Atostek ID 4.6 bruksanvisning

för Linux

v1.0

Atostek

Innehållsförteckning

1. ATOSTEK ID PROGRAMBESKRIVNING 4

2. FÖRE ANVÄNDNING OCH HUR BÖRJAR MAN ANVÄNDA ATOSTEK ID? 5

2.1. Vad är Atostek ID? 5

2.2. Vad behöver jag för att använda Atostek ID? 5

2.2.1. Installera Atostek ID 5

2.3. Aktivera smartkortet 6

3. ELEKTRONISK AUTENTISERING OCH ELEKTRONISK SIGNATUR 9

3.1. Elektronisk autentisering 9

3.1.1. mTLS-autentisering 9

3.1.2. Autentisering via SCS-gränssnittet 10

3.1.3. Användning av Atostek ERA -systemet 10

3.2. Elektronisk signatur 11

3.2.1. Signering via SCS-gränssnittet 11

3.2.2. Signering i Atostek ERA-systemet 11

4. FUNKTIONALITET 13

4.1. Start och stängning 13

4.2. Applikationsinformation och bruksanvisning 13

4.3. Byte av PIN-koder och upplåsning av låsta koder 13

4.4. Läsare och kort 14

4.5. Inställningar 16

4.5.1. Språk 16

4.5.2. Meddela om nya uppdateringar 16

4.5.3. Meddela om endast partiell anslutning till webbläsaren finns 16

4.5.4. Inaktivera SCS-gränssnittet 17

4.5.5. Visa ”Logga in i ERA-systemet” -valet i pop-up menyn 17

4.5.6. Starta Atostek ID vid datorns uppstart 17

4.5.7. Använd funktionaliteten för läsning och skrivning hos MIFARE-chippet 17

4.5.8. Aktivera personalisering för tillfälliga kort 18

4.5.9. Tillåt loggning 18

4.5.10. Ställ debug-loggning på 18
4.5.11. Kortcache-typ 18
4.5.12. Sekunders väntetid för anslutning av läsare och kort 18
4.5.13. Nya försök av automatiska inloggningar (0–5) 19
4.5.14. Minuters bufferingstid för PIN1-koden (0-420) 19
4.5.15. Tidsstämpelserverns adress 19
4.5.16. Ange inloggningskommando 19
4.5.17. Angivna öppningskommandon 20
4.5.18. Öppna nedladdningssidan för SCS-servercertifikat 20
4.5.19. Inställningsfilens parameter CLEANCERTSTOREONCARDREMOVAL 20
4.5.20. Inställningsfilens parameter EXCLUDEDREADERS 20
4.5.21. Inställningsfilens parameter EXCLUDEDCARDTYPES 21
4.5.22. Inställningsfilens parameter ERRORLOGPATH 21
4.5.23. Inställningsfilens parameter ALLOWEDBROWSERLESSANDFORWARDDOMAINS 21
4.5.24. Inställningsfilens parameter ENABLECUSTOMDIALOG 22

4.6. Uppdatering 22

4.7. Signering av dokument via applikationen 22

4.8. E-postkryptering och signering 23

4.9. Arbetsstationsinloggning 23

4.10. Hantering av MIFARE-chippet 23

4.11. Loggning och cachefilar 25
4.11.1. Loggning och loggfilar 25
4.11.2. Cachefilar 25

4.12. Felrapportering 25

4.13. Diagnostik 26

5. VANLIGA FRÅGOR OCH FELHANTERING 28

5.1. Vanliga frågor 28

5.2. Andra problem 29
5.2.1. Atostek ID PKCS11-modulen 29
5.2.2. PSCS-grässnittet är inte aktivt 29
5.2.3. Atostek ID varnar om att aktivitetsfält saknas 29
5.2.4. Säker anslutning till SCS- eller erasmartcard.ehoito.fi-grässnittet kan inte upprättas 30

1. Atostek ID programbeskrivning

Atostek Oy är ett finskt mjukvaruföretag grundat 1999 som är verksamt inom hälsovårds- och medicinska applikationer, industriproduktutveckling och IT-konsulttjänster för den offentliga sektorn. Bland Atosteks produkter finns bland annat Atostek ID-kortläsarprogramvara och Atostek ERA-systemet.

Atostek ID erbjuds som den officiella kortläsarprogramvaran av Myndigheten för digitalisering och befolkningsdata (MDB) från och med år 2024. Programvaran är avsedd att användas med certifikatkort som utfärdas av MDB. Med hjälp av programvaran kan korten användas för exempelvis elektronisk identifiering och elektronisk signering genom flera olika gränssnitt och moduler. Dessutom stöder programvaran aktivering av certifikatkort, hantering av PIN-koder och granskning av kortinformation. Utöver Atostek ID-applikationen inkluderar mjukvarupaketet Atostek ID Minidriver, Atostek ID TokenDriver, Atostek ID PKCS#11-moduler och Atostek ID AD-registreringstjänst. Atostek ID stöder också utfärdande av backup-kort från MDB. Utöver de beskrivna funktionerna erbjuder Atostek ID kompatibilitet med Atosteks ERA-system genom gränssnittet erasmartcard.ehoito.fi. Atostek ID var tidigare känt som ERA SmartCard.

Installationspaket och instruktionsdokument för Atostek ID-programvaran kan laddas ner både från MDB:s webbsidor och Atosteks egen drivrutinsnedladdningssida. MDB informerar allmänt om uppdateringar av programvaran. Atostek informerar sina kontraktskunder om uppdateringar på ett separat överenskommet sätt. I händelse av fel och problem är individer och organisationer som fått tillgång till programvaran genom MDB först i kontakt med MDB:s support (1st line support), som vid behov leder supportförfrågningar till Atostek (2nd line support). Atosteks kontraktskunder är i kontakt med Atosteks support direkt på det sätt som avtalats i kontraktet vid fel och problem. MDB och Atostek informerar vid behov om särskilda problem med programvaran.

Atostek ID-programvaran och dess användarhandböcker har genomgått en tillgänglighetsbedömning enligt WCAG 2.1 och 2.2-standarderna. Tillgänglighetsutlåtandet kan läsas på MDB:s webbsidor i samband med drivrutinsnedladdningen. Programvaran genomgår regelbunden säkerhetsrevision enligt ett separat överenskommet sätt mellan Atostek och MDB. Revisionsrapporten blir tillgänglig på MDB:s webbsidor i samband med drivrutinsnedladdningen efter revisionen. Atostek ID är också en del av den årliga revisionen av ERA-systemet. Utvecklingen av Atostek ID-programvaran styrs också av Atosteks ISO 9001-certifierade kvalitetssystem.

Garanti för funktionen av Atostek ID-kortläsarprogramvarupaketet ges inte om det finns andra liknande kortläsarprogramvaror installerade på arbetsstationen.

För ytterligare utveckling och tilläggsfunktioner av programvaran kan man kontakta Atostek direkt (Atosteks kontraktskunder) eller MDB.

2. Före användning och hur börjar man använda Atostek ID?

Det här kapitlet introducerar Atostek ID-applikationen. Dessutom förklaras kraven för att använda applikationen och instruktioner ges om hur man installerar Atostek ID-applikationen på en Linux-maskin. Atostek ID -applikationen stöder alla Debian- och Red Hat distributioner av Linux-operativsystemet som underhålls.

2.1. Vad är Atostek ID?

Atostek ID är en kortläsarprogramvara som används med certifikatkort utfärdade av MDB. Dessa kort inkluderar yrkes-, personal- och aktörskort för social- och hälsovården, organisationskort, tillfälliga kort relaterade till dessa samt medborgarcertifikatkort (identitetskort). Korten kan användas för elektronisk identifiering och elektronisk signatur i tjänster och applikationer som är kompatibla med programvaran. Dessutom stöder programvaran aktivering av certifikatkort, hantering av PIN-koder och granskning av kortinformation.

2.2. Vad behöver jag för att använda Atostek ID?

Atostek ID är kompatibelt med Linux operativsystem. Kontrollera den senaste listan över Linux-versioner som stöds på webbplatsen av Myndigheten för digitalisering och befolkningsdata https://dvv.fi/sv/kortlasarprogram eller från sidan https://downloads.ehoito.fi före installationen.

Obs! Om du använder ett Windows- eller macOS-operativsystem, se bruksanvisningen för det operativsystemet.

Obs! Det finns separata installationsinstruktioner för programvaran, där de olika stegen i installationen beskrivs i detalj.

Obs! Det finns också en separat integrationsguide tillgänglig för programvaran, som är avsedd speciellt för systemutvecklare och IT-avdelningar inom organisationer.

För att använda ett certifieringskort med Atostek ID-programvaran behöver du förutom programmet även en kortläsare och en drivrutin för kortläsaren. Drivrutinen för kortläsaren finns vanligtvis redan i operativsystemet. Om drivrutinen inte finns eller kräver uppdatering, kan du ladda ner de nödvändiga installationspaketen direkt från kortläsartillverkarens egna sidor. Atostek ID stöder kortläsare som följer PC/SC-specifikationerna.

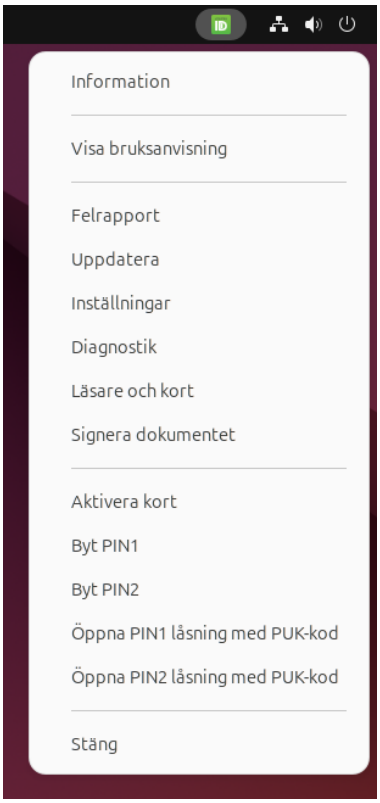
Atostek ID stöder för webbläsaranvändning versioner av Microsoft Edge, Mozilla Firefox, Apple Safari och Google Chrome som för närvarande stöds av webbläsarleverantörerna. Äldre versioner av dessa webbläsare testas inte systematiskt. Atostek ID stöder e-postapplikationerna Outlook, Apple Mail och Thunderbird när det gäller kryptering och signatur. Programvaran stöder Adobe Acrobat och PDF-XChange-programmen för att signera PDF-dokument. Atostek ID är tillgängligt på finska, svenska och engelska.

2.2.1. Installera Atostek ID

För att installera Atostek ID, följ instruktionerna nedan:

1. Gå till sidan https://dvv.fi/sv/kortlasarprogram eller https://downloads.ehoito.fi.
2. Välj drivrutinen för rätt operativsystem och ladda ner den.
3. Öppna det nedladdade installationspaketet och genomför installationen. Om nödvändigt, se hjälp från Atostek ID installationsanvisningarna.

