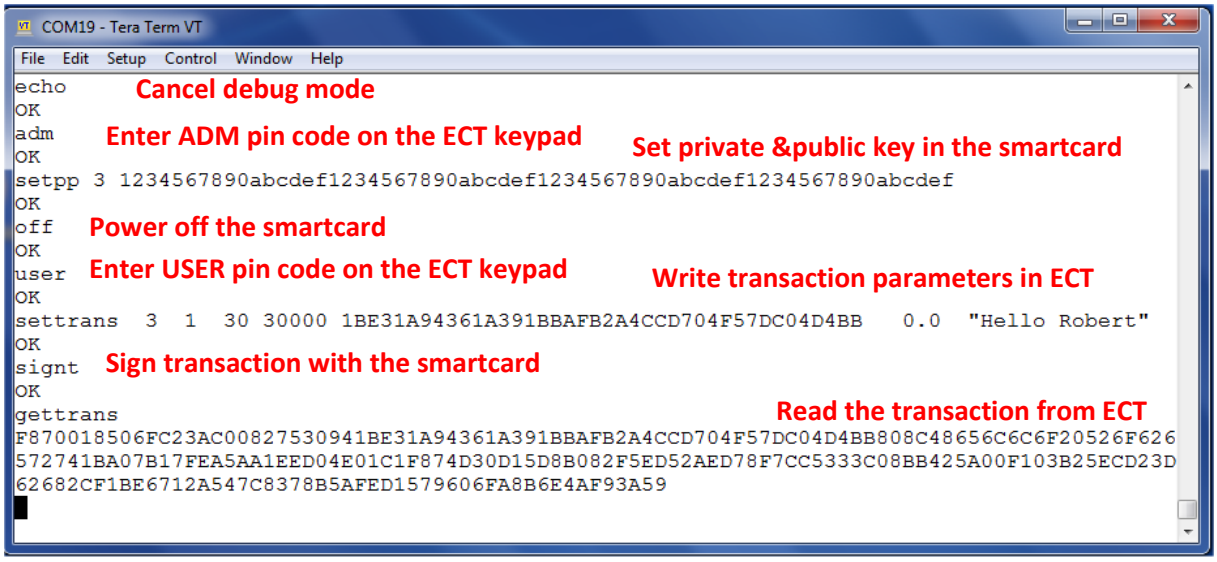
EtherTrust Crypto Terminal User Guide

Setup and introduction to basic functionality v1.0

This section of our user guide explains how to configure the USB connection between a PC/Laptop and the EtherTrust Crypto Terminal (ECT) and to conduct basic transactions, such as importing a private key into the provided smart card, and signing and executing an Ethereum[1] transaction on a test block chain network.

Prerequisites include: PC/Laptop with Windows 7 installed with a USB Port, EtherTrust Crypto Terminal with the appropriate firmware version[2], and the provided USB cable and smart card.

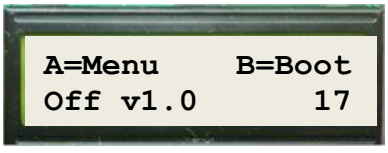


1) Setup

ECT connects to the PC via a USB Serial link, with the following parameters: 115200 bauds, 1 bit stop, no parity, command and response lines end by CrLf characters.

We will first establish a working connectivity between ECT and the Laptop/PC.

To do this, connect the ECT to its USB cable and to a USB port on the PC/Laptop.



The ECT display should light up with a generic message (ECT Main Menu)

Simultaneously Windows should search for a driver to install. Generally Windows will automatically find a driver and install it for you. If it

[1] For this tutorial we are using an Ethereum blockchain account on a test network previously provisioned to facilitate the exercise. EtherTrust crypto terminal supports other blockchain platforms.

