

SZZT_EPP_TEST Operation Description

The EPP of 596E

Suzhen Tan

17/10/2011

1. General

1) What is included

Application Program: SZZT_EPP_TEST.EXE

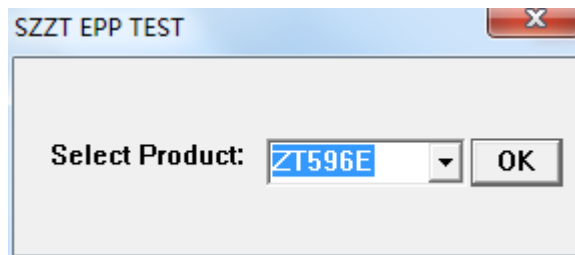
DLL: PIN_CS03_596E.dll

2)

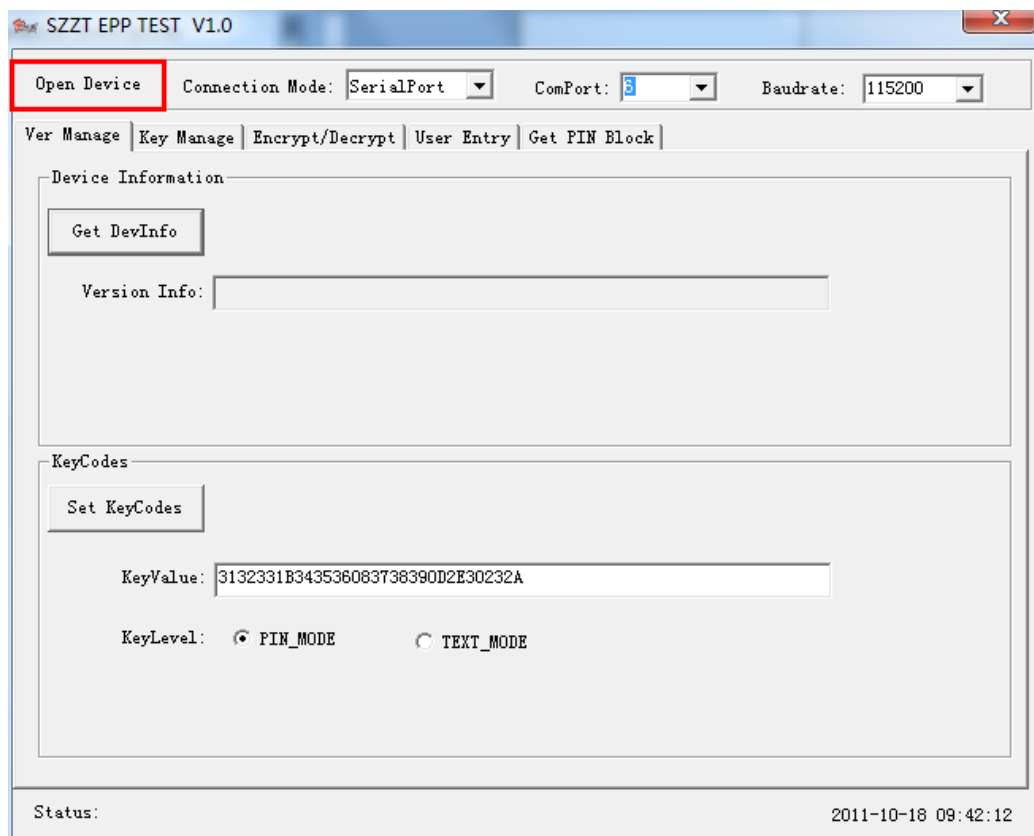
2. Operation Examples

1) Run Application of SZZT_EPP_TEST.EXE

Select the EPP Model "ZT596E", then click the button "OK".

