

IDTech Direct Integration Guide



Table of Contents

[Overview](#)

[Device Setup](#)

[JSON Configuration](#)

[Key Status](#)

[Data Encryption Status](#)

[Device Serial Number](#)

[Performing Transactions](#)

[Transaction Flow](#)

[Standard Contact Transactions](#)

[Quickchip Contact Transactions](#)

[Contactless Transactions](#)

[Contact to Fallback Swipe Transactions](#)

[Start Transaction](#)

[Standard Contact Transactions](#)

[Quickchip Contact Transactions](#)

[Contactless Transactions](#)

[Swipe Transactions](#)

[Authenticate Transaction](#)

[Standard Contact Transactions](#)

[Quickchip Contact Transactions](#)

[Contactless Transactions](#)

[Swipe Transactions](#)

[Authorise Transaction Online](#)

[API Request](#)

[Complete Transaction](#)

[Standard Contact Transactions](#)

[Quickchip Contact Transactions](#)

[Contactless Transactions](#)

[Swipe Transactions](#)

[Appendix A.1: EMV Card Swipe on Contact Transaction](#)

[Appendix A.2: Contact to Fallback Swipe Transaction](#)

[Appendix B: Server Request and Response Example](#)

[Appendix C: Cancelling Transactions](#)

Overview

This document describes the process of integrating with Worldnet using IDTech direct commands to communicate to the device. This involves preparing the device, acquiring card data, and sending a server request for authorisation.

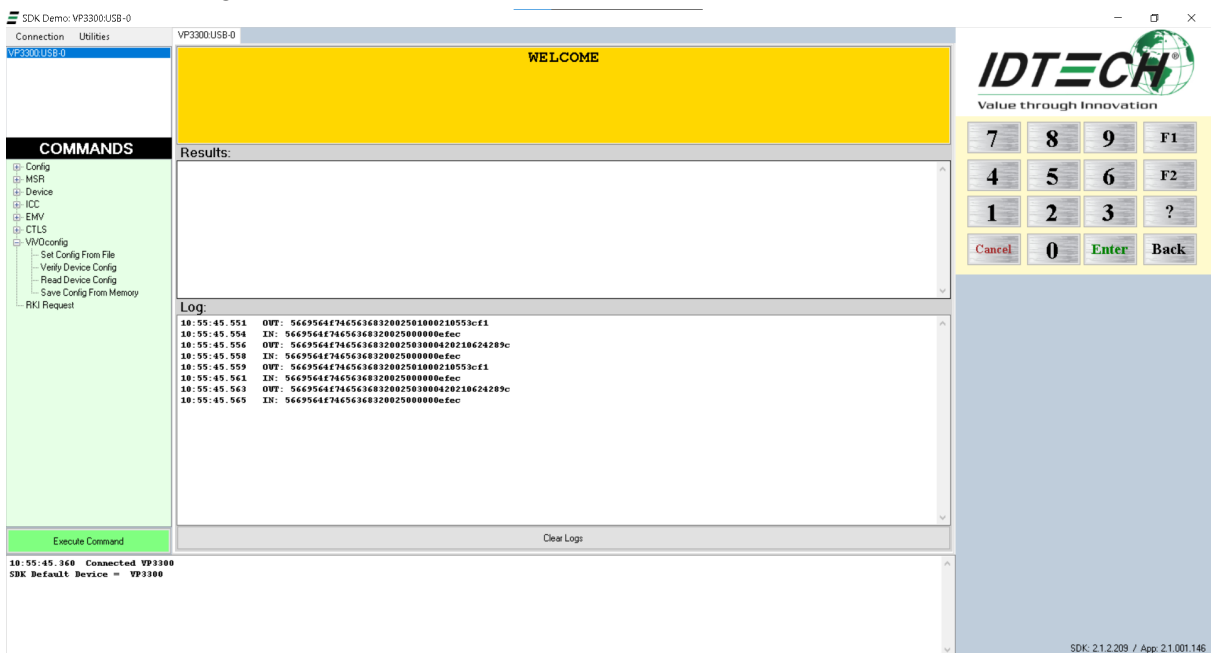
Device Setup

The device must be set up correctly to ensure that it would behave as expected. It should have the proper JSON configuration, the right keys loaded, and its encryption enabled.

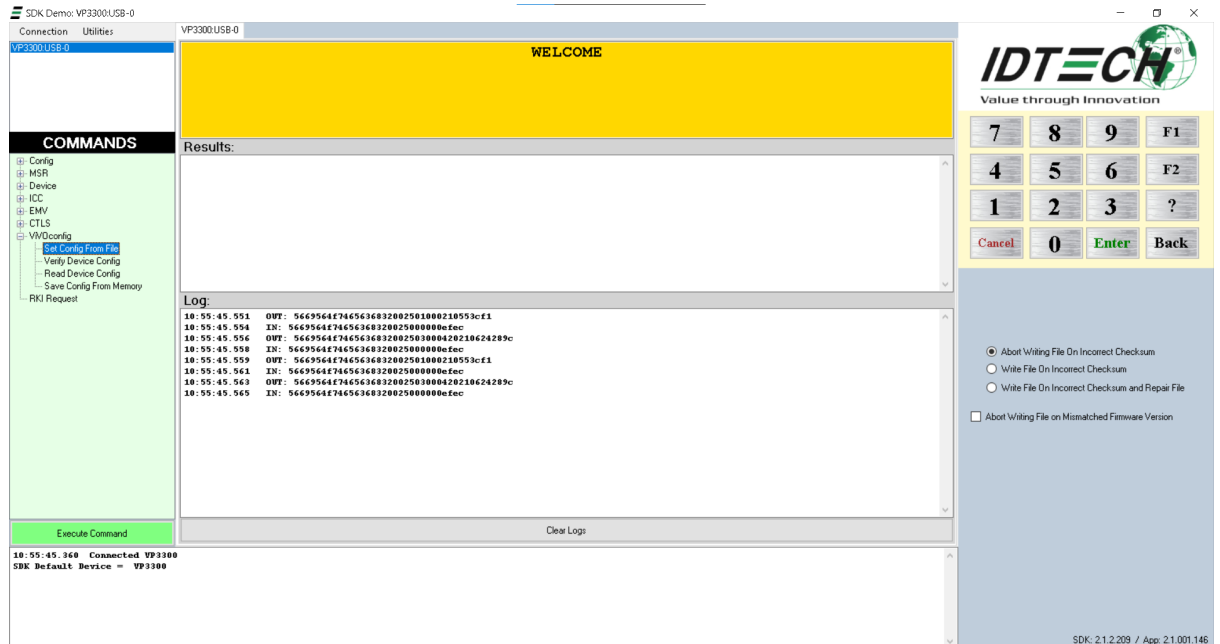
JSON Configuration

Worldnet supports Standard and Quickchip transactions and there is a required JSON configuration file for each type. Please contact our Integration Team for the said files. Once you got the configuration file you need, the next step is to load it to the device using the IDTech SDKDemo software which can be downloaded here [Universal Library for Visual Studio - Home](#) (dot NET SDK Demo.zip). To load the JSON configuration file, please follow the steps below.

