Atostek ID: Integrointikoulutus esiosa

1.7.2024

ATOSTEK

Sisältö

- Koulutuksen tarkoitus ja tavoite
- Atostek ID: Yleinen esittely ja sovelluksen asentaminen
- Rajapinnat
  - SCS
  - Minidriver, (TokenDriver)
  - PKCS#11
- Aikaa kysymyksille

- Pidetään lyhyt 5 min tauko, jos koulutus vaikuttaa kestävän koko 2 h ajan

Koulutuksen tarkoitus ja tavoite

ATOSTEK

Tarkoitus ja tavoite

- Tämä koulutus on suunnattu niille toimijoille, joiden järjestelmä integroituu käyttämään jotakin Atostek ID –ohjelmiston rajapinnoista

- Koulutus on esiosa elokuussa pidettäville integrointikoulutuksille
  - Käymme yleisellä tasolla läpi kaikki integroitavat rajapinnat ja tarjoamme dokumentaatiota
  - Jokainen rajapinta käydään syvemmin läpi elokuun koulutuksissa
  - **Tässä on tarkoituksena tutustua mahdollisuuksiin ja tarjota materiaalia tutkittavaksi ennen elokuun koulutuksia**
  - Esiosa ei ole pakollinen ennen elokuun koulutuksia, vaan suunnattu niille, jotka haluavat perehtyä asiaan jo heinäkuun aikana.

ATOSTEK

Yleinen esittely ja asentaminen

ATOSTEK

Atostek ID

- Digi- ja väestötietoviraston uusi kortinlukijaohjelmisto
- Julkaistu rajatulle joukolle testaajia jo ensimmäinen ja toinen testiversio
- Elokuussa tehdään ensimmäinen tuotantojulkaisu ja pidetään integrointikoulutukset kahdessa osassa
- Syyskuun alussa pidetään vielä käyttöönottokoulutus

Sovelluksen asentaminen

- Asennuspaketin yhteydessä tarjotaan käyttö- ja asennusohjeet joka alustalle. Niissä on tarkat ohjeet asennuksen suorittamiselle.

- Kaikilla alustoilla asennuksessa voidaan käyttää oletusasetuksia. Kaikki integroitavat rajapinnat ovat käytettävissä oletusasetusten myötä.

- Asennusten yhteydessä voidaan valita, millä kielellä Atostek ID asentuu laitteelle.

Asentaminen Windows

- Asennus käyttöliittymän kanssa: Klikkaa sovelluksen .msi asennuspaketti auki ja suorita asennus käyttöliittymässä annettujen ohjeiden mukaan.
- Asennus komentoriviltä (admin-oikeuksilla):
  - Aja komento *msiexec /quiet /i <paketin nimi>.msi*
  - Voit antaa halutessasi asennusparametreja, esimerkiksi *msiexec /quiet /i <paketin nimi>.msi LANGUAGE="en"*

- Sovellus asentuu oletuksena *C:\Program Files (x86)* kansioon
- Sovelluksen virheloki ja konfiguraatiotiedosto tallentuvat käyttäjän *AppData\Local\Atostek Oy* kansion alle
- Sovellus näkyy tehtäväpalkin piilotetuissa ikoneissa