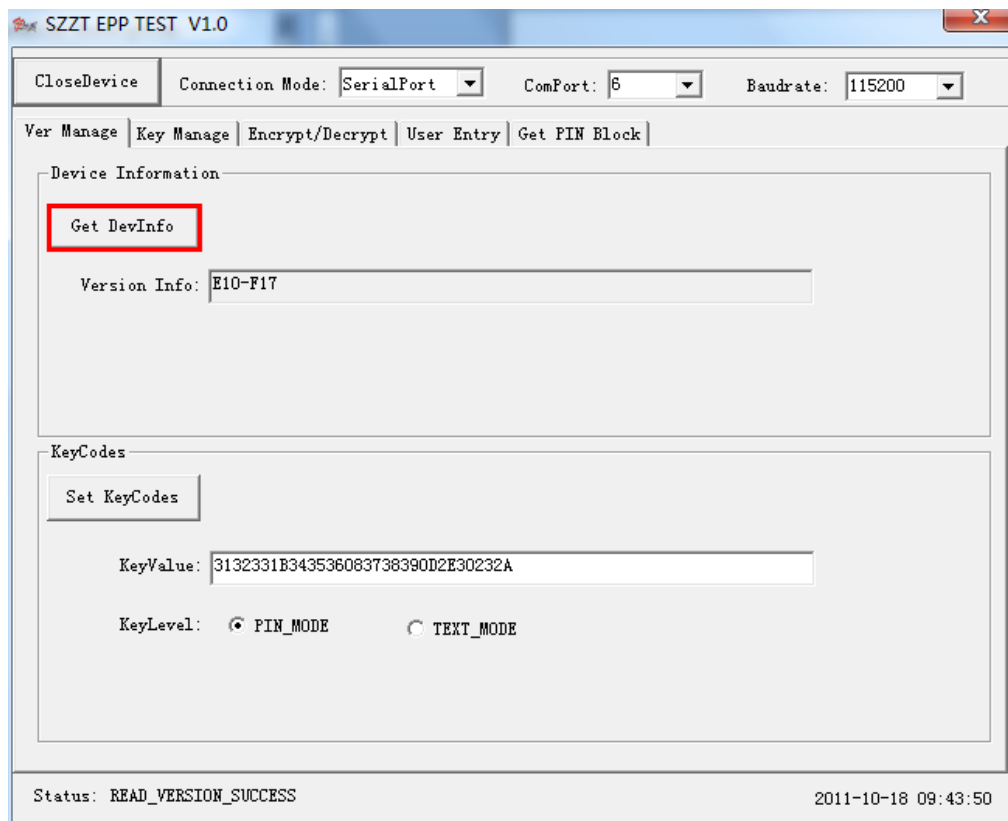


You can select serial communication or USB communication. Set com port and baud rate, if serial communication selected. Then click the button "Open Device".