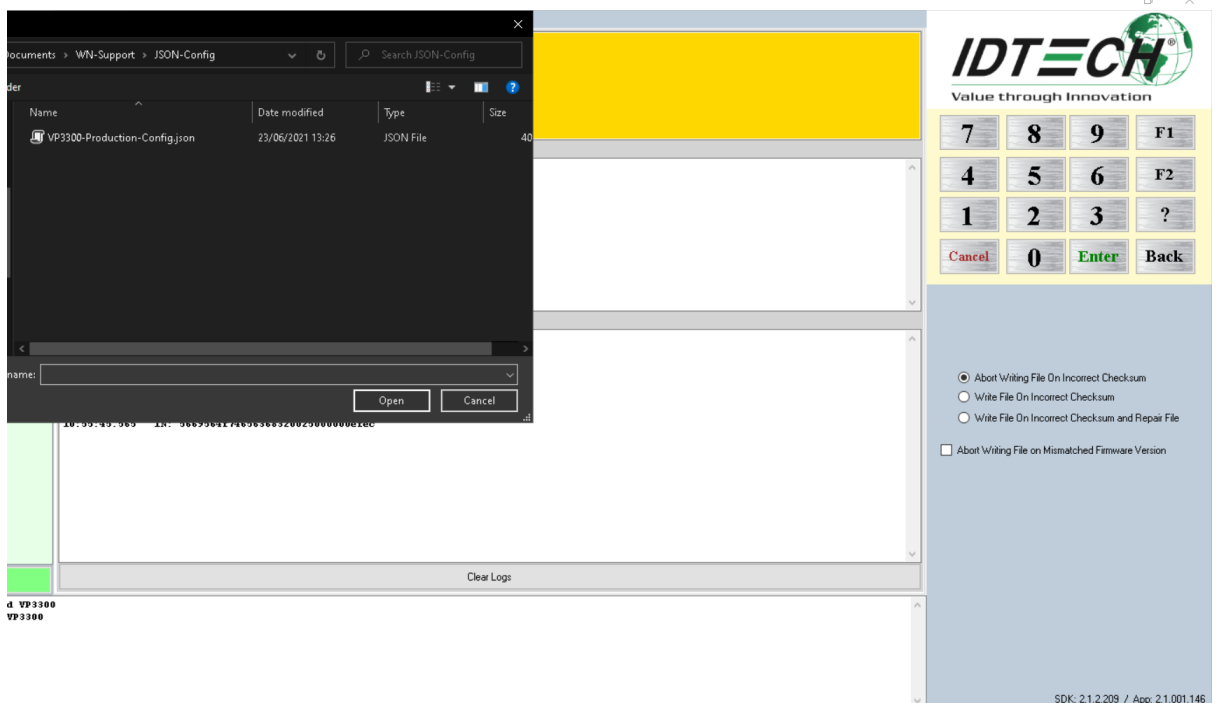
1. With the IDTech SDKDemo opened and your device connected to the machine, look for the VivOconfig option in the Commands panel and expand it.



2. Select the **Set Config From File** command and execute it. A file selection window should appear after.



3. Choose the JSON configuration file that Worldnet provided. The process would start as soon as the file is selected. Please wait as it would take a bit of time.



Key Status

Having keys injected and making sure they are the correct ones are vital as this guarantees that the device would return the required encrypted data for the transactions. To check for the key status, we need to send an IDTech command to the device.

Check DUKPT Keys (81-02)

This command checks and returns the state of the DUKPT key associated with each slot.

Slot 2: RKI-KEK (NSRED and SRED device support, use in Remote Key Injection)

Slot 3: MAC DUKPT Key (SRED device support, for future use)

Slot 5: Data encryption Key (NSRED and SRED device support, use to encrypt transaction output sensitive data)

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ~ Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Sub-Command	Data Length (MSB)	Data Length (LSB)	Data	CRC (LSB)	CRC (MSB)
ViVOtech2\0	81h	02h	00h	00h	None		

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ~ 13+n	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	81h	See Status Code Table	00h	00h or 0Ch	Nothing or Key States		

Sample Command:

5669564f746563683200 81 02 00 00 0b a1

Sample Response:

5669564f746563683200 81 00 00 0c ffff01fff01fffffffff 82 5e

Response data -

Slot 0 - ff

Slot 1 - ff

Slot 2 - 01 - RKI Key Valid

Slot 3 - ff
Slot 4 - ff
Slot 5 - 01 - Data Key Valid
Slot 6 - ff
Slot 7 - ff
Slot 8 - ff
Slot 9 - ff
Slot 10 - ff
Slot 11 - ff

The response data for this command is the key states for each slot.

Possible values for each Key State are:

00h: Unused (Slot is supported but no key injected)

01h: Valid (A valid key is available in this slot)

02h: End of Life (The key on this slot has reached end of life)

FFh: Not Available (This slot is not supported)

To confirm that the device has the right keys, at least slots 2 and 5 must be **valid** (01). If this is not the case, please reach out to our Integration Team.

Data Encryption Status

After we validated that the device is loaded with keys, we need to confirm that the data encryption is enabled on the device. To do this, we also need to send an IDTech command to the device.

Get Data Encryption Enable Flag (C7-37)

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte15
Header Tag & Protocol Version	Command	Sub-Command	Data length (MSB)	Data length (LSB)	CRC (MSB)	CRC (LSB)
ViVOtech2\0	C7h	37h	00	00		

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte14	Byte 15	Byte16
Header Tag & Protocol Version	Command	Status	Data length (MSB)	Data length (LSB)	Data1	CRC (MSB)	CRC (LSB)
ViVOtech2\0	C7h	See Status Code Table	00	01	Encryption Enable Flag		

Sample Command:

5669564f746563683200 c7 37 00 00 5b c6

Sample Response:

5669564f746563683200 c7 00 00 01 03 9c 1c

Response data: 03 - Contact and Contactless EMV and MSR Data encryption is enabled

Encryption Type	Description
Bit 0	0 -> CT/CL EMV Data Encryption Disable (default) 1 -> CT/CL EMV Data Encryption Enable
Bit 1	0 -> MSR/MSD Data Encryption Disable (default) 1 -> MSR/MSD Data Encryption Enable
Bit 2~7	Reserve

If the data encryption is disabled, sending the IDTech command below would enable it.

