Atostek ID 4.6 käyttöohje

macOS:lle

v1.0

Atostek

Sisällysluettelo

1. ATOSTEK ID OHJELMISTOKUVAUS 5

2. ENNEN KÄYTÖN ALOITTAMISTA JA KÄYTÖN ALOITTAMINEN 6

2.1. Mikä on Atostek ID? 6

2.2. Mitä tarvitsen käyttääkseni Atostek ID:tä? 6

2.2.1. Atostek ID -ohjelman asentaminen 6

2.2.2. Atostek ID -ohjelman poistaminen 7

2.3. Kortin aktivoiminen 7

3. SÄHKÖINEN TUNNISTAUTUMINEN JA SÄHKÖINEN ALLEKIRJOITUS 10

3.1. Sähköinen tunnistautuminen 10

3.1.1. mTLS-tunnistautuminen 11

3.1.2. SCS-rajapinnan kautta tunnistautuminen 11

3.1.3. Atostek ERA -järjestelmän käyttäminen 11

3.2. Sähköinen allekirjoitus 12

3.2.1. PDF-dokumenttien allekirjoittaminen (Adobe Acrobat) 12

3.2.2. SCS-rajapinnan kautta allekirjoittaminen 13

3.2.3. Atostek ERA -järjestelmän allekirjoitus 13

4. TOIMINNALLISUUS 14

4.1. Käynnistäminen ja sulkeminen 14

4.2. Sovelluksen tiedot ja käyttöohje 14

4.3. PIN-koodien vaihtaminen ja lukittuneiden koodien avaaminen 14

4.4. Lukijat ja kortit 15

4.5. Asetukset 17

4.5.1. Kieli 17

4.5.2. Ilmoita uusista päivityksistä 17

4.5.3. Ilmoita, kun vain osittainen yhteys selaimeen on saatavilla 18

4.5.4. Ota SCS-rajapinta pois käytöstä 18

4.5.5. Näytä ”Kirjaudu ERA-järjestelmään” -valinta ponnahdusvalikossa 18

4.5.6. Käynnistä Atostek ID tietokoneen käynnistyksen yhteydessä 18

4.5.7. Ota käyttöön MIFARE-sirun luku- ja kirjoitusominaisuudet 18

4.5.8. Ota käyttöön varakortin yksilöinti 19

4.5.9. Salli lokitus ... 19
4.5.10. Aseta debug-lokitus päälle ... 19
4.5.11. Korttivälimuistin tyyppi ... 19
4.5.12. Sekunnin odotusaika lukijan ja kortin yhdistämiselle ... 19
4.5.13. Automaattista kirjautumisen uudelleenyritystä (0-5) ... 20
4.5.14. PIN1-koodin bufferointiaika minuuteissa (0-420) ... 20
4.5.15. Rekisteröi erasmartcard://-protokolla ... 20
4.5.16. Aikaleimapalvelun osoite ... 20
4.5.17. Määritelty sisäänkirjautumiskomento ... 21
4.5.18. Määritellyt laukaisukomennot ... 21
4.5.19. Aseta juurivarmenne luotetuksi Firefoxiin ... 21
4.5.20. Avaa SCS-palvelinvarmenteen lataussivu ... 21
4.5.21. Asetustiedoston parametri CLEANCERTSTOREONCARDREMOVAL ... 22
4.5.22. Asetustiedoston parametri EXCLUDEDREADERS ... 22
4.5.23. Asetustiedoston parametri EXCLUDEDCARDTYPES ... 22
4.5.24. Asetustiedoston parametri ERRORLOGPATH ... 22
4.5.25. Asetustiedoston parametri ALLOWEDBROWSERLESSANDFORWARDDOMAINS ... 23
4.5.26. Asetustiedoston parametri ENABLECUSTOMDIALOG ... 23

4.6. Päivittäminen ... 23

4.7. Dokumenttien allekirjoitus sovelluksen kautta ... 24

4.8. Sähköpostin salaus ja allekirjoitus (Apple Mail) ... 25

4.9. Työasemakirjautuminen ... 26

4.10. MIFARE-sirun hallinta ... 27

4.11. Lokitus ja välimuistitiedostot ... 28
4.11.1. Lokitus ja lokitiedostot ... 28
4.11.2. Välimuistitiedostot ... 28

4.12. Virheraportointi ... 28

4.13. Diagnostiikka ... 30

5. USEIN KYSYTYT KYSYMYKSET JA VIRHETILANTEISTA ... 32

5.1. Usein kysyttyjä kysymyksiä ... 32

5.2. Muita ongelmatilanteita ... 33
5.2.1. Atostek ID ja TokenDriver ... 33
5.2.2. Korttien myöntäjävarmenteiden vieminen Avainnippuun ... 34

1. Atostek ID ohjelmistokuvaus

Atostek Oy on vuonna 1999 perustettu suomalainen ohjelmistoalan yritys, joka toimii erityisesti terveydenhuollon ja lääketieteen sovellusten, teollisuuden tuotekehityksen sekä julkisen sektorin IT-konsultoinnin parissa. Atostekin tuotteisiin kuuluu muun muassa Atostek ID -kortinlukijaohjelmisto ja Atostek ERA -järjestelmä.

Atostek ID tarjotaan Digi- ja väestötietoviraston (DVV) virallisena kortinlukijaohjelmistona vuodesta 2024 eteenpäin. Ohjelmisto on tarkoitettu käytettäväksi Digi- ja väestötietoviraston myöntämien varmennekorttien kanssa. Ohjelmistoa käyttäen korteilla voidaan suorittaa esimerkiksi sähköinen tunnistautuminen ja sähköinen allekirjoitus useiden eri rajapintojen ja moduulien kautta. Tämän lisäksi ohjelmisto tukee varmennekortin aktivointia, tunnuslukujen käsittelyä ja kortin tietojen tarkastelua. Atostek ID -sovelluksen lisäksi ohjelmistoon kuluu Atostek ID Minidriver, Atostek ID TokenDriver, Atostek ID PKCS#11-moduulit ja Atostek ID AD-rekisteröintipalvelu. Näiden lisäksi Atostek ID tukee Digi- ja väestötietoviraston varakorttien myöntämistä. Edellä kuvattujen toimintojen lisäksi Atostek ID tarjoaa esimerkiksi yhteensopivuuden Atostekin ERA-järjestelmään erasmartcard.ehoito.fi-rajapinnan kautta. Atostek ID tunnettiin aiemmin nimellä ERA SmartCard.

Atostek ID -ohjelmiston asennuspaketit ja ohjedokumentit ovat ladattavissa sekä Digi- ja väestötietoviraston sivuilta että Atostekin omalta ajurilataussivulta. Digi- ja väestötietovirasto tiedottaa yleisesti ohjelmiston päivityksistä. Atostek tiedottaa omia sopimusasiakkaitaan päivityksistä erikseen sovitulla tavalla. Virhe- ja ongelmatilanteissa DVV:n kautta ohjelmiston käyttöoikeuden saaneet yksilöt ja organisaatiot ovat ensisijaisesti yhteydessä Digi- ja väestötietoviraston tukeen (1st line support), joka ohjaa tarvittaessa tukipyynnöt Atostekille (2nd line support). Atostekin sopimusasiakkaat ovat virhe- ja ongelmatilanteissa yhteydessä suoraan Atostekin tukeen sopimuksen mukaisella tavalla. DVV ja Atostek tiedottavat tarvittaessa erityisistä ongelmatilanteista ohjelmistoon liittyen.

Atostek ID -ohjelmistolle ja sen käyttöohjeille on suoritettu WCAG 2.1 ja 2.2 -standardien mukainen saavutettavuusarvio. Saavutettavuusseloste on luettavissa Digi- ja väestötietoviraston sivuilla ajurien latauksen yhteydessä. Ohjelmistolle suoritetaan tietoturva-auditointi tasaisin väliajoin Atostekin ja DVV:n erikseen sopimalla tavalla. Auditointiseloste tulee saataville Digi- ja väestötietoviraston sivuille ajurien latauksen yhteyteen auditoinnin jälkeen. Atostek ID on myös osa vuosittaista ERA-järjestelmän auditointia. Atostek ID -ohjelmiston kehitystä ohjaa myös Atostekin ISO 9001 -sertifioitu laatujärjestelmä.

Atostek ID -kortinlukijaohjelmistokokonaisuuden toimintaa ei taata, jos työasemalle on asennettu muita vastaavia kortinlukijaohjelmistoja.

Ohjelmiston jatkokehitykseen ja lisäominaisuuksiin liittyen voi olla yhteydessä suoraan Atostekiin (Atostekin sopimusasiakkaat) tai Digi- ja väestötietovirastoon.

2. Ennen käytön aloittamista ja käytön aloittaminen

Tässä luvussa esitellään Atostek ID -sovellus. Sen lisäksi kerrotaan vaatimukset sovelluksen käytölle ja ohjeistetaan, miten Atostek ID -sovellus asennetaan macOS-koneelle. Atostek ID -sovellus tukee kaikkia Applen ylläpitämiä macOS-käyttöjärjestelmän versioita.

2.1. Mikä on Atostek ID?

Atostek ID on kortinlukijaohjelmisto, jota käytetään Digi- ja väestötietoviraston myöntämien varmennekorttien kanssa. Näitä kortteja ovat sosiaali- ja terveydenhuollon ammatti-, henkilöstö- ja toimijakortit, organisaatiokortit, näihin liittyvät varakortit sekä kansalaisvarmennekortit (henkilökortit). Korteilla voidaan suorittaa sähköinen tunnistautuminen sekä sähköinen allekirjoitus ohjelmiston kanssa yhteensopivissa palveluissa ja sovelluksissa. Näiden lisäksi ohjelmisto tukee esimerkiksi varmennekortin aktivointia, tunnuslukujen käsittelyä ja kortin tietojen tarkastelua.

2.2. Mitä tarvitsen käyttääkseni Atostek ID:tä?

Atostek ID toimii macOS-käyttöjärjestelmillä. Mikäli olet epävarma siitä, tukeeko Atostek ID käyttöjärjestelmäsi versiota, tarkista viimeisin listaus tuetuista versioista Digi ja väestöviraston sivulta https://dvv.fi/kortinlukijaohjelmisto tai Atostekin omalta ajurienlataussivulta https://downloads.ehoito.fi ennen asennusta.

Huom! Jos käytät Windows- tai Linux-käyttöjärjestelmää (Debian, Red Hat), katso kyseiselle käyttöjärjestelmälle tarkoitettu käyttöohje tämän ohjeen sijaan.

Huom! Ohjelmistolle on tarjolla erilliset asennusohjeet, joissa asennuksen eri vaiheet käydään yksityiskohtaisesti läpi.

Huom! Ohjelmistolle on tarjolla myös erillinen integraatio-ohje, joka on tarkoitettu erityisesti järjestelmäkehittäjille ja organisaatioiden IT-tahoille.

Käyttääksesi varmennekorttia Atostek ID -ohjelmistolla, tarvitset ohjelman lisäksi kortinlukijan ja kortinlukija-ajurin. Kortinlukijan ajuri löytyy yleensä jo valmiiksi käyttöjärjestelmästä. Jos ajuria ei löydy tai ajuri vaatii päivitystä, voit ladata tarvittavat asennuspaketit suoraan kortinlukijavalmistajan omilta sivuilta. Atostek ID tukee PC/SC-määritysten mukaisia kortinlukijoita.

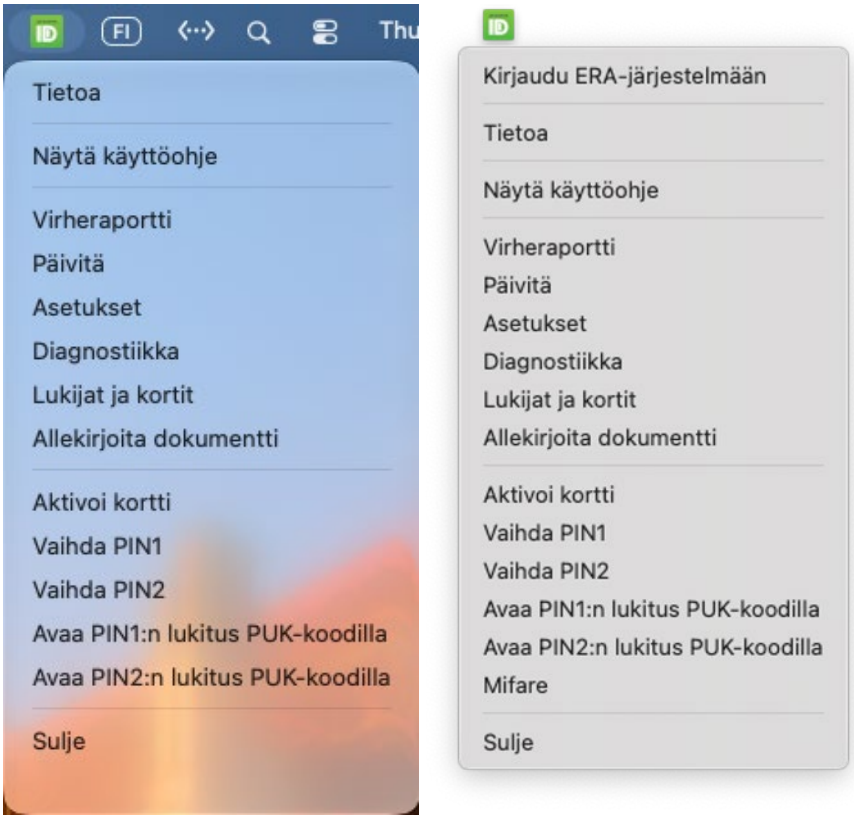
Atostek ID tukee selainkäytössä Microsoft Edge, Mozilla Firefox, Apple Safari ja Google Chrome selaimista niitä versioita, joita selaintoimittajat sillä hetkellä tukevat. Vanhempia versioita näistä selaimista ei testata systemaattisesti. Atostek ID tukee Apple Mail, Outlook ja Thunderbird sähköpostisovelluksia salauksen ja allekirjoituksen osalta. Ohjelmisto tukee Adobe Acrobat ja PDF-XChange ohjelmistoja PDF-dokumentin allekirjoituksen osalta. Atostek ID on saatavilla suomeksi, ruotsiksi ja englanniksi.

