

Guide

Installation and User Guide – Linux

With Fujitsu mPollux DigiSign Client, you can use your smart card for secure access to electronic services or organization networks, as well as to digitally sign and encrypt email messages and documents.



Contents

1	DigiSign Client smart card reader software	3
1.1	Other requirements	3
1.2	Supported operating systems	3
1.3	User guidance	3
2	Installing the DigiSign Client software	3
2.1	Removing other smart card reader programs and earlier versions of DigiSign Client	3
2.2	Installation	4
2.2.1	Requirements	4
2.2.1	Installation in SuSE Linux Enterprise Desktop environment	4
2.2.2	Installation in Red Hat Enterprise Linux environment	4
2.2.3	Installation in Ubuntu environment	5
2.3	Activating a new card	5
2.4	Verifying the installation	6
2.5	Browser and email program settings	7
2.5.1	Loading the security module	8
2.5.2	Adding certificates to browsers	9
2.5.3	Adding certificates to email programs	11
3	Using DigiSign Client	12
3.1	Basic usage	12
3.2	Managing card readers and smart cards	13
3.3	Changing a PIN code	14
3.4	Logging in to an organization network	15
3.5	Logging in to an electronic service	16
3.6	Signing a document digitally	16
3.7	Signing and encrypting an email message	17
4	Troubleshooting instructions for some common problems	18
4.1	The smart card icon is missing	18
4.2	DigiSign Client does not recognize the smart card	18
4.3	Removing the card from the reader does not change the icon	18
4.4	The page requires a client certificate	18
4.5	This connection is untrusted	18
4.6	The PIN code is blocked	18
4.7	Digital signing does not work in a browser	20

1 DigiSign Client smart card reader software

With Fujitsu mPollux DigiSign Client software, you can use your smart card for secure access to electronic services or organization networks. The software reads the certificates stored on your smart card and verifies your identity to the service provider.

You need DigiSign Client when you want to

- log in to an electronic service that requires user identification
- log in to your organization's network either directly or from another network through VPN (virtual private network)
- digitally sign a document
- sign or encrypt an email message.

1.1 Other requirements

In addition to DigiSign Client, you need

- a smart card, for example an electronic identity card or an organization card
- the PIN codes that were delivered with the card
- a smart card reader.

1.2 Supported operating systems

DigiSign Client supports the following Linux operating systems:

- SUSE Enterprise Desktop
- Red Hat Enterprise Linux
- Ubuntu

1.3 User guidance

The software is accompanied with the following documentation:

- *Fujitsu mPollux DigiSign Client Installation and User Guide – Linux* (this guide)
- *Fujitsu mPollux DigiSign Client Installation and User Guide – Mac OS*
- *Fujitsu mPollux DigiSign Client Installation and User Guide – Windows*
- *Fujitsu mPollux DigiSign Client Technical References*

2 Installing the DigiSign Client software

The installation requires that there are no other smart card reader programs or earlier versions of the DigiSign Client software installed on the computer.

2.1 Removing other smart card reader programs and earlier versions of DigiSign Client

Before installation, ensure that there are no other smart card reader programs or earlier versions of the DigiSign Client software installed.

1. Ensure that there are no other smart card reader programs or earlier versions of DigiSign Client. If there is another smart card reader program, remove it from the computer.
2. If there is a previous version of DigiSign Client, remove it with the following command:
 - In SuSE and Red Hat environments:

```
# sudo rpm -e <DigiSign installation module>
```
 - In Ubuntu environment:

```
# dpkg -r <DigiSign installation module>
```

2.2 Installation

You will get the DigiSign Client installation file from the smart card provider or your system administrator. Save the file on your computer.

2.2.1 Requirements

Installation requires root installation rights to the computer.

Before starting the DigiSign Client installation, ensure that PCSC-Lite is installed and the PCSC-Lite daemon (pcscd) is running.

DigiSign Client also requires that the card reader has the correct driver installed. You can find the driver from the card reader vendor's web site or you can test if a generic USB CCID (Chip/Smart Card Interface Devices) driver works with your card reader. Go to <http://rpm.pbone.net/> and search with "pcsc-ccid". The package contains a generic driver and a driver for the serial GemPC Twin card reader, both of which work with PCSC-Lite daemon.

2.2.1 Installation in SuSE Linux Enterprise Desktop environment

These instructions describe how to install DigiSign Client in SuSE Linux Enterprise Desktop environment. If you want to use a graphical user interface instead, you can use the YaST2 Package Manager.

1. At the command prompt, install the software with the following command:

```
# sudo rpm -Uvh <DigiSign installation module>.rpm
```

2. RPM packages may be dependent on other packages. If a necessary package is missing, the following kind of a message is shown:

```
error: Failed dependencies:
    libpcsc-lite.so.1 is needed by <DigiSign installation module>
```

Download the missing packages from a web site or SuSE installation media and add them to the command. For example:

```
# rpm -ivh pcsc-lite-<version>.rpm <DigiSign installation module>.rpm
```

3. After completing the installation, add the necessary settings to your browser and email program according to the instructions in Section 2.5 Browser and email program settings.

4. Ensure that the PC/SC Smart Card Daemon (pcscd) starts up automatically when the computer starts up.

- a) Open **YaST > System > System Services**.
- b) Ensure that pcscd is set to be run on init 5 level.

2.2.2 Installation in Red Hat Enterprise Linux environment

These instructions describe how to install DigiSign Client in Red Hat Linux Enterprise environment. If you want to use a graphical user interface instead, you can use the Package Management Tool.

1. At the command prompt, install the software with the following command:

```
# sudo yum localinstall <DigiSign installation module>.rpm
```

2. After completing the installation, add the necessary settings to your browser and email program according to the instructions in Section 2.5 Browser and email program settings.

- a) Ensure that the PC/SC Smart Card Daemon (pcscd) starts up automatically when the computer starts up, depending on your operation system version for example with the Service Configuration Utility by giving the following command:

```
# sudo system-config-services
```

- b) Ensure that pcscd is set to be run on init 5 level (graphical multi-user)

2.2.3 Installation in Ubuntu environment

These instructions describe how to install DigiSign Client in Ubuntu environment. If you want to use a graphical user interface instead, you can use the Synaptic Package Manager which provides the same functions as `apt-get`.

1. At the command prompt, install the software with the following command:

```
# dpkg -i <DigiSign installation module>.deb
```

2. Deb packages may be dependent on other packages. If a necessary package is missing, the following kind of a message is shown:

```
[sudo] password for user1:
Selecting previously deselected package mpollux-digisign-client.
(Reading database ... 133374 files and directories currently installed.)
Unpacking mpollux-digisign-client (from mpollux-digisign-client_<version>.deb)
dpkg: dependency problems prevent configuration of mpollux-digisign-client:
mpollux-digisign-client depends on pcscd; however:
Package pcscd is not installed.
dpkg: error processing mpollux-digisign-client (--install):
dependency problems - leaving unconfigured
Errors were encountered while processing:
mpollux-digisign-client
```

3. Use the Advanced Packaging Tool (`apt`) to install the package. Add the package to the command:

```
# sudo apt-get install pcscd
```

4. After completing the installation, add the necessary settings to your browser and email program according to the instructions in Section 2.5 Browser and email program settings.