Set Data Encryption Enable Flag (C7-36)

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15	Byte16
Header Tag & Protocol Version	Command	Sub-Command	Data length (MSB)	Data length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	C7h	36h	00	01	Encryption Enable Flag		

Encryption Type	Description
Bit 0	0 -> CT/CL EMV Data Encryption Disable (default) 1 -> CT/CL EMV Data Encryption Enable
Bit 1	0 -> MSR/MSD Data Encryption Disable (default) 1 -> MSR/MSD Data Encryption Enable
Bit 2~7	Reserve

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Header Tag & Protocol Version	Command	Status	Data length (MSB)	Data length (LSB)	CRC(MSB)	CRC(LSB)
ViVOtech2\0	C7h	See Status Code Table	00	00		

Sample Command:

5669564f746563683200 c7 36 00 01 03 6c 97

Sample Response:

5669564f746563683200 c7 00 00 00 86 6e

Device Serial Number

The serial number is required on the API request. Please make sure to get this value and store it somewhere in the application which is accessible anytime you plan to perform a server request. To acquire the device serial number, please use the IDTech command below.

Get Serial Number (12-01)

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Header Tag & Protocol Version	Command	Sub-Command	Data Length (MSB)	Data Length (LSB)	CRC (LSB)	CRC (MSB)
ViVOtech2\0	12h	01h	00h	00h		

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	12h	See Status Code Table	00h	0Fh	15-digit Serial Number		

The server accepts the serial number as an **ASCII** string so the data response must be converted first before storing it to a field or variable.

Sample Command:

5669564f746563683200 12 01 00 00 18 a5

Sample Response:

5669564f746563683200 12 00 00 0f 373432543038343234340000000000 0b d3

For this case, the device serial number is **742T084244**.

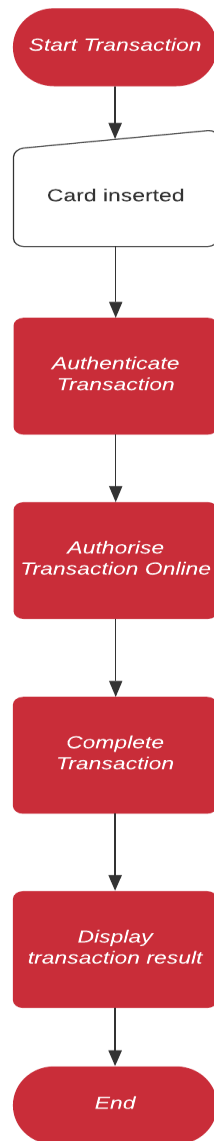
Performing Transactions

This section will describe how to use IDTech raw commands to retrieve the card data and send it to the server for online authorisation. Before performing any type of transactions, please make sure that the correct configuration is loaded.

