



www.tyfone.com

SIDE-X™ TEST TOOL

User Guide – Windows

Revision History

Date	Remarks	Version
09/26/2019	Initial draft	1.0

Trademarks and copyright

© 2004-2018, Tyfone Inc. All rights reserved. Patented and other Patents pending. All trademarks are property of their respective owners. SideCard™, SideTap™, SideSafe™, SideKey™, The Connected Smart Card, CSC are trademarks of Tyfone Inc.

For questions visit: www.tyfone.com

Proprietary Notice

The information contained is proprietary and confidential material owned by Tyfone Inc. Any unauthorized reproduction, use, or disclosure of this material, or any part thereof, is strictly prohibited. This document is solely for the use of Tyfone employees and employees of current and prospective customers of Tyfone who have signed a Non-Disclosure Agreement (NDA) with Tyfone.

The recipient acknowledges Tyfone's ownership to the material in this document and must obtain Tyfone's consent in writing before the recipient or any other person in the recipient's organization communicates any information (whether orally or in writing or any other manner whatsoever) on the contents of this document or part thereof to any third party, including an individual, an organization or an employee or employees of such an organization.

Disclaimers

Every effort has been made to ensure the accuracy of all information and statements contained in this document. However, Tyfone does not assume any liability for the use of this material. Tyfone reserves the right to make changes to this material at any time and without notice.

Customer support

Tyfone offers multiple technical support plans and service packages to help our customers get the most out of Tyfone products. For further information on Technical Support plans and pricing please send an email to support@tyfone.com.

To provide feedback on this document, send your comments to feedback@tyfone.com.

Contents

1	Overview	5
1.1	Hardware Requirements	5
1.2	Software Requirements	5
2	APDU Communication	5
3	Running Side-X Test Tool	7
3.1	Loading An Applet	9
3.2	Deleting An Applet	11
3.3	Transmit Single APDU	13
3.3.1	Using 'Single APDU' Option	13
3.4	Transmit Multiple APDUs	15
3.5	Certificates	17
3.6	HW Token	23
4	SideCard Communication Application Development	27

1 OVERVIEW

This document explains how to install and use the Side-X Test Tool on a Windows platform. It is a piece of software which is used to connect and communicate with the SideCard/SideSafe using Application Protocol Data Unit (APDU) commands. The application communicates with the SideCard/SideSafe via contact interface using ISO 7816 protocol. Requirements to run the Side-X Test Tool are defined below.

1.1 HARDWARE REQUIREMENTS

1. SideCard (which is pre-personalized)
2. Smart Card Reader
3. Desktop/Laptop System

1.2 SOFTWARE REQUIREMENTS

1. Operating Systems
 1. Windows with Windows10 OS
2. Software
 1. Side-X Test Tool
 2. Java, JRE 1.6 onwards
 3. Smart Card Reader Driver

2 APDU COMMUNICATION

Application Protocol Data Unit command is a set of bytes. APDU communication involves sending a command APDU to the Firmware or Secure Element (SE) of a smart card, processing it, and receiving a response APDU. APDU commands are a queue of binary numbers of the following form:

Command APDU						
Header (required)				Body (optional)		
CLA	INS	P1	P2	Lc	Data Field	Le

The first four sections, i.e. *CLA*, *INS*, *P1* and *P2* are mandatory in all APDU commands and **each one has one-byte length**. These one-byte length sections stand for Class, Instruction, Parameter1 and Parameter2 respectively.

The last three sections, i.e. *Lc*, *Data Field (CData)*, and *Le* are optional. *Lc* represents the length of the *CData* field. *Le* specifies the maximum length of expected response data.

The **response APDU** is expected to contain response data with status words: SW1 SW2; which denote processing state in the smart card.

Response APDU		
Body (optional)	Trailer (required)	
Data Field	SW1	SW2

Different types of APDU commands:

Case 1:

No Command data,
No Response required

CLA	INS	P1	P2
-----	-----	----	----

Case 2:

No Command data,
Yes Response required

CLA	INS	P1	P2	Le
-----	-----	----	----	----

Case 3:

Yes Command data,
No Response required

CLA	INS	P1	P2	Lc	Data Field
-----	-----	----	----	----	------------

Case 4:

