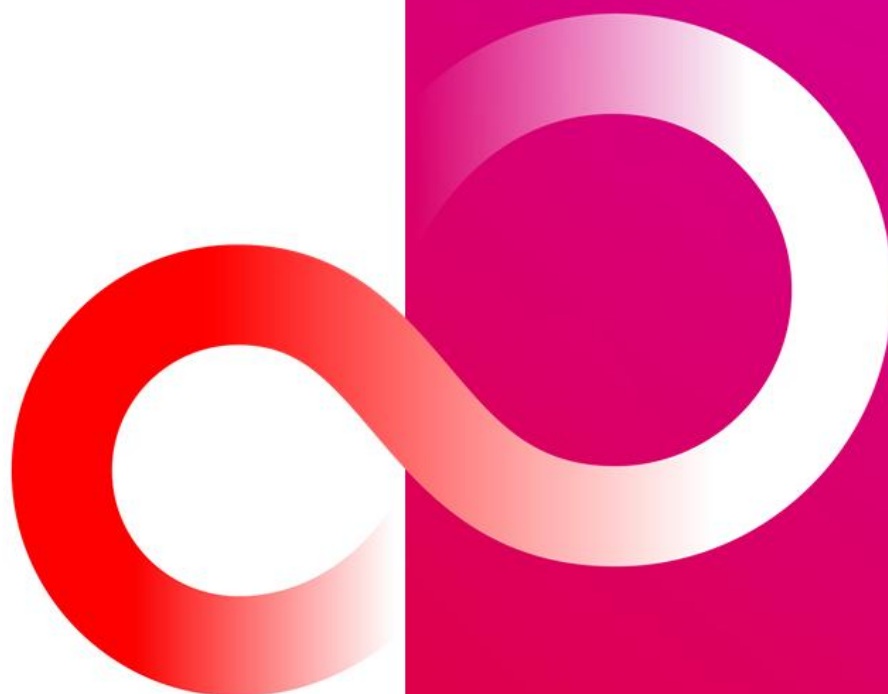


Handbok för slutanvändare Installations- och användarhandbok – Linux

V4.4.0

FUJITSU



Contents

1. Kortläsarprogramvaran DigiSign Client.....	4
1.1 Förutsättningar för användning.....	4
1.2 Operativsystem som stöds	4
1.3 Handböcker	4
2. Installation av programvaran DigiSign Client.....	5
2.1 Borttagning av tidigare kortläsarprogramvaror och versioner	5
2.2 Installation av programmet	5
2.2.1 Förutsättningar	5
2.2.2 Installation i SuSE Linux Enterprise Desktop	5
2.2.3 Installation i Red Hat Enterprise Linux	6
2.2.4 Installation i Ubuntu	6
2.2.5 DigiSign PKCS#11-modulinitiering.....	7
2.3 Aktivering av ett nytt kort.....	7
2.4 Kontroll av programvarans funktion.....	8
2.5 Inställningar i webbläsare och e-postprogram.....	9
2.5.1 Lägga till en säkerhetsmodul.....	10
2.5.2 Hämta certifikat till webbläsaren	11
2.5.3 Hämta certifikat till e-postprogrammet.....	13
3. Använda programvaran DigiSign Client.....	15
3.1 Börja använda programvaran	15
3.2 Hantering av kortläsaren och korten.....	15
3.3 Byta PIN-kod	17
3.4 Identifiering i en organisations informationsnätverk.....	18
3.5 Identifiering i en e-tjänst	18
3.6 Elektronisk signering av ett dokument	19
3.7 Signera och kryptera ett e-postmeddelande.....	20
3.8 Lägga till digital signatur i PDF-dokument.....	20
4. Problemlösning vid de vanligaste felen.....	22
4.1 Ikonen för smartkortet syns inte	22
4.2 Programvaran accepterar eller hittar inte kortet.....	22
4.3 Ikonen ändras inte fast jag tar bort kortet ur läsaren.....	22
4.4 Användarcertifikatet finns inte	22

4.5 Webbläsaren påstår att anslutningen inte är tillförlitlig22

4.6 PIN-koden (sifferkoden) har låsts22

4.7 Signaturfunktionen fungerar inte i webbläsaren24

1. Kortläsarprogramvaran DigiSign Client

Med Fujitsus programvara mPollux DigiSign Client kan du med hjälp av ett smartkort använda e-tjänster eller en organisations informationsnätverk på ett tryggt och tillförlitligt sätt. Programvaran läser av de certifikat som har sparats på det smartkort som du har beviljats och fastställer din identitet för serviceleverantörens räkning.

Du behöver programvaran DigiSign Client när du vill

- logga in i en e-tjänst som kräver identifiering,
- logga in i en organisations informationsnätverk antingen direkt eller från ett nätverk utanför organisationen med hjälp av en VPN-anslutning (virtual private network),
- underteckna ett dokument elektroniskt,
- underteckna eller kryptera ett e-postmeddelande.

1.1 Förutsättningar för användning

Förutom programmet DigiSign Client behöver du

- ett chipförsett smartkort, till exempel ett elektroniskt ID-kort eller organisationskort,
- de sifferkoder som följde med kortet, dvs. PIN-koderna,
- en kortläsare

1.2 Operativsystem som stöds

Operativsystemsversioner som stöds anges i dokumentet "Technical References".

1.3 Handböcker

Följande handböcker medföljer programvaran:

- Fujitsu mPollux DigiSign Client installations- och användarhandbok – Linux (denna handbok)
- Fujitsu mPollux DigiSign Client installations- och användarhandbok – Windows
- Fujitsu mPollux DigiSign Client installations- och användarhandbok – Mac
- Fujitsu mPollux DigiSign Client Technical References

2. Installation av programvaran DigiSign Client

För att installera eller uppdatera programvaran DigiSign Client krävs att inga andra kortläsarprogramvaror eller tidigare versioner av programvaran DigiSign Client har installerats i datorn.

2.1 Borttagning av tidigare kortläsarprogramvaror och versioner

Kontrollera före installationen att det inte finns andra kortläsarprogramvaror eller en gammal version av programvaran DigiSign Client i din dator.

1. Kontrollera att inga andra kortläsarprogramvaror har installerats i datorn. Om det finns någon annan kortläsarprogramvara i datorn ska du ta bort den på det sätt som anges i anvisningarna för programvaran.
2. Om det finns en äldre version av programvaran DigiSign i datorn ska du ta bort denna med följande kommando:
 - I SUSE- och Red Hat:

```
# sudo rpm -e <namnet på installationsmodulen för DigiSign>
```
 - I Ubuntu:

```
# dpkg -r <namnet på installationsmodulen för DigiSign>
```

2.2 Installation av programmet

Du får installationsfilen till DigiSign Client av kortleverantören eller den systemansvarige. Spara installationsfilen på din dator.

Teknisk information om installation av betrodda certifikat finns i avsnittet "Notes for Linux users" i dokumentet "DigiSign Client Technical References".

2.2.1 Förutsättningar

Du måste ha root-rättigheter på din dator för att kunna installera programvaran.

Innan den egentliga installationen av programvaran DigiSign Client påbörjas måste programvarupaketet PCSC-Lite vara installerat i datorn och PCSC-Lite daemon (pcscd) ska köras.

Programvaran mPollux DigiSign Client behöver också rätt drivrutin för smartkortläsaren. Du hittar rätt drivrutin på tillverkarens webbplats. Du kan också prova om den generiska drivrutinen USB CCID (Chip/Smart Card Interface Devices) fungerar för läsaren. Du kan söka efter drivrutinen med sökordet "pcsc-ccid" på adressen <http://rpm.pbone.net/>. Paketet innehåller en generisk drivrutin och en drivrutin till serieläsaren GemPC Twin. De här drivrutinerna är avsedda att användas med programmet PCSC-Lite daemon i programvarupaketet PCSC-Lite.

Installation includes also DigiSign PKCS11 crypto module initialization. Please see [DigiSign PKCS#11-modulinitiering](#).

2.2.2 Installation i SuSE Linux Enterprise Desktop

Den här handboken innehåller instruktioner om hur man installerar programvaran mPollux DigiSign Client i SuSE Linux Enterprise Desktop. Om du vill ha ett grafiskt gränssnitt kan du använda programvaran YaST2 Package Manager.

