

Atostek ID: Introduktion till integrationsutbildningen

1.7.2024



Innehåll

- Utbildningens syfte och målsättning
- Atostek ID: Allmän presentation och installation av applikationen
- Gränssnitt
 - SCS
 - Minidriver, (TokenDriver)
 - PKCS#11
- Tid för frågor
- Vi håller en kort paus på 5 min om utbildningen verkar ta hela 2 h

Utbildningens syfte och målsättning

Syfte och målsättning

- Denna utbildning riktar sig till de aktörer vars system integreras i något av Atostek ID –programmets gränssnitt
- Utbildningen är ett introduktion till integrationsutbildningarna som hålls i augusti
 - Vi går på ett allmänt plan igenom alla gränssnitt som ska integreras och erbjuder dokumentation
 - Vi går igenom varje gränssnitt mer ingående under utbildningarna i augusti
 - **Syftet här är att bekanta sig med möjligheterna och erbjuda material som man kan bekanta sig med före utbildningarna i augusti**
 - Introduktionen är inte obligatoriskt före utbildningarna i augusti, utan riktad till dem som vill sätta sig in i frågan redan i juli.

Allmän presentation och installation



Atostek ID



- Myndigheten för digitalisering och befolkningsdatas nya kortläsarprogram
- Den första och andra testversionen har redan publicerats för ett begränsat antal testare
- I augusti görs den första produktionspublikationen och integrationsutbildningar ordnas i två delar
- 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.
- 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 i produktionspublikationen i augusti

Atostek ID SCS- gränssnitt



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-specifiseringar](#)

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](#)



SCS-gränssnittet i allmänhet

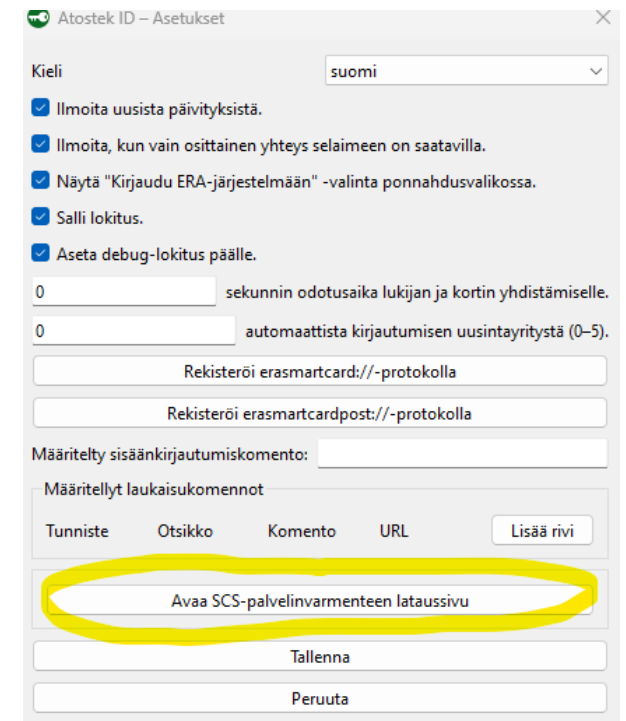
- I programvarans första och andra testversion finns det fortfarande brister i SCS-gränssnittet. De har antecknats i samband med anvisningarna för testpublikationerna.
 - Stöd för identitetskort
 - Version 1.2 av gränssnittet
 - Små reparations- och finslipningsbehov
- Korrigeringar och nödvändiga implementeringar görs i produktionsversionen för augusti

SCS-gränssnittet: certifikat och server

- Atostek ID skapar i samband med installationen de certifikat som behövs för HTTPS-servern
 - Beviljande certifikat *Atostek ID Local SCS CA* läggs samtidigt till som betrott i operativsystemets certifikatlager
- 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:** Detta fungerar inte om DigiSign är installerat och igång innan Atostek ID startas

SCS-gränssnittet certifikat och server

- Observera att certifikatet tills vidare inte automatiskt installeras i till exempel Firefox certifikatlager
 - Certifikatet kan laddas ner från applikationen *Inställningar > Nedladdningssida för SCS-servercertifikat*
 - På sidan finns också anvisningar om hur certifikatet ställs in som betrott



Atostek ID - Asetukset

Kieli: suomi

- ☒ Ilmoita uusista päivityksistä.
- ☒ Ilmoita, kun vain osittainen yhteys selaimen on saatavilla.
- ☒ Näytä "Kirjaudu ERA-järjestelmään" -valinta ponnahdusvalikossa.
- ☒ Salli lokitus.
- ☒ Aseta debug-lokitus päälle.