5. Ensure that the PC/SC Smart Card Daemon (`pcscd`) starts up automatically when the computer starts up.

- a) At the command prompt, give the following command:

```
# sysv-rc-conf --list pcscd
```

- b) Ensure that `pcscd` is set to be run on init 5 level. If not, change the runlevel to 5 with the following command:

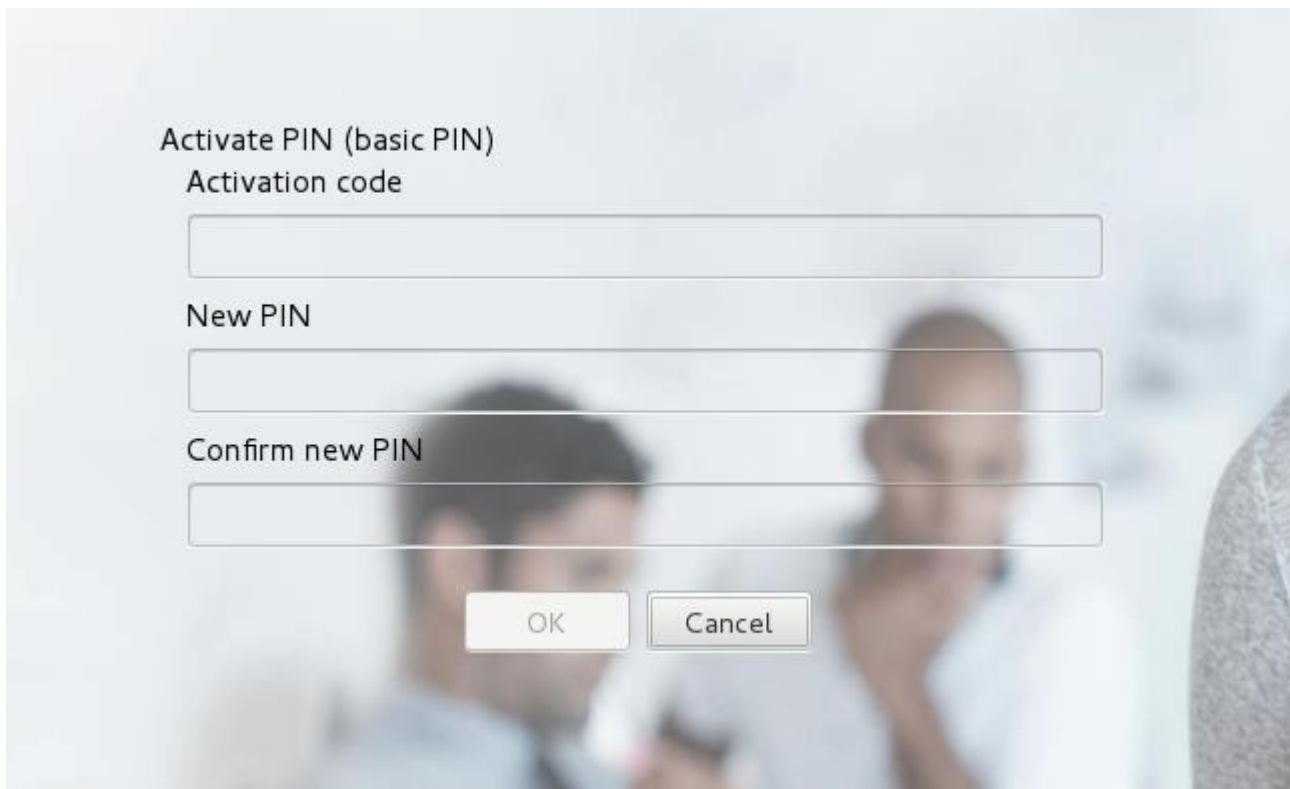
```
# sysv-rc-conf --level pcscd 5 on
```

- c) If the `sysv-rc-conf` program is not installed, you can install it with the following command:

```
# sudo apt-get install sysv-rc-conf
```

2.3 Activating a new card

In order to use a new ID card, you may need to activate it with an activation PIN. When you use the ID card for the first time, the card reader software will automatically launch the identity card activation process. During this process, you will first be prompted to enter your activation PIN, after which you can activate and specify your own personal PIN codes. After the activation process has been completed, you can use your identity card in e-services.



Activate PIN (basic PIN)

Activation code



New PIN

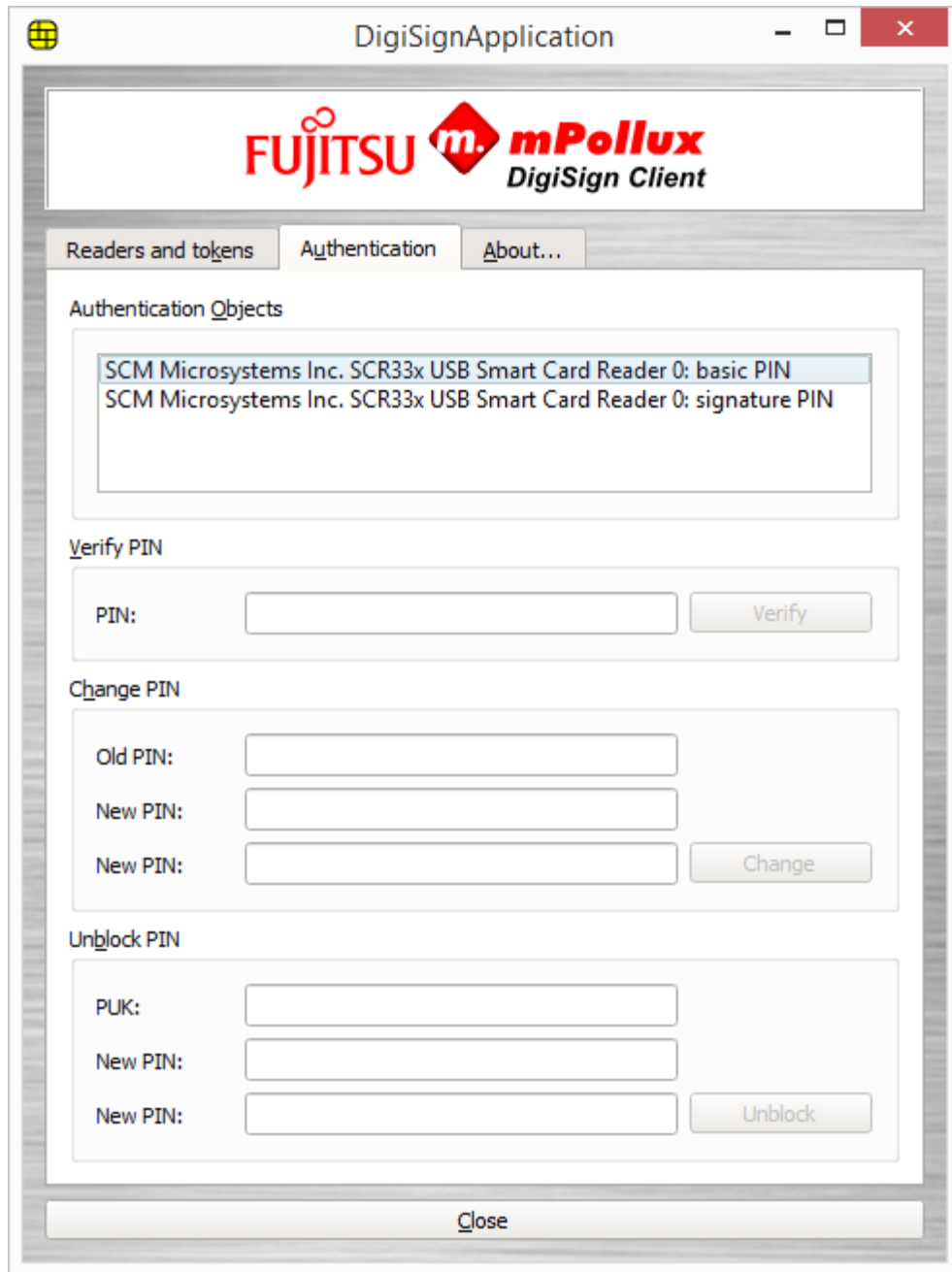
Confirm new PIN

OK Cancel

2.4 Verifying the installation

With mPollux DigiSign Client Manager, you can verify that the installation succeeded and that the smart card and the card reader work correctly.

