Atostek ID: Integraatiokoulutus 1/2 (SCS-rajapinta)

7.8.2024

ATOSTEK

Sisältö

- Koulutuksen tarkoitus ja tavoite
- Atostek ID: Yleinen esittely ja sovelluksen asentaminen
- Rajapintojen lyhyt esittely
  - SCS
  - Minidriver, (TokenDriver)
  - PKCS#11
  - erasmartcard.ehoito.fi
- SCS-rajapinta
- Aikaa kysymyksille

- Tarvittaessa pidetään sopivassa välissä lyhyt tauko


Koulutuksen tarkoitus
ja tavoite
ATOSTEK

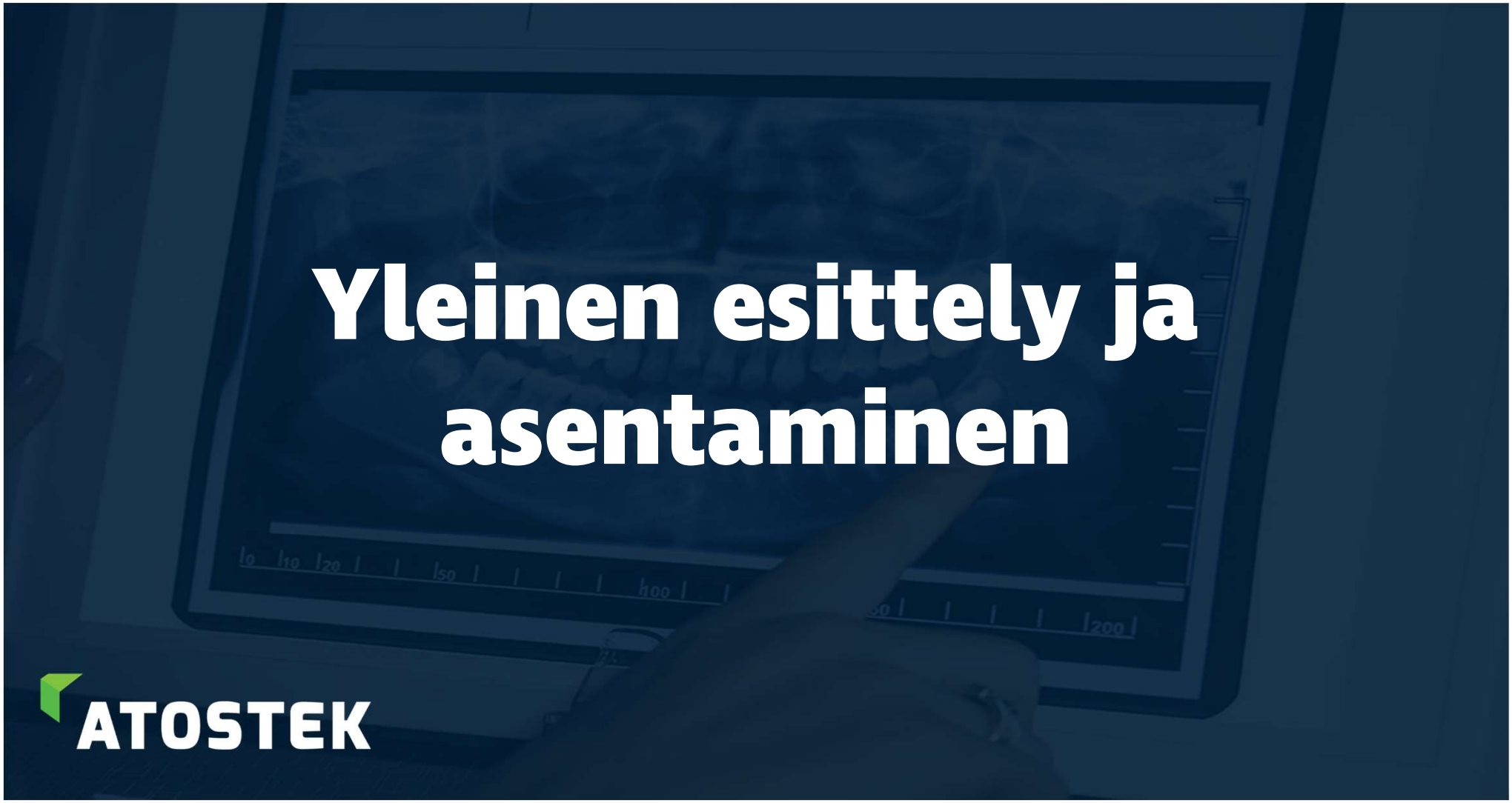
Tarkoitus ja tavoite

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

- Koulutus on kaksiosainen
  - Ensimmäisessä osassa (7.8.) käydään läpi SCS-rajapinta kokonaisuudessaan
  - Toisessa osassa (14.8.) käydään läpi Minidriver- ja PKCS#11-rajapinnat
  - Kesäkuussa järjestettiin ei-pakollinen integraatiokoulutuksen esiosa

- Koulutuksen tavoitteena on antaa Atostek ID -ohjelmistoon integroituville tahoille riittävät tiedot integraation suorittamiseen

ATOSTEK


Yleinen esittely ja asentaminen
ATOSTEK

Atostek ID

- Digi- ja väestötietoviraston uusi kortinlukijaohjelmisto
- Julkaistu rajatulle joukolle testaajia ensimmäinen ja toinen testiversio
- Elokuussa tehdään ensimmäinen tuotantojulkaisu ja pidetään kaksi integraatiokoulutusta (SCS + Minidriver & PKCS#11)
- Syyskuun alussa pidetään vielä käyttöönottokoulutus

Sovelluksen asentaminen

- Asennuspaketin yhteydessä tarjotaan käyttö- ja asennusohjeet joka alustalle. Niissä on tarkat ohjeet asennuksen suorittamiselle.
  - Asennuspaketit ja ohjeet tulevat hyväksyntätestauksen jälkeen saataville DVV:n sivuille ja Atostekin ajurilatauspalveluun
- 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