Se instruktionerna för att starta Atostek ID-programmet i underavsnitt 3.1.



Figur 1. Atostek ID applikationsmeny.

Efter installationen kan Atostek ID-applikationen hittas i operativsystemets indikatorområde. För att se applikationsmenyn högerklicka på Atostek ID-ikonen (figur 1). Programmets logo är röd om ingen kortläsare är ansluten. Programmets logo är gul om inget kort är anslutet. Programmets logo är grön när ett kort har anslutits och dess information har lästs framgångsrikt. Logon visar också situationer där läsningen av kortinformationen är pågående eller när programmet är it ett felaktigt tillstånd.

Om du får felmeddelanden från Atostek ID-appen direkt efter installationen, kontrollera att du inte har något annat kortläsarprogram installerat samtidigt. Den tidigare kortläsarprogramvaran från MDB kan störa funktionen av Atostek ID-programvaran om de används samtidigt.

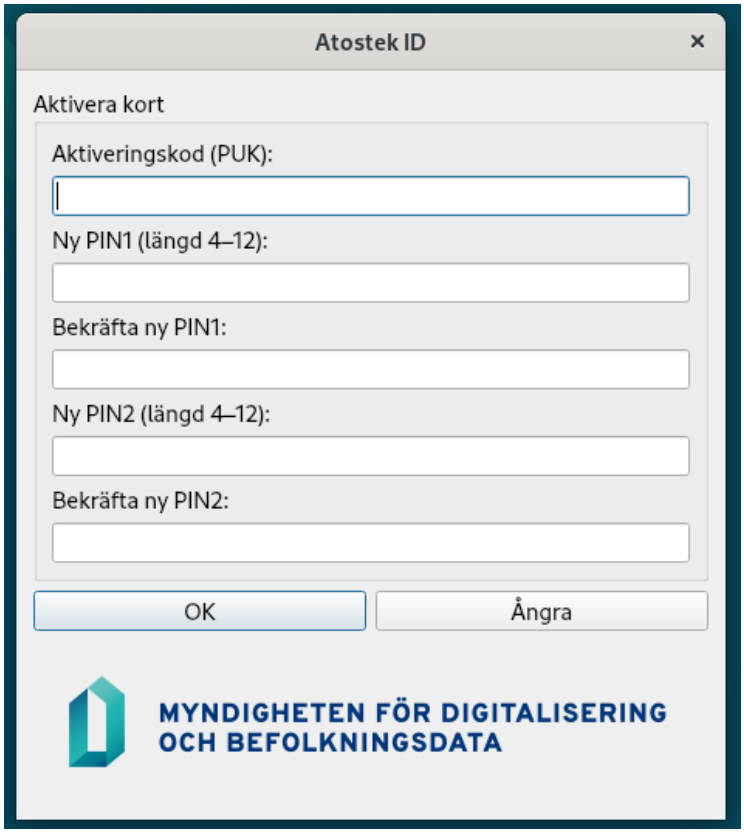
Efter detta är applikationen helt redo att användas.

2.3. Aktivera smartkortet

Aktivera smartkortet enligt följande instruktioner:

1. Anslut kortläsaren till datorn och placera kortet i kortläsaren.

2. Om kortet aldrig har aktiverats tidigare, kommer programmet automatiskt att visa ett fönster för kortaktivering. Det räcker att aktivera kortet en gång. Om fönstret för aktivering inte visas, välj *"Aktivera kort"* från menyn.
3. Ange aktiveringskoden (PUK) i det öppna fönstret (figur 2). Aktiveringskoden har skickats till dig i ett separat brev efter du beställt kortet.
4. Ange en PIN-kod för identifikationscertifikatet (PIN1) och en PIN-kod för signaturcertifikatet (PIN2). Fönstret visar de minsta och största längderna för PIN-koderna. Efter detta kan du trycka på *OK.* Om aktiveringen lyckades eller misslyckades meddelas detta i ett separat fönster.



Figur 2. Aktivering av smartkortet.

Observera att både PIN1 och PIN2 måste ställas in för att kortet ska aktiveras och bli funktionsdugligt. Minsta och största längderna för kortens PIN-koder varierar beroende på korttyp och kortgeneration, så de nödvändiga längderna kan vara olika för dina olika kort. Det är tillräckligt att aktivera kortet endast en gång. Om du har aktiverat kortet på en annan enhet eller med annan mjukvara behöver du inte aktivera kortet igen.

Observera att kortet för närvarande inte kan aktiverats med NFC-läsare, eftersom Atostek ID bara stöder användning av PIN1-koden för att etablera en säker NFC-anslutning. PIN1-koden kan inte användas för att etablera en NFC-anslutning förrän den har ställts in under aktiveringen.

Obs! Om aktiverings-PIN-koden (PUK) matas in felaktigt fem gånger i rad kommer aktiverings-PIN-koden att låsas. Därefter kan kortet inte aktiveras längre eller låsta PIN-koder låsas upp. Redan inställda PIN-koder och därmed signaturfunktionen kommer att fungera även om aktiverings-PIN-koden senare låses. Aktiverings-PIN-koden kan inte låsas upp, och för att få en fungerande aktiverings-PIN-kod krävs det att ett nytt kort

beställs. Programmet varnar varje gång en aktiverings-PIN-kod har matats in felaktigt och meddelar hur många försök som återstår innan koden låses.

Obs! Nyare medborgarcertifikatkort använder en ny aktiveringskod (PIN) med 7 siffror för kortaktivering. Aktiveringskoden skiljer sig från den separata avblockeringskoden (PUK) med 8 siffror, som kan användas för att aktivera kortet om aktiveringskoden har låsts. **Var uppmärksam på vilken kod Atostek ID efterfrågar vid aktiveringen av kortet.** Avblockeringskoden kan också användas för att låsa upp PIN1- och PIN2-koderna om de har blivit blockerade efter för många felaktiga försök. Du kan få upplåsningskoden via dina lokala myndigheter. Se Myndigheten för digitalisering och befolkningsdatas webbplats för den senaste informationen.

3. Elektronisk autentisering och elektronisk signatur

I detta kapitel beskrivs hur du kan identifiera dig med ditt certifieringskort genom att använda Atostek ID-applikationen i en tjänst som är kompatibel med Atostek ID-programvaran. Detta kapitel beskriver också hur du utför en elektronisk signatur med hjälp av Atostek ID-applikationen. Se till att också bekanta dig med användarhandboken för den tjänst eller applikation där du identifierar dig eller utför en signatur, om det behövs.

I detta kapitel beskrivs mer detaljerat några av de vanligaste användningsfallen för autentisering och signering. Inte alla möjliga tjänster har beskrivits i denna handledning, och inte alla användningsfall som beskrivs här gäller för alla användare. Detta kapitel beskriver endast funktionaliteten för identifiering och signering. I nästa kapitel beskrivs programvarans övriga funktioner mer i detalj.

3.1. Elektronisk autentisering

Användaren kan elektroniskt autentisera sig med sitt certifieringskorts autentiseringscertifikat till en tjänst som är kompatibel med Atostek ID-programvaran. Vid autentisering måste användaren mata in sin PIN1-kod för kortet.

För att autentisera dig, placera kortet i kortläsaren och anslut kortläsaren till datorn, kontrollera att Atostek ID-programmet är i gång (figur 1) och starta inloggningen till den faktiska tjänsten. Tjänsteleverantören ger detaljerade instruktioner för inloggningen. Tjänsten anropar Atostek ID-programvaran, varefter Atostek ID begär PIN1-koden (figur 3). När PIN-koden efterfrågas kan även macOS egna PIN-kodsfönster visas (utan Atostek och MDB-logotyper). PIN-kodsfönstren kan skilja sig något åt beroende på vilket gränssnitt som används för autentisering. Om ett certifikatkort håller på att löpa ut inom två månader kommer Atostek ID att meddela detta i samband med autentiseringen.

Figur 3. Autentisering av användaren med PIN1-kod. Vid autentisering kan även operativsystemets egna PIN-kodfönster visas

3.1.1. mTLS-autentisering

Autentisering kan utföras med kortets autentiseringscertifikat via mutual TLS (mTLS) i webbläsaren. Då utnyttjas Atostek ID PKCS#11-modulen, som installeras automatiskt i samband med installationen av Atostek ID Linux-versionen. Mer detaljerad information om Atostek ID PKCS#11-modulen finns i Atostek ID-programvarans integrationsguide.

Denna typ av autentisering används till exempel i samband med offentliga förvaltningens e-tjänster (**suomi.fi-autentisering**). För att autentisera dig till en tjänst, anslut kortläsaren till datorn, sätt in kortet i läsaren och starta autentiseringen i webbläsaren. Du kommer att bli ombedd att ange PIN-koden för kortets autentiseringscertifikat, det vill säga kortets PIN1-kod. Därefter är autentiseringen klar och du kommer att omdirigeras till tjänsten. Vid problem, se först kapitel 5 i denna handledning, där lösningar på vanliga problem beskrivs.

3.1.2. Autentisering via SCS-gränssnittet

Autentisering kan också utföras till exempel genom att använda Atostek ID-applikationens SCS-gränssnitt (Signature Creation Service). SCS är ett HTTPS-gränssnitt definierat av MDB. Det används alltså särskilt för autentisering i webbtjänster. SCS-gränssnittet används bland annat av många patientinformationssystem.

Användningen av SCS-gränssnittet är inte särskilt synlig för användaren när applikationen används. För att autentisera dig behöver du koppla kortläsaren till datorn och sätta in kortet i läsaren. Därefter kan du påbörja autentiseringen i systemet. Efter detta kommer Atostek ID att be dig välja det certifikat som ska användas för autentisering. När certifikatet är valt kommer du att bli ombedd att ange den motsvarande PIN-koden. Efter detta är autentiseringen klar och du kommer att omdirigeras till tjänsten.

3.1.3. Användning av Atostek ERA -systemet

Observera att detta användningsfall endast är avsett för de användare inom social- och hälsovården som är registrerade för att använda ERA-systemet. Om din organisation inte har instruerat dig att använda Atosteks ERA-system eller om du är en medborgaranvändare (använder ett identitetskort), gäller inte detta användningsfall för dig. I dessa fall kan du välja att inte läsa denna del av instruktionerna. Du bör inte logga in i ERA-systemet om du inte har fått särskilda instruktioner att göra så.