0 sekunnin odotusaika lukijan ja kortin yhdistämiselle.

0 automaattista kirjautumisen uusintayritystä (0-5).

Rekisteröi erasmartcard://-protokolla

Rekisteröi erasmartcardpost://-protokolla

Määritely sisäänkirjautumiskomento:

Määritellyt laukaisukomennot

Tunniste	Otsikko	Komento	URL	Lisää rivi
Avaa SCS-palvelinvarmenteen lataussivu				

Tallenna

Peruuta

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.
- Observera att det fortfarande kan finnas brister i SCS-gränssnittet särskilt i fråga om testpublikationer.
- SCS-gränssnittets funktion kan också testas till exempel via [MDB:s testsida](#).

SCS-gränssnittet: integration

DIGI- JA VÄESTÖTIETOVIRASTO

FI

Testaa allekirjoitusta

Syötä vapaavalintainen allekirjoitettava teksti. Palvelu ei välttämättä toimi Internet Explorer -selaimella.

✓ Kortinlukijaohjelmiston asennus on tunnistettu koneellasi. Voit nyt testata allekirjoitusta.

YKSINKERTAINEN

EDISTYNYT

Syötä vapaavalintainen allekirjoitettava teksti. Palvelu ei välttämättä toimi Internet Explorer -selaimella.

ALLEKIRJOITA TEKSTI

DIGI- JA VÄESTÖTIETOVIRASTO

FI

Testaa allekirjoitusta

Syötä vapaavalintainen allekirjoitettava teksti. Palvelu ei välttämättä toimi Internet Explorer -selaimella.

✓ Kortinlukijaohjelmiston asennus on tunnistettu koneellasi. Voit nyt testata allekirjoitusta.

YKSINKERTAINEN

EDISTYNYT

Huomioithan, että kaikki asetusyhdistelmät eivät toimi keskenään.

SCS versions

1.1

✓ 1.2

Signature mode

✓ HTTP POST

Transactional

Content type

✓ data

digest

Hash algorithm

SHA256

SHA384

SHA512

Signature type

signature

cms

cms-pades

Signature algorithm

RSA

RSASSA-PSS

ECDSA

Key usages

digitalSignature

✓ nonRepudiation

dataEncipherment

decipherOnly

encipherOnly

keyAgreement

Key algorithms

RSA

EC

Issuer

Issuer

Syötä vapaavalintainen allekirjoitettava teksti. Palvelu ei välttämättä toimi Internet Explorer -selaimella.

ALLEKIRJOITA TEKSTI

SCS-gränssnittet: integration

- Rapportera problemsituationer enligt de anvisningar som förmedlats i samband med testpublikationerna.
- 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.

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 ID Minidriver



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.
 - [Minidriver gränssnittsdocumentation](#)

Minidriver färdighetsgrad

- Den första testversionen av Atostek ID Minidriver blir tillgänglig för testarna på onsdagen
 - Den saknar dock ännu kommandon och WHQL-signatur
- I produktionspublikationen för augusti
 - Resten nödvändiga kommandon
 - WHQL-signatur
 - Installation direkt i samband med installation av Atostek ID

