

# Loppukäyttäjän ohje

## Asennus- ja käyttöohje – Mac

Fujitsun mPollux DigiSign Client on kortinlukijaohjelmisto, jonka avulla voit kirjautua luotettavasti ja turvallisesti organisaation tietoverkkoon tai sähköiseen asiointipalveluun ja allekirjoittaa tai salata sähköpostiviestin tai sähköisen asiakirjan.

---



## Sisällysluettelo

1	DigiSign Client -kortinlukijaohjelmisto	3
1.1	Käytön edellytykset	3
1.2	Tuetut käyttöjärjestelmä	3
1.3	Käyttöohjeet	3
2	DigiSign Client -ohjelmiston asentaminen	3
2.1	Aikaisempien kortinlukijaohjelmistojen ja versioiden poistaminen	3
2.2	Ohjelmiston asentaminen	3
2.3	Ohjelmiston toiminnan varmistaminen	7
2.4	Selain- ja sähköpostiohjelmien asetukset	7
2.4.1	Turvallisuusmoduulin lataaminen	8
2.4.2	Varmenteiden lataaminen selaimen	10
2.4.3	Varmenteiden lataaminen sähköpostiohjelmaan	11
3	DigiSign Client -ohjelmiston käyttäminen	12
3.1	Käytön aloittaminen	13
3.2	Kortinlukijan ja korttien hallinta	13
3.3	Tunnusluvun vaihtaminen	14
3.4	Tunnistautuminen organisaation tietoverkkoon	15
3.5	Tunnistautuminen sähköiseen asiointipalveluun	16
3.6	Asiakirjan allekirjoittaminen sähköisesti	16
3.7	Sähköpostiviestin allekirjoittaminen ja salaaminen	17
4	Yleisimmistä virhetilanteista selviytyminen	17
4.1	Älykortin kuvaketta ei näy	17
4.2	Ohjelmisto ei käynnisty	17
4.3	Ohjelmisto ei hyväksy tai löydä korttia	18
4.4	Kortin ottaminen pois lukijasta ei muuta kuvaketta	18
4.5	Käyttäjävarmennetta ei löydy	18
4.6	Selain väittää, että yhteys ei ole luotettu	18
4.7	Pin-koodi (tunnusluku) on lukkiutunut	19
4.8	Allekirjoitustoiminto ei toimi selaimessa	21

## 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 käyttöjärjestelmä

DigiSign Client tukee Mac OS v10.7 -käyttöjärjestelmää.

### 1.3 Käyttöohjeet

Ohjelmiston mukana toimitetaan seuraavat käyttöohjeet:

- *Fujitsu mPollux DigiSign Client asennus- ja käyttöohje – Mac OS* (nämä ohjeet)
- *Fujitsu mPollux DigiSign Client asennus- ja käyttöohje – Linux*
- *Fujitsu mPollux DigiSign Client asennus- ja käyttöohje – Windows*
- *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 Client -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, avaa **Ohjelmat > Lisäohjelmat > Pääte**, ja anna seuraava komento:  
`/Library/mPolluxDigiSign/Uninstall.tool`
3. Kun ohjelma kysyy, haluatko poistaa mPollux DigiSignin asennuksen, vastaa **Kyllä**.
4. Kun ohjelma kysyy salasanaasi, anna salasanaasi. mPollux DigiSign on nyt poistettu koneeltasi.

### 2.2 Ohjelmiston asentaminen

Ohjelmiston asentaminen vaatii järjestelmänvalvojan oikeudet tietokoneeseen.

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

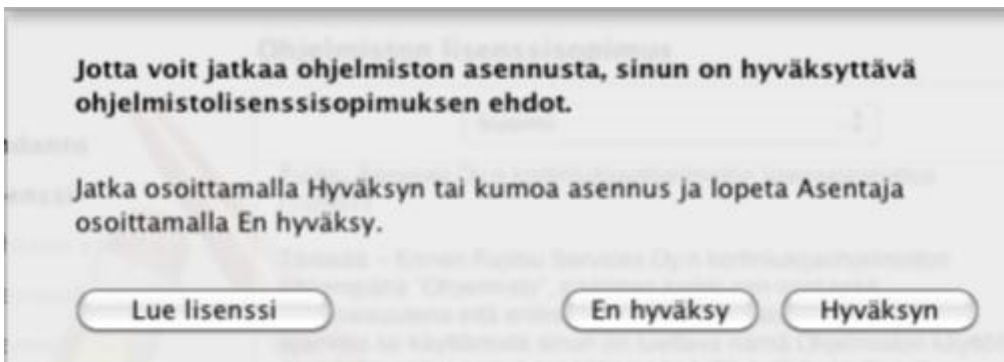
1. Avaa mPollux DigiSign -levykuva (.dmg) kaksoisnapsauttamalla sitä.
2. Avaa asennusohjelma <DigiSign-asennuspaketti>.mpkg Finderissa kaksoisnapsauttamalla sitä. Asennusohjelma avautuu.



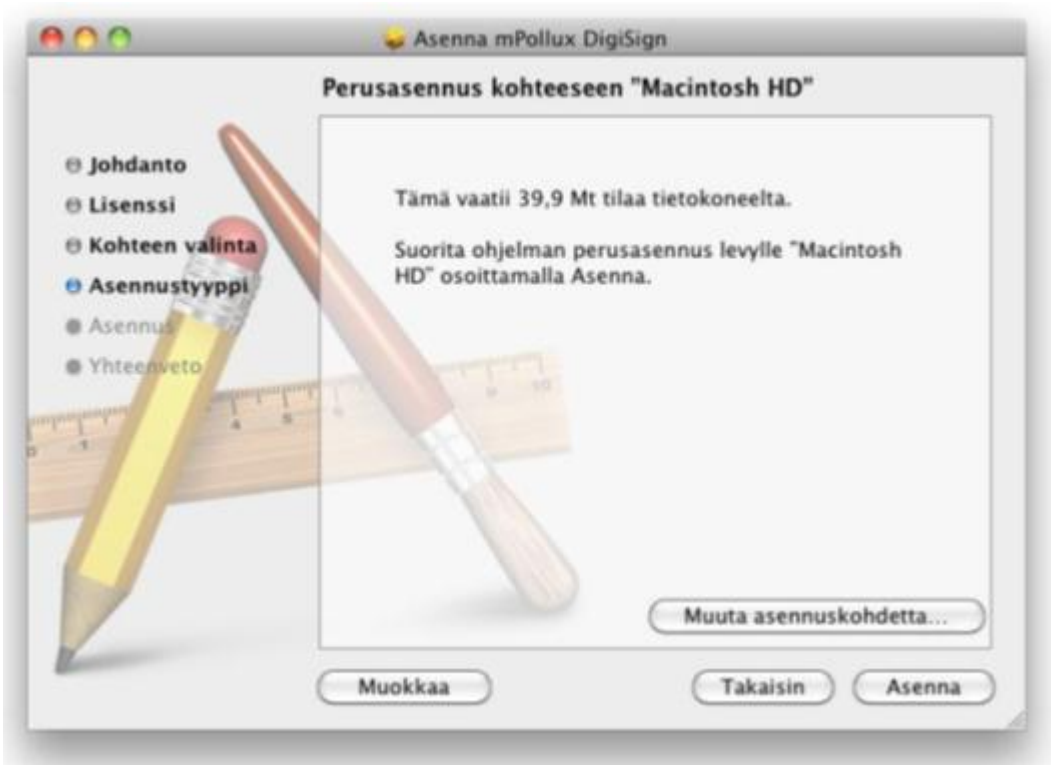
3. Valitse **Jatka**. Lisenssisopimus avautuu.