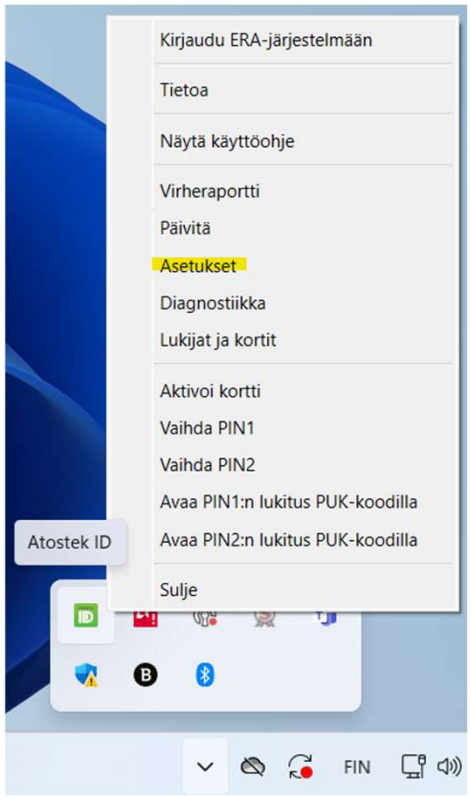
Asentaminen (Linux)

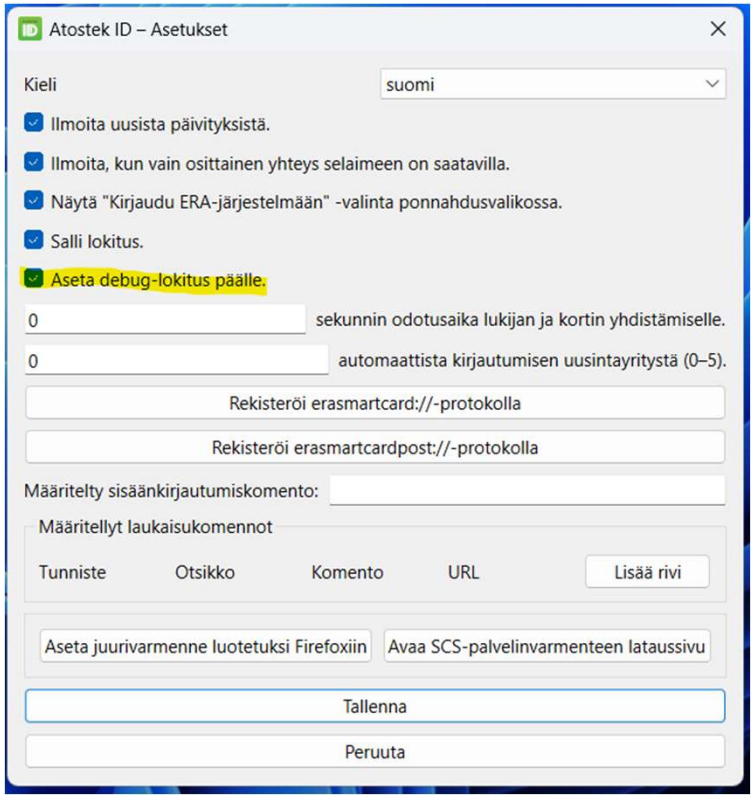
- Asennus Debianille:
  - sudo dpkg –i <paketin nimi>.deb
- Asennus Red Hatille:
  - sudo dnf install<paketin nimi>.rpm

- Mahdollisuus asetusparametrien käytölle tulee myöhemmissä tuotantojulkaisuissa

Debug-lokituksen käyttöönotto

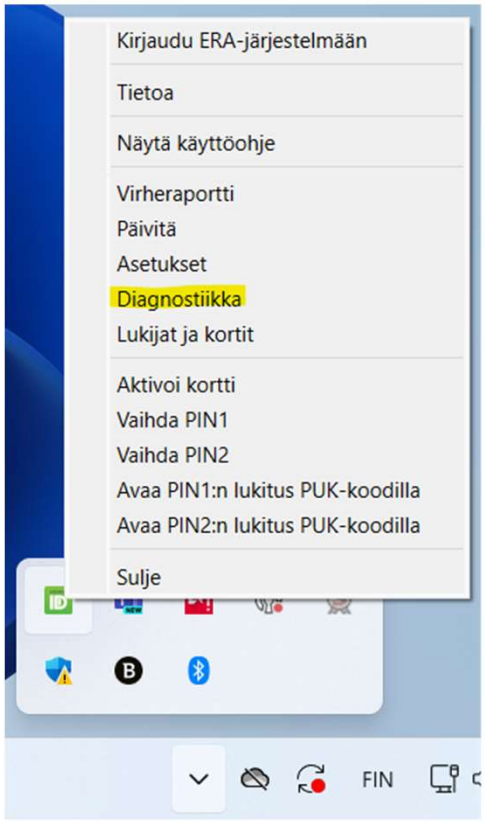
- Atostek ID – sovelluksen debug-tason lokituksen voi laittaa päälle asetuksista
  - Valikosta "Asetukset" → "Aseta debug-lokitus päälle" → "Tallenna"

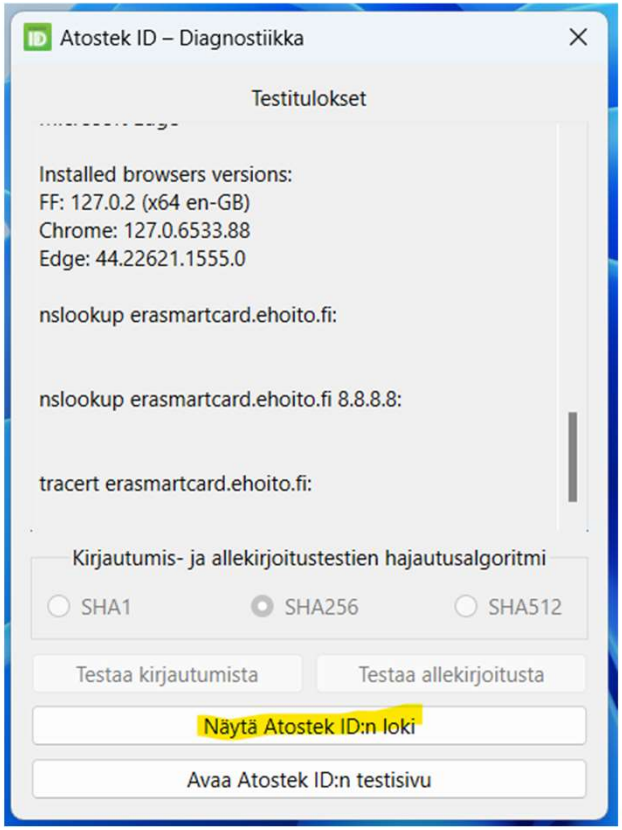




Virhelokin avaaminen

- Atostek ID – sovelluksen lokitiedoston voi avata diagnostiikka-näkymästä
  - Valikosta ”Diagnostiikka” → ”Näytä Atostek ID:n loki”






