Certifikattjänster

18.3.2024

Användningsvillkor för organisationskortet

Allmänt

Myndigheten för digitalisering och befolkningsdata (MDB) är en myndighet som upprätthåller ett personregister och producerar stödtjänster för e-tjänster, notarius publicus-tjänster och juridisk bekräftelse samt förmyndarverksamhetens tjänster, och vars uppgift enligt lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata (661/2009) också är att producera tjänster inom certifierad elektronisk kommunikation. Sedan 1.12.2010 har myndigheten (Befolkningsregistercentralen (BRC) fram till 31.12.2019) varit lagstadgad certifikatutfärdare för hälso- och sjukvården och sedan 1.4.2015 för socialvården (lag om elektronisk behandling av kunduppgifter inom social- och hälsovården (784/2021), lag om elektroniska recept (61/2007) och lag befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata (661/2009)).

Myndigheten för digitalisering och befolkningsdata beviljar certifikatkort och certifikat för organisationer och samfund.

MDB:s verksamhet i egenskap av leverantör av elektroniska identifieringstjänster och myndighet som tillhandahåller betrodda tjänster regleras av Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (s.k. eIDAS-förordningen), som trädde i kraft i september 2014. eIDAS-förordningen är direkt tillämplig rätt i medlemsstaterna och har tillämpats från och med 1.7.2016.

Ovan nämnda EU-förordning kompletteras av kommissionens genomförandeförordning (EU) 2015/1502 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (s.k. förordningen om tillitsnivåer vid elektronisk identifiering). När en tjänsteleverantör uppfyller kraven i förordningen om tillitsnivåer profilerar sig tjänsteleverantören i Finland i fråga om elektroniska identifieringstjänster som en tjänsteleverantör/leverantör av starka elektroniska identifieringstjänster med förhöjd eller hög tillitsnivå.

I den nationella lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) föreskrivs om tillhandahållande av tjänster för stark autentisering och betrodda elektroniska tjänster, bl.a. elektronisk signatur och deras rättsverkningar. Lagen har reviderats så att den motsvarar kraven i eIDAS-förordningen och ändringarna trädde i kraft 1.7.2016.

Organisationscertifikat som ingår i organisationskortet kan användas för stark autentisering av en person, kryptering av information och för elektroniska signaturer. Autentiserings- och krypteringscertifikatet uppfyller kraven på identifieringsverktyg för stark autentisering på nivån ”hög” enligt eIDAS-förordningen. Ett signaturcertifikat som endast är avsett för att genomföra signaturer uppfyller kraven på ett godkänt signaturcertifikat enligt eIDAS-förordningen. Myndigheten för digitalisering och befolkningsdata garanterar identiteten hos den som ansöker om ett certifikat.

Ett organisationscertifikat kan vara i kraft i högst fem år.

Ibruktagandet av organisationskortets elektroniska egenskaper förutsätter att organisationscertifikatet aktiveras.

Ansökan om organisationskort

Ansökan om organisationscertifikat förutsätter personligt besök hos ett registreringsställe. Uppgifterna i ansökan registreras i certifikatutfärdarens certifikatdatasystem.

En ansökan om organisationscertfikat godkänns i och med utfärdandet av certifikatet. Om förutsättningar för att utfärda certifikatet saknas för sökandens del, kan certifikatet inte utfärdas och ansökan avslås. Sökanden delges beslutet omedelbart och sökanden kan då göra en skriftlig yrkan på ändring av beslutet som riktas till certifikatutfärdaren.

Vid ansökan om certifikat kontrolleras identiteten av den som söker organisationskort med hjälp av en giltig, av polisen utfärdad identitetshandling, dvs. identitetskort (som utfärdats efter 1.3.1999) och pass. Godtagbara identifieringshandlingar är också ett giltigt pass eller identitetskort som utfärdats av myndighet i en medlemsstat inom EES, Schweiz eller San Marino eller ett giltigt pass som utfärdats av myndighet i något annat land. Om sökanden inte har nämnda handlingar ska polisen kontrollera sökandens identitet på annat sätt.

Det är också möjligt att ansöka om ett nytt certifikat när det föregående certifikatet går ut, om förutsättningarna för utfärdande fortfarande gäller. Vid ansökan om ett nytt certifikat iakttas samma rutiner som vid första ansökan om certifikat. Endast certifikatinnehavaren kan ansöka om nytt certifikat.

