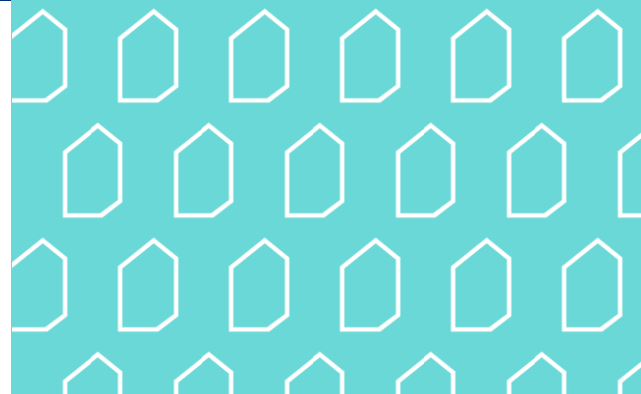


Informationstillfälle om Myndigheten för digitalisering och befolkningsdatas kortläsarprogram

14.5.2024



**MYNDIGHETEN FÖR
DIGITALISERING OCH
BEFOLKNINGSDATA**



Konkurrensutsättning av kortläsarprogram

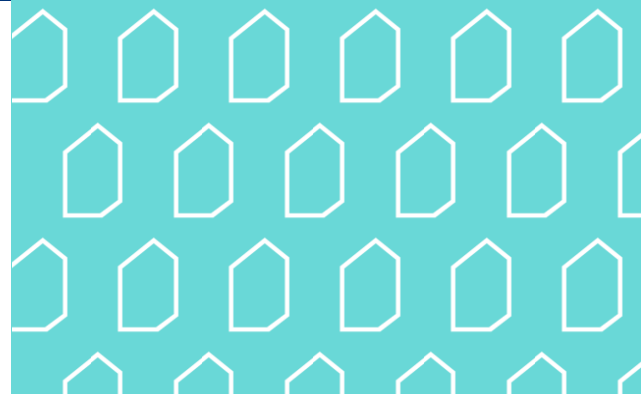
Jari Pirinen

Produktchef, certifikat

Myndigheten för digitalisering och befolkningsdata



**MYNDIGHETEN FÖR
DIGITALISERING OCH
BEFOLKNINGSDATA**



Presentationens innehåll

1. Vad gör kortläsarprogrammet?
2. Bakgrund till konkurrensutsättningen
3. Krav på den produkt som konkurrensutsätts
4. Konkurrensutsättningens resultat



Vad gör kortläsarprogrammet?

- Erbjuder datasystem och applikationer gränssnitt via vilka certifikatkortet kan utnyttjas. Kortets chip kommunicerar med APDU-kommandogränssnittet på låg nivå. Detta visas för användaren/applikationen t.ex. som ett signeringsgränssnitt.
- Stöder olika chipmodeller/-generationer med olika specifikationer.
- Erbjuder användaren ett nytt användargränssnitt för kortanvändning, t.ex. en kortaktiveringsdialog.
- Erbjuder användaren andra funktioner för kortet och de certifikat som finns på det, såsom elektronisk signering av dokument eller lagring av certifikatet från kortet till arbetsstationen.



Bakgrund till konkurrensutsättningen 1/2

- MDB erbjuder kostnadsfritt sina kortkunder ett kortläsarprogram vars licens- och utvecklingskostnader ingår i certifikatkortet.
- Det nuvarande kortläsarprogrammet **Fujitsu mPollux DigiSign Client** som MDB erbjuder sina kunder har varit i bruk sedan 2008. MDB har således bedömt att det behöver konkurrensutsättas.
- Konkurrensutsättningen genomfördes 10/2023 – 2/2024.
- Utgångspunkten för konkurrensutsättningen var att välja en produkt vars egenskaper motsvarar den nuvarande. Denna nivå bör uppnås antingen med den valda produktens nuvarande status eller genom produktutvecklingsarbete under ibruktagningsprojektet.



