Atostek ID: Integrationsutbildning 2/2 (Minidriver & PKCS#11)

14.8.2024

ATOSTEK

Innehåll

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

- Vid behov håller vi en paus

Utbildningens syfte och målsättning

ATOSTEK

Syfte och målsättning

- Denna utbildning riktar sig till de aktörer vars system integreras i användningen av Atostek ID-programmets Minidriver- och/eller PKCS#11-gränssnitt

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

ATOSTEK

Allmän presentation och installation

ATOSTEK

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 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

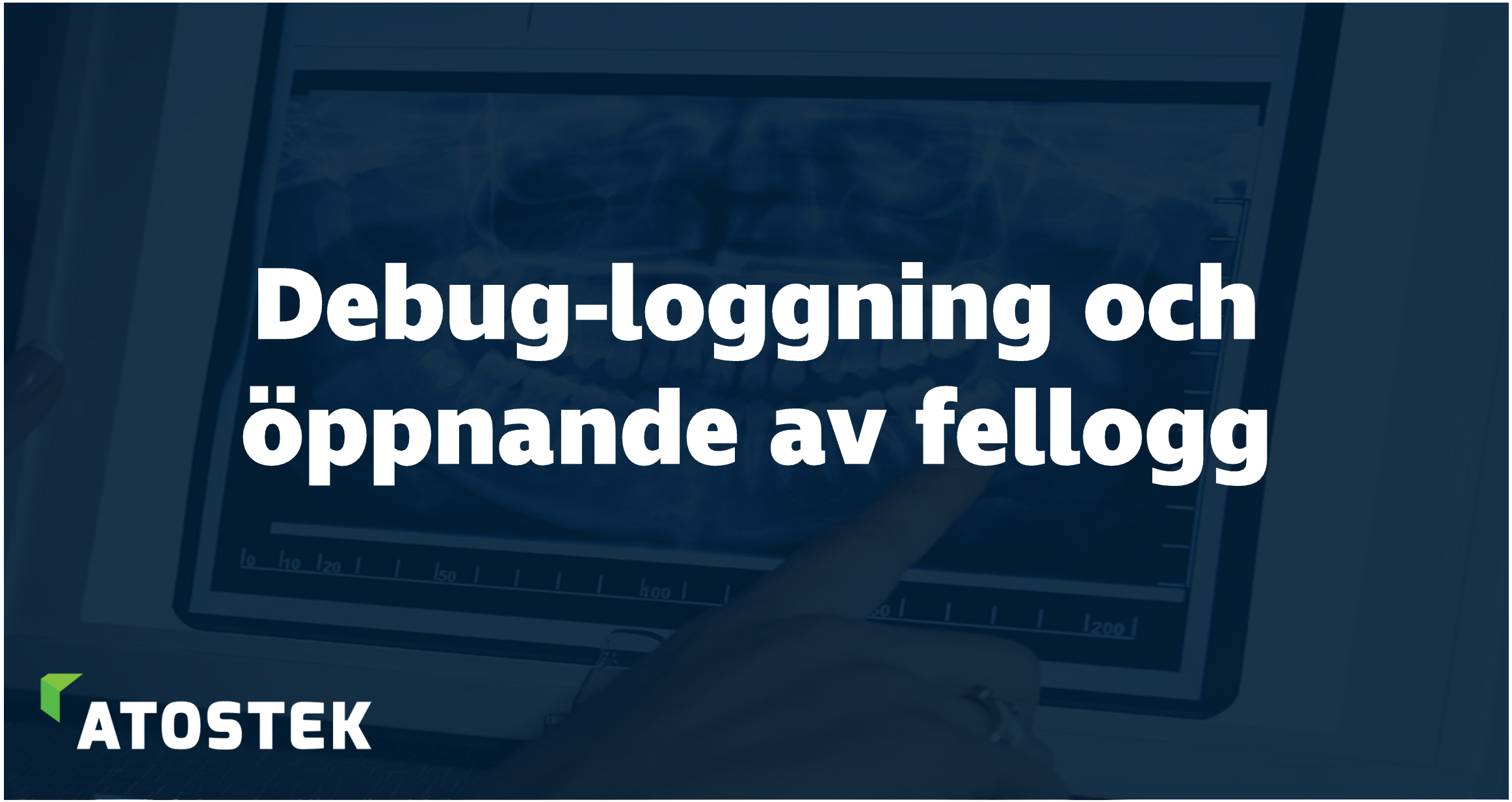
- Installation med användargränssnitt: Klicka på applikationens .pkg installationspaket för att öppna det och gör installationen enligt anvisningarna i gränssnittet.
- Installation från kommandoraden (sudo):
  - Kör kommando *sudo –installer –pkg <paketin nimi>.pkg –target /*
  - Om du vill kan du ange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