2.2.1. Atostek ID -ohjelman asentaminen

Asentaaksesi Atostek ID -ohjelman, toimi seuraavien ohjeiden mukaan:

1. Siirry sivulle https://dvv.fi/kortinlukijaohjelmisto tai https://downloads.ehoito.fi.
2. Valitse oikean käyttöjärjestelmän ajuri ja lataa se.

3. Avaa ladattu asennuspaketti ja suorita asennus. Katso tarvittaessa apua Atostek ID asennusohjeesta.



Kuva 1. Atostek ID -ohjelma.

Asennuksen jälkeen Atostek ID -sovellus löytyy macOS:n tilavalikosta. Saadaksesi ohjelman esiin valitse vihreä Atostek ID -kuvake hiiren oikealla painikkeella (kuva 1). Ohjelman logo on punainen, jos yhtään kortinlukijaa ei ole yhdistetty. Ohjelman logo on keltainen, jos yhtään korttia ei ole yhdistetty. Ohjelman logo on vihreä, jos kortti on yhdistetty ja sen tiedot luettu onnistuneesti. Logossa ilmaistaan myös tilanteet, joissa kortin tietojen lukeminen on kesken tai ohjelma on virheellisessä tilassa.

Mikäli saat Atostek ID -sovellukselta virheilmoituksia heti asennuksen jälkeen, tarkistathan, ettei sinulla ole toista kortinlukijaohjelmistoa samaan aikaan asennettuna. Digi- ja väestötietoviraston aikaisempi kortinlukijaohjelmisto voi haitata Atostek ID -ohjelmiston toimintaa, jos niitä käytetään yhtä aikaa.

Sovellus on tämän jälkeen täysin valmis käytettäväksi.

2.2.2. Atostek ID -ohjelman poistaminen

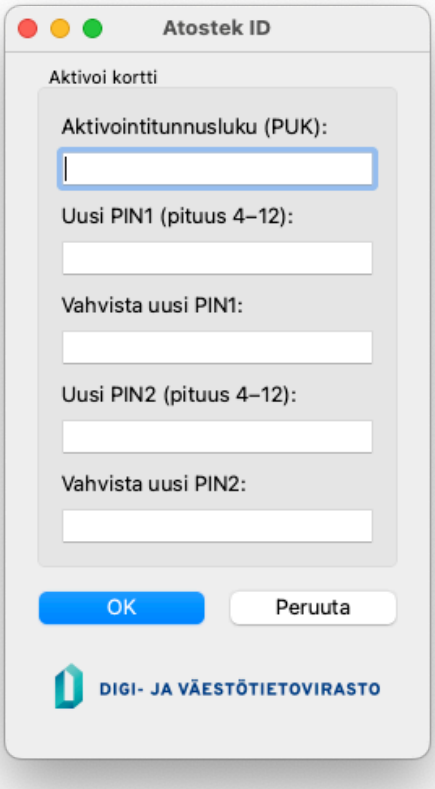
Atostek ID:n asennuksen yhteydessä asennetaan myös erillinen poisto-ohjelma. Poistaaksesi Atostek ID:n, avaa *Uninstall Atostek ID.app* Ohjelmat-kansiosta ja anna salasanasi pyydettäessä.

2.3. Kortin aktivoiminen

Aktivoi korttisi seuraavien ohjeiden mukaan:

1. Yhdistä kortinlukija tietokoneeseen ja laita kortti kortinlukijaan.

2. Jos korttia ei ole koskaan aktivoitu, näyttää sovellus kortin aktivointi-ikkunan automaattisesti. Riittää, että kortti aktivoidaan kerran. Jos aktivointi-ikkunaa ei näytetä, valitse valikosta *"Aktivoi kortti"*.
3. Anna avautuvassa ikkunassa (kuva 2) aktivointitunnusluku (PUK). Aktivointitunnusluku on toimitettu sinulle erillisessä kirjeessä kortin tilaamisen jälkeen.
4. Aseta kortille tunnistautumisvarmenteen tunnusluku (PIN1) ja allekirjoitusvarmenteen tunnusluku (PIN2). Ikkunassa ilmoitetaan tunnuslukujen minimi- ja maksimipituudet. Tämän jälkeen voit painaa *OK*. Aktivoinnin onnistumisesta tai epäonnistumisesta ilmoitetaan erillisessä ikkunassa.



Kuva 2. Kortin aktivointi.

Huomaathan, että sekä PIN1- että PIN2-tunnusluku on asetettava, jotta kortti aktivoituu toimintakuntoon. Kortin tunnuslukujen minimi- ja maksimipituudet vaihtelevat korttityypin ja korttisukupolven mukaan, joten vaaditut pituudet voivat olla erilaiset eri korteillasi. Kortin aktivointi riittää suorittaa vain kerran. Jos olet aktivoinut kortin toisella laitteella tai ohjelmistolla, sinun ei tarvitse aktivoida korttia uudelleen.

Huomaathan, että korttia ei voida toistaiseksi aktivoida käyttämällä NFC-lukijaa, sillä Atostek ID tukee suojatun NFC-yhteyden muodostamisessa vain kortin PIN1-koodin käyttöä. PIN1-koodia ei voida käyttää NFC-yhteyden muodostamiseen ennen kuin se on asetettu aktivoinnin yhteydessä.

Huom! Aktivointitunnusluvun syöttäminen väärin viisi kertaa peräkkäin lukitsee aktivointitunnusluvun. Tämän jälkeen korttia ei voida enää aktivoida tai lukkiutuneita PIN-koodeja avata. Jo aiemmin asetetut PIN-koodit ja niiden myötä allekirjoitus toimivat, vaikka aktivointitunnusluku menisi myöhemmin lukkoon. Aktivointitunnuslukua ei voida avata, vaan toimivan aktivointitunnusluvun saaminen vaatii uuden kortin tilaamisen. Ohjelma varoittaa joka kerta, kun aktivointitunnusluku on syötetty väärin ja ilmoittaa jäljellä olevat syöttökerrat ennen tunnusluvun lukkitumista.

Huom! Uudemmilla kansalaisvarmennekorteilla on käytössään PUK-koodista erillinen 7-merkkinen aktivointitunnusluku, jolla kortti aktivoidaan käyttöönoton yhteydessä. Näillä korteilla on lisäksi 8-merkkinen avaustunnusluku (PUK-koodi), jolla kortin voi aktivoida, mikäli aktivointitunnusluku on mennyt lukkoon. **Ole tarkkana, kumpaa tunnuslukua Atostek ID:n aktivointidialogi kysyy.** Avaustunnusluvulla voi myös avata kortin PIN-koodit, jos ne ovat menneet lukkoon liian monen virheellisen PIN-koodin syöttämisen seurauksena. Avaustunnusluku pitää noutaa erikseen paikallisilta viranomaisilta. Tarkista ajantasaiset ohjeet Digi- ja väestötietoviraston sivuilta.

3. Sähköinen tunnistautuminen ja sähköinen allekirjoitus

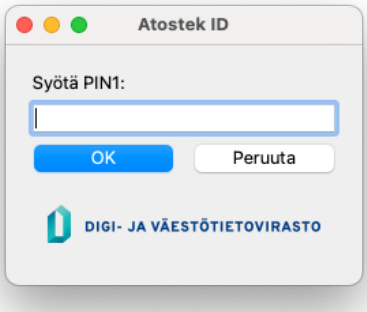
Tässä luvussa kerrotaan, miten voit tunnistautua varmennekortillasi Atostek ID -sovellusta hyödyntäen sellaiseen palveluun, joka on yhteensopiva Atostek ID -ohjelmiston kanssa. Tässä luvussa kerrotaan myös, miten sähköinen allekirjoitus tehdään Atostek ID -sovelluksen avulla. Tutustuthan tarvittaessa myös sen palvelun tai sovelluksen, johon olet tunnistautumassa tai suorittamassa allekirjoitusta, käyttöohjeisiin.

Tässä luvussa on kuvattu tarkemmin muutamia yleisimpiä käyttötapauksia tunnistautumiseen ja allekirjoitukseen liittyen. Kaikkia mahdollisia palveluita ei ole kuvattu tässä ohjeessa, eivätkä kaikki tässä kuvatut käyttötapaukset koske kaikkia käyttäjiä. Tässä luvussa kuvataan vain tunnistautumisen ja allekirjoituksen toiminnallisuus. Seuraavassa luvussa kuvataan tarkemmin ohjelmiston muita toiminnallisuuksia.

3.1. Sähköinen tunnistautuminen

Käyttäjä voi tunnistautua sähköisesti varmennekorttinsa tunnistautumisvarmenteella palveluun, joka on yhteensopiva Atostek ID -ohjelmiston kanssa. Tunnistauduttaessa käyttäjän täytyy syöttää korttinsa PIN1-koodi.

Tunnistautumista varten aseta kortti kortinlukijaan ja kortinlukija kiinni tietokoneeseen, tarkista että Atostek ID -ohjelma on käynnissä (kuva 1) ja käynnistä sisäänkirjautuminen varsinaiseen palveluun. Palvelun toimittaja tarjoaa tarkemmat ohjeet kirjautumiseen. Palvelu kutsuu Atostek ID -ohjelmistoa, minkä jälkeen Atostek ID pyytää PIN1-tunnuslukua (kuva 3). Tunnuslukua kysyttäessä voi näkyä myös macOS:n oma tunnuslukuikkuna (ilman Atostekin ja DVV:n logoja). Tunnuslukuikkunat eroavat ylipäätään hieman sen mukaan, mitä rajapintaa käyttäen tunnistautuminen suoritetaan. Jos varmennekortti on vanhenemassa kahden kuukauden sisällä, Atostek ID ilmoittaa tästä tunnistautumisen yhteydessä.



Kuva 3. Käyttäjän tunnistaminen tunnistautumisvarmenteen ja PIN1-koodin avulla. Tunnistautumisen yhteydessä voi myös näkyä macOS:n oma tunnuslukukyselyikkuna.

3.1.1. mTLS-tunnistautuminen

Tunnistautuminen voidaan tehdä kortin tunnistautumisvarmennetta käyttäen mTLS-tunnistautumisena (mutual TLS) selaimessa. Tällöin hyödynnetään Atostek ID TokenDriver -moduulia, joka asentuu automaattisesti Atostek ID macOS-version asennuksen yhteydessä. Atostek ID TokenDriver -moduulista voi lukea tarkemmin Atostek ID -ohjelmiston integraatio-ohjeesta.

Tätä tunnistautumistyyppiä käytetään esimerkiksi julkishallinnon asiointipalveluiden yhteydessä (**suomi.fi-tunnistus**). Tunnistautuaksesi palveluun liitä kortinlukija tietokoneeseen, aseta kortti lukijaan ja aloita tunnistautuminen selaimessa. Sinulta kysytään korttisi tunnistautumisvarmenteen tunnusluku eli kortin PIN1-koodi. Tämän jälkeen tunnistautuminen on valmis ja sinut ohjataan palveluun. Ongelmatilanteissa perehdy ensin tämän ohjeen lukuun 5, jossa on kuvattu ratkaisuja yleisiin ongelmatilanteisiin.

3.1.2. SCS-rajapinnan kautta tunnistautuminen

Tunnistautuminen voidaan tehdä myös esimerkiksi Atostek ID -sovelluksen SCS-rajapintaa (Signature Creation Service) hyödyntäen. SCS on Digi- ja väestötietoviraston määrittelemä HTTPS-rajapinta. Sitä käytetäänkin siis erityisesti web-palveluihin tunnistauduttaessa. SCS-rajapintaa käyttävät esimerkiksi monet potilastietojärjestelmät.

SCS-rajapinnan käyttö ei erityisesti näy käyttäjälle sovellusta käytettäessä. Tunnistautumista varten sinun tulee liittää kortinlukija koneeseen ja kortti lukijaan. Sen jälkeen voit aloittaa tunnistautumisen järjestelmään. Tämän jälkeen Atostek ID pyytää sinua valitsemaan tunnistautumisessa käytettävän varmenteen. Kun varmenne on valittu, pyydetään sinua antamaan sitä vastaava tunnusluku eli PIN-koodi. Tämän jälkeen tunnistautuminen on valmis ja sinut ohjataan palveluun.

3.1.3. Atostek ERA -järjestelmän käyttäminen

Huomaathan, että tämä käyttötapaus on tarkoitettu vain niille sosiaali- ja terveydenhuollon käyttäjille, jotka on rekisteröity käyttämään ERA-järjestelmää. Mikäli organisaatiosi ei ole ohjeistanut sinua käyttämään Atostekin ERA-järjestelmää tai olet kansalaiskäyttäjä (käytät henkilökorttia), ei tämä käyttötapaus koske sinua. Näissä tapauksissa voit jättää tämän osan ohjeistuksesta lukematta. Sinun ei kuulu kirjautua ERA-järjestelmään, jos sinua ei ole erikseen ohjeistettu tekemään niin.