4. Lue sopimusteksti ja valitse **Jatka**. Lisenssiehtojen hyväksymisikkuna avautuu.



5. Valitse **Hyväksyn**. Asennusikkuna avautuu.





6. Valitse **Asenna**. Asennusohjelma asentaa ohjelmiston ja ilmoittaa, kun asennus on valmis.

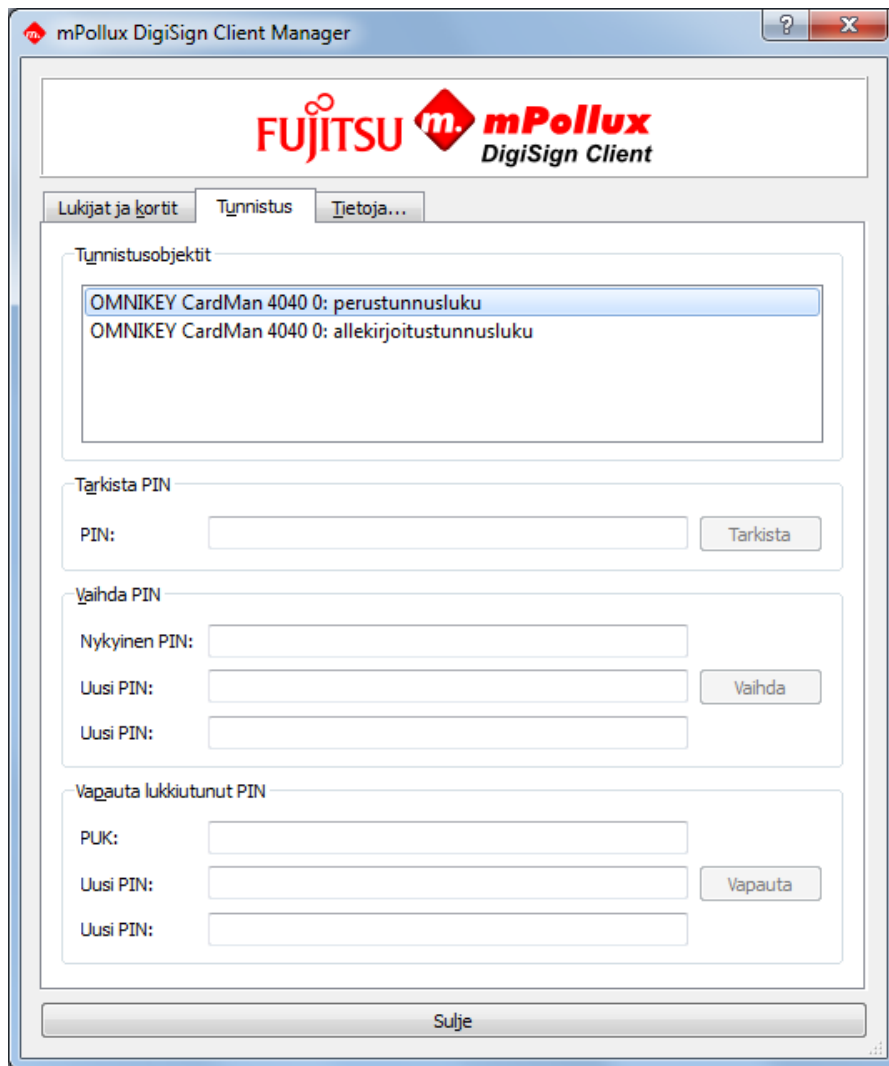


7. Valitse **Sulje**. DigiSign Client -ohjelmisto on nyt asennettu tietokoneellesi. mPollux DigiSign Manager ja mPollux DigiSign Applet -sovellukset löytyvät nyt **Sovellukset**-kansioista.

### 2.3 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. Pidä Ctrl-painiketta pohjassa, napsauta -kuvaketta ja valitse **Näytä laitteet**.
4. Valitse **Tunnistus**-välilehti.



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 puk-koodin avulla kappaleen 4.7 Pin-koodi (tunnusluku) on lukkiutunut ohjeiden mukaan.

### 2.4 Selain- ja sähköpostiohjelmien asetukset


Selain- ja sähköpostiohjelmissa (esimerkiksi Mozilla Firefox ja Thunderbird) täytyy tehdä seuraavat asetukset ennen kuin DigiSign Client -ohjelmistoa voi käyttää:

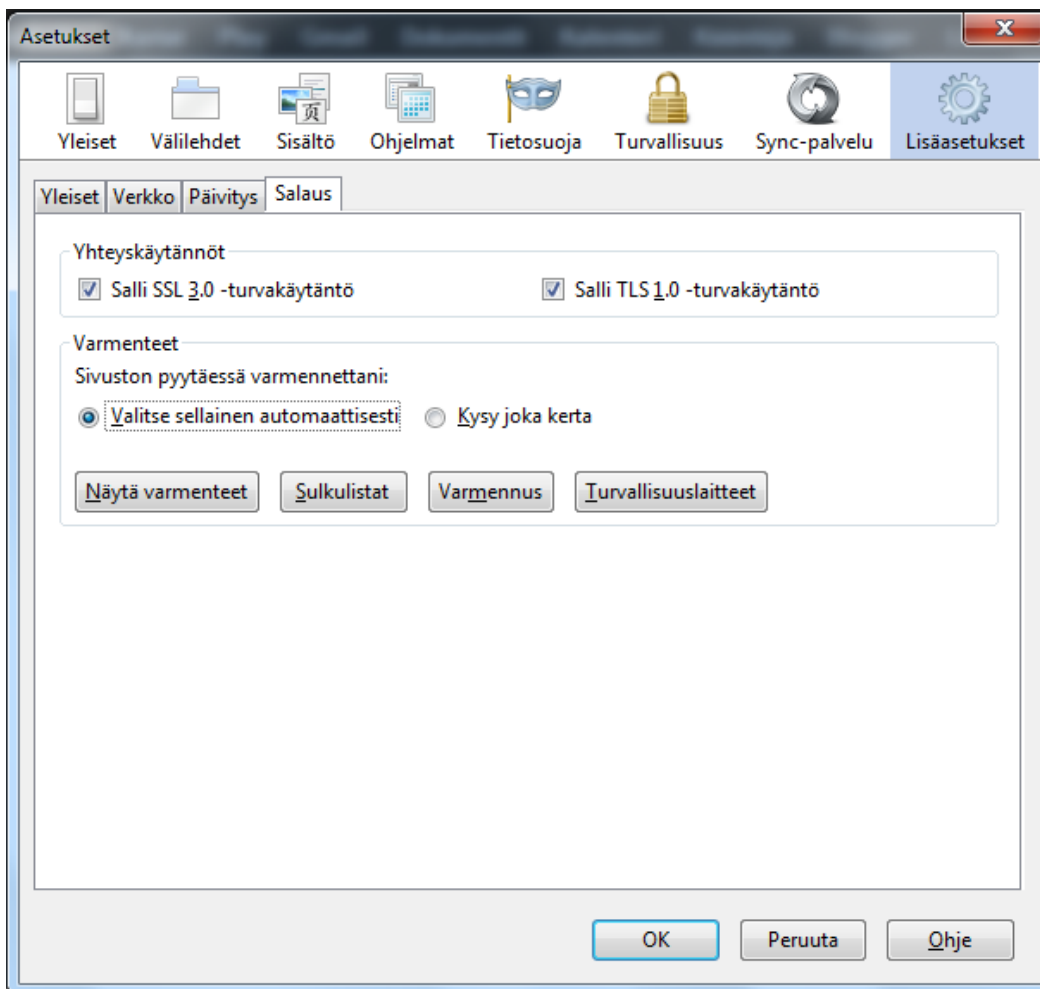
- Ladata DigiSign Client -ohjelmiston käyttämä turvallisuusmoduuli ohjelmaan.
- Ladata varmennuksen myöntäjän julkiset varmenteet ohjelmaan.

Ennen kuin nämä on tehty, selain väittää, että yhteys ei ole luotettu.

#### 2.4.1 Turvallisuusmoduulin lataaminen

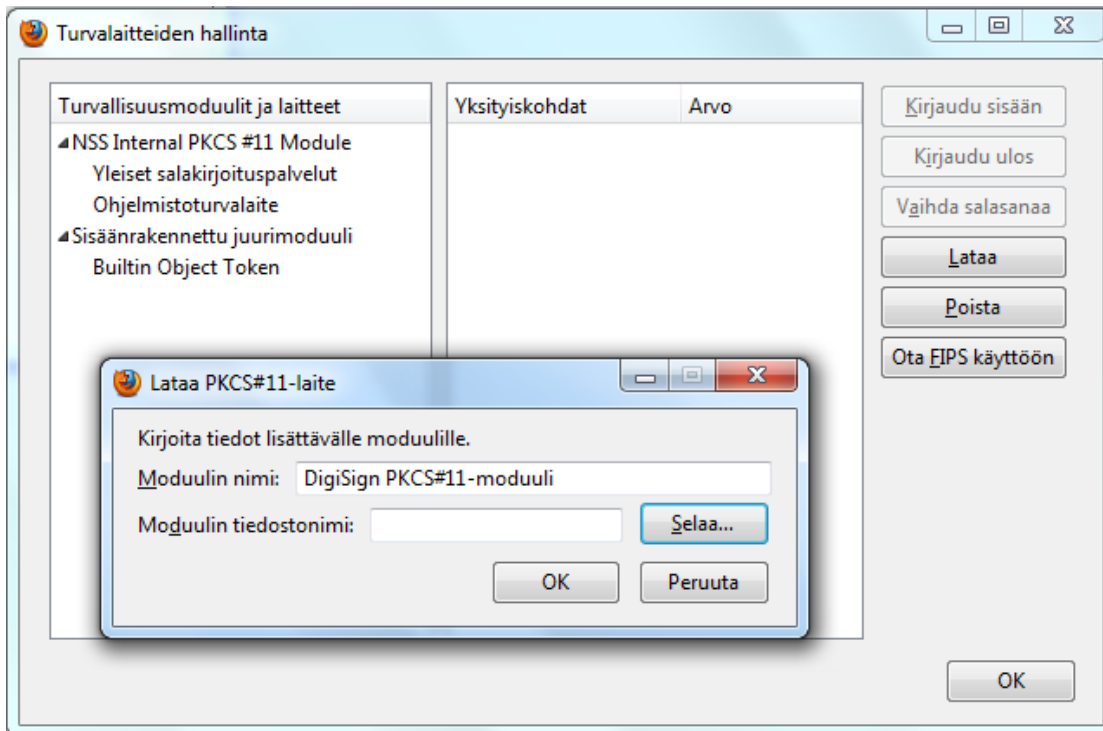
Seuraava esimerkki kertoo, kuinka turvallisuusmoduuli ladataan Mozilla Firefoxin versiossa 15 ja Mozilla Thunderbirdin versiossa 15. Muissa ohjelmissa ja versioissa asetukset saattavat olla erilaiset.

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



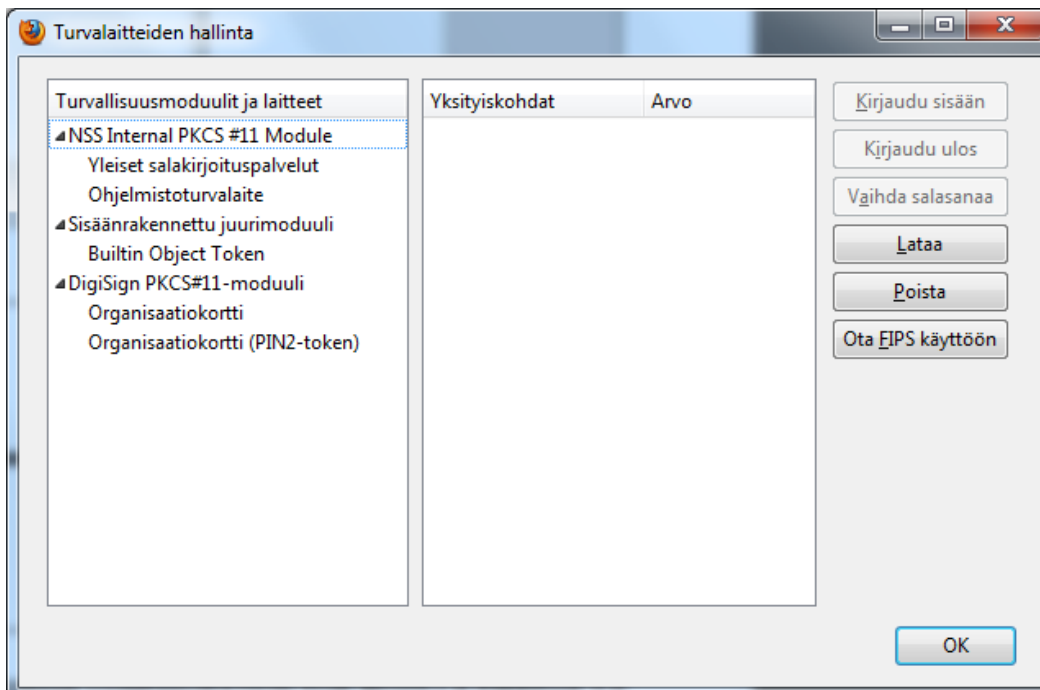
3. Valitse **Varmenteet**-otsikon alta **Valitse sellainen automaattisesti**.
4. Valitse **Turvallisuuslaitteet** ja **Lataa**.