Rajapintojen lyhyet esittelyt
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

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 soveltuvin osin
  - Minidriver rajapintadokumentaatio

ATOSTEK

TokenDriverista

- Toimikorttikirjautuminen MacOS työasemiin vaatii TokenDriverin toteuttamisen

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

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 soveltuvin osin
  - PKCS#11 rajapinnan dokumentaatio

ATOSTEK

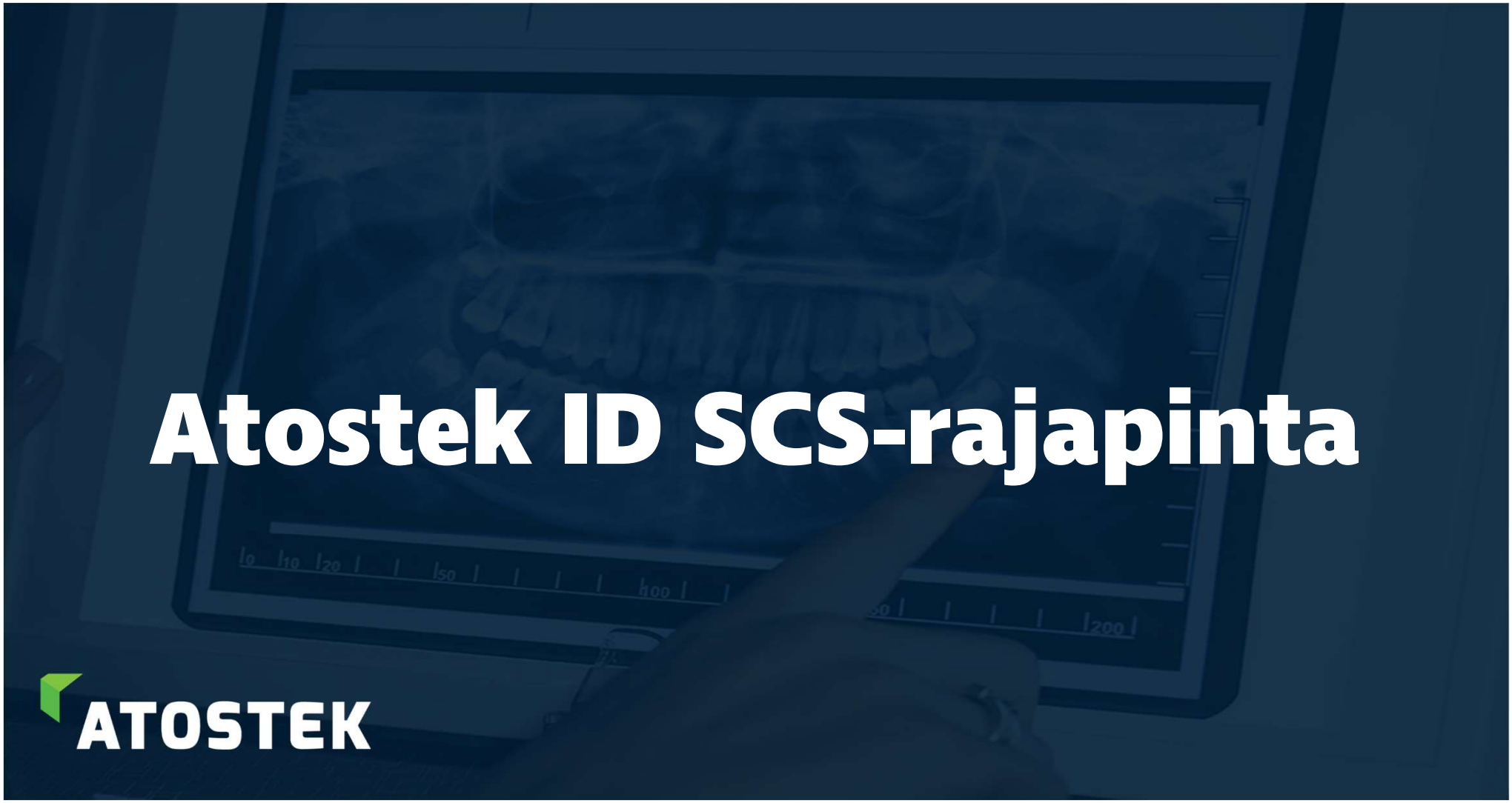
erasmartcard.ehoito.fi-rajapinta

- 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 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