Voit kirjautua eli tunnistautua Atostekin ERA-järjestelmään Atostek ID -sovellusta käyttäen. Siirry selaimella ERA-järjestelmän kirjautumissivulle tai avaa Atostek ID -sovelluksen valikosta *”Kirjaudu ERA-järjestelmään”* (Kuva 1), jolloin kirjautumissivu avataan oletusselaimessa. Huomaathan, että toiminto näkyy sovelluksen valikossa vain, jos asetus *”Näytä ’Kirjaudu ERA*-järjestelmään’ *-valinta ponnahdusvalikossa”* on asetettu päälle asetuksista tai asennuksen yhteydessä. Tällä toiminnolla voidaan kirjautua ERA-järjestelmään helposti myös silloin, kun Atostek ID ei saa yhteyttä oletusportteihin, koska toiminto avaa kirjautumissivun Atostek ID -sovelluksen porttitiedolla. Tällainen tilanne voi olla esimerkiksi silloin, kun samalla koneella on useampi käyttäjä kirjautuneena.

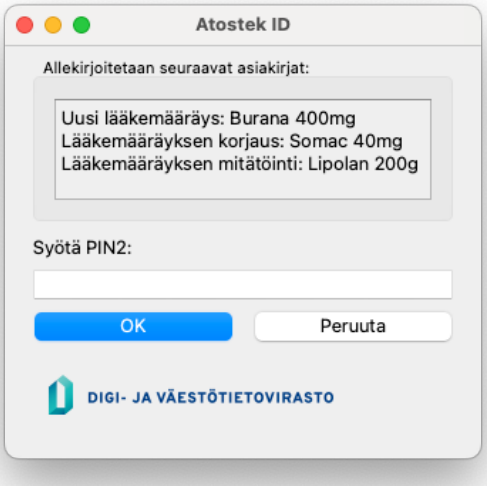
Onnistunut tunnistautuminen ERA-järjestelmään vaatii sen, että sinut on konfiguroitu järjestelmään etukäteen. Tunnistauduttaessa kortinlukijan tulee olla kiinni koneessa ja kortin lukijassa. Kun tunnistautuminen on aloitettu, kysyy Atostek ID sinulta kortin PIN1-koodin. Tunnistautumisen onnistuessa sinut ohjataan palveluun.

ERA-järjestelmä käyttää Atostek ID -sovelluksen erasmartcard.ehoito.fi-rajapintaa. Voit testata rajapinnan toimintaa avaamalla sovelluksen valikosta *”Diagnostiikka”* ja sen jälkeen *”Avaa Atostek ID:n testisivu”*. Se avaa oletusselaimessa rajapinnan testisivun, jossa lukee *”Test page loaded OK”*.

3.2. Sähköinen allekirjoitus

Käyttäjä voi suorittaa varmennekorttinsa allekirjoitusvarmenteella sähköisen allekirjoituksen palveluun tai sovellukseen, joka on yhteensopiva Atostek ID -ohjelmiston kanssa. Allekirjoitettaessa käyttäjän täytyy syöttää korttinsa PIN2-koodi.

Allekirjoitusta varten aseta kortti kortinlukijaan ja kortinlukija kiinni tietokoneeseen sekä tarkista, että Atostek ID -ohjelma on käynnissä (kuva 1). Tutustu tarvittaessa palvelun tai sovelluksen tarjoajan ohjeisiin siitä, miten sähköinen allekirjoitus tehdään kyseisessä palvelussa tai sovelluksessa. Allekirjoitettaessa palvelu tai sovellus kutsuu Atostek ID -ohjelmistoa, minkä jälkeen Atostek ID pyytää PIN2-tunnuslukua (kuva 4). Tunnuslukua kysyttäessä voi näkyä myös macOS:n oma tunnuslukuikkuna (ilman Atostekin ja DVV:n logoja). Tunnuslukuikkunat eroavat ylipäätään hieman sen mukaan, mitä rajapintaa käyttäen allekirjoitus suoritetaan.



Kuva 4. Sähköinen allekirjoitus PIN2-koodin avulla. Allekirjoituksen yhteydessä voi myös näkyä macOS:n oma tunnuslukukyselyikkuna.

3.2.1. PDF-dokumenttien allekirjoittaminen (Adobe Acrobat)

PDF-dokumentti voidaan allekirjoittaa Adobe Acrobat -sovelluksella. Tällöin hyödynnetään Atostek ID TokenDriver -moduulia, joka asentuu automaattisesti Atostek ID macOS -version asennuksen yhteydessä. Atostek ID TokenDriver -moduulista voi lukea tarkemmin Atostek ID -ohjelmiston integraatio-ohjeesta.

Adobella allekirjoitettaessa valitse allekirjoitettava dokumentti ja työkaluvalikosta varmenteen käyttäminen. Voit valita avautuvasta valikosta digitaalisen allekirjoittamisen, jolloin sinun tulee hiirellä piirtäen lisätä allekirjoitus haluamaasi kohtaan dokumenttia. Tämän jälkeen sinua pyydetään valitsemaan käytettävä varmenne. Varmenteen valitsemisen jälkeen sinun tulee syöttää avautuvaan ikkunaan varmenteen tunnusluku eli PIN-koodi. Tämän jälkeen kortti suorittaa allekirjoituksen, joka liitetään osaksi dokumenttia.

3.2.2. SCS-rajapinnan kautta allekirjoittaminen

Allekirjoitus voidaan tehdä myös esimerkiksi Atostek ID -sovelluksen SCS-rajapintaa (Signature Creation Service) hyödyntäen. SCS on Digi- ja väestötietoviraston määrittelemä HTTPS-rajapinta. Sitä käytetäänkin siis erityisesti web-palveluissa tehtävissä allekirjoituksissa. SCS-rajapintaa käyttävät esimerkiksi monet potilastietojärjestelmät.

SCS-rajapinnan käyttö ei erityisesti näy käyttäjälle sovellusta käytettäessä. Allekirjoitusta varten sinun tulee liittää kortinlukija koneeseen ja kortti lukijaan. Sen jälkeen voit aloittaa allekirjoittamisen. Tämän jälkeen Atostek ID pyytää sinua valitsemaan tunnistautumisessa käytettävän varmenteen. Kun varmenne on valittu, pyydetään sinua antamaan sitä vastaava tunnusluku eli PIN-koodi. Tämän jälkeen allekirjoitus on valmis ja välitetään sovellukselta sitä pyytäneeseen palveluun.

3.2.3. Atostek ERA -järjestelmän allekirjoitus

Huomaathan, että tämä käyttötapaus on tarkoitettu vain niille sosiaali- ja terveydenhuollon käyttäjille, jotka on rekisteröity käyttämään ERA-järjestelmää. Mikäli organisaatiosi ei ole ohjeistanut sinua käyttämään Atostekin ERA-järjestelmää tai olet kansalaiskäyttäjä (käytät henkilökorttia), ei tämä käyttötapaus koske sinua. Näissä tapauksissa voit jättää tämän osan ohjeistuksesta lukematta. Sinun ei kuulu kirjautua ERA-järjestelmään, jos sinua ei ole erikseen ohjeistettu tekemään niin.

Voit suorittaa allekirjoituksen, esimerkiksi reseptin allekirjoituksen, Atostekin ERA-järjestelmässä Atostek ID -sovellusta käyttäen, kun olet tunnistautunut ensin järjestelmään. Allekirjoitettaessa kortinlukijan tulee olla kiinni koneessa ja kortin lukijassa. Kun allekirjoittaminen on aloitettu, kysyy Atostek ID sinulta kortin PIN2-koodin. Tämän jälkeen kortti suorittaa allekirjoituksen ja palauttaa sen ERA-järjestelmälle.

ERA-järjestelmä käyttää Atostek ID -sovelluksen erasmartcard.ehoito.fi-rajapintaa. Voit testata rajapinnan toimintaa avaamalla sovelluksen valikosta *”Diagnostiikka”* ja sen jälkeen *”Avaa Atostek ID:n testisivu”*. Se avaa oletusselaimessa rajapinnan testisivun, jossa lukee *”Test page loaded OK”*.

4. Toiminnallisuus

Tässä luvussa esitellään Atostek ID -ohjelman tärkeimmät toiminnallisuudet. Niitä ovat esimerkiksi tunnuslukujen vaihtaminen sekä avaaminen. Niiden lisäksi esitellään sovellukseen liittyvät asetukset ja niiden muuttaminen.

4.1. Käynnistäminen ja sulkeminen

Atostek ID -ohjelma käynnistyy automaattisesti, kun olet asentanut sovelluksen ja kirjaudut käyttöjärjestelmään. Voit ottaa automaattisen käynnistymisen halutessasi pois päältä sovelluksen asetusten kautta.

Kun haluat sulkea sovelluksen, valitse valikosta *”Sulje”*. Tämä sulkee Atostek ID -sovelluksen kokonaan. Tähän ei yleensä ole tarvetta. Huomaathan, että palveluihin voi enää tämän jälkeen tunnistautua tai allekirjoituksia suorittaa esimerkiksi SCS-rajapinnan tai erasmartcard.ehoito.fi-rajapinnan kautta ennen kuin sovellus on käynnistetty uudelleen. Ohjelma löytyy käynnistysvalikosta nimellä *”Atostek ID”* ja sen voi sieltä tarvittaessa käynnistää uudelleen.

4.2. Sovelluksen tiedot ja käyttöohje

Atostek ID -sovelluksen tiedot, kuten versionumero ja HTTPS-palvelinten käyttämät portit, voidaan lukea sovelluksen Tietoa-näkymästä. Sen saa avattua, kun valitsee sovelluksen valikosta *”Tietoa”*. Ikkunan ylälaidassa näkyy sovelluksen versionumero. Avoimet ja suljetut portit sekä varmenteeseen liittyvät tiedot koskevat erasmartcard.ehoito.fi rajapintaa. Näiden lisäksi näkymässä kerrotaan, saadaanko SCS-rajapinnan porttiin 53952 otettua yhteys. Yhteyden ottaminen ei onnistu, jos jokin toinen sovellus varaa porttia. Näin voi käydä esimerkiksi silloin, kun koneella on asennettuna ja käynnissä DigiSign-kortinlukijaohjelmisto, joka avaa oman vastaavan palvelunsa kyseiseen porttiin. SCS-rajapinnan porttiongelmat näkyvät myös Atostek ID -sovelluksen logossa huutomerkillisenä kolmiona.

Sovelluksen käyttöohjeen saa avattua sovelluksen kautta valitsemalla valikosta *”Näytä käyttöohje”*. Käyttöohje avataan sovelluksen kielellä (suomi, ruotsi tai englanti). Ohjelmiston käyttöohjeet, asennusohjeet ja muut ohjedokumentit ovat ladattavissa myös sekä Digi- ja väestötietoviraston kortinlukijaohjelmiston sivuilta että Atostekin omalta ajurisivulta.

4.3. PIN-koodien vaihtaminen ja lukittuneiden koodien avaaminen

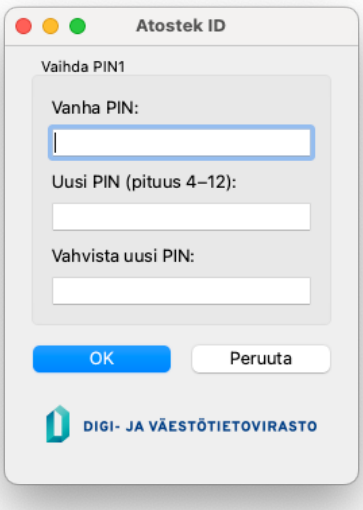
Voit vaihtaa PIN-koodeja valitsemalla valikosta *”Vaihda PIN1”* tai *”Vaihda PIN2”* ja syöttämällä sitten nykyisen PIN-koodin sekä uuden PIN-koodin kahteen kertaan (kuva 5).

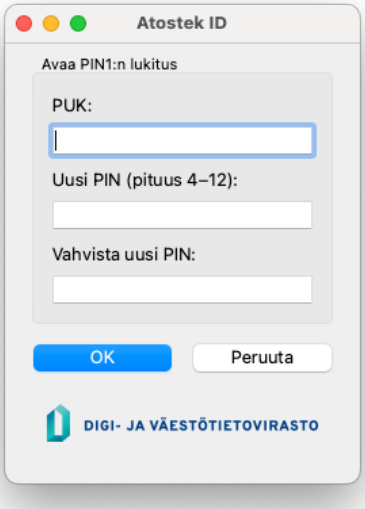
Voit avata lukkiutuneita PIN-koodeja valitsemalla valikosta *”Avaa PIN1-koodi PUK-koodilla”* tai *”Avaa PIN2-koodi PUK-koodilla”* ja syöttämällä sitten PUK-koodin eli aktivointitunnusluvun ja uuden PIN-koodin kahteen kertaan (kuva 6). PUK-koodi eli aktivointitunnusluku toimitetaan varmennekortin mukana.

Kortin voi myös aktivoida valikon *”Aktivoi kortti”*-valinnan kautta. Sovellus pyytää käyttäjää aktivoimaan kortin, kun lukijaan syötetään aktivoimaton kortti, jolloin käyttäjän ei tarvitse aloittaa aktivointia itse valikon kautta.