[2] For the purpose of this tutorial, we are using an ECT pre-configured with Version 1.0. If you do not have the correct firmware version installed, please update the firmware.

does not you will have to manually download and install it. You can directly download it from the Arduino site:

https://www.arduino.cc/en/Guide/DriverInstallation

Or if available from Ethertrust Web site: http://ethertrust.com/download

Once the driver is installed and working, next we need to be able to communicate with ECT. This is done through a Terminal Emulator. Several options are listed below. For this tutorial we use Tera Term (see below)

1.1) The free/open software btools.exe supports a terminal option ,(use the command line *btools.exe -terminal*)

- https://github.com/purien/btools/blob/version-2_0/btools.exe

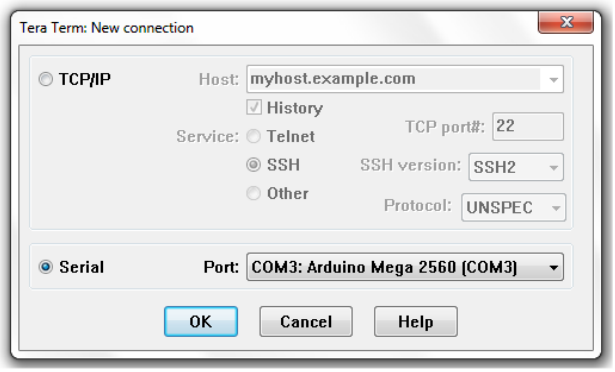
The Windows BTOOLS software has been compiled with VisualC++ 2005. Prior to execution, the Microsoft Visual C++ 2005 Redistributable Package (x64) may be required. It can be found at: https://www.microsoft.com/en-US/Download/confirmation.aspx?id=21254

1.2) Tera Term is free/open terminal software for windows.

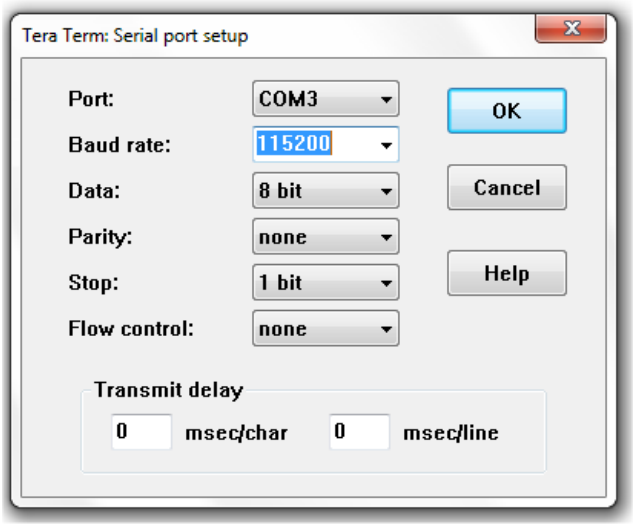
- https://osdn.net/projects/ttssh2/releases/

Please download and install following TeraTerm instructions, and launch TeraTerm.

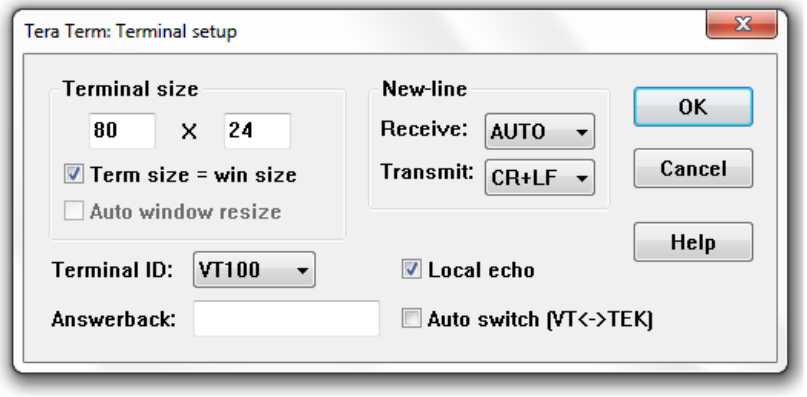
Then select the menu “File”, and the sub menu “New Connection”, and select the “Serial” radio button, and the Port as indicated on the screen shot below, then hit “OK”. If the “Port” box does not show Arduino Mega2560, this means the driver wasn’t properly installed and you need to reinstall it or seek help from Ethertrust.



Then select the menu “Setup” and the sub menu “Serial Port” and enter the parameters exactly as shown on the window below then click “OK”:



Then select the menu “Setup” and the sub menu “Terminal”, enter the parameters as shown on the window below and click “OK”.