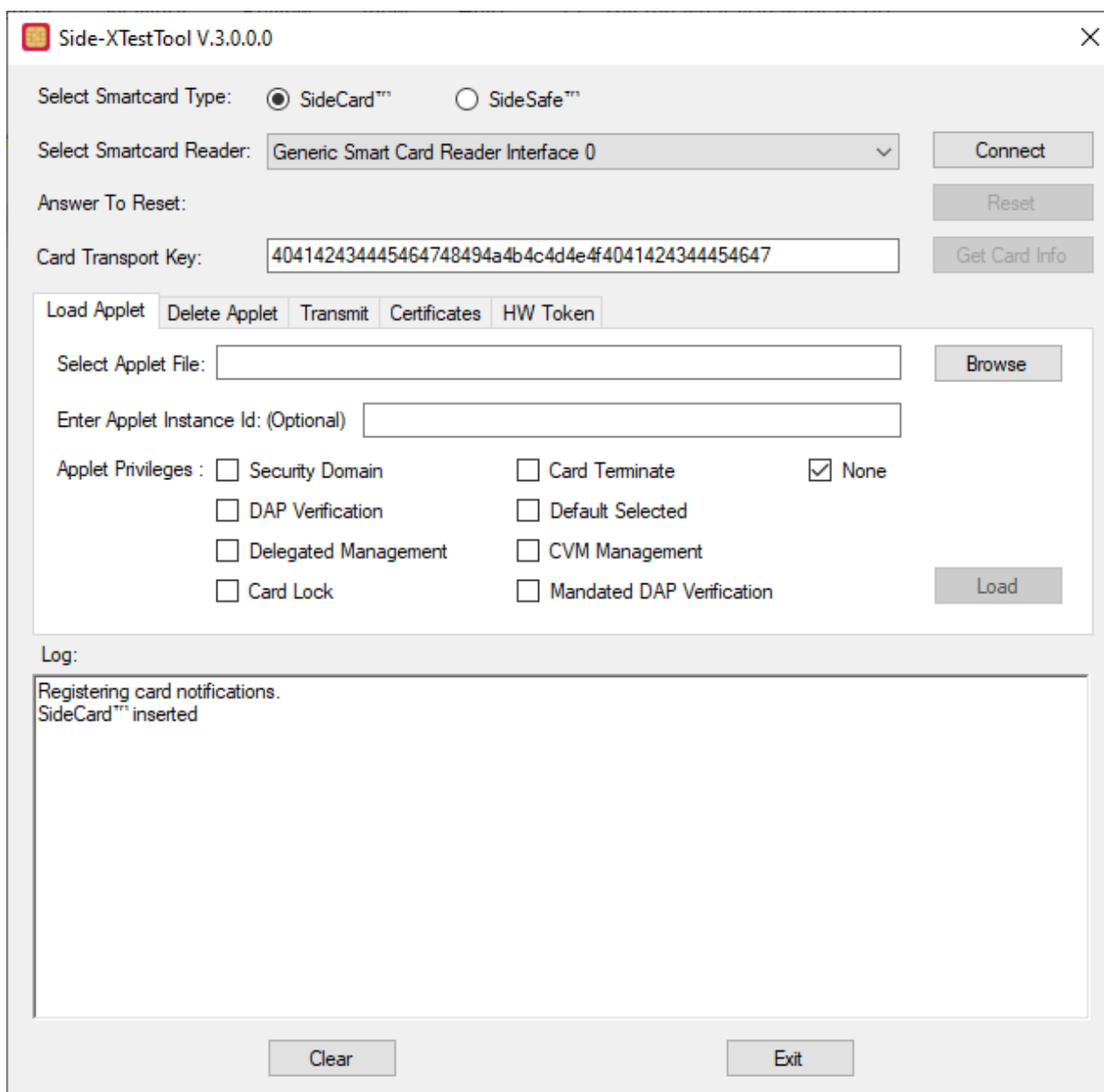
Yes Command data,
Yes Response required

CLA	INS	P1	P2	Lc	Data Field	Le
-----	-----	----	----	----	------------	----

3 RUNNING SIDE-X TEST TOOL

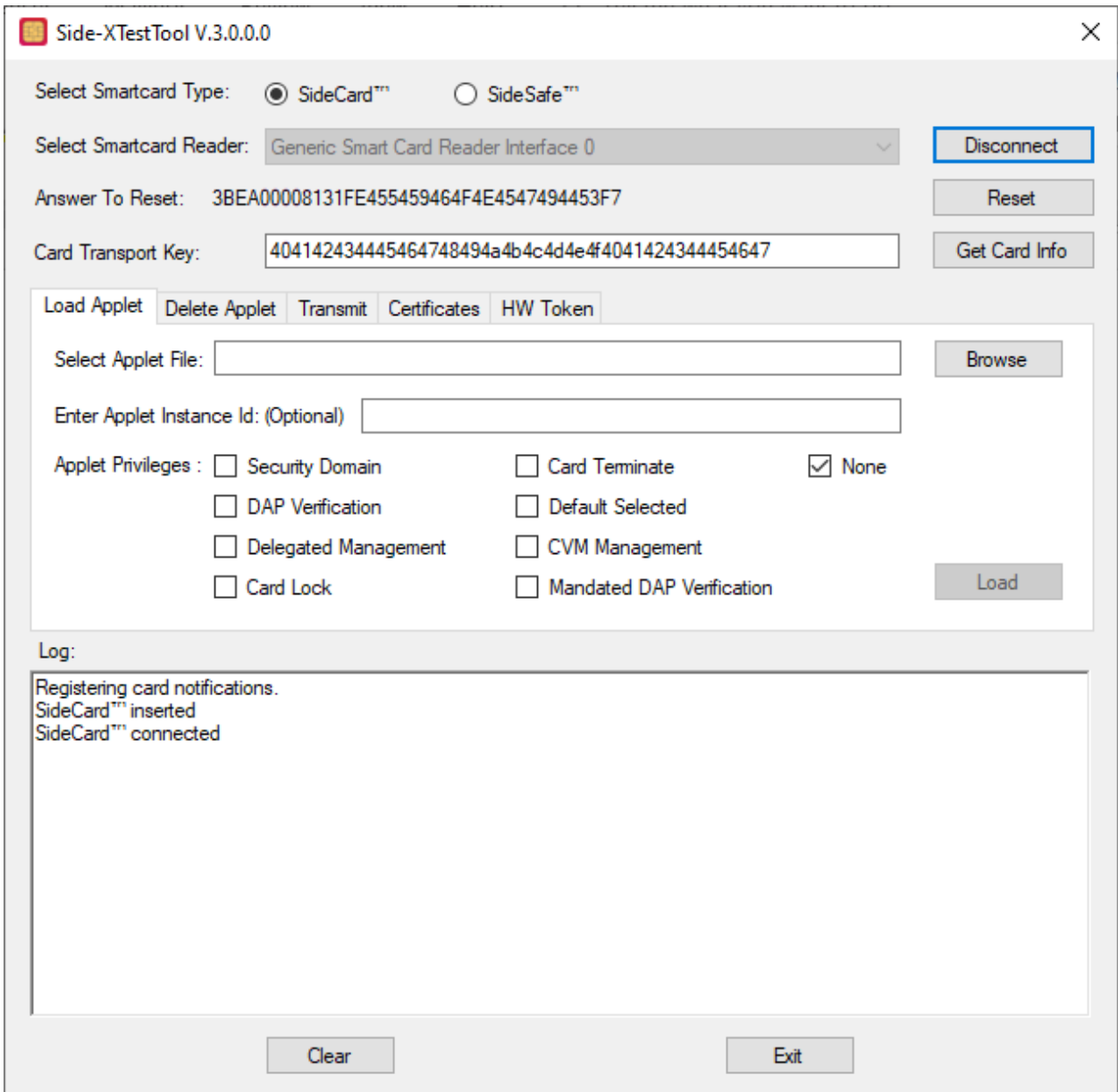
1. Connect smart card reader to the desktop/laptop system and make sure that the connected smart card reader is detected by the system/laptop. If not, please install appropriate smart card reader driver.
2. Insert SideCard into the smart card reader.
3. Open the Side-X Test Tool by double clicking on Side-X_TestTool_<X.Y.Z> icon

NOTE: The 'Card Transport Key' field displays the default key value which is required to authenticate with SideCard.

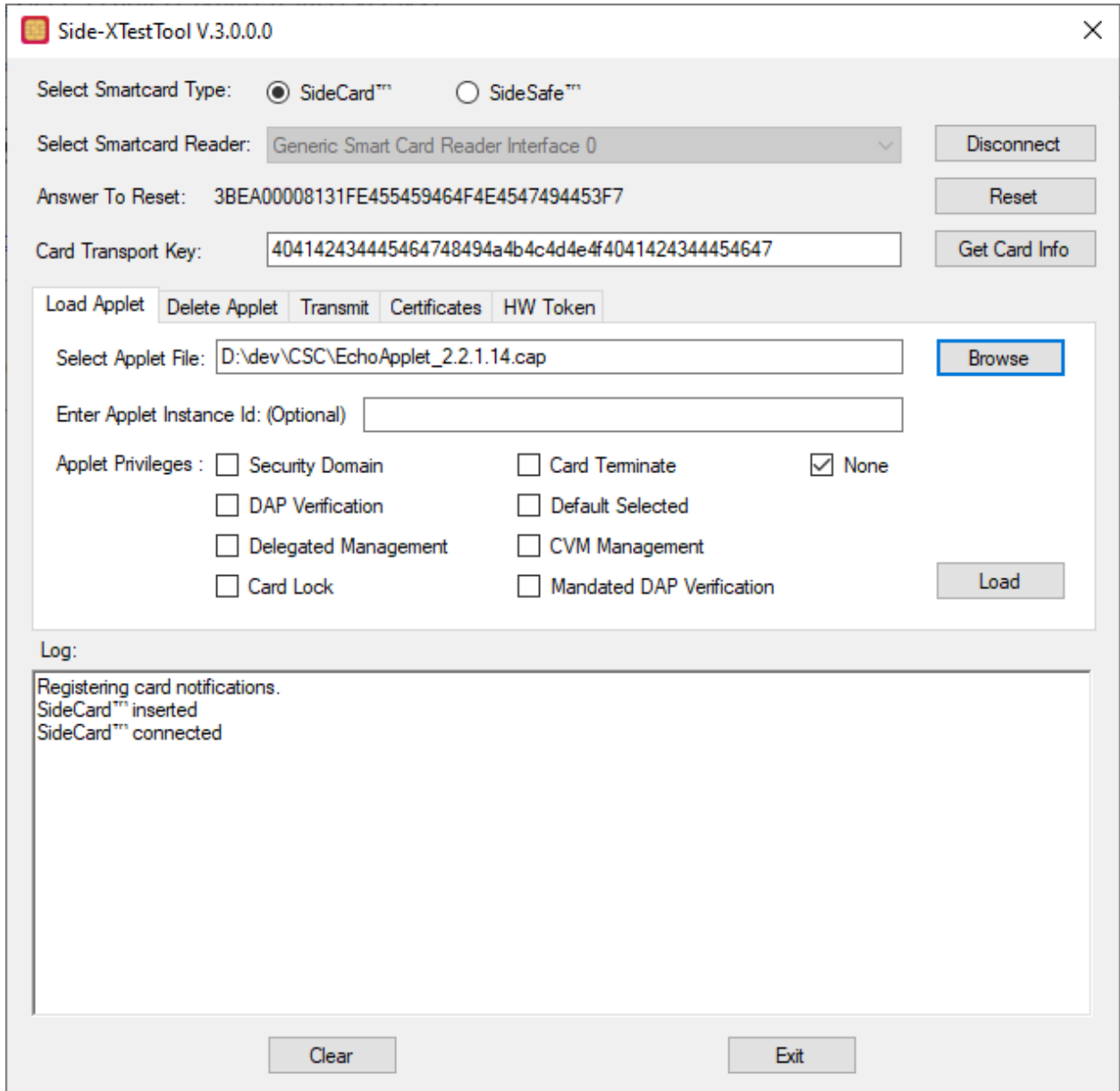


The screenshot shows the Side-XTestTool V.3.0.0.0 window. At the top, there's a title bar with the application name and a close button. Below the title bar, the 'Select Smartcard Type' section has two radio buttons: 'SideCard™' (selected) and 'SideSafe™'. The 'Select Smartcard Reader' dropdown menu shows 'Generic Smart Card Reader Interface 0'. To the right of this dropdown are three buttons: 'Connect', 'Reset', and 'Get Card Info'. Below the reader selection, there's a text field for 'Answer To Reset' and a 'Card Transport Key' field containing the value '404142434445464748494a4b4c4d4e4f4041424344454647'. A row of tabs includes 'Load Applet' (active), 'Delete Applet', 'Transmit', 'Certificates', and 'HW Token'. Under the 'Load Applet' tab, there's a 'Select Applet File' field with a 'Browse' button, and an 'Enter Applet Instance Id: (Optional)' field. The 'Applet Privileges' section contains a grid of checkboxes: 'Security Domain', 'DAP Verification', 'Delegated Management', 'Card Lock', 'Card Terminate', 'Default Selected', 'CVM Management', and 'Mandated DAP Verification'. The 'None' checkbox is checked. A 'Load' button is at the bottom right of this section. At the bottom of the window, there's a 'Log' section with a text area showing 'Registering card notifications.' and 'SideCard™ inserted'. Below the log area are 'Clear' and 'Exit' buttons.

4. If the smart card reader name is not loaded, please re-connect Smart Card Reader to the system's USB port and select 'Reload' button.
5. Choose the smart card reader and select 'Connect' button.
6. On successful connection, the SideCard's ATR (Answer To Reset) value is displayed.



3.1 LOADING AN APPLLET



The screenshot shows the Side-XTestTool V.3.0.0.0 window. The 'Load Applet' tab is selected. The 'Select Smartcard Type' section has 'SideCard™' selected. The 'Select Smartcard Reader' dropdown shows 'Generic Smart Card Reader Interface 0'. The 'Answer To Reset' field contains '3BEA00008131FE455459464F4E4547494453F7'. The 'Card Transport Key' field contains '404142434445464748494a4b4c4d4e4f4041424344454647'. The 'Log' section shows the following text: 'Registering card notifications.', 'SideCard™ inserted', and 'SideCard™ connected'. The 'Load' button is visible at the bottom right of the main configuration area.

Side-XTestTool V.3.0.0.0

Select Smartcard Type: ☒ SideCard™ ☐ SideSafe™

Select Smartcard Reader: Generic Smart Card Reader Interface 0

Answer To Reset: 3BEA00008131FE455459464F4E4547494453F7

Card Transport Key: 404142434445464748494a4b4c4d4e4f4041424344454647

Load Applet Delete Applet Transmit Certificates HW Token

Select Applet File: D:\dev\CSC\EchoApplet_2.2.1.14.cap

Enter Applet Instance Id: (Optional)

Applet Privileges : ☐ Security Domain ☐ Card Terminate ☒ None
☐ DAP Verification ☐ Default Selected
☐ Delegated Management ☐ CVM Management
☐ Card Lock ☐ Mandated DAP Verification

Log:

Registering card notifications.
SideCard™ inserted
SideCard™ connected

Clear Exit

1. Select 'Load Applet' tab.
2. Choose the applet (*.cap) file by clicking on the '...' button. After selection of the applet file, optionally an instance ID for the applet can be provided.
3. Click on 'Load' button. If the operation is successful then 'Selected applet: xxx.cap loaded successfully.' message is shown in 'Log' section. Otherwise, an error message is displayed.