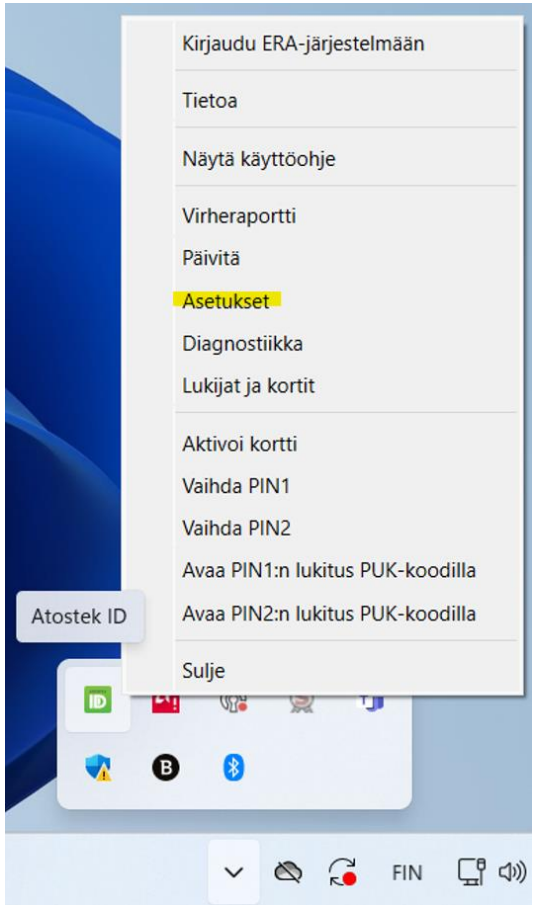


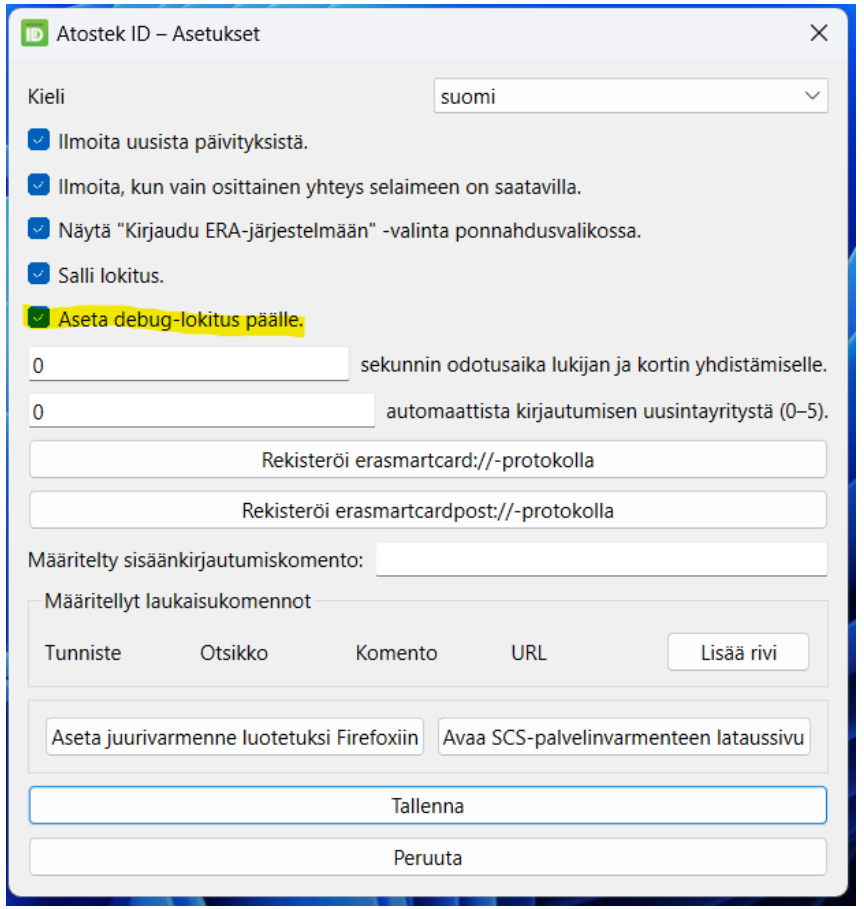
Debug-loggning och öppnande av fellogg

ATOSTEK

Drifttagning av debug-loggning

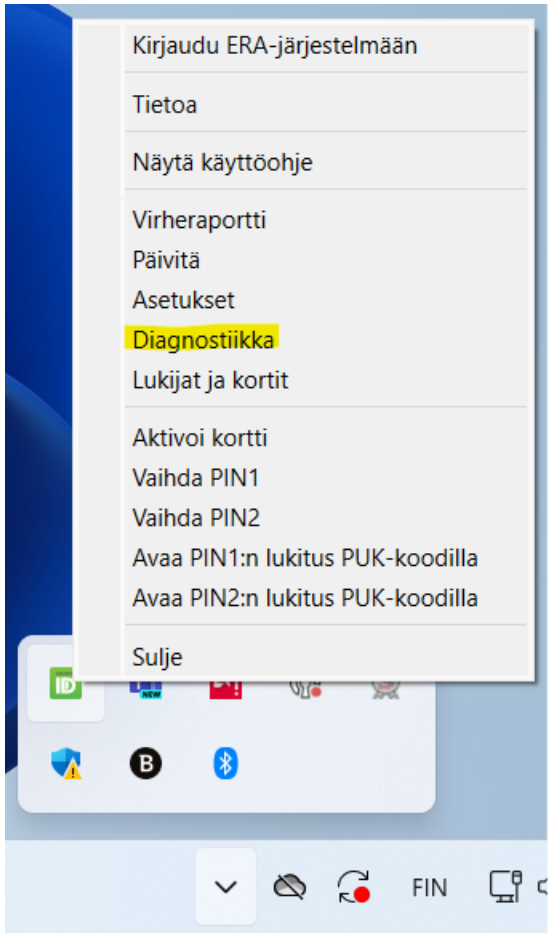
- Loggningen av applikationen Atostek ID på debug-nivå kan aktiveras i inställningarna
  - I menyn "Inställningar" → "Aktivera debug-loggning" → "Spara"