Then in the menu “Setup”, select “Save Setup”, and store the setup in a file location you’ll remember on your PC/Laptop.

2) Introduction to basic functionality.

In this section, you will learn how to upload a private key into the smart card using the ECT and sign and execute a transaction on an Ethereum blockchain.

More specifically we will import the following private key:

1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef

into the smart card, and then sign and execute a zero ETHER transaction on the account which address is 0xC847BD66181C1047f4eB6BF21D80BF89104a845a

Insert the smart card in the terminal, if not already present. Make sure it is face down, i.e. secure element facing down.

2.1) Turn-off debug mode

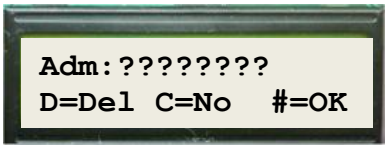
By default the terminal is in debug mode, resulting in unnecessary slower and lengthy responses to command inputs in the terminal emulator window.

In the Terminal Emulator window, type: echo[3], and hit enter

2.2) Switch to ADMIN mode

By default ECT powers off the smartcard. Only a user with ADMIN privileges can import a key onto the smart card.

In the terminal emulator window, type: adm, and hit enter. The ECT will ask you to key in the admin password, which for demo purposes is set at 00000000 (8 zeros)[4]. *On the ECT keypad press # to validate the PIN*.



2.3) Import the private key in the smart card at a defined location of the smart card « index 3"[5]

In the terminal emulator window, type (exactly as shown):

setpp 3 1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef

To facilitate the task, we suggest you copy and paste this entire command, starting with setpp, into the terminal emulator window and then hit enter.

The ECT will ask you to confirm the operation by pressing # on the ECT keyboard[6]. OK should appear on Tera Term.

2.4) Display the Ether address.

You will need this address to generate the upcoming Ether transaction.

Most ECT actions can be initiated from either the Laptop/PC via the Terminal Emulator, or from the ECT keyboard. Because of the ECT limited keyboard/display, it is much easier to initiate them from the Laptop/PC. For this tutorial we'll use the Terminal Emulator. The ECT alternative is provided in footnote. [7]

---

[3] When using Tera Term, you do not see the command appear in the window when you type. If you are in debug mode, it will appear after you hit enter. If not you simply will see OK displayed.

[4] If you wait too long to type in the password you may have to type the adm command again.

[5] The smart card stores up to 16 keys or key trees (BIP32), identified by an index ranging from 0 to 15.

[6] Press firmly but quickly. Keeping the pressure may mislead the ECT into understanding multiple inputs.

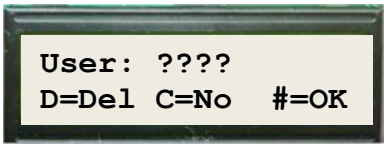
[7] On the ECT main menu, Type A to let the main menu appear, then type 2 to get to the key submenu, type 3 for the Index and the Type A again to access the extended menu, then type 3 to activate the GetPub command (short for get public key), then type 4 for Ether to display the Ether address.

On the Terminal Emulator window, type eth 3, then hit enters. The address appears 1BE31A94361A391BBAFB2A4CCD704F57DC04D4BB on the Terminal Emulator . In the Terminal Emulator window, select edit, select the characters you want to copy, then cut and paste the address in a temporary document in Windows.

2.5) Generate and Sign the Transaction.

Again, this can be done from either the ECT or the PC/Laptop. For convenience let's use the Terminal Emulator window.[8]

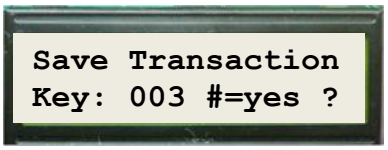
First, for security reasons, decreases your privilege level on the smartcard. This is done by typing the off command on the Terminal emulator, which power off the smartcard.