Transaction Flow

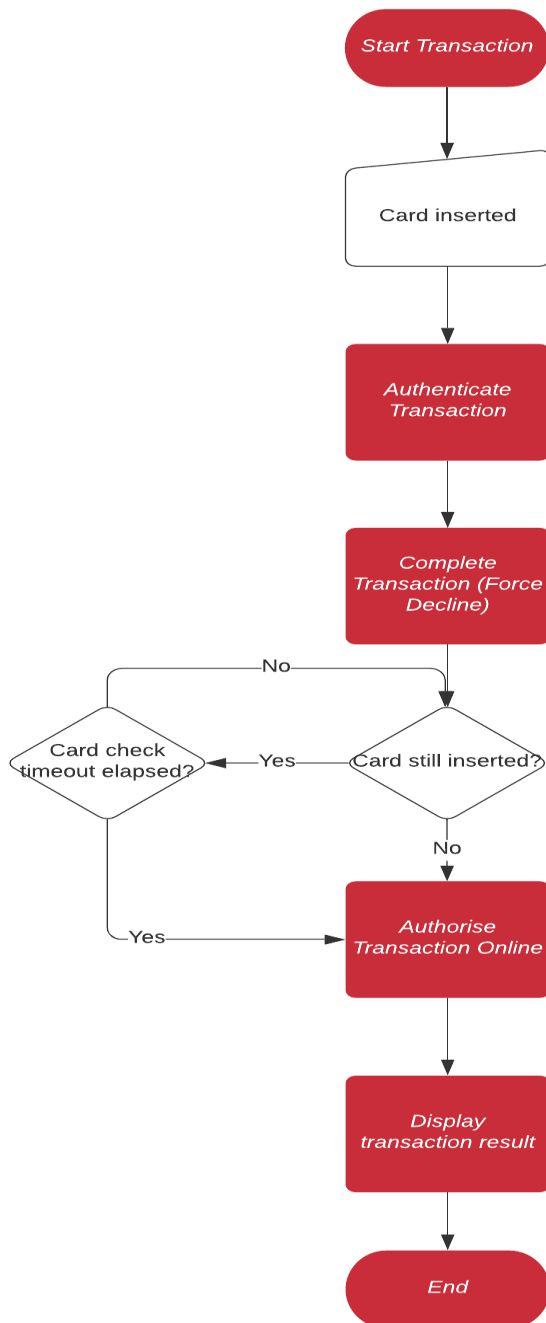
Standard Contact Transactions

Standard Contact Transaction



Quickchip Contact Transactions

Quickchip Contact Transaction



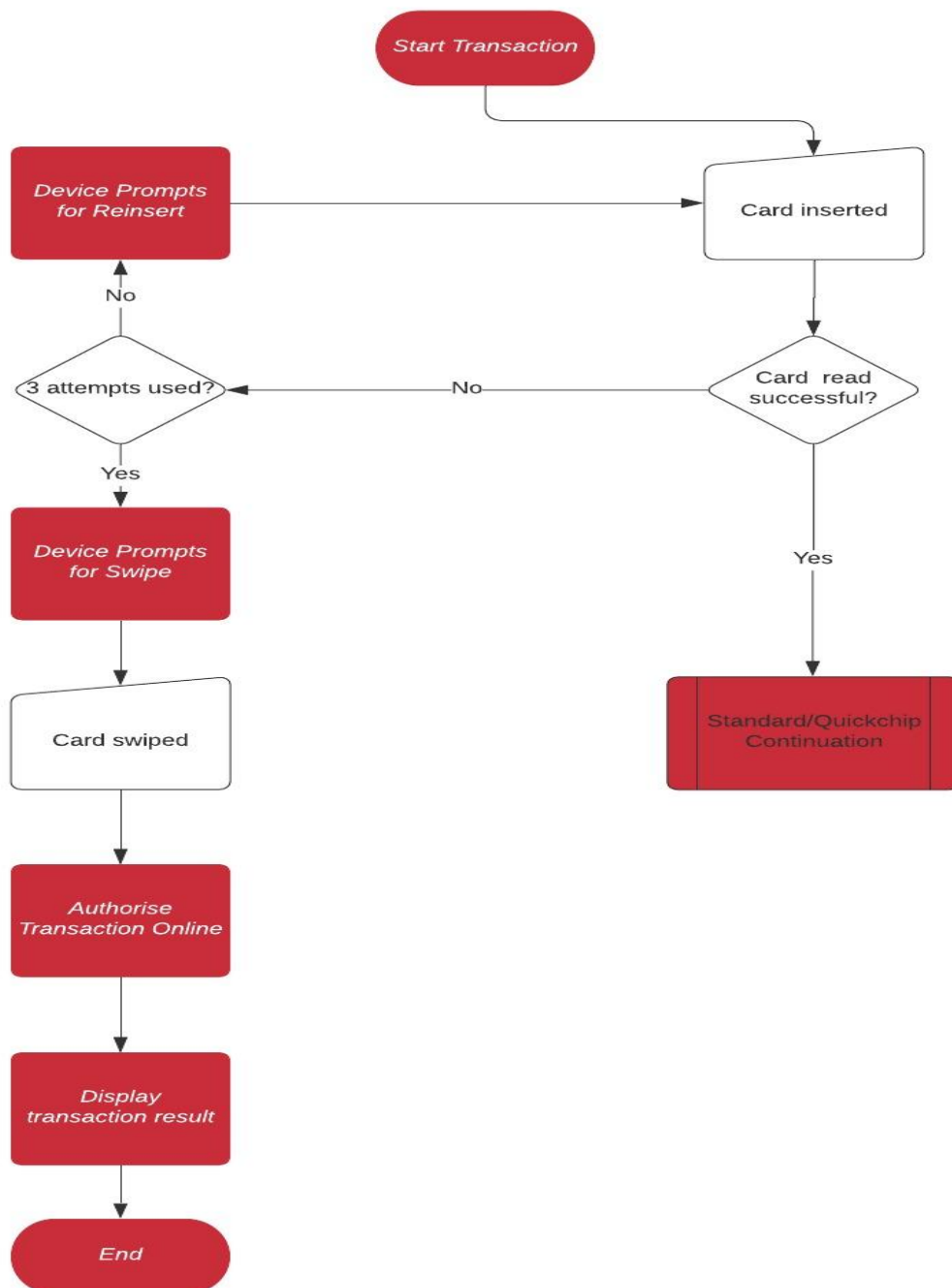
Contactless Transactions

Contactless Transaction



Contact to Fallback Swipe Transactions

Contact to Fallback Swipe Transaction



Start Transaction

Standard Contact Transactions

To start a standard contact transaction, the command below is used.

Contact Start Transaction (60-10)

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Sub- Command	Data Length (MSB)	Data Length (LSB)	Data	CRC (LSB)	CRC (MSB)
ViVOtech2\0	60h	10h			Data Objects		

Data Objects: <FallBack><TimeOut1><TimeOut2><App Data>.

Where:

- <FallBack> (1byte). 0x01 indicates FallBack to MSR support, 0x00 indicates FallBack is unsupported.
- <TimeOut1> (2 bytes, unit is Second). Timeout for card is seated.
- <TimeOut2> (2 bytes, unit is Second). Wait time until "Authenticate Transaction" command.

<App Data> format is <TLV1><TLV2> ... <TLVn>. Refer to Transaction Data.

If the command parse is successful and the ICC transaction starts, the response contains the first command and the status code is 0x63.

If the command parse fails, the response is another status code and end transaction.
The "No terminal data" response is 0x60.

First Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
VIVotech2\0	60h	See Status Code Table	00h	00h			

Because some readers don't support LCD or key pad, the external host often needs to display messages and allow key-in. When a transaction needs to display message or key-in, the device sends command 61-01 to the host.

If a host response is needed, the host responds to command 61-01 and sends the result to reader. On **Start Transaction** success, it sends a second response and the result to host.

Second Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
VIVotech2\0	60h	00h			Data Objects		

Sample Command:

Starting a transaction with fallback to MSR support, an amount of 12.50, card timeout of 30 seconds, and a wait time until *Authenticate Transaction* command of 30 seconds -

```
5669564f746563683200 60 10 00 1a
01001e001e9f02060000000012509f030600000000000009c0100 14 af
```

Sample responses:

Successful command parsing and ICC transaction started -

```
5669564f746563683200 60 63 00 00 ff 0e
```

LCD responses for displaying transaction progress messages on the implementer's application (Please see Contact LCD Display Control (61-01) in the IDTech Developer's Guide for more details) -

Insert/Swipe -

5669564f746563683200 61 01 00 10 0300000200454e0300810b1c02000000 34 c9

Please wait -

5669564f746563683200 61 01 00 10 0300000200454e030081111c02000000 a8 4f

Processing -

5669564f746563683200 61 01 00 100300000200454e0300811a1c02000000 6b ed

Card Data response:

5669564f746563683200 60 00 01 0d

c0ffee120a62994900b90000c00e49dfce2502001057a1132223cccccccc0329d2212201cccc
cccccccc57c118c908819cada8362c1a11b538f25becb00c2145beec54708d5aa1082223ccc
cccc03295ac110633862852591553f0780e524992082cb5f3401015f201a554154205553412
f5465737420436172642032312020202020205f24032212319f20005f25031604015f2d02656
e500a4d4153544552434152444f07a00000000410108407a0000000041010dfce23009f3901
059f1e083254303834323434ffee0104df300101dfef4c06002700000000dfef4d289f8c507657
18dbd7b5d49db62b499391b469d637178b4637f0405bde4c4f33bf405fae6a91c67830dfce26
01c0 5d 31

The card data above is not the one we would be sending to the server.
The correct data is the one returned after the authentication stage.

After getting this successful response, the next step is to authenticate the transaction.

Quickchip Contact Transactions

Same as Standard Contact Transaction

Contactless Transactions

To start a contactless transaction, we need to send the command below.