Bakgrund till konkurrensutsättningen 2/2

- Jämförelsegrunderna för konkurrensutsättningen var pris, kvalitet och ibruktagsplan.
- Konkurrensutsättningen var tudelad och det var möjligt att erbjuda ett eller båda delområden:
 1. kortläsarprogram: Windows, MacOS och Linux (ChromeOS optionellt)
 2. mobilkortläsarapplikation: Android och iOS
- I de delhelheter som konkurrensutsätts ingår också ett ibruktagsprojekt och tekniskt stöd.



Krav på den produkt som konkurrensutsätts

För skrivbordsprogrammet uppställdes 81 olika krav och för mobilapplikationen 58 olika krav, bl.a.:

- Stöd för alla MDB:s korttyper: Organisationskort, yrkeskort för social- och hälsovården, personalkort för social- och hälsovården, aktörskort för social- och hälsovården, identitetskort (Medborgarcertifikat), tillfälligt kort, reservkort för social- och hälsovården.
- Erbjuder gränssnitt via vilka applikationer och datasystem kan anropa kortet:
 - PKCS#11, SCS, Microsoft CryptoAPI / CNG, eventuellt produktens eget gränssnitt eller toolkit/SDK.
- Stöd för operativsystem: Windows, MacOS, Linux (ChromeOS optiona) samt i mobilen Android och iOS.
- Utnyttjande av operativsystemets certifikatlager (certificate store) och i Windows en WHQL-certifierad minidriver som direkt stöder de vanligaste Windows-skrivbordsapplikationerna.
- Stöd för identifiering och underskrift med RSA- och ECC-nycklar, kommande PQC-algoritmer ska beaktas.
- Stöd för identifiering av tillfälliga certifikat på reservkort.



Konkurrensutsättningens resultat

- I konkurrensutsättningen deltog fem tjänsteleverantörer och **Atostek Oy** vann båda delområdena.
- MDB genomför tillsammans med Atostek Oy ett nytt ibruktagningsprojekt av kortläsarprogrammet från och med 3/2024. Ibruktagningen av mobilkortläsarapplikationen sker efter ibruktagningen av skrivbordsversionen.
- Enligt tidtabellen för ibruktagningen publiceras det nya kortläsarprogrammet **Atostek ID** för MDB:s kunder för nedladdning på Windows, Mac OS och Linux i **augusti 2024**.
- Enligt nuvarande uppgifter är DigiSign tillgänglig för kunderna fram till den 31 december 2024.
- Närmare information om tidtabeller och utbildningar finns i följande presentation.

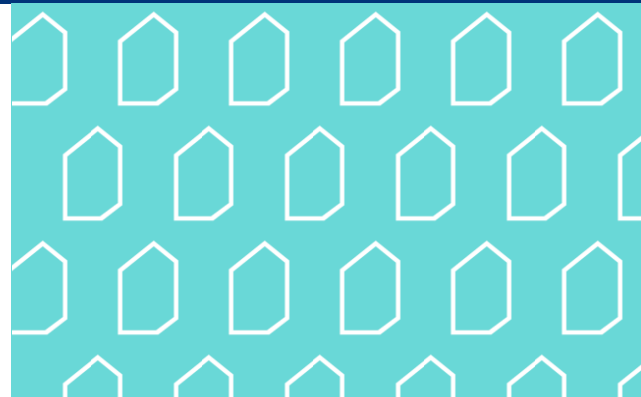


Tidtabeller för projektet för kortläsarprogram

Arttu Kailanto
Projektchef
MDB



**MYNDIGHETEN FÖR
DIGITALISERING OCH
BEFOLKNINGSDATA**



Tidtabell för ibruktagningsprojektet

Fas	Q1/2024	Q2/2024	Q3/2024	Q4/2024
Kravspecifikation		15.5.2024		
Utvecklingsarbete			1.8.2024	
Godkännandetest			16.8.2024	
Ibruktagande				
Testutgåva 1		★ 29.5.2024		
Testutgåva 2			★ 26.6.2024	

Obs: Projektet med applikationen för mobilkortläsare inleds efter projektet för kortläsarprogram. Tidtabellen meddelas senare.