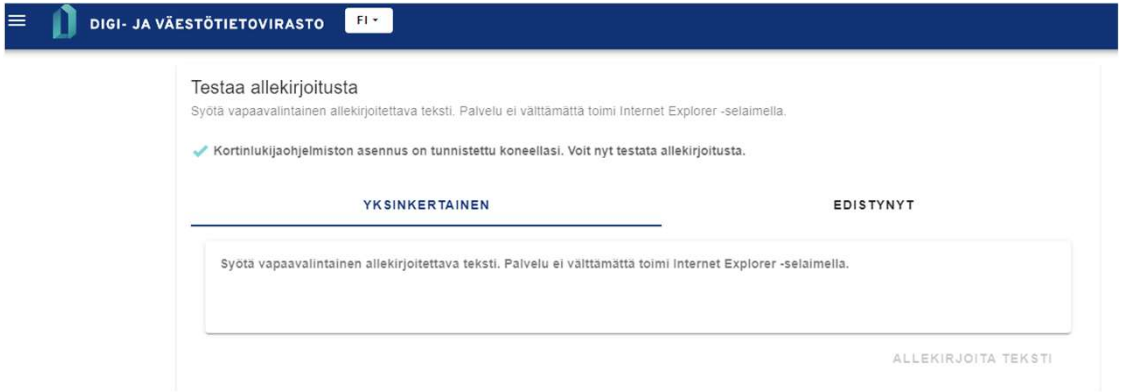
SCS-rajapinta: integroituminen

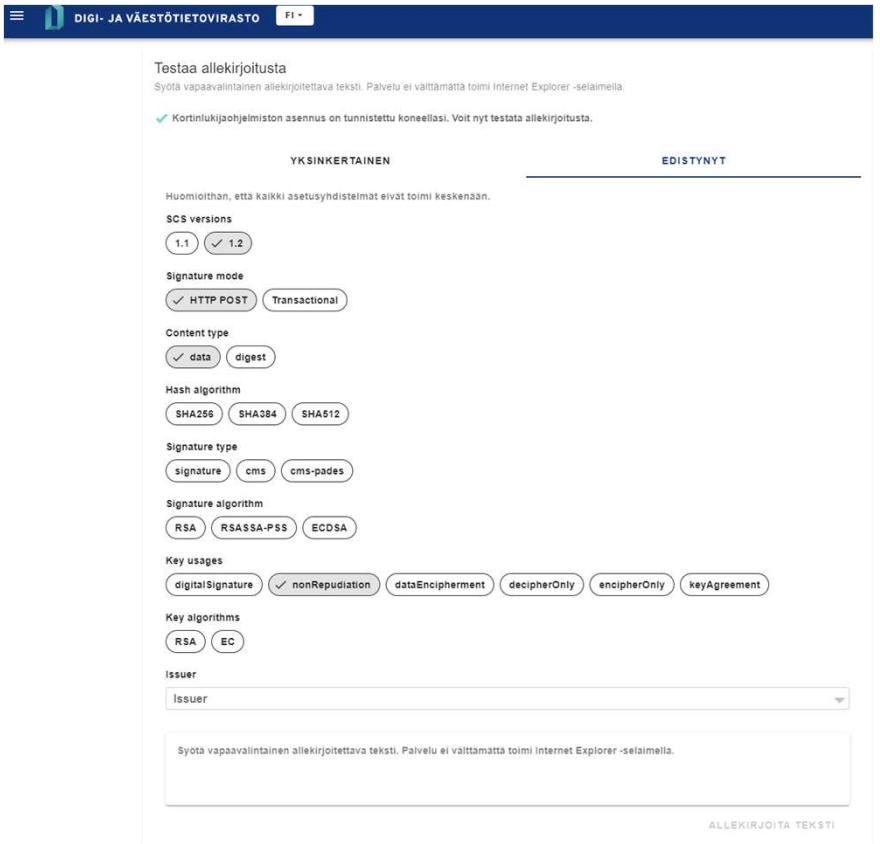
- Atotek ID toteuttaa saman SCS-rajapinnan kuin Fujitsun DigiSign. Tämän myötä **integroivan järjestelmän ei pitäisi joutua tekemään muutoksia**, kun Atostek ID –sovelluksen SCS-rajapinta vaihdetaan DigiSign-sovelluksen rajapinnan tilalle.

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

ATOSTEK

SCS-rajapinta: integroituminen





ATOSTEK

SCS-rajapinta: tunnistetut puutteet

- Ohjelmiston ensimmäisessä tuotantojulkaisussa on tunnistettuja puutteita SCS-rajapinnan osalta, jotka toteutetaan myöhemmissä julkaisuissa
  - Allekirjoitustyypit ”cms” ja ”cms-pades”
  - Kommunikointi JSON Web Tokenien avulla (transactions)

- Korjaukset ja tarvittavat implementoinnit tehdään myöhempiin tuotantoversioihin
- Yhteydenotot virhetilanteissa sähköpostiin atostek-id@atostek.com
  - Tämä kanava vain bugien raportointia varten
  - Raportoinnin sisältöön ja muotoiluun on erilliset ohjeet

ATOSTEK

SCS-rajapinta: varmenteet ja palvelin

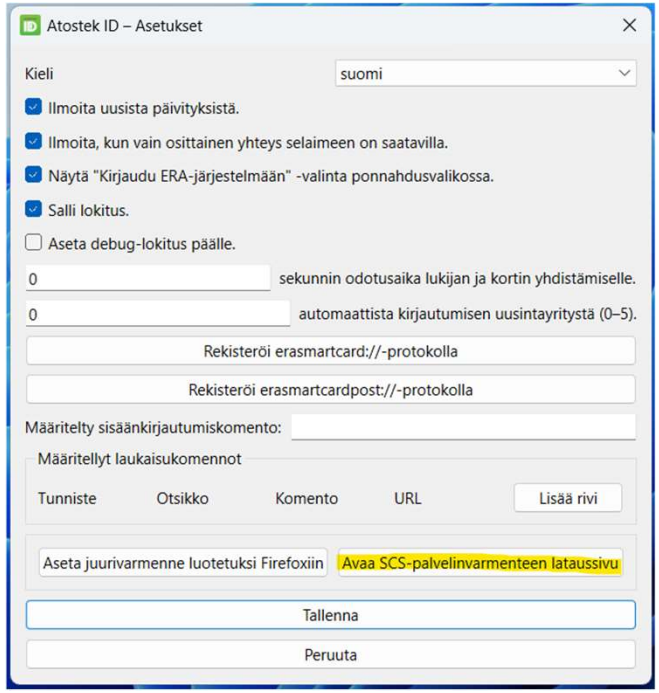
- Atostek ID luo asennuksen yhteydessä HTTPS-palvelimen tarvitsemat varmenteet
  - Palvelinvarmenteen myöntävä varmenne *Atostek ID Local SCS CA* pistetään samalla luotetuksi **käyttöjärjestelmän varmennesäilöön**
  - Luodut varmenteet (scscert.pfx ja scsca.cer) tallentuvat käyttöjärjestelmän oletussijaintiin
    - Windows: C:\Users\<käyttäjä>\AppData\Local\Atostek Oy\Atostek ID
    - MacOS: <käyttäjän kotikansio>/Library/Application Support/Atostek Oy/Atostek ID
    - Linux: <käyttäjän kotikansio>/.local/share/Atostek Oy/Atostek ID