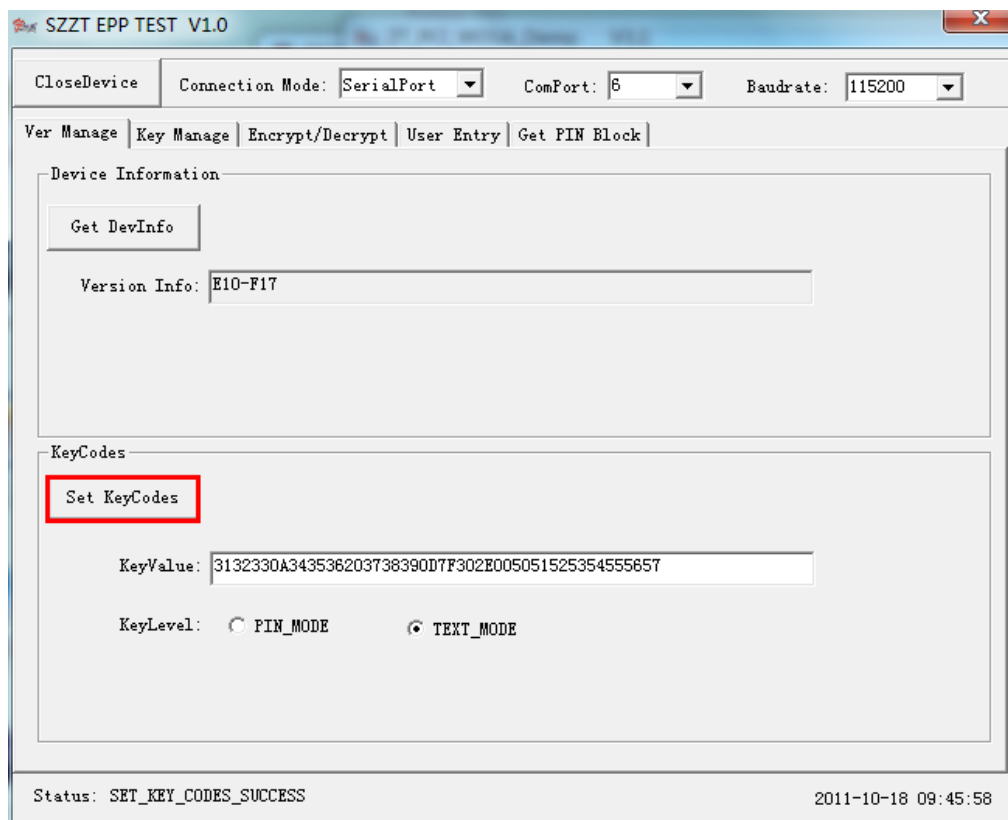


2) Read EPP's Information

Open the tab "Ver manage", then you can read the EPP's Information by click the button "Get DevInfo".



3) SET Key Codes



4) Initialization

Open the tab "Key manage". You can select the mode by selecting the combo-box value, "0" means a reset, while "1" means a Initialization which will delete all DES keys. Then

click the button “Initialization”.

The screenshot shows the 'SZTT EPP TEST V1.0' window. At the top, there are tabs: 'CloseDevice', 'Connection Mode: SerialPort', 'ComPort: 6', and 'Baudrate: 115200'. Below these are more tabs: 'Ver Manage', 'Key Manage', 'Encrypt/Decrypt', 'User Entry', and 'Get PIN Block'. The 'Initialization' section is active, showing a button labeled 'Initialization' (highlighted with a red box), a dropdown menu set to '1', and the text 'Delete all DES key'. Below this is the 'DownloadKey' section, which includes a 'DownloadKey' button, 'KeyNo: 1', 'DecKeyNo: -1', 'WriteMode: SET_MODE' (with a note 'Store the key to cover the existed key'), and a 'Key Val' field containing '0123456789ABCDEF08192A3B4C5D6E7F' and a length of '16'. To the right is the 'KeyAttri' section with radio buttons for 'Master_Key' (selected), 'Pin_Key', 'Data_Key', 'MAC_Key', 'Initialization_vector', and 'Delete_Key'. At the bottom, the 'Check-Key' section has a 'Read KCV' button, 'KeyNo: 1', and a 'Check-key Val' field. The status bar at the bottom shows 'Status: INITIALIZATION_SUCCESS' and the timestamp '2011-10-18 09:47:57'.

5) Download a clear text Master Key

- a. Set the *DecKeyNo* to “-1” (“-1” means clear text key, while others means encrypted key), *WriteMode* to “SET_MODE”, *KeyAttri* to “Master_Key”. Input the Key value, and then click the button “DownloadKey”.

This screenshot shows the same 'SZTT EPP TEST V1.0' window, but now the 'DownloadKey' section is active. The 'DownloadKey' button is highlighted with a red box. The 'KeyNo' is '1', 'DecKeyNo' is '-1' (highlighted with a red box), and 'WriteMode' is 'SET_MODE' (highlighted with a red box). The 'KeyAttri' section has 'Master_Key' selected (highlighted with a red box). The 'Key Val' field still contains '0123456789ABCDEF08192A3B4C5D6E7F' with a length of '16'. The 'Check-Key' section now shows a 'Check-key Val' of '96E4CD5A4A595ECE'. The status bar at the bottom shows 'Status: DOWN_LOAD_KEY_SUCCESS' and the timestamp '2011-10-18 09:50:31'.

- b. Set the *DecKeyNo* to “-1”, *WriteMode* to “SET_MODE”, *KeyAttri* to *Master_Key*.
Input the Key value which will XOR with the exist key, and then click the button
“DownloadKey”.