Huom! PIN-koodien käsittelyn aikana varmennekortin tulee olla kortinlukijassa. Sekä PIN1- että PIN2-koodit on avattava, jotta kortti aktivoituu toimintakuntoon. Myös kortin aktivointi avaa molemmat tunnusluvut.

Huom! Aktivointitunnusluvun syöttäminen väärin viisi kertaa peräkkäin lukitsee aktivointitunnusluvun. Tämän jälkeen korttia ei voida enää aktivoida tai lukkiutuneita PIN-koodeja avata. Jo aiemmin asetetut PIN-koodit toimivat, vaikka aktivointitunnusluku menisi myöhemmin lukkoon. Aktivointitunnuslukua ei voida avata, vaan toimivan aktivointitunnusluvun saaminen vaatii uuden kortin tilaamisen. Ohjelma varoittaa joka kerta, kun aktivointitunnusluku on syötetty väärin ja ilmoittaa jäljellä olevat syöttökerrat ennen tunnusluvun lukkitumista.





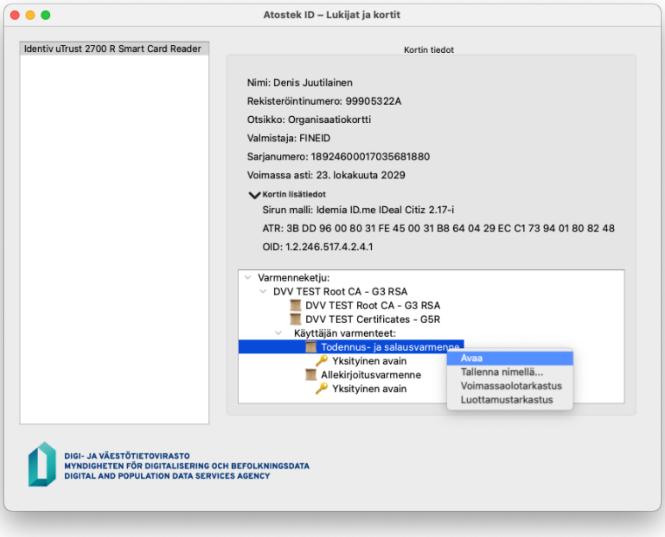
Kuvat 5 ja 6. PIN-koodin vaihto ja PIN-koodin lukituksen avaaminen.

4.4. Lukijat ja kortit

Koneeseen liitettyjä kortinlukijoita ja kortteja voi tarkastella avaamalla sovelluksen valikosta *”Lukijat ja kortit”*. Avautuvassa ikkunassa (kuva 7) näkyy vasemmassa laidassa tietokoneeseen liitetyt kortinlukijat allekkain listattuna. NFC-lukijoiden osalta listauksessa näkyy kaksi eri lukijaa, jos lukijassa on erikseen sekä NFC- että normaali USB-lukija (kontaktillinen lukija). Lukijan voi valita aktiiviseksi klikkaamalla sen nimeä ikkunan vasemman puolen listauksessa.

Kun lukija on valittu, näytetään ikkunan oikealla puolella kortinlukijaan liitetyn kortin tiedot, esimerkiksi nimitiedot ja voimassaolopäivämäärä. Ikkunassa näkyy myös kortin varmenneketju puumaisesti esitettynä juurivarmenteesta välivarmenteiden kautta käyttäjän varmenteisiin. Käyttäjän varmenteisiin liittyen näytetään sekä varmenteen julkinen osa että siihen liittyvä yksityinen avain. Varmenteiden julkiset osat voidaan avata tai tallentaa, kun varmennetta klikataan näkymässä hiiren oikealla painikkeella. Tällöin avautuu lisävalikko, jossa on vaihtoehtoina ”Avaa”, ”Tallenna nimellä…”, ”Voimassaolotarkastus”, sekä ”Luottamustarkastus”. Vaihtoehdolla ”Voimassaolotarkastus” voidaan tarkastaa varmenteiden voimassaolopäivämäärät ja sulkulistat (CRL, OCSP). Vaihtoehdolla ”Luottamustarkastus” voidaan tarkastaa varmenneketjun luotettavuus. Jos varmenneketjuun ei luoteta

siitä syystä, että myöntäjävarmenteita puuttuu varmennesäilöstä, voidaan ne lisätä säilöön käyttäjän erillisellä hyväksynnällä. Myöntäjävarmenteiden lisääminen voi vaatia järjestelmänvalvojan oikeudet, jolloin niitä kysytään käyttäjältä erikseen. Luottamustarkastus on tuettu vain Windowsilla ja macOS:lla.



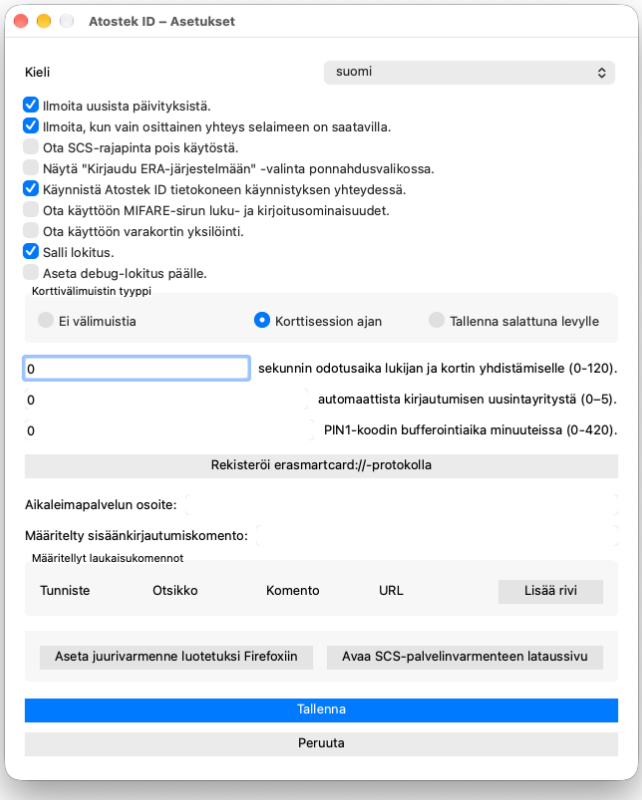
Kuva 7. Lukijat ja kortit -näkymä.

NFC-lukijaa käytettäessä käyttäjältä kysytään kortin PIN1-koodi, kun kortti tuodaan lukijaan. Tunnuslukua käytetään turvatun NFC-yhteyden muodostamiseen. Jos kortti poistetaan NFC-lukijasta, on käyttäjällä 10 sekuntia aikaa tuoda kortti takaisin, ennen kuin PIN1-koodi täytyy syöttää uudestaan yhteyden muodostamiseksi.

Atostek ID TokenDriver tallentaa käyttäjän varmenteet macOS:n avainnippuun, jos lukijassa oleva kortti paritetaan macOS-laitteen käyttäjän kanssa.

4.5. Asetukset

Voit muokata ohjelman asetuksia valitsemalla ohjelman valikosta *”Asetukset”*. Asetuksissa (kuva 8) voit esimerkiksi vaihtaa ohjelman kielen sekä muokata esimerkiksi lokitukseen liittyviä asetuksia. Huomaa, että muutokset tulevat voimaan vasta asetusten tallentamisen jälkeen. Asetukset käydään läpi yksityiskohtaisesti omissa alaotsikoissaan.



Kuva 8. Asetukset.

4.5.1. Kieli

"**Kieli**"-asetuksen avulla voit vaihtaa Atostek ID -sovelluksen kielen. Tuettuja kieliä ovat tällä hetkellä suomi, ruotsi ja englanti.

4.5.2. Ilmoita uusista päivityksistä

”Ilmoita uusista päivityksistä”-asetuksen avulla voidaan ottaa käyttöön Atostek ID:n ilmoitukset uusista versioista. Tällöin Atostek ID lähettää erillisin ilmoituksen siitä, että uusi versio on ladattavissa ja asennettavissa.

4.5.3. Ilmoita, kun vain osittainen yhteys selaimeen on saatavilla

”Ilmoita, kun vain osittainen yhteys selaimeen on saatavilla”-asetuksen avulla voidaan ottaa käyttöön Atostek ID:n ilmoitukset osittaisista yhteyksistä, kun sovelluksen erasmartcard.ehoito.fi-rajapinta ei käynnisty oletusportteihin ja käytettävä järjestelmä pitää avata käyttämällä Atostek ID:n laukaisukomentoa. Tämä asetus liittyy vain erasmartcard.ehoito.fi-rajapinnan käyttöön.

4.5.4. Ota SCS-rajapinta pois käytöstä

”Ota SCS-rajapinta pois käytöstä” -asetuksen avulla voidaan ottaa käyttöön tai poistaa käytöstä tuotteen SCS-rajapinta. Rajapinta on oletuksena käytössä eli sovellus käynnistää sen ja siihen liittyvän CA-varmenteen latauspalvelun käynnistyessään. Tämä HTTPS-rajapinta vaatii käyttöönsä määritysten (https://dvv.fi/fineid-maaritykset) mukaisen portin, joka saattaa olla varattuna esimerkiksi toisen kortinlukijaohjelmiston toimesta, jos se toteuttaa saman rajapinnan. Tällä asetuksella SCS-rajapinta voidaan ottaa pois käytöstä, mikäli halutaan vapauttaa sen varaama portti jonkin toisen sovelluksen käyttöön ja SCS-rajapintaa ei haluta käyttää Atostek ID -sovelluksen kautta. Rajapinnan poistaminen käytöstä tarkoittaa sitä, että Atostek ID ei käynnistä rajapintaa ollenkaan, eikä siten esimerkiksi varoita, jos jokin muu ohjelma käyttää rajapinnan tarvitsemia portteja. Huomaathan, että rajapinnan poistaminen käytöstä ilman korvaavia toimia estää tunnistautumiset ja allekirjoitukset järjestelmissä, jotka hyödyntävät rajapintaa Atostek ID:n kautta. Otathan rajapinnan siis pois käytöstä vain, jos olet varma, että et tarvitse sitä käyttötapauksessasi. Katso tarvittaessa myös asetus MULTIDESKTOPMODE.

4.5.5. Näytä ”Kirjaudu ERA-järjestelmään” -valinta ponnahdusvalikossa

”Näytä "Kirjaudu ERA-järjestelmään" -valinta ponnahdusvalikossa” -asetuksen avulla voidaan näyttäätai piilottaa valikossa Atostekin ERA-järjestelmän kirjautumislinkki. Huomaathan, että ERA-järjestelmän käyttö koskee vain niitä sosiaali- ja terveydenhuollon käyttäjiä, jotka on konfiguroitu käyttämään ERA-järjestelmää. Asetus on oletuksena pois päältä eli ponnahdusvalikossa ei ole kirjautumislinkkiä.

4.5.6. Käynnistä Atostek ID tietokoneen käynnistyksen yhteydessä

”Käynnistä Atostek ID tietokoneen käynnistyksen yhteydessä”-asetuksen avulla sovelluksen automaattinen käynnistyminen voidaan ottaa pois päältä tai asettaa päälle. Asetus vaatii admin-oikeudet, joita kysytään käyttäjältä asetuksen tallentamisen jälkeen. Sovellus sammuu asetuksen muuttamisen ajaksi ja käynnistyy sitten automaattisesti uudestaan.

4.5.7. Ota käyttöön MIFARE-sirun luku- ja kirjoitusominaisuudet

”Ota käyttöön MIFARE-sirun luku- ja kirjoitusominaisuudet”-asetuksen avulla sovelluksen valikkoon saadaan näkyviin valinta ”Mifare”, joka avaa erillisen MIFARE-sivun hallinnointinäkymän. Perehdythän MIFARE-sirun lukemisen ja kirjoittamisen ohjeisiin ennen kuin yrität lukemista tai kirjoittamista. Tarvitset sirun käsittelyä varten NFC-lukijan.

4.5.8. Ota käyttöön varakortin yksilöinti

”Ota käyttöön varakortin yksilöinti”-asetuksen avulla sovelluksen valikkoon saadaan näkyviin valinta ”Varakortti”, joka avaa varakorttien yksilöintinäkymän. Tätä näkymää käyttävät lähinnä rekisteröintipisteiden työntekijät, eikä käyttäjien tarvitse valita tätä asetusta voidakseen käyttää heille myönnettyjä varakortteja. Varakorttien rekisteröintipisteitä varten muut Atostek ID:n asetukset, kuten *AIDISURL*, ovat oletusarvoiltaan jo varakorttien yksilöintiin soveltuvat, eikä niitä tarvitse lähtökohtaisesti muuttaa. Tarkemmat ohjeet varakorttien yksilöinnin prosesseihin tulevat Vartti-järjestelmän puolelta.

Jos työaseman korttiyhteyksiin on konfiguroitu aikakatkaisu, tulee varmistaa, että sen aika-arvo on tarpeeksi suuri. Kortti voi vaatia pitkän ajan avainten generointiin yksilöinnin aikana, eikä korttiyhteyttä pidä sen aikana katkaista. Jotta yksilöinti onnistuisi suositellaan aikakatkaisun arvoksi vähintään 2 minuuttia.

4.5.9. Salli lokitus

”Salli lokitus”-asetuksen avulla sovelluksen tekemä lokitus voidaan ottaa kokonaan pois päältä. Lokituksen estäminen ei poista aikaisempaa lokia, vaan estää vain uusien lokiviestien kirjaamisen.

