



# **Tachograph Remote Download**

## **Command Protocol**

Rev1.3

# INDEX

<b><u>1</u></b>	<b><u>INTRODUCTION.....</u></b>	<b><u>2</u></b>
1.1	BACKGROUND .....	2
1.2	SYSTEM OVERVIEW .....	2
1.3	VEHICLE UNIT (VU) .....	3
1.4	GPRS PROTOCOL COMMAND STRUCTURE .....	3
1.5	FLOWCHART DIAGRAM FOR MUTUAL AUTHENTICATION – SERVER SIDE VIEW. ....	4
<b><u>2</u></b>	<b><u>UNIT COMMAND TYPES .....</u></b>	<b><u>5</u></b>
2.1	SENT BY THE CONTROL CENTRE .....	5
2.2	RECEIVED BY THE CONTROL CENTRE .....	5
<b><u>3</u></b>	<b><u>UNIT COMMAND DESCRIPTION .....</u></b>	<b><u>6</u></b>
3.1	CONTROL CENTRE TO LOCATION UNIT.....	6
3.2	LOCATION UNIT TO CONTROL CENTRE.....	8

**DOCUMENT ORIGIN**

AUTHOR	BUSINESS UNIT	DATE	NOTES
Rui Grafino	HW	16-02-2015	

**CHANGE TRACK**

VERSION	DATE	CHANGES
1.0	16-02-2015	Preliminary version
1.1	02-03-2015	Card Ready ACK included in Positive Response send to Host server. Flow chart changes to reflect these changes. Added missing positive and negative response codes. Tables 1,2,3,4 and 5.
1.2	28-06-2016	Added Remote Transfer Status message
1.3	11-07-2016	Added Open Remote Session message

## 1 Introduction

This document will give a brief introduction to the tachograph remote download procedure, and describes the special command messages to be exchange between Server and VU (Vehicle Unit) to accomplish this procedure.

To better understand the remote download implementation, it's mandatory to read the following documents:

- a) "Digital Tachograph RD Specifications.pdf"
- b) "COMMISSION REGULATION (EC) No 1360\_2002.pdf"
- c) "ISO7816-3"

### 1.1 Background

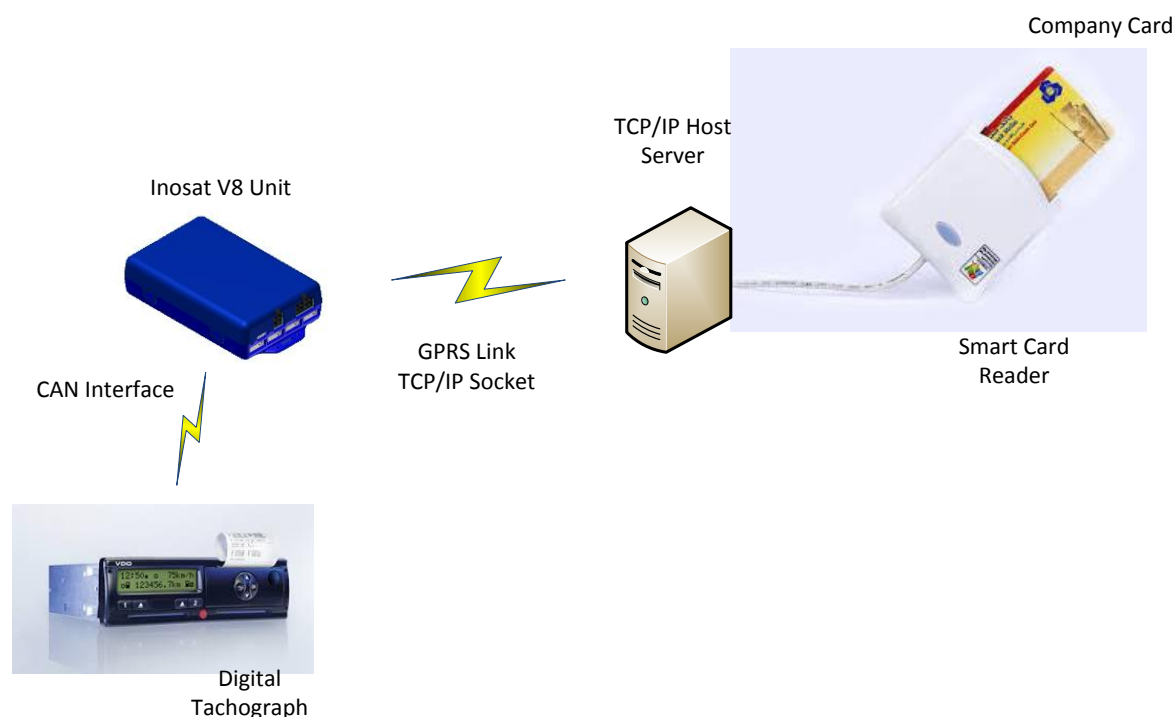
The tachograph registers certain data concerning the transport, for example: vehicle speed and times regarding driver breaks and driving hours. Physically a tachograph is a radio-sized unit in the vehicles driving compartment coupled with a motion sensor.

Previously the data has been recorded with so called analog tachographs. These units have stored the data on circular paper charts by printing on it. However the security around the system has been very poor and various techniques have emerged making it possible to circumvent and manipulate the system. In consequence the tachograph system conflicts with commercial interests of the transport companies.

To rectify the problem, EU has developed a new standard for tachographs to bring it up to phase with technology and security. The new system was called the digital tachograph, which stores information digitally and uses various encryption techniques to ensure data integrity.

From the first of May 2006 all new trucks and busses within EU are required by law to be equipped with the digital tachograph system.

### 1.2 System Overview



As illustrated by the above drawing, it is possible to tachograph data from remote vehicles, without needing to access directly to the VU (Vehicle Unit).