1. Ensure that the card reader is connected to the computer. The card reader can be located in the computer or attached to it by a cable.
2. Insert the smart card to the card reader. Wait until the  icon turns yellow.
3. Right-click the  icon and select **Display tokens**.
4. Select the **Authentication** tab.



5. In the **Authentication Objects** field, select the first row (first PIN code).
6. Enter your PIN code (PIN 1) in the **PIN** field under **Verify PIN**, and click **Verify**. The program informs you that the PIN code is correct. If the program informs you that the PIN code is incorrect, ensure that you entered the PIN code correctly.

If you enter the PIN code incorrectly several times in a row, the PIN code is blocked. The exact number of attempts depends on the card. To unlock the PIN code, follow the instructions in Section 4.6 The PIN code is blocked.

2.5 Browser and email program settings



In some browsers and email programs, DigiSign Client works without any specific settings. In other programs, such as Mozilla Firefox and Thunderbird, you must add the following settings:

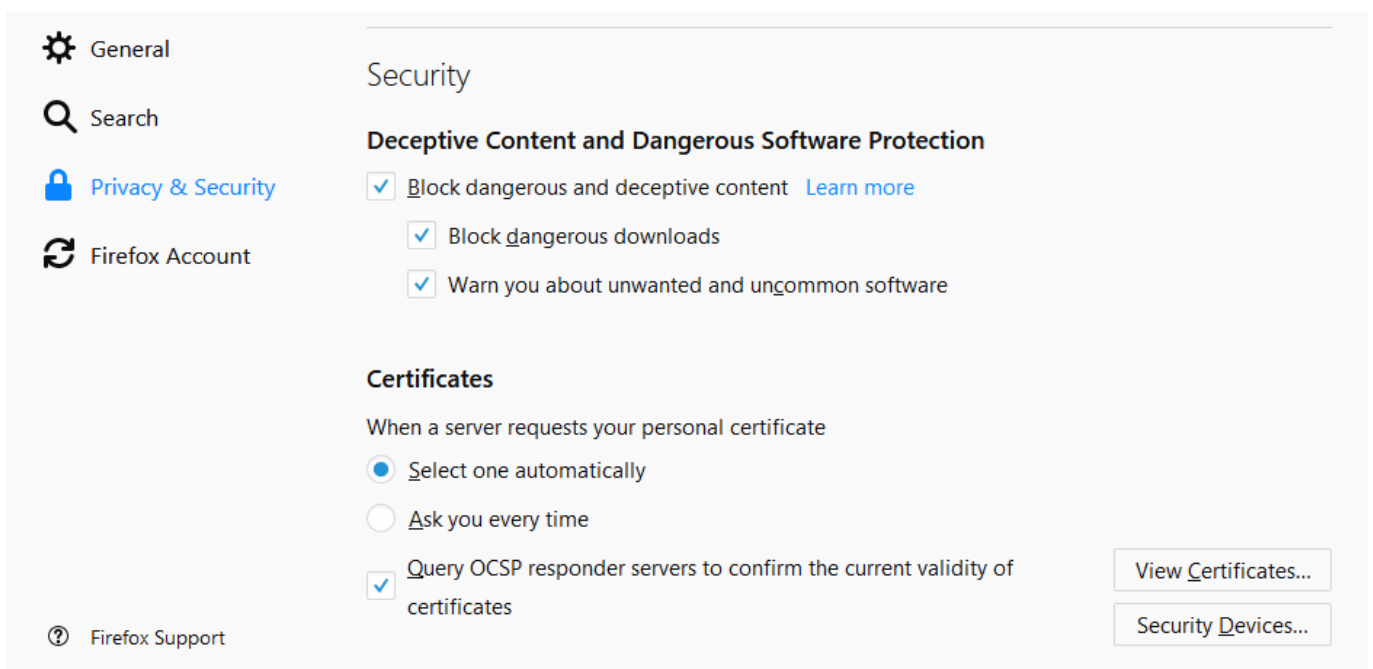
- Load the security module used by DigiSign Client to the program.

- Load the public certificates of the Certificate Authority (CA) to the program.
Until you have added these settings, the browser claims that the connection is untrusted.

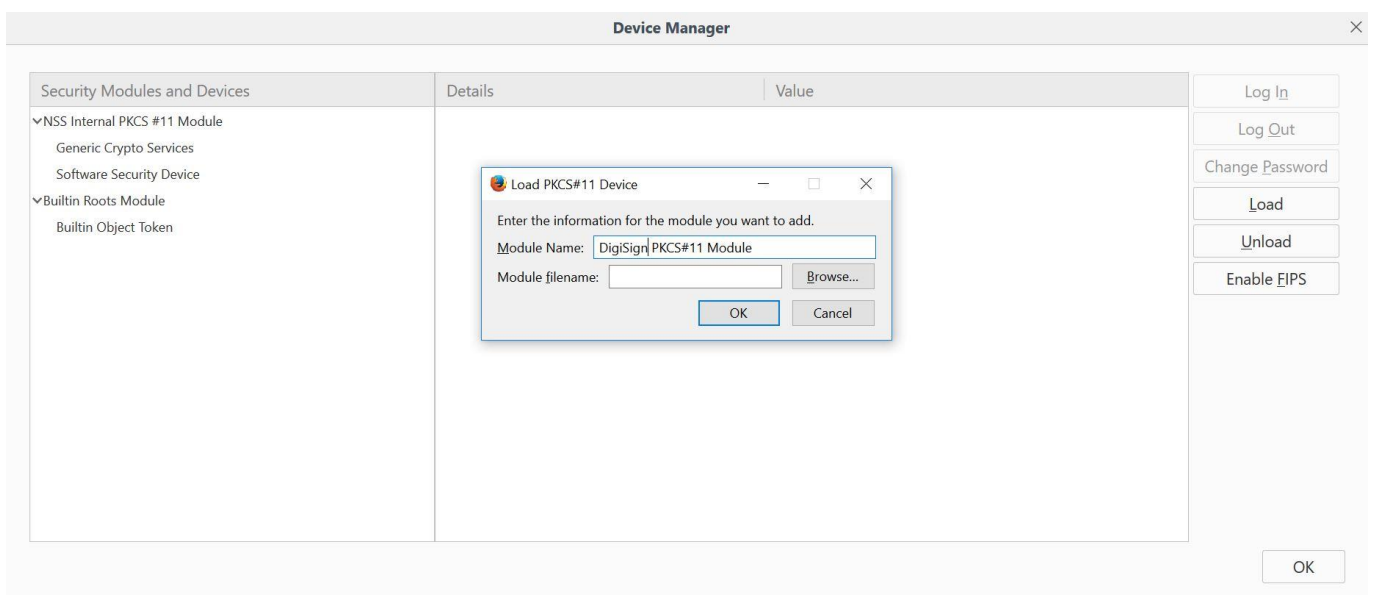
2.5.1 Loading the security module

The installation package tries to load the security module automatically on installation. In case the automatic loading fails, the following example shows how to load the security module in Mozilla Firefox and Mozilla Thunderbird. The names and locations of settings may vary slightly across versions.