Man kan också ansöka om ett nytt certifikat när certifikatinnehavarens uppgifter som påverkar certifikatets innehåll förändras eller när certifikatkortet går sönder. Då ska certifikatinnehavaren kontakta registreringsstället och ansöka om ett nytt certifikatkort och ett nytt certifikat.

Certifikatutfärdaren levererar följande till sökanden:

• ett organisationskort som innehåller kortinnehavarens personliga nyckelpar och certifikat

• ett aktiveringskodskuvert, med vars hjälp innehavaren av organisationskortet ställer PIN1-(autentiserings- och krypteringscertifikat) och PIN2-koden (signaturcertifikat) på kortet.

Dessutom ger registreraren certifikatsökanden en guide för användning av certifikatkort.

Det brev med aktiveringskoder som behövs för att ta i bruk organisationscertifikatet postas antingen till sökandens hemadress eller organisationen adresserat till kortsökanden cirka fyra dagar efter att kortet postats.

Ibruktagande av organisationscertifikatet

Ibruktagandet av de elektroniska egenskaperna av organisationscertifikatet på organisationskortet förutsätter att kortet aktiveras med hjälp av aktiveringskoden. För att kunna använda ett organisationscertifikat behöver man utöver organisationskortet och aktiveringskoden även en dator, en kortläsare och ett kortläsarprogram. Organisationscertifikatet aktiveras med hjälp av kortläsarprogrammet mPollux Digisign Client. Du kan ladda ner det nyaste kortläsarprogrammet gratis på adressen https://dvv.fi/sv/kortlasarprogram.

Kortläsarprogrammet inleder aktiveringsprocessen automatiskt när organisationskortet placeras i kortläsaren för första gången. Med hjälp av aktiveringskoden skapar användaren två personliga PIN-koder för certifikatet, dvs. baskoden (PIN1) och signaturkoden (PIN2). Med PIN1-baskoden kan användaren identifiera sig i tjänsterna och med PIN2-signaturkoden kan användaren göra en elektronisk signatur.

Detaljerade anvisningar för ibruktagandet av organisationscertifikatet finns på MDB:s webb-plats https://dvv.fi/sv/ta-i-bruk-certifikatkortet.

Rådgivningstjänsten för certifikat betjänar per telefon från måndag till fredag kl. 8–21 och på lördagar kl. 9–15 på telefonnumret 0600 96160 (lna/msa). Tjänsten är stängd på söndagar och söckenhelger. Rådgivningstjänsten betjänar på finska, svenska och engelska.

Hantering av PIN-koder

Anvisningar för hur man öppnar en låst PIN-kod och byter PIN-kod finns på MDB:s webb-plats https://dvv.fi/sv/hantering-av-pin-koder. Om aktiveringskoden försvinner, kan man beställa en ny aktiveringskod i samband med ett personligt besök vid organisationens eget registreringsställe.

Ansvar för förvaring av organisationskortet

Organisationskortet och dess aktiveringskod får endast användas av kortinnehavaren.

Innehavaren av certifikatet ska omsorgsfullt förvara och hantera sina certifikat och nyckelpar samt tillhörande koder och certifikatkort. Certifikatinnehavaren ska se till att certifikatkortet inte försvinner och att koderna inte röjs eller används på ett otillåtet sätt.

PIN-koder som används för aktivering av nycklar får inte förvaras på samma plats som certifikatkortet. Vid misstanke om att koderna råkat i händerna på utomstående ska certifikatinnehavaren byta PIN-koder.

Certifikatinnehavarens ansvar för användningen av certifikatet upphör när han eller hon anmält behövliga uppgifter till spärrtjänsten för spärrningen av certifikatet och fått ett meddelande av den tjänsteman som tog emot samtalet att spärrningen har gjorts. Närmare anvisningar om spärrning av certifikatet finns under punkten Annullering av certifikat på organisationskortet. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats att skäl för anmälan föreligger.

Kortinnehavaren ska ta hand om organisationskortet i enlighet med dessa användarvillkor och i enlighet med den godkända certifikatpolicyn som är offentligt tillgänglig. Organisationskortet ska förvaras omsorgsfullt på ett sådant sätt att det inte hamnar i utomståendes besittning, att det inte ändras och att det inte används utan tillstånd. Ett förfarande som strider mot denna bruksanvisning frigör Myndigheten för digitalisering och befolkningsdata från eventuella ansvar i anslutning till användningen av organisationskortet.

Ansvar av organisationskortets innehavare

Organisationscertifikatet innehåller ett certifikat för identifiering av en person i enlighet med den europeiska eIDAS-förordningen (910/2014) och ett kvalificerat certifikat för elektroniska signaturer.

Innehavaren av ett organisationskort ska förbinda sig till att följa certifikatpolicyn när han eller hon ansöker om och använder organisationscertifikatet. Certifikatinnehavaren svarar för att de uppgifter som anges vid ansökan om certifikatet är korrekta.

Rättigheterna och skyldigheterna av den som ansöker om organisationscertifikat är tillgängliga innan ansökan om organisationscertifikat undertecknas i användarguiden för certifikatkort (https://dvv.fi/sv/ta-i-bruk-certifikatkortet), i användarvillkoren för certifikatkortet och certifikatpolicyn (https://dvv.fi/sv/certifikatpolicydokument), där båda parters (certifikatutfärdarens och certifikatinnehavarens) rättigheter och skyldigheter beskrivs. När sökanden ansöker om organisationscertifikat godkänner han eller hon samtidigt de allmänna användarvillkoren och förbinder sig till att använda certifikaten i enlighet med anvisningarna.

I ansökningshandlingen och i användarvillkoren nämns tydligt att den som ansöker om ett organisationscertifikat intygar riktigheten av de givna uppgifterna med sin underskrift samt godkänner att organisationscertifikatet skapas och publiceras enligt avtalet som ingåtts med kundorganisationen eller i en offentlig katalogtjänst. På samma gång godkänner sökanden reglerna och villkoren i anslutning till användningen av organisationscertifikatet och förbinder sig till att förvara organisationscertifikatet och PIN-koderna omsorgsfullt samt att anmäla eventuellt missbruk eller ett försvunnet kort.

Organisationscertifikatet är innehavarens elektroniska identitet och får därför inte överlåtas att användas av någon annan.

Innehavaren av organisationscertifikatet svarar för användningen av certifikatkortet, de rättshandlingar som företas med stöd av kortet och deras ekonomiska följder.

Kortinnehavaren får inte lämna sitt certifikatkort i kortläsaren utan tillsyn och inte i något fall låta någon annan använda det.

Om ett kort som innehåller ett chip blir kvar i en kortläsare finns det risk för missbruk av organisationscertifikatet. När en terminalsession avslutas eller terminalen lämnas utan tillsyn ska certifikatinnehavaren avlägsna chipet med certifikatet från avläsaren och på föreskrivet sätt stänga de program som har använts eller annars avbryta den tekniska förbindelse som behövs för användningen av organisationscertifikatet.

Om ett certifikatkort skadas, ska kortinnehavaren spärra de certifikat som ingår i det skadade kortet och ansöka om ett nytt kort från registreringsstället. Vid ansökan om nytt certifikatkort iakttas samma rutiner som vid första ansökan om kort och certifikat.

Certifikatinnehavaren ska informera spärrtjänsten om certifikatkortet försvinner eller om han eller hon misstänker missbruk.

Om koden är låst och den PUK-kod/aktiveringskod som behövs för upplåsningen har försvunnit, ska kortinnehavaren ta kontakt med sin organisations registreringsställe för att få tillgång till PUK-/aktiveringskoden.

Ansvar hos Myndigheten för digitalisering och befolkningsdata

Skadeståndsansvaret hos Myndigheten för digitalisering och befolkningsdata i anslutning till produktionen av certifikattjänster bestäms enligt det avtal som ingåtts med kundorganisationen. Myndigheten för digitalisering och befolkningsdata omfattas av certifikatutfärdarens skadeståndsansvar enligt lagen om stark autentisering och betrodda elektroniska

tjänster. Vidare tillämpas lämpliga delar av skadeståndslagen (412/1974) och lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003).

Myndigheten för digitalisering och befolkningsdata svarar som utfärdare för säkerheten för hela certifikatsystemet. Utfärdaren svarar för införskaffade tjänster på samma sätt som om utfärdaren själv hade producerat tjänsten.

Myndigheten för digitalisering och befolkningsdata ansvarar för att organisationscertifikatet har skapats med iakttagande av de förfaranden som anges i lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster (661/2009), lagen om stark autentisering och betrodda elektroniska tjänster, lagen om elektronisk kommunikation i myndigheternas verksamhet och certifikatpolicyn samt certifieringspraxisen och i enlighet med de uppgifter som certifikatsökanden har gett. Myndigheten för digitalisering och befolkningsdata svarar endast för de uppgifter som den har lagrat på organisationscertifikatet.

Myndigheten för digitalisering och befolkningsdata ansvarar för att organisationscertifikatet, när det används på behörigt sätt, kan användas från överlåtelsetidpunkten under hela dess giltighetstid, om det inte finns upptaget på spärrlistan. Organisationscertifikatet har överlåtits till en person som identifierats på det sätt som organisationscertifikatet förutsätter. Certifikatinnehavaren har utlämnats bruksanvisningar i anslutning till användningen av organisationscertifikatet.

Genom att skapa certifikatet och underteckna organisationscertifikatet med sin hemliga nyckel intygar certifikatutfärdaren att personuppgifterna i organisationscertifikatet har kontrollerats på det sätt som beskrivs i certifikatpolicyn och certifieringspraxisen.

Utfärdaren svarar för att rätt persons organisationscertifikat införs på spärrlistan och att de tas upp på spärrlistan inom den tid som anges i certifieringspolicyn.

Begränsningar i ansvaret hos Myndigheten för digitalisering och befolkningsdata

Myndigheten för digitalisering och befolkningsdata ansvarar inte för skador som uppstår till följd av att PIN-koder, PUK- eller aktiveringskoden och organisationscertifikatinnehavarens privata nycklar röjs, om inte avslöjandet direkt beror på myndighetens omedelbara verksamhet.

Myndighetens ansvar gentemot innehavare av organisationscertifikat och förlitande parter omfattar högst de direkta skador som har orsakats dem, om skadan beror på myndighetens omedelbara åtgärder.

Myndigheten för digitalisering och befolkningsdata svarar inte för indirekta skador eller följdskador som har orsakats innehavaren av organisationscertifikatet. Myndigheten ansvarar inte heller för eventuella indirekta skador eller följdskador som orsakas förlitande parter eller andra avtalsparter till innehavaren av organisationscertifikatet.

Myndigheten för digitalisering och befolkningsdata svarar inte för funktionen i de allmänna teleförbindelserna eller datanäten, till exempel internet, eller för att en rättshandling inte kan utföras på grund av att den utrustning eller programvara som innehavaren av organisationscertifikatet använder inte fungerar eller för att organisationscertifikatet används i strid med sitt användningsändamål.

Certifikatutfärdaren har rätt att avbryta tjänsten för den tid ändringar eller underhåll av systemet utförs. Om ändringar eller underhåll av spärrlistan meddelas på förhand.

Certifikatutfärdaren har rätt att vidareutveckla certifikattjänsten. Innehavare av organisationscertifikat eller förlitande parter ska i sådana fall svara för egna kostnader som följer av detta och utfärdaren är inte skyldig att ersätta innehavare av organisationscertifikat eller förlitande parter för kostnader som orsakas av utvecklingsarbetet.

Certifikatutfärdaren svarar inte vid användningen av certifikatet för fel i en e-tjänst eller applikation som grundar sig på certifikatet och som är avsedd för certifikatinnehavaren och organisationen eller för kostnaderna för felen.

Certifikatutfärdaren svarar inte för skador som orsakas av sådan verksamhet som strider mot lag, certifikatpolicy, certifieringspraxis eller andra anvisningar som gäller certifikatinnehavaren eller organ som använder certifieringssystemet.

Force majeure

Utfärdaren svarar inte för skador som orsakas av naturkatastrofer eller andra motsvarande oöverstigliga förhållanden.

Spärrning/annullering av certifikat på organisationskortet

Certifikaten på organisationskortet spärras genom att ringa spärrtjänsten 0800 162 622 (avgiftsfri när man ringer från Finland), vid samtal från utlandet +358 800 162 622 (+ den lokala operatörens avgift).

Behörig att begära spärrning av certifikat är:

- innehavaren av organisationskortet och dennes lagstadgade företrädare vad gäller personens eget certifikat,
- utfärdaren då förutsättningarna nedan uppfylls.

Ett certifikat spärras om:

- innehavaren av certifikatet begär att certifikatet spärras
- innehavaren av certifikatet byter arbetsplats
- Certifikatkortet skadas, försvinner eller blir stulet
- nyckelkoden och certifikatkortet har försvunnit eller blivit stulna
- certifikatinnehavaren har avlidit.

Certifikatinnehavaren ska utan dröjsmål lämna en begäran om spärrning till spärrtjänsten, om de ovan nämnda förutsättningarna för spärrning uppfylls.

Certifikatutfärdaren kan spärra ett organisationscertifikat om certifikatet har använts i strid med certifikatpolicyn, certifieringspraxisen, lagen om elektronisk behandling av kunduppgifter inom social- och hälsovården, lagen om elektroniska recept eller bestämmelser som

utfärdats med stöd av dessa lagar eller krav och anvisningar som fastställts utifrån bestämmelserna.

Det är inte tillåtet att använda eller försöka använda ett certifikat efter att begäran om spärrning har gjorts.

Myndigheten för digitalisering och befolkningsdata spärrar också certifikat ifall fel upptäcks i datainnehållet.

Myndigheten för digitalisering och befolkningsdata kan spärra certifikat som signerats med myndighetens hemliga nyckel om det finns anledning att misstänka att myndighetens hemliga nycklar har röjts eller råkat i fel händer.

Samtliga giltiga certifikat som utfärdats med den röjda nyckeln ska spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast spärrade certifikatets giltighetstid har löpt ut.

Om en privat nyckel eller annan teknisk metod som Myndigheten för digitalisering och befolkningsdata använder vid skapandet av certifikat har röjts eller annars blivit oanvändbar, ska Myndigheten för digitalisering och befolkningsdata underrätta alla kortinnehavare och Transport- och kommunikationsverket (Traficom) som fungerar som tillsynsmyndighet om händelsen på behörigt sätt.

Myndigheten för digitalisering och befolkningsdata kan spärra ett certifikat av särskild anledning.

Information om behandling av uppgifter

Vid behandling av privata uppgifter i certifikatutfärdarens system följs lagstiftningen om behandling av personuppgifter och integritetsskydd, bl.a. lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster (661/2009), EU:s allmänna dataskyddsförordning (EU) 2016/679 och dataskyddslagen (1050/2018). Vid behandlingen av offentliga uppgifter inom certifikatutfärdarens system iakttas lagen om offentlighet i myndigheternas verksamhet (621/1999). Certifikatutfärdaren svarar för att den privata information som behandlas i utfärdarens system skyddas mot obehörig behandling. Utlämningen av uppgifter till myndigheter sker med stöd av lagar och förordningar eller föreskrifter som meddelats med stöd av dem.

Personens identifikationskod och andra uppgifter som anmälts i ansökan sparas i MDB:s certifikatsystem. Autentiseringskoderna på organisationskortet och personens identifikationskod lagras också i MDB:s offentliga katalogtjänst (https://dvv.fi/sv/certifikat-katalogtjanst), om inte annat överenskommits med kundorganisationen. Alla har möjlighet att få uppgifter från den offentliga katalogtjänsten på det sätt som föreskrivs i lagen om offentlighet i myndigheternas verksamhet. Arkiveringstiden är kortets giltighetstid utökad med fem år.

Personuppgiftsansvarig och beskrivningar

Organisationskortets personuppgifter samlas in i följande system: befolkningsdatasystemet, certifikatsystemet och spärrlistan. MDB och Statens ämbetsverk på Åland är registeransvariga för befolkningsdatasystemet, MDB för certifikatsystemet och spärrlistan.

Beskrivningar av registren har utarbetats i enlighet med dataskyddslagen, och kan läsas här https://dvv.fi/sv/dataskyddsbeskrivningar.

Dataskyddsbeskrivningarna för MDB:s tjänster och register anger i detalj, hur, var och varför personuppgifter behandlas.

Certifikatets datainnehåll

På organisationscertifikat som utfärdas av Myndigheten för digitalisering och befolkningsdata registreras:

- Certifikatinnehavarens identifikationskod (tidigare SV-nummer)
- Certifikatets serienummer
- Certifikatinnehavarens för- och efternamn
- UPN-fält
- Organisationens namn
- Certifikatets giltighetstid
- Titel (valfri uppgift)
- Organisationsenhet (valfri uppgift)

Närmare tekniska definitioner av certifikatens datainnehåll finns på adressen https://dvv.fi/sv/fineid-specifikationer.

Uppgifterna på certifikatet och deras riktighet bekräftas med certifikatutfärdarens elektroniska signatur.

Certifikatutfärdaren publicerar certifikatutfärdarens certifikat och spärrlistor i ett avgiftsfritt och allmän tillgänglig offentlig katalogtjänst. Beroende på certifikatet och/eller avtalet som ingåtts med kundorganisationen publicerar utfärdaren beviljade autentiserings och krypteringscertifikat antingen i det offentliga eller icke-offentliga katalogtjänsten. Signaturcertifikat publiceras inte i katalogtjänsten.

Genomförande av granskningsrätt och rättelse i enlighet med dataskyddslagstiftningen

Certifikatinnehavaren har rätt att få uppgifter som rör honom eller henne själv, t.ex. personuppgifter, i enlighet med gällande lagstiftning.

I Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), dataskyddslagen (1050/2018) och lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata (661/2009) föreskrivs det om den registrerades rätt att kontrollera sina egna registeruppgifter och om den registrerades rätt att förbjuda att den personuppgiftsansvarige behandlar den registrerades uppgifter samt om rättelse av fel. Begäran om insyn i och rättelse av uppgifter i enlighet med dataskyddslagstiftningen riktas till den registeransvariga för respektive register.

Den personuppgiftsansvariges ansvar och behandling av personuppgifter

Vid behandlingen av privat information inom certifikatutfärdarens system iakttas lagstiftningen om behandling av personuppgifter och integritetsskydd. Vid behandlingen av

offentliga uppgifter inom certifikatutfärdarens system iakttas lagen om offentlighet i myndigheternas verksamhet (621/1999). Certifikatutfärdaren svarar för att den privata information som behandlas i utfärdarens system skyddas mot obehörig behandling. Utlämningen av uppgifter till myndigheter sker med stöd av lagar och förordningar eller föreskrifter som meddelats med stöd av dem.

Tilläggsuppgifter om organisationskortet

Certifikatpolicydokument som gäller organisationskortet finns på adressen https://dvv.fi/sv/certifikatpolicydokument

MDB:s identifieringsprinciper finns på adressen https://dvv.fi/sv/certifikat

Programmet för ändring av PIN-koder och upplåsning av spärrade koder (mPollux DigiSign Client) kan laddas ner gratis på adressen https://dvv.fi/sv/kortlasarprogram

Förfarande för klagomål och avgörande av tvister

Ett organisationskort som utfärdats av MDB på ansökan är bevis på ett positivt förvaltningsbeslut, avslag på ansökan om organisationskort är bevis på ett negativt förvaltningsbeslut. Till MDB:s beslut bifogas en anvisning om rättelseyrkande och en besvärsanvisning.

Den som är missnöjd med MDB:s beslut kan yrka på rättelse av beslutet hos MDB. Rättelseyrkandet till MDB ska göras skriftligen. Rättelseyrkandet kan formuleras fritt, men ska innehålla de ärenden och bilagor som nämns i anvisningen om rättelseyrkande och besvärsanvisningen.

Den som fortfarande är missnöjd med ett beslut som fattats i rättelseförfarandet kan överklaga beslutet hos förvaltningsdomstolen. Ändring söks genom skriftliga besvär hos förvaltningsdomstolen. Besvären kan formuleras fritt, men ska innehålla de ärenden och bilagor som nämns i anvisningen om rättelseyrkande och besvärsanvisningen. Besvären riktas till den förvaltningsdomstol inom vars domkrets MDB är belägen. Besvärstiden börjar löpa från den tidpunkt när besvärsanvisningen på tillbörligt sätt har fogats till beslutet och delgivits sökanden.

Med stöd av registreringsavtalet behandlas meningsskiljaktigheter som gäller avtalet och som i förhandlingarna mellan Parterna inte leder till förlikning i Helsingfors tingsrätt på finska. Inom statsförvaltningen avgörs meningsskiljaktigheter genom förhandlingar.