Du kan logga in, det vill säga autentisera dig, i Atosteks ERA-system med hjälp av Atostek ID-applikationen. Navigera i webbläsaren till ERA-systemets inloggningssida eller öppna från Atostek ID-applikationens meny *"Logga in i ERA-systemet"*, varpå inloggningssidan öppnas i standardwebbläsaren. Observera att funktionen endast visas i applikationens meny om inställningen *"Visa 'Logga in i ERA-systemet'-valet i pop-up-menyn"* har aktiverats på inställningarna eller under installationen. Med den här funktionen kan du enkelt logga in på ERA-systemet även när Atostek ID inte kan ansluta till standardportarna, eftersom funktionen öppnar inloggningssidan med Atostek ID-applikationens portinformation. En sådan situation kan uppstå till exempel när flera användare är inloggade på samma dator samtidigt.

För att autentiseringen i ERA-systemet ska lyckas måste du först ha konfigurerats i systemet. När du autentiserar dig måste kortläsaren vara ansluten till datorn och kortet måste vara i läsaren. När autentiseringen har startat kommer Atostek ID att be om din PIN1-kod för kortet. Om autentiseringen lyckas kommer du att omdirigeras till tjänsten.

ERA-systemet använder Atostek ID-applikationens erasmartcard.ehoito.fi-gränssnitt. Du kan testa gränssnittets funktionalitet genom att öppna *"Diagnostik"* från applikationens meny och därefter *"Öppna Atostek IDs testsida"*. Detta öppnar gränssnittets testsida i standardwebbläsaren, där det står *"Test page loaded OK"*.

3.2. Elektronisk signatur

Användaren kan utföra en elektronisk signatur med sitt certifieringskorts signaturcertifikat i en tjänst eller applikation som är kompatibel med Atostek ID-programvaran. Vid signering måste användaren mata in sin PIN2-kod för kortet.

För att signera, placera kortet i kortläsaren och anslut kortläsaren till datorn samt kontrollera att Atostek ID-programmet är i gång (figur 1). Bekanta dig vid behov med tjänste- eller applikationsleverantörens instruktioner för hur den elektroniska signaturen utförs i den aktuella tjänsten eller applikationen. Vid signering anropar tjänsten eller applikationen Atostek ID-programvaran, varefter Atostek ID begär PIN2-koden (figur 4). När PIN-koden efterfrågas kan även operativsystemets egna PIN-kodsfönster visas (utan Atostek och MDB-logotyper). PIN-kodsfönstren kan skilja sig något åt beroende på vilket gränssnitt som används för signeringen.

Figur 4. Elektronisk signatur med PIN2-kod. Vid signering kan även operativsystemets egna PIN-kodfönster visas.

3.2.1. Signering via SCS-gränssnittet

Signering kan också utföras till exempel genom att använda Atostek ID-applikationens SCS-gränssnitt (Signature Creation Service). SCS är ett HTTPS-gränssnitt definierat av MDB. Det används alltså särskilt för signaturer som görs i webbtjänster. SCS-gränssnittet används bland annat av många patientinformationssystem.

Användningen av SCS-gränssnittet är inte särskilt synlig för användaren när applikationen används. För att signera behöver du koppla kortläsaren till datorn och sätta in kortet i läsaren. Därefter kan du påbörja signeringen. Efter detta kommer Atostek ID att be dig välja det certifikat som ska användas för autentiseringen. När certifikatet är valt kommer du att bli ombedd att ange den motsvarande PIN-koden. Efter detta är signeringen klar och överförs från applikationen till den tjänst som begärt den.

3.2.2. Signering i Atostek ERA-systemet

Observera att detta användningsfall endast är avsett för de användare inom social- och hälsovården som är registrerade för att använda ERA-systemet. Om din organisation inte har instruerat dig att använda Atosteks ERA-system eller om du är en medborgaranvändare (använder ett identitetskort), gäller inte detta användningsfall för dig. I dessa fall kan du välja att inte läsa denna del av instruktionerna. Du bör inte logga in i ERA-systemet om du inte har fått särskilda instruktioner att göra så.

Du kan utföra en signering, till exempel en receptsignering, i Atosteks ERA-system med Atostek ID-applikationen efter att du först har autentiserat dig i systemet. När du ska signera måste kortläsaren vara ansluten till datorn och kortet vara i läsaren. När signeringen påbörjas kommer Atostek ID att fråga efter din PIN2-kod för kortet. Därefter utför kortet signeringen och returnerar den till ERA-systemet.

ERA-systemet använder Atostek ID-applikationens erasmartcard.ehoito.fi-gränssnitt. Du kan testa gränssnittets funktionalitet genom att öppna *"Diagnostik"* från applikationens meny och sedan *"Öppna Atostek IDs testsida"*. Detta öppnar testgränssnittets testsida i standardwebbläsaren, där det står *"Test page loaded OK"*.

4. Funktionalitet

I det här kapitlet presenteras de mest väsentliga funktionerna i Atostek ID-applikationen. Dessa inkluderar till exempel byte av PIN-koder och upplåsning av dem. Dessutom presenteras inställningarna relaterade till applikationen och hur man ändrar dem.

4.1. Start och stängning

Atostek ID-programmet startar inte automatiskt, utan det måste startas från kommandoraden genom att skriva dess namn:

```
$ atostekid
```

Programmet fortsätter att köras i terminalen och skriver ut logginformation, som du inte behöver bry dig om.

Atostek ID-programmet startar automatiskt när du har installerat applikationen och loggar in på operativsystemet. Du kan vid behov inaktivera den automatiska starten via programmets inställningar.

När du vill stänga programmet, välj *”Stäng”* från menyn. Detta kommer att helt stänga Atostek ID-applikationen. Detta är vanligtvis inte nödvändigt. Observera att det inte längre är möjligt att autentisera sig till tjänster eller genomföra signaturer via till exempel SCS-gränssnittet eller erasmartcard.ehoito.fi-gränssnittet innan programmet har startats om. Programmet finns i startmenyn under namnet *”Atostek ID”* och kan vid behov startas om därifrån

4.2. Applikationsinformation och bruksanvisning

Information om Atostek ID-applikationen, såsom versionsnummer och de portar som används av HTTPS-servrar, kan läsas i applikationens Information-vy. Den kan öppnas genom att välja *"Information"* från applikationens meny. I fönstrets övre del visas applikationens versionsnummer. Öppna och stängda portar samt information relaterad till certifikatet avser erasmartcard.ehoito.fi-gränssnittet. Dessutom informerar vyn om en anslutning kan upprättas till SCS-gränssnittets port 53952. Anslutning är inte möjlig om något annat program använder porten. Detta kan inträffa till exempel när datorn har DigiSign-kortläsarprogramvaran installerad och i gång, vilket öppnar sin egen motsvarande tjänst på den porten. Problem med SCS-gränssnittets port syns också i Atostek ID-applikationens logotyp som ett utropstecken i en triangel.

Bruksanvisningen för applikationen kan öppnas genom applikationen genom att välja *"Visa bruksanvisning"* från menyn. Bruksanvisningen öppnas på applikationens språk (finska, svenska eller engelska). Programvarans bruksanvisningar, installationsinstruktioner och andra dokument är också tillgängliga för nedladdning från både MDB:s webbsida för kortläsarprogramvara och Atosteks egen drivrutinssida.

4.3. Byte av PIN-koder och upplåsning av låsta koder

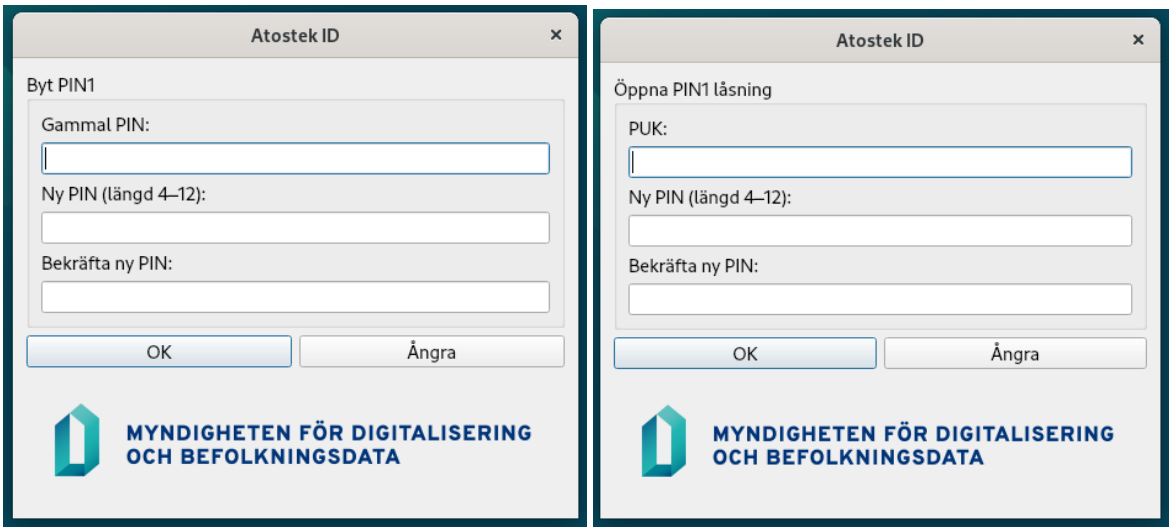
Du kan byta PIN-koder genom att välja *"Byt PIN1"* eller *"Byt PIN2"* från applikationsmenyn och ange den nuvarande PIN-koden och den nya PIN-koden två gånger (figur 5).

Du kan låsa upp låsta PIN-koder genom att välja *"Öppna PIN1 låsning med PUK-kod"* eller *"Öppna PIN2 låsning med PUK-kod"* från applikationsmenyn och ange PUK-koden och den nya PIN-koden två gånger (figur 6). PUK-koden, eller aktiveringskoden, medföljer certifikatkortet.

Korten kan också aktiveras via menys val *"Aktivera kort"*. Applikationen uppmanar användaren att aktivera kortet när ett inaktivt kort sätts i läsaren, så att användaren inte behöver starta aktiveringen själv via menyn.

Obs! Under hanteringen av PIN-koderna måste certifikatkortet vara i kortläsaren. Både PIN1- och PIN2-koderna måste låsas upp för att kortet ska aktiveras och bli funktionsdugligt. Även kortets aktivering låser upp båda koderna.

Obs! Om aktiveringskoden matas in felaktigt fem gånger i rad kommer aktiveringskoden att låsas. Därefter kan kortet inte längre aktiveras eller låsta PIN-koder låsas upp. Redan inställda PIN-koder fungerar trots att aktiveringskoden senare låses. Aktiveringskoden kan inte låsas upp, och för att få en fungerande aktiveringskod krävs det att ett nytt kort beställs. Programmet varnar varje gång en aktiveringskod har matats in felaktigt och meddelar hur många försök som återstår innan koden låses.