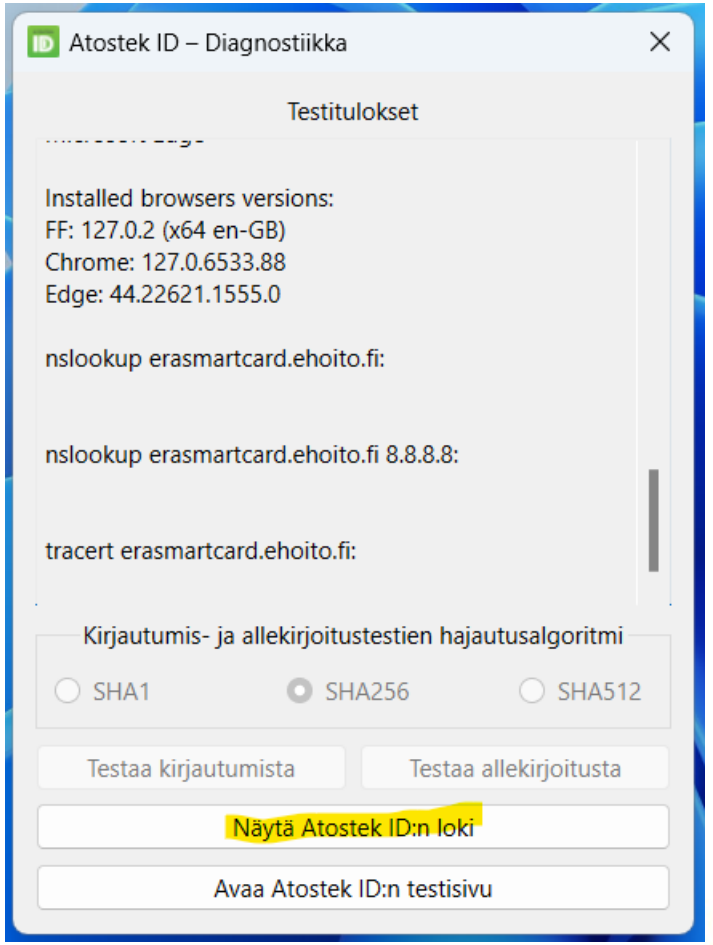




Öppning av fellogg

- 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

- En drivrutin för Windows-operativsystemet som kommunicerar med smartkort
- Implementerat för att fungera med certifikatkort som producerats av Myndigheten för digitalisering och befolkningsdata
  - FINEID-specificeringar
- Operativsystemet utnyttjar Minidriver direkt till exempel vid inloggning på arbetsstationen
- Andra applikationer kan också utnyttja Minidriver till exempel för att göra elektroniska 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
  - FINEID-specificeringar
- En egen version av modulen skapas för olika operativsystem
  - Windows, MacOS och Linux
- Atostek ID:s modul 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 Minidriver

ATOSTEK

Minidriver i allmänhet

- En drivrutin för Windows-operativsystemet som kommunicerar med smartkort
- Implementerat för att fungera med certifikatkort som producerats av Myndigheten för digitalisering och befolkningsdata
  - FINEID-specificeringar
- Operativsystemet utnyttjar Minidriver direkt till exempel vid inloggning på arbetsstationen
- Andra applikationer kan också utnyttja Minidriver till exempel för att göra elektroniska signaturer
- Atostek ID Minidriver implementerar versionen 7.07 av gränssnittet i tillämpliga delar.
  - Minidriver gränssnittsdokumentation

ATOSTEK

Minidriver i allmänhet

Smart Card Minidriver Specification, v7.07

Smart card vendors can write card minidrivers to present a consistent interface to their smart card type to the Microsoft Smart Card Base Cryptographic Service Provider (CSP) or Crypto Next Generation (CNG) Key Storage Provider (KSP) and to the Smart Card Management Interface. These card minidrivers plug in to Windows operating system code. The functionality in a card minidriver is narrowly scoped and carefully defined so that the card-dependent code is simple to implement and easy to verify functionally.

This specification provides implementation guidelines for Base CSP and KSP card minidrivers. This is the latest specification which applies to Windows 8 and later operating systems.

Document: Smart Card Minidriver Specification, v7.07

For information about our Security Development Lifecycle (SDL), see Microsoft Security Development Lifecycle (SDL) – Process Guidance.

For information about how to develop card minidrivers for Windows, see Smart Card Reader Devices Design Guide and Smart Card Minidrivers.

ATOSTEK

Minidriver: Gränssnittsfunktioner

https://learn.microsoft.com/en-us/previous-versions/windows/hardware/design/dn631754(v=vs.85)#smart-card-minidriver-specification-v707

ATOSTEK

Minidriver: identifierade brister

- Det finns brister i den första produktionspublikationen
  - Minidriver har ännu ingen officiell WHQL-signatur
  - Minidriver installeras inte heller direkt vid installation av Atostek ID
  - En separat AD-registreringstjänst är ännu inte tillgänglig

- Vid fel, ta kontakt per e-post atostek-id@atostek.com
  - Denna kanal endast för rapportering av bugie
  - Det finns separata anvisningar för rapporteringens innehåll och utformning

ATOSTEK

Kommandon som genomförts för den första produktionspublikationen

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

- Observera att alla funktioner som definieras i Minidrivers specifikation inte betjänar identifierade användningsfall för kort enligt FINEID-specifikationen
- Identifierade användningsfall har utnyttjats i den ordning funktionerna genomförts

ATOSTEK

Minidriver: Genomförda kommandon

https://learn.microsoft.com/en-us/previous-versions/windows/hardware/design/dn631754(v=vs.85)#smart-card-minidriver-specification-v707

ATOSTEK

Exempel: CardSignData

- Funktionerna återställer DWORD-typen
- Funktionernas parametrar har förklarats
- I dokumentationen ges också preciserande kommentarer

4.7.5 CardSignData

Description:

The **CardSignData** function signs a block of unpadded data. This entry either performs padding on the card or pads the data by using the PFN_CSP_PAD_DATA callback. All card minidrivers must support this entry point.

```
DWORD WINAPI CardSignData(
    __in PCARD_DATA   pCardData,
    __in PCARD_SIGNING_INFO   pInfo
);
```

Input:

pCardData	Context information for the call. For more information, see "CardAcquireContext" earlier in this specification.
pInfo	Structure that contains data to be signed, which is allocated by the Base CSP/KSP.

