

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

14.8.2024



Sisältö

- Koulutuksen tarkoitus ja tavoite
- Atostek ID: Yleinen esittely ja sovelluksen asentaminen
- Debug-lokitus ja virhelokin avaaminen
- Rajapintojen lyhyt esittely
 - SCS
 - Minidriver, (TokenDriver)
 - PKCS#11
 - erasmartcard.ehoito.fi
- Minidriver
- PKCS#11
- Aikaa kysymyksille
- Tarvittaessa pidetään tauko

Koulutuksen tarkoitus ja tavoite

Tarkoitus ja tavoite

- Tämä koulutus on suunnattu niille toimijoille, joiden järjestelmä integroituu käyttämään Atostek ID –ohjelmiston Minidriver- ja/tai PKCS#11-rajapintaa
- Koulutus on kaksiosainen
 - Kesäkuussa järjestettiin ei-pakollinen integraatiokoulutuksen esiosa
 - Ensimmäisessä osassa (7.8.) käytiin läpi SCS-rajapinta kokonaisuudessaan
 - Toisessa osassa (14.8.) käydään läpi Minidriver- ja PKCS#11-rajapinnat

Yleinen esittely ja asentaminen

Atostek ID



- Digi- ja väestötietoviraston uusi kortinlukijaohjelmisto
- Julkaistu rajatulle joukolle testaajia jo 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

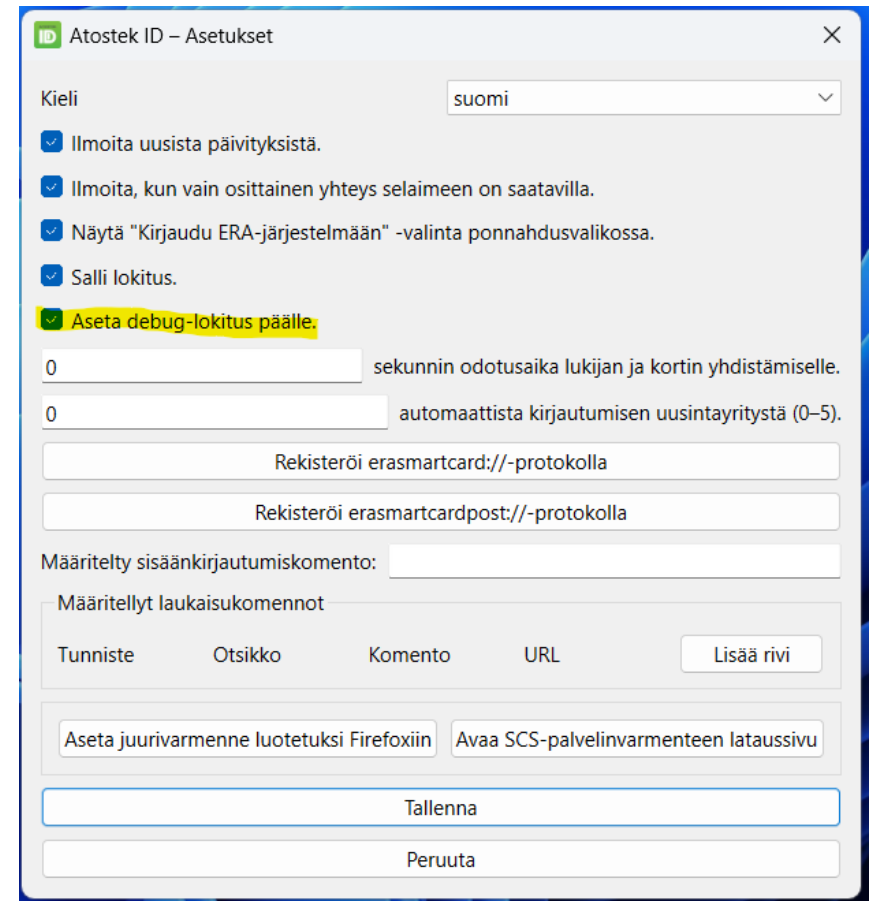
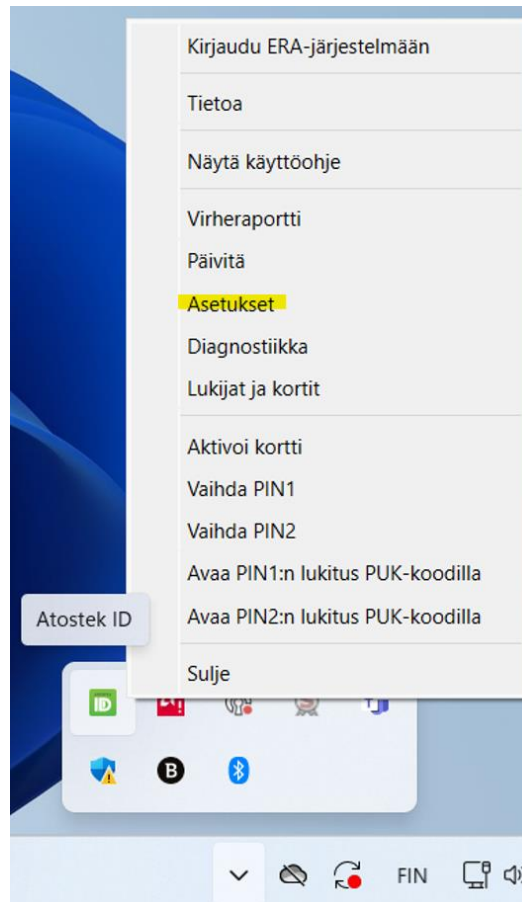
Asentaminen Linux

