



22.3.2021

Guide för användning av certifikatkort för Social- och hälsovården

22.3.2021



22.3.2021

Innehållsförteckning

1	Certifikatkort för social- och hälsovården.....	3
2	Kortets ändamål och giltighet.....	3
2.1	Tillåtna användningsändamål för certifikat	3
2.2	Förbjudna användningsändamål för certifikat.....	3
2.3	Giltighet	3
3	Kortuppgifter.....	4
3.1	Funktionskontroller	5
4	Öppnande av en låst PIN-kod och byte av certifikatkortets PIN-kod	6
4.1	Byte av PIN-koden	6
4.2	Upplåsning av låst PIN-kod.....	8
5	Ny beställning av PUK-/Aktiveringskod	9
6	Kortinnehavarens ansvar och ett förkommet kort.....	9
7	Testning av identifiering och elektronisk signatur.....	10



22.3.2021

Guide för användning av certifikatkort för Social- och hälsovården

1 Certifikatkort för social- och hälsovården

Certifikatkort för hälsovården är yrkeskort som Myndigheten för digitalisering och befolkningsdata (nedan MDB) beviljar yrkesutbildade personer inom hälso- och sjukvården och personal- och aktörskort som är avsedd för övrig personal/övriga aktörer.

Certifikatkortet och den aktiveringskod som behövs för att använda kortet är personliga och mottagning av dem har förutsatt att kortinnehavarens identitet har intygats. När kortinnehavaren tar emot kodkuvertet som innehåller certifikatkortet och koden ska han eller hon kontrollera att uppgifterna på kortet är riktiga och att kodkuvertet inte har öppnats.

Extra information och kontaktinformation som anknyter till certifikatkortet finns att få på webbplatsen <https://dvv.fi/sv/social-och-halsovard>

2 Kortets ändamål och giltighet

De viktigaste användningsområdena för certifikaten anges i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och i lagen om elektroniska recept (61/2007). Dessutom kan certifikat användas i andra datasystem inom hälsovården och apoteksväsendet.

2.1 Tillåtna användningsändamål för certifikat

Ett certifikat förenar en person och en offentlig nyckel som ställts till personens förfogande och en med PIN-kod skyddad privat nyckel. Certifikat används för elektronisk identifiering av certifikatets innehavare och för elektronisk underskrift, dvs. för verifiering av äktheten, integriteten och obestridligheten av ett digitalt dokument eller någon annan digital uppgift (t.ex. läkarintyg, elektroniskt recept).

2.2 Förbjudna användningsändamål för certifikat

Det är förbjudet att förmedla patientuppgifter per e-post. Det är således inte tillåtet att använda yrkescertifikat för hälsovården för att kryptera eller underteckna e-postmeddelanden som innehåller patientuppgifter.

2.3 Giltighet

Kortet är i kraft antingen under den allmänna giltighetstiden, som är fem år, en certifikatsspecifik frist eller tills det spärras när kriterierna för spärrning uppfylls.



22.3.2021

3 Kortuppgifter

Person- och yrkesrättighetsuppgifterna på ett yrkeskort erhålls från centralregistret för yrkesutbildade personer inom hälso- och sjukvård (Terhikki/Suosikki) som administreras av Tillstånds- och tillsynsverket för social- och hälsovården (nedan Valvira). Registreringsstället eller kortleverantören gör inga ändringar i de uppgifter som erhålls från Terhikki/Suosikki. Eventuella begäran om korrigeringar, till exempel om uppdatering av uppgifterna om yrkesrättigheter, riktas alltid till Valvira. Uppgifterna på de övriga certifikatkorten baseras på uppgifter som lämnats av den organisation som den sökande representerar samt på uppgifter som erhålls från befolkningsdatasystemet som administreras av MDB.

Trycket på kortets yta innehåller:

- kortets rubrikuppgifter
- kortinnehavarens namn
- kortinnehavarens registreringsnummer (på kortets framsida)
- (kortinnehavarens fotografi)
- datum för beviljandet
- sista giltighetsdagen
- uppgifterna om yrkesrättigheter/yrkesbeteckningen
- kontaktinformation för kortets utfärdare
- kortets nummer (på kortets baksida)
- streckkoden (innehåller registreringsnumret)
- i kortet för övriga personer/övriga aktörer organisationens namn

Utöver uppgifterna om kortinnehavaren innehåller chipset:

- verifierings- och underskriftsnyckeln
- verifierings- och underskriftscertifikatet
- utfärdarens (MDB) certifikat
- chipsets nummer

PIN-kuvertet innehåller:

- PUK-/aktiveringskod (8 siffror), med hjälp av vilken användaren själv definierar två PIN-koder:
 - baskoden (PIN1) 4–8 siffror, med vilken kortinnehavaren identifierar sig som användare av systemen
 - signaturkoden (PIN2) 4–8 siffror, med vilken kortinnehavaren gör en elektronisk signatur

Obs. Ibruktageandet av certifikatkort har ändrats hösten 2017 och i kodkuvertet levereras endast aktiveringskoden. Kortet aktiveras med aktiveringskoden som skickats per brev. Vid aktiveringen ges kortet en baskod och en underskriftskod. Bägge kan väljas fritt. Aktiveringen görs med kortläsarprogrammet mPollux Digisign Client version 4.0.12 eller nyare. Skärmen med aktiveringskoden öppnas automatiskt om båda koderna är låsta.



22.3.2021

3.1 Funktionskontroller

Kortinnehavaren gör en kontroll av kortets funktionsduglighet.

Nedan uppräknas kontroller som kan göras av kortinnehavaren med eventuell assistans av registreraren eller det lokala IT-stödet.

Kortinnehavaren bör hos registreraren anmäla om ett funktionsodugligt eller defekt kort för vidare åtgärder.

Punkter som ska kontrolleras vid kontrollen av kortets funktion:

- Om det syns brott i ytan på kortets chip och om chipet har djupa skråmor eller märken efter slag. Om något sådant framgår, har kortet eventuellt hanterats på fel sätt, chipet eventuellt fysiskt skadats och omfattas av denna orsak inte av garantin.
- Om det finns smuts på chipsets yta, torka av chipet med en ren, luddfri trasa.
- Kontrollera att arbetsstationen och kortläsaren fungerar genom att testa kortet på arbetsstationen. Om inte ett funktionsdugligt kort heller fungerar i arbetsstationen, ska du kontakta adb-stödet. Felet kan finnas i certifikatkortläsaren, kortläsarprogrammet eller dess drivrutiner.
- Pröva om kortläsarprogrammet läser kortets uppgifter (i Windows: se bruksanvisningen för mPollux Digisign Client genom att välja *Käynnistä – Fujitsu – Asennus- ja käyttöohje.pdf*). Om ikonen för Digisign Client lämnar i status "Oväntat fel" (Odottamaton virhe) eller "Väntar på smartkort" (Odotetaan älykorttia/älykortteja) är kortet eller kortläsaren sannolikt defekt.
- Pröva om du kan kontrollera eller ändra baskoden PIN1 (se bruksanvisningen för mPollux Digisign Client).
- En låst PIN-kod kan inte bytas
- En låst PIN-kod kan frigöras med PUK-/aktiveringskoden (se bruksanvisningen för mPollux Digisign Client). Innan du öppnar PIN-koden med PUK-/aktiveringskoden kan du försäkra dig om att PIN-koden faktiskt är låst genom att fem (5) gånger knappa in fel kod. Vid behov kan PUK-/Aktiveringskoden beställas på nytt för kortinnehavaren (PIN-koder kan inte beställas på nytt till ett certifikatkort som redan utfärdats).
- Om PIN-koden inte går att byta enligt anvisningen och PIN-koden inte är låst, är chipet defekt och jdet är fråga om en produkt som ska reklameras.
- Om PIN-koden inte är låst, men kortet likväl inte öppnar de applikationer/program som kortet borde ge åtkomst till, ska du ytterligare testa chipets funktionsduglighet genom att logga in på MDB:s testtjänst på adressen: <https://dvv.fi/sv/testning->



22.3.2021

av-certifikat. Om inloggningen inte lyckas är chipet sannolikt defekt och det är då fråga om en produkt som ska reklameras.

- Om inloggningen på MDB:s testtjänst lyckas, men kortet trots det inte ger åtkomst till önskade program, eller du får tillträde till tjänster och nätresurser som hänför sig till en annan användare, ska du kontakta IT-stödet eller en annan instans som ansvarar för användarrättigheterna och till vilken du hänvisas av din organisation. Dina användarrättigheter till programmen kan vara bristfälliga eller felaktiga, eller innehållet av kortets certifikat kan ha blivit defekt i samband med kortbeställningen.

De offentliga certifikatuppgifter som finns på kortet om kortinnehavaren kan ses med hjälp av kortläsarprogrammet (se bruksanvisningen för mPollux DigiSign Client genom att välja Käynnistä – Fujitsu – Asennus- ja käyttöohje.pdf)

4 Öppnande av en låst PIN-kod och byte av certifikatkortets PIN-kod

En låst PIN-kod öppnas med nyckelkoden (PUK-/Aktiveringskod). Om nyckelkoden inte är tillgänglig ska kortinnehavaren personligen kontakta närmaste registreringsställe.

Kortinnehavaren kan byta kortets bas- och signaturkoder, om han eller hon önskar. PIN-koderna kan ändras så att de har 4–8 siffror. Bytet av PIN-koderna görs

- med kortläsarprogrammet
- på registreringsstället

Mer ingående information om byte av koderna finns att få av de som ansvarar för datasystemen hos kortinnehavarens organisation eller på adressen <https://dvv.fi/sv/hantering-av-pin-koder>.

4.1 Byte av PIN-koden

Certifikatkortens PIN-koder byts med hjälp av verktyget mPollux DigiSign Client Manager. Placera kortet i läsaren och vänta på att chipikonen i uppgiftsbalken blir gul. Öppna programvaran genom att högerklicka på den gula chipsikonen som finns nere till höger på skrivbordet och välj *Näytä laitteet*.

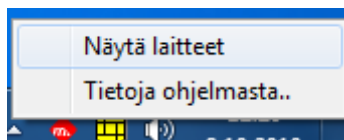


Bild 1: Dialogruta för kortläsarprogrammet

1. Välj fliken *Tunnistus*.



22.3.2021

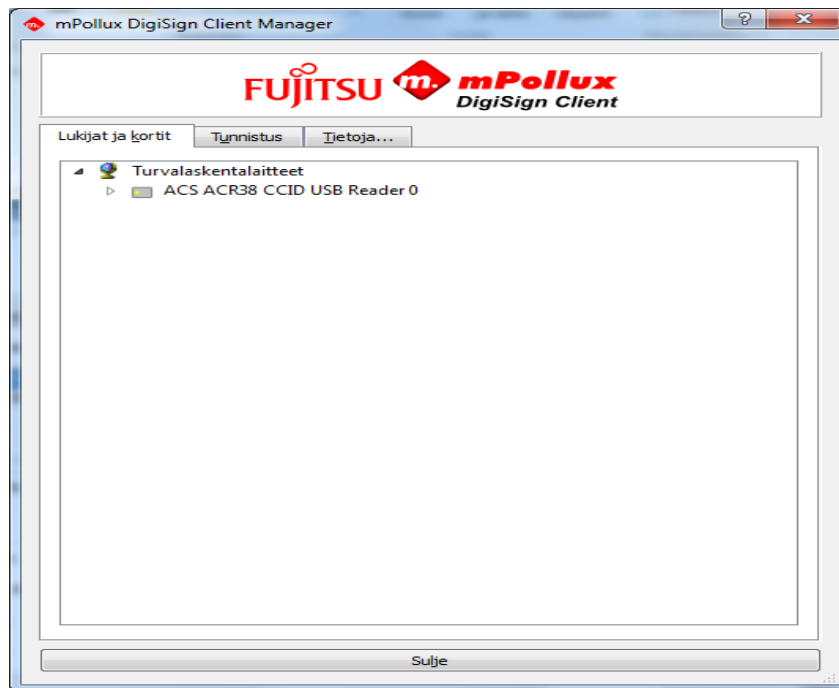


Bild 2: Kortläsarprogrammets startvy

2. Fliken Tunnistus

Visa genom att klicka med musen vilken kod du byter (baskoden / underskriftskoden). Baskoden är vald som standard.

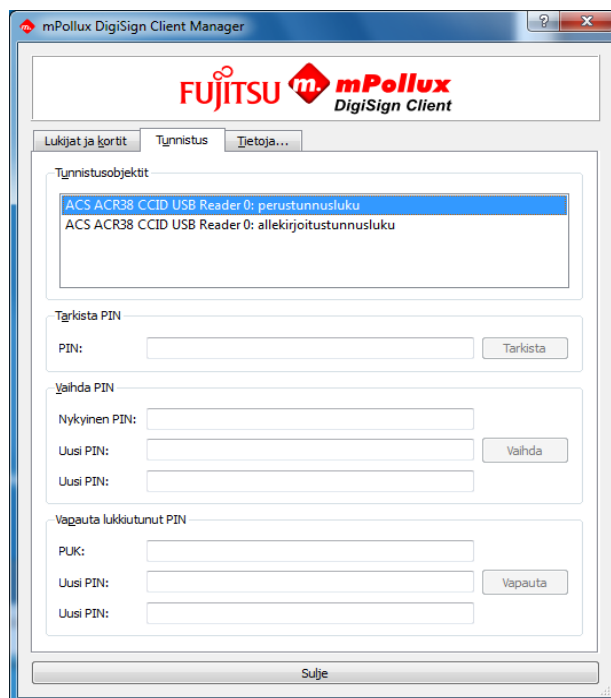


Bild 3: PIN-val (bas- eller signaturkod)



22.3.2021

3. Mata in den nuvarande PIN-koden i fältet "Nykyinen PIN"
Mata in den nya PIN-koden i fältet "Uusi PIN"
Mata in den nya PIN-koden i fältet "Uusi PIN" en gång till
Välj Vaihda med musen
4. Programmet kontrollerar att bytet av PIN-koden gjordes
5. Du kan kontrollera PIN-kodens riktighet med funktionen "Tarkista PIN".

4.2 Upplåsning av låst PIN-kod

1. En låst PIN-kod låses upp med hjälp av verktyget mPollux DigiSign Client Manager.
2. Klicka med musen för att välja den låsta PIN-koden som du vill låsa upp (baskoden / underskriftskoden).

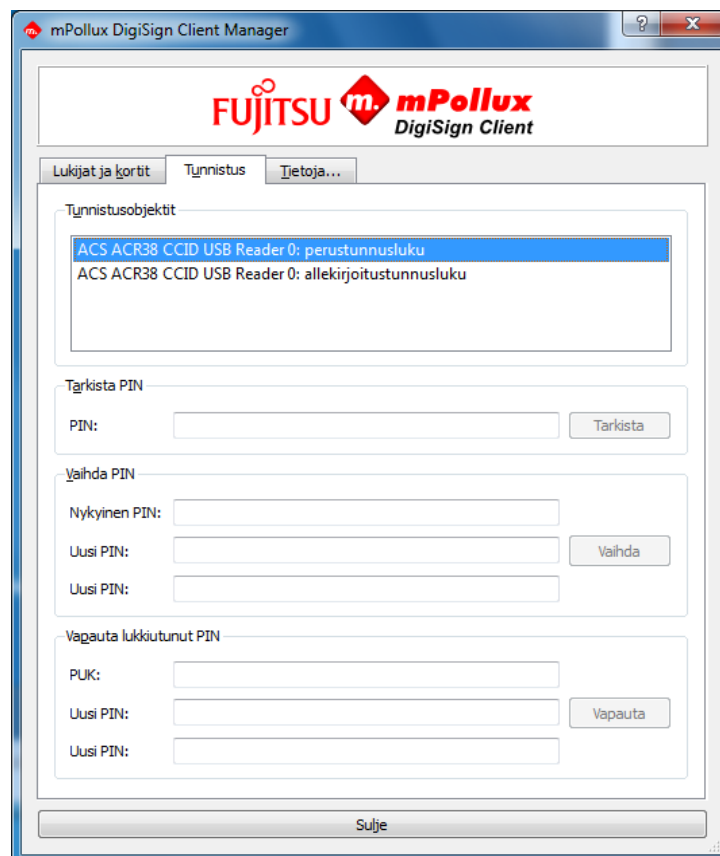


Bild 4: Frigörande av PIN

3. Mata in PUK-/aktiveringskoden i punkten *Vapauta lukkiutunut PIN*
Mata in en ny PIN-kod under "*Uusi PIN*"
Mata in PIN-koden på nytt under "*Uusi PIN*"



22.3.2021

4. Välj med musen: *Vapauta*
5. Programmet bekräftar att den låsta PIN-koden har frigjorts.

5 Ny beställning av PUK-/Aktiveringskod

PUK-/Aktiveringskoden beställs alltid på ett registreringsställe för social- och hälsovården.

En ny beställning av nyckelkods brevet förutsätter att kortinnehavaren besöker registreringsstället personligen. Kortinnehavaren ska ha med sig ett av polisen utfärdat giltigt identifieringsdokument: pass, identitetskort eller ett av polisen utfärdat separat identifieringsdokument.

6 Kortinnehavarens ansvar och ett förkommet kort

Certifikatkortet är endast avsett för kortinnehavaren, som ansvarar för användningen av kortet. Alla elektroniska transaktioner som utförs med kortet sker i kortinnehavarens namn på dennes ansvar. *Kortet ska förvaras omsorgsfullt och separat från korderna.* Det är viktigt att spara kortets nummer (till höger på kortets baksida) för den eventualiteten att kortet blir spärrat.

Om kortet har skadats, kommit bort, blivit stulet eller inte längre behövs, ska certifikaten omedelbart meddelas till spärrtjänsten för att förhindra missbruk. För yrkeskortets del är det den yrkesutbildade personens ansvar att spärra kortet. Kortinnehavarens ansvar för kortet slutar när meddelandet har tagits emot av spärrtjänsten.

Ett kort som tas ur bruk överläts till registreraren vid registreringsstället endast i reklamerationsfall. I övriga fall ska certifikatinnehavaren själv förstöra sitt onödiga eller föråldrade certifikatkort på behörigt sätt. Certifikatkortet förstörs genom att klippa kortets chip i fyra delar.

Spärrtjänsten är öppen dygnet runt under årets alla dagar:

- Tfn 0800 162 622 (gratis inom Finland)
- Från utlandet +358 800 162 622 (+ den lokala operatörens avgift)

Ett spärrat certifikat kan inte tas i bruk igen.

Ett certifikat gäller i högst 5 år från datumet för beviljandet av certifikatet.



22.3.2021

7 Testning av identifiering och elektronisk signatur

På Myndigheten för digitalisering och befolkningsdatas webbplats <https://dvv.fi/sv/testning-av-certifikat> hittar du anvisningar och en länk till testningen av identifiering och elektronisk signatur. Du behöver både PIN1- och PIN2-koderna för testet.