4.5.10. Aseta debug-lokitus päälle

"Aseta debug-lokitus päälle"-asetuksen avulla voit valita, kirjataanko virhelokiin DEBUG-tason lokiviestejä vai pelkästään INFO-, WARNING- ja ERROR-tason viestejä.

4.5.11. Korttivälimuistin tyyppi

”Korttivälimuistin tyyppi”-asetuksen avulla voit määrittää, tallentaako Atostek ID kortilta lukemiaan tiedostoja välimuistiin. Korttivälimuistin vaihtoehtoja on kolme: ”Ei välimuistia”, ”Korttisession ajan” ja ”Tallenna salattuna levylle”. Vaihtoehdolla ”Ei välimuistia” Atostek ID ei tallenna kortilta lukemiaan tiedostoja erilliseen välimuistiin, vaan tiedostot luetaan kortilta aina, kun niiden sisältöä tarvitaan. Vaihtoehto ”Korttisession ajan” on oletuksena valittu, ja tällöin kortilta luetut tiedostot säilötään Atostek ID:n sisäisessä välimuistissa niin kauan, kun kortti on lukijassa. Kortilta tallennetut tiedot poistuvat välimuistista, kun kortti irrotetaan lukijasta tai kun Atostek ID sammutetaan. Vaihtoehdossa ”Tallenna salattuna levylle” korttivälimuisti säilyy salattuna käyttäjän hakemistossa. Korttivälimuisti ei siis tyhjene, vaikka kortti poistetaan lukijasta tai Atostek ID sammutetaan. Jos asetus vaihdetaan tästä arvosta muihin arvoihin, levylle tallennettu korttivälimuisti poistetaan.

Korttivälimuistin käyttö parantaa Atostek ID:n toimintanopeutta, sillä se vähentää toimintaa hidastavaa korttikommunikaatiota. Isoin vaikutus pitkäaikaisessa käytössä saavutetaan, kun korttivälimuisti tallennetaan salattuna levylle.

4.5.12. Sekunnin odotusaika lukijan ja kortin yhdistämiselle

”Sekunnin odotusaika lukijan ja kortin yhdistämiselle"-asetuksen avulla voit määrittää sekuntimäärän, jonka aikana yhdistämätön kortinlukija tai kortti tulee yhdistää, kun tunnistautuminen aloitetaan erasmartcard.ehoito.fi-rajapinnan kautta. Asetuksen ollessa 0 kirjautuminen epäonnistuu välittömästi, jos kortinlukija tai kortti puuttuu. Asetuksen maksimiarvo on 120 sekuntia. Tämä asetus liittyy vain erasmartcard.ehoito.fi-rajapinnan käyttöön.

4.5.13. Automaattista kirjautumisen uudelleenyritystä (0-5)

"Automaattista kirjautumisen uusintayritystä (0–5)"-asetuksen avulla voit määrittää, montako kertaa kirjautumista yritetään automaattisesti uudestaan, jos kirjautuminen epäonnistuu Alcor Micro -lukijan takia erasmartcard.ehoito.fi-rajapintaa käytettäessä. Asetuksen ollessa 0 jokaista uusintayritystä kysytään erikseen (kuitenkin yhteensä enintään kolme kertaa). Tämä asetus liittyy vain erasmartcard.ehoito.fi-rajapinnan käyttöön.

4.5.14. PIN1-koodin bufferointiaika minuuteissa (0-420)

”PIN1-koodin bufferointiaika minuuteissa (0-420)”-asetuksen avulla voit määrittää, kauanko Atostek ID pitää kortin PIN1-koodia muistissaan. Arvo annetaan minuuteissa väliltä 0-420, eli PIN1-koodia säilötään muistissa enintään seitsemän (7) tuntia. Asetuksen oletusarvo on 0 minuuttia, jolloin PIN1-koodia kysytään käyttäjältä joka kerta, kun sitä tarvitaan. Kun PIN1-koodi on muistissa, Atostek ID ei kysy sitä käyttäjältä vaan käyttää suoraan säilömäänsä arvoa. PIN1-koodi poistuu muistista, kun asetettu aikamäärä ylittyy, kortti poistuu lukijasta, kortti havaitsee väärän PIN1-koodin, PIN1-koodi vaihdetaan tai Atostek ID sammutetaan. Säilömisaika aloitetaan siitä hetkestä, kun annettu PIN1-koodi saadaan onnistuneesti verifioitua kortilla.

Huom! PIN1-koodin bufferoinnin käyttöönotto on käyttäjän tai organisaation oma päätös, ja tällöin bufferointiaika tulee määrittää mahdollisimman pieneksi käyttötapausten sallimissa rajoissa. Ota myös huomioon PIN1-koodin bufferoinnin tietoturvanäkökulmat päätöstä tehdessäsi.

Huom! Asetus toimii Atostek ID:n ulkoisten moduulien (TokenDriver, PKCS#11) kanssa vain, jos asetus *ENABLECUSTOMDIALOG* on tosi.

4.5.15. Rekisteröi erasmartcard://-protokolla

"Rekisteröi `erasmartcard://`-protokolla" -painikkeen avulla voit rekisteröidä Atostek ID -sovellukselle `erasmartcard://`-protokollan. Lisätietoa löytyy asennusohjeesta. Asetus vaatii admin-oikeudet, joita kysytään käyttäjältä asetuksen tallentamisen jälkeen. Sovellus sammuu asetuksen muuttamisen ajaksi ja käynnistyy sitten automaattisesti uudestaan. Tämä asetus liittyy vain erasmartcard.ehoito.fi-rajapinnan käyttöön.

4.5.16. Aikaleimapalvelun osoite

”Aikaleimapalvelun osoite”-kenttään voidaan määritellä aikaleimapalvelu, jota käytetään korkeamman tason allekirjoituksissa aikaleiman hakemiseen (esimerkiksi PDF-dokumentin allekirjoitus sovelluksen kautta PAdES-standardin tasoilla B-T, B-LT, B-LTA). Aikaleimapalvelun osoite määritellään kenttään kokonaisuudessaan, esimerkiksi https://aikaleimapalvelu.fi/ts. Huomaathan, että esimerkkinä annettu aikaleimapalvelu ei ole aito aikaleimapalvelu. Käytä tässä esimerkiksi organisaatiosi ohjeistamaa aikaleimapalvelua.

4.5.17. Määritelty sisäänkirjautumiskomento

”Määritelty sisäänkirjautumiskomento:”-kenttään voidaan määritellä selain, joka halutaan avata oletusselaimen sijaan silloin, kun käytetään laukaisukomentoa, jolle ei ole erikseen määritelty komentoa. Selain määritellään muodossa: *”<Polku selaimen sovellukseen>” {URL}* eli esimerkiksi *"/Applications/Google Chrome.app/Contents/MacOS/Google Chrome” {URL}.*

4.5.18. Määritellyt laukaisukomennot

”Määritellyt laukaisukomennot”-osion avulla voidaan lisätä Atostek ID -valikkoon uusia laukaisulinkkejä, joilla voidaan avata Atostek ID:tä hyödyntävä järjestelmä ja välittää Atostek ID:n erasmartcard.ehoito.fi-rajapinnan porttitieto. Tämä on erityisen tärkeää Citrix- ja RDP-ympäristöissä.

Laukaisukomennon tiedoissa komennon tunniste on arvo, jolla laukaisukomentoa voidaan hyödyntää esimerkiksi komentorivilaukaisussa.

Laukaisukomennon tiedoissa komennon otsikkoon määritellään valikossa näytettävä teksti.

Laukaisukomennon tiedoissa komentokenttään voidaan määritellä selain, joka halutaan avata komennon yhteydessä. Määrittely tapahtuu samaan tapaan kuin sisäänkirjautumiskomennossa.

Laukaisukomennon tiedoissa URL-kenttään tulee avattava osoite. Tässä kentässä voidaan antaa {PORT}-upotuksena sovelluksen erasmartcard.ehoito.fi-rajapinnan portti. Laukaisun yhteydessä Atostek ID korvaa {PORT}-tekstin Atostek ID:n porttitiedolla.

Esimerkki laukaisukomennosta:

- ”Tunniste”: edemo
- ”Otsikko”: Kirjaudu edemo-palveluun
- ”Komento”: "/Applications/Google Chrome.app/Contents/MacOS/Google Chrome" {URL}
- “URL”: https://edemo.atostek.com

4.5.19. Aseta juurivarmenne luotetuksi Firefoxiin

”Aseta juurivarmenne luotetuksi Firefoxiin”-painikkeen avulla voidaan lisätä SCS-rajapinnan itsegeneroitu juurivarmenne luotetuksi Firefox-selaimen varmennesäilöön automaattisesti. Tämä asetus liittyy vain SCS-rajapinnan käyttöön.

4.5.20. Avaa SCS-palvelinvarmenteen lataussivu

”Avaa SCS-palvelinvarmenteen lataussivu”-painikkeen avulla voidaan avata sivu, josta SCS-rajapinnan juurivarmenteen saa ladattua. Sivulla on myös ohjeet sille, miten juurivarmenne asetetaan luotetuksi Firefox-selaimella. Tämä asetus liittyy vain SCS-rajapinnan käyttöön.

4.5.21. Asetustiedoston parametri CLEANCERTSTOREONCARDREMOVAL

Voit käyttää asetusparametria *”CLEANCERTSTOREONCARDREMOVAL”* suoraan sovelluksen asetustiedostossa (*"/Users/<käyttäjänimi>/Library/Application Support/Atostek Oy/Atostek ID/AtostekID.ini"*). Asetuksen oletusarvo *”true”* tyhjää käyttäjän kortin varmenteet macOS:n varmennesäilöstä, kun kortti viedään pois lukijasta. Arvo *”false”* puolestaan säilyttää varmenteet säilössä. Huomaathan, että asetustiedosto tulee tallentaa ja Atostek ID käynnistää muutosten jälkeen uudelleen, jotta asetus astuu voimaan.

4.5.22. Asetustiedoston parametri EXCLUDEDREADERS

Voit käyttää asetusparametria *”EXCLUDEDREADERS”* suoraan sovelluksen asetustiedostossa (*"/Users/<käyttäjänimi>/Library/Application Support/Atostek Oy/Atostek ID/AtostekID.ini"*). Anna asetukselle merkkijonona lista lukijoista (Lukija1, Lukija2, Lukija3), jotka halutaan poistaa käytöstä. Tällöin Atostek ID ei huomioi kortteja näissä lukijoissa. Jos näkymässä ”Lukijat ja kortit” lukijan nimessä näkyy lopussa ylimääräisiä numeroita, jätä ne pois lukijan nimestä asetusta konfiguroitaessa. Jos lukijan nimenä näkyy esimerkiksi ”Windows Hello for Business 0”, käytä asetuksessa merkkijonoa ”Windows Hello for Business”. Asetus tukee jokerimerkkejä * (korvaa yhden tai useamman merkin) ja ? (korvaa yhden merkin). Esimerkiksi arvo ExcludedReaders=ACS* piilottaa kaikki lukijat, joiden nimi alkaa merkkijonolla ”ACS”. Huomaathan, että asetustiedosto tulee tallentaa ja Atostek ID käynnistää muutosten jälkeen uudelleen, jotta asetus astuu voimaan.

4.5.23. Asetustiedoston parametri EXCLUDEDCARDTYPES

Voit käyttää asetusparametria *”EXCLUDEDCARDTYPES”* suoraan sovelluksen asetustiedostossa (*"/Users/<käyttäjänimi>/Library/Application Support/Atostek Oy/Atostek ID/AtostekID.ini"*). Anna asetukselle merkkijonona lista korttityypeistä, jotka haluat hylätä. Sallitut tyypit ovat ORGANISAATIOKORTTI, AMMATTIKORTTI, HENKILOSTOKORTTI, HENKILOKORTTI, TOIMIJAKORTTI ja FINEID (varakortit). Tyyppien kirjainkoolla ei ole merkitystä. Huomaathan, että asetustiedosto tulee tallentaa ja Atostek ID käynnistää muutosten jälkeen uudelleen, jotta asetus astuu voimaan.

4.5.24. Asetustiedoston parametri ERRORLOGPATH

Voit käyttää asetusparametria *”ERRORLOGPATH”* suoraan sovelluksen asetustiedostossa (*"/Users/<käyttäjänimi>/Library/Application Support/Atostek Oy/Atostek ID/AtostekID.ini"*). Anna asetukselle polku, johon sovelluksen lokitiedosto halutaan kirjoittaa. Polku voi olla esimerkiksi *”ErrorLogPath=/var/log/atostekid/AID.log”* Jos polku on virheellinen tai sitä ei ole olemassa, kirjaa sovellus lokit jatkossakin oletussijaintiin. Huomaathan, että asetustiedosto tulee tallentaa ja Atostek ID käynnistää muutosten jälkeen uudelleen, jotta asetus astuu voimaan.