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

6. Paina **Selaa** ja hae koneeltasi `libcryptoki.dylib`-tiedosto. Se sijaitsee oletusarvoisesti hakemistossa `/Library/mPolluxDigiSign`. Paina **OK**.




Jos saat virheilmoituksen, että turvallisuusmoduulia ei voi ladata, sulje selain ja yritä uudestaan.

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

8. Käynnistä selain tai sähköpostiohjelma uudestaan.

## 2.4.2 Varmenteiden lataaminen selaimeen

Varmennuksen myöntäjän julkiset varmenteet tulee määritellä luotetuiksi ennen käyttöä. Ennen kuin tämä on tehty, selain väittää, että yhteys ei ole luotettu.



### Tämä yhteys ei ole luotettu


Olet pyytänyt Firefoxia muodostamaan suojatun yhteyden sivustoon **vrk.fineid.fi**, mutta yhteyden turvallisuutta ei pystytä varmistamaan.

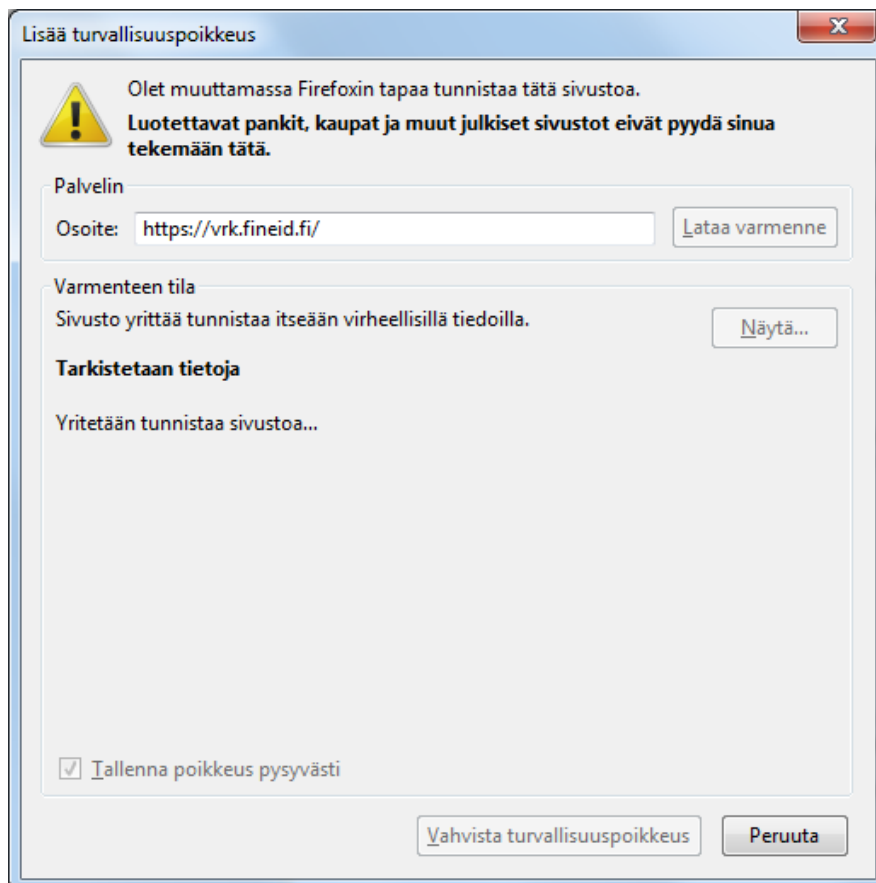
Yleensä kun suojattua yhteyttä muodostetaan, sivustot lähettävät varmenneet identiteettitietonsa, joiden perusteella voi olla varma, että tietoja siirretään oikean paikan kanssa. Tämän sivuston identiteettiä ei kuitenkaan voida varmentaa.

#### Mitä minun pitäisi tehdä?

Jos olet aikaisemmin saanut ongelmitta muodostettua suojatun yhteyden tähän sivustoon, tämä virhe voi olla merkinä siitä, että jokin taho yrittää vilpillisesti tekeytyä täksi sivustoksi, jolloin sinun ei pitäisi jatkaa sivustolle.

- ▶ **Tekniset yksityiskohdat**
- ▶ **Ymmärrän riskit**

1. Varmista, että näytössä näkyy -kuvake, joka tarkoittaa, että älykortti on valmis käytettäväksi.
2. Valitse **Ymmärrän riskit** ja **Lisää poikkeus**. Lisää turvallisuuspoikkeama -ikkuna avautuu.



3. Valitse **Lataa varmenne**. Ohjelma pyytää sinua tunnistautumaan.




Jos ohjelma tunnistaa varmenteen ja kertoo, ettei turvallisuuspoikkeusta tarvitse tehdä, valitse **Peruuta**.