The Fleet Back Office System (Server) is assumed to include a card reader able to communicate with company cards, itself connected to the internet which is able to communicate with the distant vehicles by GPRS Link method.

Specifications of the cards mostly conform to the standard ISO 7816, but with some restrictions stated in appendix 2 of [EC1360/2002].

As specified by [Annex1B], the VU may use any one from the two T=0 and T=1 protocols defined by [ISO7816-3], so the card reader shall also be able to support both protocols.

Equipment able to manage the communication with the company, and also with the tachograph is also supposed to be installed in the vehicles. The unit communicating with the VU is called Fleet Management System (FMS) and is represented in this document by INOSAT V8 Unit.

As illustrated in the drawing, a valid company card shall be first inserted in the Fleet Back Office System card reader, this is necessary to perform the remote authentication.

Remote authentication and data download shall only be possible if only driver cards or no other valid tachograph cards are inserted in the VU.

Any tachograph card insertion in the VU may lead the VU to terminate a remote card authentication or remote data download process currently in progress. But any remote card authentication or remote data download process shall always be terminated by the VU at the insertion of a valid company, control or workshop card into the VU.

Typically, the Server shall start the whole process on its own initiative by sending a request to the vehicle, informing the VU that a remote company card is ready to start a remote authentication process.

### 1.3 Vehicle Unit (VU)

The vehicle unit (VU) is the part of the system most commonly referred to when talking about digital tachographs. It is the size of a car radio, and is placed within sight and reach of the driver.

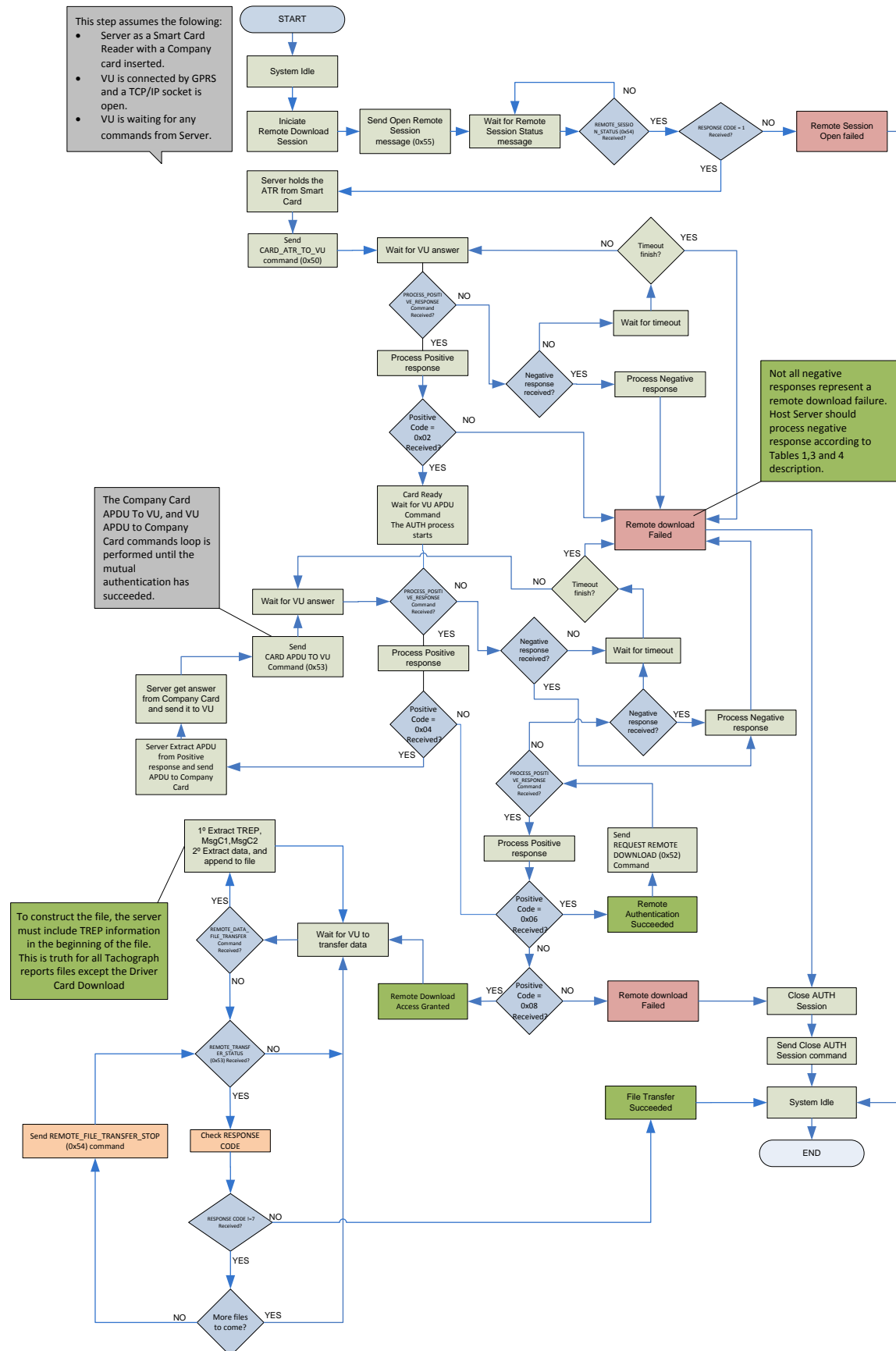
It is equipped with a display, buttons for operation and manual input, and two smart card readers for driver and co-driver, see Figure 2. Further it has embedded memory for storing data (often referred to as the mass memory), a realtime clock and a printer to use if for some reason it is not possible to transfer data from the unit, see figure. The VU is connected to the motion sensor through an encrypted data link, and may also be equipped to other devices through additional connectors.