1. Ensure that the  icon is shown. This means that the smart card is ready for use.
2. In Mozilla Firefox, select button  > Options > Privacy & Security > Certificates in Security section. In Mozilla Thunderbird the settings are located in  > Options > Options > Advanced > Certificates.

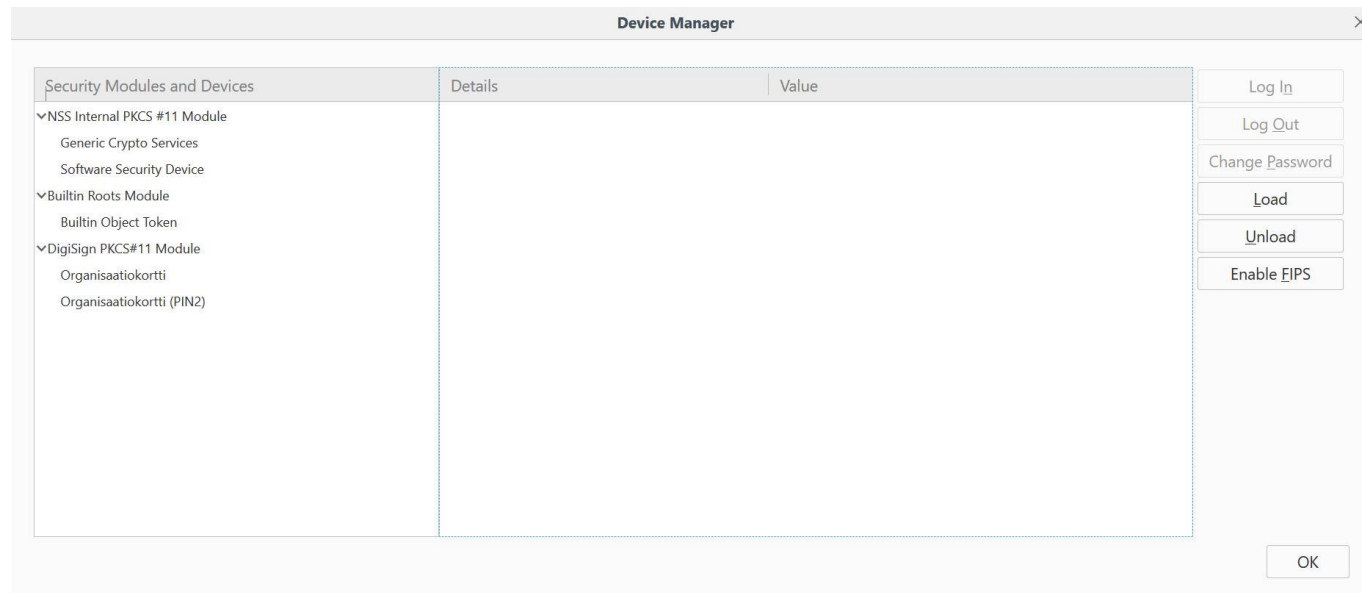


3. Under **Certificates**, select **Select one automatically**.
4. Click **Security Devices** and **Load**.



5. Name the module **DigiSign PKCS#11 Module**.

6. Click **Browse** and navigate to the `libcryptoki.so.0` file. By default, it is located in the `/usr/lib/` directory. Click **OK**.



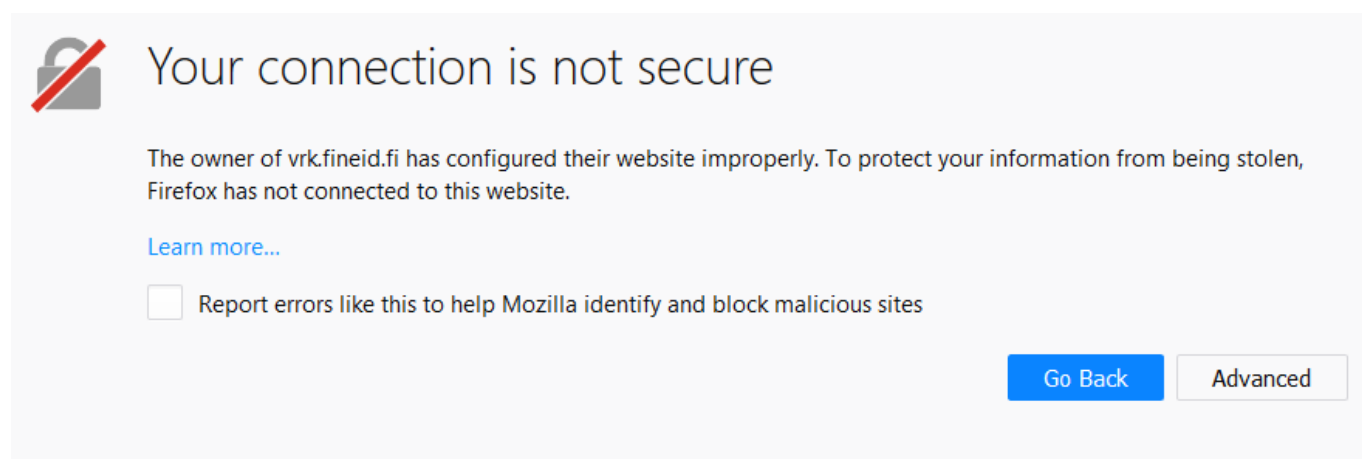
If you receive an error message saying that the security module cannot be loaded, close your browser and try again.

7. The DigiSign PKCS#11 Module is shown in the list. Click **OK** to exit the options.

8. Restart your browser or email program.

2.5.2 Adding certificates to browsers

Some browsers, such as Mozilla Firefox, require the certificates published by the Certificate Authority (CA) to be set as trusted before they can be used. If the certificate has not been set as trusted, the page claims that the connection is untrusted.



1. Ensure that the  icon is shown in the information bar. This means that the smart card is ready for use.

2. Select **Advanced**.

vrk.fineid.fi uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.
An additional root certificate may need to be imported.

Error code: [SEC_ERROR_UNKNOWN_ISSUER](#)

Add Exception...

3. Press **Add Exception**.

4. **Add Security Exception** window opens.

Add Security Exception



You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location:

[Get Certificate](#)

Certificate Status

This site attempts to identify itself with invalid information.

[View...](#)

Unknown Identity

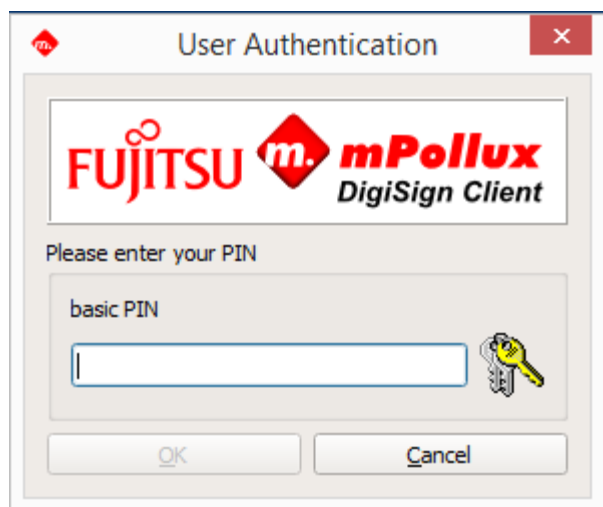
The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☒ [P](#)ermanently store this exception