- Asennus Debianille:
 - `sudo dpkg -i <paketin nimi>.deb`
- Asennus Red Hatille:
 - `sudo dnf install<paketin nimi>.rpm`
- Mahdollisuus asetusparametrien käytölle tulee myöhemmissä tuotantojulkaisuissa

Debug-lokitus ja virhelokin avaaminen

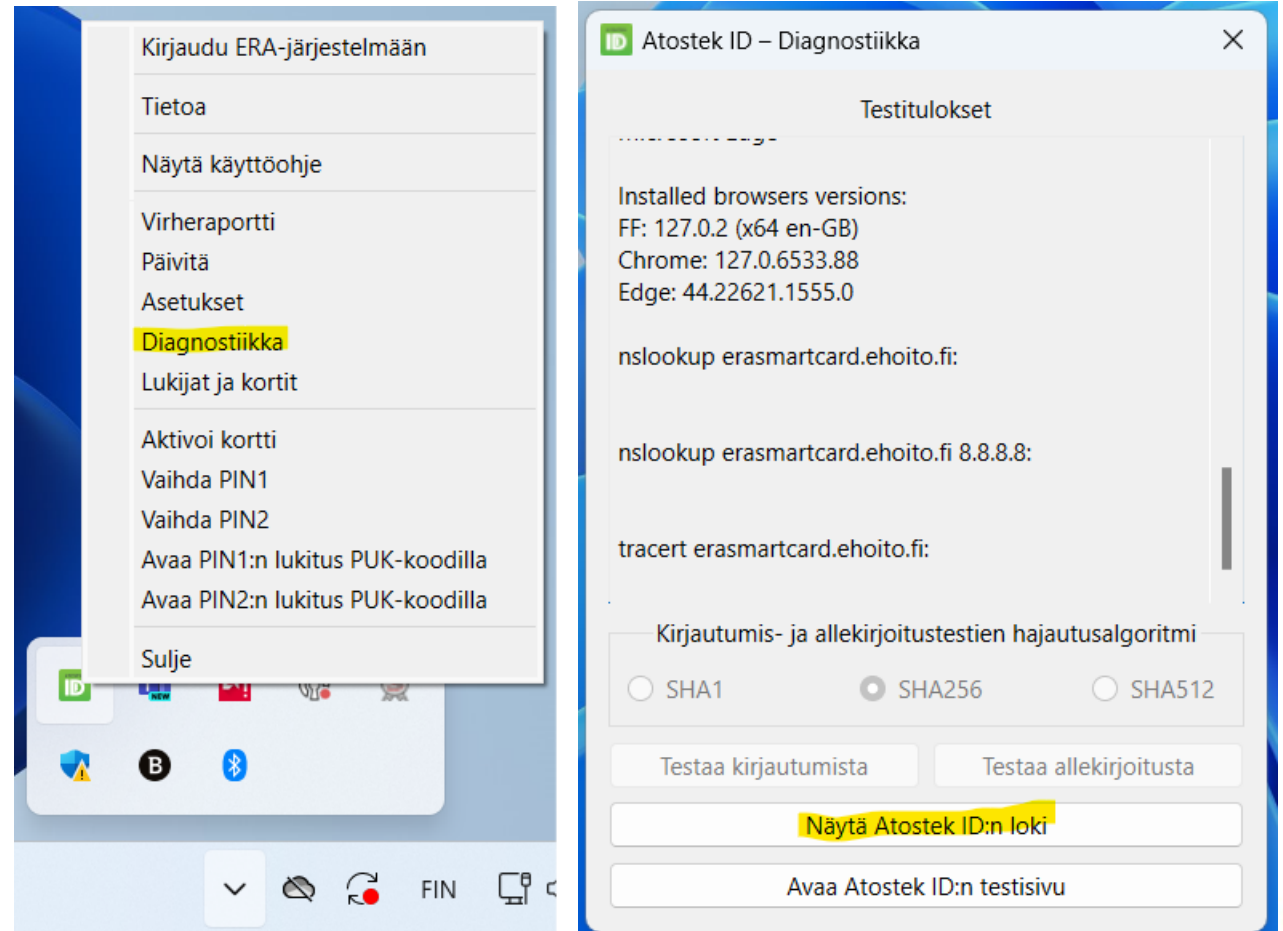
Debug-lokituksen käyttöönotto

- 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 diagnostiikkä-näkymästä
 - Valikosta "Diagnostiikka" → "Näytä Atostek ID:n loki"



Rajapintojen lyhyet esittelyt

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](#)

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](#) 



Minidriver yleisesti

- Windows-käyttöjärjestelmälle toteutettu ajuri, joka kommunikoi älykorttien kanssa
- Toteutettu toimimaan juuri Digi- ja väestötietoviraston tuottamien varmennekorttien kanssa
 - [FINEID-määrittelyt](#)
- Käyttöjärjestelmä hyödyntää Minidriveria suoraan esimerkiksi työasemakirjautumisessa
- Muut sovellukset voivat myös hyödyntää Minidriveria esimerkiksi sähköisten allekirjoitusten tekemiseksi
- Atostek ID Minidriver toteuttaa rajapinnan version 7.07 soveltuvin osin
 - [Minidriver rajapintadokumentaatio](#)