Plan för testutgåvor

1. Testutgåva 29.5.2024

- Windows-stöd, MacOS-stöd, Linux-stöd (installation, anslutning av kort och läsare och andra funktioner som redan stöds av applikationen)
- Alla korttyper och krypteringsmetoder som stöds (aktivering, byte och öppning av koder osv.) och hantering av kortobjekt
- SCS-gränssnitt.

2. Testutgåva 26.6.2024

- PKCS#11-gränssnitt
- Inloggning med certifikatkort på arbetsstationen (dvs. t.ex. Minidriver för Windows, AD-registreringstjänsten kommer dock först senare)
- mTLS-identifiering
- Stöd för e-postapplikationer
- Signering av PDF-dokument
- Preliminär version av Toolkit



Utbildningar

- Utbildning för ibruktagning: måndag 3.6.2024 kl. 9-11
 - Kort allmän presentation av applikationen
 - Installation och inställningar av applikationen
 - Hantering av kortobjekt och nyckeltal
 - Allmänt om uppdatering av applikationen, bruksanvisningar och felrapportering
 - Exempel: identifiering i systemet
- Förutbildning i integration: måndag 1.7.2024 kl. 10-12
 - Kort allmän presentation av applikationen
 - Kort om installation av applikationen
 - Presentation av olika integreringssätt och deras gränssnitsdokumentation
- Integrationsutbildning del 1: onsdag 7.8.2024 kl. 12-16
 - Kort allmän presentation av applikationen
 - Kort om installation av applikationen
 - SCS-gränssnittet och dess användning
 - Toolkit och utnyttjande av den
- Integrationsutbildning del 2: onsdag 14.8.2024 kl. 12-16
 - PKCS#11-modulen och dess användning
 - Inloggning på arbetsstationen



Frågor och svar 1/2

- Fråga: Kräver det nya kortläsarprogrammet att de nuvarande certifikatkorten förnyas?
Svar: Nej, alla tidigare beviljade kort fungerar även i fortsättningen utan förnyelse.
- Fråga: Fungerar Atostek ID och DigiSign på samma arbetsstation samtidigt?
Svar: Man kan inte lova att de fungerar samtidigt. Troligen fungerar de inte på rätt sätt samtidigt.
- Fråga: Kommer programvarans källkod att distribueras?
Svar: Nej, det är inte fråga om en open source-produkt, utan Atostek Oy:s kommersiella produkt.
- Fråga: Hur syns detta för slutanvändaren?
Svar: Användargränssnittet, till exempel frågefönstret för PIN-koden, ser lite annorlunda ut.
- Fråga: Hur syns förändringen för organisationens IT-aktörer?
Svar: Det beror på organisationerna, men de organisationer som ansvarar för installationen av produkterna måste även nu installera produktionsversionen. En del får testversioner under sommaren, men alla får produktionsversioner i augusti med installationsanvisningar.



Frågor och svar 2/2

- Fråga: Linux-stöd, vi använder RedHat? Hur fungerar Mac-kompatibilitet?
Svar: Atostek ID stöder förutom Windows även Mac OS och Linux. Linux-versionen publiceras för Ubuntu- och Red Hat Enterprise Linux-derivat av Linux-distributioner (.deb och .rpm-distributionspaket). Vi kan dock inte garantera att alla Linux-distributioner fungerar på grund av det enorma antalet, vilket gör att det inte är möjligt att beakta allas särdrag i utvecklingen och testningen.
- Fråga: Stöder det nya kortläsarprogrammet Citrix-arbetsstationsvirtualisering?
Svar: Ja, det gör det. Citrix-funktionaliteten testas under sommaren tillsammans med utvalda kunder.
- Fråga: Stöder det nya kortläsarprogrammet AD-registreringstjänsten (Microsofts kommande AD-förändring)?
Svar: Atostek har på kommande en lösning som motsvarar Fujitsu AD Registration Service och som tacklar förändringen i Microsofts AD-miljöer som träder i kraft 2/2025.