[C](#)onfirm Security Exception

Cancel

5. Click **Get Certificate** and press **Confirm Security Exception**. The site asks you to enter your PIN code.





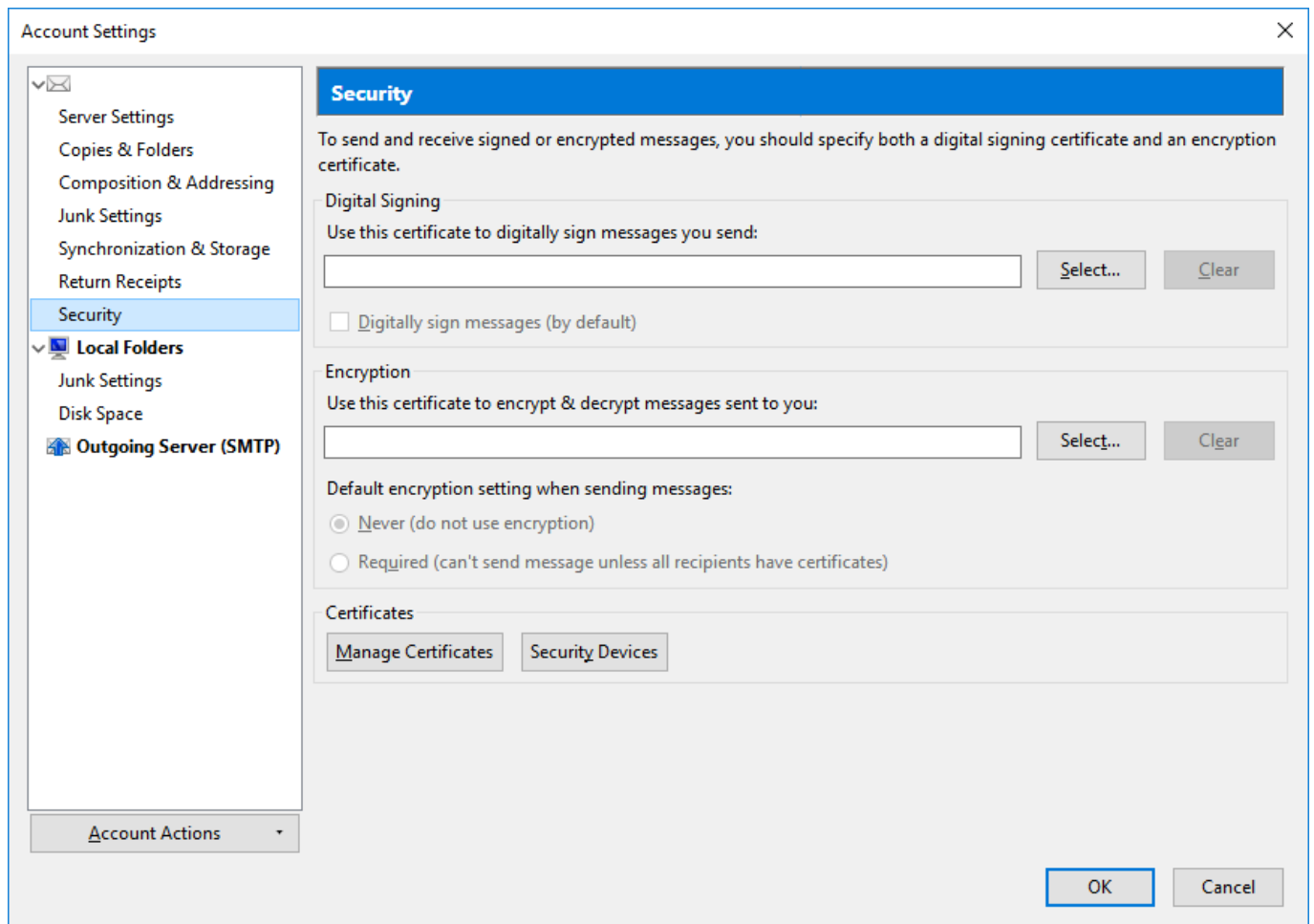
6. Enter your PIN code and click **OK**.

7. Refresh the page. You should now be able to access the site.

2.5.3 Adding certificates to email programs

The public certificates of the Certificate Authority (CA) must be added to the email program before they can be used. Note that in some programs the email address used must also be included in the smart card.

1. Ensure that the  icon is shown in the information bar. This means that the smart card is ready for use.
2. In Mozilla Thunderbird, select  > **Account Settings** > **Security**.



3. Select the certificates you want to use for signing and for encryption and decryption.


4. Click **OK**.

3 Using DigiSign Client

You need DigiSign Client when you want to

- log in to an electronic service that requires user identification
- log in to your organization's network either directly or from another network through VPN (virtual private network)
- digitally sign a document
- sign or encrypt an email message.

3.1 Basic usage

DigiSign Client starts up with Windows start-up. Using DigiSign Client requires that the smart card reader is connected to the computer, the reader driver has been installed, and the smart card has been inserted into the reader. Before starting to use a program that requires a smart card, ensure that the  icon is shown on your screen. The icon tells that the smart card is ready for use.

Upon inserting the card into the reader for the first time, you may receive a warning that the certificate is untrusted. Select **Yes** if you trust the certificate.

If you encounter any problems when using the smart card, see additional instructions in Section 4 Troubleshooting instructions for some common problems.

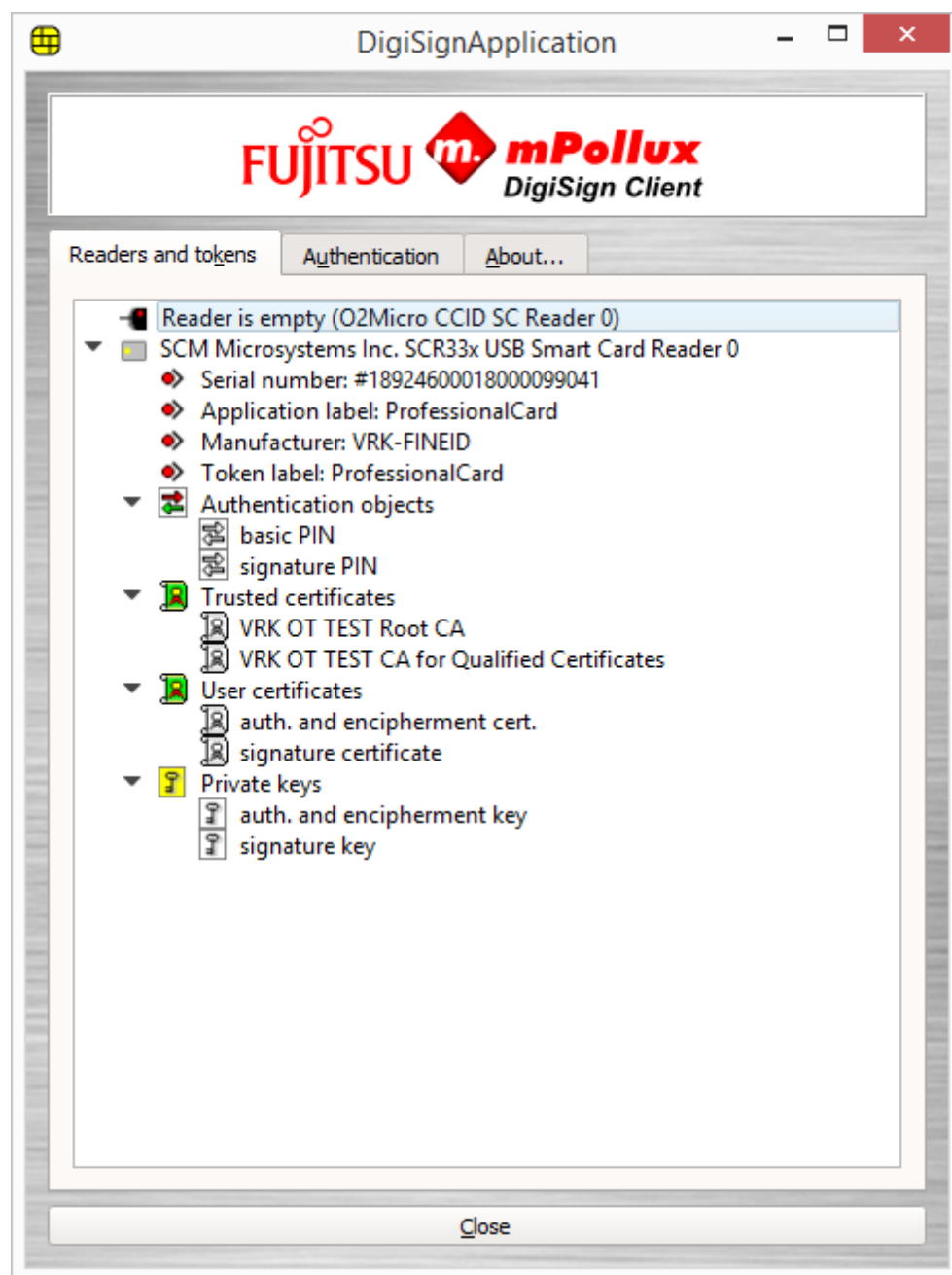
Never enter your PIN code if it is asked unexpectedly. Ensure that you have yourself started the function that asks for the PIN code.