Output:

Return value	Zero on success; otherwise, nonzero.

https://learn.microsoft.com/en-us/previous-versions/windows/hardware/design/dn631754(v=vs.85)#smart-card-minidriver-specification-v707

ATOSTEK

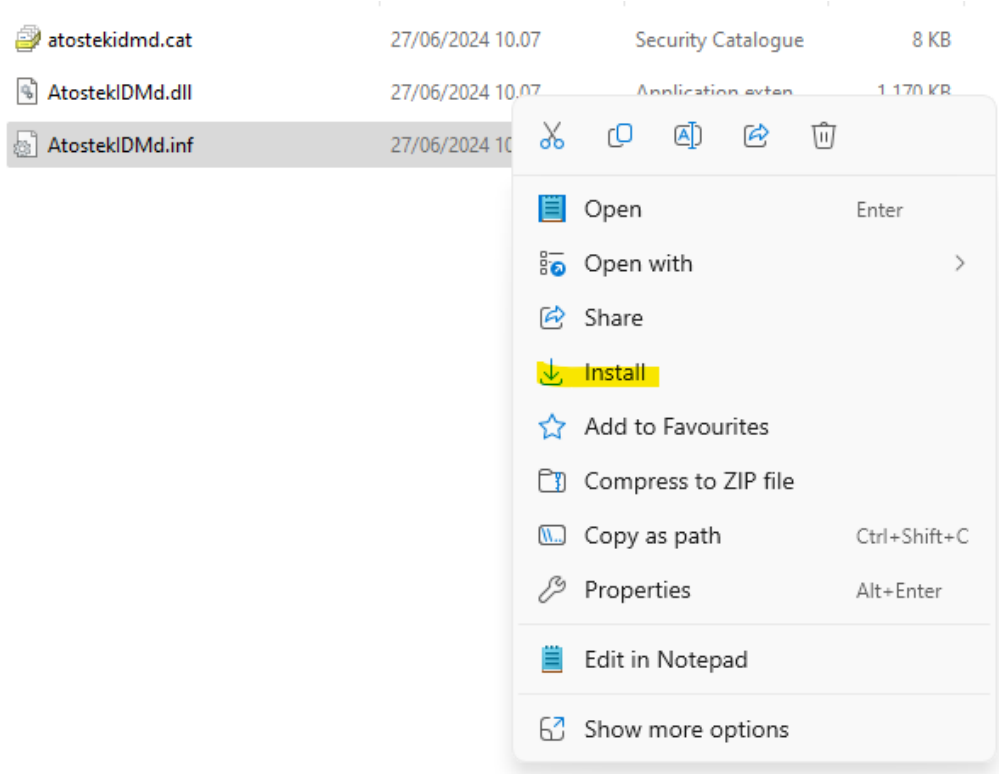
Minidriver: installation

- Atostek ID Minidriver kan testas innan den har en officiell WHQL-signatur
  - Testarna erbjuds en testsignatur (atostekidmd.cat) som ska hållas på samma plats som filerna .dll och .inf. i modulen. Alla dessa publiceras på MDB:s webbplats i samband med Minidriver
  - 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
    - kommandot "bcedit /set testing on" **kräver nästan utan undantag att datorn startas om** för att det ska aktiveras.
      - **Kom ihåg att stänga av inställningen efter testet**

ATOSTEK

Manuell installation av drivrutin

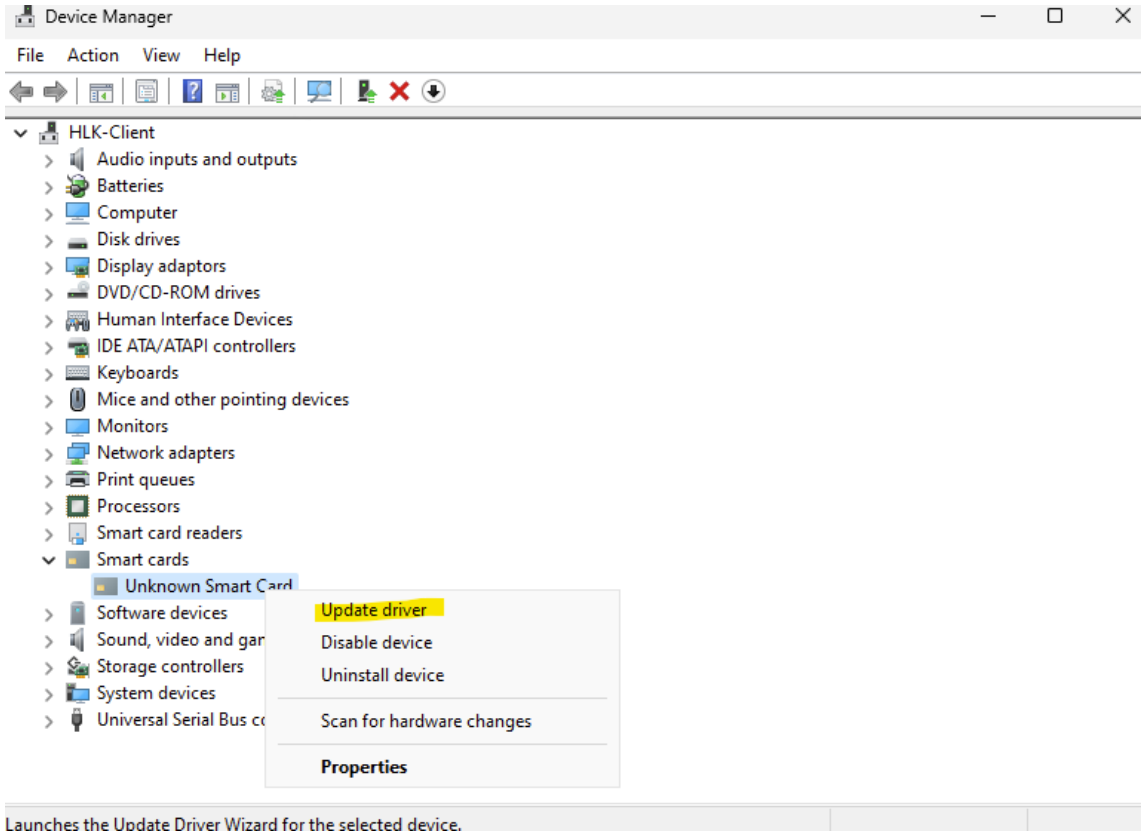
- Efter att testsignaturen är tillåten kan Atostek ID Minidriver installeras genom att högerklicka på modulens .inf och välja *Install*
- Ett separat meddelande skickas om installationen lyckades