TokenDriverista

- Toimikorttikirjautuminen MacOS työasemiin vaatii TokenDriverin toteuttamisen
- On sovittu DVV:n kanssa, että TokenDriver toteutetaan syksyllä elokuun ensimmäisen tuotantojulkaisun jälkeen

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
 - [FINEID-määritykset](#)
- Moduulista käännetään oma versio eri käyttöjärjestelmille
 - Windows, MacOS ja Linux
- Atostek ID:n PKCS#11-moduuli toteuttaa rajapinnan version 3.1 soveltuvin osin
 - [PKCS#11 rajapinnan dokumentaatio](#)

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 ID Minidriver



Minidriver yleisesti

- Windows-käyttöjärjestelmälle toteutettu ajuri, joka kommunikoi älykorttien kanssa
- Toteutettu toimimaan juuri Digi- ja väestötietoviraston tuottamien varmennekorttien kanssa
 - [FINEID-määrittelyt](#)
- Käyttöjärjestelmä hyödyntää Minidriveria suoraan esimerkiksi työasemakirjautumisessa
- Muut sovellukset voivat myös hyödyntää Minidriveria esimerkiksi sähköisten allekirjoitusten tekemiseksi
- Atostek ID Minidriver toteuttaa rajapinnan version 7.07 soveltuvin osin
 - [Minidriver rajapintadokumentaatio](#)

Minidriver yleisest

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](#).

Minidriver: Rajapintafunktiot

4	Card Minidriver API Reference	19
4.1	Initialization and Deconstruct	19
4.1.1	CardAcquireContext	19
4.1.2	CardDeleteContext	23
4.2	Card PIN Operations	23
4.2.1	Data Structures and Enumerations	24
4.2.2	CardAuthenticatePin	29
4.2.3	CardGetChallenge	30
4.2.4	CardAuthenticateChallenge	31
4.2.5	CardDeauthenticate	32
4.2.6	CardAuthenticateEx	33
4.2.7	CardGetChallengeEx	36
4.2.8	CardDeauthenticateEx	37
4.2.9	CardChangeAuthenticatorEx	38
4.2.10	CardUnblockPin	39
4.2.11	CardChangeAuthenticator	41
4.3	Public Data Operations	42
4.3.1	CardCreateDirectory	43
4.3.2	CardDeleteDirectory	44
4.3.3	CardReadFile	44
4.3.4	CardCreateFile	45
4.3.5	CardGetFileInfo	47
4.3.6	CardWriteFile	47
4.3.7	CardDeleteFile	49
4.3.8	CardEnumFiles	49
4.3.9	CardQueryFreeSpace	50
4.4	Card Capabilities (Minidriver Version 5 and Earlier)	51
4.4.1	Defines and Data Structures	51
4.4.2	CardQueryCapabilities	52
4.5	Card and Container Properties	52
4.5.1	Defines and Data Structures	52
4.5.2	CardGetContainerProperty	53
4.5.3	CardSetContainerProperty	54
4.5.4	CardGetProperty	56
4.5.5	CardSetProperty	60
4.6	Key Container	63
4.6.1	CardCreateContainer	63
4.6.2	CardCreateContainerEx	65
4.6.3	CardDeleteContainer	67
4.6.4	CardGetContainerInfo	67
4.7	Cryptographic Operations	69
4.7.1	CardRSADecrypt	69
4.7.2	CardConstructDHAgreement	70
4.7.3	CardDeriveKey	71
4.7.4	CardDestroyDHAgreement	74
4.7.5	CardSignData	74
4.7.6	CardQueryKeySizes	78
4.8	Secure Key Injection	78

Minidriver: tunnistetut puutteet

- Ensimmäisessä tuotantojulkaisussa on puutteita
 - Minidriverilla ei vielä ole virallista WHQL-allekirjoitusta
 - Minidriver ei myöskään asennu suoraan Atostek ID:n asennuksen yhteydessä
 - Erillinen AD-rekisteröintipalvelu ei ole vielä saatavilla
- Yhteydenotot virhetilanteissa sähköpostiin atostek-id@atostek.com
 - Tämä kanava vain bugien raportointia varten
 - Raportoinnin sisältöön ja muotoiluun on erilliset ohjeet

Ensimmäiseen tuotantojulkaisuun toteutetut komennot

- CardAcquireContext
 - CardDeleteContext
 - CardAuthenticatePin
 - CardAuthenticateEx
 - CardReadFile
 - CardGetFileInfo
 - CardEnumFiles
 - CardGetContainerProperty
 - CardGetProperty
 - CardGetContainerInfo
 - CardRSADecrypt
 - CardSignData
 - CardQueryFreeSpace
 - CardQuerySizes
- Huomaa, että kaikki Minidriverin speksissä määritellyt funktiot eivät palvele FINEID-speksin mukaisten korttien tunnistettuja käyttötapauksia
 - Tunnistettuja käyttötapauksia on hyödynnetty funktioiden toteuttamisjärjestykseen