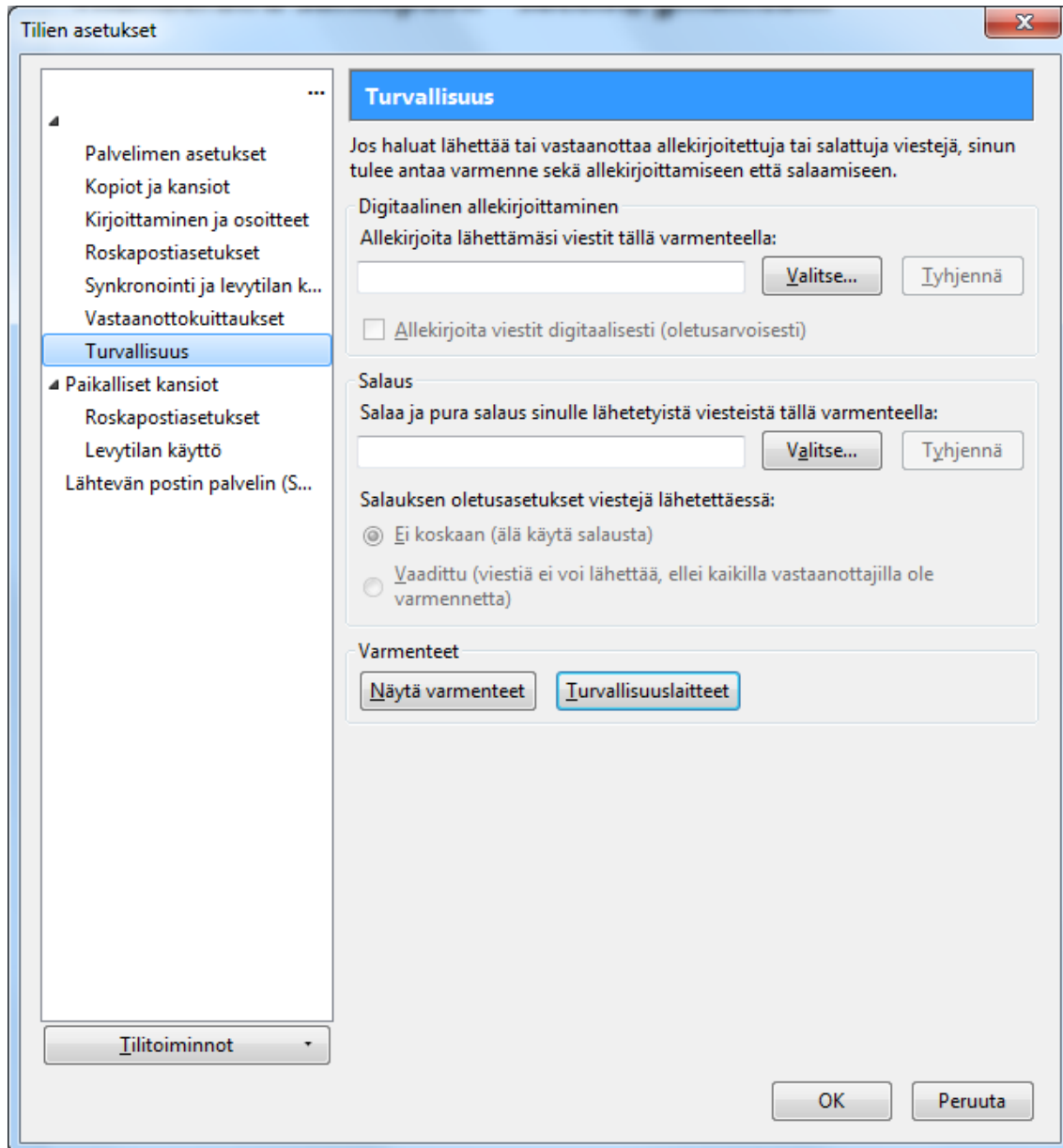
4. Anna tunnuslukusi ja valitse **OK** ja **Vahvista turvallisuuspoikkeus**.

5. Päivitä sivu. Sinun tulisi nyt päästä palveluun.

### 2.4.3 Varmenteiden lataaminen sähköpostiohjelmaan

Varmennuksen myöntäjän julkiset varmenteet täytyy ladata sähköpostiohjelmaan 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 **Työkalut > 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 luostat varmenteeseen.

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

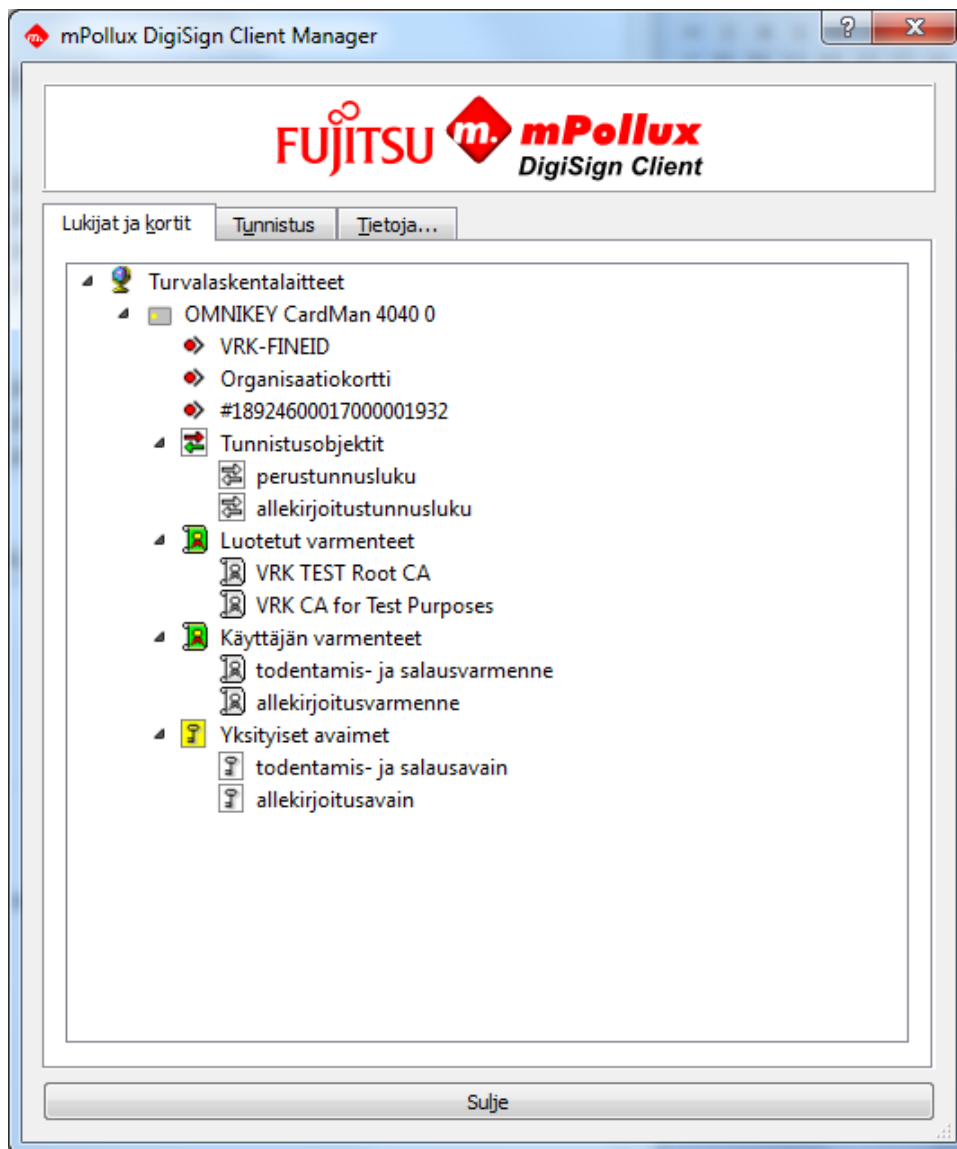
Älä koskaan anna tunnuslukuasi jos sitä kysytään odottamatta. Varmista, että olet aina itse käynnistänyt tunnuslukua kysyvän toiminnon.