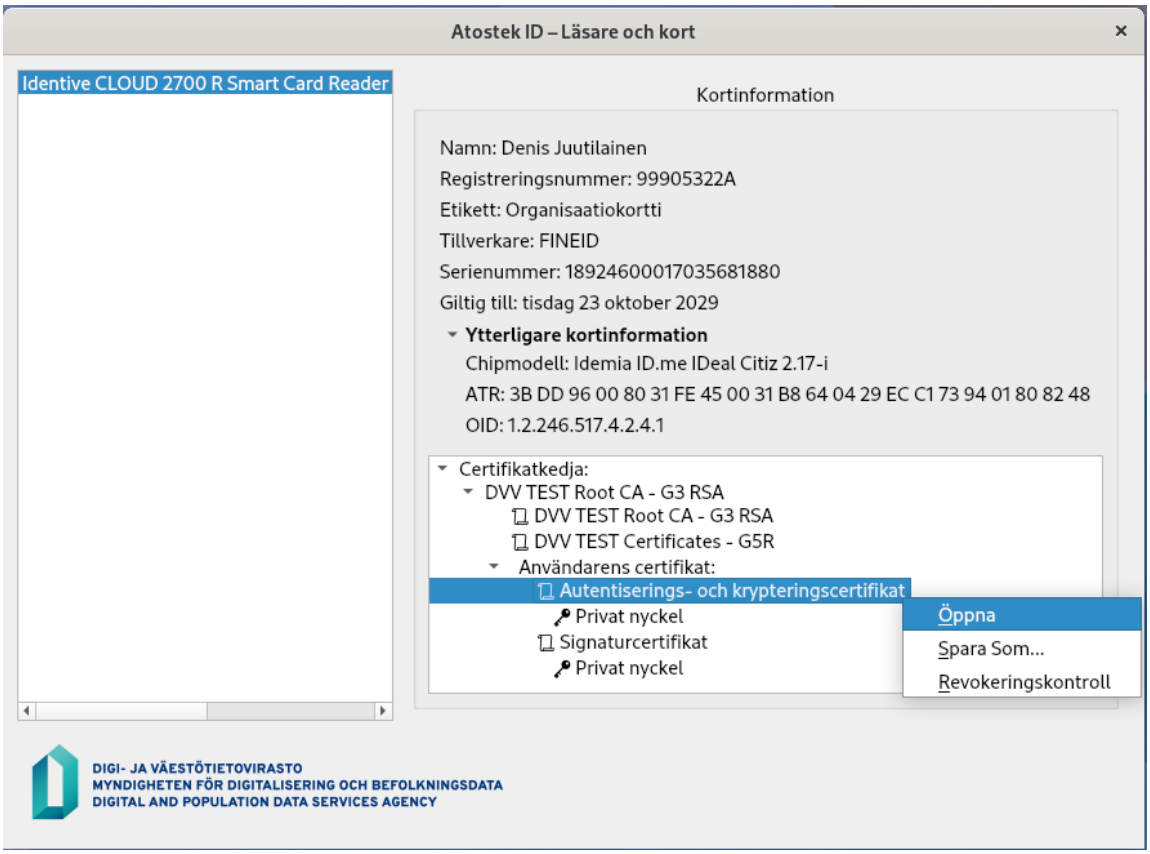


Figurer 5 och 6. Byt och låsa upp PIN1-kodet

4.4. Läsare och kort

Du kan granska de kortläsare och kort som är anslutna till datorn genom att öppna *"Läsare och kort"* från applikationens meny. I det fönster som öppnas (se figur 7) visas de anslutna kortläsarna listade under varandra på vänster sida. I listan över NFC-läsare visas två olika läsare om läsaren har både en NFC- och en vanlig USB-läsare (kontaktbaserad läsare) separat. Du kan välja en läsare som aktiv genom att klicka på dess namn i listningen på fönstrets vänstra sida.

När en läsare är vald visas uppgifter om det kort som är anslutet till kortläsaren på höger sida av fönstret, exempelvis namnuppgifter och giltighetsdatum. I fönstret visas även kortets certifikatkedja i ett trädformat, från rotcertifikatet genom mellancertifikaten till användarens certifikat. Relaterat till användarens certifikat visas både den offentliga delen av certifikatet och den tillhörande privata nyckeln. De offentliga delarna av certifikaten kan öppnas eller sparas genom att högerklicka på certifikatet i vyn. Då öppnas en extrameny med alternativen "Öppna" och "Spara som…". Dessutom kan man kontrollera certifikatens giltighet genom att välja "Revokeringskontroll". Det kontrollerar certifikatets giltighetsdatum och spärrlistor (CRL, OCSP).

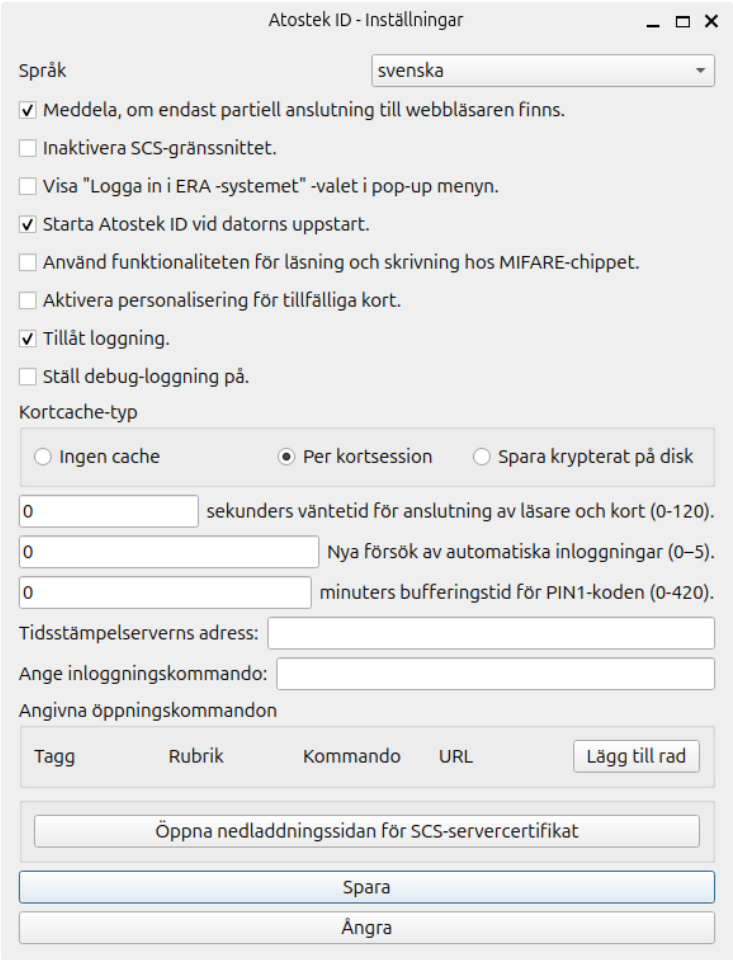


Figur 7. Läsare och kort -vyn.

När en NFC-läsare används frågas användaren efter kortets PIN1-kod när kortet förs till läsaren. PIN-koden används för att etablera en säker NFC-anslutning. Om kortet tas bort från NFC-läsaren har användaren 10 sekunder på sig att föra tillbaka kortet innan PIN1-koden måste matas in igen för att återupprätta anslutningen.

4.5. Inställningar

Du kan redigera applikationsinställningarna genom att välja *"Inställningar"* från applikationsmenyn. Med inställningarna (figur 8) kan du till exempel ändra applikationsspråk och ändra de visade meddelanden och kommandon relaterade till programmet. Observera att ändringarna träder i kraft först efter att de har sparats.



Figur 8. Applikationsinställningar.

4.5.1. Språk

"Språk" låter dig ändra språket för Atostek ID-applikationen. De språk som för närvarande stöds är finska, svenska och engelska.

4.5.2. Meddela om nya uppdateringar

"**Meddela om nya uppdateringar**" kan användas för att aktivera Atostek ID-aviseringar om nya tillgängliga versioner. Då kommer Atostek ID att skicka ett separat meddelande om att en ny version finns tillgänglig för nedladdning och installation.

4.5.3. Meddela om endast partiell anslutning till webbläsaren finns

"**Meddela, om endast partiell anslutning till webbläsaren finns**" kan användas för att aktivera Atostek ID-aviseringar om en partiell anslutning när Atostek ID inte kan ansluta till standardportar och systemet som används måste öppnas med Atostek ID-startkommandon. Denna inställning gäller endast användningen av erasmartcard.ehoito.fi-gränssnittet.

4.5.4. Inaktivera SCS-gränssnittet

"Inaktivera SCS-gränssnittet"-inställningen gör det möjligt att aktivera eller inaktivera produktens SCS-gränssnitt. Gränssnittet är aktiverat som standard, vilket innebär att applikationen startar det och den tillhörande tjänsten för nedladdning av CA-certifikat vid uppstart. Detta HTTPS-gränssnitt kräver en port enligt specifikationen (https://dvv.fi/sv/fineid-specifikationer), vilken kan vara upptagen till exempel av annan kortläsarprogramvara om den implementerar samma gränssnitt. Med denna inställning kan SCS-gränssnittet inaktiveras om man vill frigöra den port det reserverar för en annan applikation och inte vill använda SCS-gränssnittet via Atostek ID. Att inaktivera gränssnittet innebär att Atostek ID inte startar gränssnittet alls, och därmed till exempel inte varnar om något annat program använder portarna som gränssnittet behöver. Observera att inaktivering av gränssnittet utan ersättande åtgärder förhindrar autentiseringar och signeringar i system som använder gränssnittet via Atostek ID. Inaktivera därför gränssnittet endast om du är säker på att du inte behöver det i ditt användningsfall. Se vid behov även inställningen MULTIDESKTOPMODE.

4.5.5. Visa ”Logga in i ERA-systemet” -valet i pop-up menyn

"Visa ’Logga in i ERA -systemet’ -valet i pop-up menyn"-inställningen kan användas för att visa eller dölja ERA-inloggningslänken från applikationsmenyn. Observera att användningen av ERA-systemet endast gäller för de användare inom social- och hälsovården som har konfigurerats för att använda ERA-systemet. Som standard är inställningen inaktiverad, vilket innebär att inloggningslänken inte visas i menyn.

4.5.6. Starta Atostek ID vid datorns uppstart

”Starta Atostek ID vid datorns uppstart”-inställningen kan användas för att stänga av eller aktivera programmets automatiska uppstart. Inställningen kräver administratörsrättigheter, som efterfrågas av användaren efter att inställningen har sparats. Applikationen stängs av under tiden för ändringen av inställningen och startar sedan automatiskt om igen.

4.5.7. Använd funktionaliteten för läsning och skrivning hos MIFARE-chippet

”Använd funktionaliteten för läsning och skrivning hos MIFARE-chippet”-inställningen gör valet "Mifare" synligt i programmets meny, vilket öppnar en separat hanteringsvy för MIFARE-chippet. Vänligen sätt dig in i instruktionerna för att läsa och skriva MIFARE-chip innan du försöker utföra läsning eller skrivning. Du behöver en NFC-läsare för att hantera chippet.