Never remove the smart card from the card reader while using the service that you are logged in to.

3.2 Managing card readers and smart cards

With DigiSign Client you can manage your card readers and smart cards.

1. Right-click the  icon and select **Display tokens**. The DigiSign Client Manager dialog opens.



2. To view the data stored on the smart card, click on the arrows in front of each piece of text.

Security devices lists the card readers connected to the computer. The Certificate Authority (CA), card label and serial number are shown under the card reader label, if available.

Authentication objects lists the PIN codes stored on the smart card. Each card usually holds two or three PIN codes, of which the first one is used for identification (PIN 1), the second one for digital signing (PIN 2) and the third one for organizational purposes (PIN 3).

Authority certificates lists the CA certificates stored on the card.


Certificates lists the user certificates.

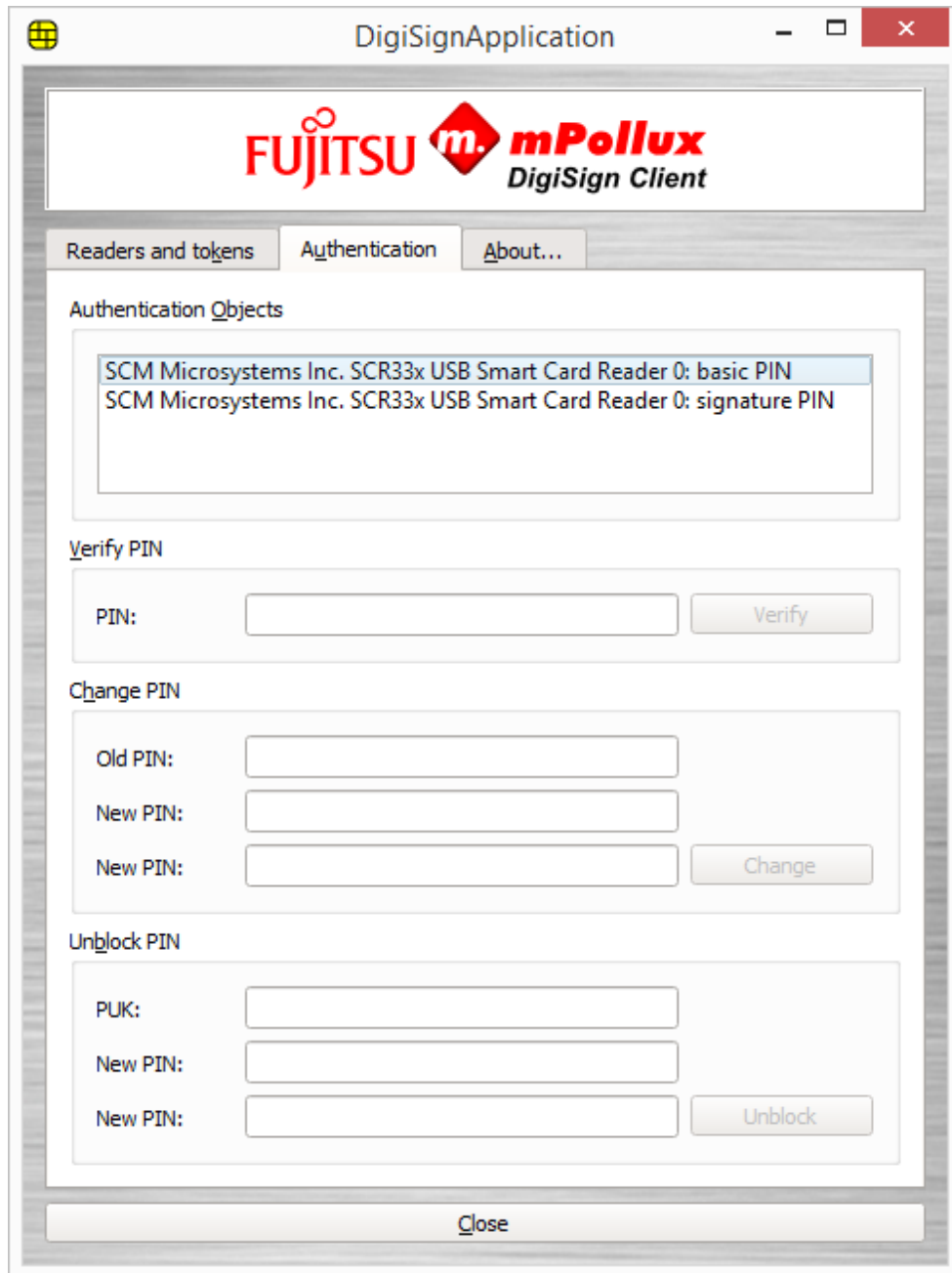
Private keys lists the user keys.

3. Right-click a certificate to open it and verify its data, such as expiry time or the email address to which the certificate is attached. You can also save the certificate.
4. Right-click a PIN code to verify, change or unlock it.
5. Right-click a key to test your PIN codes.

3.3 Changing a PIN code

You can change the PIN codes given to you. In addition to these instructions, you can change the PIN codes through the **Readers and cards** tab by holding down the Ctrl key, clicking the code, and selecting **Change**.


1. Right-click the  icon and select **Display tokens**. The DigiSign Client Manager dialog opens.
2. Select the **Authentication** tab.



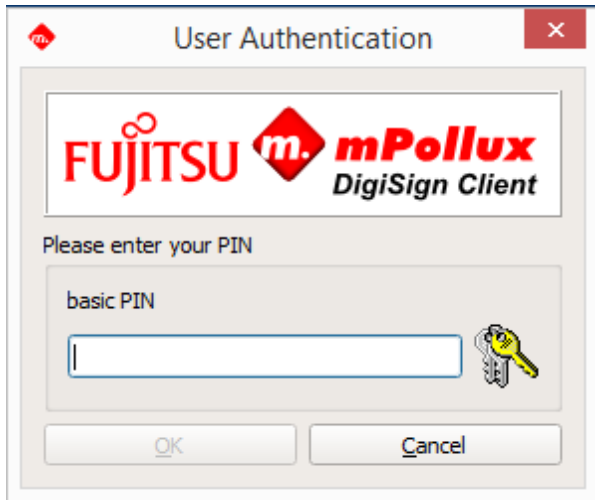
3. In the **Authentication Objects** field, select the PIN code you want to change.
4. Enter the current PIN code in the **Old PIN** field under **Change PIN**.
5. Enter your new PIN code in the **New PIN** fields. In most cases, the PIN must be 4-8 characters long.
6. Click **Change**. Your PIN code has now been changed. Memorize your new PIN code or write it down and keep it in a safe place.
7. To exit the program, click **Close**.