### 1.4 GPRS Protocol command structure

Inosat's fleet management unit communicates with a server using a proprietary protocol, compatible to the INFOFROTA 4.1, 4.2 and 4.3 protocol. For detail explanation, please read the Inofrota protocol documentation.

## 1.5 Flowchart diagram for Mutual Authentication – Server side view.



## 2 Unit Command Types

The following table shows the short names, description and Type definitions.

### 2.1 Sent by the control centre

Name	Type	Description
CARD_ATR_TO_VU	0x50	Send Server Smart Card ATR to VU (Tachograph).
CARD_APDU_TO_VU	0x51	Send APDU Data and Response Codes to VU (Tachograph).
REQUEST_REMOTE_DOWNLOAD	0x52	Request Tachograph Remote Download File
CLOSE_REMOTE_AUTH	0x53	Ends / terminates the remote authentication process.
REMOTE_FILE_TRANSFER_STOP	0x54	Abort download file transfer procedure.
OPEN_REMOTE_SESSION	0x55	Open remote session between VU (Tachograph).and FMS

### 2.2 Received by the control centre

Name	Type	Description
POSITIVE_RESPONSE	0x50	Send process positive response codes.
NEGATIVE_RESPONSE	0x51	Send process negative response codes.
REMOTE_DATA_FILE_TRANSFER	0x52	Send download data file in packets.
REMOTE_TRANSFER_STATUS	0x53	Send Status of the remote data transfer.
REMOTE_SESSION_STATUS	0x54	Send the remote session Status

**Remark: All remaining command types are reserved for future use.**

## 3 Unit Command Description

### 3.1 Control centre to Location unit

#### CARD ATR TO VU (0x50)

Command	<b><i>CARD_ATR_TO_VU</i></b>				
Description	Send Server Smart Card ATR to VU (Tachograph)				
Type	Control Centre → Location Unit				
Comment					
Command Contents:					
Byte Offset	Number Format	Value	Name	Unit	Description
0	1 Byte	0x50	TYPE	-	Command type
1	1 Byte	-	ATR Size	-	Smart Card ATR Size
2	n Bytes	-	ATR	-	Smart Card ATR Data

#### CARD APDU TO VU (0x51)

Command	<b>CARD_APDU_TO_VU</b>				
Description	Send APDU Data and Response Codes to VU (Tachograph).				
Type	Control Centre → Location Unit				
Comment					
Command Contents:					
Byte Offset	Number Format	Value	Name	Unit	Description
0	1 Byte	0x51	TYPE	-	Command type
1	1 Byte	-	SW2	-	Response Code SW2
1	1 Byte	-	SW1	-	Response Code SW1
2	1 Byte	-	APDU Size	-	Smart Card APDU Size
3	n Bytes	-	APDU	-	Smart Card APDU Data

#### REQUEST REMOTE DOWNLOAD (0x52)

Command	<b><i>REQUEST_REMOTE_DOWNLOAD</i></b>				
Description	Request Tachograph Remote Download File.				
Type	Control Centre → Location Unit				
Comment					
Command Contents:					
Byte Offset	Number Format	Value	Name	Unit	Description
0	1 Byte	0x52	TYPE	-	Command type
1	1 Byte	-	TREP	-	Corresponding to the same values as used in the EC1360/2002 standard: <b>0x01 = Overview</b> <b>0x02 = Activities</b> <b>0x04 = Events and faults</b> <b>0x08 = Detailed speed</b> <b>0x10 = Technical data</b> <b>0x20 = Card download</b>
2	4 Bytes	-	START PERIOD	-	4 byte to represent the start time of the request download period. Combined date and time field, where the date and time are expressed as seconds past 00h.00m.00s. on 1 January 1970 GMT. (Unix Epoch Time)



					Octet Aligned: Number of seconds since midnight 1 January 1970 GMT. The max possible date/time is in the year 2106. <b>1<sup>st</sup> Byte is LSB. 4<sup>th</sup> Byte MSB.</b>
6	4 Bytes	-	END PERIOD	-	4 bytes to represent end time of the request download period. Combined date and time field, where the date and time are expressed as seconds past 00h.00m.00s. on 1 January 1970 GMT. (Unix Epoch Time) Octet Aligned: Number of seconds since midnight 1 January 1970 GMT. The max possible date/time is in the year 2106. <b>1<sup>st</sup> Byte is LSB. 4<sup>th</sup> Byte MSB.</b>
10	1 Byte	-	CARD SLOT	-	Driver Card Slot: <b>0x01 : driver slot</b> <b>0x02 : co-driver slot</b>

## CLOSE REMOTE AUTH (0x53)

Command	<b><i>CLOSE_REMOTE_AUTH</i></b>				
Description	The Back Office ends / terminates the remote authentication process. Note: this command can also be used by the company / FMS to enforce to close any valid authentication.				
Type	Control Centre → Location Unit				
Comment					
Command Contents:					
Byte Offset	Number Format	Value	Name	Unit	Description
0	1 Byte	0x53	TYPE	-	Command type

## REMOTE FILE TRANSFER STOP (0x54)

Command	<b>REMOTE_FILE_TRANSFER_STOP</b>				
Description	Abort download file transfer procedure.				
Type	Control Centre → Location Unit				
Comment					
Command Contents:					
Byte Offset	Number Format	Value	Name	Unit	Description
0	1 Byte	0x54	TYPE	-	Command type

## OPEN REMOTE SESSION (0x55)

Command	<b><i>OPEN_REMOTE_SESSION</i></b>				
Description	Open remote session between VU (Tachograph).and FMS.				
Type	Control Centre → Location Unit				
Comment					
Command Contents:					
Byte Offset	Number Format	Value	Name	Unit	Description
0	1 Byte	0x55	TYPE	-	Command type

