4.4.2024

Tjänstebeskrivning

Affärsekonomisk 2023

Innehållsförteckning

1 Servicebeskrivning av certifikattjänsterna vid Myndigheten för digitalisering och befolkningsdata

Servicebeskrivningen beskriver de företagsekonomiska certifikattjänstprodukterna vid Myndigheten för digitalisering och befolkningsdata. I servicebeskrivningen definieras:

- organisationskort
- organisationscertifikat
- tillfälliga kort och tillfälliga certifikat
- beställnings- och administrationssystemet (Vartti)
- servercertifikat
- e-postcertifikat
- systemsigneringscertifikat
- Stämpeltjänst
- olika testprodukter
- katalog- och spärrtjänst
- rådgivningstjänst

2 Certifikatprodukter

2.1 Certifikat och kort för organisationer

2.1.1 Organisationskort med färdig kortmall

Organisationskort kan beställas med färdig kortmall eller så kan beställaren planera kortets utseende helt och hållet själv. Genom att välja en färdig kortmall för organisationskorten får kunden tillgång till certifikatkorten snabbare.

I den färdiga kortmallen har textfälten och fonterna definierats färdigt på produkten. Det finns fem olika kortmallar att välja mellan och kortens grundfärg är vit. Korten produceras i sin helhet med ytutskriftsteknik.

I en färdig kortmall kan placeringen av logon och textfälten inte ändras. Så kallade styrfält på framsidan av organisationskortet är kortets giltighetstid, efternamn och förnamn samt kortets identifieringskod. Kortets nummer och streckkod skrivs automatiskt ut på baksidan av kortet. Dessutom finns det, beroende på kortmallen, valfria fält där kortinnehavarens titel eller annan information kan anges. Kortmallarna är tillgängliga som horisontella och vertikala modeller. Kortet kan vara med eller utan bild. På det horisontella kortet placeras personens bild i högra kanten och på det vertikala kortet i mitten av kortet.

Grundande

Ibruktagande av en ny kortmall inkluderar att kortet planeras och produceras. Till dessa hör bland annat beredning av logotyper och val av kortmodell (utan/med bild). Till grundandet av korttypen hör dessutom att skapa kundrelationer och produktspecifikationer i MDB:s beställnings- och administrationssystem. För ibruktagandet av den färdiga kortmallen debiterar MDB kostnader för grundandet. Ingen separat underhållsavgift för korttypen debiteras.

Organisationscertifikatens informationsinnehåll

Typiska uppgifter om personen är:

- Personens för- och efternamn
- Identifieringskod för personen
- Organisation
- Organisationsenhet
- Titel
- E-postadress
- UPN-namn

Närmare tekniska specifikationer av organisationscertifikatens informationsinnehåll finns i FINEID S2-specifikationen som finns på https://dvv.fi/sv/fineid-specifikationer.

Allmänna egenskaper

Kortmallen är tillverkad av PVC. Chipet innehåller en PKI-applikation enligt FINEID S4-2 -specifikation. På chipet specificeras de kortspecifika nycklarna och de koder som skyddar användningen av dem samt certifikat som innehåller de personuppgifter som beställningen gäller. Dessa certifikat uppfyller de krav som ställs på godkända certifikat.

Till organisationskortet hör:

- PVC-kortmall
- Chipformatering och elektronisk specificering
- Visuell specificering av kortet
- aktiveringskod som behövs för ibruktagande i ett separat brev

MDB erbjuder ett kortläsarprogram för operativsystemen Windows, macOS och Linux.

Figur 1 Kortmall 1 baksida

Figur 2 kortmall 1 framsida

Figur 3Figur 4Kortmall 2 baksida

Figur 4 Kortmall 2 baksida

Figur 5 Kortmall 3 framsida

Figur 6 Kortmall 3 baksida

Figur 7Kortmall 4 baksida

Figur 8 Kortmall 4 framsida

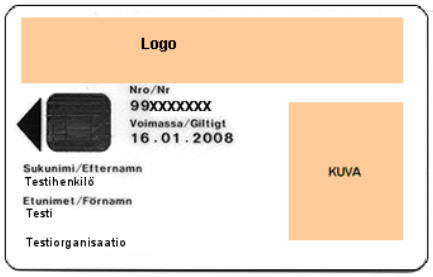
Figur 9 Kortmall 5 baksida

Figur 10 Kortmall 5 framsida

2.1.2 Standardorganisationskort

Standardorganisationskortet är ett organisationskort som kunden helt och hållet har planerat själv. Kortet definieras kundspecifikt tillsammans med kunden och kortfabriken samt eventuellt med reklambyrån.

Visuellt utseende



Figur 11 Standardorganisationskort, exempel 1

Figur 12 Standardorganisationskort, exempel 2

Standardorganisationskorten har vit grundfärg. Kortet produceras i sin helhet med ytutskriftsteknik. Texten som kommer på organisationskortets framsida, s.k. styrfält, är kortets serienummer, sista giltighetsdag, förnamn och efternamn samt ett valfritt fält där man kan ange organisation, organisationsenhet eller titel. Kortet kan vara med eller utan bild. Kortet finns också som vertikal modell.

Andra styrfält för texten är anvisningar för returnering av kortet samt returadresser på kortets baksida. Organisationskorten följer standarden ISO 7816 1-8.

Organisationscertifikatens informationsinnehåll

Typiska uppgifter om personerna är:

- Personens för- och efternamn
- Identifieringskod för personen
- Organisation
- Organisationsenhet
- Titel
- E-postadress
- UPN-namn

Närmare tekniska specifikationer av organisationscertifikatens informationsinnehåll finns i FINEID S2-specifikationen som finns på https://dvv.fi/sv/fineid-specifikationer.