Asentaminen MacOS

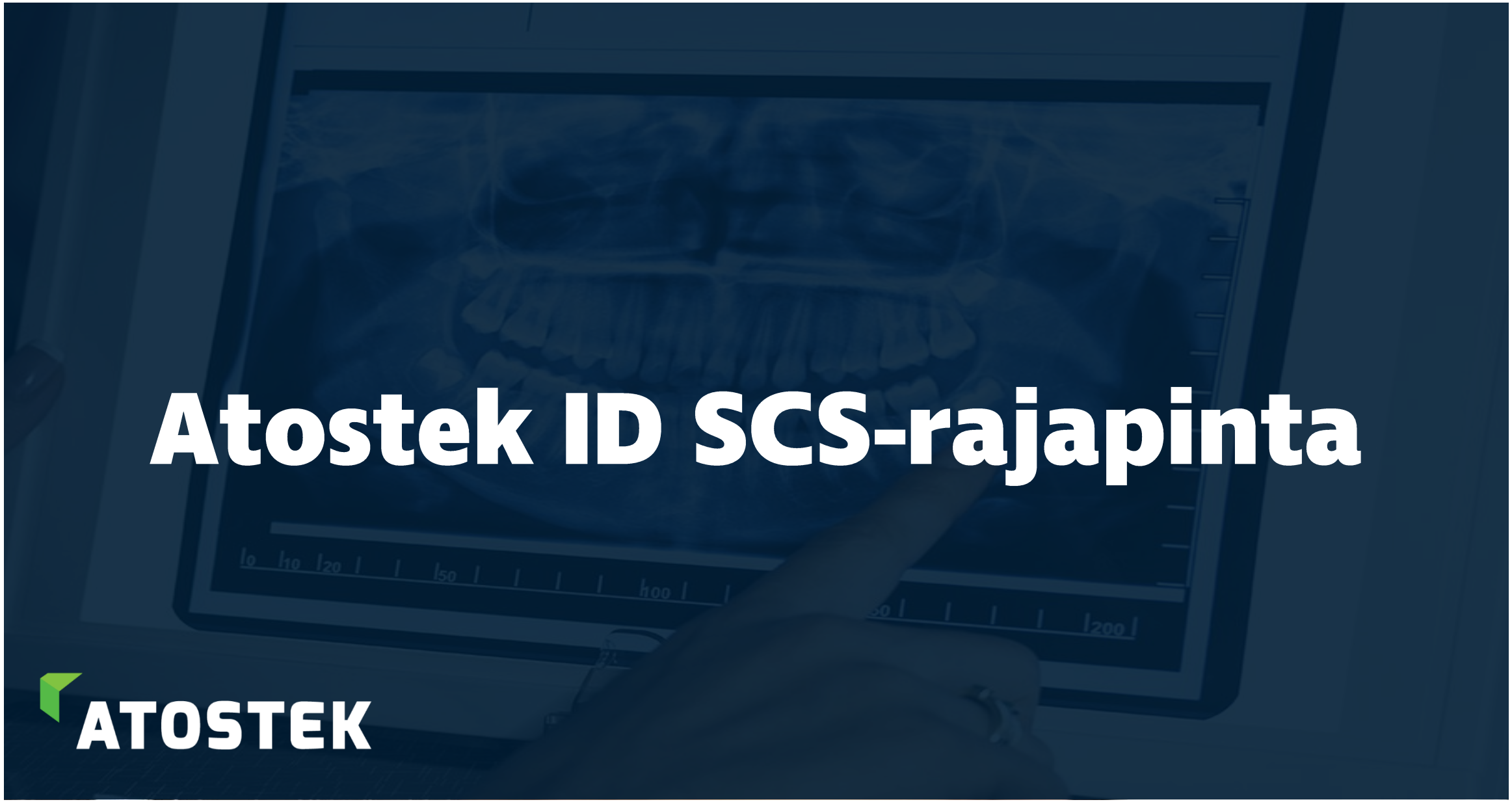
- Asennus käyttöliittymän kanssa: Klikkaa sovelluksen .pkg asennuspaketti auki ja suorita asennus käyttöliittymässä annettujen ohjeiden mukaan.
- Asennus komentoriviltä (sudo):
  - Aja komento *sudo –installer –pkg <paketin nimi>.pkg –target /*
  - Voit antaa halutessasi asennusparametritiedoston, siinä voit antaa esimerkiksi parametrin LANGUAGE=fi

- Sovellus asentuu oletuksena */Applications* kansioon
- Sovelluksen virheloki ja konfiguraatiotiedosto tallentuvat käyttäjän *Library/Application Support/Atostek Oy* kansion alle

Asentaminen Linux

- Asennus Debianille:
  - sudo dpkg –i <paketin nimi>.deb
- Asennus Red Hatille:
  - sudo dnf install<paketin nimi>.rpm

- Mahdollisuus asetusparametrien käytölle tulee elokuun tuotantojulkaisuun



Atostek ID SCS-rajapinta

ATOSTEK

SCS-rajapinta yleisesti

- Signature Creation Service
- DVV:n määrittämä rajapinta allekirjoitusten tekemiseen kortinlukijasovelluksella HTTP-rajapinnan kautta
- Atostek ID toteuttaa sekä rajapinnan versiot 1.1 että 1.2
- Rajapinnan dokumentaatio ja tarkemmat määritykset: FINEID määritykset

ATOSTEK

SCS-rajapinta yleisesti

HTML5 and Digital Signatures

Digital signatures in HTML5 applications, 16.10.2023 DVV-SCS_HTML5-and-Digital-Signatures.pdf

Digital signatures in HTML5 applications, 22.11.2017 SCS-signatures v1.1.pdf

Digital signatures in HTML5 applications, 30.6.2015 SCS-signatures_v1.0.1.pdf

ATOSTEK

SCS-rajapinta testiversioissa

- Ohjelmiston ensimmäisessä ja toisessa testiversiossa on vielä puutteita SCS-rajapinnan osalta. Ne on kirjattu testijulkaisuiden ohjeiden yhteyteen.
  - Henkilökorttien tuki
  - Rajapinnan 1.2 versio
  - Pienet korjaus- ja viilaustarpeet