Kommandon som implementerats i testversionen

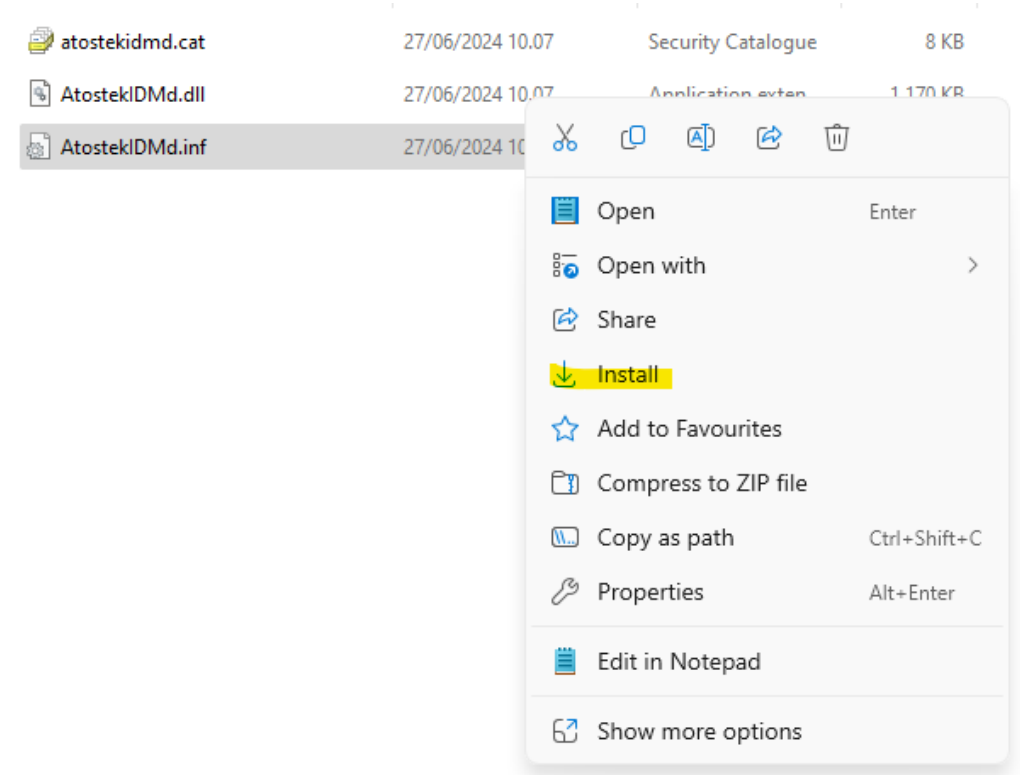
- CardAcquireContext
- CardDeleteContext
- CardSignData
- CardReadFile
- CardGetFileInfo
- CardEnumFiles
- CardQueryFreeSpace
- CardAuthenticatePin
- CardAuthenticateEx
- CardGetProperty
- CardGetContainerProperty
- CardGetContainerInfo

Installation av testversion

- Atostek ID Minidriver kan testas innan en officiell WHQL-signatur görs för den
 - Testarna erbjuds en testsignatur (atostekidmd.cat) som ska hållas på samma plats som filerna .dll och .inf. i modulen. Alla dessa publiceras för testarna onsdagen den 3.7.
 - Användningen av testsignatur kan tillåtas med kommandot ***bcdedit /set testsigning on***
 - Kommandot måste köras som administratör
 - Mer information om kommandot finns i [Microsofts Minidriver-dokumentation](#)