ATOSTEK

Manuell installation av drivrutin

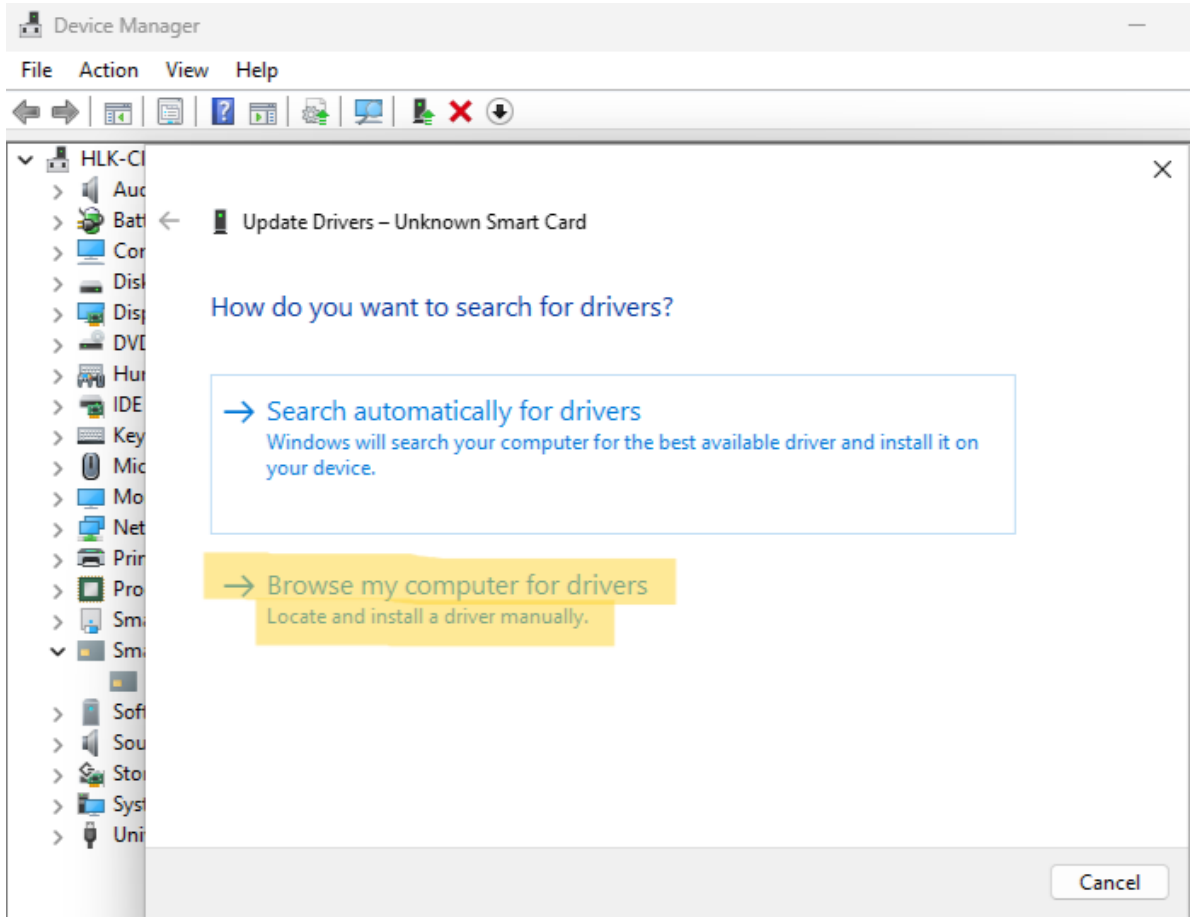
- Vid behov installeras drivrutinen separat via **Device Manager**
- Smartkortet ska vara fast i läsaren