- Korjaukset ja tarvittavat implementoinnit tehdään elokuun tuotantoversioon

ATOSTEK

SCS-rajapinta: varmenteet ja palvelin

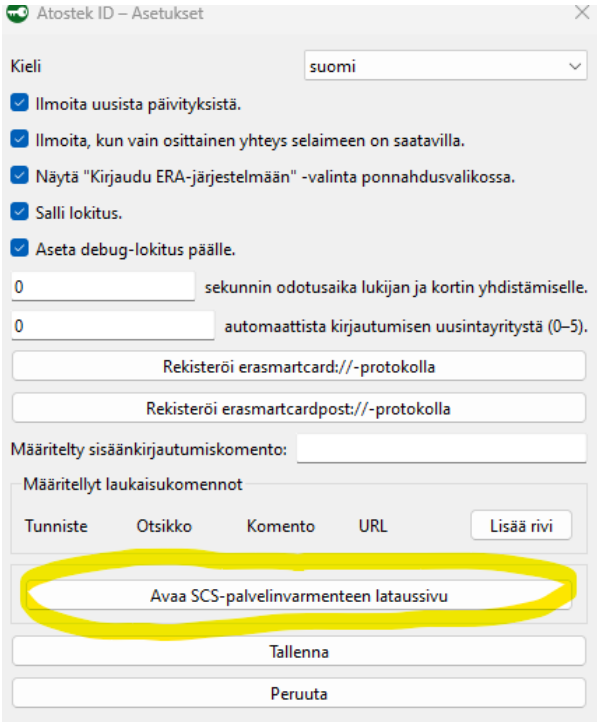
- Atostek ID luo asennuksen yhteydessä HTTPS-palvelimen tarvitsemat varmenteet
  - Myöntävä varmenne *Atostek ID Local SCS CA* pistetään samalla luotetuksi käyttöjärjestelmän varmennesäilöön

- Sovelluksen käynnistyessä käynnistetään myös SCS-rajapinnan toteuttava HTTPS-palvelin, joka löytyy portista **53952**
  - https://localhost:53952/
  - Sivulla teksti *Atostek ID SCS test page loaded OK.*
  - **HUOM:** Tämä ei toimi, jos DigiSign on asennettu ja käynnissä ennen Atostek ID käynnistämistä

ATOSTEK

SCS-rajapinta varmenteet ja palvelin

- Huomioikaa, että varmenne ei asennu toistaiseksi automaattisesti luotetuksi esimerkiksi Firefoxin varmennesäilöön
  - Varmenteen saa ladattua sovelluksesta *Asetukset > Avaa SCS-palvelinvarmenteen lataussivu*
  - Sivulla myös ohjeet siitä, miten varmenne asetetaan luotetuksi



ATOSTEK

SCS-rajapinta: integroituminen

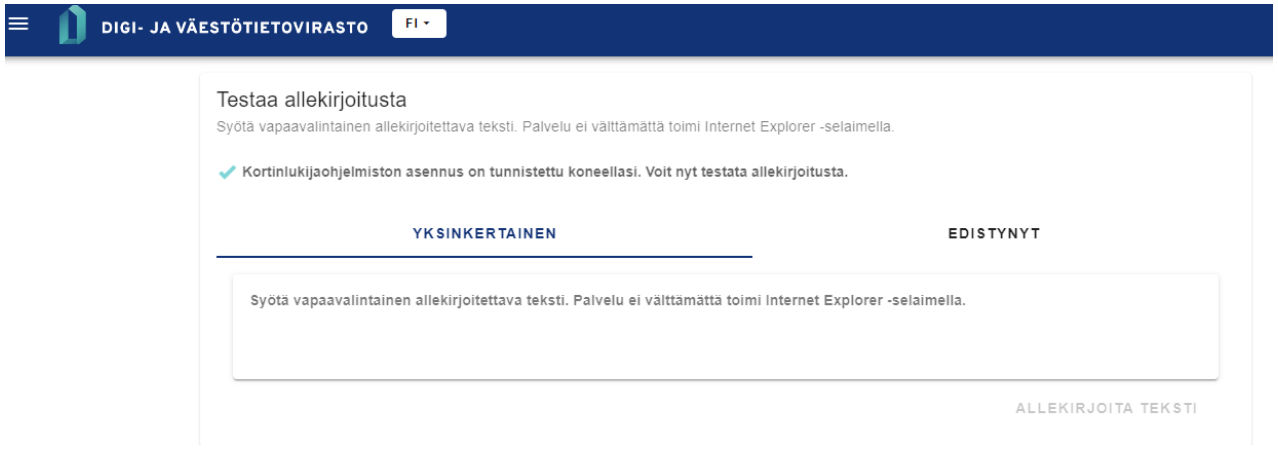
- Atotek ID toteuttaa saman SCS-rajapinnan kuin Fujitsun DigiSign. Tämän myötä integroivan järjestelmän ei pitäisi joutua tekemään muutoksia, kun Atostek ID –sovelluksen SCS-rajapinta vaihdetaan DigiSign-sovelluksen rajapinnan tilalle.

