Atostek ID: Integrationsutbildning 1/2 (SCS-gränssnitt)

7.8.2024

ATOSTEK

Innehåll

- Utbildningens syfte och målsättning
- Atostek ID: Allmän presentation och installation av applikationen
- Kort presentation av gränssnitten
  - SCS
  - Minidriver, (TokenDriver)
  - PKCS#11
  - erasmartcard.ehoito.fi
- SCS-gränssnittet
- Tid för frågor

- Vid behov hålls en kort paus vid lämpligt tillfälle

Utbildningens syfte och målsättning

ATOSTEK

Syfte och målsättning

- Denna utbildning riktar sig till de aktörer vars system integreras i användningen av Atostek ID-programmets SCS-gränssnitt

- Utbildningen består av två delar
  - I den första delen (7.8) går vi igenom SCS-gränssnittet i sin helhet
  - I den andra delen (14.8) går vi igenom Minidriver- och PKCS#11-gränssnitten.
  - I juni ordnades en icke-obligatorisk förhandsdel till integrationsutbildningen

- Målet med utbildningen är att ge aktörer som integreras i Atostek ID tillräcklig information för att genomföra integrationen

ATOSTEK

Allmän presentation och installation

ATOSTEK

Atostek ID

- Myndigheten för digitalisering och befolkningsdatas nya kortläsarprogram
- Den första och andra testversionen har publicerats för ett begränsat antal testare
- I augusti görs den första produktionspublikationen och två integrationsutbildningar ordnas (SCS + Minidriver & PKCS#11)
- I början av september ordnas ännu en ibruktagningsutbildning

Installation av applikationen

- I samband med installationspaketet erbjuds bruks- och installationsanvisningar för varje plattform. De innehåller noggranna anvisningar för installationen.
  - Installationspaketen och anvisningarna blir efter godkännandetestningen tillgängliga på MDB:s webbplats och i Atosteks laddningstjänst för drivrutin
- Standardinställningar kan användas på alla plattformar. Alla gränssnitt som ska integreras är tillgängliga i och med standardinställningarna.
- I samband med installationerna kan man välja på vilket språk Atostek ID installeras på enheten.

Installation (Windows)

- Installation med användargränssnitt: Klicka på applikationens .msi installationspaket för att öppna det och gör installationen enligt anvisningarna i gränssnittet.
- Installation på kommandoraden (med admin-rättigheter):
  - Kör kommandot *msiexec /quiet /i <paketin nimi>.msi*
  - Om du vill kan du ange installationsparametrar, till exempel *msiexec /quiet /i <paketin nimi>.msi LANGUAGE="en"*
- Programmet installeras som standard i mappen *C:\Program Files (x86)*
- Applikationens fellogg och konfigurationsfil sparas under användarens mapp *AppData\Local\Atostek Oy*
- Applikationen syns i de dolda ikonerna i uppgiftsfältet

Installation (MacOS)

- Installation med användargränssnitt: Klicka på applikationens .pkg installationspaket för att öppna det och gör installationen enligt anvisningarna i gränssnittet.
- Installation från kommandoraden (sudo):
  - Kör kommando *sudo –installer –pkg <paketin nimi>.pkg –target /*
  - Om du vill kan du ange installationsparameterfilen, där kan du till exempel ange parametern LANGUAGE=fi

- Programmet installeras som standard i mappen */Applications*
- Applikationens fellogg och konfigurationsfil sparas under användarens mapp *AppData\Local\Atostek Oy*

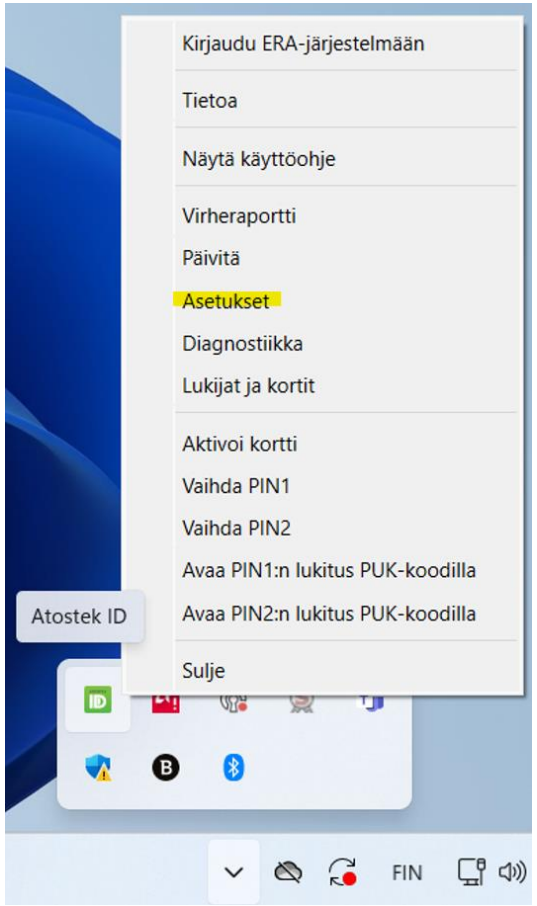
Installation (Linux)