Side-XTestTool V.3.0.0.0

Select Smartcard Type: ☒ SideCard™ ☐ SideSafe™

Select Smartcard Reader: Generic Smart Card Reader Interface 0 Disconnect

Answer To Reset: 3BEA00008131FE455459464F4E4547494453F7 Reset

Card Transport Key: 404142434445464748494a4b4c4d4e4f4041424344454647 Get Card Info

Load Applet Delete Applet Transmit Certificates HW Token

Select Applet File: D:\dev\CSC\EchoApplet_2.2.1.14.cap Browse

Enter Applet Instance Id: (Optional)

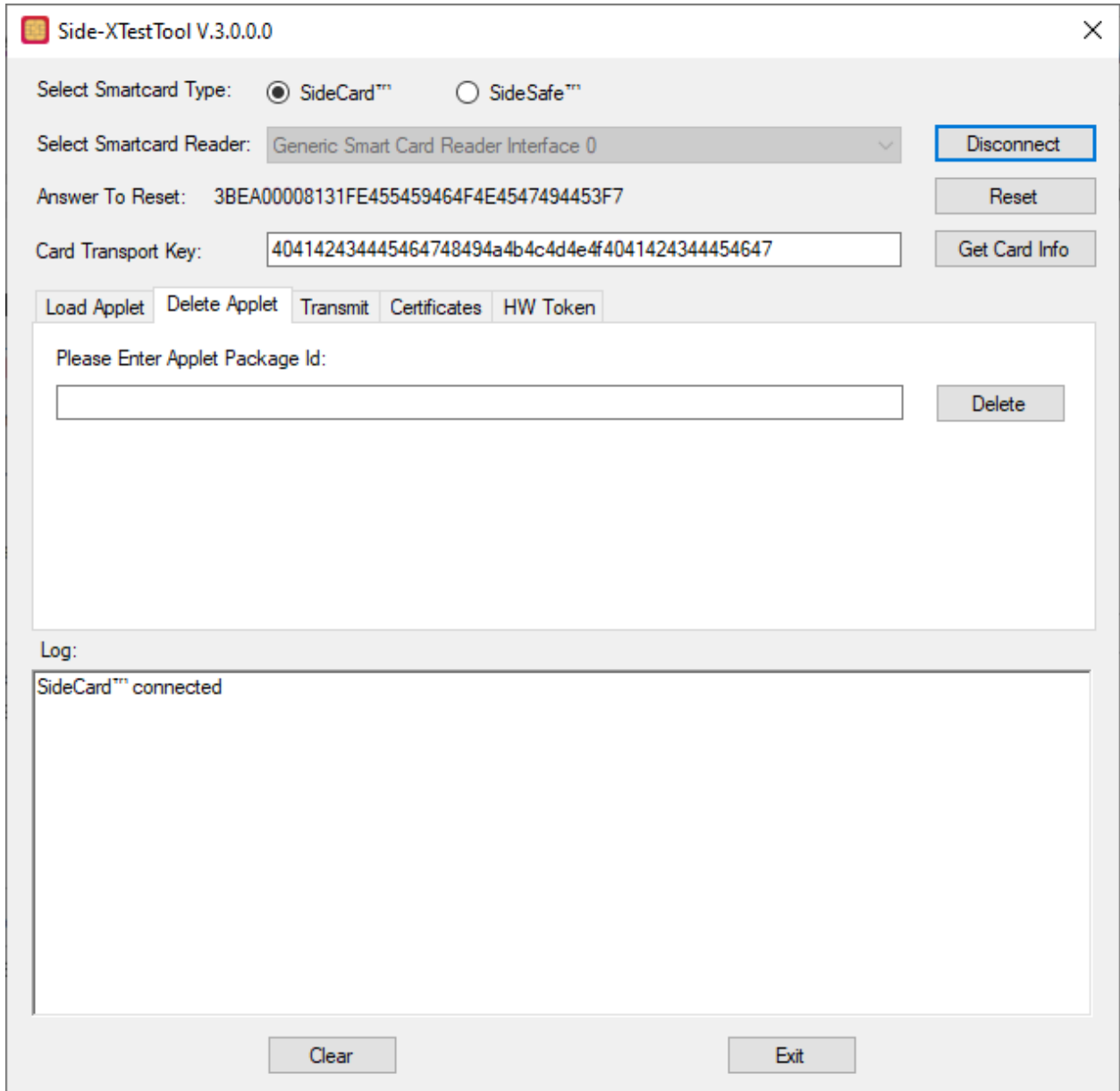
Applet Privileges : ☐ Security Domain ☐ Card Terminate ☒ None
☐ DAP Verification ☐ Default Selected
☐ Delegated Management ☐ CVM Management
☐ Card Lock ☐ Mandated DAP Verification Load

Log:

```
316078D00153B190316078B00161606160743290616041607412904160616076DCC160665C87B000416041A0316068
D00153B190316068B001603290670AF7A03301A0304381A0403381A0503381A060338180789001903AF008B00177A0
8000A0002000100000000000005006200180200000000680030001800D000680080D0500000003800D01010000000600
00090380030203800A0103800303060000
Response: 009000
APDU:
80E880035D01770600006E0680070103800A0603800A10068010030680100203800A0303800A0703800A09068010010
3800A0403800A08090028000412FF7B04002007060E03070B03040A0705080E080705090818060916060D411909081B
09082300
Response: 009000
APDU: 80E60C002409A0000005742000010009A0000005742000010109A00000057420000101010002C9000000
Response: 009000
Selected applet loaded successfully
```

Clear Exit

3.2 DELETING AN APPLETT



The screenshot shows the Side-XTestTool V.3.0.0.0 window. At the top, there's a title bar with the application name and a close button. Below it, the 'Select Smartcard Type' section has two radio buttons: 'SideCard™' (selected) and 'SideSafe™'. The 'Select Smartcard Reader' section has a dropdown menu showing 'Generic Smart Card Reader Interface 0' and a 'Disconnect' button. The 'Answer To Reset' field contains the value '3BEA00008131FE455459464F4E4547494453F7' with a 'Reset' button. The 'Card Transport Key' field contains a long hexadecimal string with a 'Get Card Info' button. Below these fields is a tabbed interface with five tabs: 'Load Applet', 'Delete Applet' (selected), 'Transmit', 'Certificates', and 'HW Token'. The 'Delete Applet' tab contains a text field labeled 'Please Enter Applet Package Id:' and a 'Delete' button. At the bottom, there's a 'Log' section with a text area showing 'SideCard™ connected'. At the very bottom, there are 'Clear' and 'Exit' buttons.

1. Select 'Delete Applet' tab.
2. Click on 'Read Card Info' button to display list of Package IDs and Applet AIDs available in the Smart Card.
3. Enter Instance ID or Package ID of the desired applet in the 'Enter Instance/Package ID' text field and click on 'Delete' button to delete the applet from the Smart Card.

Side-XTSTool V.3.0.0.0

Select Smartcard Type: ☒ SideCard™ ☐ SideSafe™

Select Smartcard Reader: Generic Smart Card Reader Interface 0 Disconnect

Answer To Reset: 3BEA00008131FE455459464F4E4547494453F7 Reset

Card Transport Key: 404142434445464748494a4b4c4d4e4f4041424344454647 Get Card Info

Load Applet Delete Applet Transmit Certificates HW Token

Please Enter Applet Package Id:

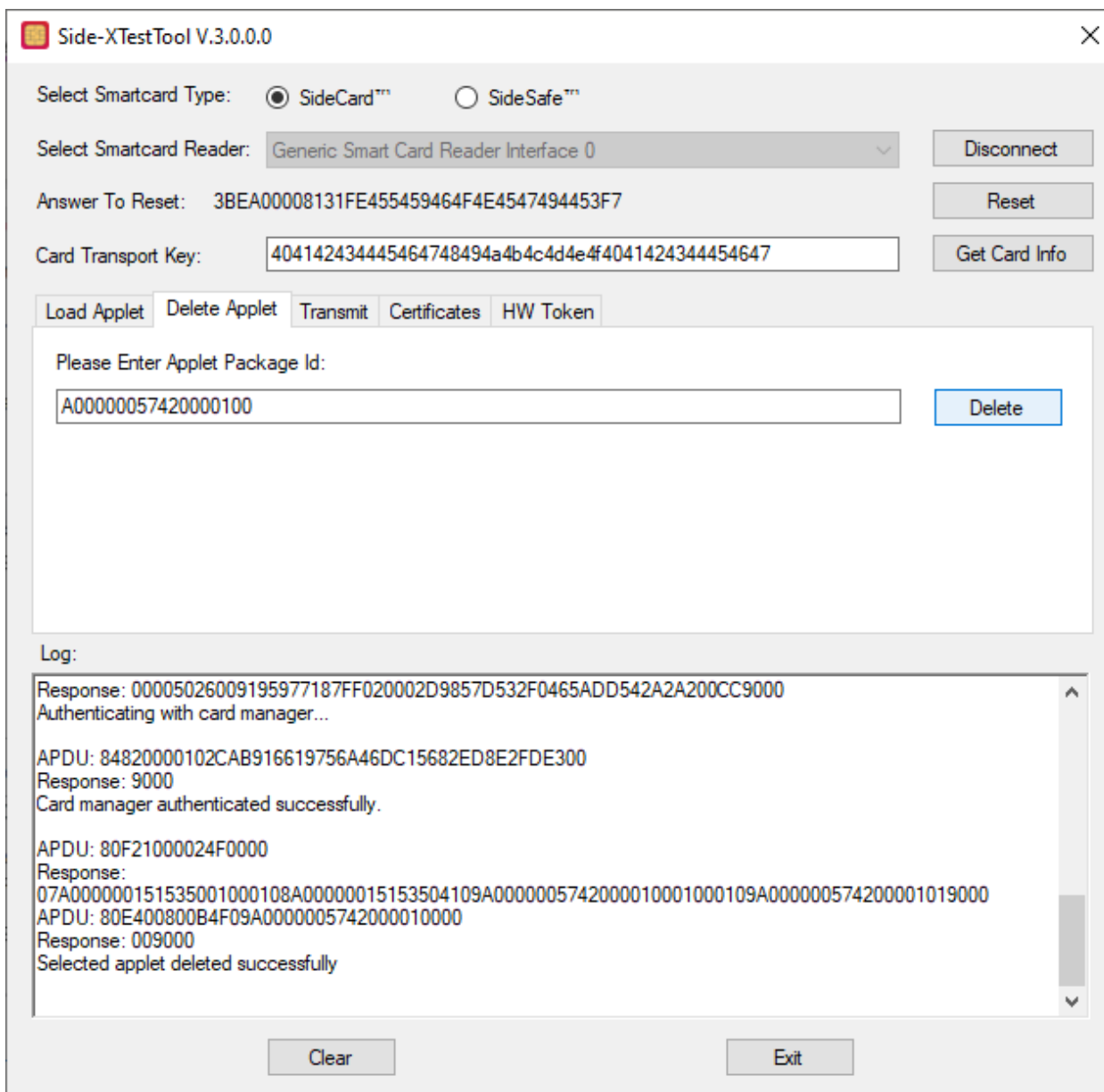
Delete

Log:

```
Capturing card info...
APDU: 80F24000024F0000
Response: 09A0000005742000010107009000
APDU: 80F21000024F0000
Response:
07A000000151535001000108A00000015153504109A0000005742000010001000109A000000574200001019000

Package IDs:...
A0000001515350
A00000057420000100
Instance IDs:...
A00000057420000101
```