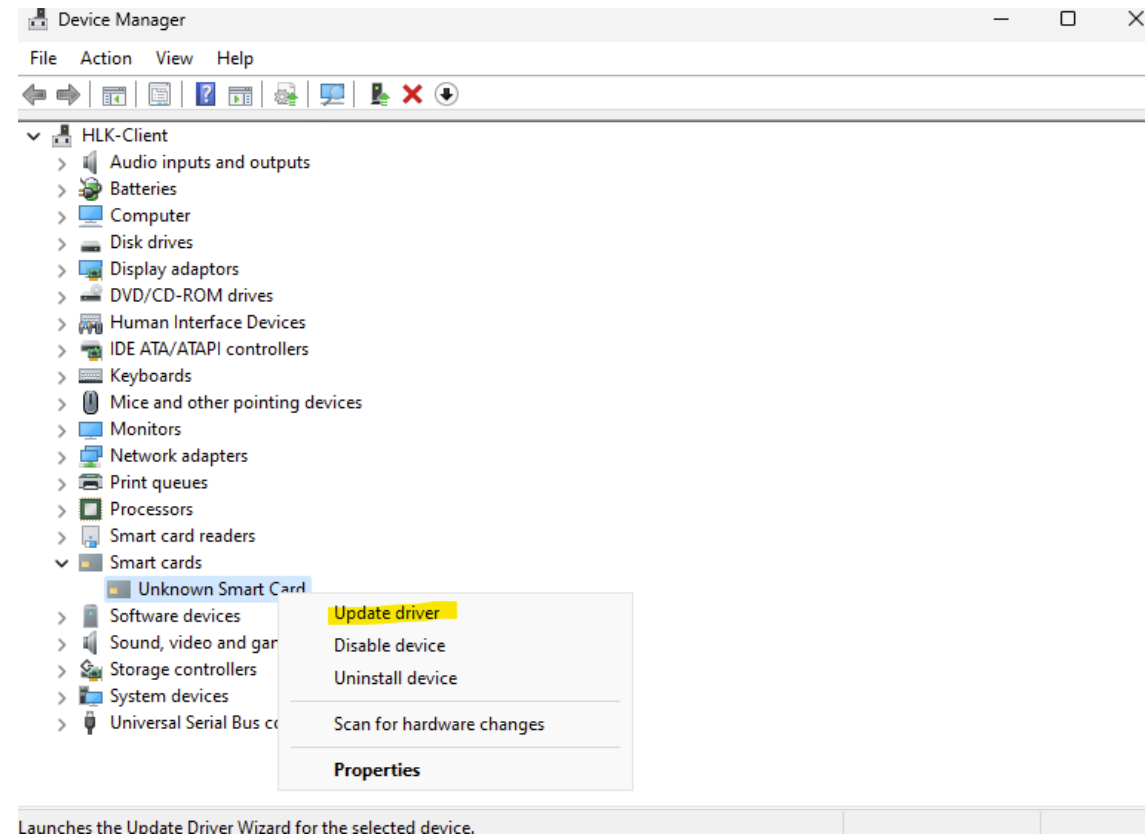
Installation av testversion

- Efter att testsignaturen är tillåten kan Atostek ID Minidriver installeras genom att högerklicka på modulens .inf och välja *Install*
- Ett separat meddelande skickas om installationen lyckades



Installation av testversion

- Vid behov installeras drivrutinen separat via Device Manager
- Välj den mapp där modulen finns på din enhet



WHQL signering och installation i produktionsversionen

- I produktionspublikationen i augusti ansöker man om en officiell WHQL-signatur för applikationen. Då kan drivrutinen installeras direkt utan att testsignaturer tillåts.
- De filer (dll, inf, cat) som behövs i produktionsversionen sparas på enheten i samband med installationen och måste inte laddas ner separat. Närmare anvisningar om detta är på kommande i produktionsversionens integrationsanvisning.
- Även i produktionsversionen använder installationen .inf-filen

Användningsexempel

- Observera att alla kommandon i testversionen inte är genomförda, så alla användningsfall kan ännu inte testas.
- I samband med produktionspublikationen i augusti publiceras också den första versionen av AD-registreringstjänsten. När AD-registreringstjänsten tas i bruk försöker Minidriver para ihop kortet när det förs till läsaren.
 - Detta stöder alltså inloggningen på arbetsstationen med kort, även efter [AD-ändringen](#). Ändringen ska beaktas vid inloggningen till arbetsstationen senast i februari 2025.

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 ID PKCS#11



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.
 - [PKCS#11 gränssnittets dokumentation](#)

PKCS#11 färdighetsgrad

- Den första testversionen av gränssnittet Atostek ID PKCS#1 blir tillgänglig för testarna på onsdagen
 - Den saknar dock ännu kommandon
- I produktionspublikationen för augusti
 - Lägg till kommandon
 - Modulen kommer direkt i samband med installationen av Atostek ID och behöver inte laddas ner separat

PKCS#11 ibruktagning

- Ibruktagningen av modulen beror på med vilken applikation eller vilket operativsystem modulen används
 - T.ex. Adobe Acrobat Reader > Menu > Preferences > Signatures > Identities & Trusted Certificates > PKCS#11 Modules and Tokens
- I samband med produktionspublikationen i augusti kommer det mer dokumentation och anvisningar om ibruktagning av modulen i olika användningsfall
- Användningsfallen behandlas också mer ingående under integrationsutbildningarna i augusti



Frågor?

Svar på frågor i chatten

- Var finns installationspaketet?
 - När det gäller produktionspublikationen för augusti kommer installationspaketen att finnas på MDB:s webbplats för nedladdning
 - För testversionernas del är installationspaketen tillgängliga i Atosteks Upload-tjänst för dem som anmält sig till testningen
- Är standardspråket finska?
 - I installationspaketen för Windows och MacOS är standardspråket systemets språk (finska, svenska, engelska) eller engelska, om systemets språk inte finns bland de språk som stöds. I Linux-installationspaketen är standarden tills vidare finska.
- Hur utreder man vilket gränssnitt som används för närvarande?
 - Det lönar sig att fråga den egna organisationens IT-personal i vilka gränssnitt ert system hittills har integrerats.

Observationer som framförts i chatten

- kommandot "bcredit /set testing on" kräver nästan utan undantag att datorn startas om för att det ska aktiveras.
 - Kom ihåg att stänga av inställningen efter testet