## 3.2 Location unit to Control centre

### PROCESS POSITIVE RESPONSE (0x50)

Command	<b><i>PROCESS_POSITIVE_RESPONSE</i></b>				
Description	Send process positive response codes.				
Type	Location Unit → Control Centre				
Comment					
Command Contents:					
Byte Offset	Number Format	Value	Name	Unit	Description
0	1 Byte	0x50	TYPE	-	Command type
1	1 Byte	-	RESPONSE CODE	-	Authentication process positive response code. See Table 2 and 5: Positive Response codes during Remote Authentication (RoutineControl request).  <i>For more information about positive responses, please read page 52, document name “Digital Tachograph Specification for remote company card authentication and remote data downloading” Vers. 02.00 dated 14/09/12.</i>
2	1 Byte	-	APDU Size	-	Smart Card APDU Size
3	n Bytes	-	APDU	-	Smart Card APDU Data If size = 0 NO data is send.

### PROCESS NEGATIVE RESPONSE (0x51)

Command		<b><i>PROCESS_POSITIVE_RESPONSE</i></b>			
Description		Send process negative response codes. Guidance for processing any error case during the remote authentication and data download process			
Type		Location Unit → Control Centre			
Comment					
Command Contents:					
Byte Offset	Number Format	Value	Name	Unit	Description
0	1 Byte	0x51	TYPE	-	Command type
2	2 Bytes	-	RESPONSE CODE	-	Negative response code. See table 1, 3 and 4.  <i>For more information about negative responses, please read page 47, document name “Digital Tachograph Specification for remote company card authentication and remote data downloading” Vers. 02.00 dated 14/09/12.</i>

## REMOTE DATA FILE TRANSFER (0x52)

Command		<b>REMOTE_DATA_FILE_TRANSFER</b>			
Description		Send to server the download data file in packets. Contains the binary data to upload to server.			
Type		Location Unit → Control Centre			
Comment					
Command Contents:					
Byte Offset	Number Format	Value	Name	Unit	Description
0	1 Byte	0x52	TYPE	-	Command type
1	1 Byte	-	TREP	-	Corresponding to the same values as used in the EC1360/2002 standard: <b>0x01 = Overview</b> <b>0x02 = Activities</b> <b>0x03 = Events and faults</b> <b>0x04 = Detailed speed</b> <b>0x05 = Technical data</b> <b>0x06 = Card download</b>
2	1 Byte	-	MsgC2	-	Block Sequence Counter, Message Counter 2 (MsgC2) Message counters will be the same as received when downloading from the tachograph. First data frame will have counter values MsgC1 = 0x01, MsgC2 = 0x00. Actual binary data transferred will be at most 255 – 4 = 251byte. The counters will make it possible to transfer 255 * 255 * 251 = 16 321 275 bytes of data and even more if another byte is used as message counter.
3	1 Byte	-	MsgC1	-	Wrap Around Counter Message Counter 1 (MsgC1)
4	1 Byte	-	SIZE	-	Size of data to transfer.
5	n Bytes	-	DATA	-	Data to transfer (251 bytes max)

## REMOTE TRANSFER STATUS (0x53)

Command	<b>REMOTE_TRANSFER_STATUS</b>				
Description	Send remote transfer status to server				
Type	Location Unit → Control Centre				
Comment					
Command Contents:					
Byte Offset	Number Format	Value	Name	Unit	Description
0	1 Byte	0x53	TYPE	-	Command type
1	1 Byte	-	RESPONSE CODE	-	<b>0x01 - Overview report end</b> <b>0x02 = Activities report end</b> <b>0x03 = Events and faults report end</b> <b>0x04 = Detailed speed report end</b> <b>0x05 = Technical data report end</b> <b>0x06 - Card download report end</b> <b>0x07 - Download end</b>

## REMOTE SESSION STATUS (0x54)

Command	<b>REMOTE_SESSION_STATUS</b>				
Description	Send the remote session Status				
Type	Location Unit → Control Centre				
Comment					
Command Contents:					
Byte Offset	Number Format	Value	Name	Unit	Description
0	1 Byte	0x54	TYPE	-	Command type
1	1 Byte	-	RESPONSE CODE	-	<b>0x00 - Remote Session is not opened</b> <b>0x01 = Remote Session is Opened</b>

**Table 1: Negative Response codes during Remote Authentication (RoutineControl request)**

Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
0x31 10	generalReject	Remote Authentication not valid TAuth not valid	Communication timeout with the remote company card (2 * Trem) has expired	<ul style="list-style-type: none"> <li>- System should send Close Authentication</li> <li>- System should start Remote Authentication from the beginning</li> <li>- If this error code is received for more than 24 hours the correct operation of all system parts must be checked</li> </ul>
			A valid company card, control card or workshop card is inserted in the VU	<ul style="list-style-type: none"> <li>- System should send Close Authentication</li> <li>- System should wait ca. 10 minutes</li> <li>- System should start Remote Authentication from the beginning</li> <li>- If this error code is received for more than 24 hours the correct operation of all system parts must be checked</li> </ul>
			Tauth timeout has expired Tauth has been closed	<ul style="list-style-type: none"> <li>- System should send Close Authentication</li> <li>- System should start Remote Authentication from the beginning</li> <li>- If this error code is received for more than 24 hours the correct operation of all system parts must be checked</li> </ul>
			The VU is not able (for internal reasons) to perform the remote card authentication	<ul style="list-style-type: none"> <li>- System should send Close Authentication</li> <li>- System should start Remote Authentication from the beginning</li> <li>- If this error code is received for more than 24 hours the correct operation of all system parts must be checked</li> </ul>
			Too many errors on low communication layers	<ul style="list-style-type: none"> <li>- Check the application for correct implementation of the communication protocol</li> <li>- If this error code is received for more than 24 hours the correct operation of all system parts must be checked</li> </ul>
0x 31 11	serviceNotSupported	Remote Authentication not valid TAuth valid	The requested service is not supported by the VU	<ul style="list-style-type: none"> <li>- Check the application for correct implementation of the communication protocol</li> <li>- System should send Close Authentication</li> <li>- System should start Remote Authentication from the beginning</li> <li>- If this error code is received for more than 24 hours the correct operation of all system parts must be checked</li> </ul>
			The remote download function is not implemented in the VU	Check whether the VU is supporting remote download function

Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
0x31 12	subFunction NotSupported	Remote Authentication not valid  TAuth valid	The routineControlType parameter is neither startRoutine, stopRoutine nor requestRoutineResults	<ul style="list-style-type: none"> <li>- Check the application for correct implementation of the communication protocol</li> <li>- System should send Close Authentication</li> <li>- System should start Remote Authentication from the beginning</li> <li>- If this error code is received for more than 24 hours the correct operation of all system parts must be checked</li> </ul>
0x31 13	incorrectMessageLength OrInvalidFormat	Remote Authentication not valid  TAuth valid	The request was incorrect	<ul style="list-style-type: none"> <li>- Check the application for correct implementation of the communication protocol</li> <li>- System should send Close Authentication</li> <li>- System should start Remote Authentication from the beginning</li> <li>- If this error code is received for more than 24 hours the correct operation of all system parts must be checked</li> </ul>
			The request was incorrectly processed by the VU	<ul style="list-style-type: none"> <li>- System should send Close Authentication</li> <li>- System should start Remote Authentication from the beginning</li> <li>- If this error code is received for more than 24 hours the correct operation of all system parts must be checked</li> </ul>
0x31 21	busyRepeatRequest	Remote Authentication not valid  TAuth valid	The VU is busy - There are higher priority tasks in the VU than the remote authentication (e.g. card insertion, printout) - The remote authentication process must be delayed for any reason	System should - wait ca. 5 minutes - open the remoteSession again - send the same request again For repeating the complete Remote Authentication the current Authentication has to be closed before (Close Authentication) If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x31 22	conditionsNotCorrect	Remote Authentication not valid (a different one is active)	TAuth is active (another remote authentication process or data transfer is already in progress)	There is a conflict between several authentication processes addressing the same VU. Check the application for correct implementation (System should prevent access to VU from different remote locations) To force a new remote Authentication: - System should send Close Authentication - System should start Remote Authentication from the beginning
		TAuth (a different one) is valid	A different DownloadRequestList has already been received by the VU in the current authentication process.	Check the application for correct implementation (DownloadRequestList)

Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
0x31 24	requestSequenceError	Remote Authentication not valid  TAuth valid	The sequence of the requests of the authentication process is not correct.	Check the application for correct implementation - System should send Close Authentication - System should start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
			The stopRoutine or requestRoutineResults subfunction is received, without having first received a startRoutine for the requested routineIdentifier	Check the application for correct implementation - System should send Close Authentication - System should start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
			The steps of the authentication process are not executed in the right order in the VU	- System should send Close Authentication - System should start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x31 31	requestOutOfRange	Remote Authentication not valid  TAuth valid	The routineIdentifier parameter is not supported (e.g. routineIdentifier 0x0180 is used in subfunctions stopRoutine or requestRoutineResults).	Check the application for correct implementation - System should send Close Authentication - System should start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
			The optional routineControlOptionRecord is not allowed in or contains invalid data for the requested routineIdentifier (e.g. max APDU size read in RemoteCompanyCardReady is strictly below 240 bytes or strictly above 250 bytes, or a period start in the activities of specified calendar day(s) parameter in a RemoteDownloadDataRequest is not immediately followed by a period stop	Check the application for correct implementation - System should send Close Authentication - System should start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked

Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
			The request was incorrect (e.g. wrong card used, wrong data request list format)	Check the application for correct implementation (data request list format, etc.) Check the used cards - System should send Close Authentication - System should start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
			The request was incorrectly processed by the VU	- System should send Close Authentication - System should start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x31 78	requestCorrectlyReceived _ResponsePending	Remote Authentication not valid  TAuth valid	The request is received well and allowed, but the VU needs more time and "ResponsePending" Messages will be send by the VU (e.g. each 4s), until final "PositiveResponse" or "NegativeResponse"	System should wait until the final "PositiveResponse" or "NegativeResponse" is received.  There is no possibility to stop this process by the System



0x31 7F	serviceNotSupported InActiveSession	Remote Authentication not valid	The current session does not support the StartRoutine (RemoteTachographCardDataTransfer) service, only allowed in remoteSession	Check the application for correct implementation System should - open remoteSession - continue Remote Authentication (repeat request to VU) If this error code is received for more than 24 hours the correct operation of all system parts must be checked
		TAAuth valid	The VU has exit the remoteSession for any reason (e.g. the FMS has not sent any request to the VU during 5s or more)	Check the application for correct implementation System should - open remoteSession - continue Remote Authentication (repeat request to VU) If this error code is received for more than 24 hours the correct operation of all system parts must be checked