Informationstillfälle om Myndigheten för digitalisering och
befolkningsdatas kortläsarprogram

14.5.2024



Innehåll

- Atostek: Presentation av företaget
- Atostek ID:
 - Allmän presentation av programvaran
 - Programvarans funktioner och gränssnitt



Allmän presentation

Atostek

Programutvecklings- och IT-konsulttjänster

- Applikationer för hälso- och sjukvård och medicin
- Produktutveckling inom industrin
- IT-konsultering inom den offentliga sektorn

Exempel

- Atostek ERA
- Atostek ID (ERA SmartCard)



Grundat



130+



3



Atostek ID



- Myndigheten för digitalisering och befolkningsdatas nya kortläsarprogram
- Tidigare känd som ERA SmartCard
- Programvaran har varit i bruk och den har vidareutvecklats i nästan ett decennium
- Stöd för ett allt större antal operativsystem och funktioner i och med leveransprojektet



Funktioner och gränssnitt

Funktioner och gränssnitt som stöds

- Operativsystem
 - Windows och Windows Server
 - Windows 10 & 11, Windows Server 2016, 2019, 2022
 - Massinstallation med t.ex. SCCM-verktyg
 - Citrix: SCS-gränssnittet Virtual Loopback IP i bruk
 - MacOS
 - MacOS 12, 13, 14
 - Intel och Apple Silicon
 - Linux
 - Debian (10, 11, 12)
 - Red Hat (6, 7, 8, 9)
- Språk
 - Finska
 - Svenska
 - Engelska
- Webbläsare
 - Edge
 - Firefox
 - Safari
 - Chrome

Funktioner och gränssnitt som stöds

- Korttyper och krypteringsmetoder
 - Social- och hälsovården, organisation, medborgarcertifikat (identitetskort)
 - RSA, ECC
- Kortläsare
 - Alla läsare som uppfyller PC/SC-standarden
 - Även NFC-läsare
- Hantering av nyckeltal
 - Aktivera kort
 - Byta nyckeltal
 - Öppna nyckeltal
- Hantering av kortobjekt
 - Granskning av uppgifter om läsare och kort
 - Öppna och spara certifikat
 - Registrera certifikat i operativsystemets certifikatlager
 - Manuell kontroll av certifikatets giltighet

Funktioner och gränssnitt som stöds

- Gränssnitt
 - SCS
 - PKCS#11
 - Microsoft CryptoAPI (Minidriver)
- Funktioner
 - Inloggning på arbetsstationen
 - Windows: Minidriver & AD-funktionalitet
 - MacOS: TokenDriver
 - Linux: PKCS#11-gränssnitt
 - Kryptering och underskrift i e-postapplikationer
 - Outlook
 - Apple Mail
 - Thunderbird
 - Skapa en skyddad mTLS-förbindelse
 - Signering av PDF-dokument (PAdES)
 - Via Atostek ID samt programvarorna Adobe och PDF-xchange
- Inställningar
 - Till exempel startinställningar, logginställningar, avgränsning av läsartyper, effekterna av att ta bort kort osv.

Funktioner och gränssnitt som stöds

- Toolkit
 - För att underlätta integrationen
- Generering av tillfälliga certifikat med hjälp av Vartti-systemet

Övrigt

- En utomstående part lämnar in en tillgänglighetsbedömning
 - Programvara
 - Bruksanvisning (WCAG 2.1)
- Datasäkerhetsauditering av programvaran
 - En omfattande auditering utförs under leveransprojektet och med jämna mellanrum därefter
- Distribution av installationspaket
 - Produktionsversioner: MDB:s webbplats
 - Testversioner: Separat egen utdelning

A hand is pointing at a dental X-ray displayed on a tablet. The X-ray shows a full set of teeth. The word "Tack!" is overlaid in large white text. A ruler is visible at the bottom of the tablet.

Tack!



**MYNDIGHETEN FÖR DIGITALISERING
OCH BEFOLKNINGSDATA**

dvv.fi