Clear Exit



Side-XTestTool V.3.0.0.0

Select Smartcard Type: ☒ SideCard™ ☐ SideSafe™

Select Smartcard Reader: Generic Smart Card Reader Interface 0 Disconnect

Answer To Reset: 3BEA00008131FE455459464F4E4547494453F7 Reset

Card Transport Key: 404142434445464748494a4b4c4d4e4f4041424344454647 Get Card Info

Load Applet Delete Applet Transmit Certificates HW Token

Please Enter Applet Package Id:

A00000057420000100 Delete

Log:

```

Response: 00005026009195977187FF020002D9857D532F0465ADD542A200CC9000
Authenticating with card manager...

APDU: 84820000102CAB916619756A46DC15682ED8E2FDE300
Response: 9000
Card manager authenticated successfully.

APDU: 80F21000024F0000
Response:
07A000000151535001000108A00000015153504109A0000005742000010001009A000000574200001019000
APDU: 80E400800B4F09A0000005742000010000
Response: 009000
Selected applet deleted successfully
  
```

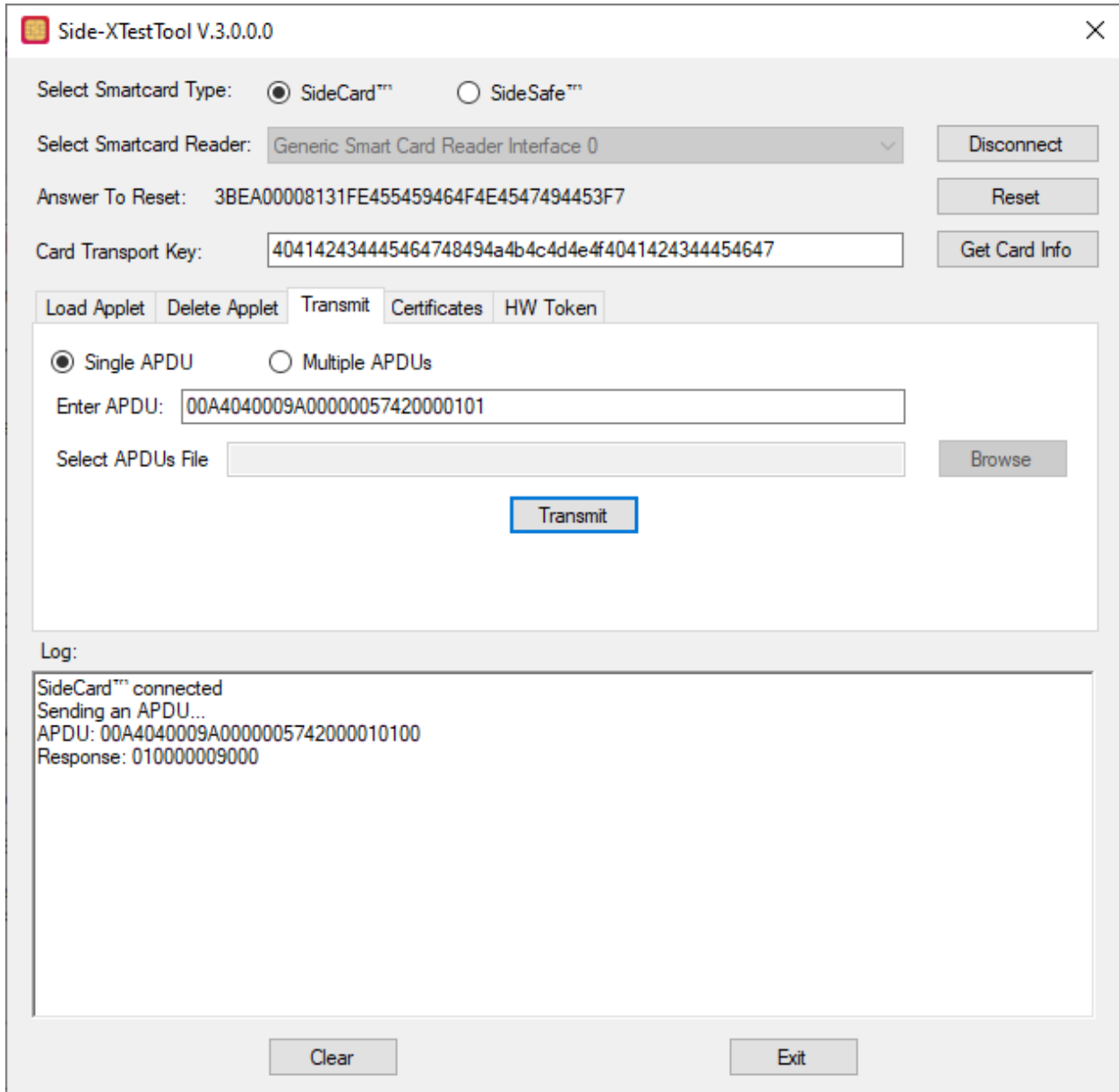
Clear Exit

3.3 TRANSMIT SINGLE APDU

3.3.1 Using 'Single APDU' Option

1. Select 'Transmit' tab.
2. Choose 'Single APDU' (default) radio button.
3. Enter an APDU command in 'APDU' field. It should be Hex string.
4. Click on 'Transmit' button to send the APDU command to the smart card and read the response.

5. APDU command and its response data along with status bytes is displayed in the 'Log' section.



The screenshot shows the Side-XTestTool V.3.0.0.0 window. At the top, there's a title bar with the application name and a close button. Below the title bar, the interface is divided into several sections. The first section contains 'Select Smartcard Type' with radio buttons for 'SideCard™' (selected) and 'SideSafe™'. Below this is 'Select Smartcard Reader' with a dropdown menu showing 'Generic Smart Card Reader Interface 0' and a 'Disconnect' button. The next section shows 'Answer To Reset' with the value '3BEA00008131FE455459464F4E4547494453F7' and a 'Reset' button. Below that is 'Card Transport Key' with a text field containing '404142434445464748494a4b4c4d4e4f4041424344454647' and a 'Get Card Info' button. A tabbed interface follows with tabs for 'Load Applet', 'Delete Applet', 'Transmit' (selected), 'Certificates', and 'HW Token'. The 'Transmit' tab contains 'Single APDU' (selected) and 'Multiple APDU's radio buttons, an 'Enter APDU' text field with the value '00A4040009A00000057420000101', a 'Select APDU's File' text field, a 'Browse' button, and a 'Transmit' button. At the bottom, there's a 'Log' section with a text area displaying the following text: 'SideCard™ connected', 'Sending an APDU...', 'APDU: 00A4040009A0000005742000010100', and 'Response: 010000009000'. At the very bottom, there are 'Clear' and 'Exit' buttons.

Side-XTestTool V.3.0.0.0

Select Smartcard Type: ☒ SideCard™ ☐ SideSafe™

Select Smartcard Reader: Generic Smart Card Reader Interface 0 Disconnect

Answer To Reset: 3BEA00008131FE455459464F4E4547494453F7 Reset

Card Transport Key: 404142434445464748494a4b4c4d4e4f4041424344454647 Get Card Info