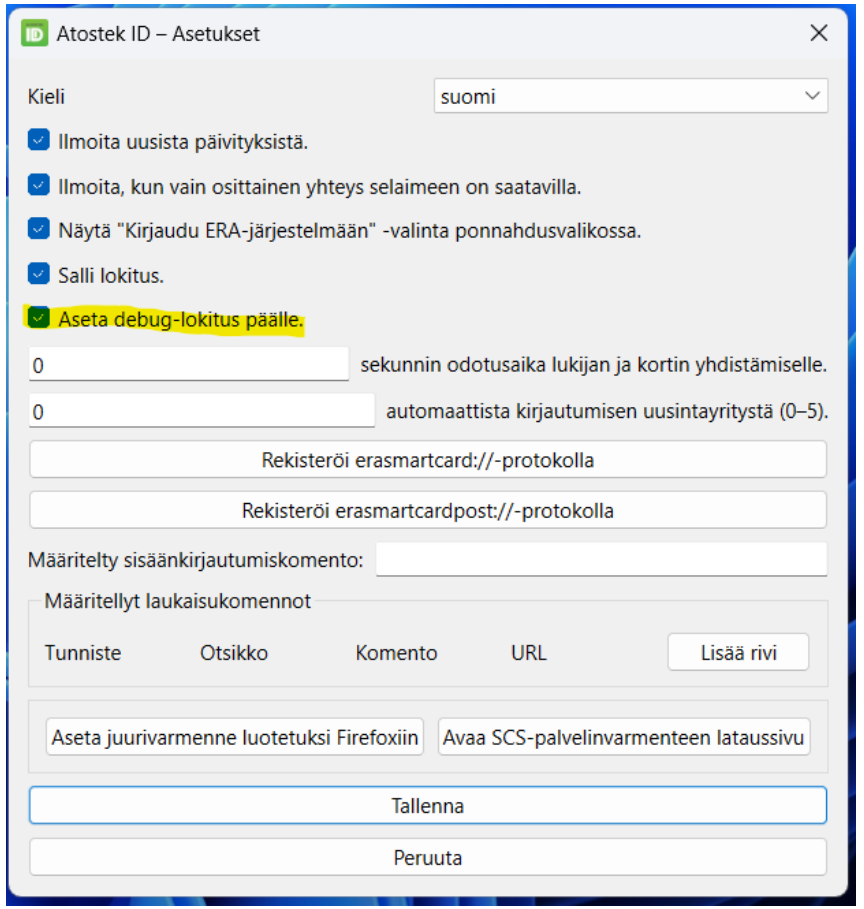
- Installation i Debian:
  - sudo dpkg –i <paketin nimi>.deb
- Installation i Red Hat:
  - sudo dnf install<paketin nimi>.rpm

- Möjlighet att använda inställningsparametrar kommer senare i produktionspublikationen

Drifttagning av debug-loggning

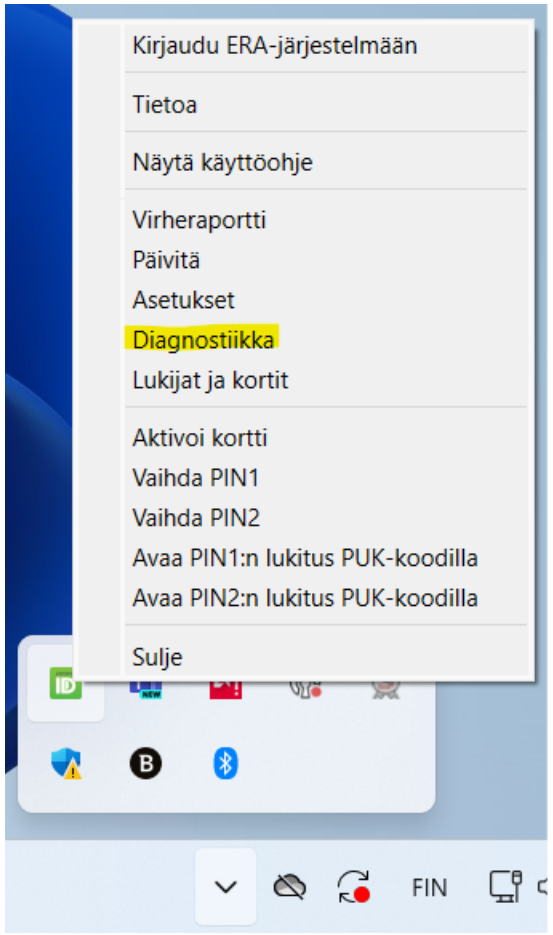
- Loggningen av applikationen Atostek ID på debug-nivå kan aktiveras i inställningarna
  - I menyn "Inställningar" → "Aktivera debug-loggning" → "Spara"