4.5.25. Asetustiedoston parametri ALLOWEDBROWSERLESSANDFORWARDDOMAINS

Voit käyttää asetusparametria *”ALLOWEDBROWSERLESSANDFORWARDDOMAINS”* suoraan sovelluksen asetustiedostossa (”/Users/<käyttäjänimi>/Library/Application Support/Atostek Oy/Atostek ID/AtostekID.ini”). Asetusparametria *”ALLOWEDBROWSERLESSANDFORWARDDOMAINS”* käytetään erasmartcard.ehoito.fi-rajapinnan käytön yhteydessä silloin, kun suoritetaan selaimeton kirjautuminen, selaimeton allekirjoitus tai /ForwardMessage-pyyntö muualle kuin Atostekin ERA- tai Atostekin Edemo-järjestelmään. Järjestelmät era.ehoito.fi ja edemo.atostek.com ovat automaattisesti sallittuja ulkopuolisia osoitteita näissä pyynnöissä. Jos haluat lisätä sallittuja osoitteita tuotanto- tai testauskäyttöön, anna sallitut osoitteet parametrissa, esimerkiksi *”AllowedBrowserlessAndForwardDomains=era.ehoito.fi, edemo.atostek.com, edemo5.atostek.com”*. Huomaathan, että asetustiedosto tulee tallentaa ja Atostek ID käynnistää muutosten jälkeen uudelleen, jotta asetus astuu voimaan.

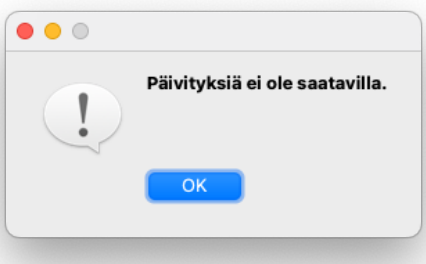
4.5.26. Asetustiedoston parametri ENABLECUSTOMDIALOG

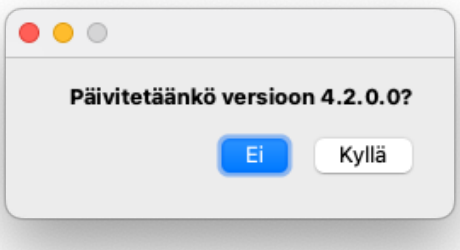
Voit käyttää asetusparametria "ENABLECUSTOMDIALOG" suoraan sovelluksen asetustiedostossa (*"/Users/<käyttäjä>/Library/Application Support/Atostek Oy/Atostek ID/AtostekID.ini"*). Oletuksena tai asetuksen arvon ollessa "true", Atostek ID:n ulkoiset moduulit näyttävät käyttäjälle Atostek ID:n PIN-koodi-ikkunan, kun PIN-koodi kysytään käyttäjältä. Poikkeuksena ovat tietoturvaan liittyvät rajoitukset, joissa käyttöjärjestelmä huolehtii PIN-koodin kyselyn, kuten työasemakirjautumisessa. Asetuksen ollessa "false" PIN-koodi kysytään käyttöjärjestelmän kyselyikkunalla.

4.6. Päivittäminen

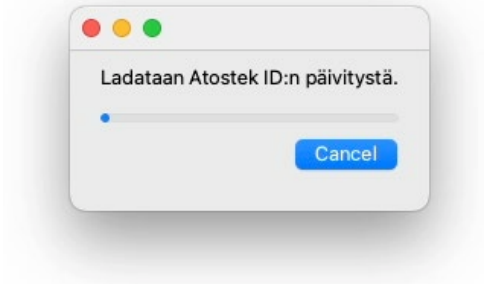
Voit päivittää ohjelman valitsemalla ohjelman valikosta *”Päivitä”*. Ohjelma tarkistaa päivitykset ja näyttää sen jälkeen päivitysten tilanteen (kuvat 9 ja 10). Mikäli päivityksiä löytyy ja haluat päivittää ohjelman uusimpaan versioon, valitse kuvan 10 mukaisessa ikkunassa *”Kyllä”*, jolloin ohjelma lataa ja asentaa uusimman version (kuvat 11 ja 12). Syötä osascript-ikkunaan käyttäjätunnuksesi ja salasanasi, jotta päivitys suoritetaan loppuun.

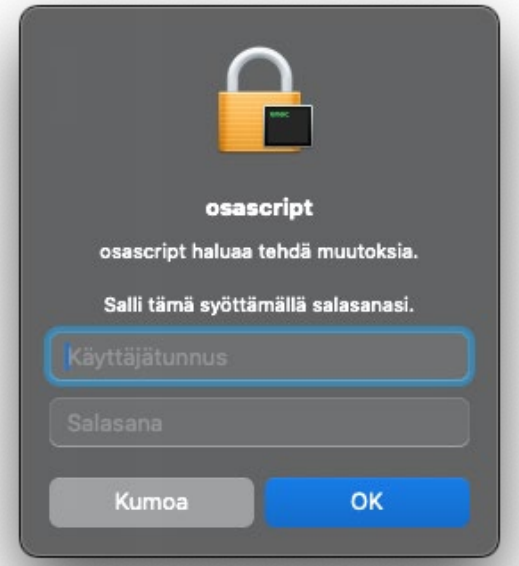
Huom! Ohjelman päivitys vaatii ylläpitäjän oikeudet, joita pyydetään käyttäjältä automaattisesti.





Kuvat 9 ja 10. Päivitysten tilanne, kun päivityksiä ei ole saatavilla ja kun päivityksiä on saatavilla.

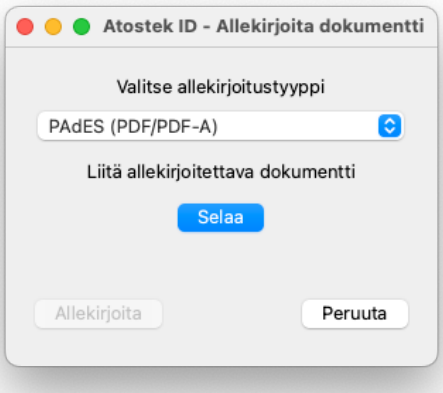




Kuvat 11 ja 12. Päivitysten lataaminen ja asentaminen.

4.7. Dokumenttien allekirjoitus sovelluksen kautta

PDF- ja PDFA-dokumentteja voidaan allekirjoittaa Adobe Acrobat -sovelluksen ja PDF-XChange-sovelluksen lisäksi myös suoraan Atostek ID -sovelluksen kautta. Allekirjoitus on tällöin PAdES-standardin mukainen. Allekirjoituksen taso (B-B, B-T, B-LT, B-LTA) on korkein mahdollinen, minkä sovellus pystyy tuottamaan. Tämä riippuu esimerkiksi siitä, onko sovellukselle konfiguroitu aikaleimapalvelun osoite asetusten kautta. PAdES-standardin lisäksi sovellus tukee CAdES (B-B), JAdES (B-B), XAdES (B-B) ja ASiC-E (B-B, B-T, B-LT) muotoisia allekirjoituksia (detached signatures) muillekin dokumenttityypeille. Muodostaaksesi allekirjoituksen avaa sovelluksen valikosta *"Allekirjoita dokumentti"*. Valitse tämän jälkeen avautuvassa ikkunassa (kuva 13) allekirjoituksen tyyppi ja hae koneeltasi allekirjoitettava dokumentti.



Kuva 13. PDF-dokumentin allekirjoittaminen Atostek ID -sovelluksessa.

Kun allekirjoitus aloitetaan, kysytään käyttäjältä ensin allekirjoitukseen käytettävä varmenne. Kun varmenne on valittu, pyydetään käyttäjältä varmennetta vastaava PIN-koodi. Koodin syöttämisen jälkeen kortti suorittaa allekirjoituksen ja allekirjoitus liitetään alkuperäisestä dokumentista kopioituun dokumenttiin, jonka nimen loppuun lisätään teksti *"_signed"*. Sovellus ilmoittaa vielä lopuksi, onnistuiko allekirjoitus vai ei.

4.8. Sähköpostin salaus ja allekirjoitus (Apple Mail)

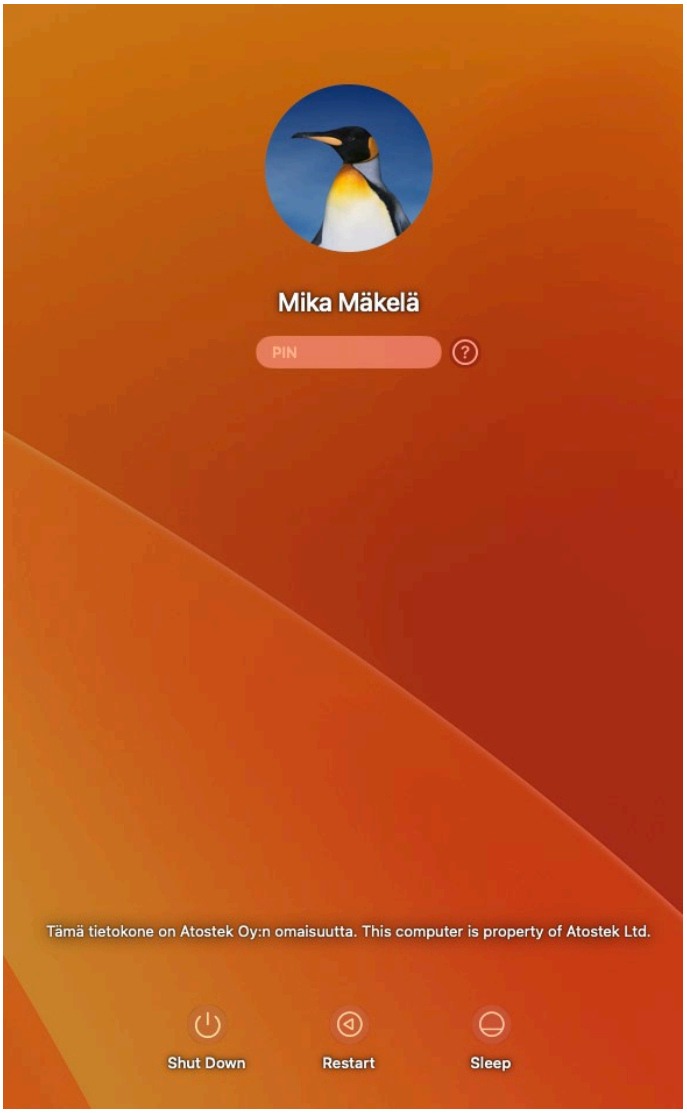
Sähköpostit voidaan salata ja allekirjoittaa Apple Mailissa varmennekortin varmenteita käyttäen. Tällöin macOS:lla hyödynnetään Atostek ID TokenDriver -moduulia, joka asentuu automaattisesti Atostek ID macOS -version asennuksen yhteydessä. Atostek ID TokenDriver -moduulista voi lukea tarkemmin Atostek ID -ohjelmiston integraatio-ohjeesta. Tutustuthan tarvittaessa Apple Mailin omaan dokumentaation sähköpostin salaamisesta ja allekirjoituksesta.

Varmennekortti pitää ensin ottaa käyttöön Apple Mail -sovelluksessa. Tämän jälkeen voit käyttää korttiasi sähköpostin salaamiseen ja allekirjoittamiseen. Lähettääksesi toiselle henkilölle salatun sähköpostin, pitää sinulla olla vastaanottajan varmenteen julkinen avain liitettynä vastaanottajan yhteystietoon.

4.9. Työasemakirjautuminen

macOS-työasemaan voidaan tunnistautua varmennekortin tunnistautumisvarmenteella. Tällöin hyödynnetään Atostek ID TokenDriver -moduulia, joka asentuu automaattisesti Atostek ID macOS -version asennuksen yhteydessä. Atostek ID TokenDriver -moduulista voi lukea tarkemmin Atostek ID -ohjelmiston integraatio-ohjeesta.