Load Applet Delete Applet **Transmit** Certificates HW Token

☒ Single APDU ☐ Multiple APDU's

Enter APDU: 00A4040009A00000057420000101

Select APDU's File Browse

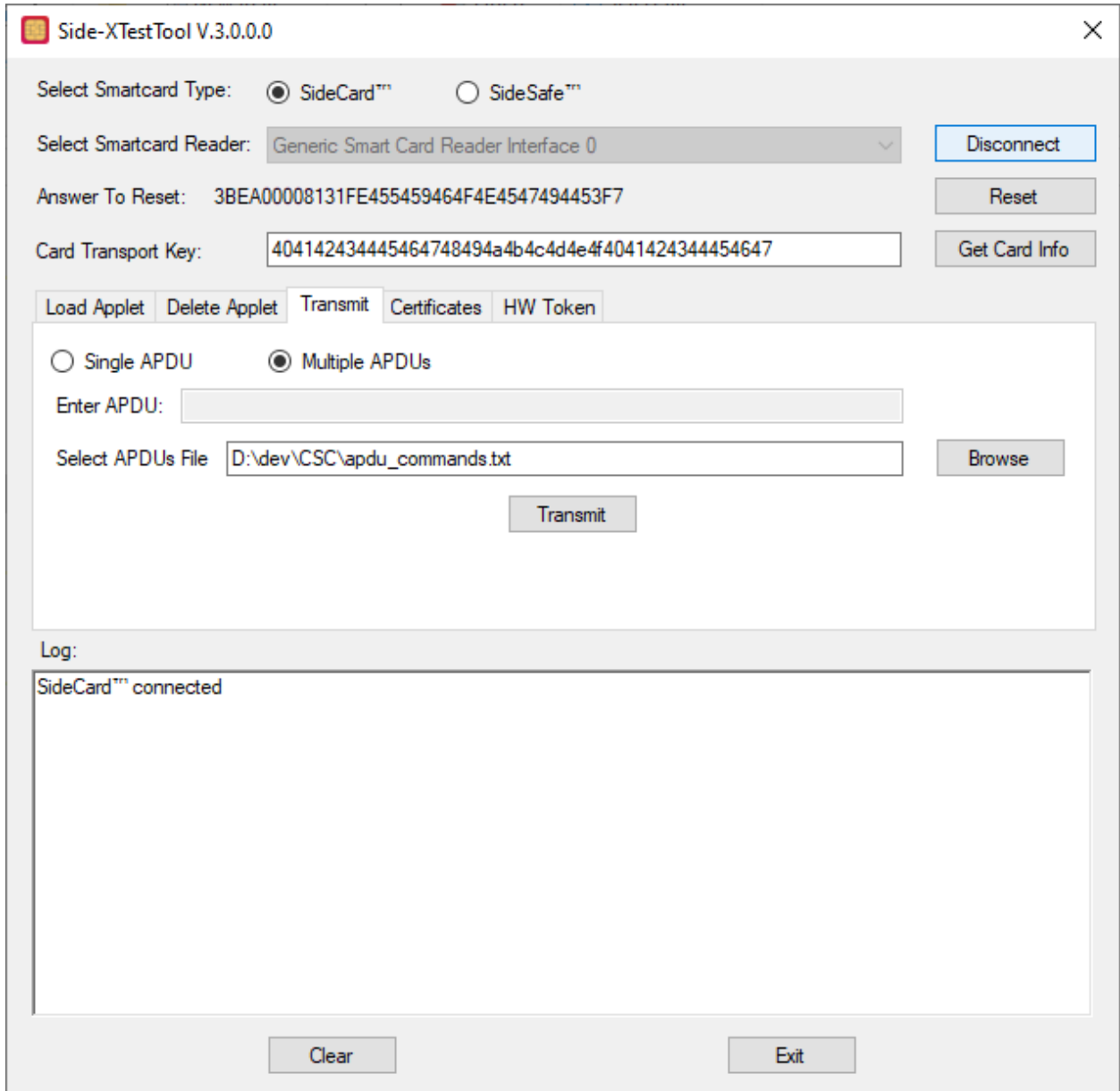
Transmit

Log:

SideCard™ connected
Sending an APDU...
APDU: 00A4040009A0000005742000010100
Response: 010000009000

Clear Exit

3.4 TRANSMIT MULTIPLE APDUS



The screenshot shows the Side-XTestTool V.3.0.0.0 window. The 'Transmit' tab is selected. Under 'Select Smartcard Type', 'SideCard™' is chosen. 'Select Smartcard Reader' is set to 'Generic Smart Card Reader Interface 0'. 'Answer To Reset' is '3BEA00008131FE455459464F4E4547494453F7'. 'Card Transport Key' is '404142434445464748494a4b4c4d4e4f4041424344454647'. Buttons for 'Disconnect', 'Reset', and 'Get Card Info' are present. In the 'Transmit' section, 'Multiple APDUs' is selected. 'Enter APDU' is empty. 'Select APDUs File' is 'D:\dev\CSC\apdu_commands.txt' with a 'Browse' button. A 'Transmit' button is at the bottom of this section. The 'Log' section shows 'SideCard™ connected'. 'Clear' and 'Exit' buttons are at the bottom.

1. Select 'Multiple APDUs' tab.
2. Select the multiple APDUs text file by clicking on '...' button.
NOTE: In the text file, any lines that start with '//' or '#' will be ignored.
3. Click on 'Transmit' button. All the APDU commands listed in the text file are sent to the smart card and the corresponding responses are also read. The 'Log' section will display all the command/response messages along with a total count of APDU commands transmitted.

Side-XTestTool V.3.0.0.0

Select Smartcard Type: ☒ SideCard™ ☐ SideSafe™

Select Smartcard Reader: Generic Smart Card Reader Interface 0 Disconnect

Answer To Reset: 3BEA00008131FE455459464F4E4547494453F7 Reset

Card Transport Key: 404142434445464748494a4b4c4d4e4f4041424344454647 Get Card Info

Load Applet Delete Applet Transmit Certificates HW Token

☐ Single APDU ☒ Multiple APDUs

Enter APDU:

Select APDUs File: D:\dev\CSC\apdu_commands.txt Browse

Transmit

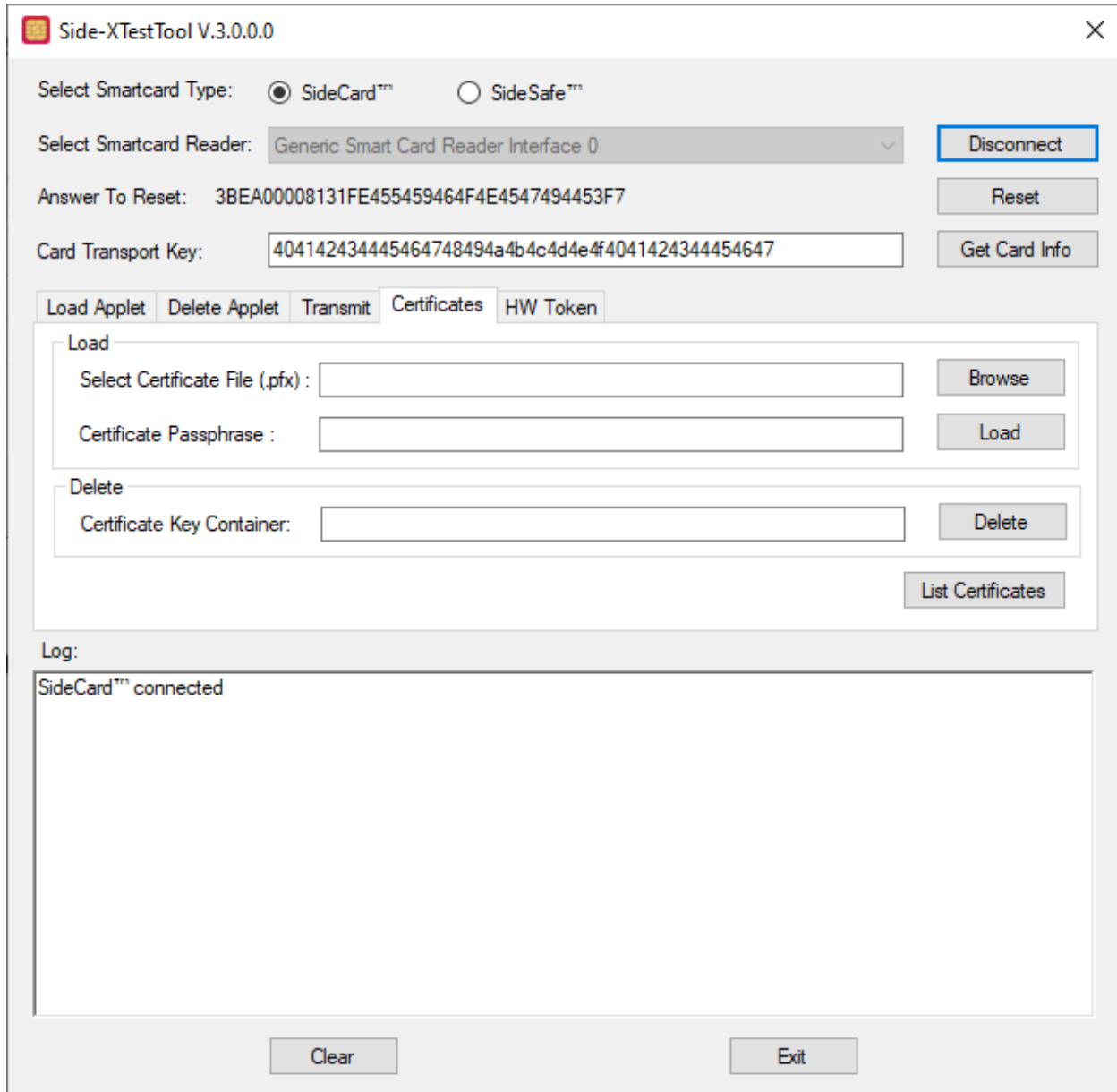
Log:

```
APDU: C0D6031E07E000008131FE4500
Response: 9000
APDU: C0D6030A010A00
Response: 9000
APDU: C0D6032D010A00
Response: 9000
APDU: C0D6030B0A5459464F4E454749445300
Response: 9000
APDU: C0D6032E0A5459464F4E454749445300
Response: 9000
APDU: 0010000000
Response: 9000
List of APDUs transmitted successfully.
```