4.5.8. Aktivera personalisering för tillfälliga kort

”Aktivera personalisering för tillfälliga kort”-inställningen gör valet ”Tillfälligt kort” synligt i programmets meny, vilket öppnar en separat dialogruta för personalisering av tillfälliga kort. Denna dialog används endast av personal vid registreringsställen och behövs inte av andra användare för att använda sitt personaliserade tillfälliga kort. Övriga inställningar avsedda för registreringsställen, såsom AIDISURL, är redan som standard lämpliga för personalisering av tillfälliga kort, men de kan ändras vid behov. Mer information om personalisering av tillfälliga kort finns i Vartti-systemets anvisningar.

Om systemet har konfigurerats med en tidsgräns för anslutningar till smartkort bör man säkerställa att den är tillräckligt lång. I samband med personalisering kan det ta lång tid för kortet att generera nya nycklar, och anslutningen får då inte avbrytas. En tidsgräns på minst 2 minuter rekommenderas för att säkerställa att personalisering kan slutföras utan problem.

4.5.9. Tillåt loggning

”Tillåt loggning”-inställningen kan användas för att stängas av applikationens loggning helt. Att inaktivera loggningen tar inte bort tidigare loggar utan förhindrar bara registrering av nya loggmeddelanden.

4.5.10. Ställ debug-loggning på

”**Ställ debug-loggning på**” låter dig välja om loggmeddelanden på DEBUG-nivå loggas i felloggen eller enbart INFO-, WARNING- och ERROR-nivåmeddelanden.

4.5.11. Kortcache-typ

”**Kortcache-typ**” låter dig ange om Atostek ID ska lagra filer lästa från kortet i en cache. Det finns tre alternativ för kortcachen: "Ingen cache", "Per kortsession" och "Spara krypterat på disk". Med alternativet "Ingen cache" sparar Atostek ID inte filer lästa från kortet i en separat cache, utan filerna läses alltid direkt från kortet när deras innehåll behövs. Alternativet "Per kortsession" är valt som standard, och då bevaras de från kortet lästa filerna i Atostek ID:s interna cache så länge kortet sitter i läsaren. Data som sparats från kortet tas bort från cachen när kortet tas ur läsaren eller när Atostek ID stängs av. Med alternativet "Spara krypterat på disk" kvarstår kortcachen krypterad i användarens mapp. Kortcachen töms alltså inte även om kortet tas ur läsaren eller Atostek ID stängs av. Om inställningen ändras från detta värde till något annat tas den kortcache som lagrats på disken bort.

Användning av kortcachen förbättrar Atostek ID:s prestanda eftersom den minskar den tidskrävande kortkommunikationen. Störst effekt vid långvarig användning uppnås när kortcachen sparas krypterad på disk.

4.5.12. Sekunders väntetid för anslutning av läsare och kort

”**Sekunders väntetid för anslutning av läsare och kort**” låter dig ange antalet sekunder under vilka en oansluten läsare eller kort ska anslutas efter att inloggningen har startat genom erasmartcard.ehoito.fi-gränssnittet. När värdet är satt till 0 misslyckas inloggningen omedelbart om läsaren eller kortet saknas. Maximalt värde för inställningen är 120 sekunder. Denna inställning gäller endast användningen av erasmartcard.ehoito.fi-gränssnittet.

4.5.13. Nya försök av automatiska inloggningar (0–5)

"**Nya försök av automatiska inloggningar (0–5)"** låter dig definiera hur många gånger inloggningen ska göras om automatiskt om inloggningen via erasmartcard.ehoito.fi-gränssnittet misslyckas på grund av Alcor Micro-läsaren. När värdet är satt till 0, frågas varje nytt försök separat (dock inte mer än tre gånger totalt). Denna inställning gäller endast användningen av erasmartcard.ehoito.fi-gränssnittet.

4.5.14. Minuters bufferingstid för PIN1-koden (0-420)

"**Minuters bufferingstid för PIN1-koden (0-420)**" låter dig ange hur länge Atostek ID ska behålla kortets PIN1-kod i minnet. Värdet anges i minuter i intervallet 0-420, det vill säga PIN1-koden sparas i minnet högst sju (7) timmar. Standardvärdet är 0 minuter, vilket innebär att PIN1-koden efterfrågas av användaren varje gång den behövs. När PIN1-koden finns i minnet efterfrågar Atostek ID den inte av användaren utan använder det sparade värdet direkt. PIN1-koden tas bort ur minnet när den angivna tiden överskrids, kortet tas ur kortläsaren, kortet upptäcker en felaktig PIN1-kod, PIN1-koden ändras eller Atostek ID stängs av. Bufferingstiden påbörjas från det ögonblicket då den angivna PIN1-koden framgångsrikt verifierats på kortet.

Obs! Aktivering av PIN1-kodens buffering är ett beslut som användaren eller organisationen själv fattar, och bufferingstiden bör anges så kort som möjligt inom de ramar som användningsfallen tillåter. Tänk också på PIN1-kodbufferings säkerhetsaspekterna vid beslutet.

Obs! Inställningen fungerar med Atostek ID:s externa moduler (PKCS#11) endast om inställningen *ENABLECUSTOMDIALOG* är sann.

4.5.15. Tidsstämpelserverns adress

”Tidsstämpleserverns adress”-fältet kan används för att definiera en tidstämpeltjänst som används för att hämta tidstämplar vid högre nivåer av signering (till exempel när man signerar PDF-dokument genom applikationen enligt PAdES-standardens nivåer B-T, B-LT, B-LTA). Adressen till tidstämpelstjänsten anges i sin helhet i fältet, till exempel https://tidstämpelserver.se/ts. Observera att den tidstämpelstjänsten som anges som exempel inte är en verklig tidstämpelstjänst. Använd i stället en tidstämpelstjänst som din organisation har instruerat dig att använda.

4.5.16. Ange inloggningskommando

"**Ange inloggningskommando:"** kan användas för att definiera en webbläsare som du vill öppna i stället för standardwebbläsaren när ett startkommando utan separat definierat kommando körs. Webbläsaren definieras som: *"Sökväg till webbläsarens applikation” {URL}*, till exempel *"/usr/bin/firefox” {URL}*

4.5.17. Angivna öppningskommandon

"**Angivna öppningskommandon**" kan användas för att lägga till nya startlänkar till Atostek ID-menyn som kan användas för att öppna ett system som använder Atostek ID och förmedlar portinformationen för applikationen. Detta är särskilt viktigt i Citrix- och RDP-miljöer. Obligatoriska fält definieras enligt följande:

Kommandots identifierare (Tagg) är det värde med vilket startkommandot kan användas, till exempel vid en kommandoradsstart.

"**Rubrik**" används för att definiera texten som visas i applikationsmenyn.

"**Kommando**" används för att definiera webbläsaren som du vill öppna med kommandot. Formatet är detsamma som i kommandot anpassad inloggning.

"**URL**" innehåller måladressen. Porten för Atostek ID kan anges med {PORT} inbäddning. Vid lanseringen ersätter Atostek ID texten {PORT} med den faktiska porten som Atostek ID är ansluten till.

Exempel av ett öppningskommando:

- "Tagg": edemo
- "Rubrik": Logga in på edemo-tjänsten
- "Kommando": "/Applications/Google Chrome.app/Contents/MacOS/Google Chrome " {URL}
- "URL": https://edemo.atostek.com/

4.5.18. Öppna nedladdningssidan för SCS-servercertifikat

”Öppna nedladdningssidan för SCS-servercertifikat” låter dig öppna sidan för SCS-gränssnittet där du kan ladda ner CA-certifikatet. Sidan innehåller också instruktioner om hur du manuellt ställer in certifikatet som tillförlitligt i Firefox. Denna inställning gäller endast användingen av SCS-gränssnittet.

4.5.19. Inställningsfilens parameter CLEANCERTSTOREONCARDREMOVAL

Du kan använda inställningsparametern *"CLEANCERTSTOREONCARDREMOVAL"* direkt i applikationens inställningsfil (*"/home/<användare>/.local/share/Atostek Oy/Atostek ID/AtostekID.ini"*). Inställningens standardvärde *"true"* tömmer användarens kortcertifikat från Windows certifikatlagring när kortet tas bort från läsaren. Värdet *"false"* behåller certifikaten i lagringen. Observera att inställningsfilen måste sparas och Atostek ID måste startas om efter ändringarna för att inställningen ska träda i kraft.

4.5.20. Inställningsfilens parameter EXCLUDEDREADERS

Du kan använda inställningsparametern *”EXCLUDEDREADERS”* direkt i applikationens inställningsfil ("/home/<användare>/.local/share/Atostek Oy/Atostek ID/AtostekID.ini"). Ange som en sträng en lista över läsare (Läsare1, Läsare2, Läsare3) som du vill inaktivera. Då kommer Atostek ID inte att registrera kort i dessa läsare. Om det i vyn "Läsare och kort" visas extra siffror i slutet av läsarens namn, uteslut dessa siffror när du konfigurerar inställningen. Om till exempel läsarens namn visas som "Windows Hello for Business 0", använd strängen "Windows Hello for Business" i inställningen. Inställningen stöder jokertecken * (ersätter ett eller flera tecken) och ? (ersätter ett tecken). Till exempel döljer värdet ExcludedReaders=ACS* alla läsare vars namn börjar med strängen ”ACS”. Observera att inställningsfilen måste sparas och Atostek ID måste startas om efter ändringarna för att inställningen ska träda i kraft.

4.5.21. Inställningsfilens parameter EXCLUDEDCARDTYPES

Du kan använda inställningsparametern "EXCLUDEDCARDTYPES" direkt i applikationens inställningsfil (*"/home/<användare>/.local/share/Atostek Oy/Atostek ID/AtostekID.ini"*). Ange en stränglista med korttyper som du vill avvisa. Tillåtna typer är ORGANISATIONSKORT, YRKESKORT, PERSONALKORT, IDENTITETSKORT, AKTORSKORT och FINEID (tillfälliga kort). Värdena är skiftlägesokänsliga. Observera att inställningsfilen måste sparas och Atostek ID måste startas om efter ändringarna för att inställningen ska träda i kraft.

4.5.22. Inställningsfilens parameter ERRORLOGPATH

Du kan använda inställningsparametern *"ERRORLOGPATH"* direkt i applikationens inställningsfil (*"/home/<användare>/.local/share/Atostek Oy/Atostek ID/AtostekID.ini"*). Ange sökvägen dit applikationens loggfil ska skrivas. Sökvägen kan vara exempelvis *"ErrorLogPath=/home/<användare>/log/AID.log"*. Om sökvägen är felaktig eller inte existerar kommer applikationen att fortsätta skriva loggar till standardplatsen. Observera att inställningsfilen måste sparas och Atostek ID måste startas om efter ändringarna för att inställningen ska träda i kraft.