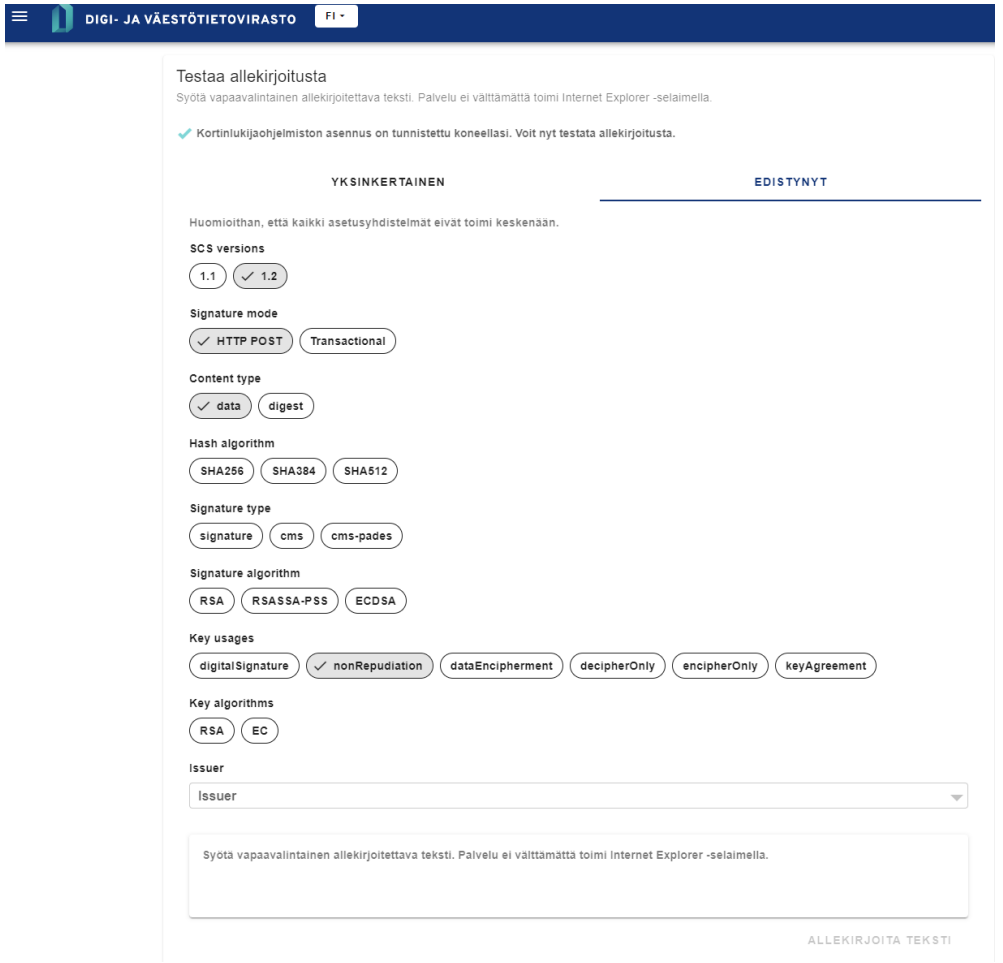
- Huomioittehan, että erityisesti testijulkaisuiden osalta SCS-rajapinnassa voi olla vielä puutteita.

- SCS-rajapinnan toimintaa voi testata myös esimerkiksi DVV:n testisivun kautta.

ATOSTEK

SCS-rajapinta: integroituminen





ATOSTEK

SCS-rajapinta: integroituminen

- Raportoittehan ongelmatilanteet testijulkaisuiden yhteydessä välitettyjen ohjeiden mukaisesti.

- SCS-rajapinnan osalta on ongelmatilanteissa yleensä mielekästä tietää tarkkaan, minkälaisen pyynnön integroiva järjestelmä lähettää kortinlukijaohjelmiston SCS-rajapintaan ja minkälaisen vastauksen rajapinta palauttaa.

ATOSTEK

Erasmartcard.ehoito.fi rajapinta

- Tuotteen oma erasmartcard.ehoito.fi rajapinta toimii SCS-rajapinnan rinnalla, eivätkä nämä rajapinnat vaikuta toistensa käyttöön

- Jo ennestään erasmartcard.ehoito.fi rajapintaan integroituneet järjestelmät voivat jatkaa rajapinnan käyttöä normaaliin tapaan

- Erasmartcard.ehoito.fi rajapinnan käytön ohjeistus tai rajapinnan dokumentaatio ei ole osa tätä toimitusprojektia ja sen käytöstä voi halutessaan olla suoraan yhteydessä Atostekiin

ATOSTEK


Atostek ID Minidriver
ATOSTEK

Minidriver yleisesti

- Moduuli (dll) Windows-käyttöjärjestelmälle älykortin kanssa kommunikoimiseksi
- Toteutettu toimimaan juurikin Digi- ja väestötietoviraston tuottamien varmennekorttien kanssa
- Käyttöjärjestelmä hyödyntää Minidriveria suoraan esimerkiksi työasemakirjautumisessa
- Muut sovellukset voivat myös hyödyntää Minidriveria esimerkiksi allekirjoitusten suorittamiseksi
- Atostek ID Minidriver toteuttaa rajapinnan version 7.07
  - Minidriver rajapintadokumentaatio

ATOSTEK

Minidriver valmiusaste

- Atostek ID Minidriverista tulee testaajille ensimmäinen testiversio saataville keskiviikkona
  - Siitä kuitenkin puuttuu vielä komentoja ja WHQL-allekirjoitus