**Table 2: Positive Response codes during Remote Authentication (RoutineControl request)**

Positive Response Code	Description	Status VU	Possible cause(s)	Recommended system behaviour
0x0C	The VU informs that 3 consecutive errors have occurred with APDU sent to the card.	Remote Authentication not valid  TAuth not valid	Company card read/write problem	<ul style="list-style-type: none"> <li>- System should send Close Authentication</li> <li>- Check the card (e.g. clean card)</li> <li>- System should start Remote Authentication from the beginning</li> <li>- If the same response occurs, please replace the company card with a new company card and start Remote Authentication again</li> </ul>
			Card reader problem	<ul style="list-style-type: none"> <li>- System should send Close Authentication</li> <li>- Check the card reader (e.g. clean card reader)</li> <li>- System should start Remote Authentication from the beginning</li> <li>- If the same response occurs, please replace the card reader with a new card reader and start Remote Authentication again</li> </ul>
			Card damaged	<ul style="list-style-type: none"> <li>- System should send Close Authentication</li> <li>- Replace the company card with a new company card and start Remote Authentication again</li> </ul>
			Card reader use different T=0/T=1 than the VU is requesting	Check the application for correct implementation of the communication protocol with the card reader (see Annex 3)
0x0E	The VU informs that the card authentication has failed	Remote Authentication not valid  TAuth not valid	Company Card expired	<ul style="list-style-type: none"> <li>- System should send Close Authentication</li> <li>- Replace the expired company card with a new valid company card and start Remote Authentication again</li> </ul> <p>Expired, failed or corrupted company cards must be sent back to the relevant Member State Authority.</p>
			Bad card type (not a Company Card)	<ul style="list-style-type: none"> <li>- System should send Close Authentication</li> <li>- Replace the bad card with a valid company card and start Remote Authentication again</li> </ul>

Positive Response Code	Description	Status VU	Possible cause(s)	Recommended system behaviour
			Company Card corrupted (e.g. invalid card public key, invalid card member state public key, failed card certificate verification, failed card member state certificate verification, card type different from 'company', failed card authentication token verification)	- System should send Close Authentication - Replace the bad card with a valid company card and start Remote Authentication again Expired, failed or corrupted company cards must be sent back to the relevant Member State Authority.
			Card reader use different T=0/T=1 than the VU is requesting	Check the application for correct implementation of the communication protocol with the card reader (see Annex 3)
0x10	The VU informs that 5 consecutive authentication errors have occurred (as requested by [Annex 1B Appendix 10], UIA_220)	Remote Authentication not valid  TAuth not valid	Invalid card repetitively used	- System should send Close Authentication - Replace the invalid card with a valid company card and start Remote Authentication again Expired, failed or corrupted company cards must be sent back to the relevant Member State Authority.
			Card reader use different T=0/T=1 than the VU is requesting	Check the application for correct implementation of the communication protocol with the card reader (see Annex 3)

**Table 3: Negative Response codes for RequestUpload**

Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
0x35 10	generalReject	Remote Authentication Not valid	Tauth timeout has expired or has been closed	The System should - stop the download process - send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
		TAuth not valid	A valid company card, control card or workshop card is inserted in the VU	The System should - stop the download process - send Close Authentication - wait for ca. 10 minutes - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x35 11	serviceNotSupported	Remote Authentication is valid  TAuth is valid	The requested service is not supported by the VU	Check the application for correct implementation The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x35 13	incorrectMessageLength OrInvalidFormat	Remote Authentication is valid  TAuth is valid	The request was incorrect	Check the application for correct implementation The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked

Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
			The request was incorrectly processed by the VU	The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x35 21	busyRepeatRequest	Remote Authentication is valid  TAuth is valid	The VU is busy - There are higher priority tasks in the VU than the remote authentication (e.g. card insertion, printout) - The remote authentication process must be delayed for any reason	System should - wait ca. 5 minutes - open the remoteSession again - send the same request again If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x35 22	conditionsNotCorrect	Remote Authentication is valid  TAuth is valid	A data transfer is already in progress, but not yet completed.	Check the application for correct implementation The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
			Rights to download data are not open (no remote download access to data has been granted)	Check the application for correct implementation
			Bad management in the FMS of simultaneous download requests from several companies	Check the application for correct implementation (System should prevent access to VU from different remote locations) To force a new remote Authentication: - System should send Close Authentication - System should start Remote Authentication from the beginning

Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
0x35 31	requestOutOfRange	Remote Authentication is valid  TAuth is valid	The specified dataFormatIdentifier is not equal to 0x00.	Check the application for correct implementation The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
			The specified addressAndLengthFormatIdentifier is not equal to 0x44.	Check the application for correct implementation The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
			The specified memoryAddress is not equal to 0x00000000.	Check the application for correct implementation The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
			The specified memorySize is not equal to 0xFFFFFFFF	Check the application for correct implementation The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
			Bad management in the FMS of simultaneous download requests from several companies	Check the application for correct implementation (System should prevent access to VU from different remote locations) To force a new remote Authentication: - System should send Close Authentication

Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
				- System should start Remote Authentication from the beginning
0x35 78	requestCorrectlyReceived_ResponsePending	Remote Authentication is valid TAuth is valid	The request is received well and allowed, but the VU needs more time and "ResponsePending" Messages will be send by the VU (e.g. each 4s), until final "PositiveResponse" or "NegativeResponse"	System should wait until the final "PositiveResponse" or "NegativeResponse" is received.  There is no possibility to stop this process by the System
0x35 7F	serviceNotSupportedIn ActiveSession	Remote Authentication is valid TAuth is valid	The current session does not support the RequestUpload service, only allowed in remoteSession.	Check the application for correct implementation System should - open remoteSession - repeat request to VU
			The VU has exit the remoteSession for any reason (e.g. the FMS has not sent any request to the VU during 5s or more	Check the application for correct implementation System should - open remoteSession - repeat request to VU

**Table 4: Negative Response codes during TransferData**

Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
0x36 10	generalReject	Remote Authentication not valid	Tauth timeout has expired or has been closed	The System should - stop the download process - send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
		TAuth not valid	A valid company card, control card or workshop card is inserted in the VU	The System should - stop the download process - send Close Authentication - wait for ca. 10 minutes - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x36 11	serviceNotSupported	Remote Authentication is valid  TAuth is valid	The requested service is not supported by the VU	Check the application for correct implementation The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x36 13	incorrectMessageLength OrInvalidFormat	Remote Authentication is valid  TAuth is valid	The request was incorrect	Check the application for correct implementation The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked



Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
			The request was incorrectly processed by the VU	The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x36 21	busyRepeatRequest	Remote Authentication is valid TAuth is valid	The VU is busy - There are higher priority tasks in the VU than the remote authentication (e.g. card insertion, printout) - The remote authentication process must be delayed for any reason	System should - wait ca. 5 minutes - open the remoteSession again - send the same request again For repeating the complete Remote Authentication the current Authentication has to be closed before (Close Authentication) If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x36 22	conditionsNotCorrect	Remote Authentication is valid	A card download is requested, but no driver card is inserted in the relevant slot.	Don't care, continue the current download process Just indicating that there is no Driver Card in the relevant slot
		TAuth is valid	The relevant driver card has been removed.	Don't care, continue the current download process Just indicating that there is no Driver Card in the relevant slot
0x36 24	requestSequenceError	Remote Authentication is valid	No data transfer has been initialised by a preceding RequestUpload service.	Check the application for correct implementation The System should - send RequestUpload - send TransferData of all data types specified in the DownloadRequestList
		TAuth is valid	Bad management of requests sequences	Check the application for correct implementation
0x36 31	requestOutOfRange	Remote Authentication is valid TAuth is valid	The TRTP#2 byte of the TransferData request is not supported by the VU	Check the application for correct implementation - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked

Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
			The TRTP#2 byte of the TransferData request is not the one expected by the VU (i.e. corresponding to the TransferData type in progress)	Check the application for correct implementation - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
			The calendar date specified in the TransferData activities request does not correspond to a day for which activities are stored in the VU (e.g. the requested day is not included in the downloadable period found in the related Overview or the VU was not supplied during that day).	Don't care, continue the current download process Just indicating that there is no data for the day stored in the VU
			The slot specified in the TransferData cardDownload request is not valid	Check the application for correct implementation
			The slot specified in the TransferData cardDownload request is not the one expected by the VU (i.e. corresponding to the TransferData type in progress)	Check the application for correct implementation
			The access to the requested data is denied because the data is not included within the accepted download request list	Check the application for correct implementation continue the current download process Just indicating that this data is not requested and granted from the VU
			The company requested to download activities for a calendar day for which no activities are stored in the VU	Don't care, continue the current download process Just indicating that there is no data for the day stored in the VU
			Bad management of requests sequences	Check the application for correct implementation

Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
0x36 71	transferDataSuspended	Remote Authentication is valid  TAuth is valid	the data transfer operation has been halted due to some internal fault in the VU	Check the application for correct implementation - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication - start Remote Authentication from the beginning If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x36 73	wrongBlockSequence Counter	Remote Authentication is valid  TAuth is valid	The VU has detected an error in the sequence of the blockSequenceCounter/wrapAround Counter	Check the application for correct implementation The System should retry to download the data type for which the error occurred by requesting the first block of the file from the beginning (TransferData request with TRTP#2 byte set to the requested file value, wrapAroundCounter equal to 0x00, blockSequenceCounter equal to 0x01)
			The VU cannot send the data corresponding to the requested blockSequenceCounter / wrapAroundCounter values (the repetition of a TransferData request message with a blockSequenceCounter / wrapAroundCounter equal to the one included in the previous TransferData request message shall be accepted by the VU	Check the application for correct implementation The System should retry to download the data type for which the error occurred by requesting the first block of the file from the beginning (TransferData request with TRTP#2 byte set to the requested file value, wrapAroundCounter equal to 0x00, blockSequenceCounter equal to 0x01)
			There is a mismatch between the block number expected by the VU and the one requested by the FMS, due to an interruption of the data download	The System should retry to download the data type for which the error occurred by requesting the first block of the file from the beginning (TransferData request with TRTP#2 byte set to the requested file value, wrapAroundCounter equal to 0x00, blockSequenceCounter equal to 0x01)
0x36 78	requestCorrectly Received_ ResponsePending	Remote Authentication is valid  TAuth is valid	The request is received well and allowed, but the VU needs more time and "ResponsePending" Messages will be send by the VU (e.g. each 4s), until final "PositiveResponse" or "NegativeResponse"	System should wait until the final "PositiveResponse" or "NegativeResponse" is received.  There is no possibility to stop this process by the System

Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
0x36 7F	serviceNotSupported InActiveSession	Remote Authentication is valid	The current session does not support the TransferData service, only allowed in remoteSession.	Check the application for correct implementation System should - open remoteSession - repeat request to VU: retry to download the data type for which the error occurred by requesting the first block of the file from the beginning (TransferData request with TRTP#2 byte set to the requested file value, wrapAroundCounter equal to 0x00, blockSequenceCounter equal to 0x01)
		TAuth is valid	The VU has exit the remoteSession for any reason (e.g. the FMS has not sent any request to the VU during 5s or more)	Check the application for correct implementation System should - open remoteSession - repeat request to VU: retry to download the data type for which the error occurred by requesting the first block of the file from the beginning (TransferData request with TRTP#2 byte set to the requested file value, wrapAroundCounter equal to 0x00, blockSequenceCounter equal to 0x01)