ATOSTEK

Manuell installation av drivrutin

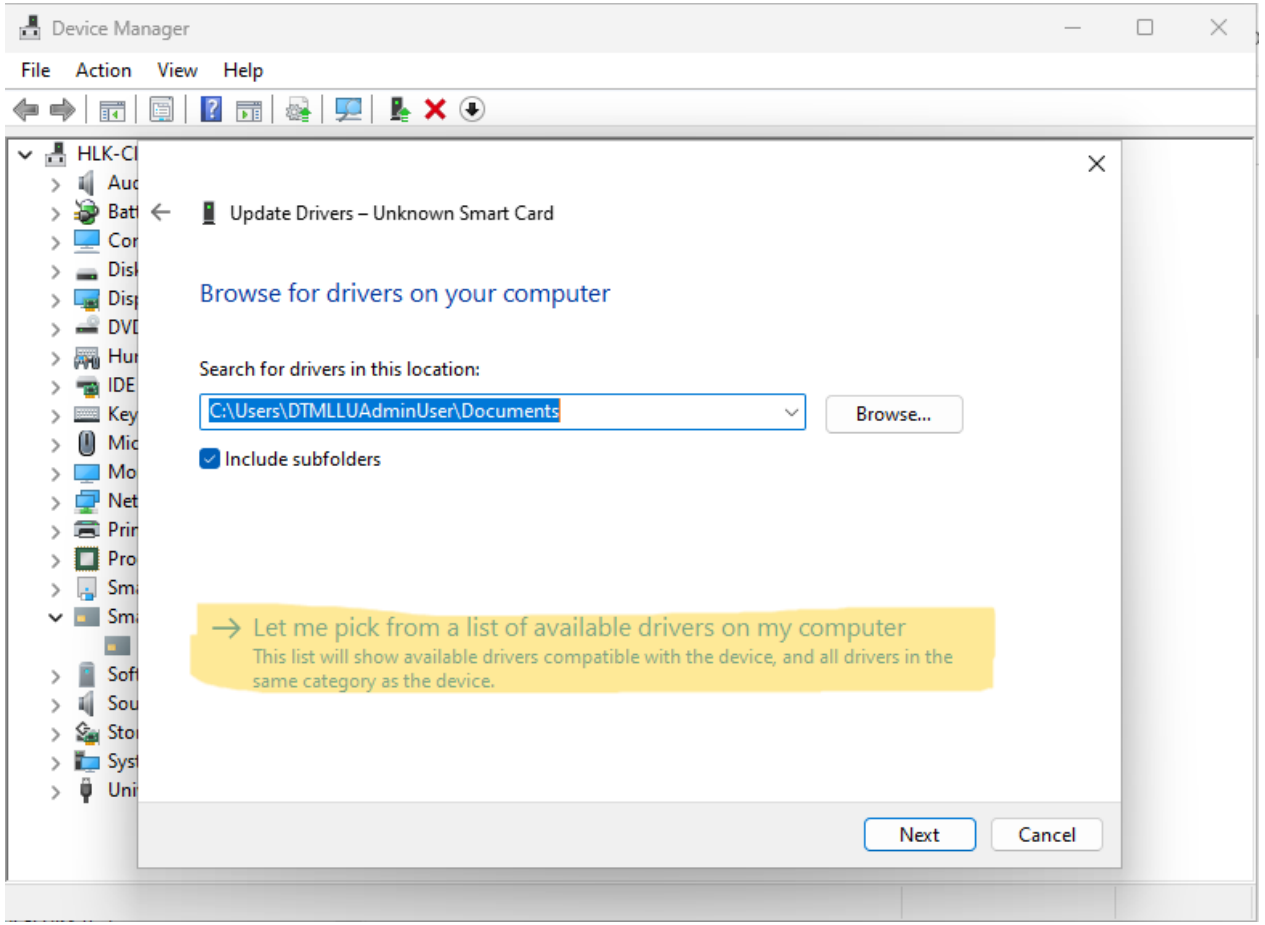
- Automatisk sökning i Windows föreslår ingen drivrutin och därför måste den sökas manuellt.



ATOSTEK

Manuell installation av drivrutin

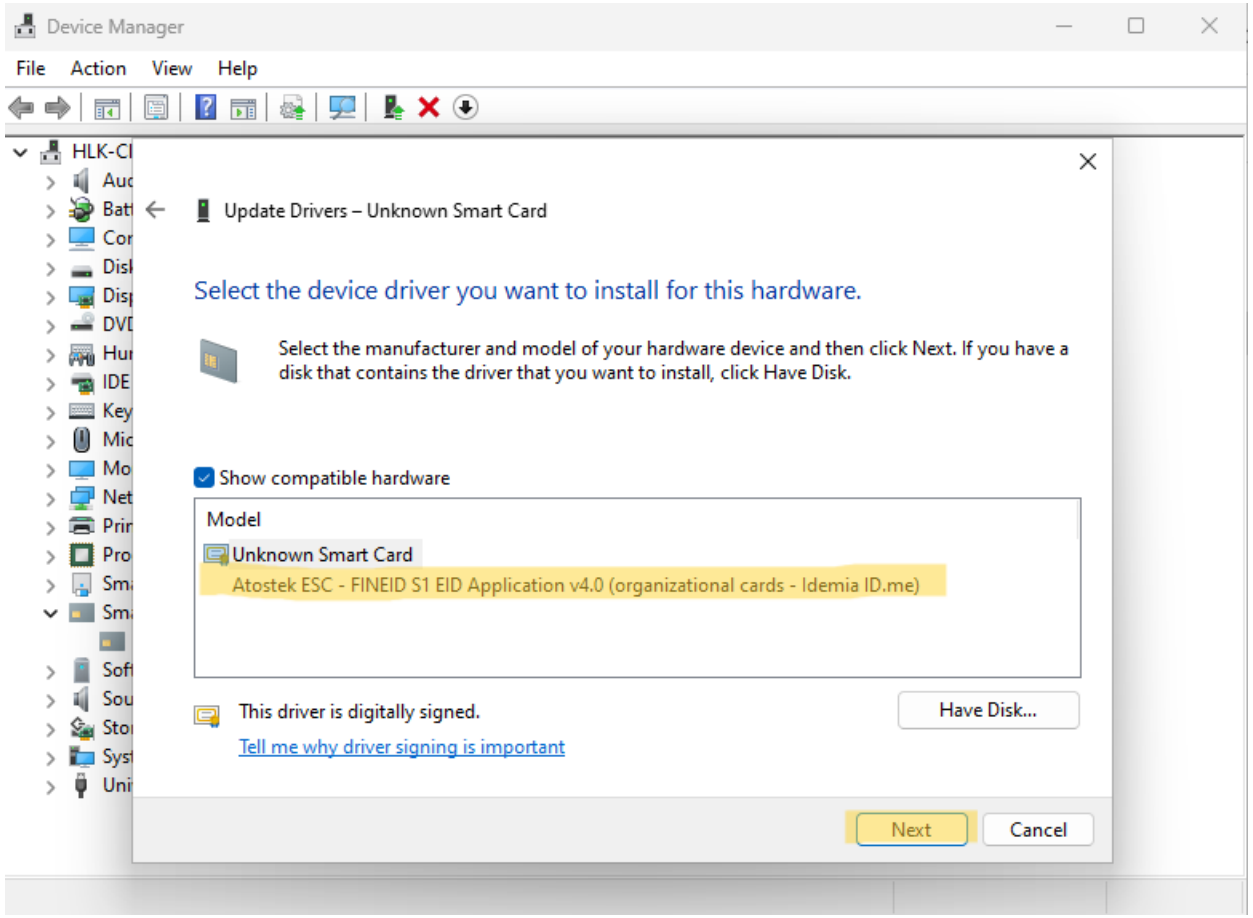
- Välj drivrutin från listan över lämpliga drivrutiner