1. När en kommandoprompt visas på skärmen installerar du programmet genom att ge följande kommando:

```
# sudo rpm -Uvh <installationsmodulen för DigiSign>.rpm
```

2. RPM-paket kan ibland vara beroende av andra paket. Om något nödvändigt paket saknas visas ett meddelande av följande slag:

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

Sök efter de paket som saknas på internet eller på installationsskivan för SUSE och lägg till dem i kommandot:
Till exempel:

```
# rpm -ivh pcsc-lite-<version>.rpm <installationsmodulen för DigiSign>.rpm
```
3. Gör de nödvändiga inställningarna i webbläsaren och e-postprogrammet enligt anvisningarna i kapitel 2.5
Inställningar i webbläsare och e-postprogram efter att installationen har slutförts.
4. Kontrollera att PC/SC Smart Card Daemon (pcscd) startar automatiskt varje gång datorn startas.
 - a) Öppna YaST > System > System Services.
 - b) Kontrollera att den angivna körnivån för pcscd är init 5.

2.2.3 Installation i Red Hat Enterprise Linux

Den här handboken innehåller instruktioner om hur man installerar programvaran DigiSign Client i Red Hat Linux Enterprise. Om du vill ha ett grafiskt gränssnitt kan du använda verktyget Package Management Tool.

1. När en kommandoprompt visas på skärmen installerar du programmet genom att ge följande kommando:

```
# sudo yum localinstall <installationsmodulen för DigiSign>.rpm
```
2. Gör de nödvändiga inställningarna i webbläsaren och e-postprogrammet enligt anvisningarna i kapitel 2.5
Inställningar i webbläsare och e-postprogram efter att installationen har slutförts.
 - a) Kontrollera att PC/SC Smart Card Daemon (pcscd) ska startas automatiskt varje gång datorn startas, (beroende på din operativsystemversion) t.ex. med Service genom att ge följande kommando på kommandoraden:

```
# service pcscd status
```
 - b) Kontrollera att den angivna körnivån för pcscd är init 5 (grafisk multiuser).
 - c) On RHEL/CentOS 7.x/8.x use `systemctl` for checking if pcscd service is started:

```
# systemctl status pcscd.service
```

På RHEL7 kommer Linux-systemet att ta hand om att starta pcscdprocessen när en applikation försöker kommunicera till en socket. Detta kan dock kräva en omstart efter installationen av DigiSign Client

2.2.4 Installation i Ubuntu

Den här handboken innehåller instruktioner om hur man installerar programvaran DigiSign Client i Ubuntu. Om du vill ha ett grafiskt gränssnitt kan du använda programvaran Synaptic Package Manager, som tillhandahåller samma funktioner som apt-get.

1. När en kommandoprompt visas på skärmen installerar du programmet genom att ge följande kommando.
Använd apt-get verktyg med full sökväg för att lösa allt beroende. Använd full sökväg till paketet:

```
# sudo apt-get install /full_path/<DigiSign installation module>.deb
```
2. Använd verktyget Advanced Packaging Tool (apt) och installera paketet som saknas. Lägg till det i kommandot:

```
# sudo apt-get install pcscd
```
3. Gör de nödvändiga inställningarna i webbläsaren och e-postprogrammet enligt anvisningarna i kapitel 2.5
Inställningar i webbläsare och e-postprogram efter att installationen har slutförts.
4. Kontrollera att PC/SC Smart Card Daemon (pcscd) startar automatiskt varje gång datorn startas.

- a) Ge följande kommando på kommandoraden:

```
# sudo systemctl is-enabled pcscd.socket
```

pcscd.socket-tjänsten utlöser pcscd-tjänsten och den bör vara i aktiverat tillstånd.

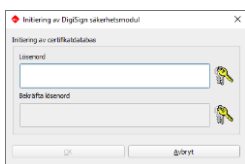
- b) Ge följande kommando på kommandoraden om tjänsten pcscd.socket i avaktiverat tillstånd:

```
# systemctl enable pcscd.socket
```

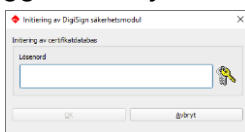
2.2.5 DigiSign PKCS#11-modulinitiering

För att smartkortsfunktionalitet ska fungera med webbläsare och andra applikationer måste PKCS#11-modulen och DigiSign-certifikatet läggas till i den lokala säkerhetsdatabasen. I de flesta fall sker detta automatiskt när DigiSign-applikationen startas för första gången. Användaren uppmanas att ange ett lösenord antingen för att skapa en ny säkerhetsdatabas eller för att komma åt en befintlig enligt följande:

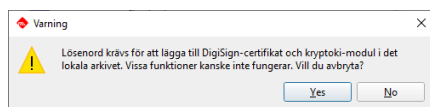
1. Säkerhetsdatabasen finns inte, så användaren ombeds ange ett lösenord för att skapa en ny säkerhetsdatabas



2. Säkerhetsdatabasen är redan konfigurerad. Användaren ombeds ange ett lösenord så att installatören kan lägga till en ny säkerhetsmodul och certifikat i den



Om användaren avbryter installationen visas följande varningsfönster. Om installationen avbryts kanske signatur-, autentiserings- och krypteringsfunktionerna inte fungerar korrekt.



I typiska fall kommer konfigurationen att frågas endast en gång när DigiSign Application startar första gången.

Om något går fel kan säkerhetsdatabasen konfigureras om enligt följande:

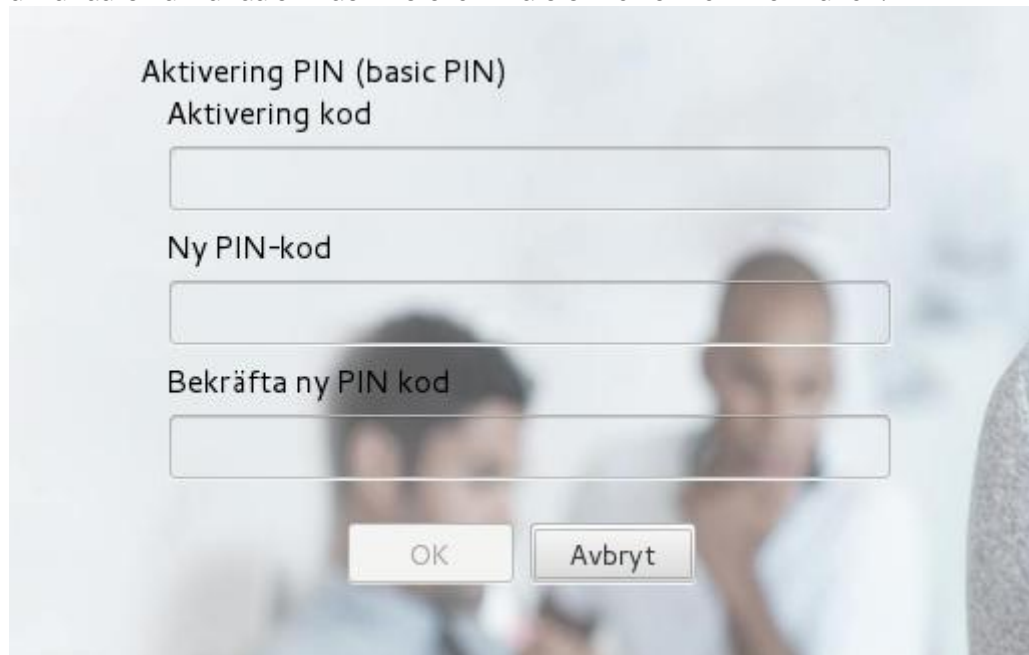
- Avlägsna ~/.digisign folder
- Säkerhetskopiering ~/.pki/nssdb folder
- Avlägsna ~/.pki/nssdb folder
- Omstart DigiSign Application

Se kapitel 2.5 för mer information om webbläsare och e-postklienter.

2.3 Aktivering av ett nytt kort

Användning av ett nytt identitetskort vid elektronisk kommunikation kan förutsätta aktivering med hjälp av en aktiveringskod. När identitetskortet används för första gången, startar kortläsarprogrammet automatiskt aktiveringsprocessen för identitetskortet. Under denna process ombeds användare först ange aktiveringskoden,

varefter användaren kan aktivera och ställa in sin egen, personliga PIN-kod. Efter aktiveringsprocessen kan användaren använda sitt identitetskort vid elektronisk kommunikation.



Aktivering PIN (basic PIN)

Aktivering kod

Ny PIN-kod

Bekräfta ny PIN kod

OK Avbryt

2.4 Kontroll av programvarans funktion

Med verktyget mPollux DigiSign Client Manager kan du kontrollera att installationen av programmet lyckades, att smartkortet är helt och att kortläsaren fungerar.

1. Kontrollera att kortläsaren är sammankopplad med datorn. Kortläsaren kan finnas i datorn eller vara kopplad till datorn med en kabel.
2. Placera smartkortet i kortläsaren. Vänta tills ikonen  blir gul.
3. Högerklicka på ikonen  och välj **Starta Client Manager**.
4. Välj fliken **Autentisering**.

Om din skrivbordsmiljö inte innehåller ett systemfält eller liknande för att visa statusikoner kan du behöva installera ytterligare komponenter, som AppIndicator eller TopIcons, för att använda  ikonen.

The screenshot shows the 'DigiSignApplication' window. At the top, there is a header with the Fujitsu mPollux DigiSign Client logo. Below the header, there are three tabs: 'Läsare och token', 'Autentisering', and 'Om...'. The 'Autentisering' tab is selected. Under this tab, there is a section titled 'Autentiseringsobjekt' which contains a list of two items: 'SCM Microsystems Inc. SCR33x USB Smart Card Reader 0: grund P' and 'SCM Microsystems Inc. SCR33x USB Smart Card Reader 0: signatur'. Below this list, there are three sections for PIN management: 'Verifera PIN' with a 'PIN-kod:' field and a 'Verifera' button; 'Ändra PIN-kod' with three fields for 'PIN-kod:', 'Ny PIN-kod:', and 'Ny PIN-kod:', and an 'Ändra' button; and 'Lås upp PIN' with three fields for 'PUK-kod:', 'Ny PIN-kod:', and 'Ny PIN-kod:', and a 'Lås upp' button. At the bottom of the window, there is a 'Stäng' button.

5. Välj den första PIN-koden i fältet **Autentiseringsobjekt**.
6. Skriv in din PIN-kod i fältet PIN-kod i avsnittet **Verifera PIN** och klicka på **Verifera**. Programmet meddelar att verifikationen av PIN-koden lyckades. Om programmet meddelar att verifikationen av PIN-koden misslyckades bör du kontrollera att du skrev in PIN-koden korrekt.

Om du anger fel PIN-kod tillräckligt många gånger i rad låser programmet koden. Det exakta antalet gånger beror på kortet. Lås upp PIN-koden med hjälp av PUK-koden i enlighet med anvisningarna i kapitel 4.6 PIN-koden (sifferkoden) har låsts.

2.5 Inställningar i webbläsare och e-postprogram

I vissa webbläsare och e-postprogram fungerar programvaran DigiSign Client utan särskilda inställningar.

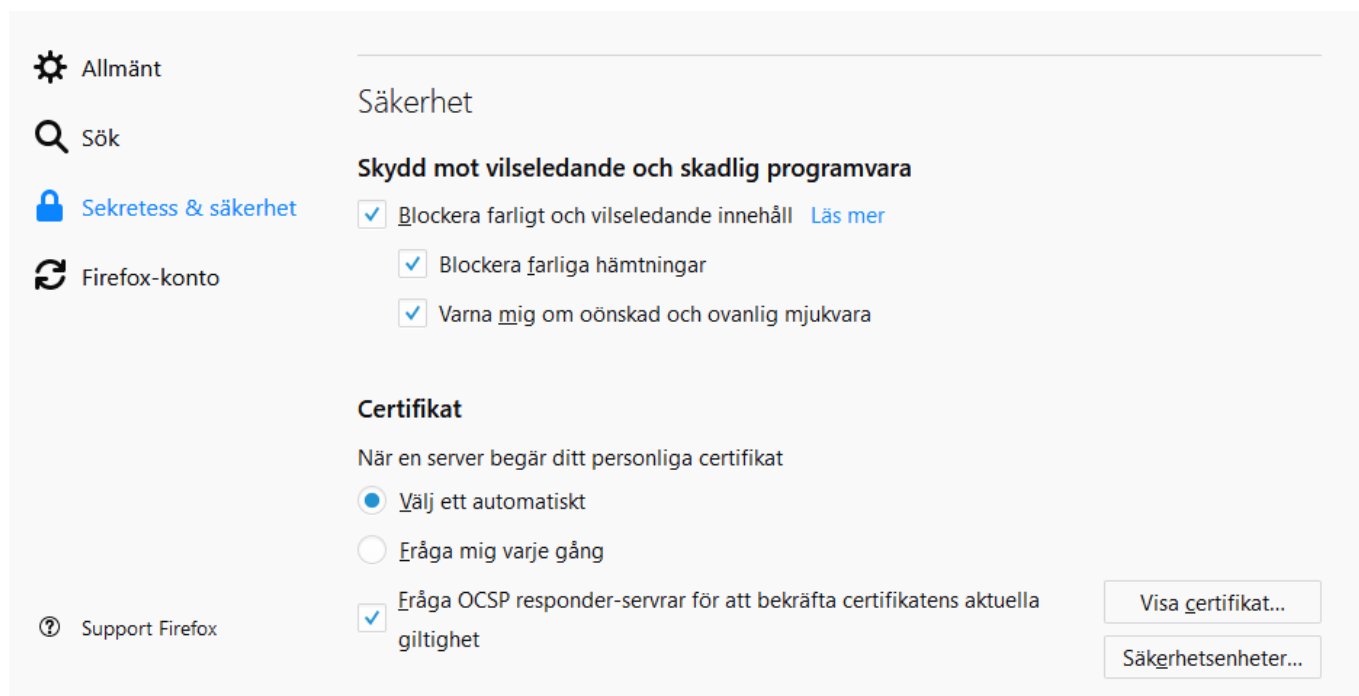
Men om säkerhetsmodul eller betrodda certifikatinstallation inte lyckades under installationen, de kan läggas till manuellt enligt följande;

- Lägga till den säkerhetsmodul som programvaran DigiSign Client använder i programmet.
- Hämta certifikatutfärdarens offentliga certifikat till programmet.
 - Innan du har gjort dessa inställningar påstår webbläsaren att anslutningen inte är tillförlitlig.

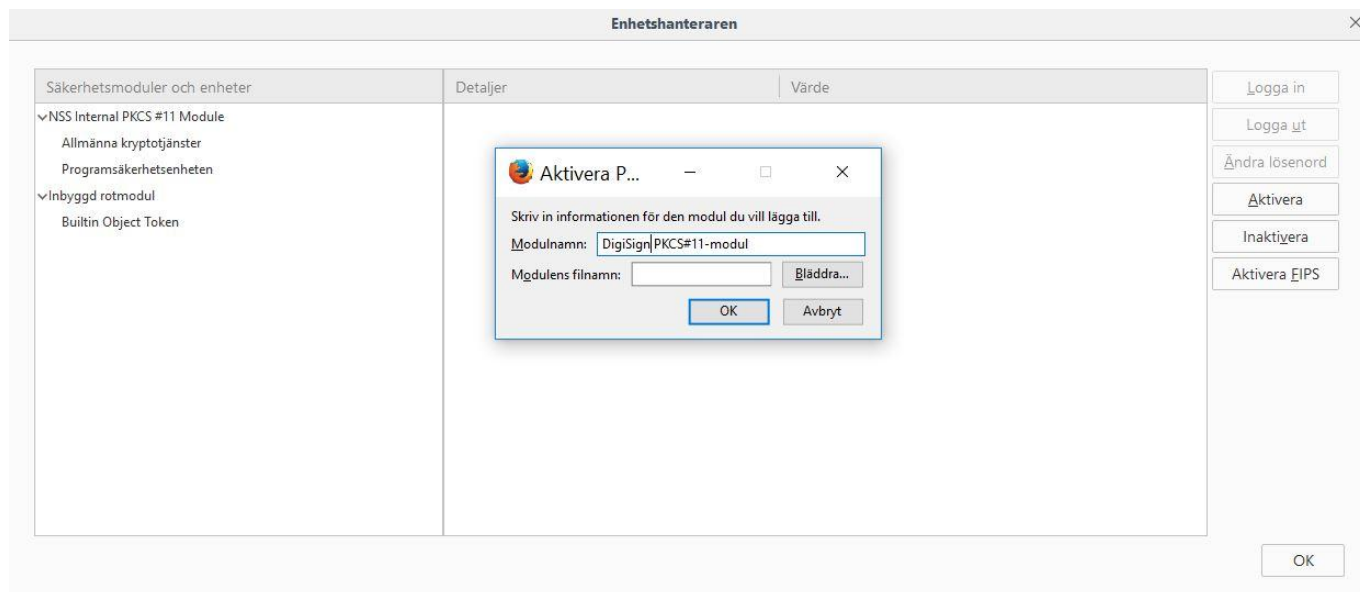
2.5.1 Lägga till en säkerhetsmodul

Installationspaketet försöker ladda säkerhetsmodulen automatiskt vid installationen. Om den automatiska laddningen misslyckas, visar följande exempel hur man lägger till en säkerhetsmodul i Mozilla Firefox och Mozilla Thunderbird. I andra program och versioner kan inställningarna se annorlunda ut.

1. Kontrollera att ikonen , som betyder att smartkortet är färdigt att användas, syns på skärmen.
2. I Mozilla Firefox välj  > **Inställningar** > **Sekretess & säkerhet** > **Certifikat** i sektionen **Säkerhet**. I Mozilla Thunderbird finns inställningarna i menyn  > **Inställningar** > **Inställningar** > **Avancerat** > **Certifikat**.



3. Välj alternativet **Välj ett automatiskt** under rubriken **Certifikat**.
4. Klicka på **Säkerhetsenheter** och **Aktivera**.



5. Ge modulen namnet DigiSign PKCS#11 Module.

6. Klicka på Bläddra och sök efter filen `libcryptoki.so.0` i din dator. I standardfallet finns den i katalogen `/usr/lib/`. Klicka på OK.



7. Modulen DigiSign PKCS#11 finns nu med på listan. Klicka på **OK** för att stänga inställningarna.

8. Starta om webbläsaren eller e-postprogrammet.

2.5.2 Hämta certifikat till webbläsaren

I vissa webbläsare, som Mozilla Firefox, måste certifikatutfärdarens offentliga certifikat anges som tillförlitliga före användningen. Innan du har gjort detta påstår webbläsaren att anslutningen inte är tillförlitlig.



Din anslutning är inte säker

Ägaren av vrk.fineid.fi har konfigurerat sin webbplats felaktigt. För att skydda din information från att bli stulen, har Firefox inte anslutit till denna webbplats.

[Läs mer...](#)

☐ Rapportera fel som detta för att hjälpa Mozilla identifiera och blockera skadliga webbplatser

Gå bakåtAvancerat

1. Kontrollera att ikonen , som betyder att smartkortet är färdigt att användas, syns på skärmen.
2. Välj **Avancerad**.

vrk.fineid.fi använder ett ogiltigt säkerhetscertifikat.

Certifikatet är inte betrott eftersom utfärdarcertifikatet är okänt.
Servern kanske inte skickar lämpliga mellanliggande certifikat.
Ett extra rotcertifikat kan behöva importeras.

Felkod: [SEC_ERROR_UNKNOWN_ISSUER](#)

Lägg till undantag...

3. Välj **Lägg till undantag**.
4. **Lägg till säkerhetsundantag** fönstret öppnas.

Lägg till säkerhetsundantag ✕



Du håller på att åsidosätta hur Firefox identifierar denna webbplats.
Legitima banker, butiker och andra offentliga webbplatser kommer inte att be dig göra detta.

Server

Adress: Hämta certifikat

Certifikatstatus

Den här webbplatsen försöker identifiera sig med ogiltig information. Visa...

Okänd identitet

Certifikatet är inte betrodd eftersom det inte har verifierats av en betrodd certifikatutfärdare med hjälp av en säker signatur.

☒ Lagra detta undantag permanent

Bekräfta säkerhetsundantag Avbryt

5. Välj **Hämta certifikat** och sedan välj **Bekräfta säkerhetsundantag**. Programmet ber dig identifiera dig.

Användarautentisering ✕



Ange din PIN-kod

grund PIN



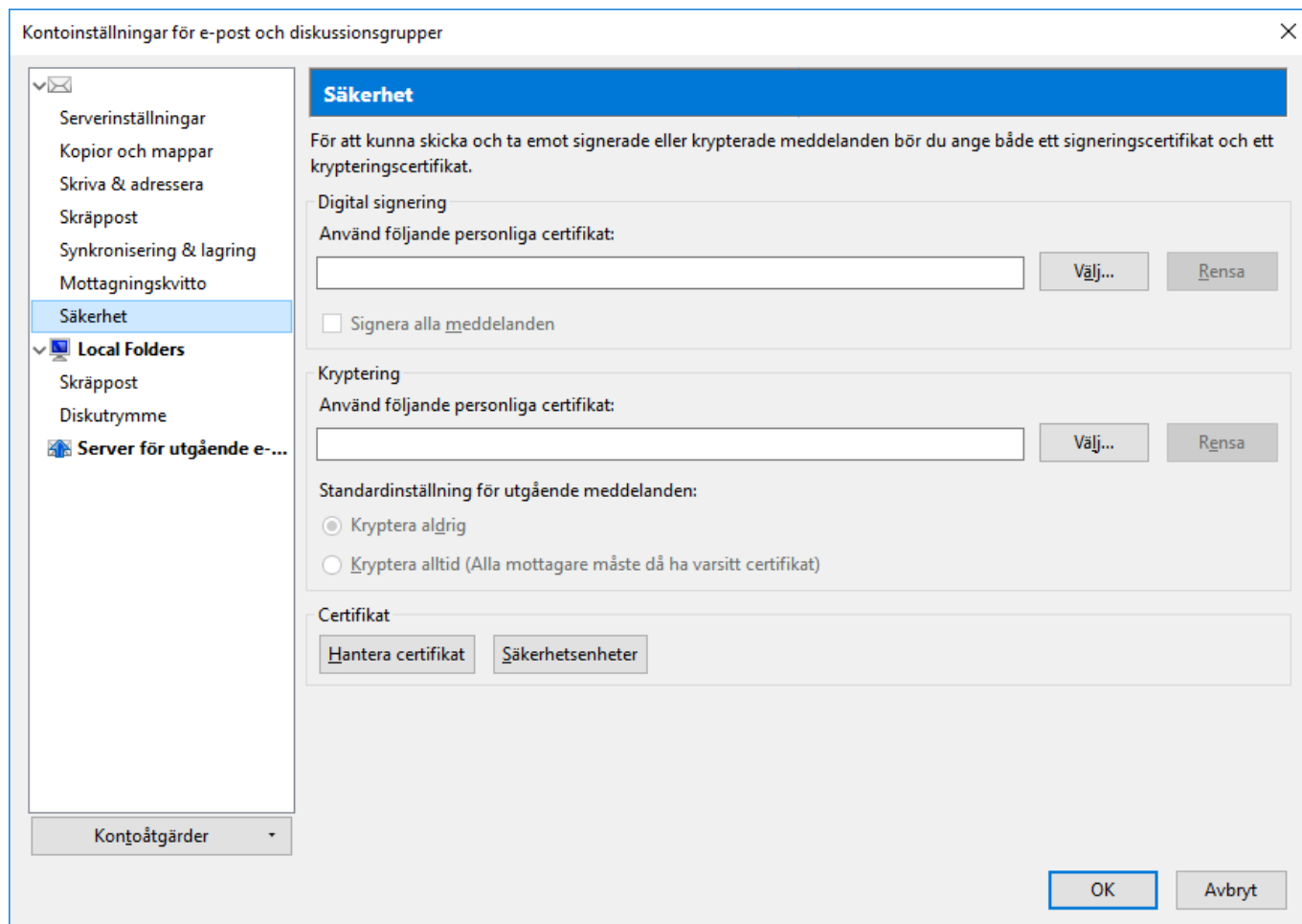
OK Avbryt

6. Skriv in din PIN-kod och klicka på **OK**.
7. Uppdatera sidan. Nu borde du kunna använda tjänsten.

2.5.3 Hämta certifikat till e-postprogrammet

Certifikatutfärdarens offentliga certifikat måste hämtas till programmet innan de kan användas. Observera att i vissa e-postprogram kan ett certifikat användas endast med den e-postlåda som hör till den adress som har sparats i certifikatet.

1. Kontrollera att ikonen , som betyder att smartkortet är färdigt att användas, syns på skärmen.
2. Välj  > **Kontoinställningar** > **Säkerhet** i Mozilla Thunderbird.



3. Välj de signerings-, autentiserings- och krypteringscertifikat du använder.
4. Klicka på **OK**.

3. Använda programvaran DigiSign Client

Du behöver programvaran DigiSign Client när du vill

- logga in i en e-tjänst som kräver identifiering,
- logga in i en organisations informationsnätverk antingen direkt eller från ett nätverk utanför organisationen med hjälp av en VPN-anslutning (virtual private network),
- underteckna ett dokument elektroniskt,
- underteckna eller kryptera ett e-postmeddelande.

3.1 Börja använda programvaran

Programvaran DigiSign Client startar när datorn startas. För att använda programvaran krävs att datorn har försetts med en kortläsare, att drivrutinerna för kortläsaren har installerats i datorn och att ett smartkort har placerats i kortläsaren. Kontrollera alltid före användningen att ikonen , som betyder att smartkortet är färdigt att användas, syns på skärmen.

När du placerar kortet i läsaren för första gången kan det hända att du får en varning om att certifikatet inte är tillförlitligt. Välj **Ja** om du litar på certifikatet.

Om det uppstår problem under användningen finns ytterligare anvisningar i kapitel 4 Problemlösning vid de vanligaste felen.

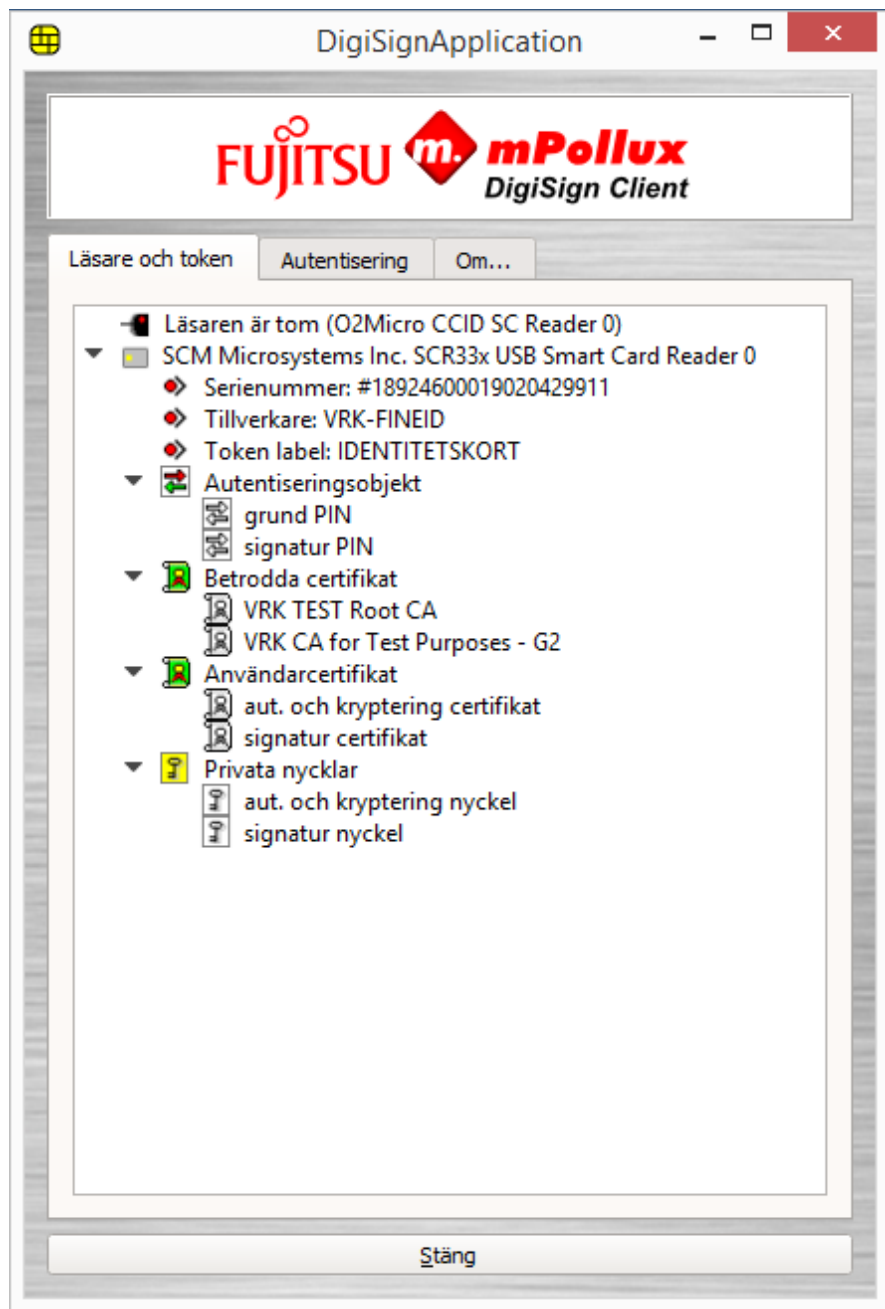
Uppge aldrig din PIN-kod om du oväntat ombeds ange den. Kontrollera alltid att du själv har startat den funktion som frågar efter PIN-koden.

Ta inte bort kortet ur kortläsaren medan du använder den tjänst som du har identifierat dig för.

3.2 Hantering av kortläsaren och korten

Med verktyget DigiSign Client Manager kan du hantera dina kortläsare och smartkort.

1. Högerklicka på ikonen  och välj **Starta Client Manager**. Fönstret DigiSign Client Manager öppnas.



2. Du får fram informationen om ett kort genom att klicka på den triangel som finns framför varje rad.

Säkerhetsanordningar visar de kortläsare som är kopplade till datorn. Under kortläsaren anges vem som har beviljat kortet, rubriken och serienumret, om denna information finns tillgänglig.

Autentiseringsobjekt visar de sifferkoder som finns på kortet, dvs. PIN-koderna. Varje kort har i allmänhet 2–3 PIN-koder, av vilka den första är bas-PIN-koden som används vid identifiering (PIN 1), den andra är signatur-PIN-koden som används vid signaturer (PIN 2) och den tredje är organisations-PIN-koden (PIN 3).

Authority-certifikat visar vilka av certifikatutfärdarens certifikat som finns på kortet.

Certifikat visar de certifikat som har beviljats kortanvändaren.

Privatnycklar visar de nycklar användaren har på kortet.

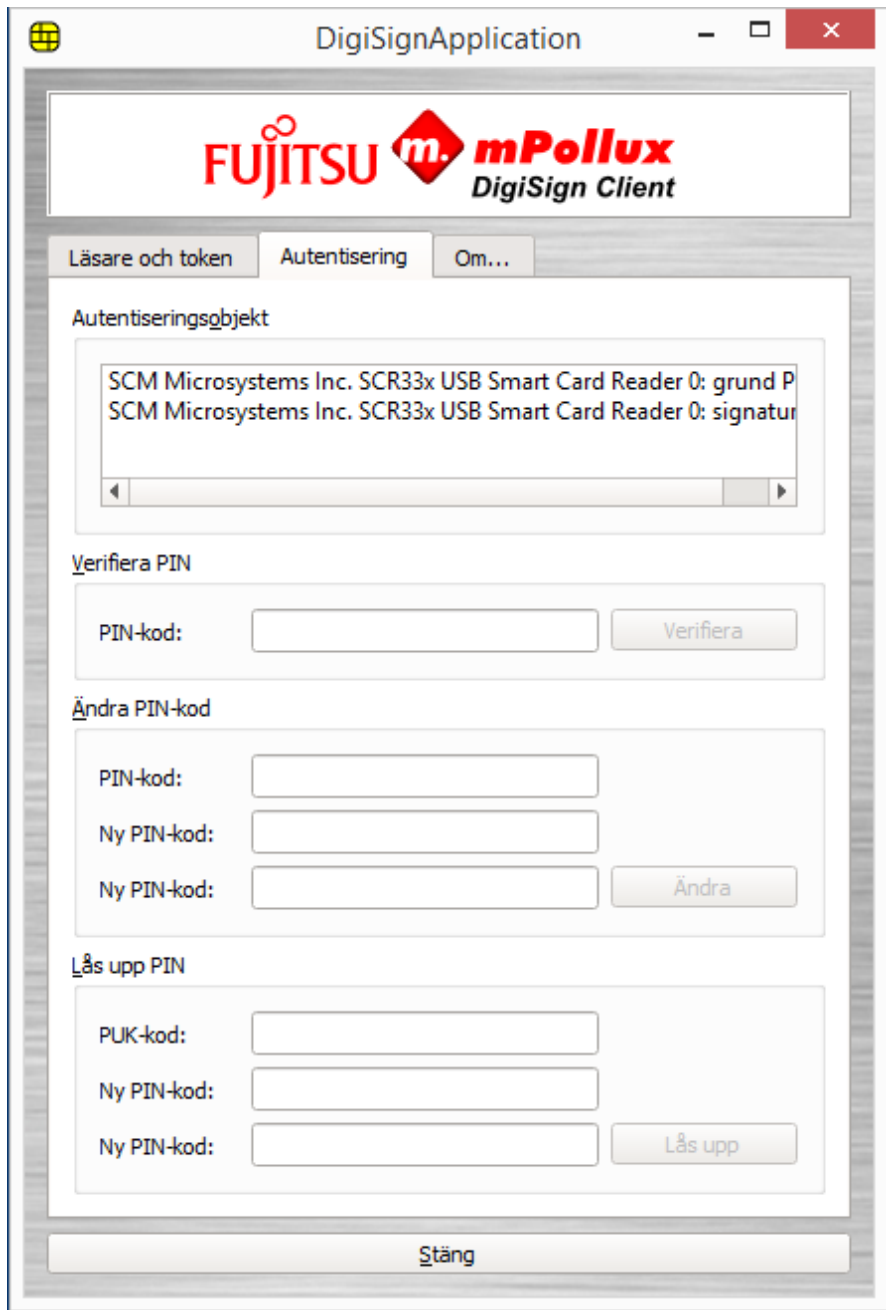
3. Genom att högerklicka på ett certifikat kan du öppna det aktuella certifikatet och kontrollera informationen om detta, till exempel giltighetstiden eller den e-postadress som har anknutits till certifikatet. Du kan även spara certifikatet.
4. Genom att högerklicka på en PIN-kod kan du kontrollera att PIN-koden är korrekt, byta ut den eller låsa upp en låst PIN-kod.

5. Genom att högerklicka på en krypteringsnyckel kan du testa att PIN-koderna fungerar.

3.3 Byta PIN-kod

Om du vill kan du byta ut de PIN-koder du har fått. Du kan byta PIN-kod genom att följa de här anvisningarna eller på fliken **Läsare och token** genom att högerklicka på PIN-koden och välja **Byt**.

1. Högerklicka på ikonen  och välj **Starta Client Manager**. Fönstret DigiSign Client Manager öppnas.
2. Välj fliken **Autentisering**.



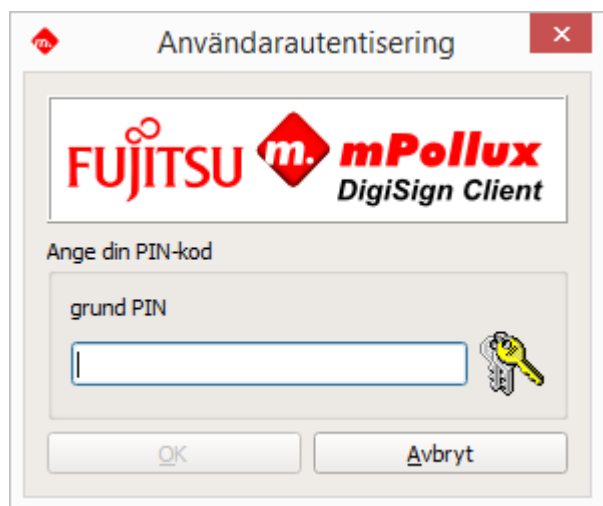
3. Välj vilken PIN-kod du vill byta ut i fältet **Autentiseringsobjekt**.
4. Skriv in den gamla PIN-koden i fältet **Gammal PIN-kod** i avsnittet **Ändra PIN**.
5. Skriv in den nya PIN-koden i fälten **Ny PIN-kod**, som finns nedanför. PIN-koden ska i allmänhet bestå av 4–8 tecken.

6. Klicka på **Ändra**. Du har nu bytt PIN-kod. Memorera den nya PIN-koden eller skriv ner den och förvara den på en säker plats.
7. Klicka på **Stäng** för att avsluta programmet.

3.4 Identifiering i en organisations informationsnätverk

Med hjälp av programvaran DigiSign Client kan du använda ditt smartkort för att logga in i din organisations informationsnätverk. Det måste finnas en anslutning mellan din dator och din organisations informationsnätverk, antingen direkt eller via en VPN-anslutning (virtual private network).

1. Kontrollera att ikonen , som betyder att smartkortet är färdigt att användas, syns på skärmen.
2. Välj inloggningsfunktionen i datorn.
3. Klicka på **OK** om programmet ber dig kontrollera att certifikatet är korrekt. Programmet frågar efter din PIN-kod.



4. Skriv in din bas-PIN-kod i fältet och klicka på **OK**. Du har nu loggat in i din organisations informationsnätverk.
5. Kom ihåg att logga ut och ta smartkortet ur läsaren när du avslutar användningen av tjänsten.

3.5 Identifiering i en e-tjänst

Med hjälp av programvaran DigiSign Client kan du använda ditt smartkort för att logga in i olika e-tjänster som kräver identifiering.

1. Kontrollera att ikonen , som betyder att smartkortet är färdigt att användas, syns på skärmen.
2. Välj på tjänstens inloggningssida den knapp eller länk som för dig till den elektroniska identifieringen. Programmet frågar dig vilket certifikat du vill använda.
3. Välj det certifikat som du vill använda för att identifiera dig i den här tjänsten och klicka på **OK**. Programmet frågar efter din PIN-kod.



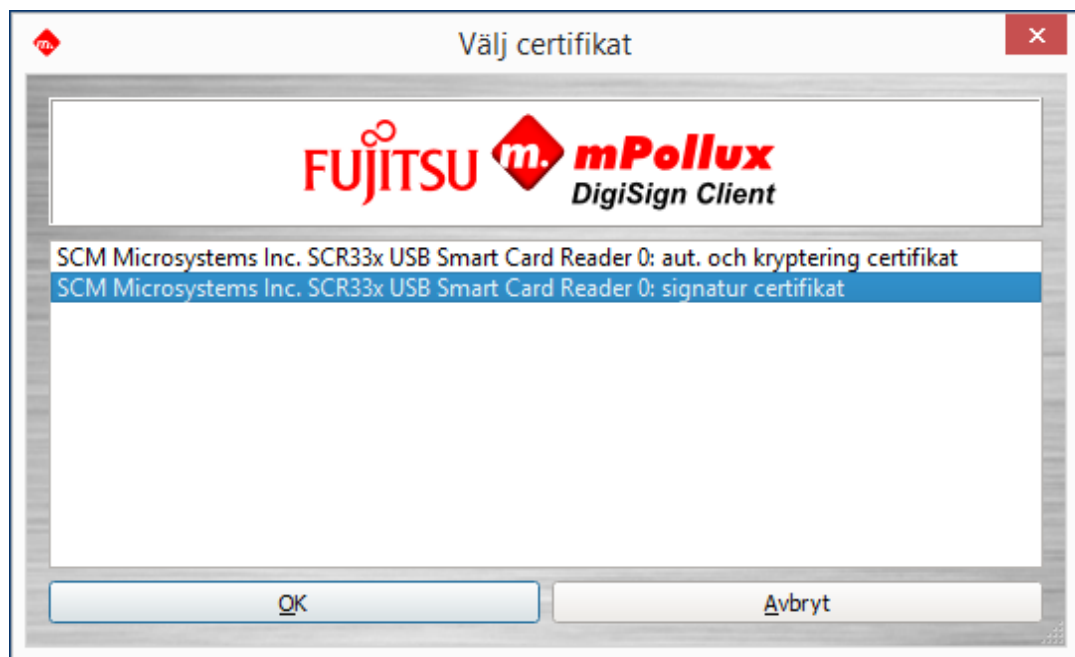
4. Skriv in din PIN-kod och klicka på **OK**.
5. Kom ihåg att logga ut och ta smartkortet ur läsaren när du avslutar användningen av tjänsten.

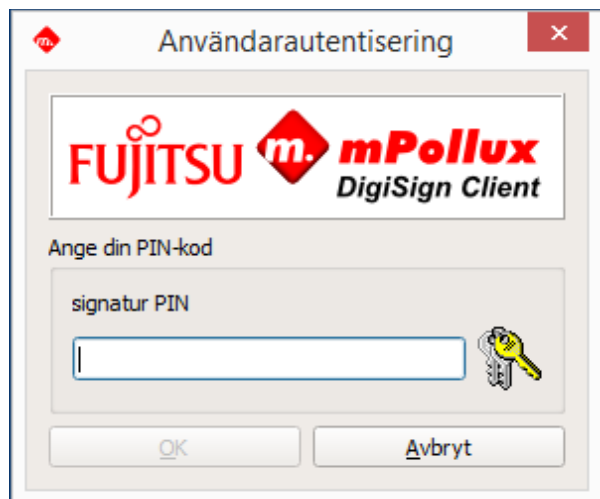
3.6 Elektronisk signering av ett dokument

Med programvaran DigiSign Client kan du skriva under ett elektroniskt dokument eller en elektronisk serviceblankett.

Programmet ber om antingen bas-PIN-koden (PIN 1) eller signatur-PIN-koden (PIN 2) som signatur. Bas-PIN-koden är avsedd för signaturer av engångsnatur i till exempel e-postmeddelanden. Signatur-PIN-koden är avsedd för obestridliga signaturer, dvs. signaturer som har laga kraft, i till exempel avtal.

1. Kontrollera att ikonen , som betyder att smartkortet är färdigt att användas, syns på skärmen.
2. Välj elektronisk signatur i tjänsten eller dokumentet. Programmet frågar efter din PIN-kod.





3. Skriv in din PIN-kod och klicka på OK.

3.7 Signera och kryptera ett e-postmeddelande

Med programvaran DigiSign Client kan du skriva under och kryptera ett e-postmeddelande. Observera att den e-postadress som används i vissa e-postprogram måste finnas sparad i certifikatet.

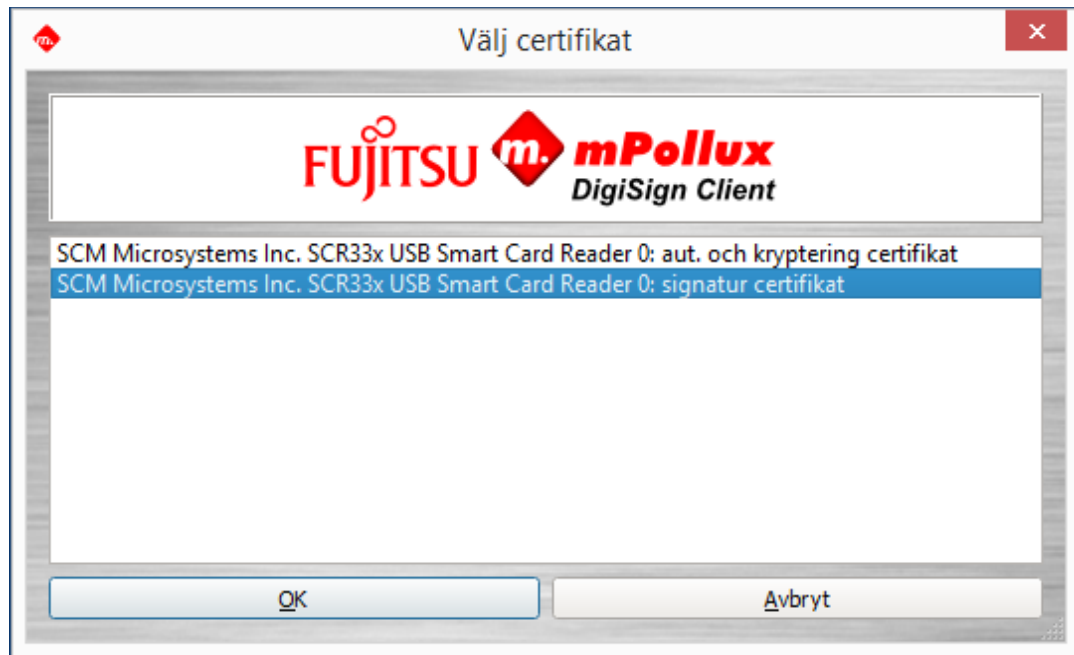
Mottagaren måste också ha ditt certifikat. Du kan överlämna det genom att skicka ett meddelande med en elektronisk underskrift till honom eller henne.

1. Kontrollera att ikonen , som betyder att smartkortet är färdigt att användas, syns på skärmen.
2. Lägg till en elektronisk signatur till e-postmeddelandet och skicka det till mottagaren. Du hittar instruktioner i bruksanvisningen för det program du använder.
3. Mottagaren kan nu skicka ett svar till dig genom att använda certifikatet i meddelandet. Meddelandet skickas i krypterad form.
4. Använd ditt certifikat för att öppna det krypterade meddelandet.

3.8 Lägga till digital signatur i PDF-dokument

Från version 4.1.0 innehåller DigiSign Client möjligheten att lägga till digitala signaturer till PDF-dokument. Så här lägger du till en digital signatur i ett PDF-dokument:

1. Kontrollera att ikonen , som betyder att smartkortet är färdigt att användas, syns på skärmen.
2. Högerklicka på ikonen  och välj "Sign .pdf-document ..."
3. Välj certifikatet du vill använda för digital signering.



4. Välj dokumentet som ska undertecknas och ange PIN-koden om det behövs.
5. Efter framgångsrik signeringsoperation öppnas signerat dokument med standardvisaren för pdf.

4. Problemlösning vid de vanligaste felen

I det här kapitlet finns instruktioner för hur man löser de vanligaste felen. Du får ytterligare råd av certifikatutfärdaren.

4.1 Ikonen för smartkortet syns inte

DigiSign Client startar när datorn startas. När DigiSign Client körs syns en ikon, , på skärmen. Om ikonerna för smartkortet inte finns kan det hända att programmets certifikathämtningstjänst inte är i bruk.

4.2 Programvaran accepterar eller hittar inte kortet

Om ikonerna  visas på skärmen kan programvaran DigiSign Client inte identifiera smartkortet. Kortet kan vara trasigt eller av fel sort. Kontrollera att kortet är avsett för just den tjänst som du vill använda.

Om ikonerna  visas på skärmen kan programvaran DigiSign Client inte hitta smartkortet eller det certifikat som finns på detta. Kontrollera att du har placerat kortet åt rätt håll i kortläsaren och att du har fört det ända in.

Det kan också vara fel på kortläsarens drivrutiner. Uppdatera drivrutinerna enligt de anvisningar som tillverkaren av kortläsaren har gett.

Kortet kan även vara smutsigt. Rengör omsorgsfullt chipdelen av kortet och försök igen.

4.3 Ikonen ändras inte fast jag tar bort kortet ur läsaren

Om ikonerna  inte ändras fast du tar bort kortet ur kortläsaren fungerar kortläsarens drivrutiner inte som de ska. Uppdatera drivrutinerna enligt de anvisningar som tillverkaren av kortläsaren har gett.

4.4 Användarcertifikatet finns inte

DigiSign-säkerhetsmodulen måste hämtas till webbläsaren före användningen. Innan du har gjort detta påstår webbplatsen att det inte finns något användarcertifikat. Hämta säkerhetsmodulen enligt anvisningarna i kapitel 2.5.1 Lägga till en säkerhetsmodul.

Samma felmeddelande visas om smartkortet inte finns i kortläsaren när du försöker använda tjänsten.

4.5 Webbläsaren påstår att anslutningen inte är tillförlitlig

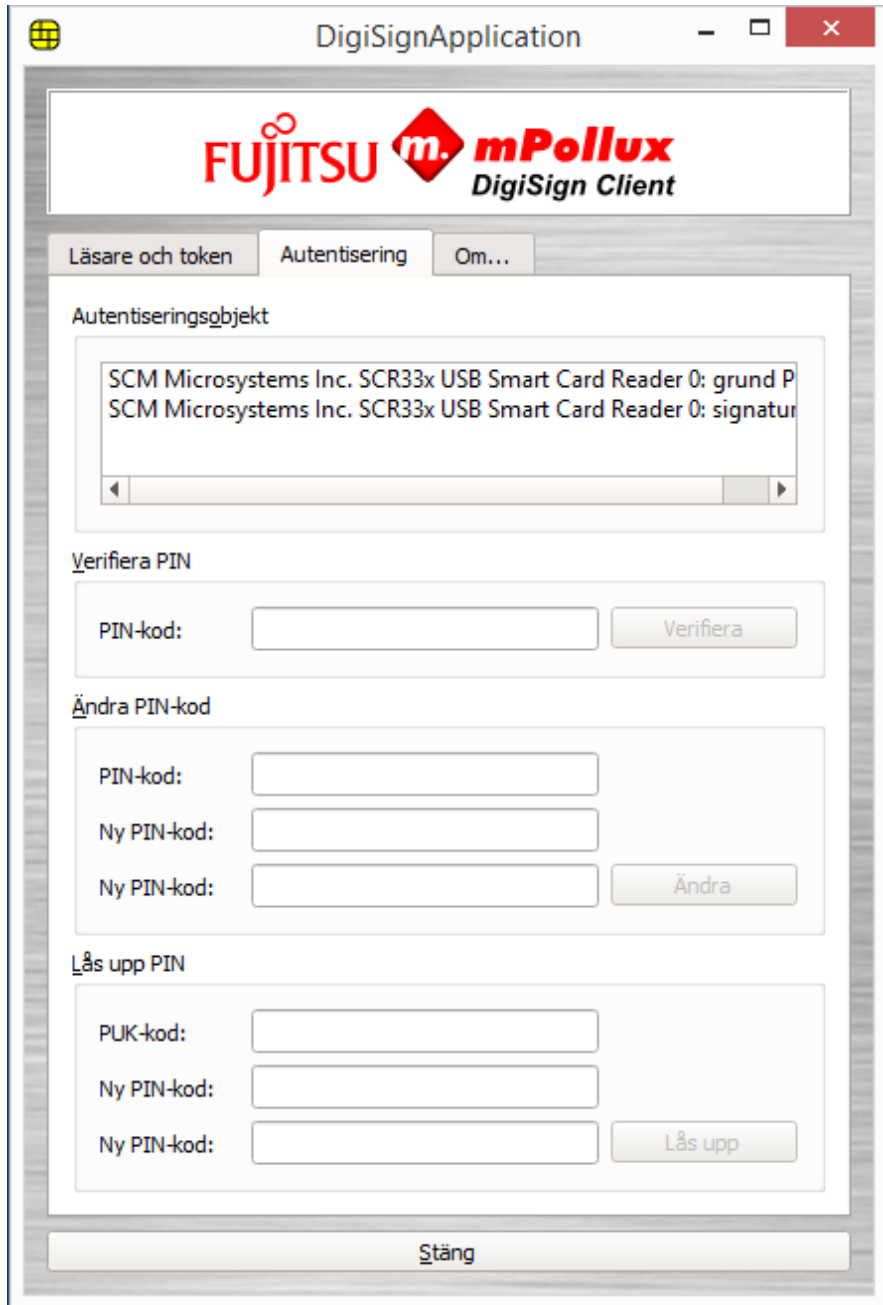
Certifikatutfärdarens offentliga certifikat måste anges som tillförlitliga före användningen. Innan du har gjort detta påstår webbläsaren att anslutningen inte är tillförlitlig.

Hämta certifikatet till webbläsaren enligt anvisningarna i kapitel 2.5.2 Hämta certifikat till webbläsaren.

4.6 PIN-koden (sifferkoden) har låsts

Om du anger fel PIN-kod tillräckligt många gånger låser programmet den. För att låsa upp koden behöver du en upplåsningskod, dvs. en PUK-kod. Om du inte har någon PUK-kod kan du beställa en av den som har beviljat kortet. Med det nya identitetskortet följer ett brev med en aktiveringskod. Om pinkoden av någon orsak låser sig kan den aktiveras på nytt med aktiveringskoden som nämns i brevet.

1. Högerklicka på ikonen  och välj **Starta Client Manager**.
2. Välj fliken **Autentisering**.



The screenshot shows the 'DigiSignApplication' window with the 'Autentisering' tab selected. The window has a title bar with standard Linux window controls. Below the title bar is a header area with the 'FUJITSU mPollux DigiSign Client' logo. The main content area is divided into three sections: 'Läsare och token', 'Autentisering', and 'Om...'. The 'Autentisering' section contains three sub-sections: 'Autentiseringsobjekt' with a list box showing two entries for 'SCM Microsystems Inc. SCR33x USB Smart Card Reader 0'; 'Verifiera PIN' with a 'PIN-kod' input field and a 'Verifiera' button; and 'Ändra PIN-kod' with three input fields for 'PIN-kod', 'Ny PIN-kod', and 'Ny PIN-kod', and an 'Ändra' button. Below these is the 'Lås upp PIN' section with three input fields for 'PUK-kod', 'Ny PIN-kod', and 'Ny PIN-kod', and a 'Lås upp' button. At the bottom of the window is a 'Stäng' button.

3. Välj den låsta PIN-koden i fältet **Autentiseringsobjekt**.
Om du har flera PIN-koder och inte är säker på vilken av dem som är låst kan du kontrollera saken på följande sätt:
 - a) Välj den första PIN-koden i fältet **Autentiseringsobjekt**.
 - b) Skriv in PIN-koden i fältet **PIN-kod** i avsnittet **Verifiera PIN** och klicka på **Verifiera**.
 - c) Om PIN-koden är låst visar programvaran meddelandet "PIN-koden är låst".
 - d) Om PIN-koden du valde inte är låst fortsätter du med att kontrollera nästa PIN-kod.
4. Kontrollera att du har valt den låsta PIN-koden i fältet **Autentiseringsobjekt**. Skriv in din PUK-kod i fältet **PUK-kod** i avsnittet **Lås upp PIN**.

Om du anger fel PUK-kod tillräckligt många gånger i rad låses kortet permanent. Det exakta antalet gånger beror på kortet.

5. Skriv in en ny PIN-kod i fälten **Ny PIN-kod**.
6. Klicka på **Lås upp**. Programvaran meddelar att "PIN-koden har låsts upp och ändrats". Memorera den nya PIN-koden eller skriv ner den och förvara den på en säker plats.
7. Klicka på **Stäng** för att avsluta programmet.

4.7 Signaturfunktionen fungerar inte i webbläsaren

DigiSign Client använder en intern internetserver för elektroniska signaturer. Vissa brandmurar förhindrar att en server av detta slag används i datorn. Kontrollera inställningarna för brandmuren om signaturer inte fungerar i webbläsaren.

1. Kontrollera att ikonen , som betyder att smartkortet är färdigt att användas, syns på skärmen.
2. Gå till adressen <https://127.0.0.1:53952> Sidan påstår att anslutningen inte är tillförlitlig. Hämta certifikatet till webbläsaren enligt anvisningarna i kapitel 2.5.2 Hämta certifikat till webbläsaren.