The screenshot shows the 'SZST EPP TEST V1.0' application window. At the top, there are controls for 'CloseDevice', 'Connection Mode' (set to 'SerialPort'), 'ComPort' (set to '6'), and 'Baudrate' (set to '115200'). Below this is a tabbed interface with 'Ver Manage', 'Key Manage', 'Encrypt/Decrypt', 'User Entry', and 'Get PIN Block'. The 'Key Manage' tab is active, showing two sub-sections: 'Initialization' and 'DownloadKey'. In the 'DownloadKey' section, the 'DownloadKey' button is highlighted with a red box. Below it, 'KeyNo' is set to '1' and 'DecKeyNo' is set to '-1'. The 'WriteMode' dropdown is set to 'XOR_MODE' and is also highlighted with a red box, with a note 'Key is XORed with existing key' next to it. To the right, the 'KeyAttri' section has radio buttons for 'Master_Key' (selected), 'Pin_Key', 'Data_Key', 'MAC_Key', 'Initialization_vector', and 'Delete_Key'. At the bottom of this section, 'Key Val' is a text field containing a long string of zeros, followed by a '16' in a small box. Below the 'DownloadKey' section is the 'Check-Key' section, which includes a 'Read KCV' button, 'KeyNo' set to '1', and a 'Check-key Val' field containing '96E4CD5A4A595ECE'. At the very bottom of the window, the status bar shows 'Status: DOWN_LOAD_KEY_SUCCESS' and the timestamp '2011-10-18 09:53:06'.

6) Download a PIN Key

Download a PIN key by a master key for decrypting; this key will be used to encrypt PIN information.

SZZT EPP TEST V1.0

CloseDevice Connection Mode: SerialPort ComPort: 8 Baudrate: 115200

Ver Manage Key Manage Encrypt/Decrypt User Entry Get PIN Block

Initialization
Initialization 1 Delete all DES key

DownloadKey
DownloadKey

KeyNo: 2 DecKeyNo: 1

WriteMode: SET_MODE Store the key to cover the existed key

Key Val: 11111111111111111111111111111111 16

KeyAttri
☐ Master_Key
☒ Pin_Key
☐ Data_Key
☐ MAC_Key
☐ Initialization_vector
☐ Delete_Key

Check-Key
Read KCV

KeyNo: 2

Check-key Val: 0F6104B94B3EFDD6

Status: DOWN_LOAD_KEY_SUCCESS 2011-10-18 09:54:38

7) Download a Data Key

Download a Data key by a master key for decrypting; this key will be used to encrypt/decrypt Data information.

SZZT EPP TEST V1.0

CloseDevice Connection Mode: SerialPort ComPort: 8 Baudrate: 115200

Ver Manage Key Manage Encrypt/Decrypt User Entry Get PIN Block

Initialization
Initialization 1 Delete all DES key

DownloadKey
DownloadKey

KeyNo: 3 DecKeyNo: 1

WriteMode: SET_MODE Store the key to cover the existed key

Key Val: 22222222222222222222222222222222 16

KeyAttri
☐ Master_Key
☐ Pin_Key
☒ Data_Key
☐ MAC_Key
☐ Initialization_vector
☐ Delete_Key

Check-Key
Read KCV

KeyNo: 3

Check-key Val: 1BAD307CFB1D752B

Status: DOWN_LOAD_KEY_SUCCESS 2011-10-18 09:56:01

8) Download a Mac Key

Download a MAC key by a master key for decrypting; this key will be used to encrypt MAC information.

The screenshot shows the 'SZTZ EPP TEST V1.0' application window. At the top, there are tabs: 'Ver Manage', 'Key Manage', 'Encrypt/Decrypt', 'User Entry', and 'Get PIN Block'. The 'Key Manage' tab is active. Below the tabs, there are settings for 'Connection Mode' (SerialPort), 'ComPort' (6), and 'Baudrate' (115200). The main area is divided into sections: 'Initialization' with a 'Delete all DES key' button; 'DownloadKey' with a 'DownloadKey' button, 'KeyNo' (4), 'DecKeyNo' (1), 'WriteMode' (SET_MODE), and a 'Key Val' field; 'Check-Key' with a 'Read KCV' button, 'KeyNo' (4), and a 'Check-key Val' field. A 'KeyAttri' section on the right has radio buttons for 'Master_Key', 'Pin_Key', 'Data_Key', 'MAC_Key' (selected), 'Initialization_vector', and 'Delete_Key'. The status bar at the bottom shows 'Status: DOWN_LOAD_KEY_SUCCESS' and the timestamp '2011-10-18 09:57:42'.

9) Data Encrypt/Decrypt

The *KeyNO* must be TDK (Data Key), and the *Algorithm* is “CRYPTEDSECB”, “CRYPTDESCBC”, “CRYPTTRIDSECB”, or “CRYPTTRIDESCBC”. Checkbox “Encrypt HEX” ticked means that the data you will enter to be encrypted/decrypted is a sixteen hexadecimal string. Click the button “Data Operation after finished setting the parameters.