- 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:** DigiSign ei saa olla asennettu ja käynnissä ennen Atostek ID käynnistämistä

ATOSTEK

SCS-rajapinta: varmenteet ja palvelin

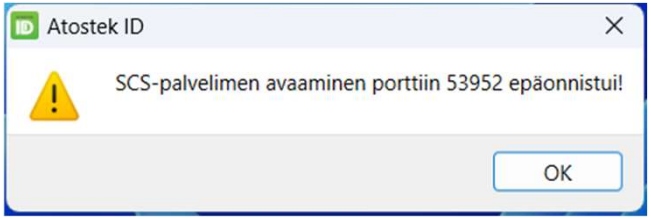
- Huomioi, että varmenne ei Linuxilla asennu toistaiseksi automaattisesti luotetuksi Firefoxin varmennesäilöön
  - Varmenteen saa ladattua sovelluksesta *Asetukset > Avaa SCS-palvelinvarmenteen lataussivu*
  - Sivulla myös ohjeet siitä, miten varmenne asetetaan luotetuksi Firefoxilla

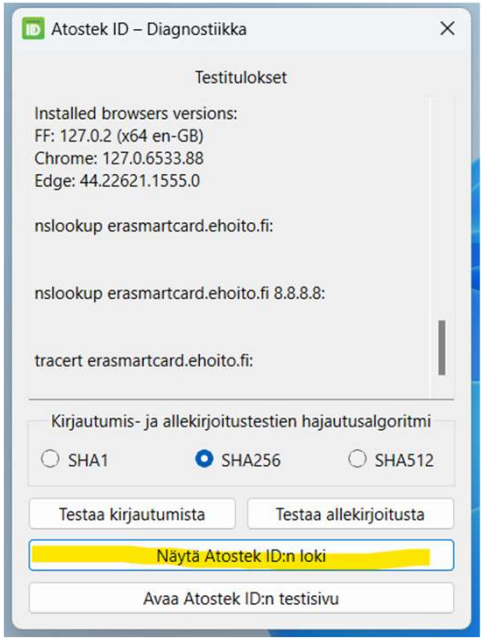


ATOSTEK

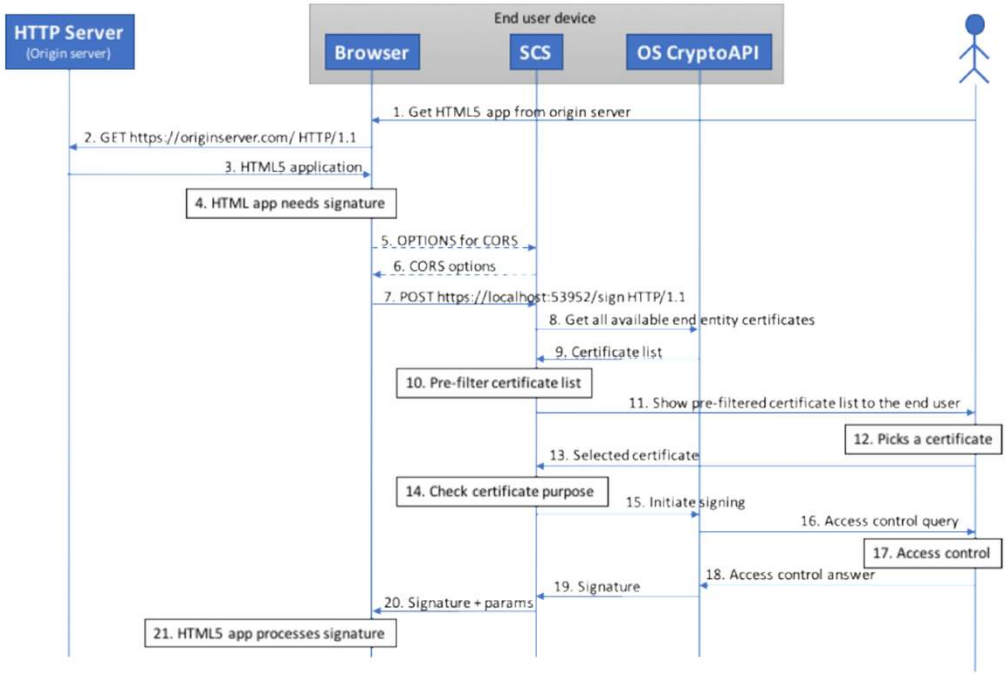
SCS-rajapinta: varmenteet ja palvelin

- Sekä palvelinvarmenne (scscert.pfx) että juurivarmenne (scsca.cer) tarvitaan, jotta SCS-palvelin toimii oikein
- Mahdollisia ongelmatilanteita
  - Atostek ID –sovelluksen asennusta ei suoriteta riittävillä oikeuksilla, jolloin esimerkiksi
    - Varmenteita ei saada tallennettua oletussijaintiin
    - Palvelinvarmenteen myöntävää juurivarmennetta ei saada lisättyä käyttöjärjestelmän varmennesäilöön
  - DigiSign on asennettuna ja käynnissä samaan aikaan
    - Tämä estää Atostek ID –sovelluksen SCS-palvelimen käynnistymisen samaan porttiin 53952
- SCS-palvelin on saatu pystytettyä ja varmenteet generoitua oikein, jos testisivu https://localhost:53952/ avautuu ilman varoituksia ja sivulla lukee teksti *Atostek ID SCS test page loaded OK.*





SCS-rajapinta: sekvenssikaavio



https://dvv.fi/documents/16079645/17324992/DVV-SCS_HTML5-and-Digital-Signatures.pdf/dbb89387-6aaa-4c0e-5ac3-f69b234ee25b/DVV-SCS_HTML5-and-Digital-Signatures.pdf?t=1697787548881