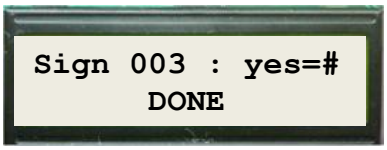
Type user on the Terminal emulator, to switch to user mode. The ECT will ask you to enter the user password, which is set for demonstration purposes at 0000 (4 zeros), then press #

Then in the Terminal emulator window type (or to avoid typos, cut and paste) the entire following line, exactly as is:

```
settrans  3  1  30 30000 1BE31A94361A391BBAFB2A4CCD704F57DC04D4BB   0.0  "Hello Robert"
```



This means that: the transaction will use the key at Index 3, a nonce equal to 1, a Gas Price 30 GWEI, the GasLimit 30000, the Address 1BE31A94361A391BBAFB2A4CCD704F57DC04D4BB, the amount of the transaction 0.0 ETH, and the data included in the transaction the sentence "Hello Robert".



Signing the transaction can either done via the ECT or from the terminal.

- On the Terminal emulator type signt and then press return. Confirm the signature on the ECT terminal by pressing the # key.
- On the ECT, press A to get to the main menu, then press 5 to get to the transaction menu, then 3 for the KeyIndex, then 1 for ETHER, then 4 to sign.

[8] For the more adventurous, here are the steps to generate and sign the transaction from the ECT: Generation: GoTo: A=Menu => 5=Tr => KeyIndex=3 => 1=Eth => 1=Create =>4=N. Adjust the nonce to right (integer) value1, and then press # to save the transaction. Signature : GoTo A=Menu => 5=Tr => KeyIndex=3 => 1=Eth => 4=Sign

Confirm the signature on the ECT terminal by pressing the # key. *!! Press the C (clear) key several time in order to go back to the main menu.*

You can then read the transaction by typing on the PC/Laptop Terminal Emulator Window the command gettrans.

It will then display the transaction:

F870018506FC23AC00827530941BE31A94361A391BBAFB2A4CCD704F57DC04D4BB808C48656C6C6F20526F626572741CA07AF70694ACC0740799AD2A223CA37EE438809E7D2D4260B4B4B3760ACB240110A058F030107F03784D049F7BD99230B20BF7A6376078409BA38690ABF74FA287F5

Keep this information, as you'll need to cut and paste it in the next and final step

2.6) Send the transaction to the blockchain via a WEB page[9]

Open the following URL in your brower https://ropsten.etherscan.io/pushTx. Then cut and paste the transaction value (see screen shots below), then click on "send the transaction", and you are done!

Congratulations!

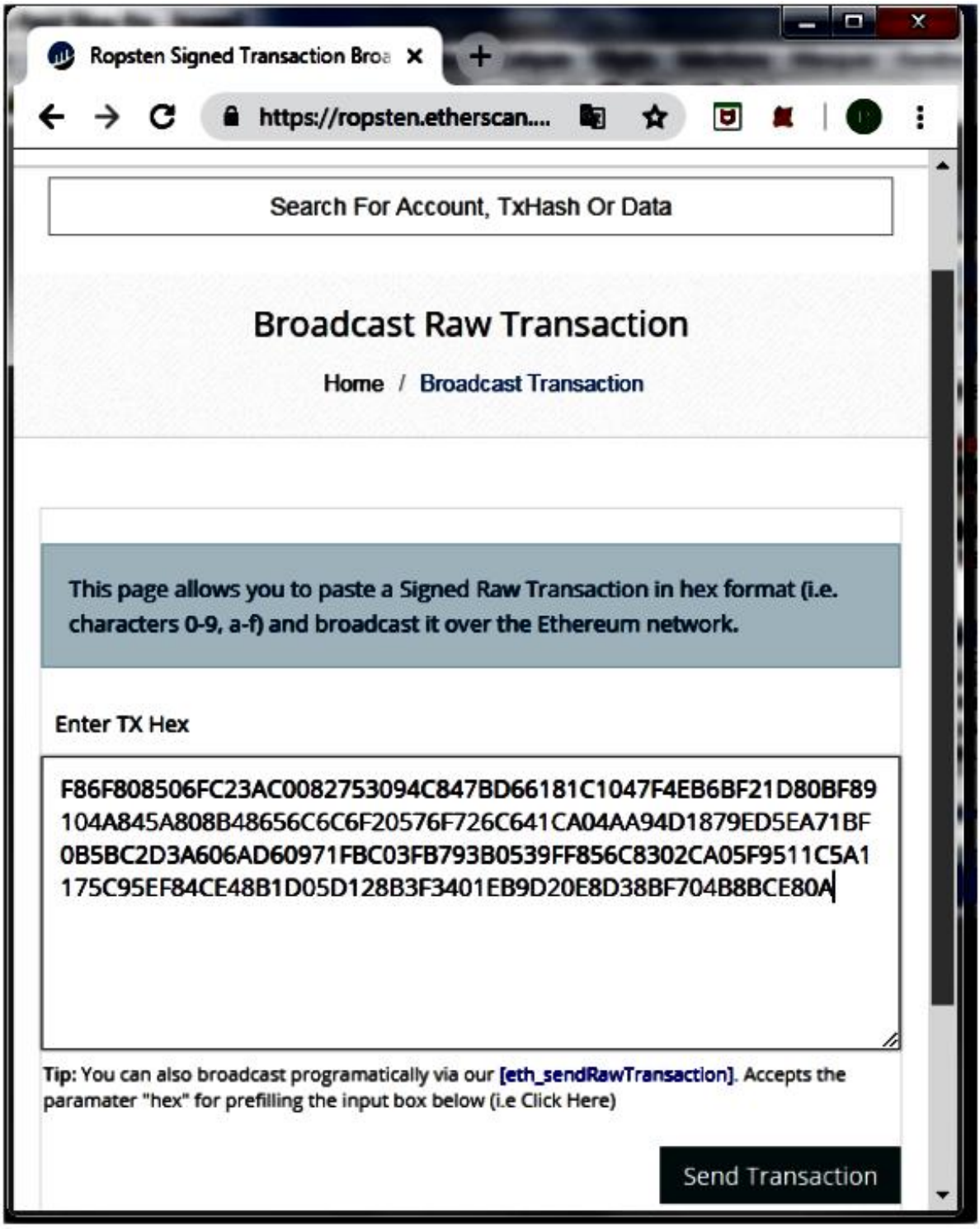
[9] You can also do this via an API. Add the transaction to the prefix:

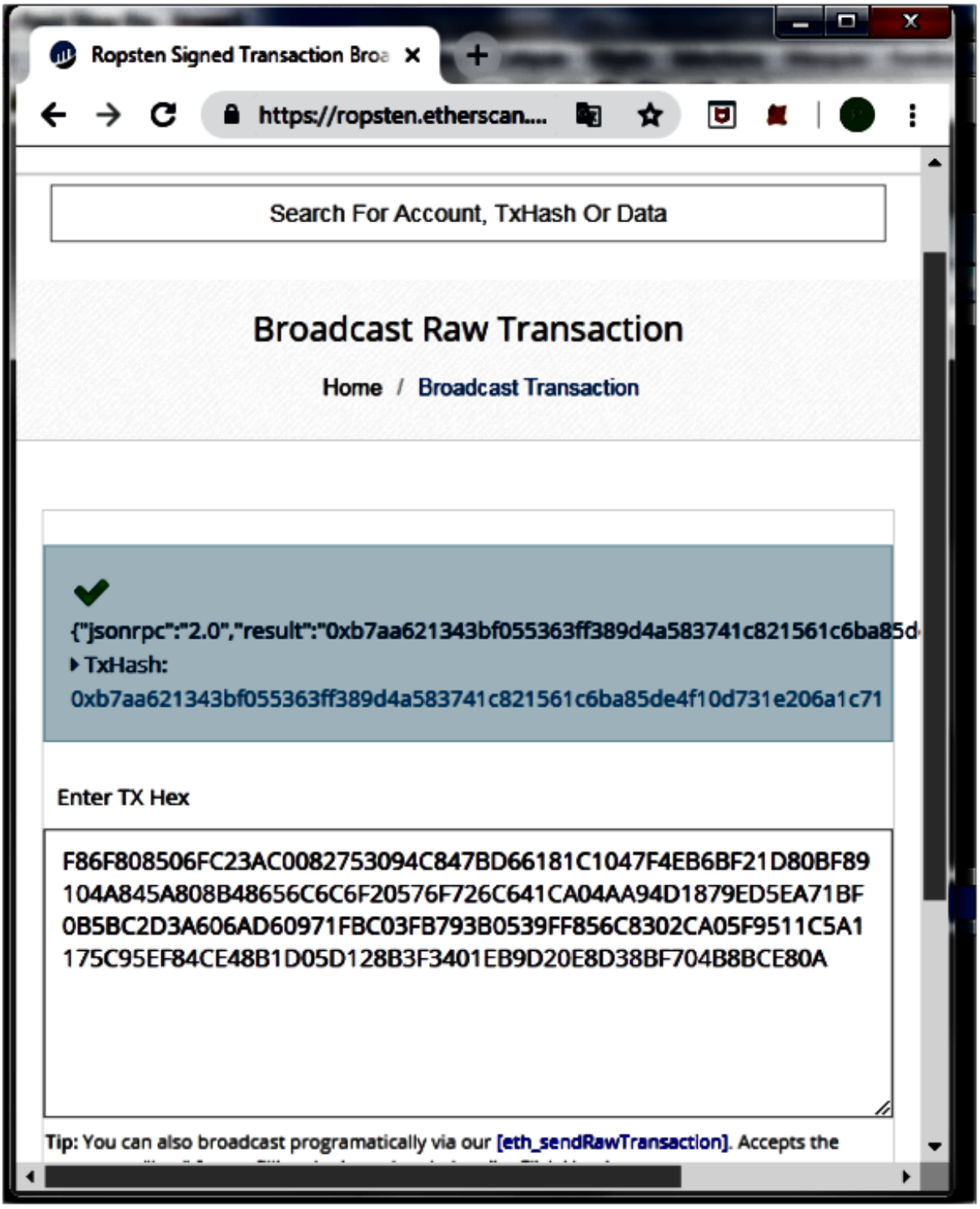
https://api-ropsten.etherscan.io/api?module=proxy&action=eth_sendRawTransaction&hex=0x