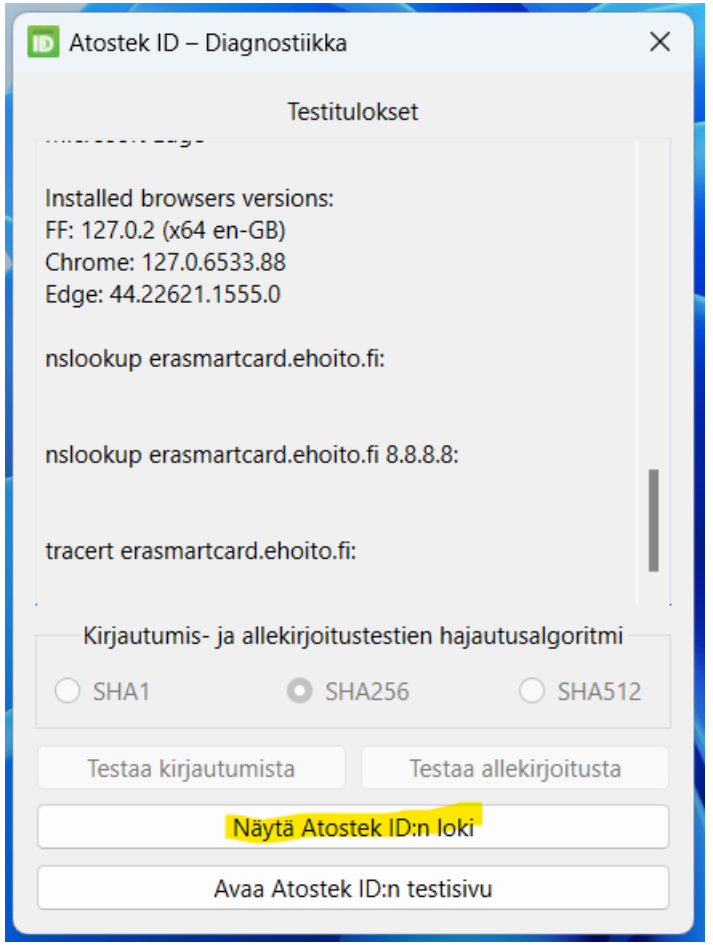




Öppning av fellogg

- Loggfilen för Atostek ID kan öppnas i diagnostikvyn
  - I menyn "Diagnostik" → "Visa logg för Atostek ID"





Korta presentationer av gränssnitten

ATOSTEK

SCS-gränssnittet i allmänhet

- Signature Creation Service
- Av MDB fastställt gränssnitt för signaturer med kortläsarapplikationen via HTTP-gränssnittet
- Atostek ID implementerar både versionerna 1.1 och 1.2 av SCS-gränssnittet.
- Dokumentation av gränssnittet och närmare specificeringar: FINEID-specificeringar

ATOSTEK

SCS-gränssnittet i allmänhet

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 i allmänhet

- Modul (dll) för Windows-operativsystem för kommunikation med smartkort
- Implementerat för att fungera med certifikatkort som producerats av Myndigheten för digitalisering och befolkningsdata
- Operativsystemet utnyttjar Minidriver direkt till exempel vid inloggning på arbetsstationen
- Andra applikationer kan också utnyttja Minidriver till exempel för att göra signaturer
- Atostek ID Minidriver implementerar versionen 7.07 av gränssnittet i tillämpliga delar.
  - Minidriver gränssnittsdokumentation

ATOSTEK

Om TokenDriver

- Inloggning med certifikatkort i MacOS-arbetsstationer kräver att TokenDriver implementeras

- Man har kommit överens med MDB om att TokenDriver genomförs på hösten efter den första produktionspublikationen i augusti

ATOSTEK

PKCS#11 gränssnitt i allmänhet

- Standarden PKCS#11 definieras av gränssnittet Cryptokis, via vilket man till exempel kan använda smartkort för att utföra kryptografiska funktioner
- Implementerat för att fungera med certifikatkort som producerats av Myndigheten för digitalisering och befolkningsdata
- En egen version av modulen skapas för olika operativsystem
- Modulen Atostek ID PKCS#11 implementerar versionen 3.1 av gränssnittet i tillämpliga delar
  - PKCS#11 gränssnittets dokumentation

ATOSTEK

erasmartcard.ehoito.fi gränssnitt

- Produktens eget gränssnitt erasmartcard.ehoito.fi fungerar parallellt med SCS-gränssnittet och dessa gränssnitt påverkar inte varandras användning

- System som redan tidigare integrerats i gränssnittet erasmartcard.ehoito.fi kan fortsätta att använda gränssnittet som normalt

- Anvisningarna för användning eller dokumentation av gränssnittet på erasmartcard.ehoito.fi ingår inte i detta leveransprojekt och om man vill kan man kontakta Atostek direkt i anslutning till användningen av gränssnittet.

ATOSTEK

Atostek ID SCS-gränssnitt

ATOSTEK

SCS-gränssnittet i allmänhet

- Signature Creation Service
- Av MDB fastställt gränssnitt för signaturer med kortläsarapplikationen via HTTP-gränssnittet
- Atostek ID implementerar både versionerna 1.1 och 1.2 av SCS-gränssnittet.
- Dokumentation av gränssnittet och närmare specificeringar: FINEID-specificeringar