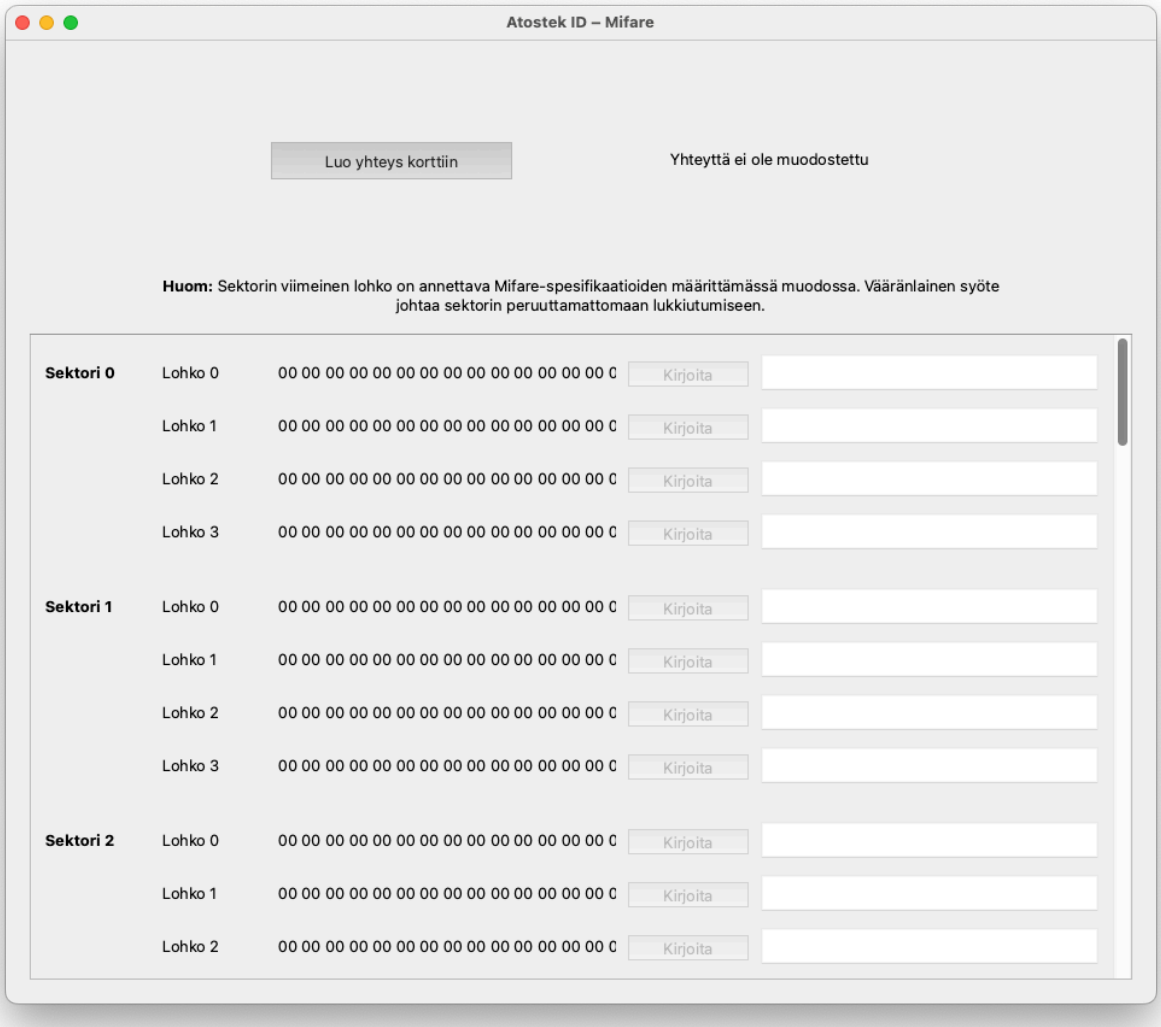
Kun ajuri on asennettu, kortinlukija on kiinni koneessa, kortti on kortinlukijassa ja käyttäjän kortit tedot paritettu macOS-käyttäjään, käyttäjän pitää kirjautua työasemaansa varmennekortillaan. macOS:n sisäänkirjautumisnäkymässä salasanan sijaan käyttäjältä pyydetään PIN-koodia (kuva 14). Kirjauduttaessa tulee syöttää kortin PIN1-koodi.



Kuvat 14. Työasemakirjautumisen näkymä, kun varmennekortti on paritettu käyttäjään.

4.10. MIFARE-sirun hallinta

Kun olet asennuksen yhteydessä tai asetusten kautta asettanut valituksi MIFARE-valinnan, saat Atostek ID -sovelluksen valikkoon näkyviin vaihtoehdon ”Mifare” (kuva 1). Kun valitset sen, avautuu kuvan 15 mukainen näkymä MIFARE-sirun sektoreista



Kuva 15. Mifare-sirun hallintanäkymä.

MIFARE-sirun lukemista ja kirjoittamista varten tarvitset NFC-lukijan. Yhdistä lukija normaalisti tietokoneeseen ja laita kortti lukijaan. Anna kortin PIN1-koodi, kun sitä kysytään turvatun yhteyden muodostamiseksi. Tämän jälkeen voit painaa Mifare-näkymässä nappia ”Luo yhteys korttiin”. Näkymässä kerrotaan, onnistuuko vai epäonnistuuko yhteyden luominen. Näkymään luetaan automaattisesti MIFARE-sirun kuusitoista sektoria ja niiden kaikkien neljän lohkon sisällöt.

Näkymässä on myös mahdollista kirjoittaa sirun lohkoihin. **Ethän kirjoita MIFARE-sirulle mitään ellet ole ehdottoman varma siitä, mitä olet kirjoittamassa ja että kirjoittaminen on tarpeellista! Kirjoittamista ei ole tarpeen tehdä normaaleissa käyttötapauksissa tai sovelluksen muun toiminnan takaamiseksi. Ole tarpeen tullen yhteydessä organisaatiosi IT-tukeen.** Vääränlainen kirjoitus voi johtaa sektorin pysyvään lukkiutumiseen (erityisesti sektorin viimeisen lohkon vääränlainen kirjoittaminen). Tutustuthan NXP:n MIFARE Classic EV1 -dokumentaatioon ennen kuin teet kirjoituksia. Yksi suhteellisen turvallinen tapa testata kirjoittamista on kirjoittaa sektorin 2 lohkoon 1 kaikki tavut arvoon 0xFF (eli syöte *”FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF”*). Arvot voidaan palauttaa kirjoittamalla kaikki tavut takaisin alkuperäisiin arvoihinsa (eli yleensä syöte *”00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00*”).

4.11. Lokitus ja välimuistitiedostot

4.11.1. Lokitus ja lokitiedostot

Atostek ID lokittaa omaan lokitiedostoonsa lokiviestejä sovelluksen toiminnasta ja virhetilanteista. Lokitiedosto löytyy oletuksena polusta *"/Users/<käyttäjänimi>/Library/Application Support/Atostek Oy/Atostek ID/AtostekID/Error.log"*. Lokitiedoston saa avattua valitsemalla valikosta *”Dignostiikka”* ja avautuvasta ikkunasta *”Näytä Atostek ID:n loki”*. Lokitiedoston sijaintia voi muuttaa asetusten kautta.

Oletuksena lokitusta tehdään informaatio-, varoitus- ja virhetasoisista huomioista. Asetusten kautta voi asettaa päälle debug-tasoisen lokituksen, jolloin lokitus on tarkempaa ja lokia tuotetaan enemmän. Debuug-tasoinen lokitus on erityisen oleellista virhetilanteiden selvittämisen kannalta. Lokituksen voi ottaa myös kokonaan pois päältä asetusten kautta. Aikaisempi lokitiedosto ei tällöin poistu, uusia lokiviestejä ei vain kirjata.

Atostek ID lokittaa virhetasoiset lokiviestit myös käyttöjärjestelmän lokiin (System Log).

Atostek ID:n PKCS#11-moduulin pääasiallinen lokitiedosto löytyy polusta ”*/Users/<käyttäjä>/Library/Application Support/Atostek Oy/Atostek ID/PKCS11.log*”. TokenDriverin ajamana moduuli kuitenkin lokittaa tiedostoon ”*/Users/<käyttäjä>/Library/Containers/com.atostekid.AtostekIDToken/Data/Library/Logs/*”.

Atostek ID TokenDriverin lokia voi tarkastella kohdasta 5.2.1 löytyvällä komennolla.

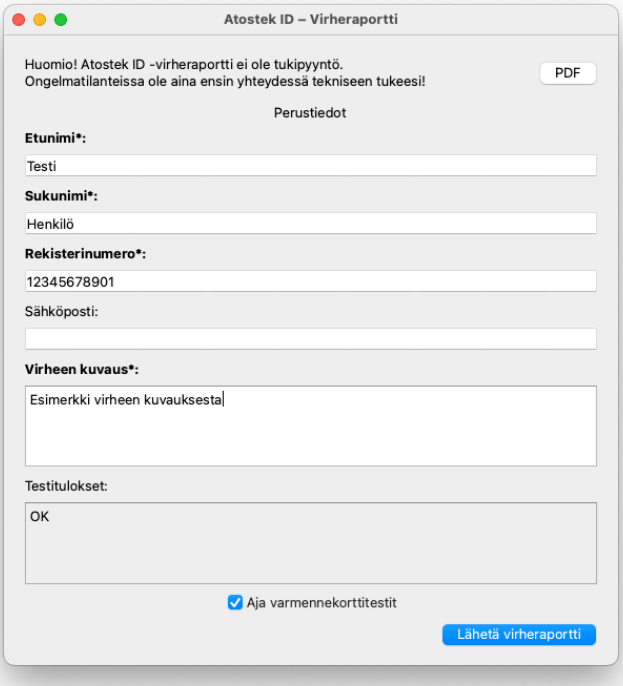
4.11.2. Välimuistitiedostot

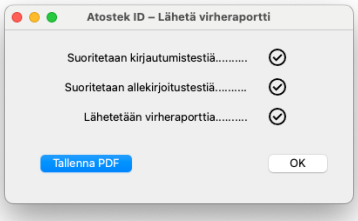
Mikäli korttivälimuistin tyypiksi on asetettu ”Tallenna salattuna levylle”, se tallennetaan tiedostoon ”*C:\Users\<käyttäjä>\AppData\Local\Atostek Oy\Atostek ID\cache.json*”. Korttivälimuistitiedosto tyhjennetään automaattisesti, jos korttivälimuistin tyyppi vaihdetaan. Korttivälimuistin tyhjentämiseksi voikin vaihtaa tämän asetuksen arvon tai vaihtoehtoisesti poistaa itse mainitun tiedoston.

4.12. Virheraportointi

Atostek ID -sovelluksen valikosta löytyy kohta "*Virheraportti*", jonka avulla voit lähettää virheraportin Atostekin AIDERA-palveluun. Virheraportti itsessään ei kuitenkaan ole tukipyyntö. Jos kohtaat ongelmatilanteen, ole aina yhteydessä ensin tekniseen tukeesi. Tarvittaessa sinua pyydetään lähettämään virheraportti tämän toiminnon kautta. Virheraportteja voi lähettää vain rajatun määrän vuorokaudessa.

Virheraportti muodostetaan antamalla riittävät yhteystiedot ja kirjoittamalla virheen kuvaus (kuva 16). Jos kortinlukija ja kortti on yhdistetty, etsitään kortin tiedot automaattisesti.





Kuvat 16 ja 17. Virheraportti ja sen lähettäminen.

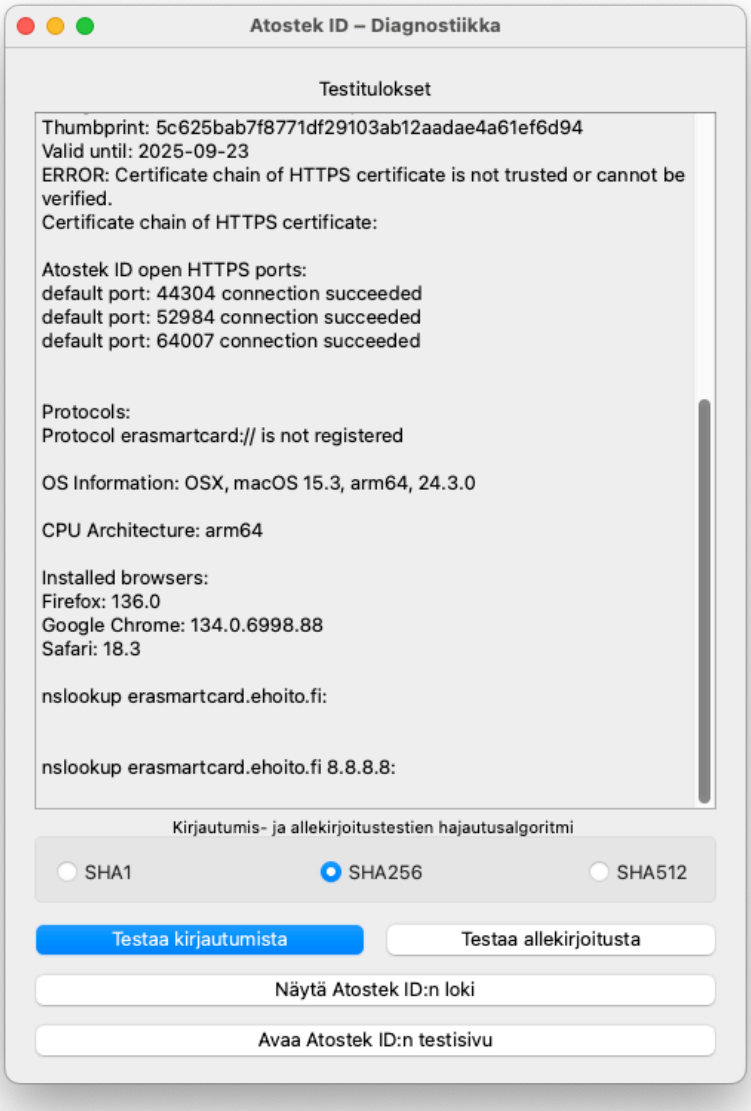
Pakolliset kentät on merkitty tähdellä ja lihavoinnilla. Virheraportin voi lähettää alaoikealta löytyvästä painikkeesta "*Lähetä virheraportti*". Huomaa, että painiketta ei voi painaa, jos yksikin pakollisista kentistä puuttuu.

Voit myös halutessasi tallentaa virheraportista PDF-tiedoston omalle koneellesi yläoikealta löytyvästä painikkeesta "*PDF*". Näkymässä alhaalta löytyvän valintaruudun "*Aja varmennekorttitestit*" avulla voit valita, ajetaanko korttitestit virheraportin lähettämisen yhteydessä.

Virheraportin lähettämisestä avautuu ikkuna, josta voit seurata lähettämisen edistymistä (kuva 16). Virheraportin lähettämisen ikkunassa näkyy korttitestien tila ainoastaan silloin, jos olet valinnut korttitestit ajettavaksi kuvan 15 ikkunassa. Jos virheraportin lähettäminen onnistuu, virheraportin ikkuna (kuva 15) sulkeutuu automaattisesti. Virheraportin lähettämisen ikkunasta (kuva 16) voit vielä halutessasi tallentaa virheraportin PDF-tiedostona painikkeesta "*Tallenna PDF*".

