4.6 Using and Managing Smart Cards

SoftEther VPN Client supports Public Key Infrastructure (PKI) using smart cards. This section describes how to use SoftEther VPN Client together with smart cards. For an overview of smart card authentication, please refer to 1.5 Strong Security Features.

4.6.1 Smart Card Device Driver

Required Device Driver

To use the PKI function along with a smart card or hardware security token compatible with a smart card (hereafter collectively referred to as "smart card"), the following two device drivers must be installed on the client computer.

- Device driver of the smart card reader or other hardware device
- Device driver with PKCS#11 interface that supports the smart card in use

In addition, after installing VPN Client and then installing the smart card reader and smart card device driver, you must restart the VPN Client service or the computer.

Furthermore, if any settings need to be made in order to use the smart card with the smart card reader or smart card device driver, you must make these settings in advance. For information about the settings for using a smart card reader or smart card, please refer to the hardware manual for that device.

Supported Smart Card Types

Some PKCS#11-supported smart cards can be used with SoftEther VPN Client.

4.6.1 Selecting a Smart Card

To select the type of smart card to use, click [Select Which Smart Card to Use] on the [Smart Card] menu of VPN Client Manager. The [Select Which Smart Card to Use] window is displayed.

Select the desired type of the smart card listed here and click [OK] to enable the use of that smart card. Please note that the smart cards listed here may not necessarily work with SoftEther VPN Client.

4-6-1.png

Select Smart Card Window.

4.6.3 Listing and Obtaining Smart Card Objects

Smart Card Manager

SoftEther VPN Client has a smart card manager function that allows you to list and obtain objects on supported smart cards and write objects to a smart card. To start Smart Card Manager, click [Smart Card Manager] on the [Smart Card] menu.

When Smart Card Manager is started, a window for entering the PIN code to access the smart card is displayed. When the PIN code is correctly entered, a list of the objects on the smart card is created.

4-6-2.png

Smart Card Access Window.

You can use Smart Card Manager to list, obtain, and write the following types of data on the smart card.

- **X.509 type certificate object**
- **RSA-type private key object**
- **Arbitrary type data (binary data)**

Writing Objects to a Smart Card

To write a new object to a smart card that supports object writing, click [Import to Card]. The [Select Object Type] window is displayed. Select [Certificate], [Private Key], or [Data], click [OK], and then specify the file you want to write.

4-6-4.png

Window for Importing an Object to a Smart Card.

You must specify the name of the object you want to create on the smart card. You can specify any alphanumeric characters for the object name, but some characters may be restricted depending on the smart card.

4-6-5.png

Window for Entering the Name of the Object to be Imported.

Reading an Object from a Smart Card

You can read a certificate object or binary data in an arbitrary format from a smart card. You cannot read a private key object. To read an object, select the object, click [Export from Card], name the file, and then save it.

Creating a Certificate and RSA Private Key and Writing them to a Smart Card

You can create a certificate and RSA private key and immediately write them to a smart card. Start by clicking [Write New Certificate and Private Key to Card]. Select a root certificate or a certificate signed using another certificate for the type of certificate to be created. In addition, specify the subject names of the certificate.

4-6-6.png

Window for Creating a Certificate and Private Key.

Starting Smart Card Manager on VPN Server Manager

A smart card manager similar to VPN Client Manager is provided in VPN Server Manager, which is a VPN Server management tool. To manage smart cards with VPN Server Manager, click [Smart Card Manager] on the startup window.

4.6.4 Deleting Smart Card Objects

If a smart card allows for objects to be deleted, you can delete objects on that smart card. Select the object you want to delete and click [Delete from Card]. Please note that once an object is deleted, it cannot be restored.

4.6.5 Changing a PIN Code

Smart cards are protected by PIN codes. To change the PIN code of a smart card, click [Change PIN Code] and then enter the current and new PIN codes. Please note that some smart cards may not allow the PIN code to be changed. In this case, you can change the PIN code by using the utility provided with that smart card.

4-6-7.png

Window for Changing a Smart Card PIN Code.

4.6.6 Using Smart Card Authentication to Connect to VPN Server

To connect to VPN Server with [Smart card authentication] selected as the type of user authentication in the connection setting, insert the smart card and then enter the PIN code on the displayed PIN code entry window.

4-6-8.png

Window for Entering the Smart Card PIN Code.

4.6.8 Limitations

The following are some limitations and precautions when using the SoftEther VPN smart card function.

- Not all PKCS#11 smart cards are supported.
- When SoftEther VPN calls the PKCS#11 driver or other external program, the user must use that external program in accordance with the licensing agreement set forth by the provider of the external program at the call destination.
- You can use the smart card manager function of SoftEther VPN to write a certificate or private key to a smart card, but we recommend using the utility provided with the smart card or commercially-available PKI software.
- SoftEther VPN can't handle RSA key which have strength over 1024 bits in smart-cards.