Activate Transaction Command (02-40)

NOTE: 02-01 is a legacy command, applicable to non-encrypted transactions only. When EMV mode encryption is ON or MSR/MSD encryption is ON, if Data encryption Key is loaded, 02-01 will be disabled. Use 02-40 for production; 02-40 is a unified command for both non-encrypted and encrypted transactions, but if a key is present (unit is injected), encryption will occur.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Sub-Command	Data Length (MSB)	Data Length (LSB)	Data	CRC (LSB)	CRC (MSB)
VIVotech2\0	02h	01h			See Data Format below		

The format and contents of the data field in the Command Frame are given in the following table. *All length values include the Tag and Length bytes.*

Table 45: Activate Transaction Command Frame Data Format

Data Item	Length (bytes)	Description
Timeout	1	Time in seconds that the reader waits for a card to be presented before timing out and returning an Error response. The reader will continue to poll for this amount of time if no card is found. Note that if a card is found, the transaction may not complete within the timeout period. This field must be present in the Activate Command. Format: Binary
TLV Data	varies	See Activate Command TLVs below.

*Please see the IDTech Developer's guide for the TLV data details.

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOTech2\0	02h	See Status Code Table			See Response Frame Data Format		

Sample Command:

Starting a transaction with an amount of 12.50 and a timeout of 30 seconds -

5669564f746563683200 02 40 00 16 1e9f02060000000012509c01009f0306000000000000 f1 34

Sample Response:

5669564f746563683200 02 23 01 ae
c1ffee120a62994900b90000c00e46e1820120500b444953434f56455220434c57a1136510c
cccccc0133d2312201cccccccccccc57c1180d62b8a7cf6e39c5223835de25b59ad1ba01fe
6e5de026005aa1086510cccccccc01335ac110914659706dd447941b2f4b1ca9e7e5f55f2403
2312315f25031902015f2a0208405f2d02656e5f340101820218008407a0000001523010950
500000080009a032106249b0208009c01009f02060000000001009f0306000000000009f06
07a00000015230109f0702ff009f090200019f100a011520900010000080009f1101019f120b4
46973636f76657220434c9f1a0208409f1e08303030303030309f2608763a12a33aec8cb09
f2701809f3602046b9f3704068688459f4104000000019f6604b0804000ffee0108df300100df5
201005f280208409f080200019f1e0832543038343234349f21031330359f33036008c89f350
1259f3901079f4104000000019f530820900010000080009f7102000dfef4c06002700000000
dfef4d28ca95048b9354513a43675c649f740bd8e8e2b08b4ff94ea637c57a79dfe51ab78e2ae
55af1db7b5bdfef2601c1 11 61

After getting this response, take out the data which will be used in the online authorisation request.

Please see [Authorise Transaction Online](#).

Swipe Transactions

Starting a contact or contactless transaction will also enable the MSR interface.

For a couple of cases with Swipe Transactions, please see [Appendix A.1 EMV Card Swipe on Contact Transaction](#) and [Appendix A.2: Contact to Fallback Swipe Transactions](#).

Authenticate Transaction

Standard Contact Transactions

To authenticate a standard contact transaction, please refer to the IDTech command below.

Contact Authenticate Transaction (60-11)

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Sub-Command	Data Length (MSB)	Data Length (LSB)	Data	CRC (LSB)	CRC (MSB)
ViVOtech2\0	60h	11h			Data Objects		

Data Objects : <GoOnline><TimeOut> <Output Data List>.

<GoOnline>(1byte). 0x01 means force the transaction to go online, 0x00 means do not force online (allow normal processing to occur via Terminal Action Analysis).

<TimeOut> (2 byte, unit is Second).means terminal waiting time for host response when online.-

<Output Tag List DFEE1A> format is <TLV> (V is output tag list.)

If command parse is successful and ICC transactions continue, response is first command and status code is 0x63.

If command parse fails, response is some other status code and end of transaction.

First Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
VIVotech2\ 0	60h	See Status Code Table	00h	00h			

When transaction needs display or Get PIN, reader sends command 61-01, 61-02 to host.
If host response is needed, host should respond with command 61-01, 61-02 and send result to reader.
Authenticate Transaction success: send second response and result to host.

Second Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
VIVotech2\ 0	60h	00h			Data Objects		

Sample Command:

Authenticate transaction with the following parameters:

GoOnline - 01 (force online)

TimeOut - 001e (30 seconds)

Output Tag List (DFEE1A) - tags that is requested to be returned

57, dfee04, dfee12, dfee13, dfee14, 86, 9f4e, 9f42, 9f41, 9f40, 9f39, 9f37, 9f36, 9f35, 9f34, 9f33, 9f27, 9f26, 9f21, 9f1e, 9f1c, 9f1a, 9f16, 9f10, 9f0f, 9f0e, 9f0d, 9f09, 9f07, 9f06, 9f03, 9f02, 9f01, 9f1b, 9c, 9b, 9a, 95, 8e, 8d, 8c, 84, 82, 4f, 5f34, 5f30, 5f2a, 5f25, 5f24, 5f20, 5a, 50

5669564f7465636832006011006501001edfee1a5e57dfee04dfee12dfee13dfee14869f4e9f429f419f409f399f379f369f359f349f339f279f269f219f1e9f1c9f1a9f169f109f0f9f0e9f0d9f099f079f069f039f029f019f1b9c9b9a958e8d8c84824f5f345f305f2a5f255f245f205a5067d1

Sample Responses:

Successful command parsing and transaction continues -

```
5669564f746563683200 60 63 00 00 ff 0e
```

LCD responses for displaying transaction progress messages on the implementer's application (Please see Contact LCD Display Control (61-01) in the IDTech Developer's Guide for more details) -

```
5669564f746563683200 61 01 00 10 0300000200454e030081151c02000000 ae ee
```

Card Data response -

```
5669564f746563683200 60 00 02 2d
```

```
c0ffee120a62994900b90000c00e52dfee2502000457a1135413cccccccc411d2212201cccccccccccccccc57c1180110ce1ef16e3bca6d9af383d9c44a72ac22aab4d8e5c302dfee0400dfee1200dfee1300dfee140086009f4e2231303732312057616c6b65722053742e20437970726573732c204341202c5553412e9f420208409f4104000000069f40056000f050019f3901059f3704f9c107479f3602030d9f3501259f34031f03029f33036008c89f2701809f2608b2a818e9857ba2899f21031425019f1e0832543038343234349f1c0838373635343332319f1a0208409f160f3030303030303030303030303030309f10120110a00003220400000000000000000000ff9f0f05b0709c98009f0e0500000000009f0d05b0509c80009f090200029f0702ff009f0607a00000000410109f03060000000000009f02060000000012509f01009f1b04000000009c01009b0248009a03210701950580000080008e0e00000000000000042015e031f038d0c910a8a0295059f37049f4c088c219f02069f03069f1a0295055f2a029a039c019f37049f35019f45029f4c089f34038407a0000000041010820218004f07a00000000410105f3401015f300202015f2a0208405f25032004015f24032212315f201a554154205553412f54657374204361726420303620202020202020205aa1085413cccccccc4115ac1106e3ed65cf14d51502eb203c95c542bc2500a4d415354455243415244ffee0104df300101dfee2601c0dfef7b0100 eb 2c
```

The data part is what we are going to include in the server request for online authorisation. For standard contact transactions, there is still an additional IDTech command to be sent after receiving the response from the server.