Grundande

Grundandet av ett standardorganisationskort omfattar planering och produktion av kortet. Dessa omfattar bl.a. förberedelse av logotyper, bestämning av standardtexter, bestämning av innehåll i textfält som ska specificeras, bestämning av rubriktexter, bestämning av läsriktning och val av kortmodell (med/utan bild). Grundandet av korttypen omfattar dessutom skapandet av kundrelationer och produktspecifikationer i MDB:s beställnings- och administrationssystem samt till exempel att genomföra systemets säkerhetskrav för korttypen i fråga.

Underhållstjänst

Underhållet av standardorganisationskortet består av ändringar i leveransadressuppgifter och kontaktpersoner, upprätthållande och utveckling av systemets funktionsförmåga samt kundorienterade ändringsarbeten. Kundspecifik hantering av lagringen av kortmallar är en del av underhållstjänsten

Allmänna egenskaper

Kortmallen är tillverkad av PVC. Det finns en neutralt förtryckt botten utan ledande texter. Specificeringen görs i regel som ytutskrift i färg på båda sidorna av kortet, texterna är ändå alltid i standardfärg. Bilden är alltid i standardstorlek både vertikalt och horisontellt.

På kortet kan man skriva ut 1-5 rader text antingen vertikalt eller horisontellt. En maximilängd har bestämts för raden, men radens innehåll kan fastställas enligt korttyp. Kortet kan ha en logotyp i färg.

Chipet innehåller en PKI-applikation enligt FINEID S4-2 -specifikation. På chipet specificeras de kortspecifika nycklarna och de koder som skyddar användningen av dem samt certifikat som innehåller de personuppgifter som beställningen gäller. Dessa certifikat uppfyller de krav som ställs på godkända certifikat.

Korten kan också innehålla säkerhetsegenskaper eller andra funktionella egenskaper som inte ingår i standardlösningar för organisationskort.

Organisationskortet innehåller:

- PVC-kortmall
- Chipformatering och elektronisk specificering
- Visuell specificering av kortet
- aktiveringskod som behövs för ibruktagande i ett separat brev

MDB erbjuder ett kortläsarprogram för operativsystemen Windows, macOS och Linux.

2.1.3 Certifikatkort

MDB har fastställt ett standardutseende för certifikatkortet för att påskynda kundspecifika ibruktaganden. Med denna lösning får kunderna snabbare tillgång till sina certifikatkort. Kortet är avsett för små produktionspartier.

Visuellt utseende

Den visuella specificeringen av kortets fram- och baksida är färdigt bestämd. Kortet förses inte med en organisationens logo eller ett personfoto. Kortets framsida produceras med samma grunddefinitioner som standardorganisationskortet i punkt 2.1.2. På framsidan visas kortets serienummer, sista giltighetsdag, personens förnamn och efternamn samt som option ett fält med titel, organisationsenhet eller organisation. På baksidan av kortet finns en returanvisning och en returadress enligt beställningsmaterialet

Figur 13 Certifikatkort

Certifikatets innehåll

Certifikatets informationsinnehåll är identiskt med det koncept för standardorganisationskort som beskrivs i punkt 2.1.2.

Underhållstjänst

Underhåll av certifikatkort består av ändringar av leveransadressuppgifter och kontaktpersoner, underhåll och utveckling av systemets funktionsförmåga samt ändringsarbeten som utgår från kunden i en i övrigt standardiserad lösning. Kundspecifik hantering av lagringen av kortmallar är en del av underhållstjänsten

2.1.4 Tillfälliga kort och tillfälligt certifikat

Tillfälliga kortet kan överlåtas till en anställd i situationer då organisationskortet har gått sönder eller inte är tillgängligt för den anställde av en annan orsak. När behovet att använda tillfälliga kortet upphör returnerar arbetstagaren kortet till registreraren som spärrar tillfälliga certifikat på kortet.

Certifikat på tillfällig kort kallas tillfälligt certifikat. Informationsinnehållet i det tillfälliga certifikatet motsvarar informationsinnehållet i organisationskortets certifikat. Med tillfälliga kortet kan du identifiera dig i datasystem i huvudsak på samma sätt som med egentliga certifikatkortet. Tillfälliga kortet kan dock inte användas som identifieringsmedel i Suomi.fi-identifikation. Utifrån användningsbehovet kan kunden välja både autentiseringscertifikat och signeringscertifikat för sina tillfälliga kort.

Tillfälliga certifikat är verktyg för stark autentisering enligt lagen om stark autentisering och betrodda elektroniska tjänster.

Till sina visuella egenskaper är tillfälliga kortet förenklat.

Tillfälliga kortet är inte en engångsprodukt, utan tillfälliga certifikat kan läggas till och tas bort genom att det specificeras på nytt.

2.1.5 Ombeställning av aktiveringskoden

Koden (PIN) för ett låst kort frigörs med aktiveringskoden. Om
kortinnehavaren har tappat bort sin aktiveringskod, ska hen beställa en ny aktiveringskod av registreraren. Den kod som registreraren beställt skickas till kortinnehavaren per post.

2.1.6 Servercertifikat

Vid elektronisk kommunikation är det nödvändigt att identifiera även den som levererar tjänsten. För detta ändamål beviljar Myndigheten för digitalisering och befolkningsdata servercertifikat. De kan användas för identifiering av såväl den offentliga förvaltningens, hälsovårdens som den privata sektorns tjänster. Med hjälp av servercertifikatet kan den som utnyttjar tjänsten försäkra sig om att tjänsteleverantören är äkta.

- Servercertifikat möjliggör krypterad datakommunikation mellan en webbläsare och en server eller mellan två servrar.
- Servicecertifikatet beviljas för högst ett år.
- Den som underhåller servern skapar nyckelparen som används av servercertifikaten. Nyckeln ska vara minst 2048 bit lång på RSA-certifikatet och minst 256 bit på ECC-certifikatet.

Beroende på användningsmålet kan servercertifikatets användningssyfte specificeras:

- identifiering av server (server authentication)
- identifiering av kund (client authentication)
- båda samtidigt (server authentication och client authentication).