Minidriver: Toteutetut komennot

4	Card Minidriver API Reference	19	
4.1	Initialization and Deconstruct	19	
4.1.1	CardAcquireContext	19	
4.1.2	CardDeleteContext	23	
4.2	Card PIN Operations	23	
4.2.1	Data Structures and Enumerations	24	
4.2.2	CardAuthenticatePin	29	
4.2.3	CardGetChallenge	30	
4.2.4	CardAuthenticateChallenge	31	
4.2.5	CardDeauthenticate	32	
4.2.6	CardAuthenticateEx	33	
4.2.7	CardGetChallengeEx	36	
4.2.8	CardDeauthenticateEx	37	
4.2.9	CardChangeAuthenticatorEx	38	
4.2.10	CardUnblockPin	39	
4.2.11	CardChangeAuthenticator	41	
4.3	Public Data Operations	42	
4.3.1	CardCreateDirectory	43	
4.3.2	CardDeleteDirectory	44	
4.3.3	CardReadFile	44	
4.3.4	CardCreateFile	45	
4.3.5	CardGetFileInfo	47	
4.3.6	CardWriteFile	47	
4.3.7	CardDeleteFile	49	
4.3.8	CardEnumFiles	49	
4.3.9	CardQueryFreeSpace	50	
4.4	Card Capabilities (Minidriver Version 5 and Earlier)	51	
4.4.1	Defines and Data Structures	51	
4.4.2	CardQueryCapabilities	52	
4.5	Card and Container Properties	52	
4.5.1	Defines and Data Structures	52	
4.5.2	CardGetContainerProperty	53	
4.5.3	CardSetContainerProperty	54	
4.5.4	CardGetProperty	56	
4.5.5	CardSetProperty	60	
4.6	Key Container	63	
4.6.1	CardCreateContainer	63	
4.6.2	CardCreateContainerEx	65	
4.6.3	CardDeleteContainer	67	
4.6.4	CardGetContainerInfo	67	
4.7	Cryptographic Operations	69	
4.7.1	CardRSADecrypt	69	
4.7.2	CardConstructDHAgreement	70	
4.7.3	CardDeriveKey	71	
4.7.4	CardDestroyDHAgreement	74	
4.7.5	CardSignData	74	
4.7.6	CardQueryKeySizes	78	
4.8	Secure Key Injection	78	

Esimerkki: CardSignData

- Funktiot palauttavat DWORD-tyyppin
- Funktioiden parametrit on selitetty
- Dokumentaatioissa on annettu myös täsmennyksiä kommentteja

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

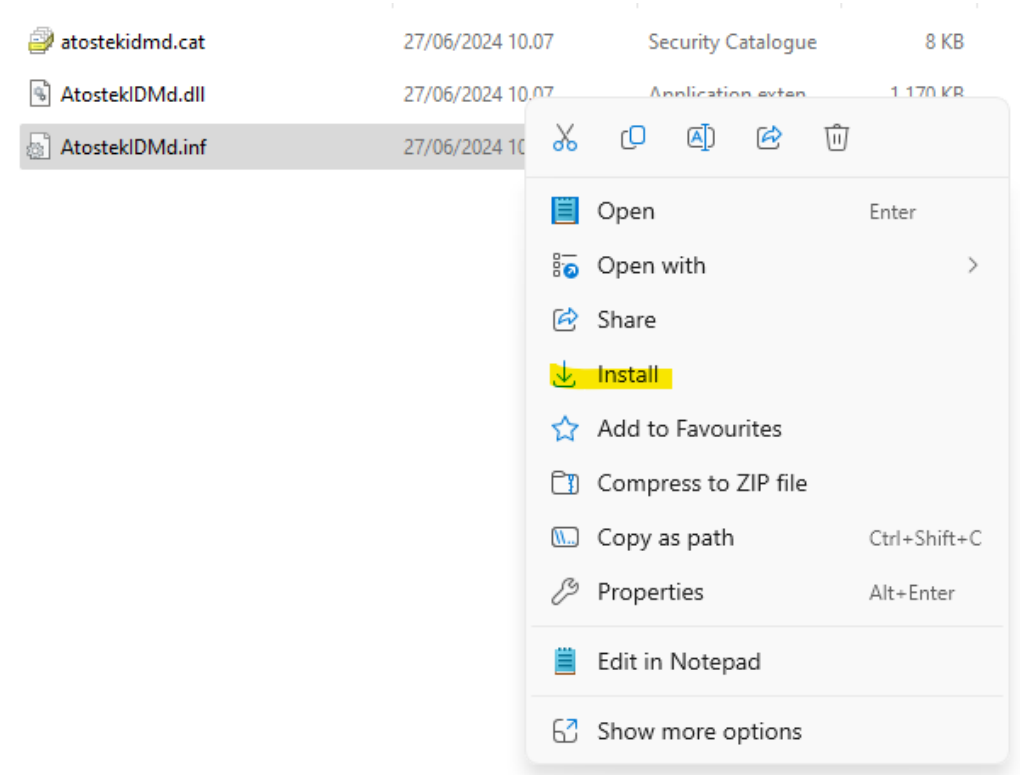
Zero on success; otherwise, nonzero.