4.5.23. Inställningsfilens parameter ALLOWEDBROWSERLESSANDFORWARDDOMAINS

Du kan använda inställningsparametern *"ALLOWEDBROWSERLESSANDFORWARDDOMAINS"* direkt i applikationens inställningsfil (*"/home/<användare>/.local/share/Atostek Oy/Atostek ID/AtostekID.ini"*). Inställningsparametern *"ALLOWEDBROWSERLESSANDFORWARDDOMAINS"* används i samband med användningen av gränssnittet erasmartcard.ehoito.fi när inloggning utan webbläsare, signering utan webbläsare eller en /ForwardMessage-begäran görs till andra destinationer än Atosteks ERA- eller Atosteks Edemo-system. Systemen era.ehoito.fi och edemo.atostek.com är automatiskt tillåtna externa adresser i dessa förfrågningar. Om du vill lägga till tillåtna adresser för produktions- eller teständamål, ange de tillåtna adresserna i parametern, till exempel *"AllowedBrowserlessAndForwardDomains=era.ehoito.fi, edemo.atostek.com, edemo5.atostek.com"*. Observera att inställningsfilen måste sparas och Atostek ID måste startas om efter ändringarna för att inställningen ska träda i kraft.

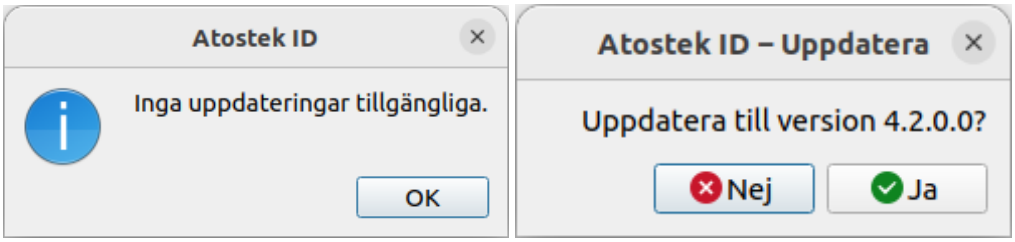
4.5.24. Inställningsfilens parameter ENABLECUSTOMDIALOG

Du kan använda inställningsparametern ”ENABLECUSTOMDIALOG” direkt i applikationens konfigurationsfil *(”/home/<användare>/.local/share/Atostek Oy/Atostek ID/AtostekID.ini”)*. Vid standardvärdet ”true” visar Atostek ID:s externa moduler Atostek ID:s PIN-kodsfönster för användaren när PIN-koden efterfrågas. Undantaget är säkerhetsrelaterade begräsningar där operativsystemet hanterar PIN-kodsförfrågan, till exempel vid inloggning på en arbetsstation. Om inställningen är ”false” frågas PIN-koden i operativsystemets frågedialog.

4.6. Uppdatering

Du kan uppdatera Atostek ID genom att välja *"Uppdatera"* från applikationsmenyn. Atostek ID söker först efter uppdateringar och visar sedan uppdateringsstatus (figurer 9 och 10). Om det finns uppdateringar och du vill uppdatera programmet till den senaste versionen, välj "*Ja"* i fönstret som visas i figur 10. Programmet kommer att ladda ner och installera den senaste versionen.

Notera! Uppdatering av applikationen kräver administratörsrättigheter och denna funktion kan därför döljas under installationsfasen.

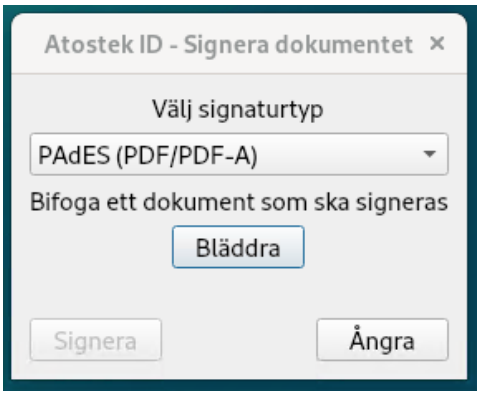


Figur 9 och 10. Status för uppdateringar när det inte finns några uppdateringar tillgängliga och när det finns uppdateringar tillgängliga.

4.7. Signering av dokument via applikationen

PDF- och PDFA-dokument kan signeras inte bara med Adobe Acrobat och PDF-XChange utan också direkt genom Atostek ID-applikationen. Signeringen är då i enlighet med PAdES-standarden. Signeringsnivån (B-B, B-T, B-LT, B-LTA) är den högsta möjliga som applikationen kan generera. Detta beror exempelvis på om en adress till en tidstämpeltjänst har konfigurerats för applikationen via inställningarna. Utöver PAdES-standarden stödjer applikationen även CAdES (B-B), JAdES (B-B), XAdES (B-B) och ASiC-E (B-B, B-T, B-LT) format för fristående signaturer (detached signatures) för andra dokumenttyper.

För att skapa en signatur, öppna "Signera dokument" från applikationens meny. Välj därefter signeringstyp i det fönster som öppnas (bild 13) och hämta dokumentet som ska signeras från din dator.



Figur 11. Dokumentsignering via Atostek ID -programsvaran.

När signeringen påbörjas frågas användaren först efter det certifikat som ska användas för signeringen. När certifikatet har valts efterfrågas användarens PIN-kod som motsvarar certifikatet. Efter att koden har matats in utför kortet signeringen och signeringen kopplas till en kopia av det ursprungliga dokumentet, vars namn kompletteras med texten *"_signed"*. Applikationen meddelar slutligen om signeringen lyckades eller inte

4.8. E-postkryptering och signering

I flera e-postprogram kan e-postmeddelanden krypteras och signeras med hjälp av certifikat från en autentiseringskort. På Linux utnyttjas då Atostek ID:s PKCS#11-modul, som installeras automatiskt i samband med installationen av Atostek ID Linux-versioner. Mer detaljerad information om Atostek ID PKCS#11-modulen finns i integrationsguiden för Atostek ID-programvaran. Vänligen konsultera e-postprogrammens egen dokumentation om e-postkryptering och signering vid behov.

Autentiseringskortet måste aktiveras i e-postprogrammet innan e-postmeddelanden kan krypteras eller signeras. För att skicka ett krypterat e-postmeddelande till en annan person, måste du ha mottagarens offentliga certifikatnyckel kopplad till mottagarens kontaktinformation

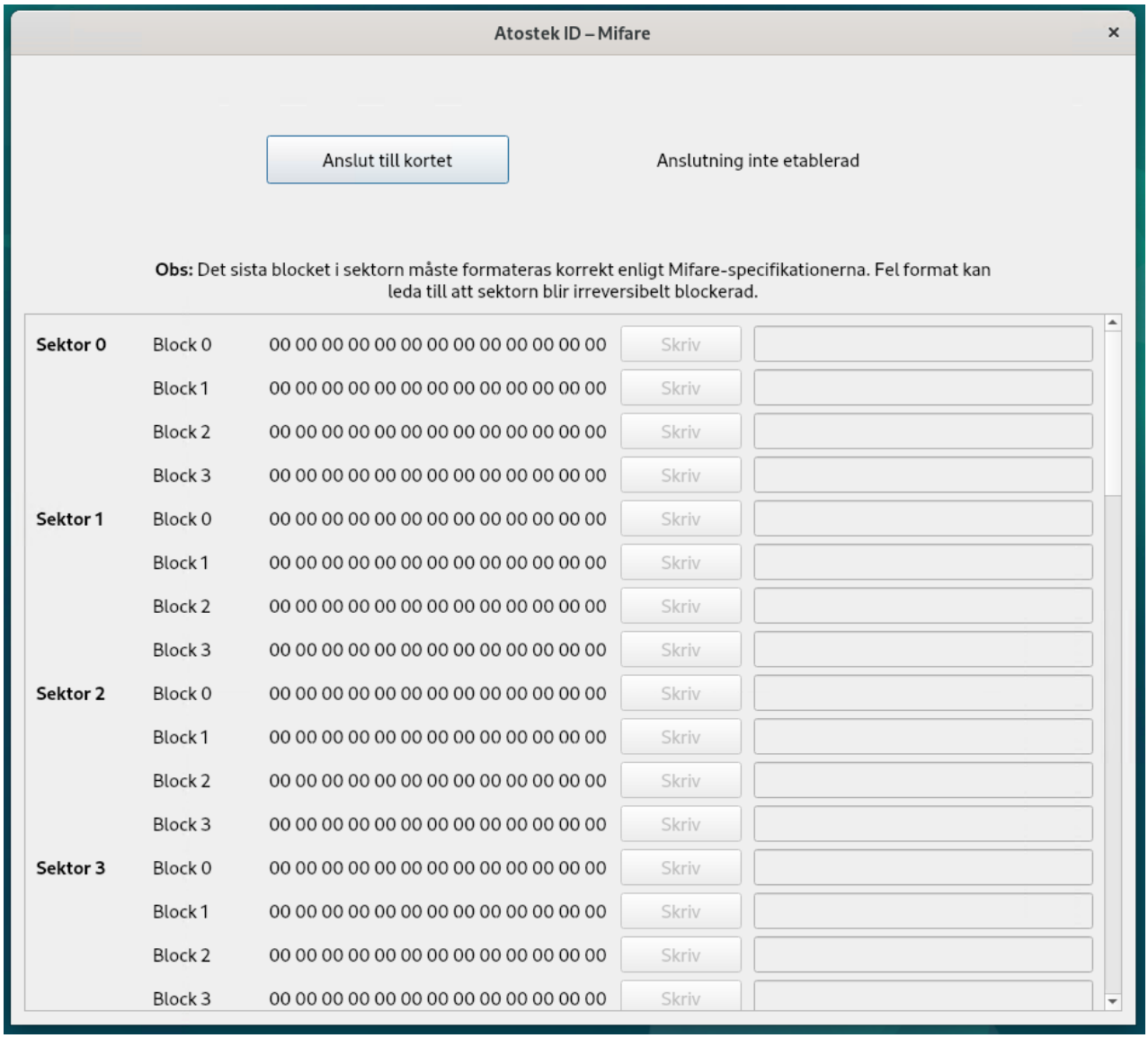
4.9. Arbetsstationsinloggning

På en Linux-arbetsstation kan man autentisera sig med ett autentiseringscertifikat från ett certifieringskort. Då utnyttjas Atostek ID:s PKCS#11-modul, som installeras automatiskt i samband med installationen av Atostek ID Linux-versionerna. Mer detaljerad information om Atostek ID PKCS#11-modulen finns i integrationsguiden för Atostek ID-programvaran.