ATOSTEK

SCS-rajapinta: rajapinnan funktiot

- SCS-rajapintaan https://localhost:53952/ voi lähettää HTTP/1.1-protokollan mukaisia pyyntöjä
- Versiossa 1.2 tuetut pyynnöt
  - GET /version
  - POST /sign
  - GET /sign

ATOSTEK

SCS-rajapinta: GET /version

- Saadaan tieto käytössä olevan SCS-rajapinnan versiosta ja tuetuista toiminnallisuuksista
- Pyynnössä ei anneta parametreja
- Vastauksena saadaan listaus SCS-rajapinnan tiedoista

ATOSTEK

SCS-rajapinta: GET /version pyyntö

- GET https://localhost:53952/version
- Pyynnössä ei anneta parametreja

ATOSTEK

SCS-rajapinta: GET /version vastaus

- Parametrien tarkemmat kuvaukset löytyvät SCS-rajapinnan dokumentaatiosta.


```
{
  "applicationOIDs": "1.2.246.517.4.1.7",
  "contentTypes": "data, digest",
  "hashAlgorithms": "SHA256, SHA384, SHA512",
  "httpMethods": "GET, POST",
  "selectorAvailable": true,
  "signatureAlgorithms": "ECDSA",
  "signatureTypes": "signature,signature-plain,cms,cms-pades",
  "version": "1.2"
}
```


ATOSTEK

SCS-rajapinta: POST/GET /sign

- Muodostetaan sähköinen allekirjoitus toimikortin avulla
- Pyynnössä annetaan vähintäänkin allekirjoitettava data
- Muut parametrit täsmentävät pyyntöä, esimerkiksi:
  - Minkälaisella varmenteella allekirjoitus halutaan tehdä
  - Mitä tiivistealgoritmia halutaan käyttää
  - Minkälainen sähköinen allekirjoitus halutaan muodostaa
    - Tällä hetkellä tuettuna on vain kortin raaka allekirjoitus

ATOSTEK

SCS-rajapinta: POST /sign pyyntö

- POST https://localhost:53952/sign
- Parametrien tarkemmat kuvaukset löytyvät SCS-rajapinnan dokumentaatiosta.
- "content"-parametri ainoa pakollinen
  - Allekirjoitettava data Base64-enkoodattuna

```
{
  "version": "1.2",
  "selector": {
    "keyusages": [
      "nonRepudiation"
    ]
  },
  "content": "VGVzdGk=",
  "contentType": "data",
  "hashAlgorithm": "SHA512",
  "signatureType": "signature"
}
```

ATOSTEK

SCS-rajapinta: GET /sign pyyntö

- GET https://localhost:53952/sign?<pyynnön parametrit>
- Huomaa, että selector-parametria ei voi antaa GET /sign -pyynnössä!

- https://localhost:53952/sign?content=VGVzdGk=&hashAlgorithm=SHA512

ATOSTEK

SCS-rajapinta: POST /sign vastaus

- Parametrien tarkemmat kuvaukset löytyvät SCS-rajapinnan dokumentaatiosta.


```
{
  "chain": [
    "MIIHbD...DwWcZ0k=",
    "MIIH1jC...OF92bo9",
    "MIIGM...uFMNbWu"
  ],
  "reasonCode": 200,
  "reasonText": "Signature created successfully",
  "signature": "ZoF7...h3NFfv",
  "signatureAlgorithm": "SHA512withRSA",
  "signatureType": "signature",
  "status": "ok",
  "version": "1.2"
}
```


ATOSTEK

SCS-rajapinta: virhekoodit

- Allekirjoituspyynnön vastauksessa löytyy aina pyynnön onnistumisesta/epäonnistumisesta kertovat parametrit
  - Status ("ok"/"failed")
  - ReasonCode
  - ReasonText
- Näiden tarkemmat kuvaukset löytyvät SCS-rajapinnan dokumentaatiosta.

ATOSTEK

SCS-rajapinta: virhekoodit


```
{
   "reasonCode": 400,
   "reasonText": "Bad request: Given JSON is not valid.",
   "status": "failed",
   "version": "1.2"
}
```

```
{
   "reasonCode": 401,
   "reasonText": "Unauthorized: No smart card found",
   "status": "failed",
   "version": "1.2"
}
```

```
{
   "reasonCode": 501,
   "reasonText": "Not Implemented: Signature type cms-pades not implemented",
   "status": "failed",
   "version": "1.2"
}
```

```
{
   "reasonCode": 400,
   "reasonText": "Bad request: Missing mandatory parameters (content)",
   "status": "failed",
   "version": "1.2"
}
```


ATOSTEK

SCS-rajapinta: ongelmatilanteet

- Raportoittehan ongelmatilanteet tuotantojulkaisun yhteydessä välitettyjen ohjeiden mukaisesti.
  - atostek-id@atostek.com

- SCS-rajapinnan osalta on ongelmatilanteissa yleensä mielekästä tietää tarkkaan, **minkälaisen pyynnön integroiva järjestelmä lähettää kortinlukijaohjelmiston SCS-rajapintaan** ja **minkälaisen vastauksen rajapinta palauttaa.**
  - Pyyntö ja vastauksen status lokitetaan DEBUG-tasolla virhelokiin

ATOSTEK

SCS-rajapinta: tulevat ominaisuudet

- Allekirjoitustyypit "cms" ja "cms-pades"
  - Noudattavat CMS-allekirjoitusformaattia, jossa mukana on esimerkiksi allekirjoituksen aikaleima
  - "cms-pades" tarkoitettu erityisesti PDF-dokumenttien allekirjoitukseen
  - Saadaan myöhemmissä tuotantojulkaisuissa käyttöön POST /sign –pyynnössä
    - signatureType-parametri

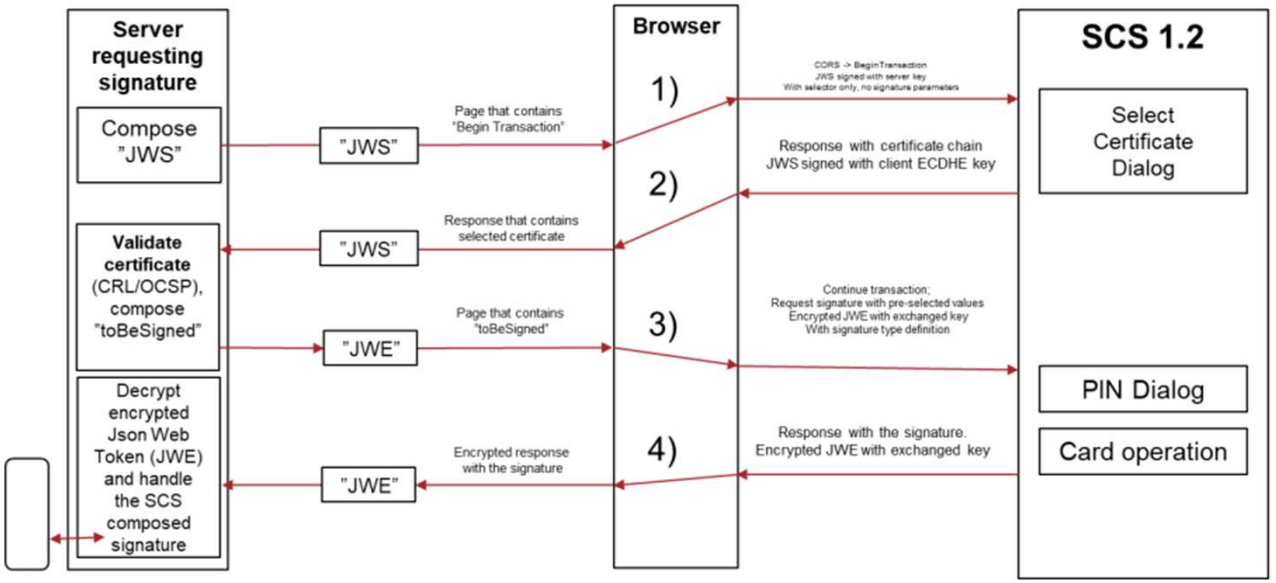
ATOSTEK

SCS-rajapinta: tulevat ominaisuudet

- Kommunikointi JSON Web Tokenien avulla (transactions)
  - Uusi ominaisuus versiossa 1.2
  - Turvallisempi tapa kommunikoida allekirjoituspyynnön lähettävän tahon ja SCS-rajapinnan välillä
  - Perustuu siihen, että allekirjoituspyynnön lähettävä taho ja SCS-rajapinta luovat yhteisen salausavaimen (ECDH), jolla kommunikointi salataan
  - Yksityiskohdat SCS-rajapinnan dokumentaatiossa

ATOSTEK

SCS-rajapinta: tulevat ominaisuudet

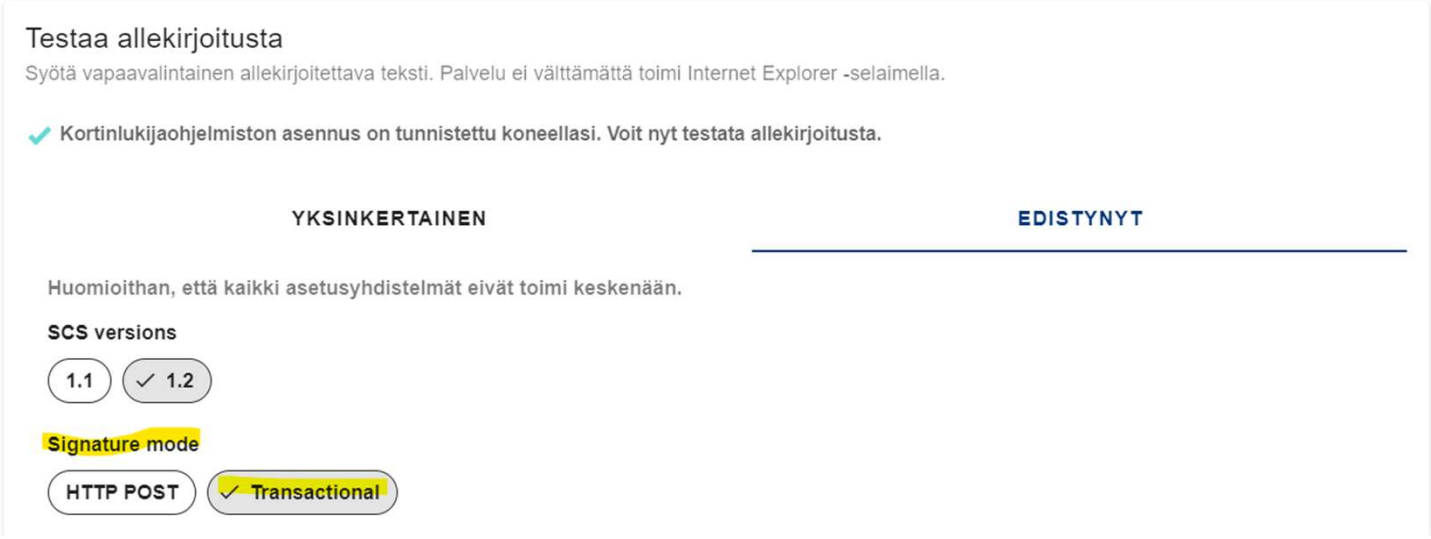


https://dvv.fi/documents/16079645/17324992/DVV-SCS_HTML5-and-Digital-Signatures.pdf/dbb89387-6aaa-4c0e-5ac3-f69b234ee25b/DVV-SCS_HTML5-and-Digital-Signatures.pdf?t=1697787548881

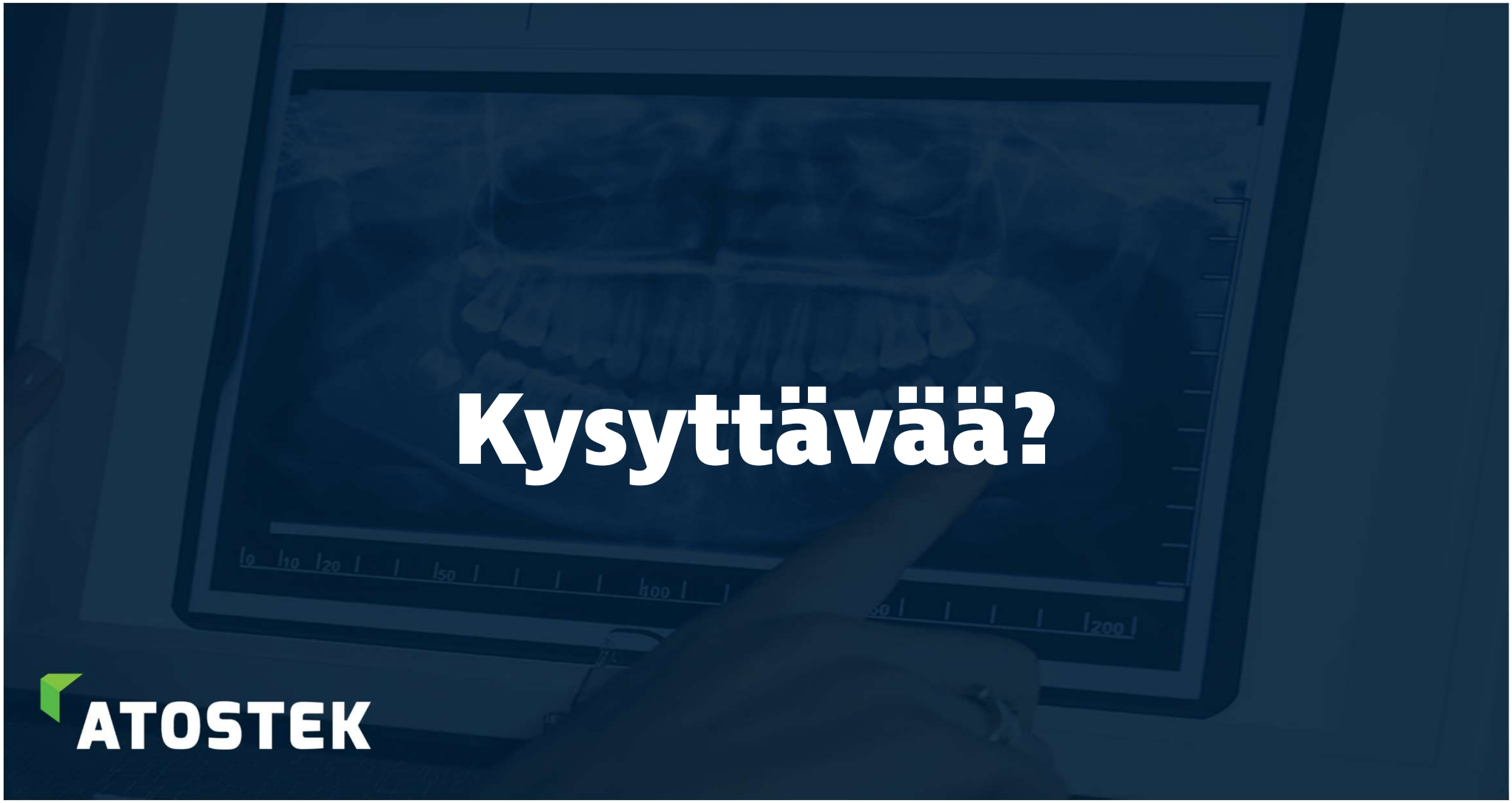
ATOSTEK

SCS-rajapinta: tulevat ominaisuudet

- Ominaisuutta voi jatkossa testata DVV:n testisivulta



ATOSTEK


Kysyttävää?
ATOSTEK

Vastauksia chatissa esitettyihin kysymyksiin

- Kuinka laajalti SCS-rajapinta on nykyisellään käytössä? Millaisia ovat sen pääasialliset käyttötapaukset?
  - SCS-rajapinta on avoin dokumentti, jonka käyttöä ei seurata, joten käytön laajuudesta on vaikea mennä takuuseen. Merkittävin käyttökohde lienee Kelan Kelain-sovellus.
- Millä aikataululla signatureType ”cms” on tulossa mukaan?
  - Alustavan suunnitelman mukaan tämä julkaistaan viimeistään marraskuun toisessa tuotantojulkaisussa. Samaan julkaisuun pyritään saamaan JSON Web Tokeneilla kommunikointi tavallisen viestintätavan rinnalle.
- Onko henkilökortille tulossa tukea julkisella avaimella tehtävään salaukseen ja salauksen purkuun?
  - Henkilökortilla ei suoranaisesti ole estettä tälle, vaikka käyttötapaus onkin harvinainen tavallisen käyttäjän näkökulmasta. Tämän käytölle ei DVV:llä ole kuitenkaan erillistä ohjeistusta.

ATOSTEK

Vastauksia chatissa esitettyihin kysymyksiin

- SCS-rajapinta ja tiivisteen allekirjoittaminen
  - Allekirjoitettava data voi olla joko alkuperäinen data tai siitä muodostettu tiiviste. Tämä määritetään contentType-parametrilla (”data”/”digest”).
  - Jos allekirjoitettava data ei ole tiiviste, tiivistää SCS-rajapinta datan annetulla tiivistealgoritmilla. Jos algoritmia ei ole annettu, käytetään oletuksena SHA256-algoritmia.
  - Jos allekirjoitettava data on tiiviste, pitää käytetty tiivistealgoritmi antaa pyynnössä, jotta SCS-rajapinta voi validoida tiivisteen.
  - CMS-allekirjoituksessa allekirjoitettavaa dataa ei liitetä palautuvaan allekirjoitukseen, mikäli data oli alkujaan tiiviste.

ATOSTEK

Chatissa esitettyjä huomioita

- Kaikki Atostek ID -koulutukset tallennetaan ja tallenteet ja materiaalit julkaistaan DVV:n verkkosivuilla www.dvv.fi/kortinlukijaohjelmisto.

ATOSTEK