4.13. Diagnostiikka

Atostek ID -sovelluksen diagnostiikkanäkymän (kuva 18) saat avattua valikon kohdasta "*Diagnostiikka*". Näkymän avautuessa ajetaan yleisiä testejä, mikä kestää muutamia sekunteja. Testitulokset pitävät sisällään tietoa muun muassa Atostek ID -sovelluksen versiosta, yhdistetyistä lukijoista sekä tuetuista selaimista.



Kuva 18. Atostek ID -sovelluksen diagnostiikkanäkymä.

Diagnostiikkanäkymässä voit myös testata kirjautumista (tunnistautumista) ja allekirjoitusta kortin ollessa yhdistettynä. Voit valita käytettävän hajautusalgoritmin valintanappien avulla. Kirjautumis- ja allekirjoitustestin tulokset tallentuvat "*Testitulokset*"-näkymään.

Saat näkyviin sovelluksen lokin "*Näytä Atostek ID:n loki*" -painikkeen avulla. Loki avautuu erilliseen ikkunaan.

Painikkeesta "*Avaa Atostek ID:n testisivu*" voit kokeilla, toimiiko Atostek ID -sovelluksen erasmartcard.ehoito.fi-rajapinta oikein. Jos painikkeesta ei avaudu muutoin tyhjää nettisivua tekstillä "*Test page loaded OK*", jotakin on pielessä. Esimerkiksi jos Atostek ID -sovelluksen tarvitsemat varmenteet eivät ole luotettuina varmennesäilössä, ei testisivu aukea oikein.

5. Usein kysytyt kysymykset ja virhetilanteista

Atostek ID näyttää erillisiä virheikkunoita virhetilanteiden sattuessa. Näitä ovat esimerkiksi tilanteet, joissa

- Atostek ID ei saa käynnistettyä SCS-rajapinnan HTTPS-palvelinta porttiin 53952, koska portti ei ole vapaana.
- Toimintoa ei voida suorittaa, koska korttia ei ole lukijassa.
- Toiminto epäonnistuu (esimerkiksi tunnistautuminen tai allekirjoitus) virheellisten pyyntöjen tai kortin ongelmien takia.

Näiden lisäksi Atostek ID kirjaa lokiin virhetilanteisiin liittyviä viestejä ja näyttää logossaan, jos jotakin on pielessä.

5.1. Usein kysyttyjä kysymyksiä

K: Sovellus näyttää varoituksen ”SCS-palvelimen avaaminen porttiin 53952 epäonnistui!” tai ”SCS-CA-palvelimen avaaminen porttiin 53953 epäonnistui!”.

V: Tämä virhe johtuu yleensä siitä, että ilmoitetut portit eivät ole vapaana eli jokin toinen ohjelma varaa niitä. Varmistathan, että sinulla ei ole esimerkiksi asennettuna tai käynnissä toista kortinlukijaohjelmistoa, joka varaisi näitä samoja portteja. Nämä varoitukset estävät vain sovelluksen SCS-rajapinnan käytön eli ne eivät välttämättä estä sinua käyttämästä ohjelmistoa omien käyttötapaustesi puitteissa. Mikäli toisen kortinlukijaohjelmiston sulkeminen ja poistaminen ei auta, voit tutkia koneesi komentokehotteen avulla, mikä ohjelma varaa Atostek ID -sovelluksen tarvitsemia portteja (lsof-komento). Ole mahdollisuuksien mukaan yhteydessä oman organisaatiosi IT-tukeen. Mikäli et tarvitse SCS-rajapintaa käyttötapauksessasi ollenkaan ja portin vapauttaminen ei ole mahdollista, voit ottaa koko rajapinnan pois käytöstä sovelluksen asetusten kautta. Tällöin sovellus ei käynnistä rajapintaa lainkaan, minkä johdosta myöskään varoituksia ei näytetä.

K: Kortin tietojen lukeminen ei onnistu.

V: Onhan kortti lukijassa oikein päin? Huomaathan, että kortin kontaktipinnan (metallinen neliö) täytyy osua lukijan kontaktipintoihin, jotta yhteys saadaan muodostettua (muut kuin NFC-lukijat). Kontaktipintaa voi myös yrittää pyyhkiä kevyesti, koska kaikenlainen lika vaikeuttaa lukemista. Onhan kortinlukija kunnolla kiinni laitteessa? Voitko kokeilla jotakin toista USB-porttia? Onhan kortinlukijan oma ajuri asennettu ja ajantasainen, jos kortinlukijavalmistaja sellaisen tarjoaa? Kortinlukijavalmistajien ajureita on yleensä valmiiksi asennettuna käyttöjärjestelmässä. Ne voivat kuitenkin myös puuttua tai kaivata päivitystä. Ajuripaketteja saa ladattua yleensä kortinlukijavalmistajan omilta sivuilta.

K: Sovellus sanoo, että PIN-koodi on lukossa.

V: PIN-koodi on tällöin syötetty väärin liian monta kertaa peräkkäin. Voit avata PIN-koodin PUK-koodin eli aktivointitunnusluvun avulla sovelluksen valikon kautta.

K: Mikä on PUK-koodi?

V: PUK-koodi eli aktivointitunnusluku on tunnusluku, joka sinulle on lähetetty erillisessä kirjeessä, kun olet tilannut korttisi. Aktivointitunnuslukua käytetään kortin aktivointiin ja lukkiutuneiden PIN1- ja PIN2-koodien avaamiseen.

K: Tunnistautuminen tai allekirjoitus ei onnistu selaimessa.

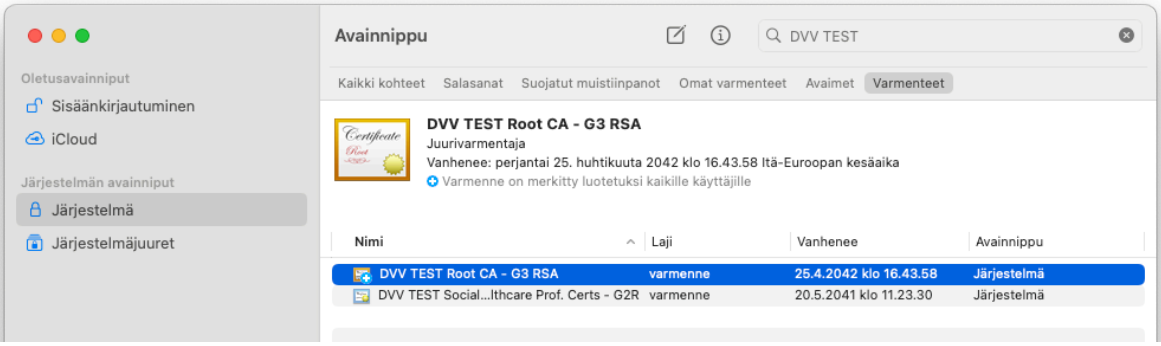
V: Tässä ongelman tarkempi selvitys riippuu siitä, mitä rajapintaa käytetään. Jos kysessä on mTLS-tunnistautuminen (esim. suomi.fi), tarkistathan, että Atostek ID TokenDriver on asentunut oikein. Jos kyseessä on tunnistautuminen tai allekirjoitus SCS- tai erasmartcard.ehoito.fi-rajapinnan kautta, voit tarkistaa, pääsetkö rajapinnan testisivulle (https://localhost:53952/ tai https://erasmartcard.ehoito.fi:44304/). Selain yleensä kertoo, jos sivulle ei pääse DNS-ongelmien tai varmenteiden epäluottavuuden takia. DNS-ongelmissa ole yhteydessä organisaatiosi IT-tahoon. Varmenteet voi asentaa luotetuiksi selaimen tai käyttöjärjestelmän varmennesäilöön käsin. Voit myös tarkistaa sovelluksen valikon *"Tietoa"*-näkymästä, ovatko rajapintojen vaatimat oletusportit sovelluksen käytössä.

5.2. Muita ongelmatilanteita

5.2.1. Atostek ID ja TokenDriver

Atostek ID TokenDriver -moduulia käytetään esimerkiksi mTLS-tunnistautumisessa (suomi.fi), dokumenttien allekirjoittamisessa Adobe-ohjelmistolla, sähköpostin salaamisessa ja allekirjoittamisessa Apple Mail -sovelluksella sekä kirjauduttaessa varmennekortilla työasemaan. Moduuli asentuu automaattisesti järjestelmään asennuksen yhteydessä. Asennuksessa tai moduulissa voi kuitenkin esiintyä ongelmia. Tarkistathan seuraavat kohdat, mikäli havaitset ongelmia.

Kun käytetään Safaria tai Firefoxia mTLS-tunnistautumisessa, on asetettava kortin juuri- ja välivarmenteet luotetuksi Avainnipun varmennesäilöön. Atostek ID yrittää tehdä tämän automaattisesti asennuksen yhteydessä, mutta jos asennuksessa tulee ongelmia, varmenteet saa lisättyä Avainnippuun Lukijat ja kortit -näkymästä painamalla niitä hiiren oikealla painikkeella ja valitsemalla aukeavasta valikosta *"Avaa"*.



Kuva 19. Kortin juuri- ja välivarmenne avainnipussa.

TokenDriver-moduulin asennuksen voi tarkistaa komennolla *"pluginkit -vv -m -p com.apple.ctk-tokens"*. TokenDriver-moduulin lokiin tulevia merkintöjä, kuten mainintoja virhetilanteista, voi seurata komennolla *"log stream --predicate '(subsystem == "com.apple.CryptoTokenKit") || (process == "AtostekIDToken")'"*.

Asennuksen jälkeen on hyvä kirjautua ulos tai käynnistää koko kone uudelleen, jotta uusi TokenDriver varmasti rekisteröityy käyttöön.

Komennolla *”sc_auth list”* voi tarkistaa voimassa olevat paritukset käyttäjien ja korttien välillä. Komennolla *”sc_auth unpair -u <käyttäjänimi>”* voi purkaa voimassa olevan parituksen valitulta käyttäjältä. Parituksen täytyy olla voimassa, jotta korttia voi käyttää työasemakirjautumiseen.

Jos kaikki edelliset kohdat toimivat ja käyttötapauksesi silti epäonnistuu selaimessa, voit yrittää selaimen välimuistin tyhjäämistä tai selaimen yksityisen ikkunan käyttöä, jotta mikään välimuistissa ei pääse häiritsemään kortin käyttöä.

5.2.2. Korttien myöntäjävarmenteiden vieminen Avainnippuun

Jos Atostek ID:n asennuksessa menee jokin vikaan siten, ettei korttien juuri- ja välivarmenteita aseteta luotetuiksi Avainnippuun, voi varmenteet lisätä Avainnippuun ainakin seuraavilla tavoilla:

Vaihtoehto 1: Kun kortti on lukijassa, avaa ”Lukijat ja kortit”-dialogi ja klikkaa jotakin varmenteista hiiren oikealla painikkeella. Valitse aukeavasta valikosta ”Luottamustarkastus”. Jos varmenneketju ei ole vielä luotettu, sovellus tarjoaa mahdollisuutta asettaa se luotetuksi. Valitse ok ja syötä salasana niin monta kertaa kuin sitä kysytään. Tämä lisää lukijassa olevan kortin juuri- ja välivarmenteet Avainnippuun ja asettaa juurivarmenteen luotetuksi, mikäli näin ei vielä ole.

Vaihtoehto 2: Poista Atostek ID:n asennus ja yritä asentaa se uudelleen. Varmista, että asennuspaketin asetus ”Asenna DVV:n juurivarmenteet, jos niitä ei ole vielä asennettu” on valittuna ja syötä salasana niin monta kertaa kuin asennuspaketti sitä pyytää.

Vaihtoehto 3: Lukijassa olevan kortin juuri- ja välivarmenteen saa lisättyä myös kohdassa 5.2.1 kuvatulla tavalla.

Vaihtoehto 4: Atostek ID:n asennuksen mukana asentuu hakemistoon ”*/Library/Atostek ID*” tiedosto ”*DVV-VRK-certificates.mobileconfig*”, jonka avulla juuri- ja välivarmenteet voi lisätä oman käyttäjän Avainnippuun. Etsi tiedosto esimerkiksi avaamalla uusi Finderin ikkuna, valitsemalla sitten yläpalkista ”Siirry”-valikosta ”Siirry kansioon…” ja kirjoittamalla näytölle ilmestyvään tekstikenttään *”/Library/Atostek ID*” ja painamalla sitten Enter. Valittu kansio aukeaa ja siellä pitäisi näkyä muiden tiedostojen ohella ”*DVV-and-VRK-certificates.moblieconfig*”. Kaksoisnapsauta tiedostoa. Näytölle ilmestyy ponnahdusikkuna, joka kertoo, että profiili on lisätty ja että asentamista varten pitää vielä tarkistaa se Järjestelmäasetuksissa. Avaa Järjestelmäasetukset ja valitse sen vasemman sivupalkin listan yläosasta kohta ”Profiili ladattu”. Kaksoisnapauta sitten Järjestelmäasetuksien ikkunassa näkyvää ”Atostek ID – DVV & VRK CA” -profiilia, jonka alla on varoituskolmio ja teksti ”Profiilia ei asennettu. Tarkista kaksoisklikkaamalla.” Valitse sitten ”Asenna” kaikista seuraavaksi näytölle aukeavista ponnahdusikkunoista, jotka kysyvät tämän profiilin asentamisesta.

Vaihtoehto 5: Lataa juuri- ja välivarmenteet DVV:n sivuilta osoitteesta https://dvv.fi/ca-varmenteet ja asenna ne Avainnippuun.