När Atostek ID PKCS#11-modulen är installerad, kortläsaren är ansluten till datorn, kortet är i kortläsaren och användarens kortinformation är kopplad till Linux-användaren, kan användaren logga in på sin arbetsstation med sitt certifieringskort

4.10. Hantering av MIFARE-chippet

När du under installationen eller via inställningarna har valt alternativet för MIFARE, får du upp alternativet "Mifare" i Atostek ID-applikationens meny (Figur 1). När du väljer det, öppnas en vy enligt figur 12 över MIFARE-chippets sektorer.



Figur 12. Mifare-chippets hanteringsvy

För att läsa och skriva till ett MIFARE-chip behöver du en NFC-läsare. Anslut läsaren till datorn som vanligt och placera kortet i läsaren. Ange kortets PIN1-kod när du blir ombedd att skapa en säker anslutning. Därefter kan du i Mifare-vyn trycka på knappen "Skapa anslutning till kortet". Vyn kommer att informera om anslutningen lyckas eller misslyckas. Vy läser automatiskt in de sexton sektorerna på MIFARE-chippet och innehållet i alla fyra blocken.

I vyn är det också möjligt att skriva till chipets block. **Skriv inte något på MIFARE-chippet om du inte är helt säker på vad du skriver och att skrivningen är nödvändig! Skrivning är inte nödvändig för normala användningsfall eller för att garantera programmets övriga funktioner. Var i kontakt med din organisations IT-support om det behövs.** Felaktig skrivning kan leda till att en sektor permanent låses (särskilt felaktig skrivning av det sista blocket i en sektor). Se till att bekanta dig med NXP:s dokumentation för MIFARE Classic EV1 innan du utför några skrivningar. Ett relativt säkert sätt att testa skrivning är att skriva till block 1 i sektor 2 och sätta alla bytes till värdet 0xFF (det vill säga inmatningen FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF). Värdena kan återställas genom att skriva tillbaka alla bytes till deras ursprungliga värden (vilket vanligtvis är inmatningen 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00).

4.11. Loggning och cachefilar

4.11.1. Loggning och loggfilar

Atostek ID loggar meddelanden om applikationens funktion och fel i sin egen loggfil. Loggfilen finns som standard på sökvägen *"/home/<användare>/.local/share/Atostek Oy/Atostek ID/Error.log"*. För att öppna loggfilen väljer du *"Diagnostik"* från menyn och i det fönster som öppnas väljer du *"Visa Atostek Ids logg"*. Platsen för loggfilen kan ändras via inställningarna.

Som standard loggas information på informations-, varnings- och felnivå. Via inställningarna kan du aktivera debug-nivåloggning, vilket ger mer detaljerad loggning och skapar mer loggdata. Debug-nivåloggning är särskilt viktigt för felsökning. Loggningen kan också stängas av helt via inställningarna. Då tas inte den tidigare loggfilen bort, men inga nya loggmeddelanden registreras.

Atostek ID loggar också felmeddelanden i operativsystemets logg (Syslog).

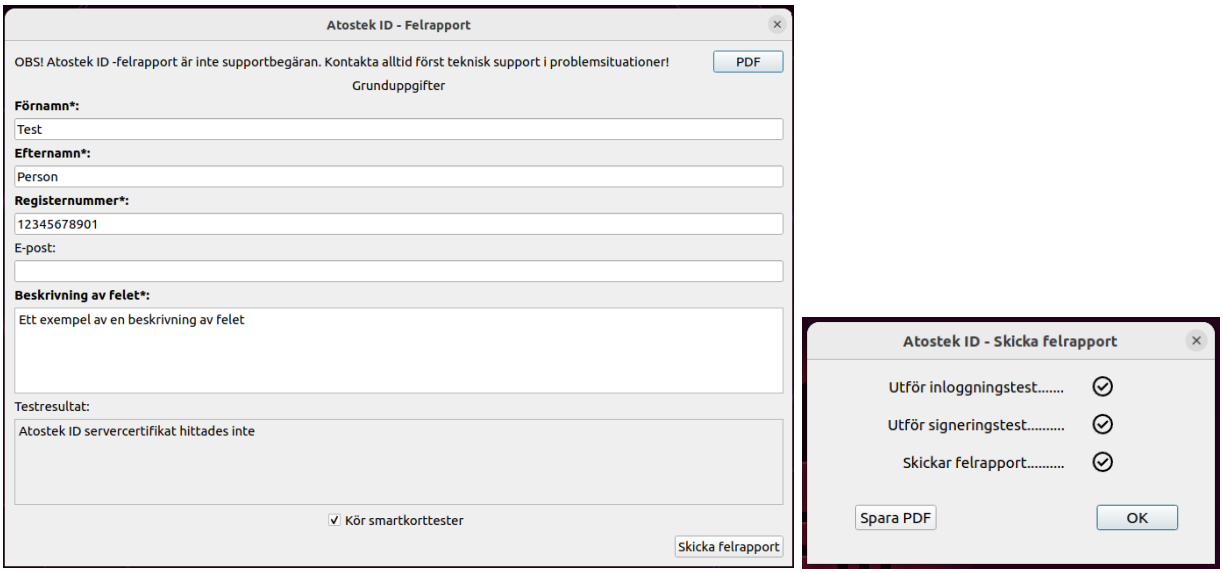
Loggfilen av Atostek ID PKCS#11 -modulen finns på sökvägen *"/home/<användare>/.local/share/Atostek Oy/Atostek ID/PKCS11.log"*.

4.11.2. Cachefilar

Om ”Spara krypterat på disk” har valts som kortcachetyp lagras cachen i filen *“/home/<användare>/.local/share/Atostek Oy/Atostek ID/cache.json”*. Cachefilen rensas automatiskt när en annan kortcachetyp väljs. Du kan därför rensa cachen antingen genom att ändra inställningen för kortcachetyp eller genom att ta bort cachefilen manuellt.

4.12. Felrapportering

I applikationsmenyn hittar du "*Felrapport*" som du kan använda för att skicka en felrapport till ERA-tjänsten. En felrapport i sig är dock inte en supportförfrågan. Om du stöter på ett problem, kontakta alltid din tekniska support först. En felrapport skapas genom att tillhandahålla tillräcklig kontaktinformation och skriva en beskrivning av felet (figur 13). Om läsaren och kortet är sammankopplade fylls kortinformationen i automatiskt.



Figurer 13 och 14. Felrapporten och skickandet av den

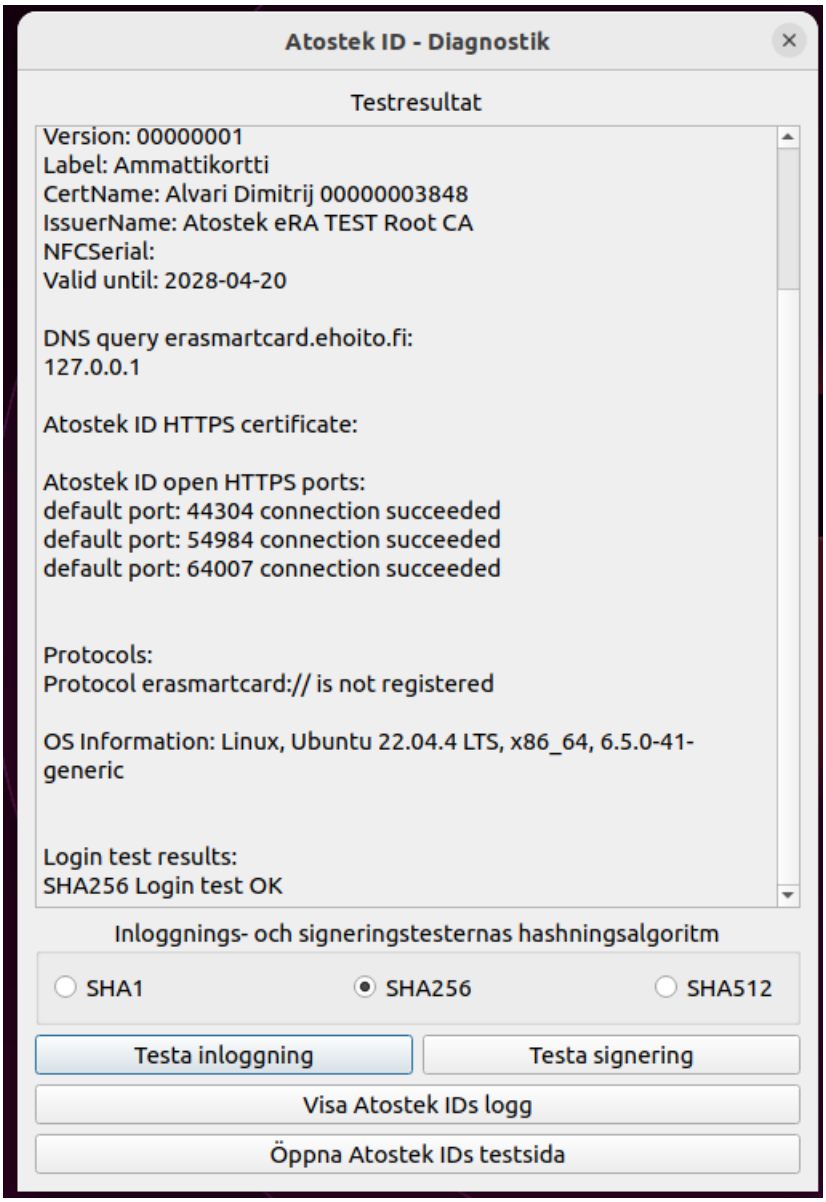
Obligatoriska fält är i fetstil och markerade med en asterisk. Du kan skicka en felrapport genom att klicka på "*Skicka felrapport*"-knappen nere till höger. Observera att knappen inte kan tryckas in om något av de obligatoriska fälten saknas.

Om du vill kan du även spara en .pdf-fil från felrapporten till din dator genom att använda "*PDF*"-knappen uppe till höger. Med kryssrutan "*Kör smartkorttester"* längst ner kan du välja om du vill köra korttester när du skickar en felrapport.

Efter att ha skickat felrapporten öppnas ett fönster där du kan övervaka skickningsförloppet (figur 14). Fönstret för att skicka en felrapport visar status för korttesterna endast om du har valt att korttesterna ska köras i fönstret i figur 13. Om felrapporten skickas framgångsrikt stängs felrapportfönstret (figur 13) automatiskt. Från fönstret för att skicka felrapporter (figur 14) kan du också spara felrapporten som en PDF-fil genom att klicka på knappen "*Spara PDF*".

4.13. Diagnostik

Du kan öppna diagnostikvyn för Atostek ID (figur 15) från applikationsmenyn med "*Diagnostik*". När vyn öppnas körs tester som tar några sekunder. Testresultaten innehåller information om bland annat versionen av Atostek ID-applikationen, anslutna läsare och webbläsare som stöds.