3.4 Logging in to an organization network

You can use DigiSign Client to log in to your organization network. Your computer must be connected to the organization network either directly or through VPN (virtual private network).

1. Ensure that the  icon is shown on the screen. This means that the smart card is ready for use.
2. Select to log in from the computer.

3. If the program asks you to verify the certificate, click **OK**. The program asks for your PIN code.




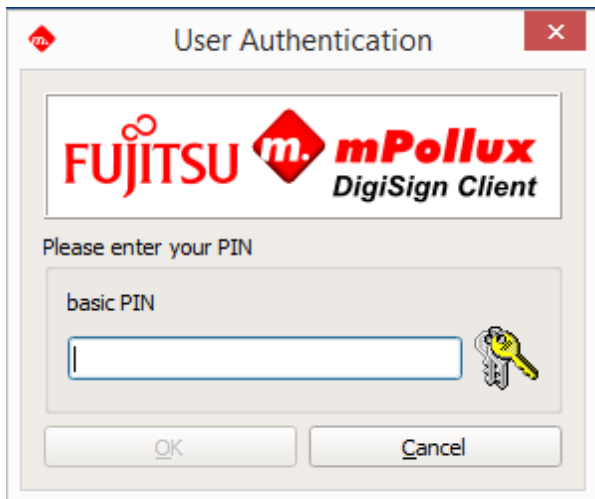
4. Enter your PIN code (PIN 1) in the field and click **OK**. You are now logged in to your organization's network.

5. When you stop using the network, remember to log out and remove the smart card from the reader.

3.5 Logging in to an electronic service

You can use DigiSign Client to log in to different electronic services that require identification.

1. Ensure that the  icon is shown on the screen. This means that the smart card is ready for use.
2. Go to the service pages and select the button or link that takes you to digital identification. The program asks you which certificate you want to use.
3. Select the certificate you want to use to log in to this service, and click **OK**. The program asks for your PIN code.




4. Enter your PIN code and click **OK**.

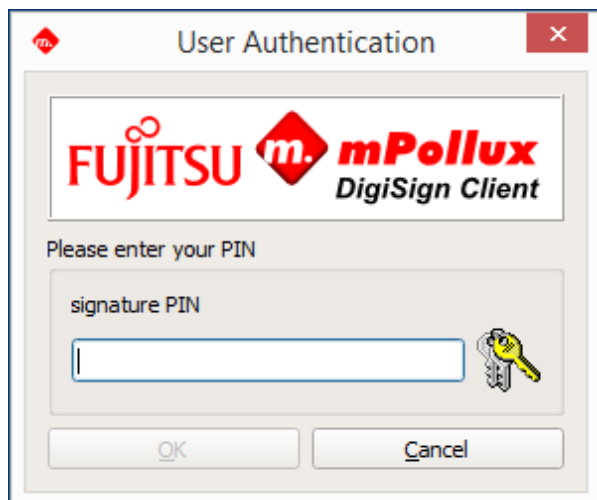
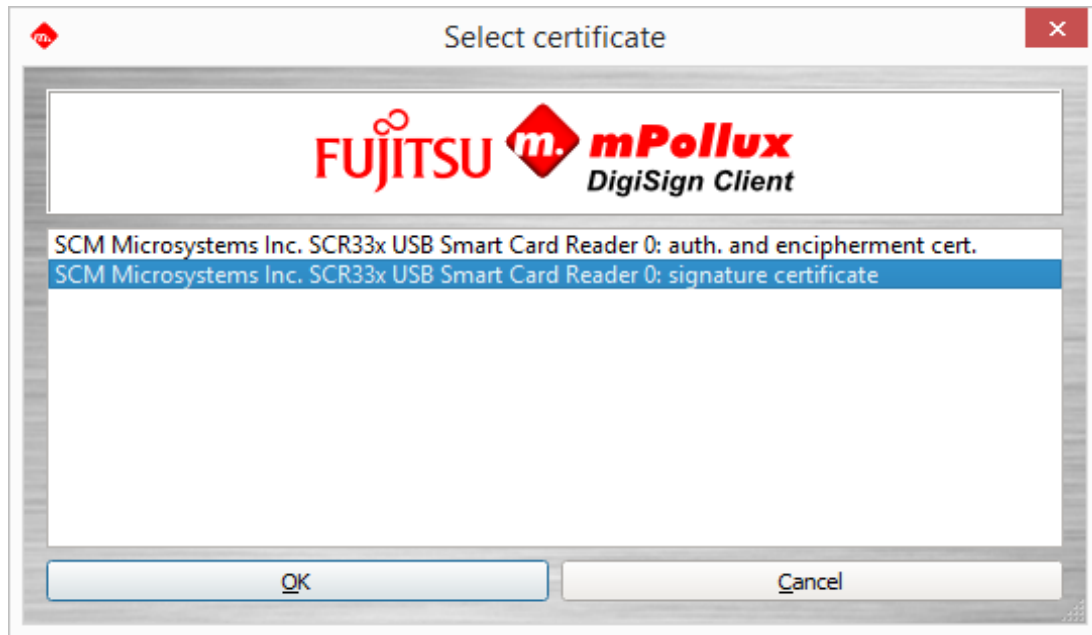
5. When you stop using the service, remember to log out and remove the smart card from the reader.

3.6 Signing a document digitally

You can use DigiSign Client to sign a digital form or document.

The program asks either PIN 1 or PIN 2 for the signature. PIN 1 is used for one-time signatures in, for example, email messages. PIN 2 is used for signatures in legally binding documents, such as contracts.

1. Ensure that the  icon is shown on the screen. This means that the smart card is ready for use.
2. Select the digital signing function in the service or document. The program asks for your PIN code.




3. Enter your PIN code and click **OK**.

3.7 Signing and encrypting an email message

You can use DigiSign Client to sign and encrypt email messages. Note that some email programs allow a message to be signed or encrypted only when the address is stored on the card with the certificate.



In addition, the recipient must have your certificate. You can deliver the certificate by sending a digitally signed message to the recipient.

1. Ensure that the  icon is shown in the information bar. This means that the smart card is ready for use.
2. Add a digital signature to a message and send it to the recipient. For more detailed instructions, see the email program's user guide.
3. The recipient can now reply to you by using the certificate attached to the message. The message is encrypted.
4. Use your certificate to decrypt the message.


4 Troubleshooting instructions for some common problems


This section gives instructions for troubleshooting some common problems when using DigiSign Client. For further instructions, contact the Certificate Authority (CA).

4.1 The smart card icon is missing

DigiSign Client starts up with system start-up. When DigiSign Client is running, there are two icons shown on the screen,  and . If you do not see smart card icon, the Certificate Loader may be disabled. For instructions on how to enable it, see the next section.

4.2 DigiSign Client does not recognize the smart card


The  icon on the screen means that DigiSign Client does not recognize the smart card. The card may be faulty or incorrect. Ensure that the card is meant to be used in the service that you are trying to use.