ATOSTEK

Manuell installation av drivrutin

- Windows föreslår en drivrutin som är kompatibel med kortet. Installera drivrutinen.



ATOSTEK

WHQL signering och installation i produktionsversionen

- En officiell WHQL-signatur söks för Minidriver, varefter man strävar efter att publicera drivrutinen så snart som möjligt. Då kan drivrutinen installeras direkt utan att testsignaturer tillåts.

- De filer (dll, inf, cat) som behövs i versionen som publiceras strävar man efter att spara på enheten i samband med installationen och måste då de inte laddas ner separat. Närmare anvisningar om detta är på kommande i publikationens integrationsanvisning.

- Även i produktionsversionen använder installationen .inf-filen

Användningsfall

- Observera att alla kommandon i den första produktionspublikationen inte är genomförda, så alla användningsfall kan ännu inte testas.

- I samband med senare produktionspublikationen 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.

ATOSTEK

TokenDriver

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

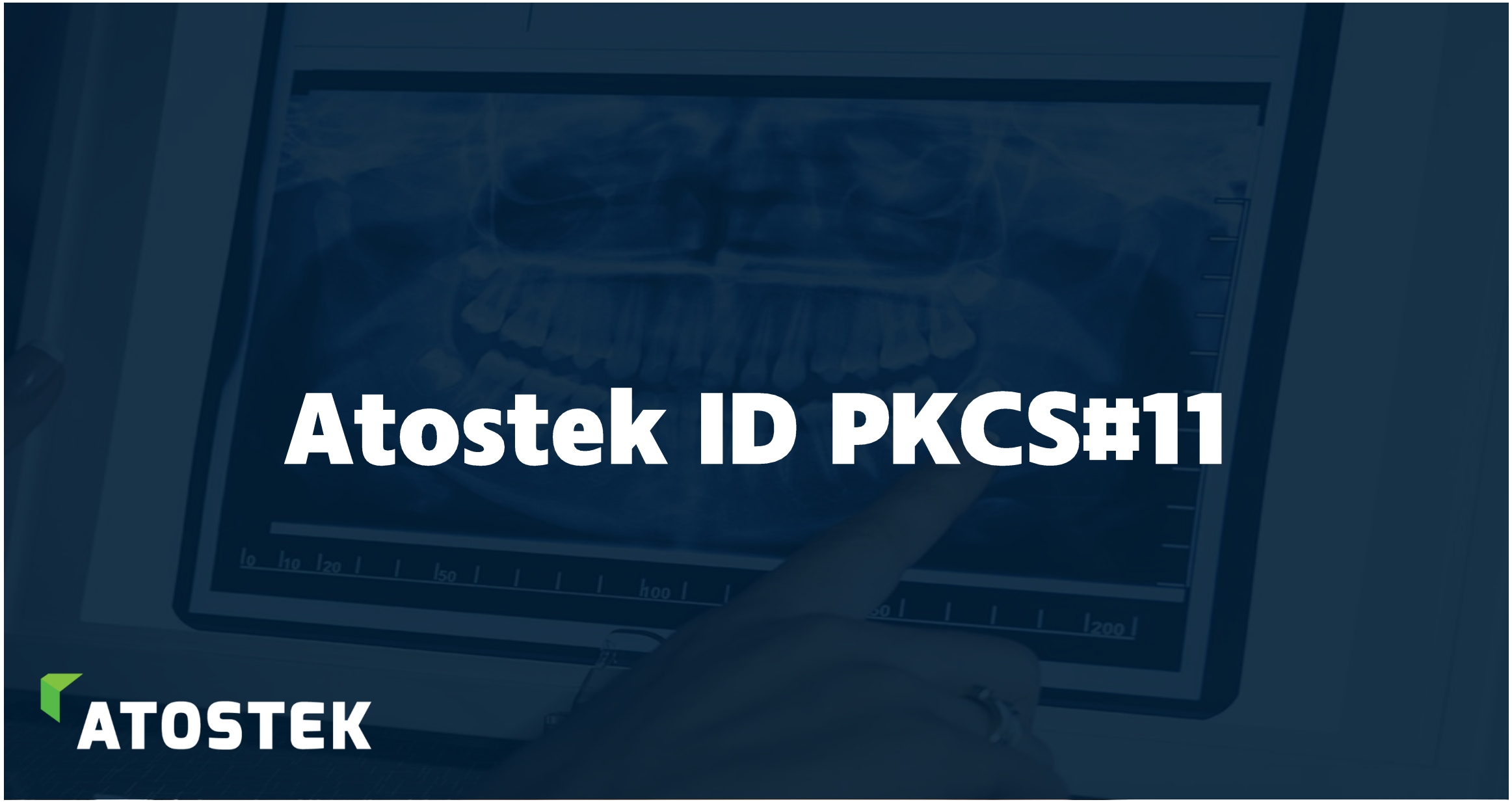
- Man har kommit överens med MDB om att TokenDriver genomförs på hösten efter den första produktionspublikationen i augusti