as follows:

https://api-ropsten.etherscan.io/api?module=proxy&action=eth_sendRawTransaction&hex=0xF870018506FC23AC00827530941BE31A94361A391BBAFB2A4CCD704F57DC04D4BB808C48656C6C6F20526F626572741CA07AF70694ACC0740799AD2A223CA37EE438809E7D2D4260B4B4B3760ACB240110A058F030107F03784D049F7BD99230B20BF7A6376078409BA38690ABF74FA287F5

The following response indicates the success of the transaction,
{"jsonrpc":"2.0","result":"0x273adb78249be9de8303035b399dd1dbb7699e6b818018fdaa6508f0d6837a9a","id":1} , in which 0x27…9a is the transaction identifier.


Ropsten Signed Transaction Broa
https://ropsten.etherscan....
Search For Account, TxHash Or Data
Broadcast Raw Transaction
Home / Broadcast Transaction
This page allows you to paste a Signed Raw Transaction in hex format (i.e. characters 0-9, a-f) and broadcast it over the Ethereum network.
Enter TX Hex
F86F808506FC23AC0082753094C847BD66181C1047F4EB6BF21D80BF89
104A845A808B48656C6C6F20576F726C641CA04AA94D1879ED5EA71BF
0B5BC2D3A606AD60971FBC03FB793B0539FF856C8302CA05F9511C5A1
175C95EF84CE48B1D05D128B3F3401EB9D20E8D38BF704B8BCE80A
Tip: You can also broadcast programatically via our [eth_sendRawTransaction]. Accepts the paramater "hex" for prefilling the input box below (i.e Click Here)
Send Transaction


Ropsten Signed Transaction Broa
https://ropsten.etherscan....
Search For Account, TxHash Or Data
Broadcast Raw Transaction
Home / Broadcast Transaction
{"jsonrpc":"2.0","result":"0xb7aa621343bf055363ff389d4a583741c821561c6ba85d
TxHash:
0xb7aa621343bf055363ff389d4a583741c821561c6ba85de4f10d731e206a1c71
Enter TX Hex
F86F808506FC23AC0082753094C847BD66181C1047F4EB6BF21D80BF89
104A845A808B48656C6C6F20576F726C641CA04AA94D1879ED5EA71BF
0B5BC2D3A606AD60971FBC03FB793B0539FF856C8302CA05F9511C5A1
175C95EF84CE48B1D05D128B3F3401EB9D20E8D38BF704B8BCE80A
Tip: You can also broadcast programatically via our [eth_sendRawTransaction]. Accepts the