ATOSTEK

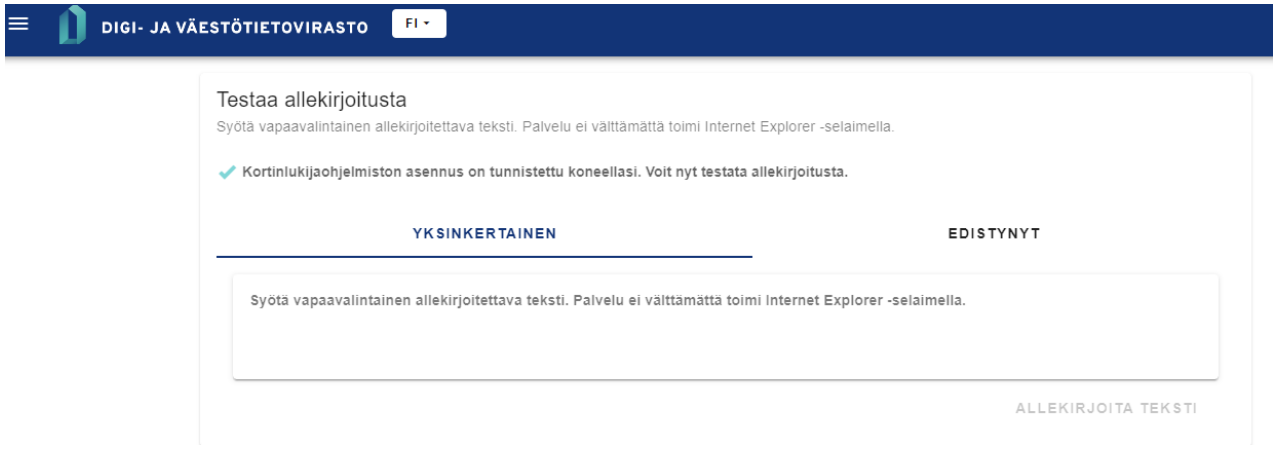
SCS-gränssnittet: integration

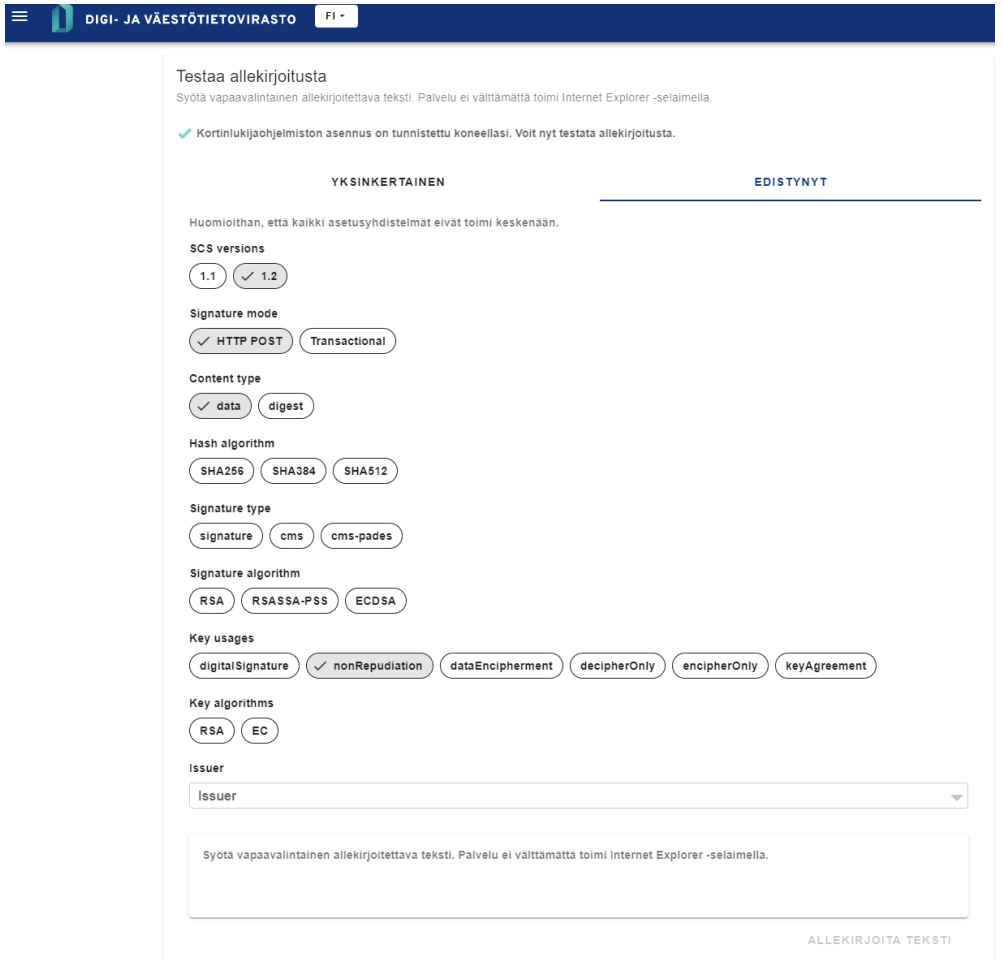
- Atostek ID genomför samma SCS-gränssnitt som Fujitsus DigiSign. I och med detta **borde det inte vara nödvändigt att göra ändringar i systemet som integreras** när Atostek ID-applikationens SCS-gränssnitt byts ut mot DigiSign-applikationens gränssnitt.

- SCS-gränssnittets funktion kan också testas till exempel via MDB:s testsida.