SZZT EPP TEST V1.0

CloseDevice Connection Mode: SerialPort ComPort: 6 Baudrate: 115200

Ver Manage Key Manage Encrypt/Decrypt User Entry Get PIN Block

Data-Manager

Data Operation

Algorithm

- ☐ CRYPTDESECB
- ☐ CRYPTDESCBC
- ☐ CRYPTDESMAC
- ☒ CRYPTTRIDSECB
- ☐ CRYPTTRIDSCBC
- ☐ CRYPTTRIDSMAC

Operation-Mode

- ☒ MODEENCRYPT
- ☐ MODEDECRYPT
- ☐ MODERANDOM

KeyNO 3 Padding 00

EnKeyValue

EnKeyLen

Start Val 0000000000000000

Encrypt HEX ☒

Encrypt Val 0001020304050607

Result 577AC5C403F11F1C

Status: CRYPT_SUCCESS 2011-10-18 09:59:09

10) Mac

The *KeyNO* must be TAK (MAC Key), and the *Algorithm* is “CRYPTDESMAC” or “CRYPTTRIDSMAC”. Checkbox “Encrypt HEX” ticked means that the data you will enter to be encrypted is a sixteen hexadecimal string. Click the button “Data Operation” after finished setting the parameters.

SZZT EPP TEST V1.0

CloseDevice Connection Mode: SerialPort ComPort: 6 Baudrate: 115200

Ver Manage Key Manage Encrypt/Decrypt User Entry Get PIN Block

Data-Manager

Data Operation

Algorithm

☐ CRYPTDESECB
☐ CRYPTDESCBC
☐ CRYPTDESMAC
☐ CRYPTTRIDESECB
☐ CRYPTTRIDESCBC
☒ CRYPTTRIDESMAC

Operation-Mode

☐ X9.9
☒ X9.19
☐ CBC
☐ PBOC
☐ China Union Pay

KeyNO 4 Padding 00

EnKeyValue

EnKeyLen

Start Val 0000000000000000

Encrypt HEX ☒

Encrypt Val 0001020304050607

Result 3B6A19E426EB6013

Status: CRYPT_SUCCESS 2011-10-18 10:00:01

11) PIN Test

- a. Open the tab "User Entry". Set the entry mode to "MODE_PIN", and then click the button "OpenKeyBoard". If the Status shows "OPEN_KEYBOARD_SUCCESS", says the encrypting pin pad have been opened success, then you can entry your password and end with the "enter" key.

SZZT EPP TEST V1.0

CloseDevice | Connection Mode: SerialPort | ComPort: 6 | Baudrate: 115200

Ver Manage | Key Manage | Encrypt/Decrypt | User Entry | Get PIN Block

User Entry

OpenKeyBoard | Mode: ☐ MODE_TEXT ☒ MODE_PIN ☐ MODE_KEY

CloseKeyBoard | Input Val: *****

Clear

Status: OPEN_KEYBOARD_SUCCESS 2011-10-18 10:01:30

- b. Open the tab "Get PIN Block". The KeyNO must be TPK (PIN Key). Click the button "Get PINBlock" after setting the parameters.

SZZT EPP TEST V1.0

CloseDevice | Connection Mode: SerialPort | ComPort: 6 | Baudrate: 115200

Ver Manage | Key Manage | Encrypt/Decrypt | User Entry | Get PIN Block

Get PINBlock

KeyNO: 2 | EnKeyNO: | Padding: 0F | PinLen: 6

VI: 0

CustomerData: 1234567890123

XORData:

PIN Block: 55A0BE6433360536

PIN Block Len: 8 | Clear

PIN-Type

- ☒ IBM3624
- ☐ ANSI9.8
- ☐ ISO-0
- ☐ ISO-1
- ☐ ECI2
- ☐ ECI3
- ☐ VISA
- ☐ DIEBOLD
- ☐ DIEBOLDCO
- ☐ VISA3
- ☐ BANKSYS
- ☐ EMV
- ☐ ISO3

Status: GET_PIN_SUCCESS 2011-10-18 10:02:09

12) Clear Test

Click the button of “OpenKeyBoard”, and then you can input key form EPP. Click the button of “CloseKeyBoard”, if you want to end the entry.