Please see [Authorise Transaction Online](#).

Quickchip Contact Transactions

Once the card data response is received from the authentication step, store it to a variable that could be accessed later when it is ready to be sent to the server. Then, we would force the device to decline the transaction by completing it using an IDTech command.

Contact Apply Host Response (60-12) – "Complete Transaction"

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Sub-Command	Data Length (MSB)	Data Length (LSB)	Data	CRC (LSB)	CRC (MSB)
ViVOtech2\0	60h	12h			Data Objects		

Data Objects : <1Byte ComFlag> [<Authorization Response Code (TLV,Tag 8A)>< Issuer Authentication Data (TLV, Tag 91)>< Scripts (TLV, Tag 71/72)>] <Output Data List>

Where:

<1Byte ComFlag>:0x01 indicates went online with host,0x00 indicates unable to go online.

Data in [] indicate these data are optional:

If ComFlag is 0x01, the Data exists.

If ComFlag is 0x00, the Data does not exist.

<Output Tag List DFEE1A> format is <TLV> (V is output tag list.)

Ex: DFEE1A 06 95 5A 84 9F39 50

If command parse is successful, and ICC transaction continues, response is first command and status code is 0x63.

If command parse has failed, response will contain other status code and end transaction.

First Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
VIVotech2\ 0	60h	See Status Code Table	00h	00h			

When transaction needs LCD display or key in, it sends command 61-01 to host.

If the device needs a host response, host should respond with command 61-01 and result to reader.

Second Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
VIVotech2\ 0	60h	00h			Data Objects		

Sample Command:

Complete the transaction with the following parameters:

Comflag - 01

Data Objects -

8a (Authorisation Response Code) - 5a33

dfee1b (ARC define) - 303030315a330000

[5669564f746563683200](#) 60 12 00 11 018a025a33dfee1b08303030315a330000 93 8f

Sample Responses:

Successful command parsing and transaction continues -

5669564f746563683200 60 63 00 00 ff 0e

LCD responses for displaying transaction progress messages on the implementer's application (Please see Contact LCD Display Control (61-01) in the IDTech Developer's Guide for more details) -

Declined -

5669564f746563683200 61 01 00 10 0300000200454e030081071c02000000 3f 2a

Successful data response -

5669564f746563683200 60 00 00 97

c0ffee120a62994900b90000c00e51dfee250200039f1012011020000362040000000000000
 000000ff9f2608ab14957bc8a020af9f2701009f360203049f3704d4f2bf3c9f020600000000125
 09f4d009f4f009f1300950580000080009b0268009f030600000000000009f34035e030099009f
 3901059f1e0832543038343234349f5b00ffee0104df300101dfee2601c0dfef7b0100 19 81

You do not need to do anything about the data above as we already have the card data from the authentication step.

In our solution, when we get this response, we prompt the user to remove the card. We are doing that by checking if the card is still inserted or not using an IDTech command below. We send the method several times until our set timeout has elapsed. If our timeout has been reached, we send the card data for online authorisation. The prompt is just for the user to know that the card is ready to be removed.

Contact Get Reader Status (60-14)

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Sub- Command	Data Length (MSB)	Data Length (LSB)	Data	CRC (LSB)	CRC (MSB)
ViVOTEch2\0	60h	14h			Command Data		

Command Data

Data Item	Length (bytes)	Description/Example
Interface	1	20h = ICC

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOTEch2\ 0	60h	See Status Code Table			Data Objects		

Data Objects (1 byte)

Bit Position	Meaning if '0'	Meaning if '1'
0	ICC Power not ready	ICC Powered
1	Card not seated	Card seated
2	Front switch not detected	Front switch detected
3~7	RFU	RFU

Sample Command:

5669564f746563683200 60 14 00 01 20 fb 14

Sample Responses:

Card seated response -

5669564f746563683200 60 00 00 01 02 c1 8d

Card not seated response -

5669564f746563683200 60 00 00 01 00 e1 cf

Contactless Transactions

The authentication step is not applicable for Contactless Transactions.

Swipe Transactions

The authentication step is not applicable for Swipe Transactions.

Authorise Transaction Online

This section discusses the server API request for authorising the card data from the previous section online and completing the transaction.

API Request

Please see [Appendix B: Server Request and Response Example](#) for the sample API request to authorise the card data from the [Standard Contact Transactions](#) section.

The full API documentation can be found here [Worldnet Merchant API Documentation](#).

Complete Transaction

The sale transaction does not end with the online authorisation. Once the server response is received, there are still a few steps to perform to finalise the transaction depending on its type.

Standard Contact Transactions

Standard contact transactions are required to be completed. This allows us to tell the device whether there is a communication error with the host or the transaction has been successfully authorised online. To do this, we use the same **Complete Transaction**.

Contact Apply Host Response (60-12) – "Complete Transaction"

Complete the transaction with the following parameters:

Comflag - 01

Data Objects -

EMV Tag 8a (Authorisation Response Code)

- "3030" if server **resultCode** under **transactionResult** is "A". Otherwise, "3035"
- could also be derived from tag 8A from server response's **emvTags**

EMV Tag 91 (Issuer Authentication Data)

- from server response's **emvTags** (if any)

If EMV tags 71/72 are present in the response's **emvTags** field, please include them in the command as well.

```
5669564f746563683200 60 12 00 11 018a023030910a26a6e3d08861c4e23030 ea 5e
```

Sample Responses:

Successful command parsing -

```
5669564f746563683200 60 63 00 00 ff 0e
```

LCD responses for displaying transaction progress messages on the implementer's application (Please see Contact LCD Display Control (61-01) in the IDTech Developer's

Guide for more details) -

```
5669564f746563683200 61 01 00 10 0300000200454e030081071c02000000 3f 2a
```

Successful data response -

```
5669564f746563683200 60 00 00 97  
c0ffee120a62994900b90000c00e52dfce250202039f1012011020100322040000000000000000  
000000ff9f2608491c26f64aa523b99f2701009f3602030d9f3704f9c107479f02060000000012  
509f4d009f4f009f1300950580000080009b0268009f030600000000000009f34031f030299009  
f3901059f1e0832543038343234349f5b00ffee0104df300101dfce2601c0dfef7b0100 56 dd
```

After obtaining the successful response, please check the tag **DFEE25 (EMV Result Code)** for the transaction result. This would help determine whether to display an approved/declined message on your application or perform a reversal. Please refer to the IDTech Developer's Guide for the values.