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. Pidä Ctrl-painiketta pohjassa, napsauta -kuvaketta ja valitse **Näytä laitteet**. DigiSign Client Manager -ikkuna avautuu.



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

**Turvaskentälaitteet** näyttää koneessa kiinni olevat kortinlukijat. Kortinlukijan alla kerrotaan kortin myöntäjä, otsikko ja sarjanumero, jos nämä tiedot ovat saatavilla.

**Tunnistusobjektit** näyttää 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** näyttää kortilla olevat varmentajan varmenteet.

**Käyttäjän varmenteet** näyttää kortin käyttäjälle myönnettyt varmenteet

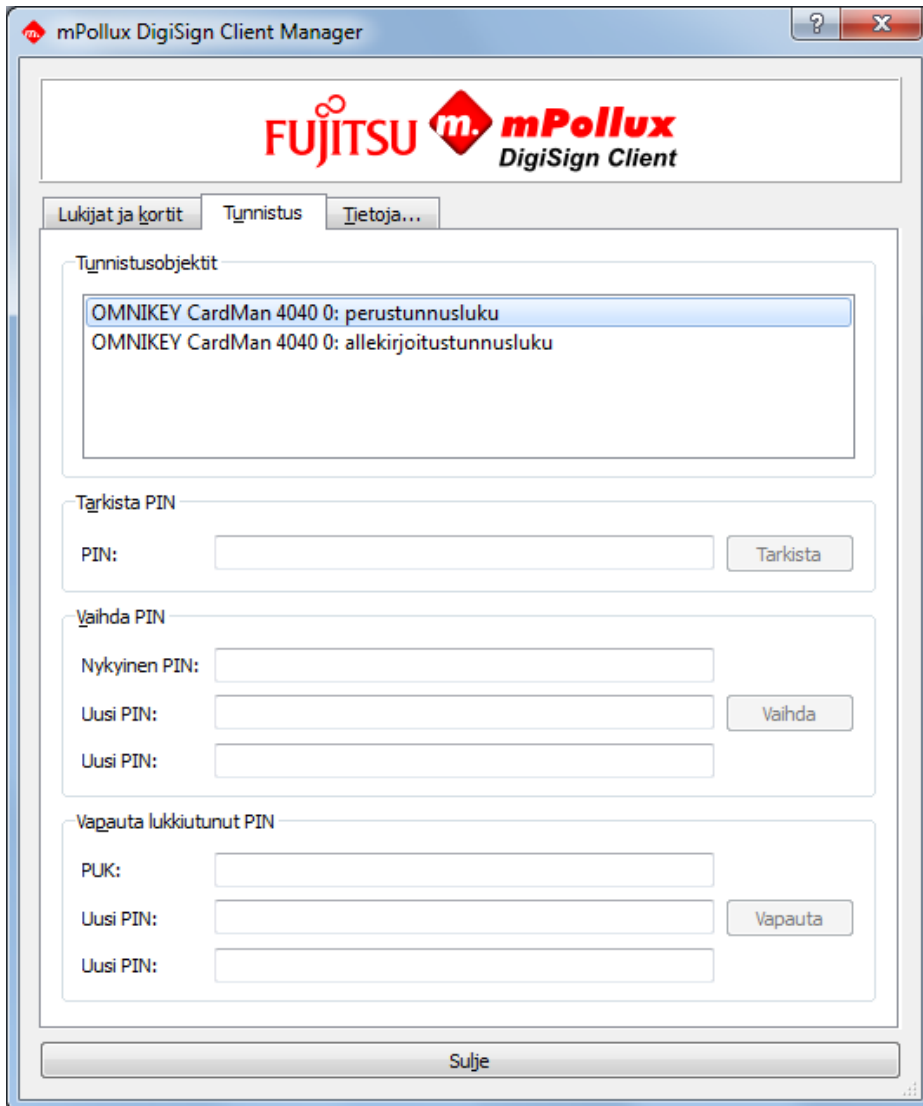
**Yksityiset avaimet** näyttää kortilla olevat käyttäjän avaimet.

3. Pitämällä Ctrl-painiketta pohjassa ja napsauttamalla varmennetta voit avata varmenteen ja tarkistaa sen tiedot, kuten voimassaoloajan tai sen sähköpostiosoitteen, joka varmenteeseen on liitetty. Voit myös tallentaa varmenteen.
4. Pitämällä Ctrl-painiketta pohjassa ja napsauttamalla tunnuslukua voit tarkistaa tunnusluvun oikeellisuuden, vaihtaa sen tai avata lukitun tunnusluvun.
5. Pitämällä Ctrl-painiketta pohjassa ja napsauttamalla salausavainta 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 pitämällä Ctrl-painiketta painettuna, napsauttamalla tunnuslukua ja valitsemalla **Vaihda**.


1. Pidä Ctrl-painiketta pohjassa, napsauta -kuvaketta 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.

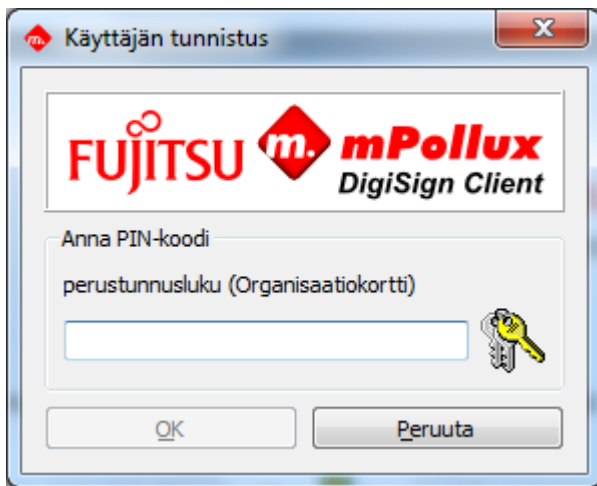


4. Kirjoita perustunnuslukusi kenttään ja valitse **OK**. Olet nyt kirjautunut organisaatiosi tietoverkkoon.
5. Kun lopetat palvelun käytön, muista kirjautua ulos ja poistaa älykortti lukijasta.