Minidriver: asentaminen

- Atostek ID Minidriveria voi testata ennen kuin sillä on virallinen WHQL-allekirjoitus
 - Testaajille tarjotaan testiallekirjoitus (atostekidmd.cat), joka tulee pitää samassa sijainnissa moduulin .dll ja .inf tiedostojen kanssa. Nämä kaikki julkaistaan DVV:n sivuilla Minidriverin yhteydessä
 - Testiallekirjoituksen käyttö voidaan sallia komennolla ***bcdedit /set testsigning on***
 - Komento täytyy ajaa adminina
 - Lisää tietoa komennosta löytyy [Microsoftin Minidriver dokumentaatiosta](#)
 - "bcdedit /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**

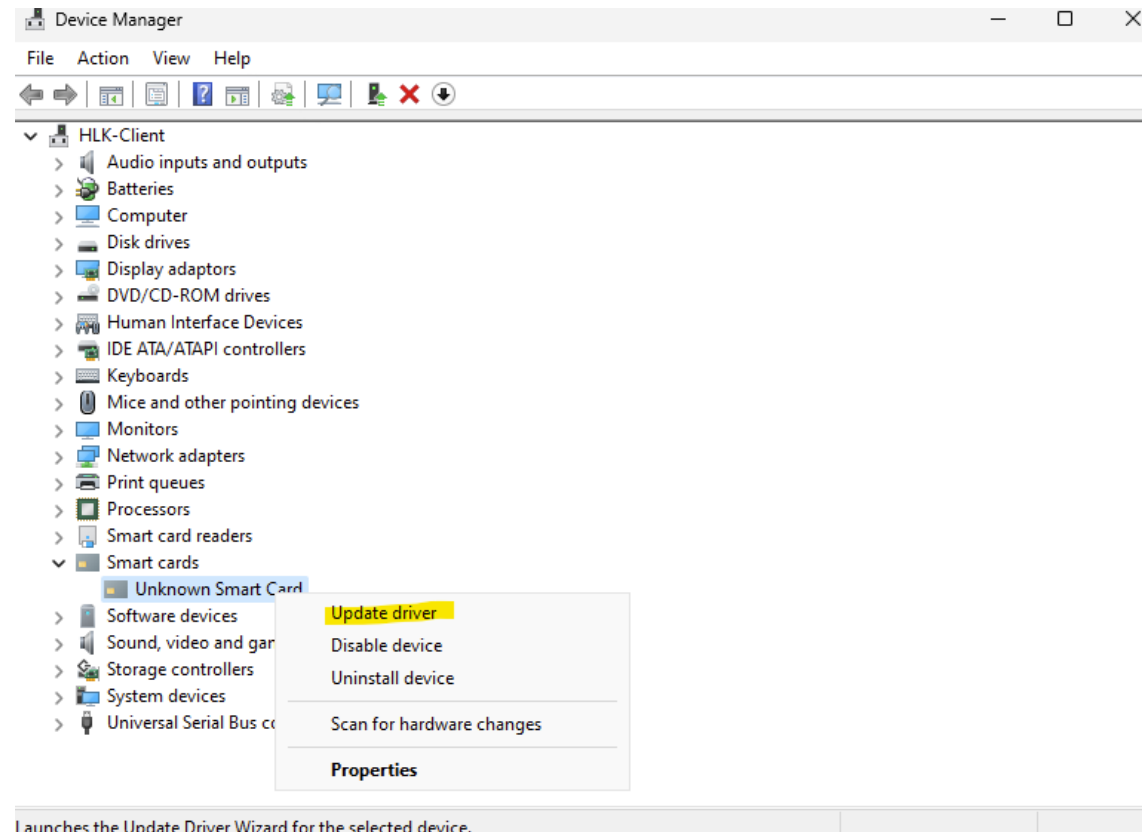
Ajurin manuaalinen asentaminen

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



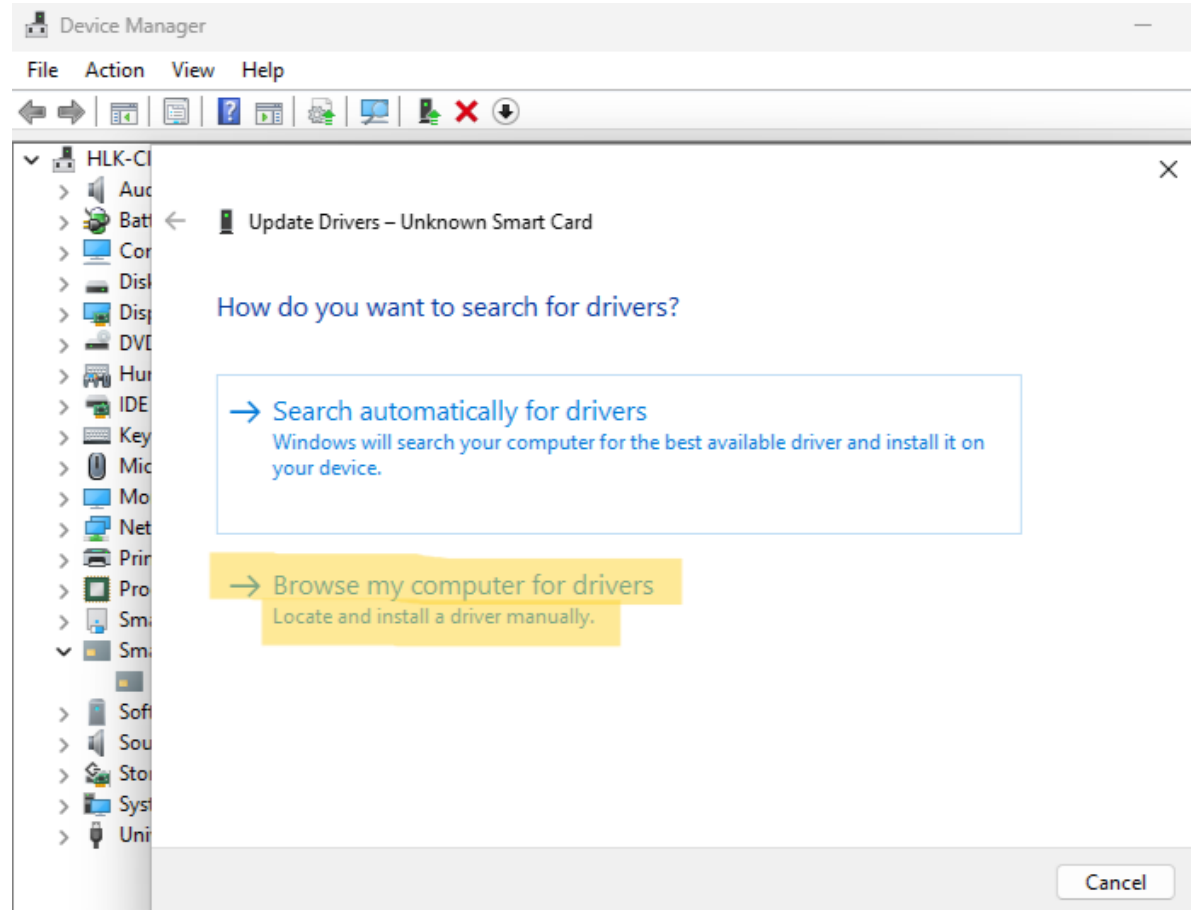
Ajurin manuaalinen asentaminen

- Tarvittaessa ajuri asetetaan vielä erikseen **Device Managerin** kautta
- Älykortin pitää olla kiinni lukijassa



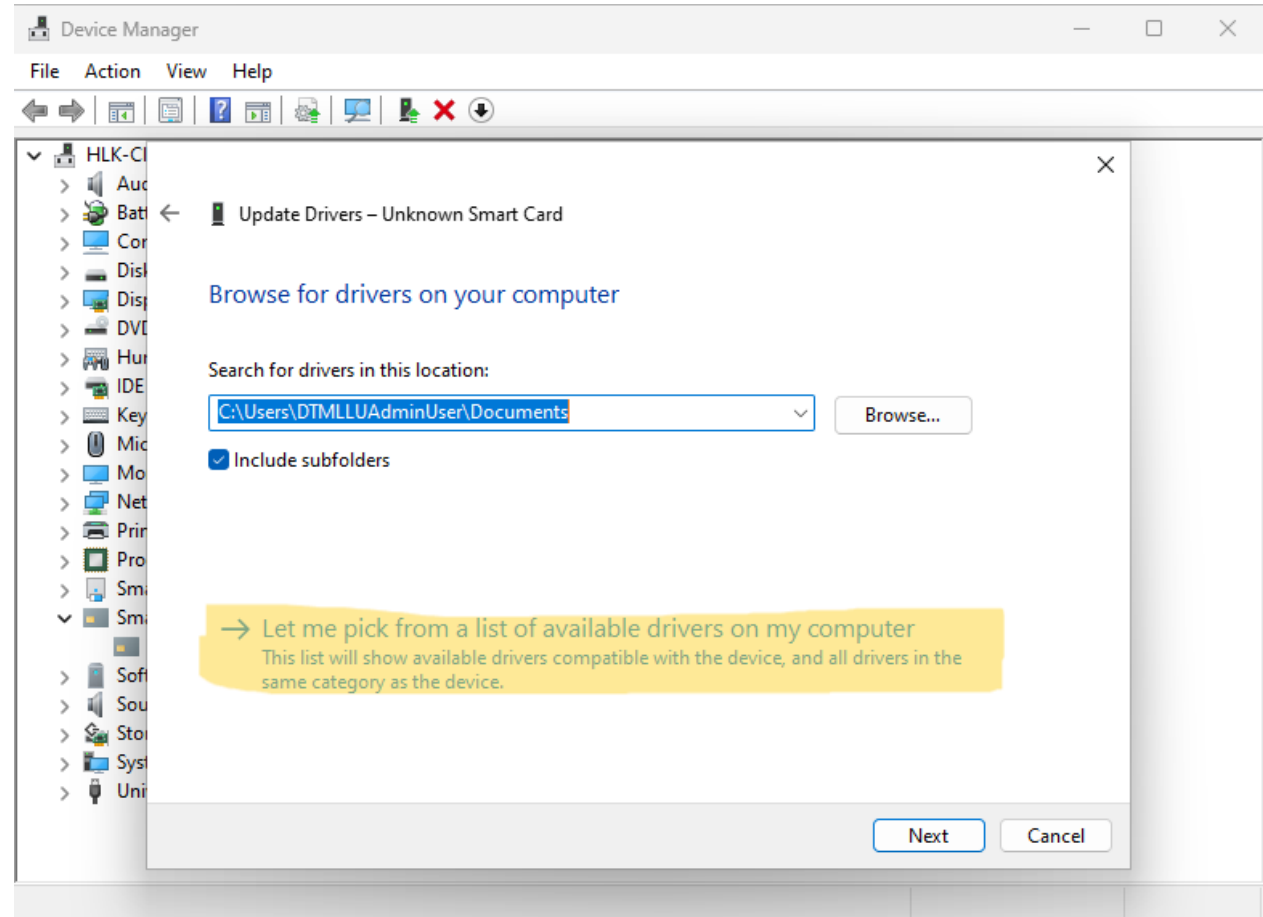
Ajurin manuaalinen asentaminen

- Windowsin automaattinen haku ei ehdota ajuria, joten se on etsittävä manuaalisesti.