In our implementation, we perform reversals when the **EMV Result Code** is not **EMV_RESULT_CODE_APPROVED** and the server response's **resultCode** under **transactionResult** is "A". Additionally, we only send reversals in production. For testing, it is fine skipping it.

Quickchip Contact Transactions

After receiving the server response, it is up to the implementer to display the transaction results (Approved/Declined message) in the application based on the server response's **resultCode** under **transactionResult**.

Contactless Transactions

Same as Quickchip Contact Transaction

Swipe Transactions

Same as Quickchip Contact Transaction

Appendix A.1: EMV Card Swipe on Contact Transaction

When a contact transaction is started, the device would also accept card swipes. However, swiping an EMV card would cause the device to prompt the user to insert the card.

Assuming a contact transaction is already started, swiping an EMV card would return the following response from the device.

LCD responses for displaying transaction progress messages on the implementer's application (Please see Contact LCD Display Control (61-01) in the IDTech Developer's Guide for more details) -

Use Chip Reader -

5669564f746563683200 61 01 00 10 0300000200454e0300810e1c02000000 77 c8

Appendix A.2: Contact to Fallback Swipe Transaction

For some instances, the device would fail to read the inserted chip card for some reasons such as improper card orientation. The device would respond with a message for prompting the user to try again. If the read still fails after 3 tries, the device would then request for a fallback swipe.

The device already handles insert attempts and switching to fallback swipe. The implementer just needs to display the messages.

Below is a sample Standard Contact to Fallback Swipe transaction.

Sample Command:

Starting a transaction with fallback to MSR support, an amount of 12.50, card timeout of 30 seconds, and a wait time until *Authenticate Transaction* command of 30 seconds -

```
5669564f746563683200 60 10 00 1a
01001e001e9f02060000000012509f0306000000000009c0100 14 af
```

Sample responses:

Here, the card is intentionally inserted the wrong way to trigger fallback.

Successful command parsing and ICC transaction started -

```
5669564f746563683200 60 63 00 00 ff 0e
```

LCD responses for displaying transaction progress messages on the implementer's application (Please see Contact LCD Display Control (61-01) in the IDTech Developer's Guide for more details) -

Please wait -

```
5669564f746563683200 61 01 00 10 0300000200454e030081111c02000000 a8 4f
```

Try ICC again -

Appendix B: Server Request and Response Example

Sample API Request

terminal - the terminal ID which Worldnet provided

orderId - unique identifier for the order

serialNumber - the serial number of the device where the card data is taken from

rawData - the card data obtained from the **Card Data Retrieval** section

```
{
  "channel": "POS",
  "terminal": "136007",
  "order": {
    "orderId": "TPRI_0022",
    "currency": "USD",
    "totalAmount": 12.50
  },
  "customerAccount": {
    "payloadType": "RAW",
    "device": {
      "type": "VP3300_KEM",
      "category": "UNATTENDED",
      "serialNumber": "742T084244"
    }
  },
  "rawData":
  "c0ffee120a62994900b90000c00e52dfee2502000457a1135413cccccccc4111d2212201cccccccccccc57c11801
  10ce1ef16e3bca6d9af383d9c44a72ac22aab4d8e5c302dfee0400dfee1200dfee1300dfee140086009f4e22313037
  32312057616c6b65722053742e20437970726573732c204341202c5553412e9f420208409f4104000000069f400
  56000f050019f3901059f3704f9c107479f3602030d9f3501259f34031f03029f33036008c89f2701809f2608b2a818
  e9857ba2899f21031425019f1e0832543038343234349f1c0838373635343332319f1a0208409f160f30303030303
  03030303030303030309f10120110a000032204000000000000000000ff9f0f05b0709c98009f0e05000000000
  9f0d05b0509c80009f090200029f0702ff009f0607a00000000410109f030600000000000009f02060000000012509f
  01009f1b04000000009c01009b0248009a03210701950580000080008e0e00000000000000042015e031f038d0
  c910a8a0295059f37049f4c088c219f02069f03069f1a0295055f2a029a039c019f37049f35019f45029f4c089f34038
  407a0000000041010820218004f07a00000000410105f3401015f300202015f2a0208405f25032004015f24032212
```

```
315f201a554154205553412f546573742043617264203036202020202020205aa1085413cccccccc41115ac1106e3e
d65cf14d51502eb203c95c542bc2500a4d415354455243415244ffee0104df300101dfce2601c0dfef7b0100"
},
"autoCapture": true,
"processAsSale": false
}
```