- Elokuun tuotantojulkaisussa
  - Loput tarvittavat komennot
  - WHQL-allekirjoitus
  - Asennus suoraan Atostek ID asennuksen yhteydessä

ATOSTEK

Testiversioon toteutetut komennot

- CardAcquireContext
- CardDeleteContext
- CardSignData
- CardReadFile
- CardGetFileInfo
- CardEnumFiles
- CardQueryFreeSpace
- CardAuthenticatePin
- CardAuthenticateEx
- CardGetProperty
- CardGetContainerProperty
- CardGetContainerInfo

ATOSTEK

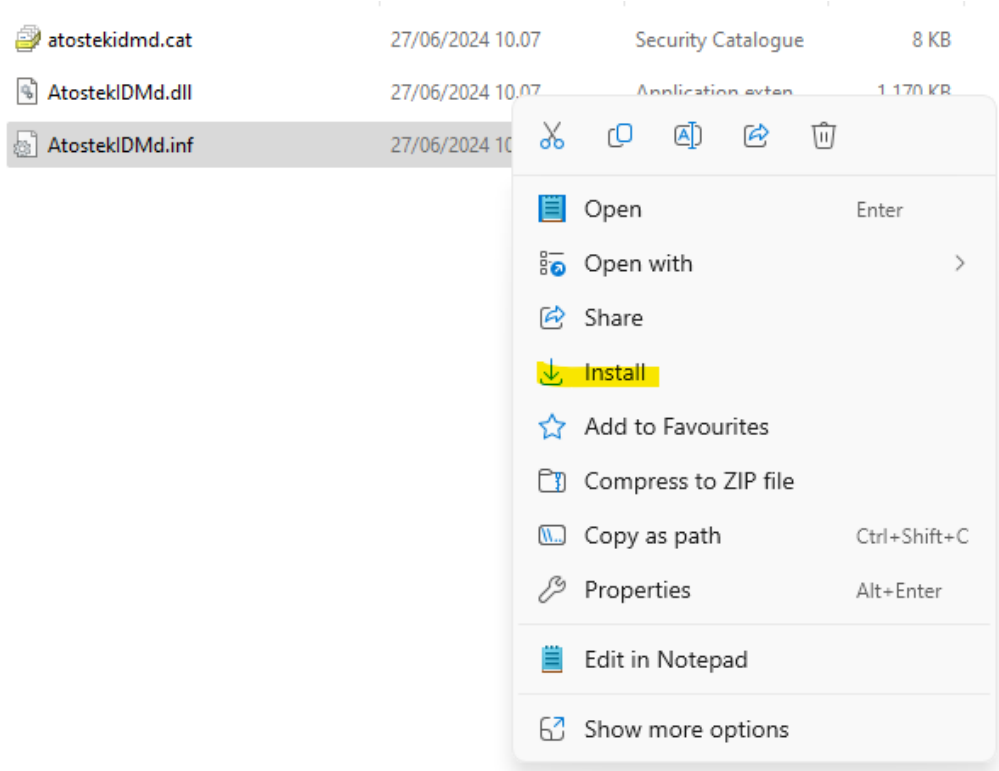
Testiversion asentaminen

- Atostek ID Minidriveria voi testata ennen kuin sille on tehty virallinen WHQL-allekirjoitus
  - Testaajille tarjotaan testiallekirjoitus (atostekidmd.cat), joka tulee pitää samassa sijainnissa moduulin .dll ja .inf tiedostojen kanssa. Nämä kaikki julkaistaan testaajille keskiviikkona 3.7.
  - Testiallekirjoituksen käyttö voidaan sallia komennolla ***bcdedit /set testsigning on***
    - Komento täytyy ajaa adminina
    - Lisää tietoa komennosta löytyy Microsoftin Minidriver dokumentaatiosta