**Table 5: Negative Response codes during RequestTransferExit**

Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
0x37 10	generalReject	Remote Authentication not valid	Tauth timeout has expired or has been closed	No action (the RequestTransferExit service is used by the System to close the Tauth timeout). This error has no influence on the already downloaded files
		TAuth not valid	A valid company card, control card or workshop card is inserted in the VU	No action (the RequestTransferExit service is used by the System to close the Tauth timeout). This error has no influence on the already downloaded files
0x37 11	serviceNotSupported	Remote Authentication is valid  TAuth is valid	The requested service is not supported by the VU	Check the application for correct implementation The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication This error has no influence on the already downloaded files If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x37 13	incorrectMessageLengthOrInvalidFormat	Remote Authentication is valid  TAuth is valid	The request was incorrect	Check the application for correct implementation The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication This error has no influence on the already downloaded files If this error code is received for more than 24 hours the correct operation of all system parts must be checked
			The request was incorrectly processed by the VU	The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication This error has no influence on the already downloaded files If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x37 21	busyRepeatRequest	Remote Authentication is valid	The VU is busy - There are higher priority tasks in the VU than the remote authentication (e.g. card insertion, printout)	System should - wait ca. 5 minutes - open the remoteSession again - send the same request again

Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
		TAuth is valid	- The remote authentication process must be delayed for any reason	This error has no influence on the already downloaded files If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x37 22	conditionsNot Correct	Remote Authentication is valid TAuth is valid	Unclear: internal conditions in the VU not met	Check the application for correct implementation The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication This error has no influence on the already downloaded files If this error code is received for more than 24 hours the correct operation of all system parts must be checked
0x37 24	requestSequence Error	Remote Authentication is valid TAuth is valid	no data transfer has been initialised (no RequestUpload service has been positively answered)	Check the application for correct implementation The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession restart the download process from the beginning (RequestUpload, and then TransferData of all data types specified in the DownloadRequestList) If this error code is received for more than 24 hours the correct operation of all system parts must be checked
			Bad management of requests sequences	Check the application for correct implementation
0x37 31	requestOutOfRange	Remote Authentication is valid TAuth is valid	The transferRequestParameter#1 is not valid (not equal to 0x00)	Check the application for correct implementation The System should - repeat the request - if the error code is received for more than 5 times during the same remoteSession send Close Authentication This error has no influence on the already downloaded files If this error code is received for more than 24 hours the correct operation of all system parts must be checked
			Bad management of requests sequences	Check the application for correct implementation
0x37 78	requestCorrectlyReceived_ResponsePending	Remote Authentication is valid TAuth is valid	The request is received well and allowed, but the VU needs more time and "ResponsePending" Messages will be send by the VU (e.g. each 4s), until final "PositiveResponse" or "NegativeResponse"	System should wait until the final "PositiveResponse" or "NegativeResponse" is received.  There is no possibility to stop this process by the System

Negative Response code	Description	Status VU	Possible cause(s)	Recommended system behaviour
0x37 7F	serviceNotSupported InActiveSession	Remote Authentication is valid	The current session does not support the RequestTransferExit service, only allowed in remoteSession	Check the application for correct implementation System should - open remoteSession - repeat request to VU retry to download the data type for which the error occurred by requesting the first block of the file from the beginning (TransferData request with TRTP#2 byte set to the requested file value, wrapAroundCounter equal to 0x00, blockSequenceCounter equal to 0x01)
		TAAuth is valid	The VU has exit the remoteSession for any reason (e.g. the FMS has not sent any request to the VU during 5s or more)	Check the application for correct implementation System should - open remoteSession - repeat request to VU (retry to download the data type for which the error occurred by requesting the first block of the file from the beginning (TransferData request with TRTP#2 byte set to the requested file value, wrapAroundCounter equal to 0x00, blockSequenceCounter equal to 0x01)

**Table 5. Positive Response Codes.**

Dir.	Message Type	Message Name	Response Code	Message process	Data
->VU	Request	RemoteCompanyCardReady	01	This message indicates to the VU that a remote company card is inserted in an appropriate card reader and ready to start the mutual authentication protocol. The ATR of the remote company card is attached.	ATR
VU->	Positive Response	VUReady	02	The VU confirms the readiness for starting the mutual authentication protocol.	
->VU	Request	CompanyCardToVUData	03	The FMS provides a tachograph card APDU from the remote company card to the VU.	None or Tachograph card APDU: Remote company card -> VU
VU->	Positive Response	VUToCompanyCardData	04	The VU sends a tachograph card APDU to the remote company card. CompanyCardToVUData and VUToCompanyCardData provide a data transport for the mutual authentication protocol described in Annex 1B, Appendix 11, CSM_020 "Mutual authentication mechanism"	Tachograph card APDU: VU -> Remote company card
			...	Continue with CompanyCardToVUData and VUToCompanyCardData until RemoteAuthenticationSucceeded.	
VU->	Positive Response	RemoteAuthenticationSucceeded	06	The remote mutual authentication process has succeeded.	
->VU	Request	RemoteDownloadDataRequest	07	The FMS provides the Fleet Back Office download request list to the VU.	Download request list.
VU->	Positive Response	RemoteDownloadAccessGranted	08	The VU grants the download access to the requested data.	
->VU	Request	CloseRemoteAuthentication	09	The Back Office ends / terminates the remote authentication process. Note: this command can also be used by the company / FMS to enforce to close any valid authentication.	



The following additional positive responses from the VU to the FMS are used to indicate to the company that an error occurred in one of the steps of the authentication process and to inform the company about the possible reason of the error :

VU->	Positive Response	RemoteAuthenticationClosed	0A	The VU confirms that the authentication process is ended / terminated or a previously valid authentication closed.	
VU->	Positive Response	APDUError	0C	The VU informs the company that 3 consecutive APDU errors have occurred.	
VU->	Positive Response	AuthenticationError	0E	The VU informs the company that the card authentication has failed	
VU->	Positive Response	TooManyAuthenticationErrors	10	The VU informs the company that 5 consecutive card authentication errors have occurred	

Please note that the AuthenticationError and the TooManyAuthenticationErrors messages will be sent by the VU if expired remote company cards are used.