Sample API Response

```
{
  "uniqueReference": "JAY1X5WCA4",
  "terminal": "136007",
  "order": {
    "orderId": "TPRI_0022",
    "currency": "USD",
    "totalAmount": 12.50
  },
  "customerAccount": {
    "cardType": "MasterCard",
    "cardholderName": "Test Card 06 Uat Usa",
    "maskedPan": "541333*****4111",
    "expiryDate": "1222",
    "entryMethod": "ICC"
  },
  "securityCheck": {
    "cvvResult": "M",
    "avsResult": "Y"
  },
  "transactionResult": {
    "type": "SALE",
    "status": "READY",
    "approvalCode": "OK120",
    "dateTime": "2021-07-01T09:56:04.58-04:00",
    "currency": "USD",
    "authorizedAmount": 12.50,
    "resultCode": "A",
    "resultMessage": "OK120",
    "storedPaymentCredentials": {
```

```
"terminal": "136007",
"merchantReference": "MREF_e6e24d0b-e198-4918-97ac-115c51340da8UZ",
"credentialsNumber": "2967533404679695",
"maskedPan": "541333*****4111",
"securityCheck": "CVV_VALIDATED"
}
},
"additionalDataFields": [
  {
    "name": "ORDER_NUM",
    "value": "07076317"
  }
],
"emvTags": [
  {
    "hex": "8A",
    "value": "3030"
  },
  {
    "hex": "84",
    "value": "a0000000041010"
  },
  {
    "hex": "91",
    "value": "26a6e3d08861c4e23030"
  }
],
"receipts": [
  {
    "copy": "CARDHOLDER_COPY",
    "header": "CARDHOLDER COPY",
    "merchantDetails": [
      {
        "order": 0,
        "label": "Company",
        "value": "WorldnetTest"
      },
      {
```

```
"order": 1,
  "label": "Address",
  "value": "11 WorldnetTest, SomePlace, SomeStreet, Ireland"
},
{
  "order": 2,
  "label": "Phone",
  "value": "0899998989"
}
],
"transactionData": [
  {
    "order": 0,
    "label": "Cardholder Name",
    "value": "Test Card 06 Uat Usa"
  },
  {
    "order": 1,
    "label": "Card acceptor number",
    "value": "*****4505"
  },
  {
    "order": 2,
    "label": "Terminal ID",
    "value": "****0001"
  },
  {
    "order": 3,
    "label": "Date/Time",
    "value": "Jul 1, 2021 9:56:04 AM"
  },
  {
    "order": 4,
    "label": "Transaction Data Source",
    "value": "ICC"
  },
  {
    "order": 5,
```

```
"label": "Transaction",
"value": "Purchase"
},
{
  "order": 6,
  "label": "Type",
  "value": "Customer Present"
},
{
  "order": 7,
  "label": "Status",
  "value": "READY"
},
{
  "order": 8,
  "label": "Card",
  "value": "541333*****4111 12/22 (MasterCard)"
},
{
  "order": 9,
  "label": "PAN Sequence number",
  "value": "01"
},
{
  "order": 10,
  "label": "Auth Response",
  "value": "OK120"
},
{
  "order": 11,
  "label": "Authorisation Code",
  "value": "OK120"
},
{
  "order": 12,
  "label": "Amount",
  "value": ""
},
}
```

```
{
  "order": 13,
  "label": "Total Amount",
  "value": "USD 12.50"
},
"customFields": [],
"iccData": [
  {
    "order": 0,
    "label": "Mode",
    "value": "Issuer"
  },
  {
    "order": 1,
    "label": "AID",
    "value": "A0000000041010"
  },
  {
    "order": 2,
    "label": "APN",
    "value": "MASTERCARD"
  },
  {
    "order": 3,
    "label": "TVR",
    "value": "8000008000"
  },
  {
    "order": 4,
    "label": "IAD",
    "value": "0110A00003220400000000000000000000FF"
  },
  {
    "order": 5,
    "label": "TSI",
    "value": "4800"
  }
]
```



```
{
  "order": 6,
  "label": "ARC",
  "value": "00"
},
{
  "order": 7,
  "label": "CVM",
  "value": "1F0302"
}
],
"footer": "PLEASE RETAIN FOR YOUR RECORDS"
},
{
  "copy": "CARD_ACCEPTOR_COPY",
  "header": "MERCHANT COPY",
  "merchantDetails": [
    {
      "order": 0,
      "label": "Company",
      "value": "WorldnetTest"
    },
    {
      "order": 1,
      "label": "Address",
      "value": "11 WorldnetTest, SomePlace, SomeStreet, Ireland"
    },
    {
      "order": 2,
      "label": "Phone",
      "value": "0899998989"
    }
  ],
  "transactionData": [
    {
      "order": 0,
      "label": "Cardholder Name",
      "value": "Test Card 06 Uat Usa"
    }
  ]
}
```

```
},
{
  "order": 1,
  "label": "Card acceptor number",
  "value": "*****4505"
},
{
  "order": 2,
  "label": "Terminal ID",
  "value": "****0001"
},
{
  "order": 3,
  "label": "Order ID",
  "value": "TPRI_0022"
},
{
  "order": 4,
  "label": "Unique Ref",
  "value": "JAY1X5WCA4"
},
{
  "order": 5,
  "label": "Date/Time",
  "value": "Jul 1, 2021 9:56:04 AM"
},
{
  "order": 6,
  "label": "Transaction Data Source",
  "value": "ICC"
},
{
  "order": 7,
  "label": "Transaction",
  "value": "Purchase"
},
{
  "order": 8,
```

```
"label": "Type",
"value": "Customer Present"
},
{
  "order": 9,
  "label": "Status",
  "value": "READY"
},
{
  "order": 10,
  "label": "Card",
  "value": "541333*****4111 12/22 (MasterCard)"
},
{
  "order": 11,
  "label": "PAN Sequence number",
  "value": "01"
},
{
  "order": 12,
  "label": "Auth Response",
  "value": "OK120"
},
{
  "order": 13,
  "label": "Authorisation Code",
  "value": "OK120"
},
{
  "order": 14,
  "label": "Amount",
  "value": ""
},
{
  "order": 15,
  "label": "Total Amount",
  "value": "USD 12.50"
}
```

```
],
"customFields": [],
"iccData": [
  {
    "order": 0,
    "label": "Mode",
    "value": "Issuer"
  },
  {
    "order": 1,
    "label": "AID",
    "value": "A0000000041010"
  },
  {
    "order": 2,
    "label": "APN",
    "value": "MASTERCARD"
  },
  {
    "order": 3,
    "label": "TVR",
    "value": "8000008000"
  },
  {
    "order": 4,
    "label": "IAD",
    "value": "0110A000032204000000000000000000FF"
  },
  {
    "order": 5,
    "label": "TSI",
    "value": "4800"
  },
  {
    "order": 6,
    "label": "ARC",
    "value": "00"
  },
]
```

```
{
  "order": 7,
  "label": "CVM",
  "value": "1F0302"
},
"footer": "PLEASE DEBIT MY ACCOUNT WITH TOTAL SHOWN"
]
```

Appendix C: Cancelling Transactions

There would be some cases where you need to cancel a transaction. To do that, please send the IDTech command below.

Cancel Transaction Command (05-01)

After the terminal has issued the Cancel Transaction command, the terminal should not send any commands until it receives a response from the reader. If the reader receives the Cancel Transaction command before it sends the response to an Activate command, it only sends the Cancel Transaction response. The reader then enters an “idle” state and waits for the next command from the terminal.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Header Tag & Protocol Version	Command	Sub-Command	Data Length (MSB)	Data Length (LSB)	CRC (LSB)	CRC (MSB)
ViVOtech2\0	05h	01h	00h	00h		

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	CRC (MSB)	CRC (LSB)
ViVOtech2\0	05h	See Status Code Table	00h	00h		

Sample Command:

5669564f746563683200 05 01 00 00 92 ef

Sample Response:

5669564f746563683200 05 00 00 00 d8 a2