ATOSTEK

Testiversion asentaminen

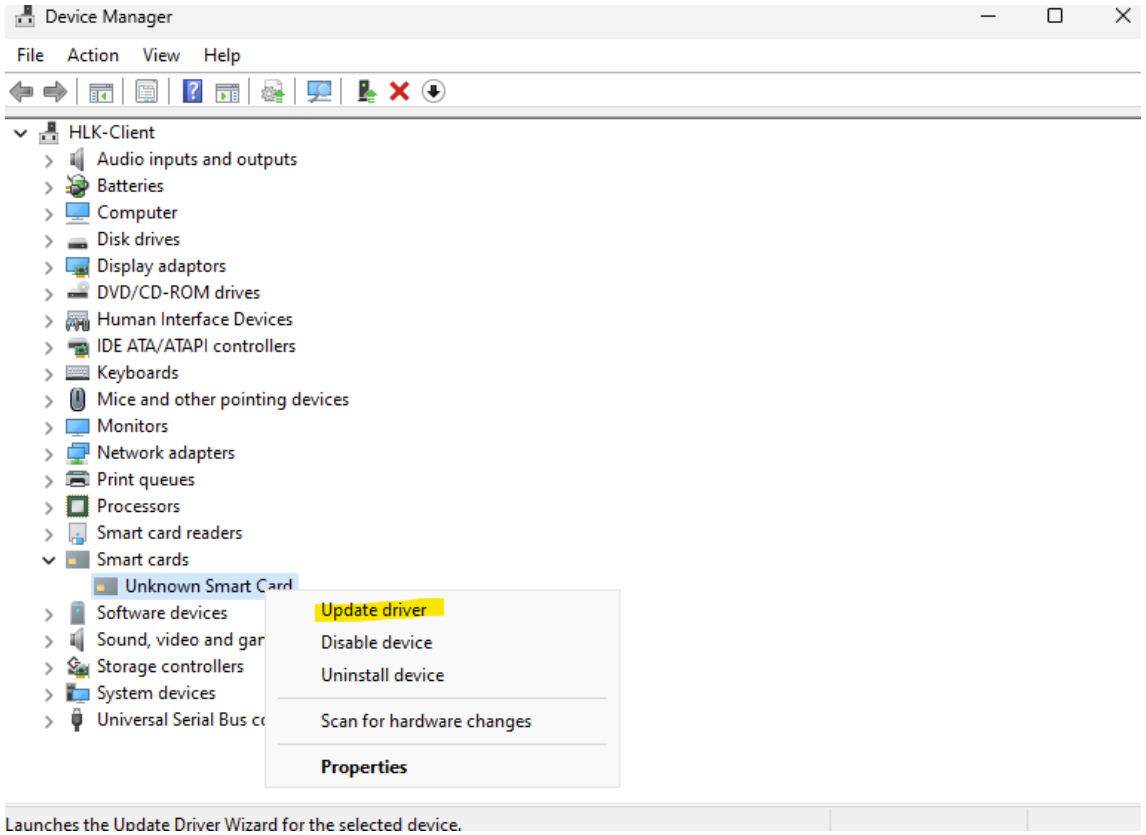
- Testiallekirjoituksen sallimisen jälkeen Atostek ID Minidriver voidaan asentaa klikkaamalla moduulin .inf tiedostoa hiiren oikealla ja valitsemalla *Install*
- Onnistuneesta asennuksesta ilmoitetaan erikseen



ATOSTEK

Testiversion asentaminen

- Tarvittaessa ajuri asetetaan vielä erikseen Device Managerin kautta
- Valitse se kansio, jossa moduuli on laitteellasi



ATOSTEK

WHQL allekirjoitus ja asentaminen tuotantoversiossa

- Sovellukselle haetaan virallinen WHQL-allekirjoitus elokuun tuotantojulkaisuun. Tällöin ajurin asennus onnistuu suoraan ilman testiallekirjoitusten sallimista.

- Tuotantoversiossa tarvittavat tiedostot (dll, inf, cat) tallennetaan laitteelle asennuksen yhteydessä eikä niitä tarvitse erikseen ladata. Tästä tulee tarkemmat ohjeet tuotantoversion integraatio-ohjeeseen.

- Myös tuotantoversiossa asennus käyttää .inf tiedostoa

ATOSTEK

Käyttötapaukset

- Huomioittehan, että testiversiossa ei ole kaikki komentoja toteutettuna, joten kaikkia käyttötapauksia ei voida vielä testata.

- Elokuun tuotantojulkaisun yhteydessä julkaistaan myös ensimmäinen versio AD-rekisteröintipalvelusta. Kun AD-rekisteröintipalvelu otetaan käyttöön, yrittää Minidriver parittaa kortin, kun se tuodaan lukijaan.
  - Tämä tukee siis korttikirjautumista työasemaan myös AD-muutoksen jälkeen. Muutos on otettava huomioon työasemakirjautumisessa viimeistään helmikuuhun 2025 mennessä.