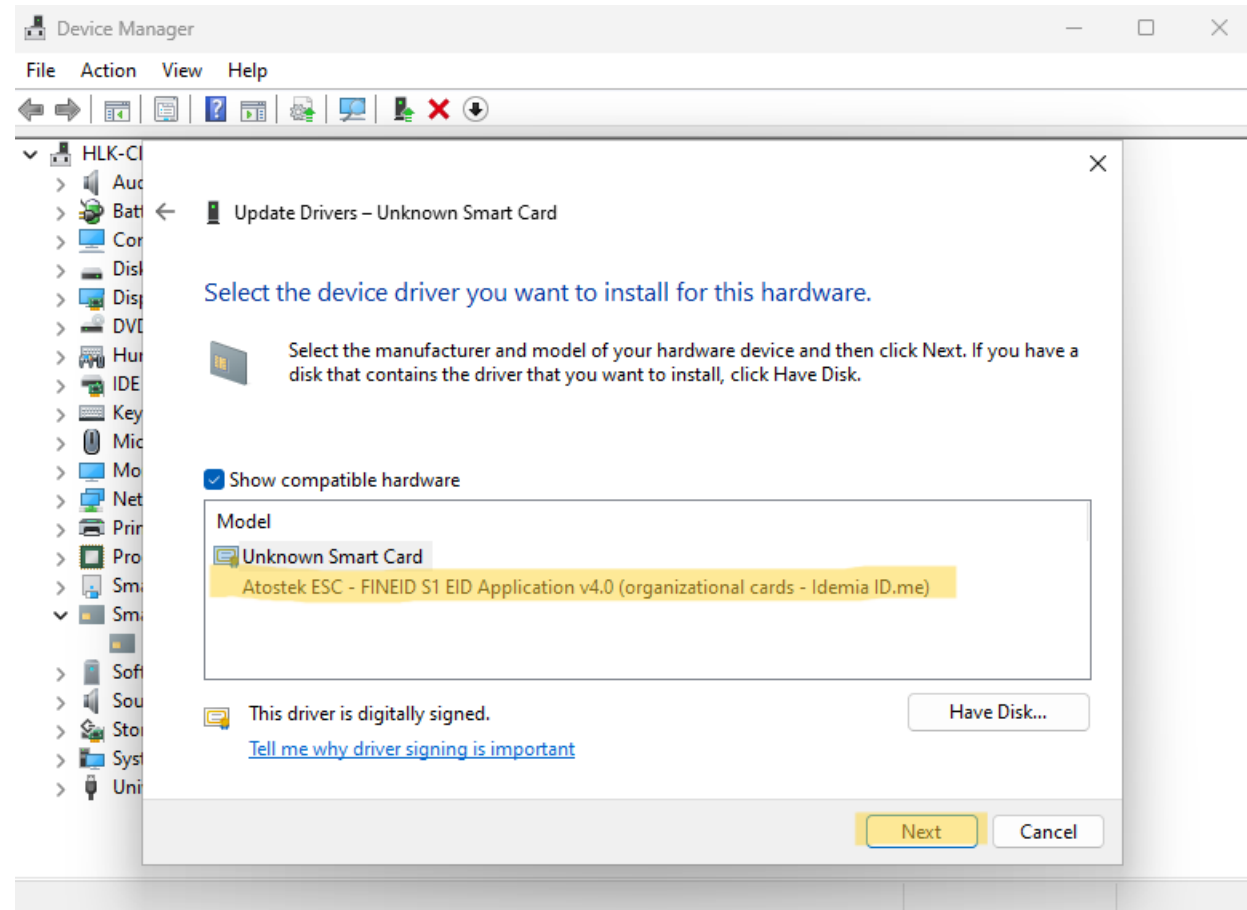
Ajurin manuaalinen asentaminen

- Valitaan ajuri sopivien ajurien listasta



Ajurin manuaalinen asentaminen

- Windows ehdottaa ajuria kortille yhteensopivana. Asennetaan ajuri.



WHQL allekirjoitus ja asentaminen tuotantoversiossa

- Minidriverille haetaan virallinen WHQL-allekirjoitus, minkä jälkeen ajuri pyritään julkaisemaan mahdollisimman pian. Tällöin ajurin asennus onnistuu suoraan ilman testiallekirjoitusten sallimista.
- Julkaistavassa versiossa tarvittavat tiedostot (dll, inf, cat) pyritään tallentamaan laitteelle asennuksen yhteydessä eikä niitä tällöin tarvitse erikseen ladata. Tästä tulee tarkemmat ohjeet julkaisun integraatio-ohjeeseen.
- Myös tuotantoversiossa asennus käyttää .inf tiedostoa

Käyttötapaukset

- Huomioittehan, että ensimmäisessä tuotantojulkaisussa ei ole toteutettu kaikkia komentoja, joten kaikkia käyttötapauksia ei voida vielä testata.
- Myöhempien tuotantojulkaisuiden 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.