Clear Exit

NOTE: Please refer to Applet Specification document to form the list of APDUs

3.5 CERTIFICATES



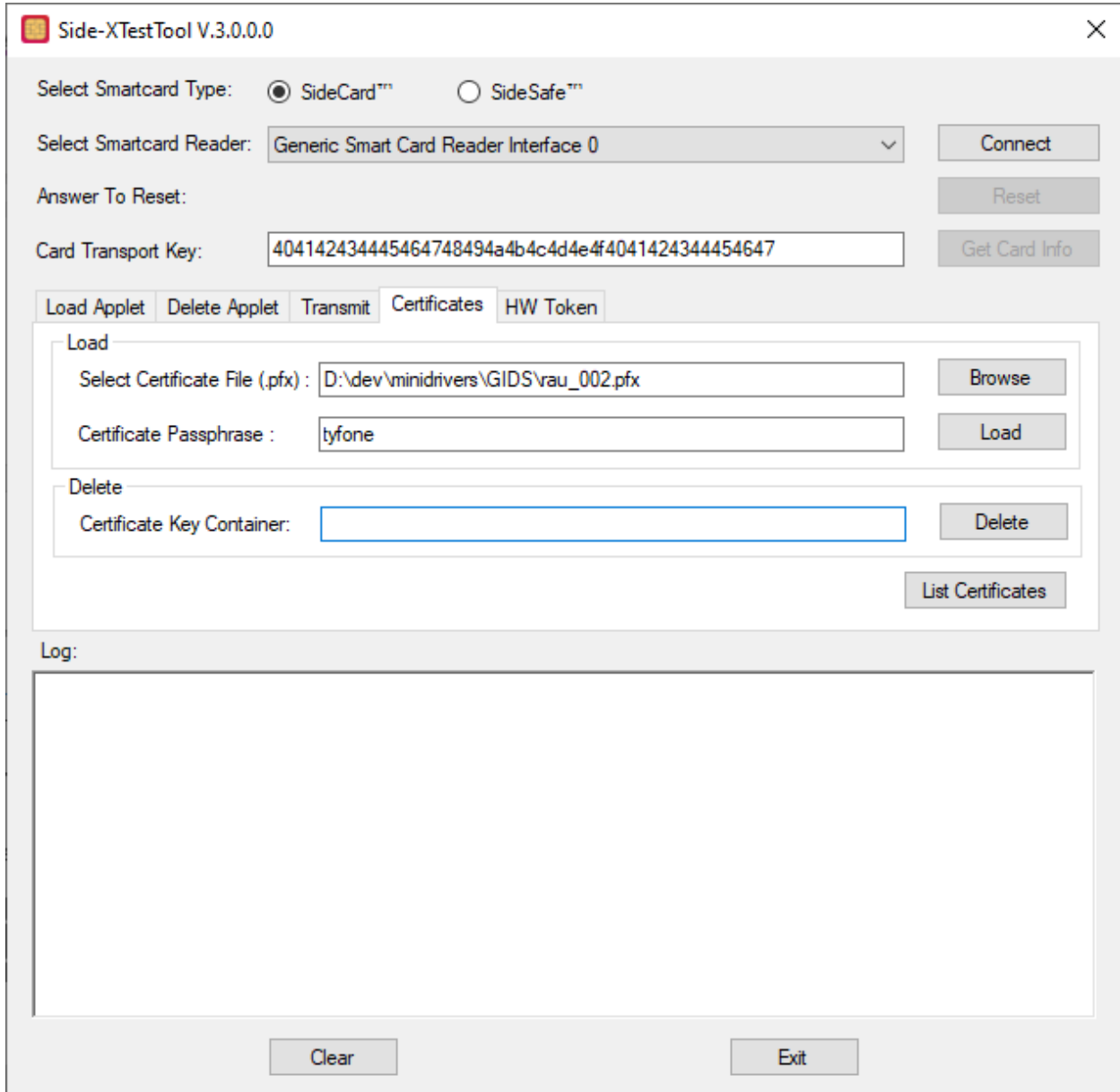
The screenshot shows the Side-XTestTool V.3.0.0.0 window. At the top, there's a title bar with the application name and a close button. Below it, the 'Select Smartcard Type' section has two radio buttons: 'SideCard™' (selected) and 'SideSafe™'. The 'Select Smartcard Reader' dropdown is set to 'Generic Smart Card Reader Interface 0'. To the right of this dropdown are three buttons: 'Disconnect' (highlighted with a blue border), 'Reset', and 'Get Card Info'. Below the reader selection, the 'Answer To Reset' field contains the value '3BEA00008131FE455459464F4E4547494453F7'. The 'Card Transport Key' field contains a long hexadecimal string. Below these fields is a tabbed interface with five tabs: 'Load Applet', 'Delete Applet', 'Transmit', 'Certificates' (active), and 'HW Token'. The 'Certificates' tab is divided into two sections: 'Load' and 'Delete'. The 'Load' section has two input fields: 'Select Certificate File (.pfx):' and 'Certificate Passphrase:', each followed by a 'Browse' or 'Load' button. The 'Delete' section has one input field: 'Certificate Key Container:', followed by a 'Delete' button. At the bottom of the 'Certificates' tab is a 'List Certificates' button. Below the tabs is a 'Log:' section with a text area showing 'SideCard™ connected'. At the very bottom of the window are two buttons: 'Clear' and 'Exit'.

In this option you can view the list of certificates from connected smartcard. You can load or delete a .pfx certificate from the connected smartcard.

1. Load Certificate:

To load a certificate SideCard should have supported applet in it. For example, if the card loaded with GIDS applet then we can load a .pfx certificate.

- a. Select 'Browse' button and select a .pfx certificate
- b. Enter certificate passphrase if it has a passphrase or leave it as empty



Side-XTTestTool V.3.0.0.0

Select Smartcard Type: ☒ SideCard™ ☐ SideSafe™

Select Smartcard Reader: Generic Smart Card Reader Interface 0 Connect

Answer To Reset: Reset

Card Transport Key: 404142434445464748494a4b4c4d4e4f4041424344454647 Get Card Info

Load Applet Delete Applet Transmit Certificates HW Token

Load

Select Certificate File (.pfx): D:\dev\minidrivers\GIDS\rau_002.pfx Browse

Certificate Passphrase: tyfone Load

Delete

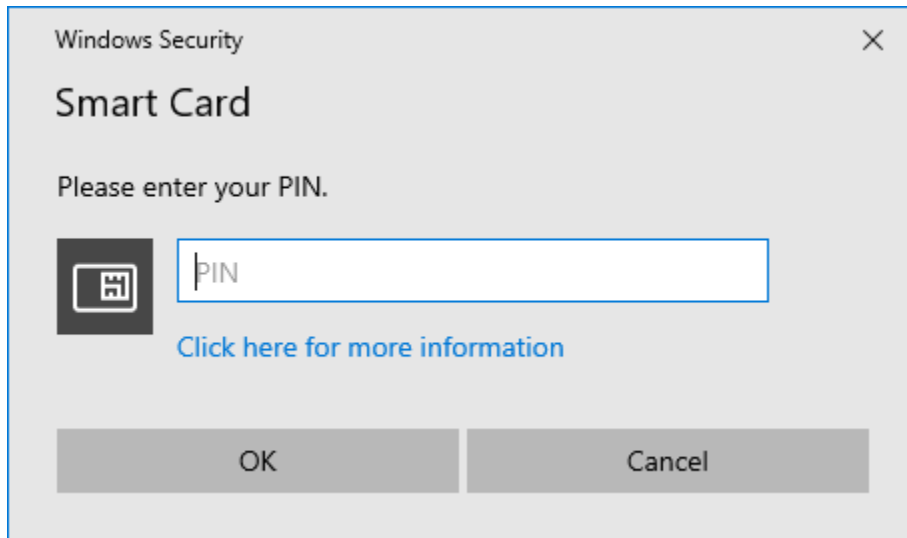
Certificate Key Container: Delete

List Certificates

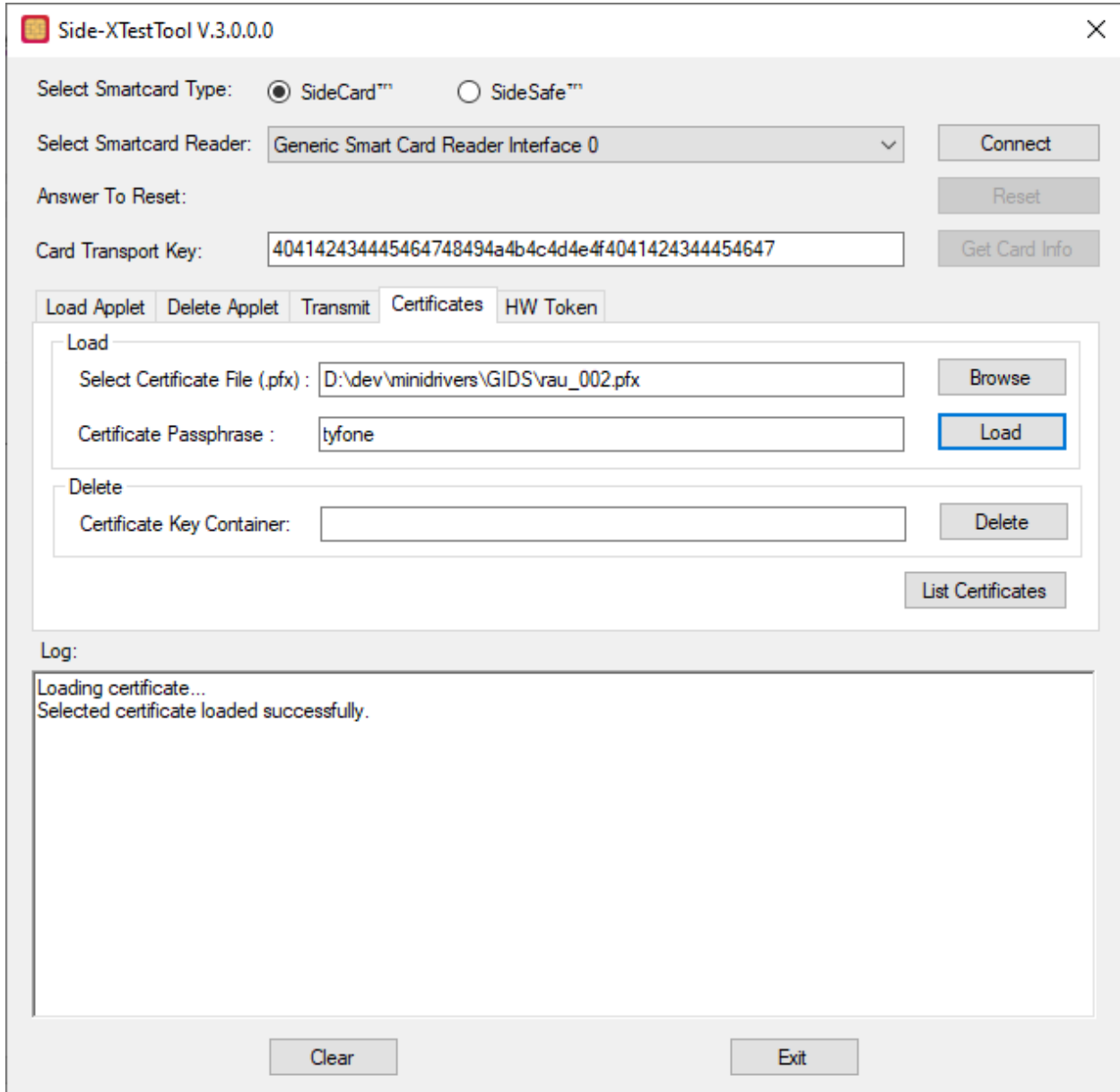
Log:

Clear Exit

c. Click 'Load' button to load the certificate



Enter smartcard PIN,



Side-XTestTool V.3.0.0.0

Select Smartcard Type: ☒ SideCard™ ☐ SideSafe™

Select Smartcard Reader: Generic Smart Card Reader Interface 0 Connect

Answer To Reset: Reset

Card Transport Key: 404142434445464748494a4b4c4d4e4f4041424344454647 Get Card Info

Load Applet Delete Applet Transmit **Certificates** HW Token

Load

Select Certificate File (.pfx): D:\dev\minidrivers\GIDS\rau_002.pfx Browse

Certificate Passphrase: tyfone Load

Delete

Certificate Key Container: Delete

List Certificates

Log:

Loading certificate...
Selected certificate loaded successfully.