### 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

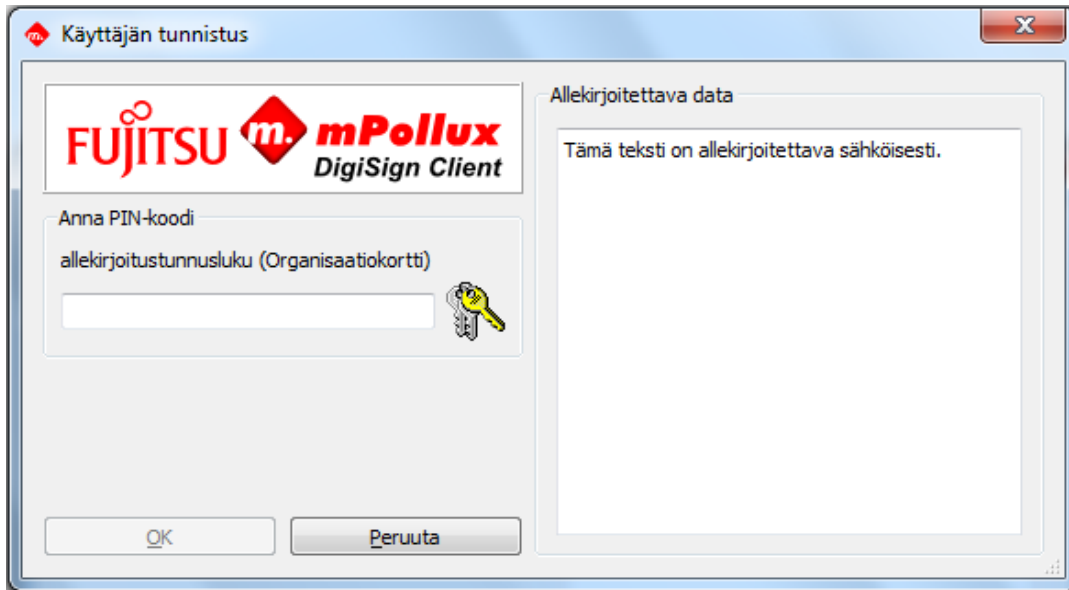
DigiSign Client -ohjelmistolla voit allekirjoittaa sähköisen asiakirjan tai palvelulomakkeen.

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.


## 4 Yleisimmistä virhetilanteista selviytyminen

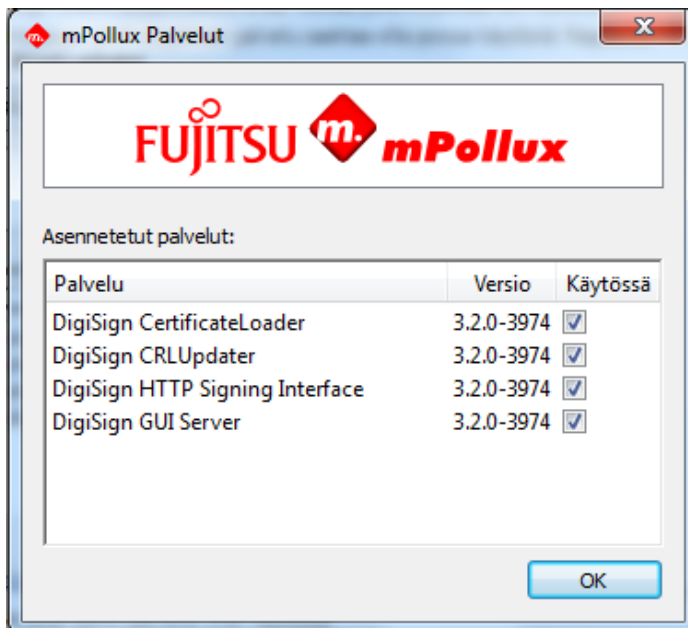
Tässä kappaleessa kerrotaan mitä tehdä yleisimmissä virhetilanteissa. Lisää neuvoja saat varmenteen myöntäjältä.

### 4.1 Älykortin kuvaketta ei näy

DigiSign Client käynnistyy tietokoneen käynnistyessä. Kun DigiSign Client on käynnissä, näytössä näkyy kaksi kuvaketta,  ja . Jos älykortin kuvaketta ei löydy, ohjelman varmenteenlatauspalvelu saattaa olla poissa käytöstä. Katso ohjeet seuraavasta kappaleesta.

### 4.2 Ohjelmisto ei käynnisty


Jos DigiSign Client -ohjelmisto ei avaa ruutua, jolle kirjoittaa tunnusluku, tai älykortin kuvaketta ei näy, jokin ohjelman palvelu saattaa olla poissa käytöstä. Pidä Ctrl-painiketta pohjassa, napsauta -kuvaketta ja valitse **Näytä palvelut**. mPollux Palvelut -ikkuna avautuu.




Tarkista, että kaikki palvelut ovat käytössä:

- **DigiSign CertificateLoader** tarvitaan sähköisessä tunnistautumisessa.
- **DigiSign CRLUpdate** on DigiSign Toolkitin käyttämä apuohjelma, joka nopeuttaa ohjelmiston toimintaa.
- **DigiSign HTTP Signing Interface** tarvitaan sähköisessä allekirjoituksessa.
- **DigiSign GUI Server** käynnistää graafiset käyttöliittymät.

#### 4.3 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.

#### 4.4 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.

#### 4.5 Käyttäjävarmennetta ei löydy

DigiSign-turvallisuusmoduuli tulee ladata selaimen ennen käyttöä. Ennen kuin tämä on tehty, sivusto kertoo, että käyttäjävarmennetta ei löydy. Lataa turvallisuusmoduuli kappaleen 2.4.1 Turvallisuusmoduulin lataaminen ohjeiden mukaan.

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

#### 4.6 Selain väittää, että yhteys ei ole luotettu

Varmennuksen myöntäjän julkiset varmenteet tulee määritellä luotetuiksi ennen käyttöä. Ennen kuin tämä on tehty, selain väittää, että yhteys ei ole luotettu.



### Tämä yhteys ei ole luotettu

Olet pyytänyt Firefoxia muodostamaan suojatun yhteyden sivustoon **vrk.fineid.fi**, mutta yhteyden turvallisuutta ei pystytä varmistamaan.

Yleensä kun suojattua yhteyttä muodostetaan, sivustot lähettävät varmenneet identiteettitietonsa, joiden perusteella voi olla varma, että tietoja siirretään oikean paikan kanssa. Tämän sivuston identiteettiä ei kuitenkaan voida varmentaa.

#### Mitä minun pitäisi tehdä?

Jos olet aikaisemmin saanut ongelmitta muodostettua suojatun yhteyden tähän sivustoon, tämä virhe voi olla merkinä siitä, että jokin taho yrittää vilpillisesti tekeytyä täksi sivustoksi, jolloin sinun ei pitäisi jatkaa sivustolle.