Figur 15. Diagnostikvy.

I diagnostikvyn kan du även testa inloggning och signatur när kortet är anslutet. Du kan välja vilken hashalgoritm som ska användas med hjälp av radioknapparna. Resultaten av inloggnings- och signaturtestet sparas i vyn *"Testresultat"*.

Du kan se felloggen för Atostek ID-applikationen genom att klicka på knappen *"Visa Atostek IDs logg"* Felloggen öppnas i ett separat fönster.

Från knappen "*Öppna Atostek IDs testsida*" kan du testa om Atostek ID-applikationen fungerar korrekt. Om knappen inte öppnar en vit webbplats med texten "*Test page loaded OK*" är något fel. Till exempel, om certifikaten som krävs av Atostek ID inte är inställda på betrodda, öppnas inte testsidan korrekt.

5. Vanliga frågor och felhantering

Atostek ID visar separata felmeddelandefönster när fel inträffar. Dessa inkluderar situationer där

- Atostek ID inte kan starta HTTPS-servern för SCS-gränssnittet på port 53952, eftersom porten inte är ledig.
- Funktionen kan inte utföras eftersom det inte finns något kort i läsaren.
- Funktionen misslyckas (till exempel autentisering eller signering) på grund av felaktiga förfrågningar eller problem med kortet.

Utöver dessa loggar Atostek ID felmeddelanden relaterade till fel och visar i sin logotyp om något är fel.

5.1. Vanliga frågor

F: Appen visar varningen ”Misslyckades med att starta SCS-server på port 53952!” eller ” Misslyckades med att starta SCS CA -server på port 53952!”

S: Det här felet beror vanligtvis på att de angivna portarna inte är lediga, det vill säga att något annat program använder dem. Se till att du inte har ett annat kortläsarprogram installerat eller igång som använder dessa portar. Dessa varningar hindrar endast användningen av applikationens SCS-gränssnitt, så de kanske inte nödvändigtvis förhindrar dig från att använda programvaran inom ramen för dina egna användningsfall. Om det inte hjälper att stänga av och avinstallera ett annat kortläsarprogram kan du undersöka vilket program som använder de portar som Atostek ID-applikationen behöver med hjälp av din dators kommandotolk (lsof-kommandot). Var i kontakt med din organisations IT-support om möjligt. Om du inte alls behöver SCS-gränssnittet i ditt användningsfall och porten kan inte frigörs, kan du inaktivera gränssnittet med inställningarna. Då startar appen inte gränssnittet och ingen varning visas.

F: Jag kan inte läsa information från kortet.

S: Är kortet korrekt insatt i läsaren? Observera att kortets kontaktplatta (den metalliska kvadraten) måste träffa läsarens kontaktplattor för att en anslutning ska kunna upprättas (förutom NFC-läsare). Du kan också försöka torka av kontaktplattan försiktigt eftersom smuts kan försvåra läsningen. Är kortläsaren ordentligt ansluten till enheten? Kan du prova en annan USB-port? Är kortläsarens egen drivrutin installerad och uppdaterad om kortläsartillverkaren erbjuder en sådan? Drivrutiner från kortläsartillverkare finns vanligtvis förinstallerade i operativsystemet. De kan dock också saknas eller behöva uppdateras. Drivrutinspaket kan vanligtvis laddas ner från kortläsartillverkarens egna sidor.

F: Programmet säger att PIN-koden är låst.

S: PIN-koden har då angetts felaktigt för många gånger i rad. Du kan låsa upp PIN-koden med din PUK-kod eller aktiveringskod genom programmet meny.

F: Vad är en PUK-kod?

S: PUK-koden eller aktiveringskoden är en kod som skickats till dig i ett separat brev när du beställde ditt kort. Aktiveringskoden används för att aktivera kortet och för att låsa upp låsta PIN1- och PIN2-koder.

F: Autentisering eller signering fungerar inte i webbläsaren.

S: Den mer detaljerade lösningen på problemet beror på vilket gränssnitt som används. Om det är mTLS-autentisering (till exempel suomi.fi), kontrollera att Atostek ID TokenDriver -drivrutinen har installerats korrekt. Om det gäller autentisering eller signering via SCS-gränssnittet eller erasmartcard.ehoito.fi, kan du kontrollera om du kan nå gränssnittets testsida (https://localhost:53952/ eller https://erasmartcard.ehoito.fi:44304/). Webbläsaren brukar oftast berätta om det finns problem med att nå sidan på grund av DNS-problem eller om certifikaten är misstrodda. Vid DNS-problem, kontakta din organisations IT-avdelning. Certifikat kan manuellt installeras som betrodda i webbläsarens eller operativsystemets certifikatförråd. Du kan också kontrollera i programmets *"Information"*-vy i menyn om de standardportar som krävs av gränssnitten är tillgängliga för användning av programmet.

5.2. Andra problem

5.2.1. Atostek ID PKCS11-modulen

Atostek ID PKCS11-modulen används till exempel för mTLS-autentisering (suomi.fi), dokumentsignering, E-postkryptering och -signering med Thunderbird-programmen samt inloggning till arbetsstationen med ett certifikatkort. Modulen installeras automatiskt i systemet under installationen. Det finns mer information av hur modulen installeras och används i installations- och integrationsanvisning. Följande punkter kan hjälpa med att diagnostisera problem.

Se till att p11-kit-plattformen, som hanterar PKCS11-modulerna på systemet, hittar Atostek ID PKCS11-modulen med kommandot "*p11-kit list-modules*". Om listan inte innehåller modulen under namnet atostek-id, se till att filen "*/etc/pkcs11/modules/atostek-id.module*" innehåller en referens till modulens sökväg enligt integrationsanvisning och att modulen har installerats på sökvägen. Om modulen har installerats korrekt och ett kort är insatt i en ansluten läsare bör kommandot "*p11-kit list-modules*" också lista tokens på kortet.

Obs! Vid första användningen av mTLS-autentisering kan webbläsaren begära PIN-koden flera gånger. Detta är normalt beteende som beror på hur webbläsare hanterar certifikat. Ange din PIN-kod för varje förfrågan.

5.2.2. PSCS-grässnittet är inte aktivt

Atostek ID använder programvaran PC/SC Smart Card Daemon (pcscd) för att kommunicera med kortet. Därför måste systemd-tjänsterna pcscd.service och pcscd.socket för PCSCD vara aktiva för att Atostek ID ska kunna kommunicera med kortet. Du kan kontrollera status för dessa tjänster med kommandona *sudo systemctl status pcscd.service* och *sudo systemctl status pcscd.socket*. Om tjänsterna inte är aktiva kan du aktivera dem med kommandona *sudo systemctl start pcscd.service* och *sudo systemctl start pcscd.socket*. För mer detaljerade instruktioner, se installationsguiden för motsvarande version och operativsystem.

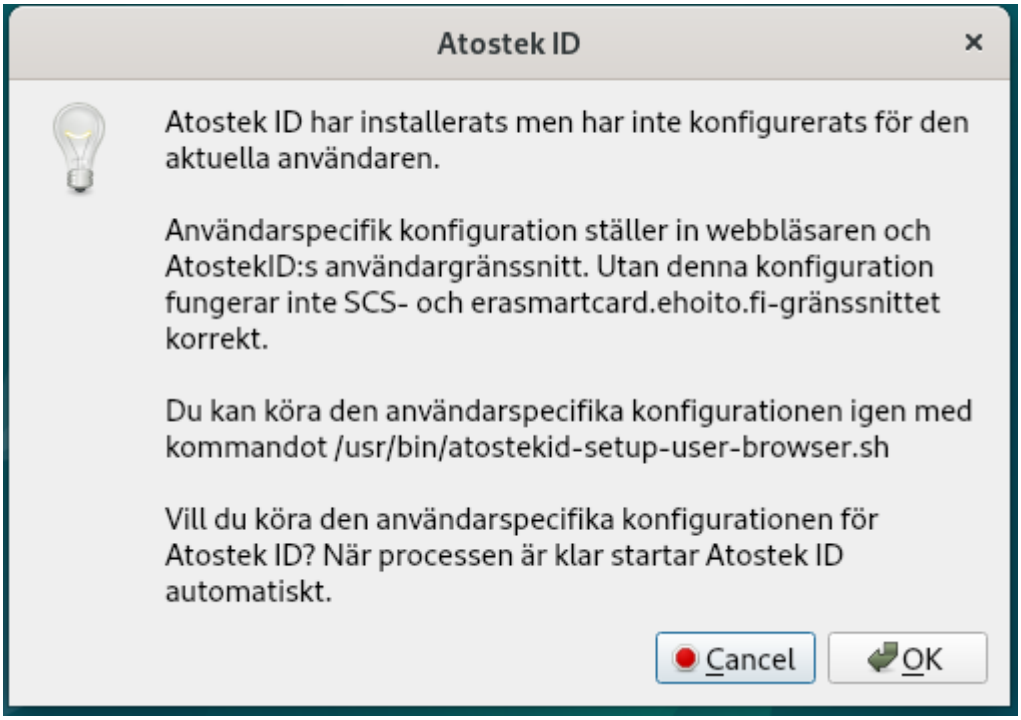
5.2.3. Atostek ID varnar om att aktivitetsfält saknas

Atostek ID använder GNOME AppIndicator för att göra applikationen synlig i aktivitetsfältet. Om ett lämpligt aktivitetsfält inte finns tillgängligt i operativsystemet, informerar Atostek ID användaren om detta med en separat varning vid uppstart. Problemet kan åtgärdas genom att installera paketet *gnome-shell-extension-appindicator* med pakethanteraren och administratörsrättigheter. För mer detaljerade instruktioner, se installationsguiden för motsvarande version och operativsystem.

5.2.4. Säker anslutning till SCS- eller erasmartcard.ehoito.fi-grässnittet kan inte upprättas

Installationen av Atostek ID kräver slutförande av användarspecifika inställningar, vilket inte kan utföras automatiskt av installationspaketet. Därför måste användaren själv slutföra installationen genom att köra skriptet */usr/bin/atostekid-setup-user-browser.sh*, som installeras tillsammans med installationspaketet, med användarbehörighet. Skriptet konfigurerar de SCS- och erasmartcard.ehoito.fi-servercertifikat som Atostek ID genererar som betrodda i de webbläsare som används. För mer detaljerade instruktioner, se installationsguiden för motsvarande version och operativsystem.

Atostek ID försöker identifiera om slutförandeskriptet för installationen har körts. Om skriptet inte har körts erbjuder Atostek ID vid uppstart möjlighet att köra det enligt figur 16.



Figur 16. Notis om slutförande av användarspecifika inställningar

När du godkänner förslaget i figur 16 kör Atostek ID slutförandeskriptet, vilket kan ta flera sekunder. Efter att skriptet har körts startas Atostek ID automatiskt och applikationen är då klar att användas.