ATOSTEK

Minidriver: framtida egenskaper

- WHQL signerad drivrutin
- Separat AD-registreringstjänst för Windows
- Atostek ID:s PIN-dialoger tas i bruk
- Installation av drivrutin i samband med installation av Atostek ID
- MacOS TokenDriver (inloggning med aktivkort via MacOS)

ATOSTEK


Atostek ID PKCS#11
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 översätts för olika operativsystem
- Atostek ID:s odul PKCS#11 implementerar versionen 3.1 av gränssnittet.
  - PKCS#11 gränssnittets dokumentation

ATOSTEK

PKCS#11: Gränssnittsfunktioner

- PKCS#11-gränssnittet definierar som helhet över 100 olika funktioner
  - Av dessa genomförs till en början de som stöder identifierade användningsfall
- Funktionerna kan delas in i olika kategorier av användningssyfte
  - Allmänna funktioner
  - Sessionsfunktioner
  - Krypteringsfunktioner
  - Signerings- och verifieringsfunktioner
  - Packningsfunktioner
  - Funktioner för skapande och derivat av nyckelpar
  - …

Exempel: C_Sign

5.13.2 C_Sign

```
CK_DECLARE_FUNCTION(CK_RV, C_Sign)(
  CK_SESSION_HANDLE hSession,
  CK_BYTE_PTR pData,
  CK_ULONG ulDataLen,
  CK_BYTE_PTR pSignature,
  CK_ULONG_PTR pulSignatureLen
);
```

C_Sign signs data in a single part, where the signature is an appendix to the data. *hSession* is the session's handle; *pData* points to the data; *ulDataLen* is the length of the data; *pSignature* points to the location that receives the signature; *pulSignatureLen* points to the location that holds the length of the signature.

C_Sign uses the convention described in Section 5.2 on producing output.

https://docs.oasis-open.org/pkcs11/pkcs11-spec/v3.1/pkcs11-spec-v3.1.pdf

PKCS#11: identifierade brister

- Det finns brister i den första produktionspublikationen
  - Alla nödvändiga funktioner i modulen PKCS#11 har ännu inte genomförts
  - Modulen är för närvarande endast översatt till Windows

- Vid fel, ta kontakt per e-post atostek-id@atostek.com
  - Denna kanal endast för rapportering av bugie
  - Det finns separata anvisningar för rapporteringens innehåll och utformning

ATOSTEK

Kommandon som genomförts för den första produktionspublikationen

- Initialize
- Finalize
- GetInfo
- GetFunctionList
- GetInterfaceList
- GetInterface
- GetFunctionStatus
- CancelFunction
- OpenSession
- CloseSession
- CloseAllSessions
- GetSessionsInfo
- Login
- Logout
- GetSlotList
- GetSlotInfo
- GetTokenInfo
- WaitForSlotEvent
- GetMechanismList
- GetMechanismInfo

- Observera att alla funktioner som definieras i specifikationen för PKCS#11 inte betjänar identifierade användningsfall för kort enligt FINEID-specifikationen
- Ordningen för genomförandet av funktionerna stöder sig i stor utsträckning på identifierade användningsfall

ATOSTEK

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

PKCS#11: framtida egenskaper

- Genomförande av de sista nödvändiga gränssnittsfunktionerna
- Översättning av modulen även för operativsystemen MacOS och Linux


Frågor?
ATOSTEK

Svar på frågor i chatten

- Är Atostek ID kompatiblem med Citrix och har funktionen testats och bekräftats med Citrix?
  - Atostek ID:s SCS-gränssnitt fungerar i Citrix-miljön med Virtual Loopback IP
- När är den första publikationsversionen av Atostek ID tillgänglig?
  - Inget officiellt beslut har ännu fattats. Information om publikationen ges senare separat.

ATOSTEK

Svar på frågor i chatten

- Finns felloggen för Atostek ID på någon av datorns diskar?
  - Felloggens lagringsplatser har sammanställts på de bilder som finns i början av presentationen och som används för att hantera installationen av applikationen.
- I vilka mappar sparas SCS- och ERA-tjänsternas CA- och arbetsstationscertifikat samt nyckelfiler?
  - Svaren på dessa frågor finns i den första integrationsutbildningen.

ATOSTEK

Svar på frågor i chatten

- Kommer de certifikat som krävs för signering av WHQL-drivrutinen med installationspaketet?
  - Alla nödvändiga filer kommer att inkluderas i installationspaketet.
- Hur omfattande är de vanligaste biblioteken för programutveckling (.NET, Java, andra)? funktionen av signatur/crypto gränssnitt ”på högre nivå” har testats med AtostekID (dvs. motsvarar den det tidigare DigiSign-genomförandet)?
  - De nämnda gränssnitten har inte testats separat, men Atostek ID genomför version 7.07 av Minidriver och version 3.1. av standarden PKCS#11. Således motsvarar genomförandet till största delen DigiSigns genomförande.

ATOSTEK

Svar på frågor i chatten

- Hur länge kan DigiSign fortfarande användas?
  - MDB informerar separat om detta.
- Finns det en testversion av PKCS#11-biblioteket?
  - Det finns ingen testversion av PKCS#11-gränssnittet. I den första produktionspublikationen erbjuds en modul för Windows från gränssnittet.

ATOSTEK