[Siirry pois sivulta](#)

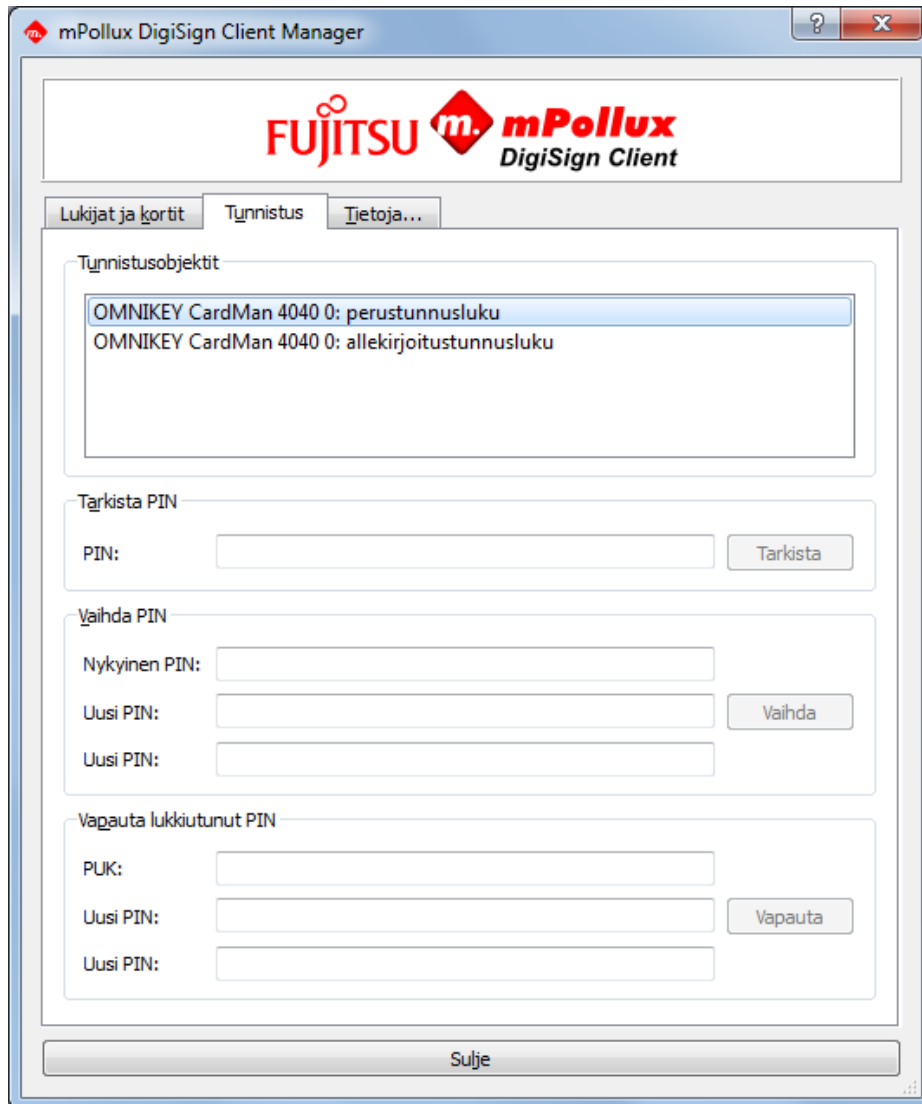
- ▶ **Tekniset yksityiskohdat**
- ▶ **Ymmärrän riskit**

Lataa varmenne selaimeen kappaleen 2.4.2 Varmenteiden lataaminen selaimeen ohjeiden mukaan.

#### 4.7 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.


1. Pidä Ctrl-painiketta pohjassa, napsauta -kuvaketta ja valitse **Näytä laitteet**.
2. Valitse **Tunnistus**-välilehti.




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:
  - a) Valitse **Tunnistusobjektit**-kentästä ensimmäinen tunnusluku.
  - b) Anna tunnusluku **Tarkista PIN** -osion **PIN**-kenttään, ja valitse **Tarkista**.
  - c) Jos tunnusluku on lukkiutunut, ohjelmisto antaa ilmoituksen "Tunnusluku on lukittu".
  - d) 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.

#### 4.8 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/sign>. Sivu kertoo, että yhteys ei ole luotettu.



### Tämä yhteys ei ole luotettu

Olet pyytänyt Firefoxia muodostamaan suojatun yhteyden sivustoon **127.0.0.1:53952**, mutta yhteyden turvallisuutta ei pystytä varmistamaan.

Yleensä kun suojattua yhteyttä muodostetaan, sivustot lähettävät varmennetut identiteettitietonsa, joiden perusteella voi olla varma, että tietoja siirretään oikean paikan kanssa. Tämän sivuston identiteettiä ei kuitenkaan voida varmentaa.

#### Mitä minun pitäisi tehdä?


Jos olet aikaisemmin saanut ongelmitta muodostettua suojatun yhteyden tähän sivustoon, tämä virhe voi olla merkinä siitä, että jokin taho yrittää vilpillisesti tekeytyä täksi sivustoksi, jolloin sinun ei pitäisi jatkaa sivustolle.

- ▶ **Tekniset yksityiskohdat**
- ▶ **Ymmärrän riskit**

Jos sivu ei lataa, käynnistä tietokoneesi uudelleen.

3. Valitse **Ymmärrän riskit** ja **Lisää poikkeus**. 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:

Varmenteen tila  
Sivusto yrittää tunnistaa itseään virheellisillä tiedoilla.

**Tuntematon identiteetti**  
Varmenteeseen ei luoteta, koska yksikään tunnistettu varmentaja ei todenna sitä.

Tallenna poikkeus pysyvästi

4. Valitse **Vahvista turvallisuuspoikkeus**. Sivulla pitäisi nyt näkyä pieni valkea piste mustalla pohjalla.

---

**Yhteystiedot**

FUJITSU FINLAND OY  
PL 100, 00012 FUJITSU  
+358 029 302 302  
[www.fujitsu.com/fin](http://www.fujitsu.com/fin)

© Tekijänoikeus 2012 Fujitsu. Fujitsu sekä Fujitsu logo ovat Fujitsu Limitedin tavaramerkkejä. Muut toimi-, tuote- ja palvelunimet voivat olla niiden omistajien tavaramerkkejä. Tekniset tiedot voivat muuttua ja toimitus tapahtuu saatavuuden mukaan. Kaikki vastuu tietojen tai kuvien oikeellisuudesta tai täydellisyydestä pidätetään. Käytetyt nimikkeet voivat olla kunkin valmistajan tavaramerkkejä tai muutoin tekijänoikeuden alaisia, ja niiden käyttö kolmansien osapuolten taholta omiin käyttötarkoituksiinsa voi loukata kyseisen oikeudenhaltijan oikeuksia.