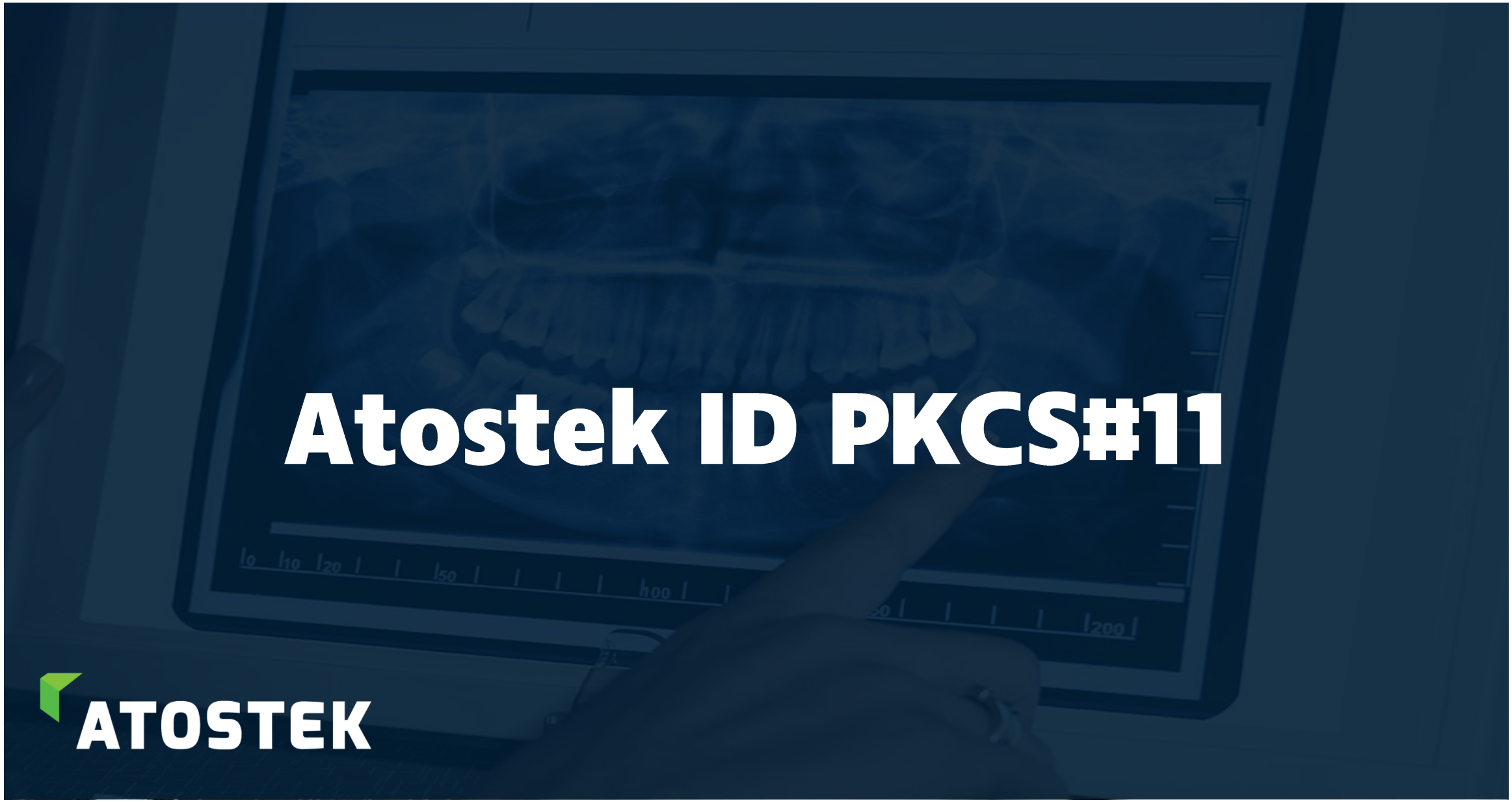
ATOSTEK

TokenDriver

- Toimikorttikirjautuminen MacOS työasemiin vaatii TokenDriverin toteuttamisen

- On sovittu DVV:n kanssa, että TokenDriver toteutetaan syksyllä elokuun ensimmäisen tuotantojulkaisun jälkeen

ATOSTEK


Atostek ID PKCS#11
ATOSTEK

PKCS#11 rajapinta yleisesti

- PKCS#11 standardi määrittelee Cryptoki rajapinnan, jonka kautta voidaan käyttää esimerkiksi älykorttia kryptografisten toimintojen suorittamiseen
- Toteutettu toimimaan juurikin Digi- ja väestötietoviraston tuottamien varmennekorttien kanssa
- Moduulista käännetään oma versio eri käyttöjärjestelmille
- Atostek ID PKCS#11 moduuli toteuttaa rajapinnan version 3.1
  - PKCS#11 rajapinnan dokumentaatio

ATOSTEK

PKCS#11 valmiusaste

- Atostek ID PKCS#11 rajapinnasta tulee testaajille ensimmäinen testiversio saataville keskiviikkona
  - Siitä kuitenkin puuttuu vielä komentoja