2.1.7 Systemsignaturcertifikat

Systemsignaturcertifikatet är avsett för elektroniska signaturer som bildas i informationssystem Systemsignaturcertifikatet används för att elektroniskt underteckna sådana handlingar som inte undertecknas med personcertifikat. När man anslutning sig som användare i Kanta-tjänsternas patientuppgiftsarkiv behövs ett systemsignaturcertifikat.

2.1.8 E-postcertifikat

E-postcertifikat är avsedda för enskilda e-postadresser som används av flera personer inom en organisation. Meddelanden till dessa adresser tas emot av en enhet eller avdelning inom organisationen, inte av en enskild anställd.

Exempel på adresser som eventuellt använder e-postcertifikat:

- registratorskontorens adresser
- beställningsadresser
- anmälningsadresser
- e-postadresser (där inkommande meddelanden innehåller konfidentiell information).

Krypterade meddelanden som inkommit till organisationens e-postadress öppnas med hjälp av e-postcertifikatet. Certifikatet kan även användas för signering av organisationens utgående meddelanden.

Vid användning av e-postcertifikat som beviljats av Myndigheten för digitalisering och befolkningsdata som filbaserat certifikat behövs inga kortläsare eller separata program. E-postcertifikatet fungerar i de vanligaste e-postprogrammen med stöd för S/MIME-meddelanden.

2.2 Olika testprodukter

2.2.1 Testkort

Testkortet lämpar sig för testning av olika tekniska funktioner, bland annat testning av kortläsare samt inloggning i olika datasystem. Med testkorten kan man också testa skapandet av elektroniska signaturer.

Personuppgifterna i testkortens certifikat är påhittade. Datainnehållet på certifikatet motsvarar i övrigt datainnehållet i organisationscertifikatet. Testkorten är tillgängliga med organisationscertifikatets och medborgarcertifikatets datainnehåll.

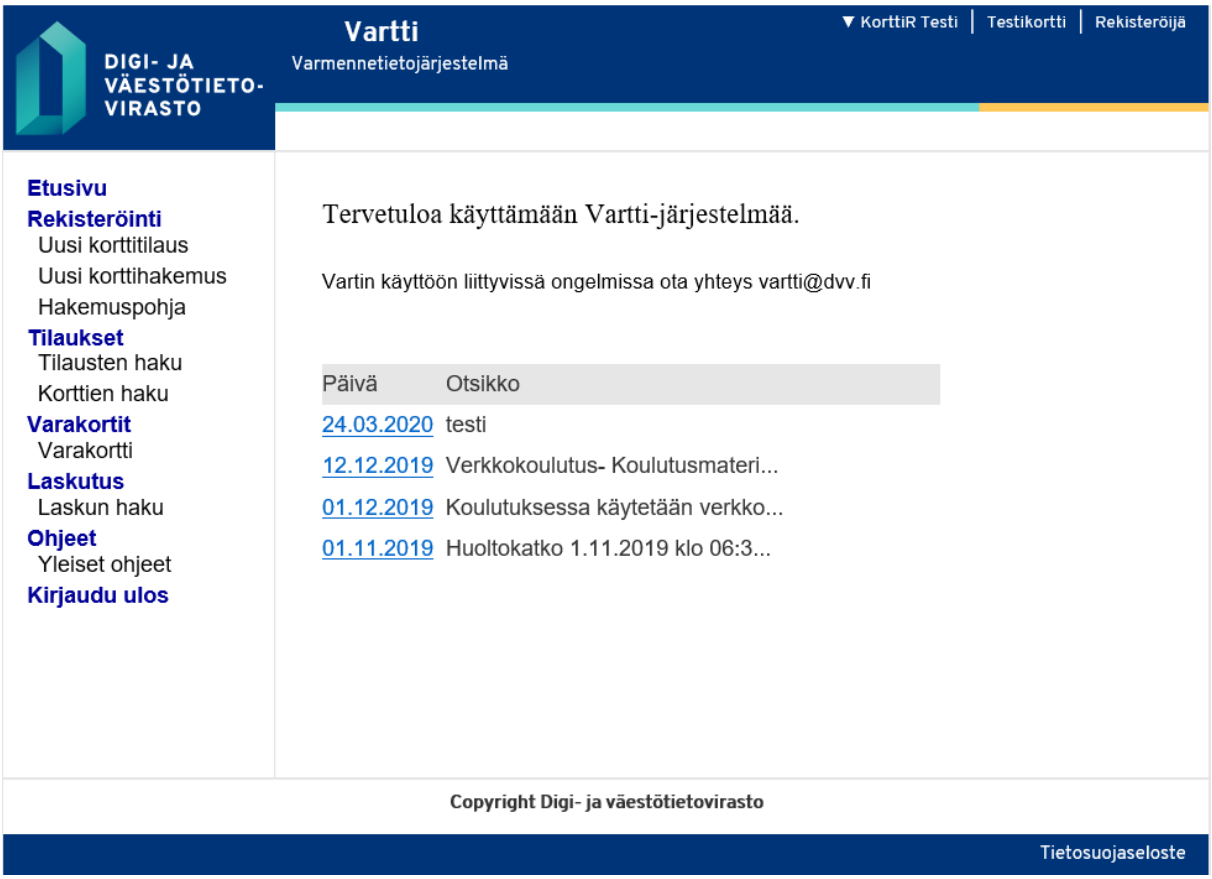
2.2.2 Testserver- och teste-postcertifikat

Testserver- och teste-postcertifikat kan användas för att testa informationssystemens funktion och utveckla applikationer för programmen.

Testservercertifikat möjliggör krypterad datakommunikation mellan en webbläsare och en server eller mellan två servrar. Användningsområden för teste-postcertifikatet är bland annat att öppna krypterade meddelanden och underteckna utgående e-postmeddelanden.

3 Allmän beskrivning av Vartti-systemet

I Vartti-systemet produceras tjänster för registrering, beställning, produktion och uppföljning av organisationskort och -certifikat samt tillfälliga kort. I Vartti-systemet identifieras användare med organisationscertifikat beviljat av MDB.



Figur 14 Vartti-startsida

3.1 Användning av systemet

Anslutning till tjänsten

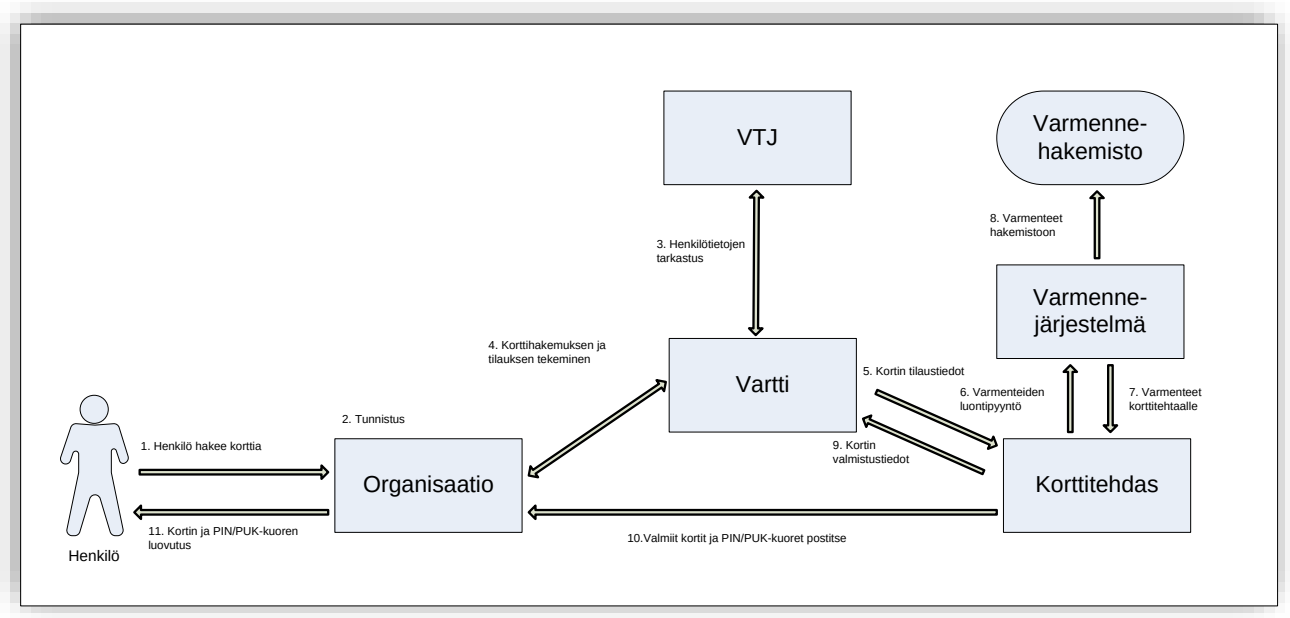
MDB och klienten ingår ett avtal om produktion av certifikattjänsterna i MDB:s e-tjänst. Efter att avtalet undertecknats beviljar MDB personer som utbildas för registreringsuppgifter inom organisationen (registrerare) behörighet till Vartti-systemet. Registrerarna i organisationen sköter registreringen av anställda, beställningen av kort och överlåtelsen av tillverkade kort till de anställda.

För produktionen överförs avtalets uppgifter från e-tjänsten till Vartti-systemet. Avtalets uppgifter är bl.a. organisationens namn, FO-nummer, besöks- och postadress, kontaktpersonernas namn, kundnummer och kundgrupp samt offentligrättsliga eller företagsekonomiska prestationsuppgifter.

MDB lägger också till uppgifter om de produkter som nämns i avtalet i Vartti-systemet.

Organisationen fungerar enligt överenskommelse som registrerare vid ansökan om organisationscertifikat. I kund- och registreringsavtalet som ingåtts med organisationen och avtalsprodukterna i anslutning till det fastställs hurdana kort som kan beställas på basis av avtalet, och vilka avtalsproduktspecifika uppgifter som kan läggas till i kortansökan.

Behandlingsprocessen för organisationskort och organisationscertifikat



Figur 15 Behandlingsprocess för organisationskort

1. En person ansöker om kort
2. Identifikation
3. Kontroll av personuppgifter
4. Kortansökan och beställning görs
5. Beställningsdata för kortet
6. Begäran om att certifikaten skapas
7. Certifikaten till kortfabriken
8. Certifikaten till katalogen
9. Tillverkningsdata för kortet
10. De färdiga korten och PIN/PUK-kuverten per post
11. Kortet och PIN/PUK-kuvertet överlämnas

3.2 Registrering och skapande av beställning

Den anställda ansöker om certifikatkort hos registreraren i sin organisation. Registreraren identifierar den arbetstagare som ansöker om kortet enligt avtalet med MDB och börjar fylla i kortansökan i Vartti-systemet.

Vartti-systemet hämtar den sökandes personuppgifter från Befolkningsdatasystemet.

Registreraren sparar kortansökan i Vartti-systemet och skapar en beställning av den.

Beställningsmaterial skapas för kortfabrikerna utifrån beställningar som gjorts i Vartti-systemet en gång per dygn.

3.3 Sökning av beställningsuppgifter och tillverkning av kort

Kortfabrikerna hämtar kortbeställningsuppgifterna från Vartti-systemet genom att använda en skyddad dataöverföringsförbindelse och returnerar uppgifter om att beställningsuppgifterna har hämtats till Vartti. Kortfabrikerna specificerar korten enligt beställningsuppgifterna.

Av beställningsuppgifterna bildar kortfabrikerna certifikatbegäran som skickas via ett slutet datakommunikationsnät till certifikatsystemet (DVV Organisational Certificates - G4R). Certifikatsystemet skapar organisationscertifikat för mottagna certifikatbegäran.

Kortfabrikerna tar emot organisationscertifikat som skapats av certifikatdatasystemet och sparar dem på chipet på organisationskorten.

Skapade organisationscertifikat publiceras i ett offentligt register där de är tillgängliga under hela sin giltighetstid. Organisationscertifikat behöver inte publiceras i registret, om så avtalas.

Kortfabrikerna returnerar tillverkningsuppgifterna för de tillverkade korten till Vartti-systemet via en skyddad datakommunikationsförbindelse.

3.4 Överlåtelse av organisationskort

Kortfabrikerna levererar organisationskort och aktiveringskoder som tillverkats utifrån beställningsmaterialet till klienten.

Organisationen överlåter kortet till kortinnehavaren och sparar kortets överlåtelseuppgifter i Varttisystemet. Brevet med aktiveringskoden skickas direkt till kortinnehavaren.

3.5 Spärrning av organisationscertifikat

Vid behov kan certifikatet spärras i spärrtjänsten. Spärrtjänsten betjänar dygnet runt alla dagar i året.

Om organisationskortet förkommer eller inte behövs ska certifikaten på kortet omedelbart anmälas till spärrtjänsten för att förhindra missbruk. Begäran om spärrning av certifikat kan meddelas av kortinnehavaren själv eller av den person inom organisationen som ansvarar för registreringen. Begäran om spärrning meddelas i första hand per telefon (0800 162 622). Uppgifterna i anslutning till anmälan om begäran om spärrning sparas.

I samband med ibruktagande av organisationscertifikat kommer man överens om frågor i anslutning till användningen av spärrtjänsten samt om anmälningsförfarandet för begäran om spärrning. Certifikatsystemet publicerar uppgifterna om spärrade certifikat (tidpunkt för spärrning och serienummer för spärrade certifikat) på spärrlistor som hämtas från det offentliga registret.

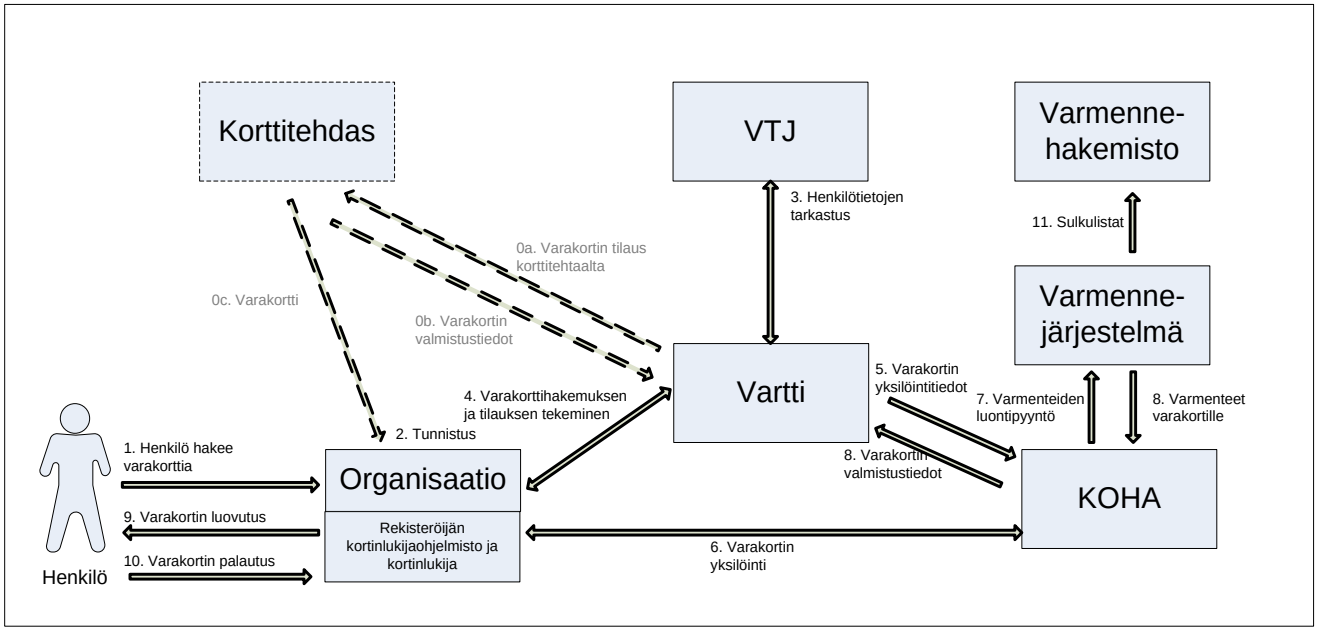
3.6 Tillfälliga kort och tillfälligt certifikat

Tillfälliga kortet och tillfälliga certifikat är avsedda för tillfälligt bruk i stället för ett kort som förkommit, glömts eller gått sönder. Organisationer kan använda ett tillfälligt kort till exempel i en situation där en anställd till exempel har tappat bort sitt kort och tillfälligt behöver ett ersättande kort. Tillfälliga kortet är en standardiserad lösning som omfattar ett visuellt färdigt definierat certifikatkort vars chip har formaterats, men inga certifikat har sparats på kortet. Registreraren sparar tillfälliga certifikat på chipet med hjälp av Vartti-systemet.

På tillfälliga kortet kan man förutom autentiseringscertifikatet även lagra ett signeringscertifikat. Tillfälliga certifikat på tillfälliga kort är identifieringsverktyg enligt lagen för stark autentisering och elektroniska signaturer.

Tillfälliga kort beställs till organisationen redan innan behovet för tillfällig användning har uppkommit (när registreringsstället grundas). Tillfälliga korten beställs via Vartti-systemet på samma sätt som organisationskort.

Behandlingsprocessen för tillfälliga kort



Figur 16 Behandlingsprocessen för tillfälliga kort

0a. Beställning av tillfälliga kort från kortfabriken
0b. Tillverkningsdata för tillfälliga kortet
0c. Tillfälliga kort

1. En person ansöker om tillfälligt kort
2. Identifikation
3. Kontroll av personuppgifter
4. Ansökan och beställning av tillfälliga kort görs
5. Tillfälliga kortets identifieringsuppgifter
6. Specificering av tillfälliga kortet
7. Begäran om att certifikaten skapas
8. Certifikaten till tillfälliga kortet
9. Tillfälliga kortet överlämnas
10. Tillfälliga kortet returneras
11. Spärrlistorna

Registreraren beställer via applikationen Vartti det antal tillfälliga kort som behövs. Tillfälliga korten kan levereras i samma försändelse eftersom chipsen inte har personuppgifter, koder, nycklar eller certifikat färdiga. Registrerarna ansvarar för administrationen av tillfälliga kort och tillfälliga certifikat på samma sätt som för organisationskort och organisationscertifikat. Det finns en separat instruktion för administration av tillfälliga kort.

Registreraren identifierar den anställda i organisationen och ansöker om ett tillfälligt certifikat för

denna via Vartti-systemet. Ett tillfälligt certifikat kan vara giltigt i högst 3 månader.

Med hjälp av en onlineförbindelse skapar registreraren ett tillfälligt certifikat för personen enligt uppgifterna i det redan beviljade organisationscertifikatet och sparar certifikatet på det tillfälliga kortets chip. Registreraren överlämnar reservkortet till arbetstagaren.

I samband med identifieringen skapas alltid nya nycklar till tillfälliga kortet. Kortinnehavaren väljer själv kortets koder. Dessa uppgifter raderas från chipet i samband med att tillfälliga kortet returneras.

Skapade tillfälliga certifikat publiceras inte i MDB:s offentliga certifikat katalogtjänst.

Registrerarna anmäler vid behov tillfälliga certifikat till spärrlistan. Notifikationen kan göras elektroniskt direkt via Vartti-systemet. Begäran om spärrning av ett tillfälligt kort kan också anmälas per telefon till spärrtjänsten.

Tillfälliga korten kan användas på nytt. När behovet av att använda tillfälliga certifikat har upphört spärras de tillfälliga certifikaten och tas bort från tillfälliga kortets chip. Därefter kan tillfälliga kortet överlämnas, dvs. specificeras på nytt för följande person.

4 Allmän beskrivning av stämpeltjänsten

MDB erbjuder kunderna en stämpeltjänst där organisationerna kan underteckna, dvs. stämpla data i digitalt format med ett stämpelcertifikat som beviljats organisationen. Stämpelcertifikatet innehåller uppgifter om en juridisk person. Objektet som stämplas kan vara vilken som helst digital data, till exempel avtal, utdrag, beslut eller annat elektroniskt dokument, till exempel attributintyg för en elektroniskt plånbok.

4.1 Ansökan om stämpelcertifikat och anslutning till tjänsten

MDB och kunden ingår ett avtal om ibruktagning av stämpelcertifikatet och stämpeltjänsten i MDB:s e-tjänst. Vid behov skickar organisationen en fullmakt till MDB i samband med att avtalet ingås. Organisationen har antecknat de personer som har rätt att ansöka om certifikat i organisationen i fullmakten. Efter att avtalet har undertecknats beviljar MDB de certifikat som behövs för att använda tjänsten. Därefter kan de som organisationen befullmäktigat börja stämpla dokumenten i stämpeltjänsten.

Stämpelcertifikat beviljas för högst 5 år åt gången. Stämpelcertifikatets giltighetstid kan avvika från ovan nämnda användningsändamål.

Ett avtal om stämpeltjänsten ingås i princip inte och certifikat utfärdas inte utanför EU- och EES-området, men MDB kan även göra undantag från detta från fall till fall.

4.2 Stämpling av elektroniska dokument i stämpeltjänsten

Man kan stämpla elektroniska dokument i stämpeltjänsten på två sätt:

- **Genom att stämpla hashsumman av det elektroniska dokumentet**. Då överförs endast hashsumman av det dokument som ska stämplas till stämpeltjänsten, där den stämplas och returneras till kunden. Att stämpla hashsummor är snabbt och varaktigt.

- **Genom att stämpla ett elektroniskt dokument.** Då överförs hela dokumentet till stämpeltjänsten, där det stämplas och därefter returneras till kunden. Hur snabbt stämplingen tar påverkas av organisationens nätförbindelse och storleken på det dokument som ska stämplas. Det dokument som ska stämplas fördröjs i tjänsten under stämplingen. Dokumentet sparas inte i stämpeltjänsten. Kunden ansvarar för att den har rätt att skicka ett dokument som ska stämplas till tjänsten.

Kunden meddelar i samband med ibruktagningen hur många stämpelcertifikat som ska beställas. Med ett stämpelcertifikat är det möjligt att stämpla både hashsummor och dokument.

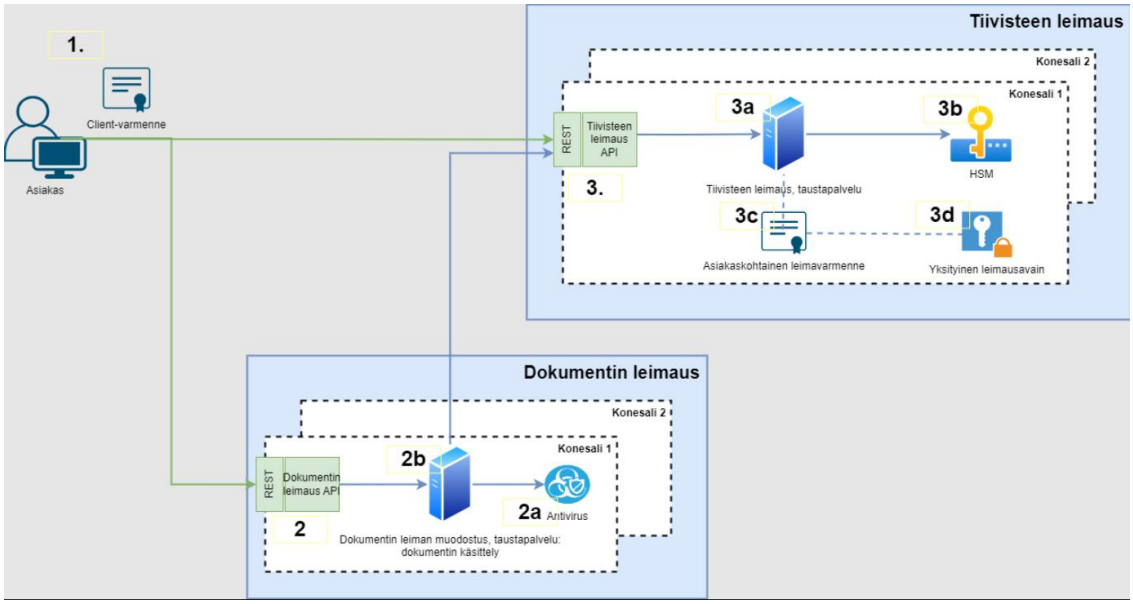
Behandling av personuppgifter

MDB är personuppgiftsansvarig för personuppgiftsbehandlingen i samband med ibruktagningen av stämpeltjänsten samt för personuppgiftsbehandlingen i anslutning till upprätthållandet av tjänsten. Registrerade är kundorganisationernas företrädare och kontaktpersoner.

Den kundorganisation som använder tjänsten är personuppgiftsansvarig i samband med stämplingen av det elektroniska dokumentet. MDB behandlar eventuella personuppgifter i de dokument som ska stämplas för de kundorganisationers räkning som använder tjänsten när ett elektroniskt dokument stämplas i tjänsten. MDB fungerar inte som personuppgiftsbiträde när en hashsumma av ett elektroniskt dokument stämplas i tjänsten.

4.3 Stämplingsprocessen

Stämpeltjänsten använder ett REST-gränssnitt. Närmare uppgifter finns i stämpeltjänstens gränssnittsbeskrivning, som finns i integreringsanvisningen. Signeringsnycklarna förvaras i en HSM-utrustning som uppfyller kraven FIPS 140-2 eller 140-3 nivå 3.



Figur 17: Stämpelprocessen av ett elektroniskt dokument eller hashsumma.

1. Kundens system skapar en begäran om stämpling. Kundens system identifierar sig i stämpeltjänstens gränssnitt med hjälp av stämpeltjänstens gränssnittscertifikatet.

2. Dokumentet och begäran om stämpling skickas till stämpeltjänsten med hjälp av REST-gränssnittet för stämpling av dokumentet.

a. Dokumentets stämpeltjänst utför en viruskontroll av dokumentet.

b. Dokumentets stämpeltjänst räknar ut en hashsumma av dokumentet och skapar en hashsumma för vidarebefordran av begäran om stämpling. När tjänsten får tillbaka den stämplade hashsumman bildar den det önskade digitalt stämplade dokumentet och returnerar det till kunden.

3. Begäran om stämpling av hashsumman skickas via REST-gränssnittet till stämpeltjänsten för hashsumma.

    a. Tjänsten granskar hashsummans syntax och stämplar hashsumman med hjälp av ett kundspecifikt stämpelcertifikat och dess privata nyckel.

    b. Kundens privata nycklar finns i säkerhetskalkylatorn (HSM).

    c. Det kan finnas ett eller flera stämpelcertifikat för kunden i tjänsten.

    d. Varje stämpelcertifikat har en privat nyckel för varje certifikat.

4.4 Spärrning av stämpelcertifikat och stämpeltjänstens gränssnittscertifikat

Avvikande från punkten Spärrtjänst i avtalet iakttas följande villkor vid spärrning av stämpelcertifikat:

Vid behov kan certifikatet spärras i spärrtjänsten. Spärrtjänsten betjänar dygnet runt alla dagar i året.

MDB ser till att stämpeltjänstens gränssnittscertifikat spärras när avtalet om stämpeltjänsten upphör eller när stämpelcertifikatets giltighet går ut. Spärrning av stämpelcertifikat avtalas separat. Om användaren av tjänsten vill spärra stämpelcertifikatet av någon annan anledning, ska stämpelcertifikatet anmälas till spärrtjänsten. Begäran om spärrning av ett certifikat kan anmälas av certifikatinnehavaren själv eller av en företrädare för den organisation som ingått serviceavtalet.

I samband med ibruktagande av stämpeltjänstens gränssnittscertifikat och stämpelcertifikat kommer man överens om frågor i anslutning till användningen av spärrtjänsten samt om anmälningsförfarandet för begäran om spärrning. Certifikatsystemet publicerar uppgifterna om spärrade certifikat (tidpunkt för spärrning och serienummer för spärrade certifikat) på spärrlistor som hämtas från det offentliga registret.

4.5 Teststämpeltjänst

Organisationerna kan om de så önskar testa att använda stämpeltjänsten i MDB:s teststämpeltjänst. I teststämpeltjänsten stämplas dokumenten med ett teststämpelcertifikat.

Användningen av teststämpeltjänsten förutsätter att organisationen ansöker om nyttjanderätt till teststämpeltjänsten och testcertifikat i MDB:s e-tjänst.

Ansökan om teststämpeltjänsten och anslutning till testtjänsten

Användning av teststämpeltjänsten förutsätter att organisationen skickar en ansökan om teststämpeltjänsten samt ansöker om ett teststämpelcertifikat och ett gränssnittscertifikat för stämpeltjänsten som är avsett för testanvändning. Ansökningarna skickas i MDB:s e-tjänst.

Certifikat som beviljats för testanvändning har en giltighetstid på 3 månader.

Spärrning av teststämpelcertifikat och gränssnittscertifikat som är avsett för testanvändning

Organisationen kan om de önskar spärra teststämpelcertifikatet innan dess giltighetstid går ut. Gränssnittscertifikatet som är avsett för testanvändning ska spärras om behovet av dess användning upphör innan certifikatets giltighetstid på tre månader löper ut.

Frågor gällande användningen av spärrtjänsten och anmälningsförfarandet för spärrbegäran avtalas i samband med idrifttagandet av teststämpeltjänstens teststämpelcertifikat och gränssnittscertifikat som utfärdas för testanvändning.

5 Beställnings- och administrationsprocesser utanför Vartti-systemet

5.1.1 Processen för beställning och administration av servercertifikat

Servercertifikaten söks via e-tjänsten. Mer information om e-tjänsten på adressen https://dvv.fi/sv/e-tjanster.

På ansökningsblanketter laddar kunden upp en begäran om servercertifikat som hen skapat. Servercertifikatet skapas i enlighet med den. Innan certifikatet beviljas kontrollerar MDB den sökandens uppgifter. Uppgifter som ska kontrolleras är bland annat besittningsrätten till det domännamn som anges i ansökan. Det beviljade servercertifikatet skickas till kunden per e-post.

Det skapade servercertifikatet publiceras i certifikat katalogtjänsten, där det finns tillgängligt under certifikatets giltighetstid.

Servercertifikatets giltighetstid är högst 1 år. Certifikatets pris är en årsavgift enligt serviceprislistan. Årsavgifterna för servercertifikatet tas ut på förhand.

5.1.2 Processen för beställning och administration av systemsignaturcertifikat

Myndigheten för digitalisering och befolkningsdata kan på ansökan bevilja systemsignaturcertifikat som söks via e-tjänsten. Mer information om e-tjänsten på adressen https://dvv.fi/sv/e-tjanster.

Systemsignaturcertifikatet ansöks enligt den praxis som MDB fastställt och vid beviljandet av certifikatet iakttas relevanta bakgrundskontroller.

Systemsignaturcertifikatet skapas på basis av ansökan och skickas till kunden som krypterad e-post.

Systemsignaturcertifikat beviljas för högst två år.

5.1.3 Processen för beställning och administration av e-postcertifikat

Myndigheten för digitalisering och befolkningsdata kan på ansökan bevilja e-postcertifikat som söks via e-tjänsten. Mer information om e-tjänsten på adressen https://dvv.fi/sv/e-tjanster.

E-postcertifikatet ansöks enligt den praxis som MDB fastställt och vid beviljandet iakttas samma bakgrundskontroller som vid ansökan om servercertifikat. E-postcertifikatet är inte avsett för personlig e-post, utan för e-post som är i gemensamt bruk, till exempel kirjaamo@xxx.fi.

E-postcertifikatet skapas på basis av ansökan och skickas till kunden som krypterad e-post.

E-postcertifikat beviljas för högst två år.

5.1.4 Register över certifikat beviljade av MDB, spärr- och rådgivningstjänst

Certifikatsökning

I certifikat katalogtjänsten kan du ladda ner certifikat som utfärdats av Myndigheten för digitalisering och befolkningsdata och spärrlistor för certifikaten. Certifikat katalogtjänsten innehåller certifikattyper som beviljats för flera olika användningsändamål. Certifikat katalogtjänst är en offentlig tjänst på adressen https://dvv.fi/sv/certifikat-katalogtjanst och kräver inga användarnamn eller lösenord.

Spärrtjänst för certifikat

Om organisationskortet förkommer eller inte behövs ska certifikaten på kortet omedelbart anmälas till spärrtjänsten för att förhindra missbruk. Spärrtjänsten betjänar dygnet runt alla dagar i året. Spärrtjänstens servicespråk är finska, svenska och engelska.

Spärrtjänstens kontaktinformation

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

Rådgivningstjänst för certifikat

Rådgivningstjänsten ges per telefon stöd för användning av certifikat och rådgivning vid de vanligaste problemen vid ibruktagande, som användning och byte av PIN-koder samt upplåsning av en låst PIN-kod. Rådgivningstjänsten är öppen vardagar kl. 8–21 och lördagar kl. 9–15 Rådgivningstjänstens servicespråk är finska, svenska och engelska.

Rådgivningstjänstens kontaktinformation

- 0600 9 6160 (lna/msa)

5.1.5 Certifikatens testtjänst och kontroll av PDF-dokumentets underskrift

Certifikatens testtjänst

I certifikatens testtjänst kan du testa certifikatet och kortläsaren och pröva på hur man gör en elektronisk signatur. Certifikatens testtjänst kan användas med alla certifikatkort som beviljats av Myndigheten för digitalisering och befolkningsdata. Tjänsten finns på adressen https://dvv.fi/sv/testning-av-certifikat

Kontroll av signatur i PDF-dokument

Autenticiteten hos elektroniska signaturer i PDF-dokument kan kontrolleras i tjänsten för granskning av PDF-dokument som tillhandahålls av Myndigheten för digitalisering och befolkningsdata.

Tjänsten tar ställning till

- signaturens tekniska giltighet och juridiska ställning
- riktigheten hos den undertecknande personen eller organisationen.

Tjänsten tar inte ställning till innehållets tillförlitlighet eller till exempel den undertecknande personens eller organisationens behörighet. Tjänsten finns på adressen https://dvv.fi/sv/granska-pdf-dokument

Versionshantering

versions nr	vad som har gjorts	datum/person
1.0	Lade till versionshantering och stycke 4.*5 Teststämpeltjänst.*	4.4.2024/AG