData correctly received: 1 (Success), 0 (Failure)

}


RCDT-Communication-Link-Termination-Request ::= SEQUENCE

{

linkIdentifier INTEGER(0..255) -- 0x00 = RTM, 0x01 = OWS, 0x02 = RTM V2, 0x03..0xFF reserved for future use

}
```

```
RCDT-Communication-Link-Termination-Response ::= SEQUENCE
{
linkIdentifier INTEGER(0..255), -- 0x00 = RTM, 0x01 = OWS, 0x02 = RTM V2, 0x03..0xFF reserved for future use
answer INTEGER(0..255) -- Link termination accepted: 1 (Success), 0 (Failure)
}
-- Annex 1C, DSC_38 The payload (RTM data) consists of the concatenation of
-- 1. encryptedTachographPayload data, which is the encryption of the TachographPayload
-- defined in ASN.1 in section 5.4.5. The method of encryption is described in Appendix 11
-- 2. dSRCSecurityData, specified in Appendix 11.
-- The SignedTachographPayload corresponds to the payload (RTM data).
-- In the DSRC communication the SignedTachographPayload is the RtmData as per ASN.1
-- definition of DSC_40. SignedTachographPayload ::= RtmData
RtmData ::= SEQUENCE
{
encryptedTachographPayload OCTET STRING (SIZE(67))
        (CONSTRAINED BY { -- calculated encrypting TachographPayload as per Appendix 11 --}),
        dSRCSecurityData OCTET STRING
}
END
```

2.2 Tachograh Payload Definition

The definition is given is the Appendix 14 of the Regulation (EU) 2016/799 amended by regulations (EU) 2018/502 and (EU) 2021/1228.

2.3 Definition of OWS data structure

```
OwsData ::= OBWdata


OBWdata::= SEQUENCE {
recordedWeight                  INTEGER (0..65535),
maximumTechnicalWeight          INTEGER (0..65535),
axlesConfiguration              OCTET STRING (SIZE (4)),
axlesRecordedWeight             OCTET STRING (SIZE (26)),
tp15638Timestamp                INTEGER (0..4294967295),
tp15638DSRCCommunicationError   BOOLEAN,
tp15638OBWCommunicationError    BOOLEAN,
tp15638SecurityBreachAttempt    BOOLEAN
 }
```

2.4 UPER Encoded RCDTData

RCDTDATA (RTMData) shall have the following lenghts:

96 octets (for MAC(8)), 100 octets (for MAC(10)) or 104 octets (for MAC(12)).

Example: sendData with length of RCDTData=67+1+28 = 96 octets (MAC(8)), where 67 octets are the encryptedTachographPayload, 1 octet is the length indicator for the following DSRCSecurityData and the 28 octets are the DSRCSecurityData.

I.e. since the DSRCSecurityData is variable, a length indicator is included in the payload.

VU-RTM -> DSRC-VU: 02 00 87 41 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx

1C 81 10 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx 8E 08 xx xx xx xx xx xx xx xx.

Header	RTM / OWS Payload (hex data)
02 commandID sendData 00 linkIdentifier remoteTachographMonitoring	87 41 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx encryptedTachographPayload **1C** length indicator 81 10 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx dSRCSecurityData (excl MAC) 8E 08 xx xx xx xx xx xx xx xx MAC(8)

Table 19 UPER encoded RCDTData

JRC129396

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub

ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub