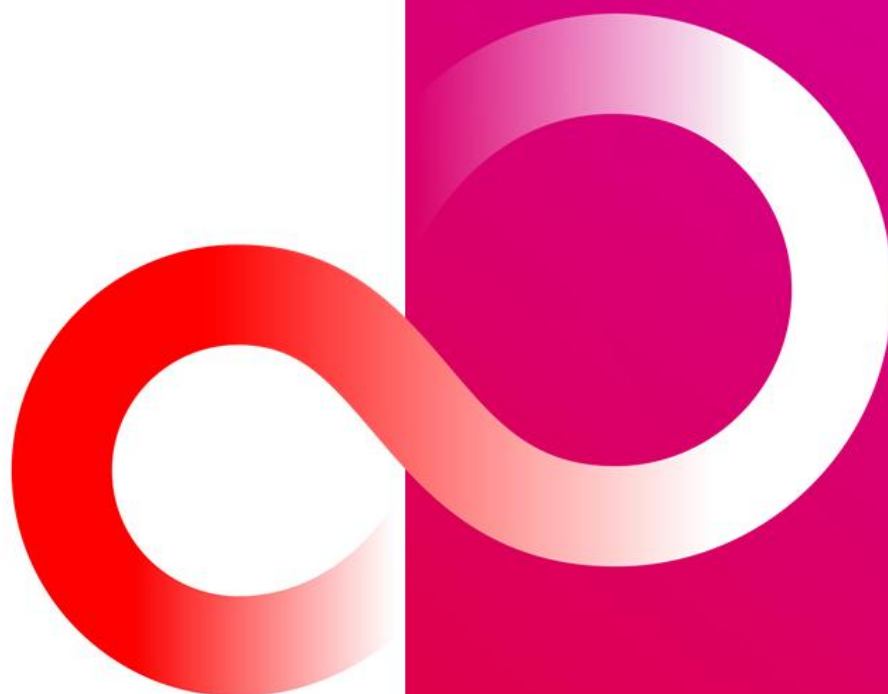


Loppukäyttäjän ohje Asennus- ja käyttöohje – Linux

V4.4.0

FUJITSU



FUJITSU  **mPollux**
DigiSign Client

Contents

1. DigiSign Client -kortinlukijaohjelmisto	4
1.1 Käytön edellytykset.....	4
1.2 Tuetut käyttöjärjestelmät.....	4
1.3 Käyttöohjeet.....	4
2. DigiSign Client -ohjelmiston asentaminen	5
2.1 Aikaisempien kortinlukijaohjelmistojen ja versioiden poistaminen	5
2.2 Ohjelmiston asentaminen	5
2.2.1 Vaatimukset	5
2.2.2 Asentaminen SuSE Linux Enterprise Desktop -ympäristössä	5
2.2.3 Asentaminen Red Hat Enterprise Linux -ympäristössä	6
2.2.4 Asentaminen Ubuntu-ympäristössä.....	6
2.2.5 DigiSign PKCS#11 Moduulin asentaminen.....	7
2.3 Uuden kortin aktivointi.....	8
2.4 Ohjelmiston toiminnan varmistaminen.....	8
2.5 Selain- ja sähköpostiohjelmien asetukset.....	9
2.5.1 Turvallisuusmoduulin lataaminen.....	10
2.5.2 Varmenteiden lataaminen selaimen.....	11
2.5.3 Varmenteiden lataaminen sähköpostiohjelmaan	14
3. DigiSign Client -ohjelmiston käyttäminen.....	15
3.1 Käytön aloittaminen	15
3.2 Kortinlukijan ja korttien hallinta	15
3.3 Tunnusluvun vaihtaminen.....	17
3.4 Tunnistautuminen organisaation tietoverkkoon	18
3.5 Tunnistautuminen sähköiseen asiointipalveluun.....	18
3.6 Asiakirjan allekirjoittaminen sähköisesti.....	19
3.7 Sähköpostiviestin allekirjoittaminen ja salaaminen.....	20
3.8 PDF-dokumentin allekirjoittaminen	20
4. Yleisimmistä virhetilanteista selviytyminen.....	22
4.1 Älykortin kuvaketta ei näy.....	22
4.2 Ohjelmisto ei hyväksy tai löydä korttia	22
4.3 Kortin ottaminen pois lukijasta ei muuta kuvaketta	22
4.4 Käyttäjävarmennetta ei löydy	22

4.5 Selain väittää, että yhteys ei ole luotettu22

4.6 PIN-koodi (tunnusluku) on lukkiutunut22

4.7 Allekirjoitustoiminto ei toimi selaimessa.....24

1. DigiSign Client -kortinlukijaohjelmisto

Fujitsun mPollux DigiSign Client -ohjelmistolla voit käyttää sähköisiä asiointipalveluita tai organisaation tietoverkkoa turvallisesti ja luotettavasti älykortin avulla. Ohjelmisto lukee sinulle myönnetylle älykortille tallennetut varmenteet ja varmistaa henkilöllisyytesi palvelun tarjoajalle.

DigiSign Client -ohjelmistoa tarvitset, kun haluat

- kirjautua sähköiseen asiointipalveluun joka vaatii tunnistautumista
- kirjautua organisaation tietoverkkoon joko suoraan tai organisaation ulkopuolisesta verkosta vpn-yhteyden (virtual private network) avulla
- allekirjoittaa asiakirjan sähköisesti
- allekirjoittaa tai salata sähköpostiviestin.

1.1 Käytön edellytykset

DigiSign Client -ohjelmiston lisäksi tarvitset

- sirullisen älykortin, esimerkiksi sähköisen henkilökortin tai organisaatiokortin
- kortin mukana tulevat tunnusluvut eli PIN-koodit
- kortinlukijan.

1.2 Tuetut käyttöjärjestelmät

Tuetut käyttöjärjestelmät on luetteloitu "Technical References" dokumentaatioissa.

1.3 Käyttöohjeet

Ohjelmiston mukana toimitetaan seuraavat käyttöohjeet:

- Fujitsu mPollux DigiSign Client asennus- ja käyttöohje – Linux (nämä ohjeet)
- Fujitsu mPollux DigiSign Client asennus- ja käyttöohje – Windows
- Fujitsu mPollux DigiSign Client asennus- ja käyttöohje – Mac OS
- Fujitsu mPollux DigiSign Client Technical References

2. DigiSign Client -ohjelmiston asentaminen

DigiSign Client -ohjelmiston asentaminen tai päivittäminen edellyttää, että tietokoneelle ei ole asennettu muita kortinlukijaohjelmistoja tai DigiSign Client -ohjelmiston aikaisempia versioita.

2.1 Aikaisempien kortinlukijaohjelmistojen ja versioiden poistaminen

Varmista ennen asentamista, että koneessasi ei ole muita kortinlukijaohjelmistoja tai vanhaa versiota DigiSign-ohjelmistosta.

1. Tarkista, ettei tietokoneelle ole asennettu muita kortinlukijaohjelmistoja. Jos koneelta löytyy jokin muu kortinlukijaohjelmisto, poista se ohjelmiston ohjeiden mukaisesti.
2. Jos tietokoneeltasi löytyy DigiSign-ohjelmiston vanhempi versio, poista ohjelmisto seuraavalla komennolla:
 - SUSE- ja Red Hat -ympäristöissä:
`# sudo rpm -e <DigiSign-asennusmoduulin nimi>`
 - Ubuntu-ympäristössä:
`# dpkg -r <DigiSign-asennusmoduulin nimi>`

2.2 Ohjelmiston asentaminen

DigiSign Client -asennustiedoston saat kortin toimittajalta tai järjestelmän ylläpitäjältä. Tallenna asennustiedosto tietokoneellesi.

Teknisiä yksityiskohtia luotettujen varmenteiden asentamisesta löytyy "DigiSign Client Technical References"-dokumentin kappaleesta "Notes for Linux users".

2.2.1 Vaatimukset

Ohjelmiston asentaminen vaatii juurioikeudet tietokoneeseen.

Ennen varsinaisen DigiSign Client -ohjelmiston asennuksen aloittamista koneessa täytyy olla PCSC-Lite -ohjelmistopakkaus asennettuna ja PCSC-Lite daemon (pcscd) käynnistettynä.

mPollux DigiSign Client -ohjelmisto vaatii myös oikean ajurin älykortin lukijaa varten. Oikea ajuri löytyy laitteen valmistajan kotisivuilta tai voit kokeilla, toimiiko lukijalle geneerinen USB CCID (Chip/Smart Card Interface Devices) -ajuri. Voit hakea ajuria hakusanalla "pcsc-ccid" osoitteessa <http://rpm.pbone.net/>. Pakkaus sisältää geneerisen ajurin sekä ajurin sarjamuotoiselle GemPC Twin -lukijalle. Nämä ajurit on tarkoitettu käytettäväksi PCSC-Lite -ohjelmistopaketin PCSC-Lite daemon -ohjelman kanssa.

2.2.2 Asentaminen SuSE Linux Enterprise Desktop -ympäristössä

Tässä ohjeessa kerrotaan, kuinka mPollux DigiSign Client -ohjelmisto asennetaan SuSE Linux Enterprise Desktop -ympäristössä. Jos haluat graafisen käyttöliittymän, voit käyttää YaST2 Package Manager -ohjelmistoa.

1. Kun näyttöön ilmestyy komennon kehote, asenna ohjelmisto antamalla seuraava komento:
`# sudo rpm -Uvh <DigiSign-asennusmoduuli>.rpm`
2. RPM-pakkaukset saattavat joskus olla riippuvaisia muista pakkauksista. Jos jokin tarvittava pakkaus puuttuu, näkyviin tulee seuraavantyyppinen sanoma:
`error: Failed dependencies:
libpcsc-lite.so.1 is needed by <DigiSign-asennusmoduuli>`

Hae puuttuvat pakkaukset internetistä tai SuSE-asennuslevyltä ja lisää ne komentoon. Esimerkiksi:

```
# rpm -ivh pcsc-lite-<versio>.rpm <DigiSign-asennusmoduuli>.rpm
```

3. Kun asennus on suoritettu, tee tarvittavat asetukset selaimeen ja sähköpostiohjelmaan kappaleen 2.55 Selain- ja sähköpostiohjelmien asetukset ohjeiden mukaisesti.
4. Tarkista, että PC/SC Smart Card Daemon (pcscd) käynnistyy automaattisesti aina koneen käynnistytyn yhteydessä.
 - Avaa YaST > System > System Services.
 - Tarkista, että pcscd on määritetty ajettavaksi init 5 -tasolla.

2.2.3 Asentaminen Red Hat Enterprise Linux -ympäristössä

Tässä ohjeessa kerrotaan, kuinka DigiSign Client -ohjelmisto asennetaan Red Hat Linux Enterprise -ympäristössä. Jos haluat graafisen käyttöliittymän, voit käyttää Package Management Tool -työkalua.

1. Kun näyttöön ilmestyy komennon kehote, asenna ohjelmisto antamalla seuraava komento:

```
# sudo yum localinstall <DigiSign-asennusmoduuli>.rpm
```
2. Tarkista, että PC/SC Smart Card Daemon (pcscd) käynnistyy automaattisesti aina koneen käynnistytyn yhteydessä käyttöjärjestelmäversiosta riippuen esimerkiksi Service -työkalulla antamalla seuraava komento komentoriviltä:

```
# service pcscd status
```

 - Tarkista, että pcscd on määritetty ajettavaksi init 5 -tasolla (graafinen monenkäyttäjänympäristö).
 - Käytä RHEL/CentOS 7.x/8.x:ssä systemctl:ää tarkistaaksesi, onko pcscd-palvelu käynnistetty

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

RHEL 7 versiossa Linuxin systemd huolehtii pcscd prosessing käynnistyksestä tarvittaessa. Tämä voi kuitenkin edellyttää tietokoneen uudelleenkäynnistystä DigiSign Client -asennuksen jälkeen.

3. Kun asennus on suoritettu, tee tarvittavat asetukset selaimeen ja sähköpostiohjelmaan kappaleen 2.55 Selain- ja sähköpostiohjelmien asetukset ohjeiden mukaisesti.

2.2.4 Asentaminen Ubuntu-ympäristössä

Tässä ohjeessa kerrotaan, kuinka DigiSign Client -ohjelmisto asennetaan Ubuntu -ympäristössä. Jos haluat graafisen käyttöliittymän, voit käyttää Synaptic Package Manager -ohjelmistoa, joka tarjoaa samat toiminnot kuin apt-get.

1. Asenna DigiSign-Client apt-get-apuohjelmalla komentoriviltä. Anna asennuspaketin koko polku, jotta apt-get voi ratkaista kaikki asennuspaketin riippuvuudet:

```
# sudo apt-get install <DigiSign installation module>.deb
```
2. Käytä Advanced Packaging Tool -työkalua (apt) ja asenna puuttuva paketti. Lisää se komentoon:

```
# sudo apt-get install pcscd
```
3. Kun asennus on suoritettu, tee tarvittavat asetukset selaimeen ja sähköpostiohjelmaan kappaleen 2.55 Selain- ja sähköpostiohjelmien asetukset ohjeiden mukaisesti.
4. Tarkista, että PC/SC Smart Card Daemon (pcscd) käynnistyy automaattisesti aina koneen käynnistytyn yhteydessä.
 - a) Anna seuraava komento komentoriviltä:

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

`pcsd.socket` palvelu laukaisee `pcsd`-palvelun ja sen pitäisi olla `enabled` tilassa.

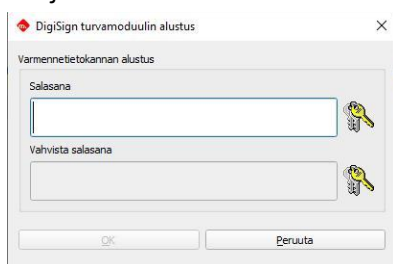
b) Anna seuraava komento komentoriviltä jos `pcsd.socket` palvelu on `disabled` tilassa:

```
# systemctl enable pcsd.socket
```

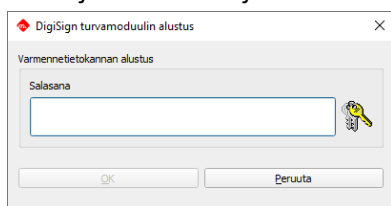
2.2.5 DigiSign PKCS#11 Moduulin asentaminen

Jotta älykorttitoiminnallisuus toimisi selainten ja muiden sovellusten kanssa, PKCS#11-moduuli ja DigiSign-sertifikaatti on lisättävä paikalliseen suojaustietokantaan. Useimmissa tapauksissa tämä tapahtuu automaattisesti, kun DigiSign-sovellus käynnistetään ensimmäisen kerran. Käyttäjää pyydetään antamaan salasana joko uuden suojaustietokannan luomiseksi tai olemassa olevan tietokannan käyttämiseksi seuraavasti;

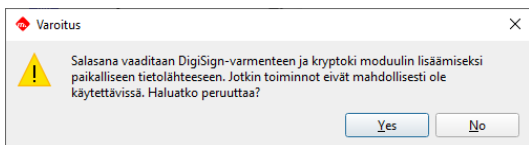
a) Suojaustietokantaa ei ole olemassa, joten käyttäjältä pyydetään salasanaa uuden suojaustietokannan Luomiseksi



b) Suojaustietokanta on jo määritetty. Käyttäjältä kysytään salasanaa, jotta asentaja voi lisätä siihen uuden suojausmoduulin ja varmenteen



Seuraava varoitussikkuna tulee näkyviin, jos käyttäjä peruuttaa asennuksen. Jos asennusta ei viimeistellä, allekirjoitus-, todennus- ja salaustoiminnot eivät ehkä toimi oikein.



Tyypillisissä tapauksissa salasanaa kysytään vain kerran silloin kun DigiSign-sovellus käynnistetään ensimmäisen kerran.

Jos jokin menee pieleen, suojaustietokanta voidaan rakentaa uudelleen seuraavasti;

- Poista `~/digisign` folder
- Varmuuskopioi `./pki/nssdb` folder
- Poista `./pki/nssdb` folder
- Uudelleenkäynnistä DigiSign Application

Lisätietoja selainten ja sähköpostiohjelmien käytöstä kappaleessa "2.5 Selain- ja sähköpostiohjelmien asetukset".

2.3 Uuden kortin aktivointi

Uusi kortti saattaa käyttöönotettaessa vaatia aktivoinnin. Kun henkilökorttia käytetään ensimmäisen kerran, käynnistetään kortinlukijaohjelmiston toimesta automaattisesti henkilökortin aktivointiprosessi. Tämän prosessin aikana käyttäjältä ensin kysytään aktivointitunnusluku, jonka jälkeen käyttäjä voi aktivoida ja määritellä omat, henkilökohtaiset PIN-tunnuslukunsa. Aktivointiprosessin jälkeen käyttäjä pystyy käyttämään henkilökorttiaan sähköisessä asioinnissa.



Tunnusluvun aktivointi (basic PIN)

Aktivointitunnusluku



Uusi PIN

Vahvista uusi PIN

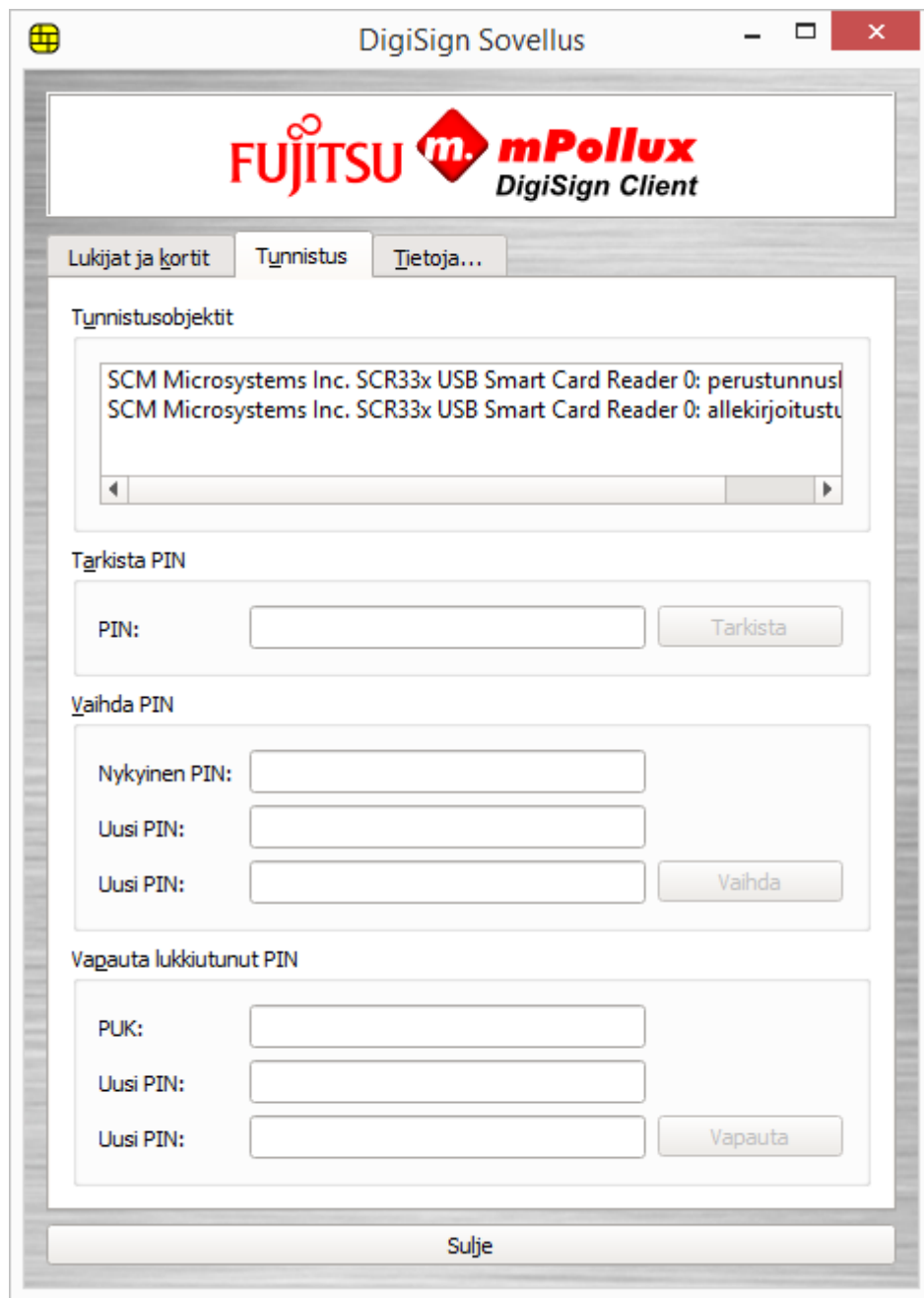
OK Keskeytä

2.4 Ohjelmiston toiminnan varmistaminen

mPollux DigiSign Client Manager -työkalulla voit varmistaa, että ohjelman asennus onnistui, älykortti on ehjä ja kortinlukija toimii.

1. Varmista, että kortinlukija on kiinni tietokoneessa. Kortinlukija voi olla tietokoneen sisällä tai tietokoneessa kiinni kaapelilla.
2. Aseta älykortti kortinlukijaan. Odota, että -kuvake muuttuu keltaiseksi.
3. Napsauta -kuvaketta hiiren oikealla painikkeella, ja valitse **Näytä laitteet**.
4. Valitse **Tunnistus**-välilehti.

Jos käyttämäsi työpöytäympäristö ei tarjoa tehtäväpalkkia kuvakkeille voit joutua asentamaan lisäosan kuten AppIndicator tai TopIcons pystyäksesi hyödyntämään -kuvaketta.



5. Valitse **Tunnistusobjektit**-kentästä ensimmäinen tunnusluku.
6. Anna tunnuslukusi **Tarkista PIN** -osion **PIN**-kenttään, ja valitse **Tarkista**. Ohjelma ilmoittaa, että tunnusluvun tarkistus onnistui. Jos ohjelma ilmoittaa, että tunnusluvun tarkistus epäonnistui, tarkista että syötit tunnusluvun oikein.

Jos annat tunnusluvun tarpeeksi monta kertaa peräkkäin väärin, tunnusluku lukittuu. Tarkka määrä riippuu kortista. Avaa tunnusluku aktivointitunnusluvulla tai PUK-koodin avulla kappaleen 4.6 PIN-koodi (tunnusluku) on lukkiutunut ohjeiden mukaan.




2.5 Selain- ja sähköpostiohjelmien asetukset

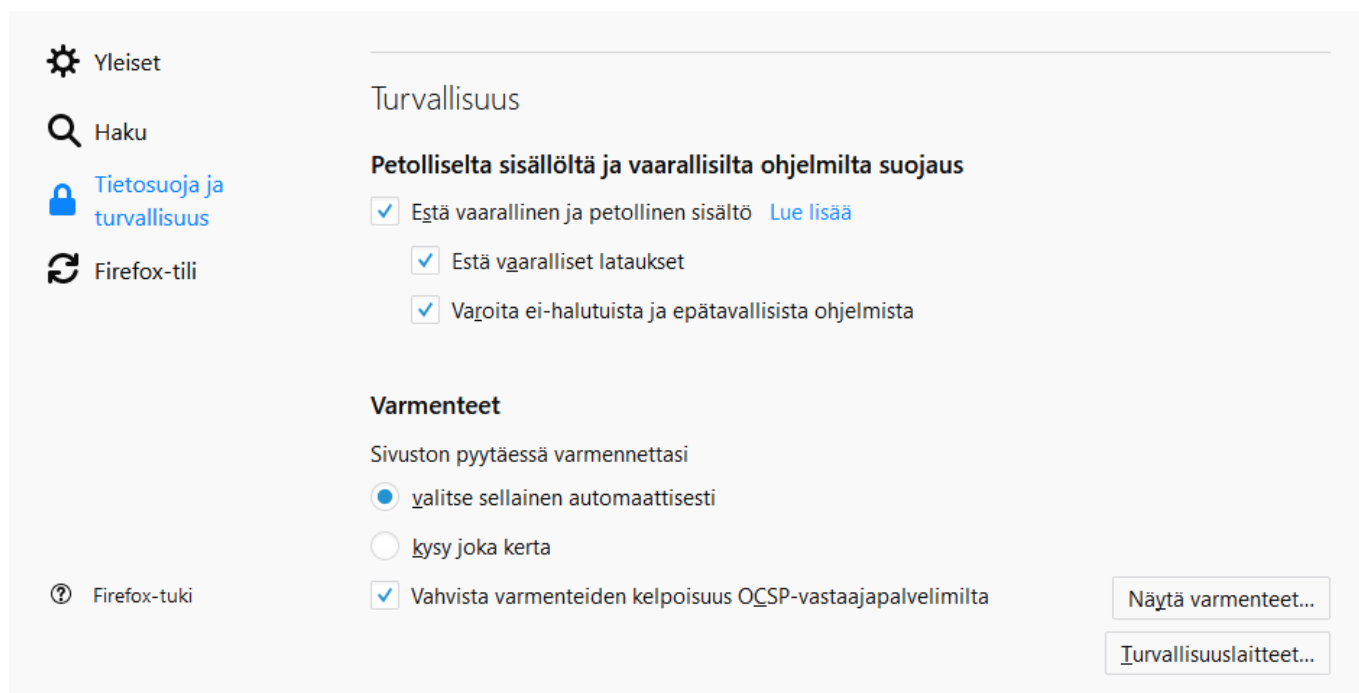
Suurimmassa osassa tapauksista DigiSign Client -ohjelmisto toimii web selaimien ja sähköpostiohjelmien kanssa ilman erityisiä asetuksia. Jos turvallisuusmodulin ja/tai luotetun varmenteen asennus epäonnistui asennuksen yhteydessä, voi asentaa ne Mozilla Firefoxissa ja Thunderbirdissä seuraavasti:

- Ladata DigiSign Client -ohjelmiston käyttämä turvallisuusmoduuli ohjelmaan.
- Ladata varmennuksen myöntäjän julkiset varmenteet ohjelmaan.
 - Ennen luotetun varmenteen lisäämistä selain väittää, että yhteys ei ole luotettu.

2.5.1 Turvallisuusmoduulin lataaminen

Asennuspaketti yrittää ladata turvallisuusmoduulin automaattisesti asennuksen yhteydessä. Jos automaattilataus ei ole onnistunut, kertoo seuraava esimerkki, kuinka turvallisuusmoduuli ladataan Mozilla Firefoxissa ja Mozilla Thunderbirdissa. Muissa ohjelmissa ja eri versioissa asetukset saattavat poiketa ohjeesta.

1. Varmista, että näytössä näkyy -kuvake, joka tarkoittaa, että älykortti on valmis käytettäväksi.
2. Mozilla Firefoxissa asetukset löytyvät  -painike > Asetukset > Tietosuoja ja turvallisuus > Turvallisuus -osion kohta **Varmenteet**. Mozilla Thunderbirdissä asetukset löytyvät  -painike > Asetukset > Asetukset > **Lisäasetukset > Varmenteet**.



Turvallisuus

Petolliselta sisällöltä ja vaarallisilta ohjelmilta suojaus

- ☒ Estä vaarallinen ja petollinen sisältö [Lue lisää](#)
- ☒ Estä vaaralliset lataukset
- ☒ Varoita ei-halutuista ja epätavallisista ohjelmista

Varmenteet

Sivuston pyytäessä varmennettasi

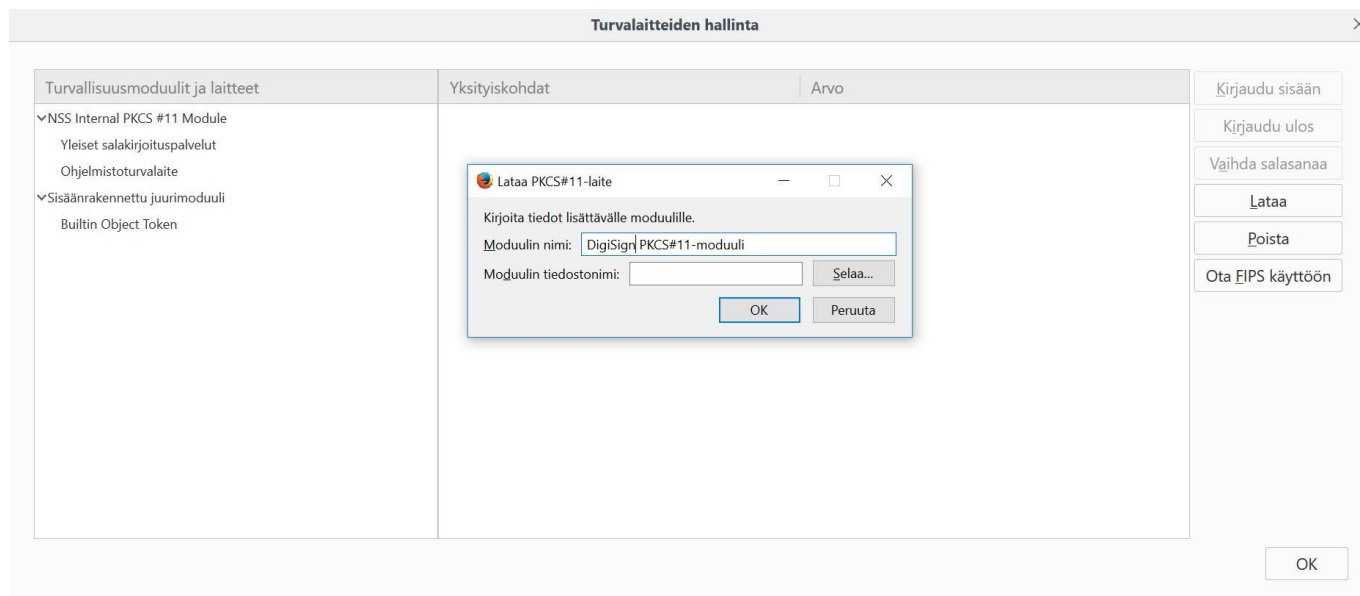
- ☒ valitse sellainen automaattisesti
- ☐ kysy joka kerta

☒ Vahvista varmenteiden kelpoisuus OCSP-vastaajapalvelimilta

[Näytä varmenteet...](#)

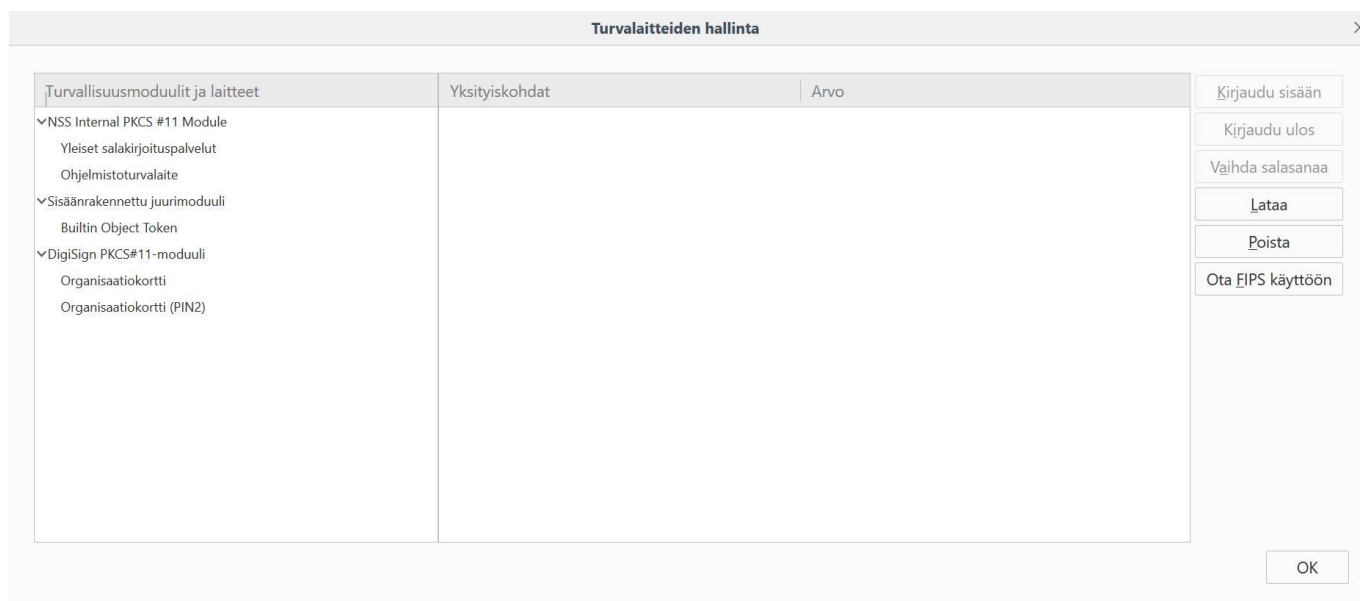
[Turvallisuuslaitteet...](#)

3. Valitse Varmenteet-otsikon alta Valitse sellainen automaattisesti.
4. Valitse Turvallisuuslaitteet ja Lataa.



5. Anna moduulin nimeksi **DigiSign PKCS#11-moduuli**.

6. Paina **Selaa** ja hae koneeltasi `libcryptoki.so`-tiedosto. Se sijaitsee oletusarvoisesti hakemistossa `/usr/lib64/`. Paina **OK**.



Jos saat virheilmoituksen, ettei turvallisuusmoduulia voitu ladata, käynnistä selain uudelleen.

7. DigiSign PKCS#11-moduuli näkyy nyt listalla. Paina **OK** poistuaksesi asetuksista.

8. Käynnistä selain tai sähköpostiohjelma uudestaan.

2.5.2 Varmenteiden lataaminen selaimen

Joissain selaimissa, kuten Mozilla Firefoxissa, varmennuksen myöntäjän julkiset varmenteet tulee määritellä luotetuiksi ennen käyttöä. Ennen kuin tämä on tehty, selain väittää, että yhteys ei ole luotettu.



Yhteys ei ole suojattu

Sivuston vrk.fineid.fi omistaja on määrittänyt sivustonsa asetukset väärin. Firefox ei muodostanut yhteyttä sivustoon suojelemaan tietojasi varkaudelta.


[Lue lisää...](#)

☐

Ilmoita tällaisista virheistä auttaaksesi Mozillaa tunnistamaan ja estämään haitallisia sivustoja

Palaa

Yksityiskohdat

1. Varmista, että näytössä näkyy -kuvake, joka tarkoittaa, että älykortti on valmis käytettäväksi.
2. Valitse **Yksityiskohdat**.

Sivuston vrk.fineid.fi tietoturvakvarmenne ei ole kelvollinen.

Varmenteeseen ei luoteta, koska sen myöntäjän varmenne on tuntematon.
Palvelin ei mahdollisesti lähetä kaikkia asianmukaisia välivaiheen varmenteita.
Voi olla, että täytyy tuoda uusi juurivarmenne.

Virhekoodi: [SEC_ERROR_UNKNOWN_ISSUER](#)

Lisää poikkeus...

3. Paina **Lisää poikkeus**.
4. Lisää turvallisuuspoikkeama -ikkuna avautuu.

Lisää turvallisuuspoikkeus



Olet muuttamassa Firefoxin tapaa tunnistaa tätä sivustoa.

Luotettavat pankit, kaupat ja muut julkiset sivustot eivät pyydä sinua tekemään tätä.

Palvelin

Osoite:

<https://vrk.fineid.fi/>

Lataa varmenne

Varmenteen tila

Sivusto yrittää tunnistaa itseään virheellisillä tiedoilla.

Näytä...

Tuntematon identiteetti



Varmenteeseen ei luoteta, koska yksikään luotettu varmentaja ei todenna sitä suojatulla allekirjoituksella.


☒ Tallenna poikkeus pysyvästi

Vahvista turvallisuuspoikkeus

Peruuta


5. Valitse **Lataa varmenne** ja paina **Vahvista turvallisuuspoikkeus**. Ohjelma pyytää sinua tunnistautumaan.

Käyttäjän tunnistus



Anna PIN-koodi

perustunnusluku





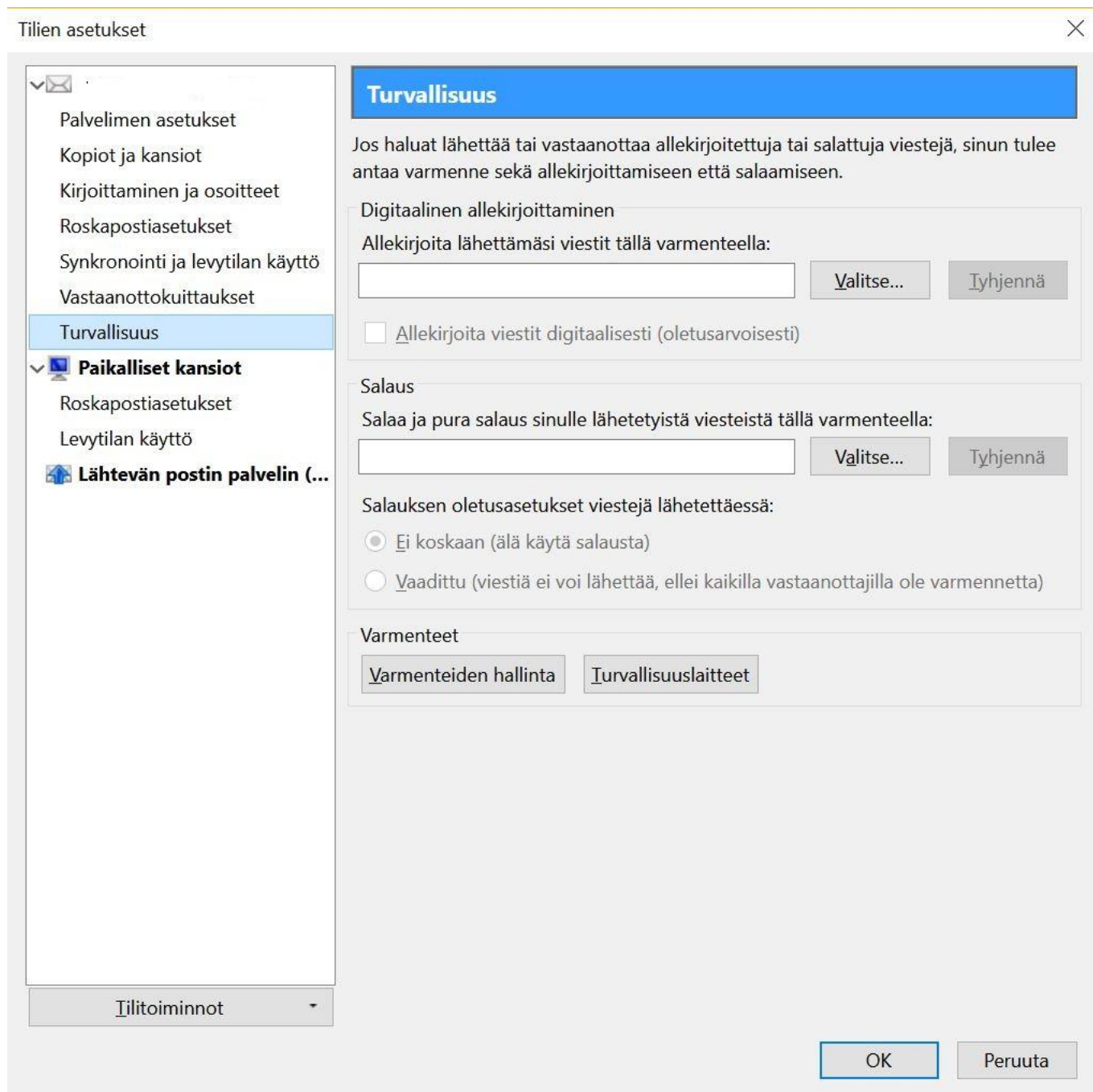
6. Anna tunnuslukusi ja valitse **OK**.

7. Päivitä sivu. Sinun tulisi nyt päästä palveluun.

2.5.3 Varmenteiden lataaminen sähköpostiohjelmaan

Joissain sähköpostiohjelmissa täytyy varmennuksen myöntäjän julkiset varmenteet ladata ohjelmaan ennen kuin niitä voi käyttää. Huomaa, että joissain sähköpostiohjelmissa varmennetta voi käyttää ainoastaan varmenteelle tallennetulle osoitteelle kuuluvan sähköpostilaatikon kanssa.

1. Varmista, että näytössä näkyy -kuvake, joka tarkoittaa, että älykortti on valmis käytettäväksi.
2. Valitse Mozilla Thunderbirdissä  > **Asetukset** > **Tilien asetukset** > **Turvallisuus**.




3. Valitse käyttämäsi allekirjoitus- ja todentamis- ja salausvarmenteet.
4. Valitse OK.

3. DigiSign Client -ohjelmiston käyttäminen

DigiSign Client -ohjelmistoa tarvitset, kun haluat

- kirjautua sähköiseen asiointipalveluun joka vaatii tunnistautumista
- kirjautua organisaation tietoverkkoon joko suoraan tai organisaation ulkopuolisesta verkosta vpn-yhteyden (virtual private network) avulla
- allekirjoittaa asiakirjan sähköisesti
- allekirjoittaa tai salata sähköpostiviestin.

3.1 Käytön aloittaminen

DigiSign Client -ohjelmisto käynnistyy tietokoneen käynnistyessä. Ohjelmiston käyttö edellyttää, että kortinlukija on asetettu tietokoneeseen, kortinlukijan ajurit on asennettu tietokoneeseen ja älykortti on asetettu kortinlukijaan. Varmista aina ennen käyttöä, että tietokoneen näytössä näkyy  -kuvake, joka tarkoittaa, että älykortti on valmis käytettäväksi.

Kun laitat kortin ensimmäistä kertaa lukijaan, saatat saada varoituksen siitä, että varmenne ei ole luotettu. Valitse **Kyllä** jos luotat varmenteeseen.


Jos käytön aikana tulee ongelmia, katso lisäohjeita kappaleesta 4 Yleisimmistä virhetilanteista selviytyminen.

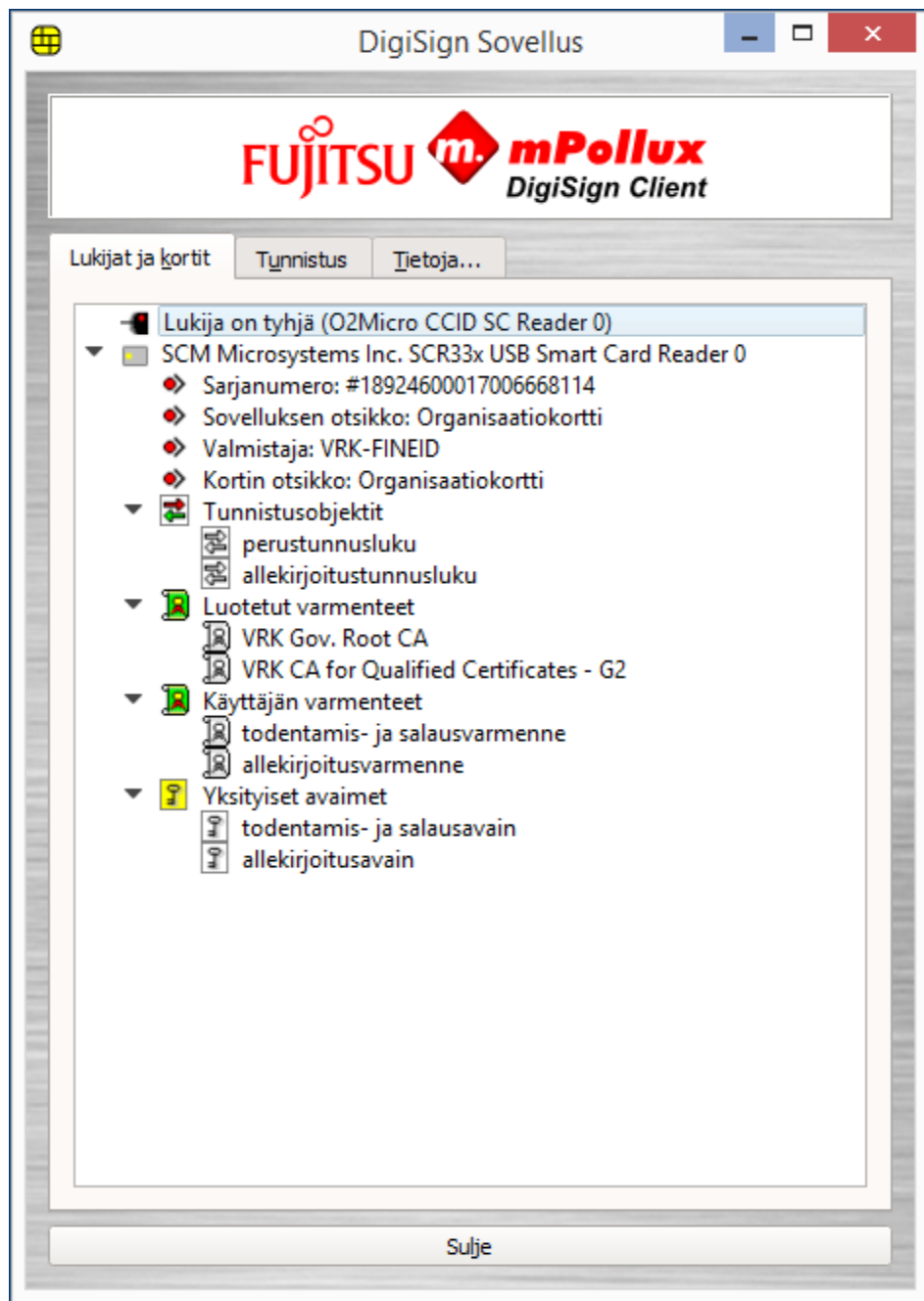
Älä koskaan anna tunnuslukuasi, jos sitä kysytään odottamatta. Varmista, että olet aina itse käynnistänyt tunnuslukua kysyvän toiminnon.

Älä poista korttia kortinlukijasta niin kauan kuin käytät palvelua, johon olet tunnistautunut.

3.2 Kortinlukijan ja korttien hallinta

DigiSign Client -työkalulla voit hallita kortinlukijoitasi ja älykorttejasi.

1. Napsauta  -kuvaketta hiiren oikealla painikkeella, ja valitse **Näytä laitteet**. DigiSign Client Manager -ikkuna avautuu.



2. Saat kortin tiedot näkyviin napsauttamalla kunkin rivin edessä olevaa kolmiota.

Turvalaskentalaitteet näyttävät koneessa kiinni olevat kortinlukijat. Kortinlukijan alla kerrotaan kortin myöntäjä, otsikko ja sarjanumero, jos nämä tiedot ovat saatavilla.

Tunnistusobjektit näyttävät kortilla olevat tunnusluvut eli PIN-koodit. Kullakin kortilla on yleensä 2-3 tunnuslukua, joista ensimmäinen on tunnistautumisessa käytettävä perustunnusluku (PIN 1), toinen allekirjoituksessa käytettävä allekirjoitustunnusluku (PIN 2) ja kolmas organisaatiotunnusluku (PIN 3).

Luotetut varmenteet näyttävät kortilla olevat varmentajan varmenteet.


Käyttäjän varmenteet näyttävät kortin käyttäjälle myönnetty varmenteet

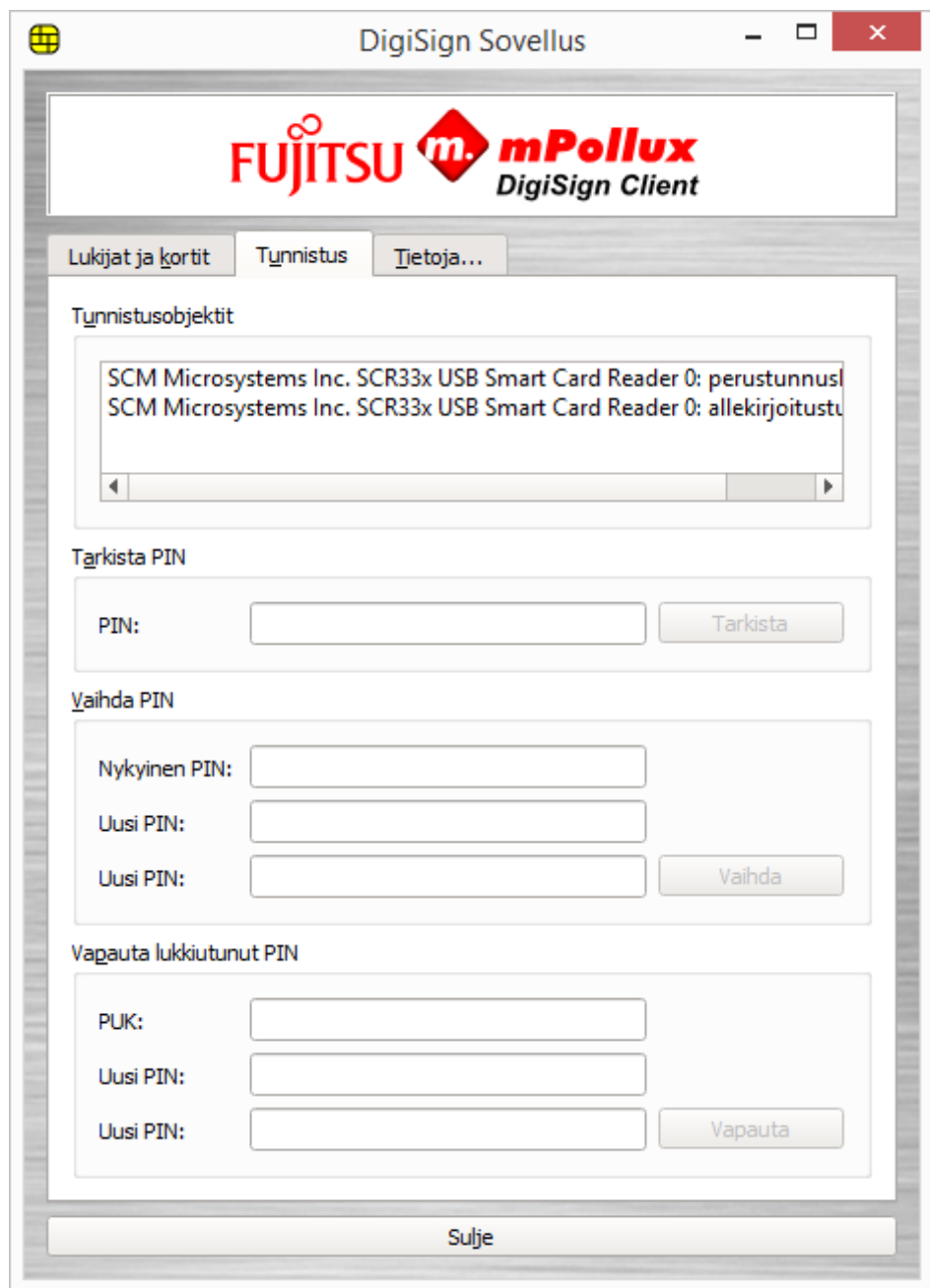
Yksityiset avaimet näyttävät kortilla olevat käyttäjän avaimet.

3. Napsauttamalla varmennetta hiiren oikealla painikkeella voit avata varmenteen ja tarkistaa sen tiedot, kuten voimassaoloajan tai sen sähköpostiosoitteen, joka varmenteeseen on liitetty. Voit myös tallentaa varmenteen.
4. Napsauttamalla tunnuslukua hiiren oikealla painikkeella voit tarkistaa tunnusluvun oikeellisuuden, vaihtaa sen tai avata lukitun tunnusluvun.
5. Napsauttamalla salausavainta hiiren oikealla painikkeella voit testata tunnuslukujen toimivuuden.

3.3 Tunnusluvun vaihtaminen

Voit halutessasi vaihtaa sinulle annetut tunnusluvut. Tässä kuvattujen ohjeiden lisäksi tunnusluvun voi myös vaihtaa **Lukijat ja kortit** -välilehdeltä napsauttamalla tunnuslukua hiiren oikealla painikkeella ja valitsemalla **Vaihda**.


1. Napsauta -kuvaketta hiiren oikealla painikkeella, ja valitse **Näytä laitteet**. DigiSign Client Manager -ikkuna avautuu.
2. Valitse **Tunnistus**-välilehti.

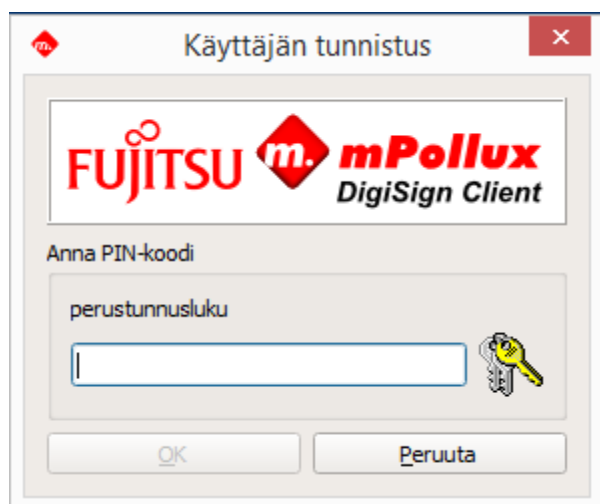


3. Valitse **Tunnistusobjektit**-kentästä se tunnusluku (pin-koodi), jonka haluat vaihtaa.
4. Anna vanha tunnusluku **Vaihda PIN** -osiossa olevaan **Vanha PIN** -kenttään.
5. Anna uusi tunnusluku sen alla oleviin **Uusi PIN** -kenttiin. Tunnusluvussa tulee yleensä olla 4-8 merkkiä.
6. Valitse **Vaihda**. Tunnuslukusi on nyt vaihdettu. Paina uusi tunnusluku muistiin tai kirjoita se ylös ja säilytä turvallisessa paikassa.
7. Valitse **Sulje** poistuaksesi ohjelmasta.

3.4 Tunnistautuminen organisaation tietoverkkoon

DigiSign Client -ohjelmiston avulla voit kirjautua älykortillasi organisaatiosi tietoverkkoon. Koneesi tulee olla yhteydessä organisaatiosi tietoverkkoon joko suoraan tai vpn-yhteyden (virtual private network) kautta.


1. Varmista, että näytössä näkyy  -kuvake, joka tarkoittaa, että älykortti on valmis käytettäväksi.
2. Valitse koneelta kirjautumisen toiminto.
3. Jos ohjelma pyytää sinua varmistamaan varmenteen oikeellisuuden, valitse **OK**. Ohjelma kysyy tunnuslukuasi.

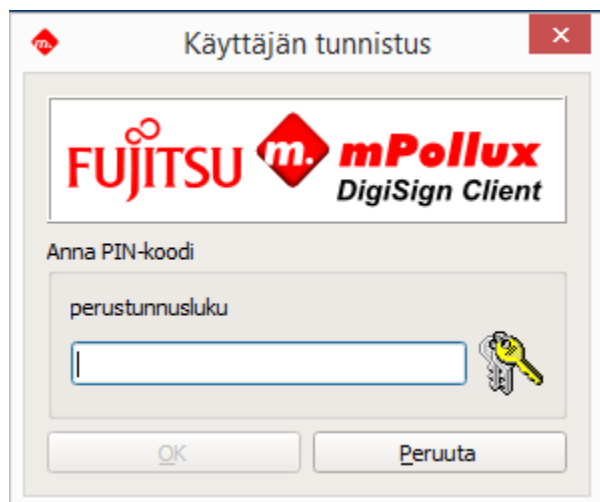


4. Kirjoita perustunnuslukusi kenttään ja valitse **OK**. Olet nyt kirjautunut organisaatiosi tietoverkkoon.
5. Kun lopetat palvelun käytön, muista kirjautua ulos ja poistaa älykortti lukijasta.

3.5 Tunnistautuminen sähköiseen asiointipalveluun

DigiSign Client -ohjelmiston avulla voit kirjautua älykortillasi erilaisiin sähköisiin asiointipalveluihin jotka vaativat tunnistautumista.

1. Varmista, että näytössä näkyy  -kuvake, joka tarkoittaa, että älykortti on valmis käytettäväksi.
2. Valitse palvelun kirjautumissivulla painike tai linkki, joka vie sähköiseen tunnistautumiseen. Ohjelma kysyy sinulta, mitä varmennetta haluat käyttää.
3. Valitse varmenteista se, jota haluat käyttää tähän palveluun tunnistautumiseen, ja valitse **OK**. Ohjelma kysyy tunnuslukuasi.




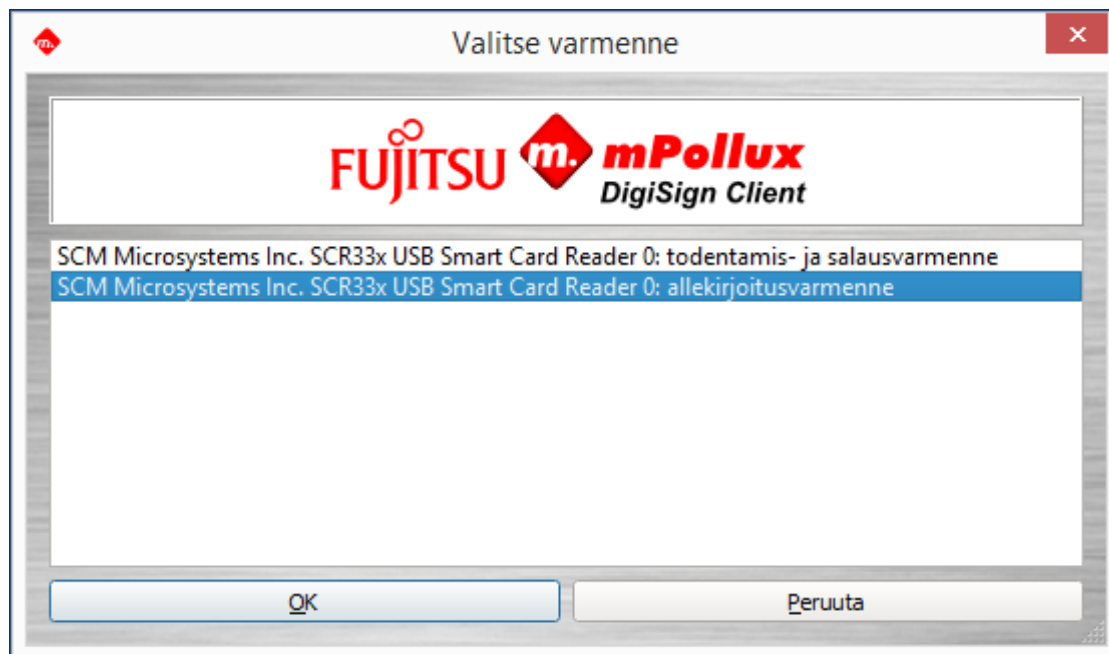
4. Anna tunnuslukusi ja valitse **OK**.
5. Kun lopetat palvelun käytön, muista kirjautua ulos ja poistaa älykortti lukijasta.

3.6 Asiakirjan allekirjoittaminen sähköisesti

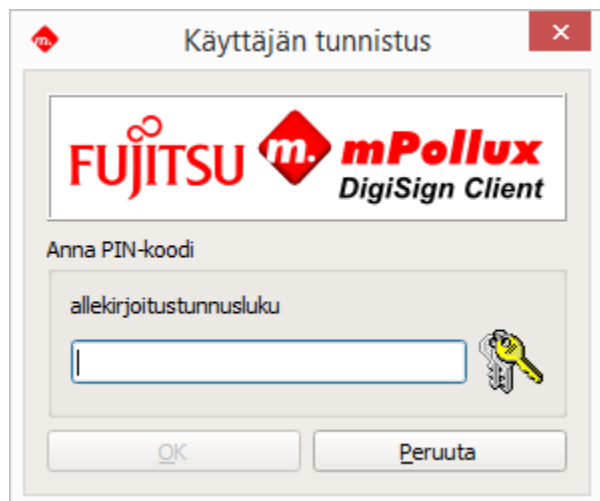
DigiSign Client -ohjelmistolla voit allekirjoittaa sähköisen asiakirjan tai palvelulomakkeen.

Ohjelma pyytää allekirjoitukseen joko perustunnuslukua (PIN 1) tai allekirjoitustunnuslukua (PIN 2). Perustunnusluku on tarkoitettu kertakäyttöiseen allekirjoitukseen esimerkiksi sähköpostiviesteissä. Allekirjoitustunnusluku on tarkoitettu kiistämättömään eli lainvoimaiseen allekirjoitukseen esimerkiksi sopimuksissa.

1. Varmista, että näytössä näkyy -kuvake, joka tarkoittaa, että älykortti on valmis käytettäväksi.
2. Valitse palvelussa tai asiakirjassa sähköinen allekirjoitus. Ohjelma kysyy tunnuslukuasi.




3. Anna tunnuslukusi ja valitse **OK**.



3.7 Sähköpostiviestin allekirjoittaminen ja salaaminen



DigiSign Client -ohjelmistolla voit allekirjoittaa ja salata sähköpostiviestin. Huomaa, että joissain sähköpostiohjelmissa käytettävän sähköpostiosoitteen on oltava tallennettu varmenteelle.

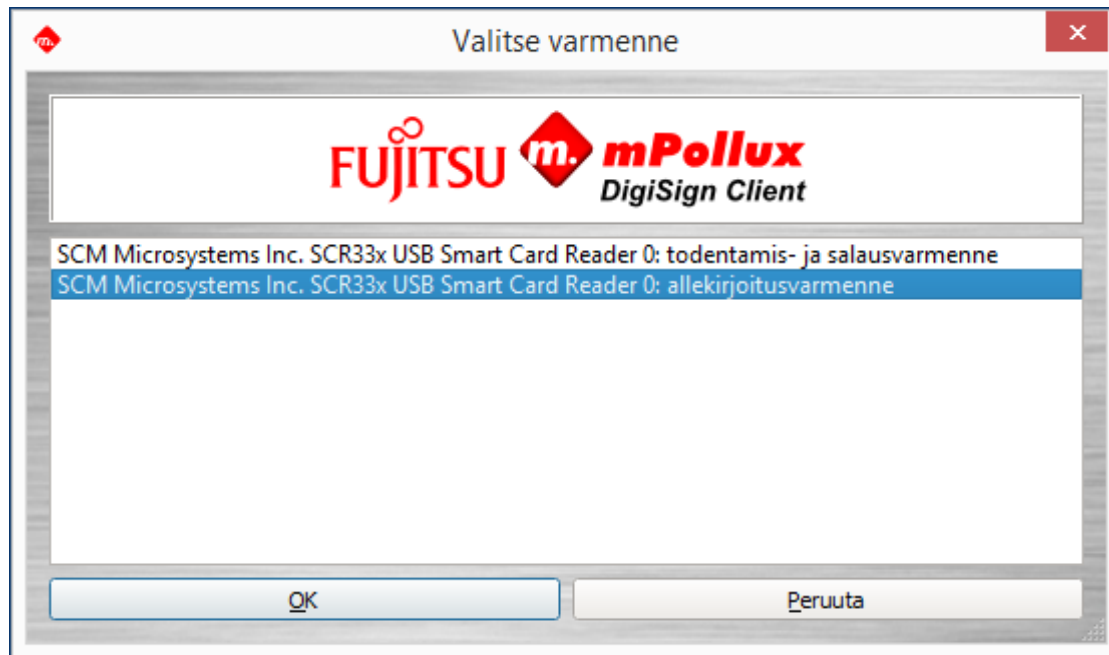
Vastaanottajalla on myös oltava varmenteesi. Voit toimittaa sen lähettämällä hänelle sähköisesti allekirjoitetun viestin.

1. Varmista, että näytössä näkyy -kuvake, joka tarkoittaa, että älykortti on valmis käytettäväksi.
2. Lisää sähköpostiviestiin sähköinen allekirjoitus ja lähetä se vastaanottajalle. Ohjeet löydät käyttämäsi ohjelman käyttöohjeista.
3. Vastaanottaja voi nyt vastata sinulle käyttämällä viestissä olevaa varmennetta. Viesti toimitetaan salattuna.
4. Käytä varmennettasi avataksesi salatun viestin.

3.8 PDF-dokumentin allekirjoittaminen

Versiosta 4.1.0 lähtien DigiSign Client -ohjelmiston avulla voit allekirjoittaa PDF-dokumentteja. Allekirjoittamine tapahtuu seuraavasti:

1. Varmista, että näytössä näkyy -kuvake, joka tarkoittaa, että älykortti on valmis käytettäväksi.
2. Napsauta -kuvaketta hiiren oikean puoleisella napilla ja valitse "Allekirjoita .pdf-dokumentti..."
3. Valitse varmenne, millä haluat tehdä allekirjoituksen.




4. Valitse allekirjoitettava PDF tiedosto ja syötä PIN-koodi tarvittaessa
5. Allekirjoitettu dokumentti avataan .pdf tiedostopäätteisen oletusohjelman kanssa.


4. Yleisimmistä virhetilanteista selviytyminen


Tässä kappaleessa kerrotaan mitä tehdä yleisimmissä virhetilanteissa. Lisää neuvoja saat varmenteen myöntäjältä.

4.1 Älykortin kuvaketta ei näy

DigiSign Client käynnistyy tietokoneen käynnistyessä. Kun DigiSign Client on käynnissä, näytössä näkyy kuvake . Jos älykortin kuvaketta ei näy, ohjelmisto ei ole käynnissä.

4.2 Ohjelmisto ei hyväksy tai löydä korttia


Jos näytössä näkyy -kuvake, DigiSign Client -ohjelmisto ei tunnista älykorttia. Kortti saattaa olla viallinen tai vääränlainen. Tarkista, että kortti on tarkoitettu juuri siihen palveluun, jota olet käyttämässä.

Jos näytössä näkyy -kuvake, DigiSign Client -ohjelmisto ei löydä älykorttia tai siinä olevaa varmennetta. Tarkista, että kortti on kortinlukijassa oikein päin ja pohjaan asti työnnetty.

Vika voi myös olla kortinlukijan ajureissa. Päivitä ajurit kortinlukijan valmistajan ohjeiden mukaan.

Kortti saattaa myös olla likainen. Puhdista kortin siruosa huolellisesti ja yritä uudestaan.

4.3 Kortin ottaminen pois lukijasta ei muuta kuvaketta

Jos -kuvake ei muutu, vaikka otat kortin pois kortinlukijasta, kortinlukijan ajurit eivät toimi kunnolla. Päivitä ajurit kortinlukijan valmistajan ohjeiden mukaan.

4.4 Käyttäjävarmennetta ei löydy

DigiSign-turvallisuusmoduuli tulee ladata selaimeen ennen käyttöä. Ennen kuin tämä on tehty, sivusto kertoo, että käyttäjävarmennetta ei löydy. Lataa turvallisuusmoduuli kappaleen 2.5.1 Turvallisuusmoduulin lataaminen ohjeiden mukaan.

Sama virheilmoitus näytetään, jos älykortti ei ole kortinlukijassa kun yrität käyttää palvelua.

4.5 Selain väittää, että yhteys ei ole luotettu

Joissain selaimissa, kuten Mozilla Firefoxissa, varmennuksen myöntäjän julkiset varmenteet tulee määritellä luotetuiksi ennen käyttöä. Ennen kuin tämä on tehty, selain väittää, että yhteys ei ole luotettu.

Lataa varmenne selaimeen kappaleen 2.5.2 Varmenteiden lataaminen selaimeen ohjeiden mukaan.

4.6 PIN-koodi (tunnusluku) on lukkiutunut

Jos annat tunnuslukusi tarpeeksi monta kertaa väärin, ohjelma lukitsee sen. Koodin avaamiseen tarvitset avaustunnusluvun eli PUK-koodin. Jos sinulla ei ole PUK-koodia, voit tilata sen kortin myöntäjältä. Uudemmissa korteissa on kortin mukana toimitettu aktivointitunnusluku, jonka avulla lukkiutuneen PIN-koodin voi aktivoida uudelleen.

1. Napsauta -kuvaketta hiiren oikealla painikkeella, ja valitse **Näytä laitteet**.

2. Valitse **Tunnistus**-välilehti.

The screenshot shows the 'DigiSign Sovellus' application window. The 'Tunnistus' tab is active, displaying options for managing smart cards. The 'Tunnistusobjektit' section lists available smart card readers. The 'Tarkista PIN' section allows checking the current PIN. The 'Vaihda PIN' section provides fields for the current PIN and a new PIN, with a 'Vaihda' button. The 'Vapauta lukkiutunut PIN' section provides fields for the PUK and a new PIN, with a 'Vapauta' button. A 'Sulje' button is located at the bottom of the window.

3. Valitse **Tunnistusobjektit**-kentästä se tunnusluku, joka on lukkiutunut.

Jos sinulla on useampi tunnusluku etkä ole varma siitä, mikä niistä on lukkiutunut, tarkista asia seuraavasti:

- Valitse **Tunnistusobjektit**-kentästä ensimmäinen tunnusluku.
 - Anna tunnusluku **Tarkista PIN** -osion **PIN**-kenttään, ja valitse **Tarkista**.
 - Jos tunnusluku on lukkiutunut, ohjelmisto antaa ilmoituksen "Tunnusluku on lukittu".
 - Jos valitsemasi tunnusluku ei ole lukossa, jatka tarkistamalla seuraava tunnusluku.
4. Varmista, että olet valinnut **Tunnistusobjektit**-kentästä sen tunnusluvun, joka on lukkiutunut. Anna PUK-koodisi **Vapauta lukkiutunut PIN** -osiossa olevaan **PUK**-kenttään.


Jos annat PUK-koodin tarpeeksi monta kertaa peräkkäin väärin, kortti lukittuu lopullisesti. Tarkka määrä riippuu kortista.

5. Anna uusi tunnusluku **Uusi PIN** -kenttiin.

6. Valitse **Vapauta**. Ohjelmisto antaa ilmoituksen "Tunnusluku on avattu ja vaihdettu". Paina uusi tunnusluku muistiin tai kirjoita se ylös ja säilytä turvallisessa paikassa.
7. Valitse **Sulje** poistuaksesi ohjelmasta.

4.7 Allekirjoitustoiminto ei toimi selaimessa

DigiSign Client käyttää sisäistä internetpalvelinta sähköiseen allekirjoitukseen. Jotkut palomuurit estävät tällaisen palvelimen käytön tietokoneessa. Jos allekirjoitus ei onnistu selaimessa, tarkista palomuurin asetukset.

1. Varmista, että näytössä näkyy -kuvake, joka tarkoittaa, että älykortti on valmis käytettäväksi.
2. Mene osoitteeseen <https://127.0.0.1:53952> Sivu kertoo, että yhteys ei ole luotettu.
Lataa varmenne selaimeen kappaleen 2.5.2 Varmenteiden lataaminen selaimeen ohjeiden mukaan.