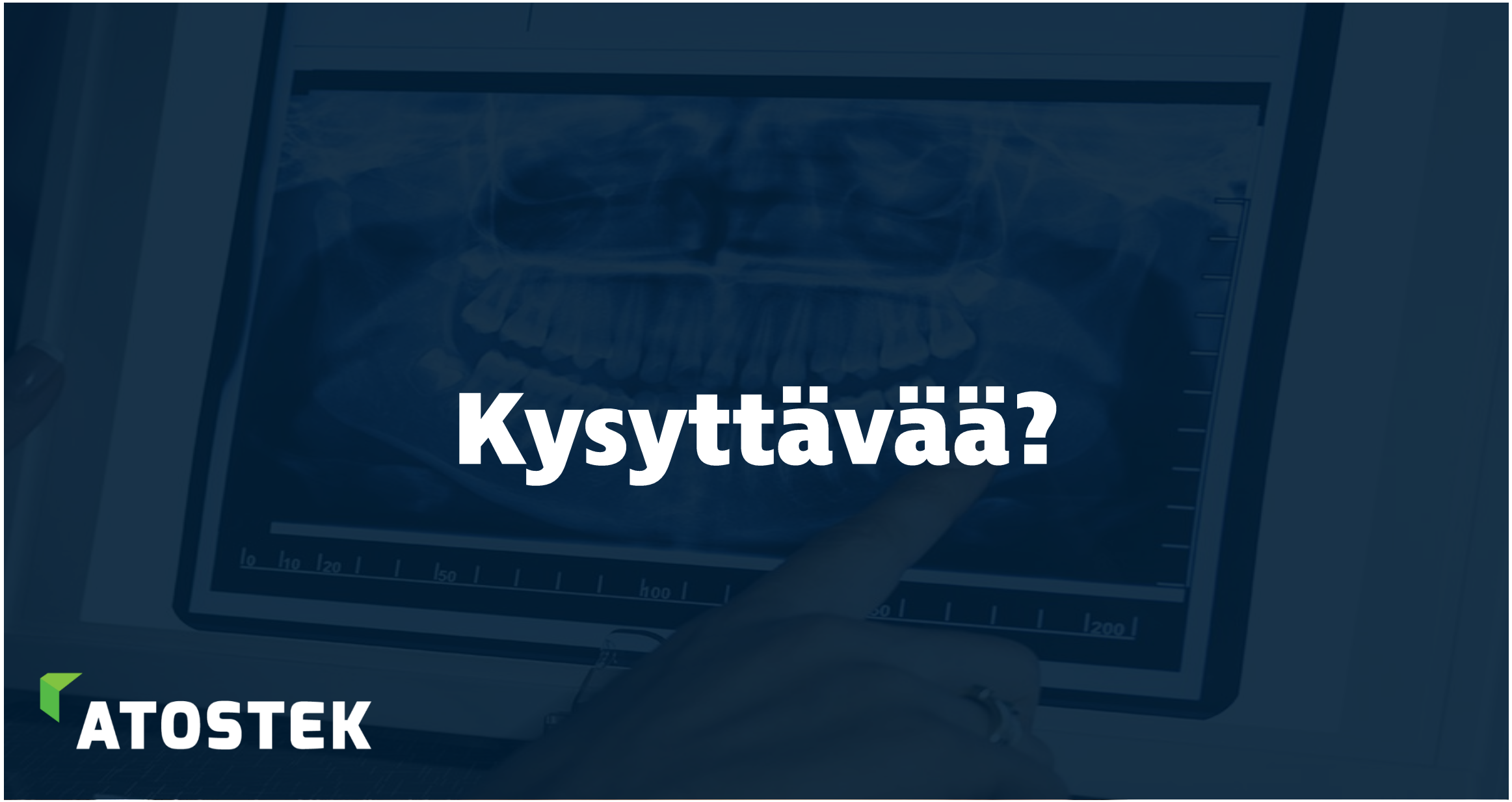
- Elokuun tuotantojulkaisussa
  - Lisää komentoja
  - Moduuli tulee suoraan Atostek ID asennuksen yhteydessä eikä sitä tarvitse ladata mistään erikseen

ATOSTEK

PKCS#11 käyttöönotto

- Moduulin käyttöönotto riippuu siitä, millä sovelluksella tai käyttöjärjestelmällä moduulia hyödynnetään
  - Esim. Adobe Acrobat Reader > Menu > Preferences > Signatures > Identities & Trusted Certificates > PKCS#11 Modules and Tokens
- Elokuun tuotantojulkaisun yhteydessä tulee enemmän dokumentaatiota ja ohjeistuksia moduulin käyttöönotosta eri käyttötapauksissa
- Käyttötapauksia käydään myös tarkemmin läpi elokuun integraatiokoulutuksissa

ATOSTEK


Kysyttävää?
ATOSTEK

Vastauksia chatissa esitettyihin kysymyksiin

- Mistä asennuspaketti löytyy?
  - Elokuun tuotantojulkaisun osalta asennuspaketit tulevat DVV:n sivuille ladattavaksi
  - Testiversioiden osalta asennuspaketit ovat saatavilla testaukseen ilmoittautuneille tahoille Atostekin Upload-palvelussa

- Onko oletuskieli suomi?
  - Windows ja MacOS asennuspaketeissa oletuskieli on järjestelmän kieli (suomi, ruotsi, englanti) tai englanti, jos järjestelmän kieli ei ole tuettujen kielten joukossa. Linux asennuspaketeissa oletus on vielä toistaiseksi suomi.

- Miten selvittää, mikä rajapinta tällä hetkellä on käytössä?
  - Kannattaa kysyä oman organisaation IT-henkilöstöltä, mihin rajapintoihin järjestelmänne on tähän mennessä integroitunut.

ATOSTEK

Chatissa esitettyjä huomioita

- "bcedit /set testsigning on" komentona on sellainen, että se vaatii lähes poikkeuksetta tietokoneen uudelleenkäynnistämisen, jotta se menee päälle.
  - Testin jälkeen asetus pitää muistaa laittaa pois päältä