The  icon on the screen means that DigiSign Client does not find the smart card or the certificate stored in the card. Ensure that the card is inserted chip side up and as far into the card reader as possible.

The problem may also be in the card reader driver. Update the driver according to the vendor's instructions.

The card may also be dirty. Clean the chip carefully and try again.

4.3 Removing the card from the reader does not change the icon

If the  icon remains even though you removed the card from the reader, the reader driver is not working correctly. Update the driver according to the vendor's instructions.

4.4 The page requires a client certificate

The DigiSign security module must be loaded to the browser before DigiSign Client can be used. If the security module has not been loaded, the page gives an error message saying that it requires a client certificate. Load the security module according to instructions in Section 2.5.1 Loading the security module.

The same error is given if there is no smart card in the card reader.


4.5 This connection is untrusted

Some browsers, such as Mozilla Firefox, require the certificates published by the Certificate Authority (CA) to be set as trusted before they can be used. If the certificate has not been set as trusted, the page gives an error message saying that the connection is untrusted.

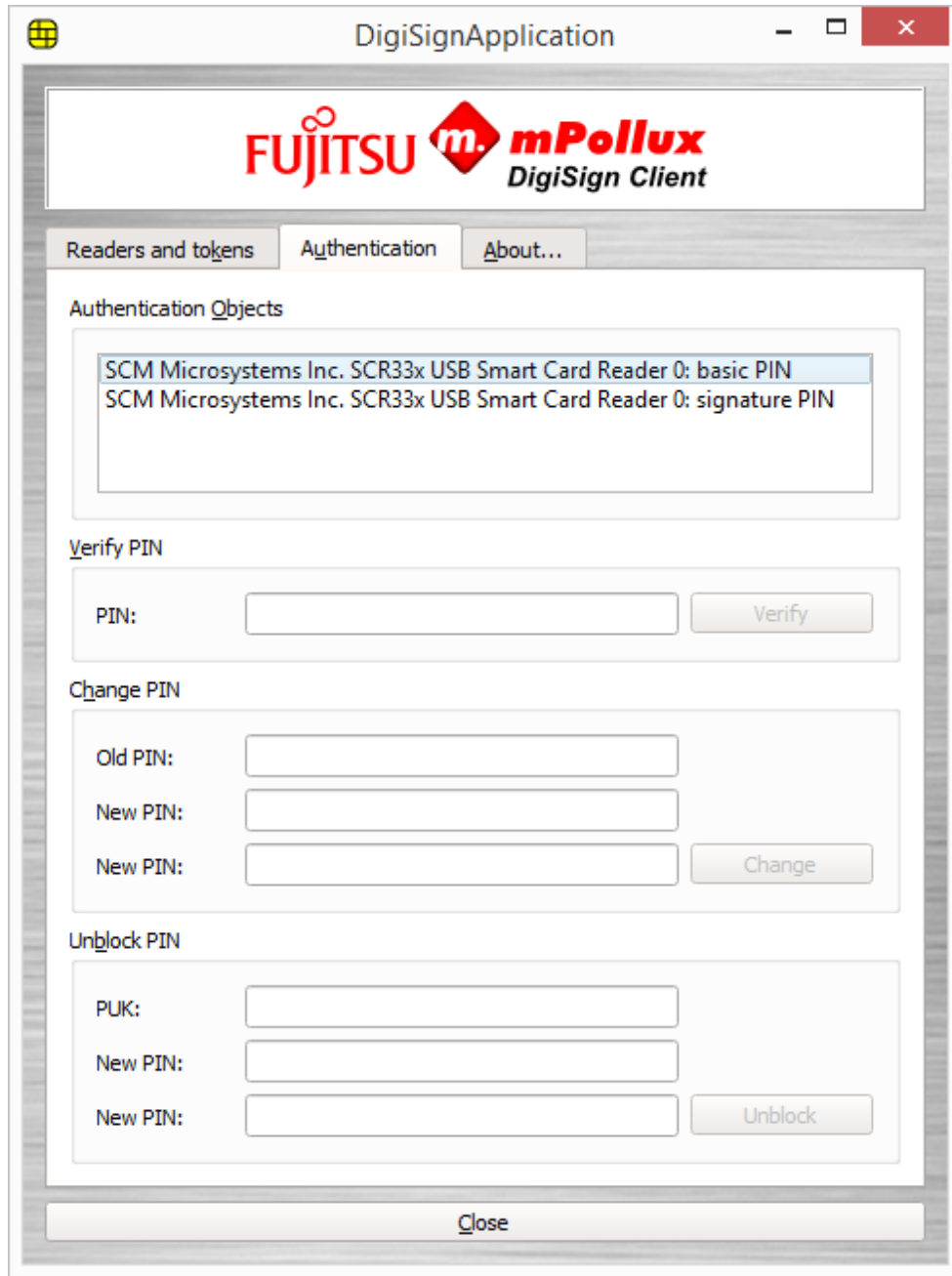
Load the certificate to the browser according to the instructions in Section 2.5.2 Adding certificates to browsers.

4.6 The PIN code is blocked

If you enter the PIN code incorrectly several times in a row, the PIN code is blocked. To unblock the PIN code, you need a PUK code. If you do not have a PUK code, request one from the Certificate Authority (CA). Newer cards are accompanied by an activation PIN letter, indicating the activation PIN of the card. If the PIN is locked for some reason, the user can reactivate it using the activation PIN indicated in the letter.

1. Right-click the  icon and select **Display tokens**.

2. Select the **Authentication** tab.



3. In the **Authentication Objects** field, select the PIN code that is blocked.

If you have several PIN codes and you do not remember which one is blocked, check that as follows:

- Select the first PIN code in the **Authentication Objects** field.
 - Enter the PIN code in the **PIN** field under **Verify PIN**, and click **Verify**.
 - If the PIN code is blocked, the program responds, "PIN code is blocked".
 - If the PIN code you selected is not blocked, continue by verifying the next PIN code.
4. Ensure that you have selected the blocked PIN code in the **Authentication Objects** field, and enter your PUK code in the **PUK** field under **Unblock PIN**.

If you enter the PUK code incorrectly several times in a row, the smart card is blocked for good. The number of tries depends on the card.


5. Enter a new PIN code in the **New PIN** fields.

6. Click **Unblock**. The program responds, "PIN unblocking successful". Memorize the new PIN code or write it down and keep it in a safe place.
7. To exit the program, click **Close**.

4.7 Digital signing does not work in a browser

DigiSign Client uses an internal web server for digital signing. Some firewalls prevent this kind of behaviour by default. If you cannot sign a digital document through a browser, check the firewall settings.

In some browsers, such as Mozilla Firefox, you must add a security exception for the DigiSign Client signature component before you can use digital signing.

1. Ensure that the  icon is shown in the information bar. This means that the smart card is ready for use.
2. Go to the following address: `https://127.0.0.1:53952/Sign`. The page says that the connection is untrusted. Load the certificate to the browser according to the instructions in Section 2.5.2 Adding certificates to browsers.

Contact

FUJITSU FINLAND OY
Address: PL 100, 00012 FUJITSU
Phone: +358 029 302 302
Website: www.fujitsu.com/fi

© Copyright 2012 Fujitsu, the Fujitsu logo are trademarks or registered trademarks of Fujitsu Limited in Japan and other countries. Other company, product and service names may be trademarks or registered trademarks of their respective owners. Technical data subject to modification and delivery subject to availability. Any liability that the data and illustrations are complete, actual or correct is excluded. Designations may be trademarks and/or copyrights of the respective manufacturer, the use of which by third parties for their own purposes may infringe the rights of such owner.