ATOSTEK

SCS-gränssnittet: integration





ATOSTEK

SCS-gränssnittet: identifierade brister

- I programvarans första produktionspublikation finns identifierade brister i SCS-gränssnittet, som genomförs i senare publikationer
  - Signaturtyperna "cms" och "cms-pades”
  - Kommunikation med hjälp av JSON Web Token (transactions)

- Korrigeringar och nödvändiga implementeringar görs i senare produktionsversioner
- Kontakt per e-post i felsituationer atostek-id@atostek.com
  - Denna kanal endast för rapportering av bugie
  - Det finns separata anvisningar för rapporteringens innehåll och utformning

ATOSTEK

SCS-gränssnittet: certifikat och server

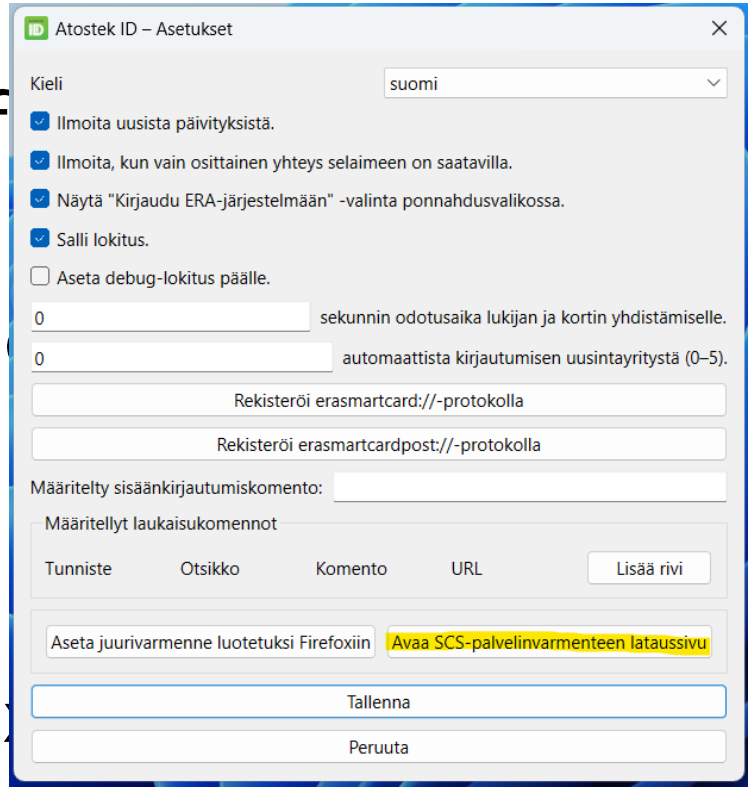
- Atostek ID skapar i samband med installationen de certifikat som behövs för HTTPS-servern
  - Det servercertifikat beviljande certifikatet *Atostek ID Local SCS CA* läggs samtidigt till som betrott **i operativsystemets certifikatlager**
  - Skapade certifikat (scscert.pfx och scsca.cer) sparas i operativsystemets standardposition
    - 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

- När applikationen startar startas också en HTTPS-server som genomför SCS-gränssnittet och som finns i port **53952**
  - https://localhost:53952/
  - På sidan texten *Atostek ID SCS test page loaded OK*.
  - **OBS:** DigiSign får inte vara installerat och igång innan Atostek ID startas

ATOSTEK

SCS-gränssnittet: certifikat och server

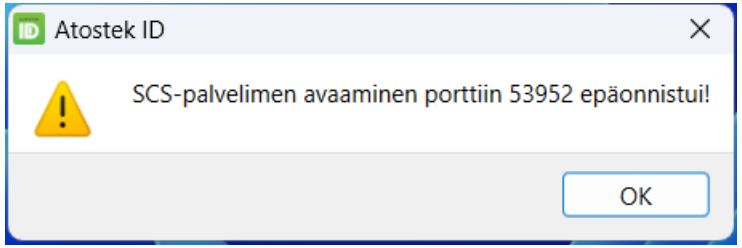
- Observera att certifikatet på Linux tills vidare inte automatiskt installeras i Firef certifikatlager
  - Certifikatet kan laddas ner från applikation *Inställningar > Nedladdningssida för SCS-servercertifikat*
  - På sidan finns också anvisningar om hur certifikatet ställs in som betrott med Firefo

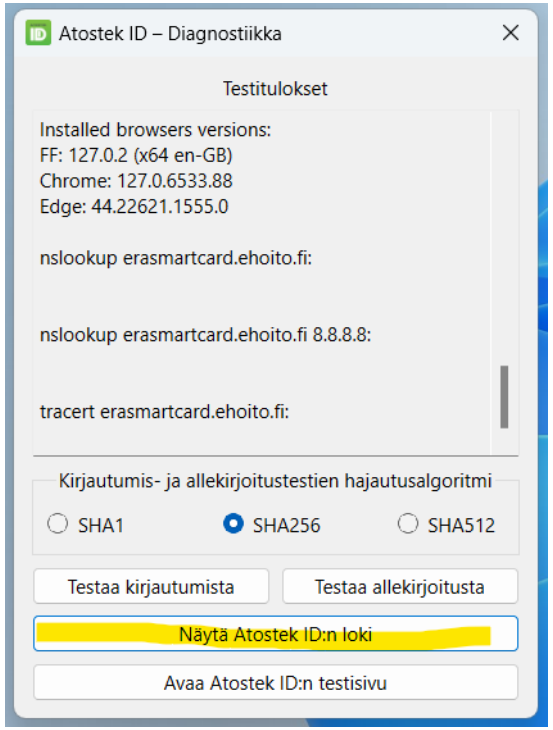


ATOSTEK

SCS-gränssnittet: certifikat och server

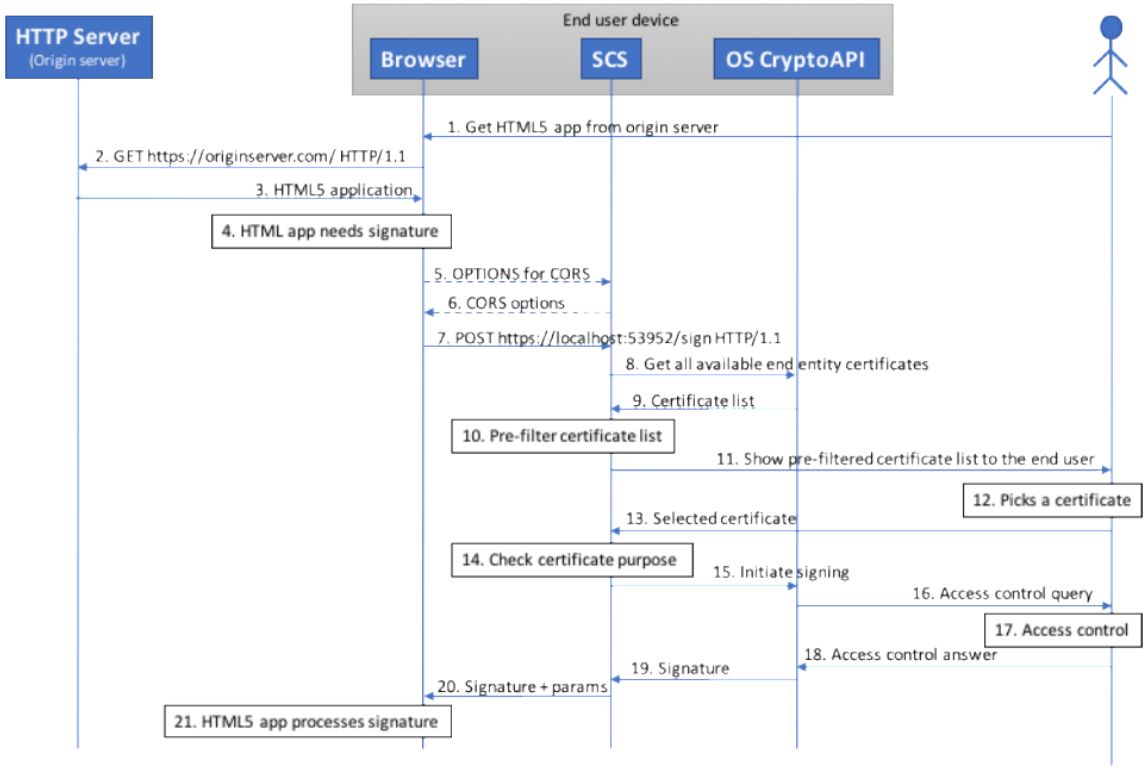
- Både servercertifikat (scscert.pfx) och rotcertifikat (scsca.cer) behövs för att SCS-servern ska fungera korrekt
- Eventuella problemsituationer
  - Installation av applikationen Atostek ID utförs inte med tillräckliga rättigheter, varvid till exempel
    - Certifikaten inte kan sparas i standardläget
    - Rotcertifikat som beviljar servercertifikat inte kan läggas till i operativsystemets certifikatlager
  - DigiSign är installerad och igång samtidigt
    - Detta förhindrar att SCS-servern i applikationen Atostek ID startar i samma port 53952
- SCS-servern har kunnat sättas upp och certifikaten genereras korrekt om testsidan https://localhost:53952/ öppnas utan varningar och texten *Atostek ID SCS test page loaded OK* visas på sidan.





ATOSTEK

SCS-gränssnittet: sekvensschema



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-gränssnitt: gränssnittets funktioner

- Begäran enligt HTTP/1.1-protokollet kan skickas till SCS-gränssnittet https://localhost:53952/
- Begäran som stöds i version 1.2
  - GET /version
  - POST /sign
  - GET /sign

ATOSTEK

SCS-gränssnitt: GET /version

- Information fås om versionen av det SCS-gränssnitt som används och om de funktioner som stöds
- Inga parametrar anges i begäran
- Som svar får man en förteckning över uppgifterna i SCS-gränssnittet

ATOSTEK

SCS-gränssnitt: GET /version begäran

- GET https://localhost:53952/version
- Inga parametrar anges i begäran

ATOSTEK

SCS-gränssnitt: GET /version svar

- Närmare beskrivningar av parametrarna finns i dokumentationen för SCS-gränssnittet.


```
{
   "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-gränssnitt: POST/GET /sign

- En elektronisk signatur skapas med certifikatkortet
- I begäran ges åtminstone de data som ska undertecknas
- Andra parametrar preciserar begäran, t.ex.:
  - Med hurdant certifikat man vill signera
  - Vilken hashalgoritm man vill använda
  - Hurdan elektronisk signatur man vill skapa
    - För närvarande stöds endast rå signatur med kortet

SCS-gränssnitt: POST /sign begäran

- POST https://localhost:53952/sign
- Närmare beskrivningar av parametrarna finns i dokumentationen för SCS-gränssnittet.
- "content"-parameter den enda obligatoriska
  - Data som ska undertecknas med Base64-kodning

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

ATOSTEK

SCS-gränssnitt: GET /sign begäran

- GET https://localhost:53952/sign?<pyynnön parametrit>
- Observera att selector-parametern inte kan anges i en GET /sign -begäran!

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

ATOSTEK

SCS-gränssnitt: POST /sign svar

- Närmare beskrivningar av parametrarna finns i dokumentationen för SCS-gränssnittet.


```
{
  "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"
}
```

SCS-gränssnittet: felkoder

- I svaret på begäran om signatur finns alltid parametrar som visar att begäran har lyckats/misslyckats
  - Status ("ok"/"failed")
  - ReasonCode
  - ReasonText
- Närmare beskrivningar av dessa finns i dokumentationen av SCS-gränssnittet.

ATOSTEK

SCS-gränssnittet: felkoder


```
{
   "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-gränssnittet: problemsituationer

- Rapportera problemsituationer enligt de anvisningar som förmedlats i samband med produktionspublikationen.
  - atostek-id@atostek.com

- När det gäller SCS-gränssnittet är det i allmänhet meningsfullt att i problemsituationer veta exakt **vilken typ av begäran som integreras i kortläsarprogrammets SCS-gränssnitt och hurdant svar gränssnittet returnerar.**
  - Begäran och svarets status loggas på DEBUG-nivå i felloggen

ATOSTEK

SCS-gränssnitt: framtida egenskaper

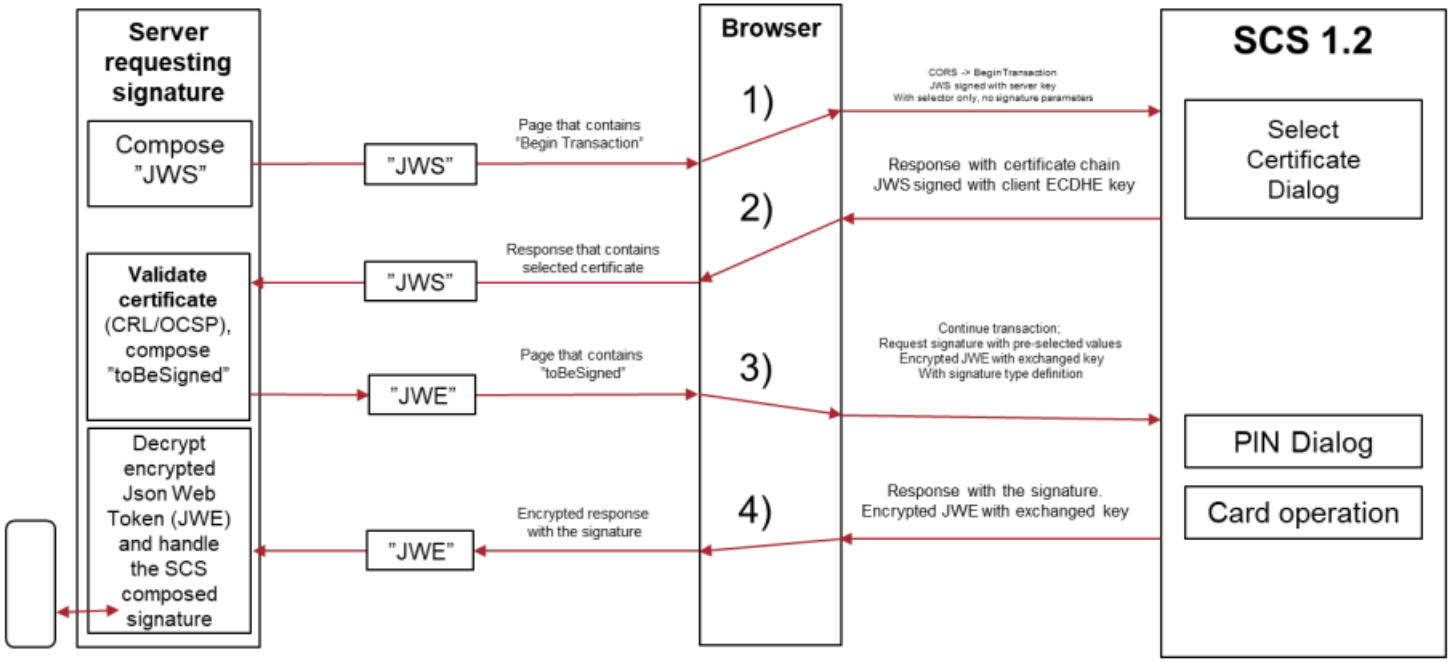
- Signaturtyperna ”cms" och "cms-pades”
  - Följer CMS-signaturformat där till exempel signaturens tidsstämpel ingår
  - "cms-pades" särskilt avsedd för signering av PDF-dokument
  - Kan användas i senare produktionspublikationer i POST/sign begäran
    - signatureType-parameter

ATOSTEK

SCS-gränssnitt: framtida egenskaper

- Kommunikation med hjälp av JSON Web Token (transactions)
  - Ny egenskap i version 1.2
  - Ett säkrare sätt att kommunicera mellan den som skickar begäran om signering och SCS-gränssnittet
  - Grundar sig på att den instans som skickar begäran om signering och SCS-gränssnittet skapar en gemensam krypteringsnyckel (ECDH) med vilken kommunikationen krypteras
  - Detaljerna i dokumentationen av SCS-gränssnittet

SCS-gränssnitt: framtida egenskaper

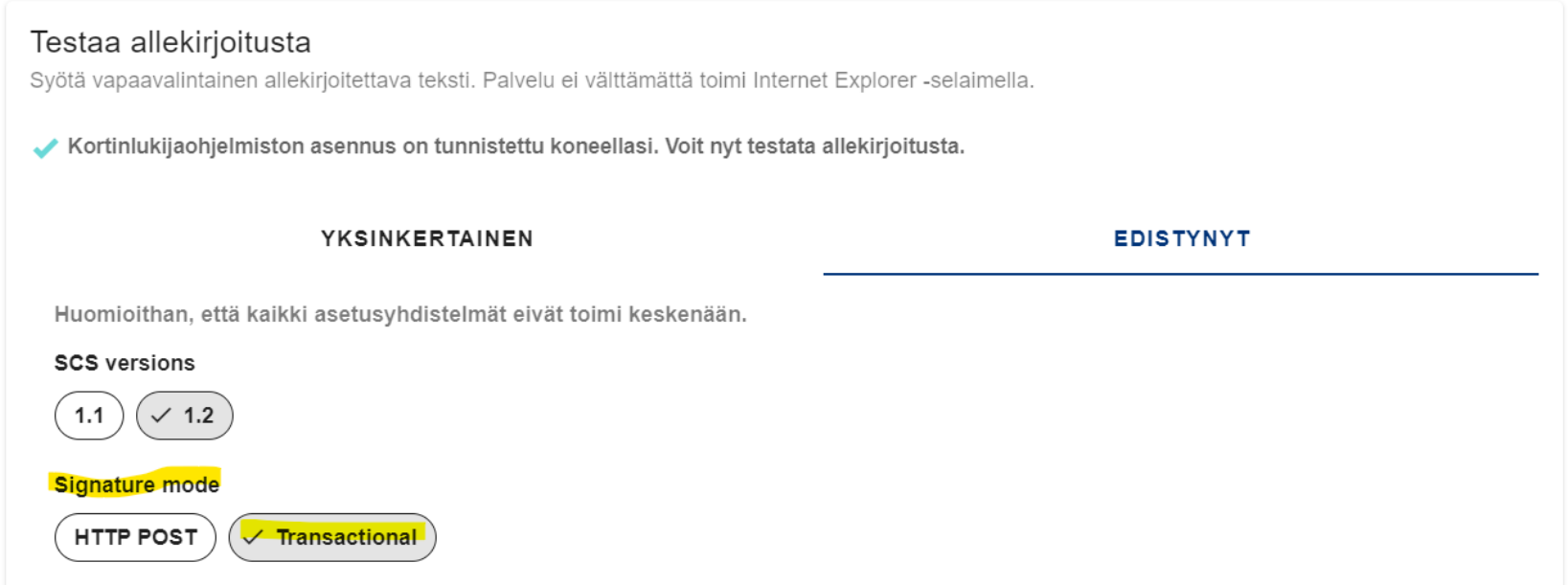


https://dvv.fi/documents/16079645/17324992/DVV-SCS_HTML5-and-Digital-Signatures.pdf/dbb89387-6aaa-4c0e-5ac3-f69b234ee25b/DVV-SCS_HTML5-and-Digital-Signatures.pdf?t=1697787548881

ATOSTEK

SCS-gränssnitt: framtida egenskaper

- Egenskapen kan i fortsättningen testas på MDB:s testsida



ATOSTEK


Frågor?
ATOSTEK

Svar på frågor i chatten

- Hur omfattande är användningen av SCS-gränssnittet i nuläget? Hurdana är gränssnittets huvudsakliga användningsfall?
  - SCS-gränssnittet är ett öppet dokument vars användning inte följs upp. Därför är det är svårt att garantera användningens omfattning. Det viktigaste användningsobjekt är sannolikt FPA:s applikation Kelain.
- Enligt vilken tidtabell kommer signatureType "cms" att komma med?
  - Enligt den preliminära planen publiceras detta senast i den andra produktionspublikationen i november. Målet är att samma publikation ska omfatta kommunikation med JSON Web Token vid sidan av det vanliga kommunikationssättet.
- Kommer identitetskortet att få stöd för kryptering och dekryptering med öppen nyckel?
  - Identitetskort är inte direkt ett hinder för detta, även om användningsfallet är sällsynt med tanke på en vanlig användare. MDB har dock inga separata anvisningar för användningen av detta.

ATOSTEK

Svar på frågor i chatten

- SCS-gränssnittet och signering av hashalgoritm
  - De data som ska signeras kan vara antingen ursprungliga data eller en sammanfattning av dem. Detta bestäms med contentType-parametern ("data"/"digest").
  - Om de data som ska undertecknas inte är en hashalgoritm, sammanfattar SCS-gränssnittet data med den angivna hashalgoritmen. Om ingen algoritm har angetts används algoritmen SHA256 som standardvärde.
  - Om de data som ska signeras är en sammanfattning ska den använda hashalgoritmen anges i begäran för att SCS-gränssnittet ska kunna validera hashalgoritmen.
  - Data som ska signeras i CMS-signaturen fogas inte till den underskrift som returneras om data ursprungligen var en hashalgoritm.

ATOSTEK

Observationer som framförts i chatten

- Alla Atostek ID-utbildningar sparas och inspelningar och material publiceras på MDB:s webbsida https://dvv.fi/sv/kortlasarprogram.

ATOSTEK