Clear Exit

2. Delete Certificate

To delete a certificate from SideCard, it requires certificate key container name. Certificate key container names can get by 'List Certificates' option.

- a. Click on 'List Certificates'

Side-XTestTool V.3.0.0.0

Select Smartcard Type: ☒ SideCard™ ☐ SideSafe™

Select Smartcard Reader: Generic Smart Card Reader Interface 0 Connect

Answer To Reset: Reset

Card Transport Key: 404142434445464748494a4b4c4d4e4f4041424344454647 Get Card Info

Load Applet Delete Applet Transmit Certificates HW Token

Load

Select Certificate File (.pfx): Browse

Certificate Passphrase: Load

Delete

Certificate Key Container: Delete

List Certificates

Log:

Key Container Name:	f0086245-62a9-48ed-8fc8-7e7a706114cb
Subject:	E=rau_002@tyfone.com, CN=rau_002, OU=U4ia
Issuer:	CN=epriad-TY-PCSD-DC01-CA-1, DC=epriad, DC=tyfone, DC=com
UPN Name:	nj@tyblr.local
Certificate Verified:	False
Simple Name:	epriad-TY-PCSD-DC01-CA-1
Signature Algorithm:	sha256RSA
ValidFrom:	01-11-2019 14:30:15
ValidTo:	07-10-2019 14:30:15
Key Size:	2048

Clear Exit

- b. Copy Key Container Name from the Log area and paste in Delete Certificate Key Container field.

Side-XTestTool V.3.0.0.0

Select Smartcard Type: ☒ SideCard™ ☐ SideSafe™

Select Smartcard Reader: Generic Smart Card Reader Interface 0 Connect

Answer To Reset: Reset

Card Transport Key: 404142434445464748494a4b4c4d4e4f4041424344454647 Get Card Info

Load Applet Delete Applet Transmit Certificates HW Token

Load

Select Certificate File (.pfx): Browse

Certificate Passphrase: Load

Delete

Certificate Key Container: f0086245-62a9-48ed-8fc8-7e7a706114cb Delete

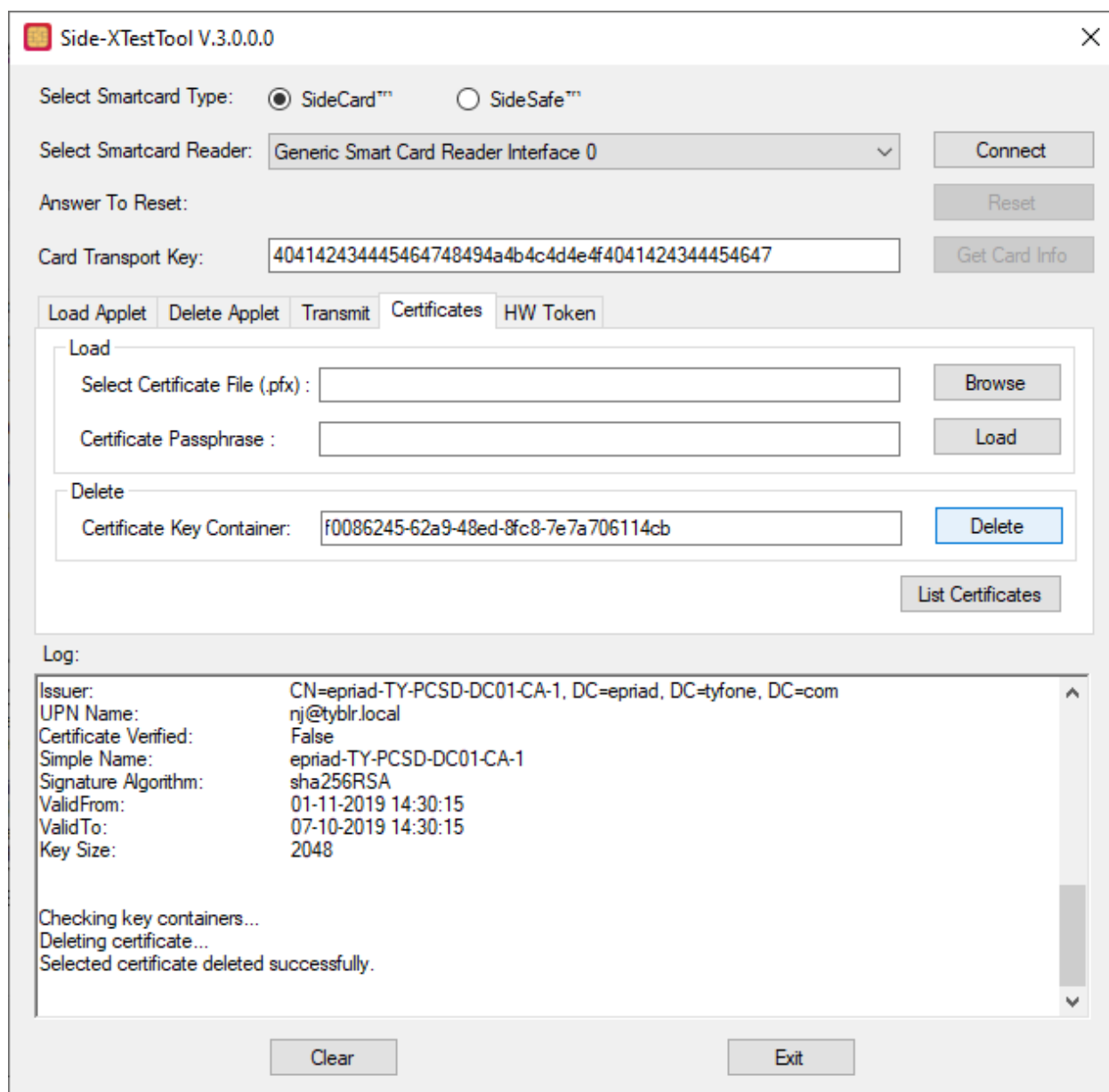
List Certificates

Log:

Key Container Name: f0086245-62a9-48ed-8fc8-7e7a706114cb
Subject: E=rau_002@tyfone.com, CN=rau_002, OU=U4ia
Issuer: CN=epriad-TY-PCSD-DC01-CA-1, DC=epriad, DC=tyfone, DC=com
UPN Name: nj@tyblr.local
Certificate Verified: False
Simple Name: epriad-TY-PCSD-DC01-CA-1
Signature Algorithm: sha256RSA
ValidFrom: 01-11-2019 14:30:15
ValidTo: 07-10-2019 14:30:15
Key Size: 2048

Clear Exit

c. Now, click on Delete button



Side-XTestTool V.3.0.0.0

Select Smartcard Type: ☒ SideCard™ ☐ SideSafe™

Select Smartcard Reader: Generic Smart Card Reader Interface 0 Connect

Answer To Reset: Reset

Card Transport Key: 404142434445464748494a4b4c4d4e4f4041424344454647 Get Card Info

Load Applet Delete Applet Transmit Certificates HW Token

Load

Select Certificate File (.pfx): Browse

Certificate Passphrase: Load

Delete

Certificate Key Container: f0086245-62a9-48ed-8fc8-7e7a706114cb Delete

List Certificates

Log:

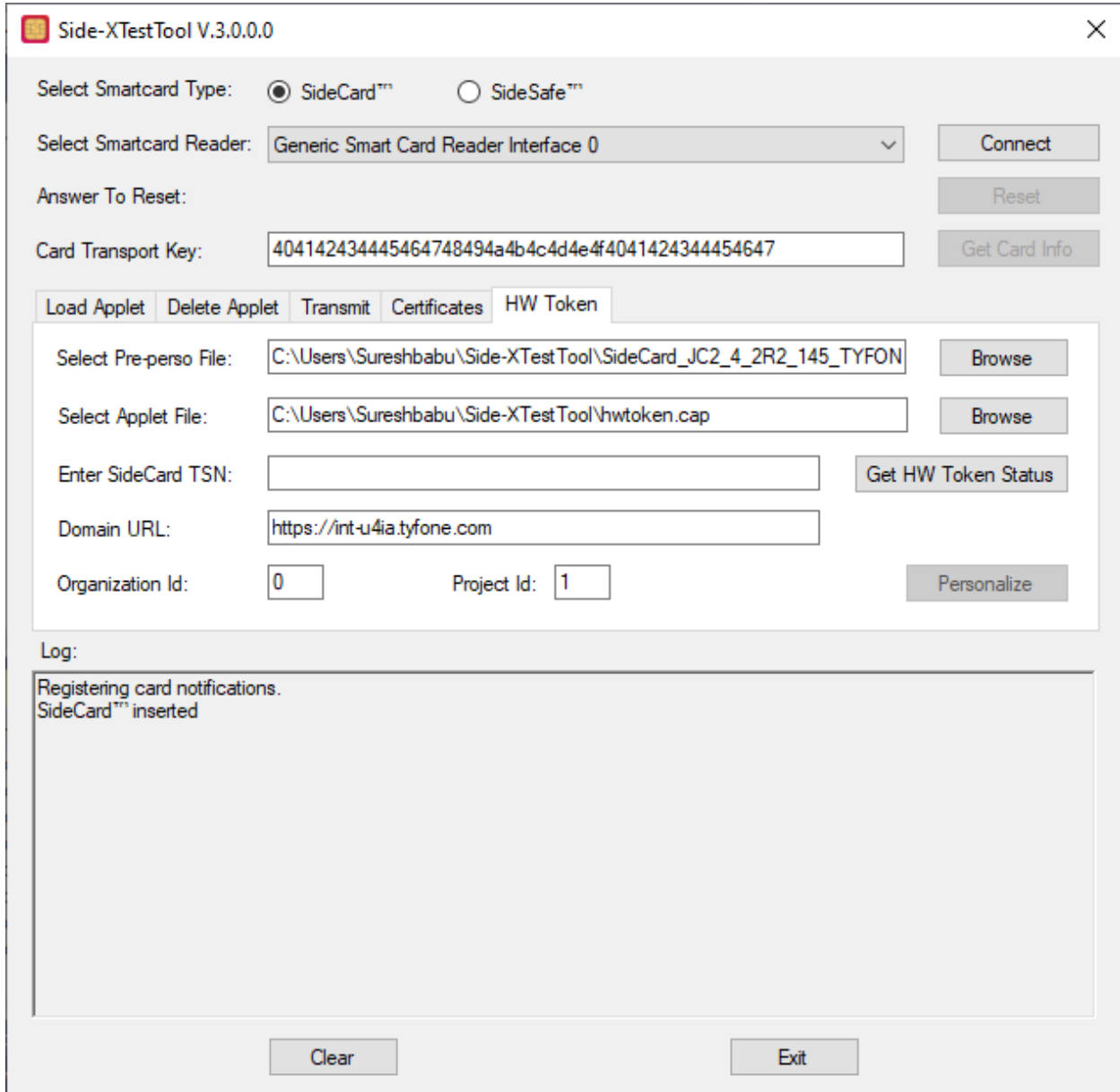
Issuer:	CN=epriad-TY-PCSD-DC01-CA-1, DC=epriad, DC=tyfone, DC=com
UPN Name:	nj@tyblr.local
Certificate Verified:	False
Simple Name:	epriad-TY-PCSD-DC01-CA-1
Signature Algorithm:	sha256RSA
ValidFrom:	01-11-2019 14:30:15
ValidTo:	07-10-2019 14:30:15
Key Size:	2048

Checking key containers...
Deleting certificate...
Selected certificate deleted successfully.

Clear Exit

3.6 HW TOKEN

This section is to personalize the SideCard for HW Token service. In this feature default applet and pre-persono scripts are loaded. 'Get HW Token Status' button gives the provided SideCard TSN card status.



Side-XTSTool V.3.0.0.0

Select Smartcard Type: ☒ SideCard™ ☐ SideSafe™

Select Smartcard Reader: Generic Smart Card Reader Interface 0 Connect

Answer To Reset: Reset

Card Transport Key: 404142434445464748494a4b4c4d4e4f4041424344454647 Get Card Info

Load Applet Delete Applet Transmit Certificates **HW Token**

Select Pre-perso File: C:\Users\Sureshbabu\Side-XTSTool\SideCard_JC2_4_2R2_145_TYFON Browse

Select Applet File: C:\Users\Sureshbabu\Side-XTSTool\hwtoken.cap Browse

Enter SideCard TSN: Get HW Token Status

Domain URL: https://int-u4ia.tyfone.com

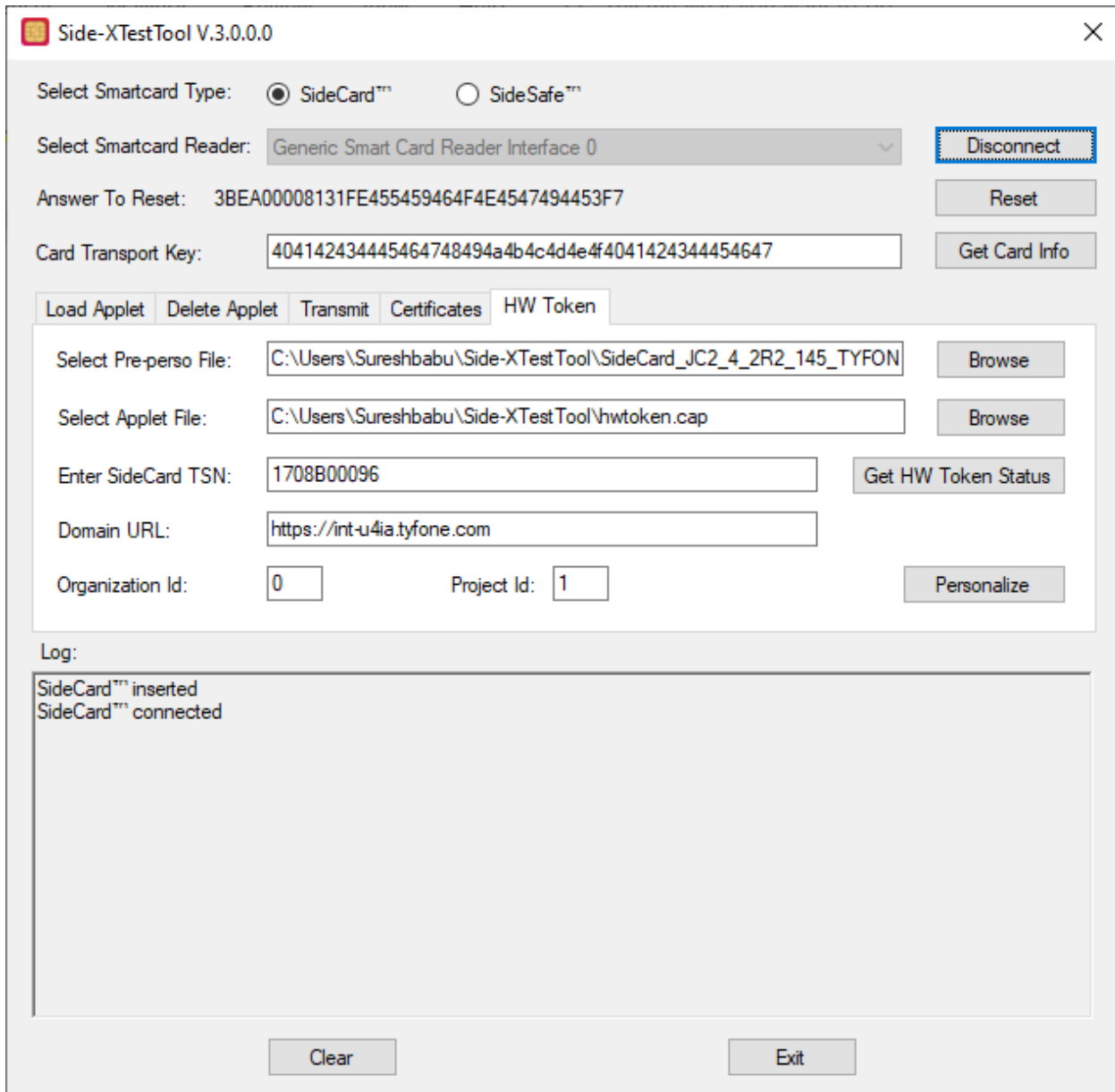
Organization Id: 0 Project Id: 1 Personalize

Log:

Registering card notifications.
SideCard™ inserted

Clear Exit

1. Enter SideCard TSN value in 'Enter SideCard TSN'
2. Click on 'Connect' button



Side-XTestTool V.3.0.0.0

Select Smartcard Type: ☒ SideCard™ ☐ SideSafe™

Select Smartcard Reader: Generic Smart Card Reader Interface 0 Disconnect

Answer To Reset: 3BEA00008131FE455459464F4E4547494453F7 Reset

Card Transport Key: 404142434445464748494a4b4c4d4e4f4041424344454647 Get Card Info

Load Applet Delete Applet Transmit Certificates **HW Token**

Select Pre-perso File: C:\Users\Sureshbabu\Side-XTestTool\SideCard_JC2_4_2R2_145_TYFON Browse

Select Applet File: C:\Users\Sureshbabu\Side-XTestTool\hwtoken.cap Browse

Enter SideCard TSN: 1708B00096 Get HW Token Status

Domain URL: https://int-u4ia.tyfone.com

Organization Id: 0 Project Id: 1 Personalize

Log:

SideCard™ inserted
SideCard™ connected

Clear Exit

- For change of “Domain URL”, “Organization Id” and “Project Id” please contact administrator, otherwise keep the default value as it is. Now, click on ‘Personalize’ button.

Side-XTestTool V.3.0.0.0

Select Smartcard Type: ☒ SideCard™ ☐ SideSafe™

Select Smartcard Reader: Generic Smart Card Reader Interface 0 Disconnect

Answer To Reset: 3BEA00008131FE455459464F4E4547494453F7 Reset

Card Transport Key: 404142434445464748494a4b4c4d4e4f4041424344454647 Get Card Info

Load Applet Delete Applet Transmit Certificates **HW Token**

Select Pre-perso File: C:\Users\Sureshbabu\Side-XTestTool\SideCard_JC2_4_2R2_145_TYFON Browse

Select Applet File: C:\Users\Sureshbabu\Side-XTestTool\hwtoken.cap Browse

Enter SideCard TSN: 1708B00096 Get HW Token Status

Domain URL: https://int-u4ia.tyfone.com

Organization Id: 0 Project Id: 1 Personalize

Log:

```
002FA810839383635373336339000
APDU: 802B000000
Response: 9000

Signed data:
3045022012B0B4F5E29ED6337DD94663DC70E46B78DA0B96571819D73760C7BD575B3FE8022100A660B151F346FA
8DE85BCE26F0D8694D8D8274530F581A1A559F802AA8B5E428
Personalizing HW Token at u4ia...

Connected SideCard personalized successfully for HW Token service.

Now, SideCard is in PROJECT_PROVISIONED state.
```

Clear Exit

If the card is 'PROJECT_PROVISIONED' state means its ready to register with HW Token application.

4 SIDECARD COMMUNICATION APPLICATION DEVELOPMENT

We use PCSC Smart Card communication APIs to communicate with our SideCard.

Refer:

<https://docs.microsoft.com/en-us/windows/win32/api/winscard/>