TokenDriver

- Toimikorttikirjautuminen MacOS työasemiin vaatii TokenDriverin toteuttamisen
- On sovittu DVV:n kanssa, että TokenDriver toteutetaan syksyllä elokuun ensimmäisen tuotantojulkaisun jälkeen

Minidriver: tulevat ominaisuudet

- WHQL-allekirjoitettu ajuri
- Erillinen AD-rekisteröintipalvelu Windowsille
- Otetaan Atostek ID:n PIN-dialogit käyttöön
- Ajurin asentaminen Atostek ID –sovelluksen asentamisen yhteydessä
- MacOS TokenDriver (toimikorttikirjautuminen MacOS:lla)



Atostek ID PKCS#11



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:n PKCS#11-moduuli toteuttaa rajapinnan version 3.1
 - [PKCS#11 rajapinnan dokumentaatio](#)

PKCS#11: Rajapintafunktiot

- PKCS#11-rajapinta määrittelee kokonaisuudessaan yli 100 eri funktiota
 - Näistä toteutetaan aluksi ne, jotka tukevat tunnistettuja käyttötapauksia
- Funktiot voidaan jaotella eri käyttötarkoituksiluokkiin
 - Yleiset funktiot
 - Istuntofunktiot
 - Salausfunktiot
 - Allekirjoitus- ja varmennusfunktiot
 - Tiivistefunktiot
 - Avainparin luonti- ja johdannaisfunktiot
 - ...

Esimerkki: 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.

PKCS#11: tunnistetut puutteet

- Ensimmäisessä tuotantojulkaisussa on puutteita
 - PKCS#11-moduulin kaikkia tarvittavia funktioita ei ole vielä toteutettu
 - Moduuli on tällä hetkellä käännetty vain Windowsille
- Yhteydenotot virhetilanteissa sähköpostiin atostek-id@atostek.com
 - Tämä kanava vain bugien raportointia varten
 - Raportoinnin sisältöön ja muotoiluun on erilliset ohjeet

Ensimmäiseen tuotantojulkaisuun toteutetut komennot

- Initialize
 - Finalize
 - GetInfo
 - GetFunctionList
 - GetInterfaceList
 - GetInterface
 - GetFunctionStatus
 - CancelFunction
 - OpenSession
 - CloseSession
 - CloseAllSessions
 - GetSessionsInfo
 - Login
 - Logout
 - GetSlotList
 - GetSlotInfo
 - GetTokenInfo
 - WaitForSlotEvent
 - GetMechanismList
 - GetMechanismInfo
- Huomaa, että kaikki PKCS#11:n speksissä määritellyt funktiot eivät palvele FINEID-speksin mukaisten korttien tunnistettuja käyttötapauksia
 - Funktioiden toteuttamisjärjestys nojaa pitkälti tunnistettuihin käyttötapauksiin

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

PKCS#11: tulevat ominaisuudet

- Loppujen tarvittavien rajapintafunktioiden toteutus
- Moduulin kääntäminen myös MacOS- ja Linux-käyttöjärjestelmille



Kysyttävää?

Vastauksia chatissa esitettyihin kysymyksiin

- Onko Atostek ID Citrix-yhteensopiva ja toimivuus testattu ja varmistettu Citrix:llä?
 - Atostek ID:n SCS-rajapinta toimii Citrix-ympäristössä käyttäen Virtual Loopback IP:tä
- Milloin Atostek ID:n ensimmäinen julkaisuversio on saatavilla?
 - Virallista päätöstä ei vielä ole tehty. Julkaisusta tiedotetaan myöhemmin erikseen.

Vastauksia chatissa esitettyihin kysymyksiin

- Löytyykö Atostek ID:n virheloki jostain koneen levyltä?
 - Virhelokin tallennussijainnit on koottu esityksen alusta löytyville kalvoille, joilla käsitellään sovelluksen asentamista.
- Mihin kansioihin työasemakohtaiset SCS- ja ERA-palveluiden CA- ja työasemavarmenteet sekä avaintiedostot tallentuvat?
 - Vastaukset näihin kysymyksiin löytyvät ensimmäisestä integraatiokoulutuksesta.

Vastauksia chatissa esitettyihin kysymyksiin

- Tulevatko WHQL ajurin allekirjoituksen vaatimat sertifikaatit asennuspaketin mukana?
 - Asennuspakettiin tullaan sisällyttämään kaikki tarvittavat tiedostot.
- Kuinka laajasti yleisimpien ohjelmistokehityskirjastojen (.NET, Java, muita?) "korkeamman tason" allekirjoitus/crypto rajapintojen toimivuutta on testattu AtostekID:n kanssa (so. vastaako aikaisempaa DigiSign toteutusta)?
 - Mainittujen rajapintojen toimivuutta ei ole erikseen testattu, mutta Atostek ID toteuttaa Minidriverin version 7.07 ja PKCS#11-standardin version 3.1. Näin ollen toteutus vastaa suurimmilta osin DigiSignin toteutusta.

Vastauksia chatissa esitettyihin kysymyksiin

- Mihin saakka DigiSignia voidaan edelleen käyttää?
 - DVV tiedottaa tästä erikseen.
- Onko PKCS#11-kirjastosta testiversiota?
 - PKCS#11-rajapinnasta ei ole testiversiota. Ensimmäisessä tuotantojulkaisussa rajapinnasta on tarjolla moduuli Windowsille.