MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

CERTIFIKATBESKRIVNING SOCIAL HÄLSO YRKESCERTIFIKAT

för yrkescertifikat för social- och hälsovården

13.9.2025

Tel. **0295 536 000** (växel) | Kontaktuppgifter, se **www.dvv.fi/sv**

13.9.2025

Dokumenthantering

Ägare	
Utarbetats av	Ville Aarnio, Anniina Tamminen
Granskats av	
Godkänts av	Mikko Pitkänen

Versionshantering

versions nr	vad som har gjorts	datum/person
v. 1.0	Versio 1.0	1.6.2021/VA
v. 1.1	Tillagd information om loggdata	1.10.2021/VA
v 1.2	Uppdaterade versionen och länkarna till CPS dokument	30.9.2022/SK
v 1.3	Uppdaterade versionen. Raderade delen som nämnde PUK-kod och körkort som godkänd handling.	15.9.2023/AT
v 1.4	Uppdaterade versionen och datumet. Förenade politikerna för G3- och G2-rotcertifikathierarkierna till ett och samma dokument. Lade till force majeure till stycke 2.6.	13.9.2024/JH
v 1.5	Uppdaterade versionen och datumet.	13.9.2025/JH

13.9.2025

Innehållsförteckning

1 Inledning

Detta dokument är ett sammandrag av Myndigheten för digitalisering och befolkningsdatas (nedan MDB) certifikatpolicy för yrkescertifikat för social- och hälsovården. I certifikatpolicyn beskrivs förutsättningarna, tillämpningsområdet och begränsningarna för Myndigheten för digitalisering och befolkningsdatas certifieringsåtgärder inom den öppna nyckeltekniken. Principerna i certifikatpolicyn definieras på praktisk nivå i certifieringspraxisen och i andra uppförandekoder som kompletterar certifikatpolicyn.

Denna certifikatbeskrivning hänför sig till dokumenten:

Certifikatpolicy för yrkescertifikat för social- och hälsovården, OID: 1.2.246.517.1.10.206, 1.2.246.517.1.10.306 och 1.2.246.517.1.10.306.

Certifieringspraxis för yrkescertifikat för social- och hälsovården, OID: 1.2.246.517.1.10.206.1, 1.2.246.517.1.10.306.1 och 1.2.246.517.1.10.306.1.

Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (Förordningen) tillämpas på signeringscertifikat inom betrodda tjänster från och med den 1 juli 2016. I detta dokument fastställs kraven på verksamheten och förvaltningspraxisen hos dem som utfärdar autentiserings- och signeringscertifikat enligt Förordningen. I kraven på förfaringssätt i detta dokument beskrivs användningen av anordningar för signaturframställning.

När det gäller signaturcertifikat som tillhandahålls allmänheten iakttar Myndigheten för digitalisering och befolkningsdata en certifikatpolicy förenlig med betrodda tjänster i Förordningen ((EU) 910/2014). Dokumentens referensuppgifter är ETSI EN 319 411-1 [2], punkten QSCD; OID: 0.4.0.194112.1.2. Signeringscertifikat som utfärdas i enlighet med denna certifikatpolicy kan användas för att bekräfta sådana elektroniska signaturer som motsvarar kvalificerade certifikat och anordningar för framställning av elektroniska signaturer som beskrivits i artikel 28 och 29 i Förordningen. Graden av tillförlitlighet på autentiseringscertifikatet är "hög" enligt Förordningen och i förordningen om tillitsnivåer som utfärdats med stöd av Förordningen.

2 Certifikatbeskrivning

2.1 Certifikatutfärdarens kontaktuppgifter

Myndigheten för digitalisering och befolkningsdata

PB 123 (Fågelviksgränden 2)
00531 Helsingfors
FO-nummer: 0245437-2

Tfn +358 295 535 001
kirjaamo@dvv.fi

13.9.2025

Myndigheten för digitalisering och befolkningsdata (MDB) Certifikattjänster

PB 123

00531 Helsingfors

www.dvv.fi/sv

2.2 Certifikattyp, kontrollförfarande och syfte

MDB beviljar autentiseringscertifikat och signeringscertifikat till sådana yrkesutbildade personer som avses i lagen om yrkesutbildade personer inom hälso- och sjukvården (559/1994) samt till sådana yrkesutbildade personer som uppfyller behörighetsvillkoren enligt lagen om behörighetsvillkoren för yrkesutbildad personal inom socialvården (272/2005).

Vid ansökan om certifikatet kontrolleras identiteten med hjälp av en giltig identitetshandling som utfärdats av polisen, dvs. identitetskort eller pass. Godtagbara identifieringshandlingar är också ett giltigt pass eller identitetskort som utfärdats av en myndighet i en medlemsstat inom EES, Schweiz eller San Marino och ett giltigt pass som utfärdats av en myndighet i någon annan stat. Om sökanden inte har nämnda handlingar ska polisen kontrollera sökandens identitet på annat sätt. Att en yrkesutbildad person inom social- och hälsovården har en giltig yrkesrätt kontrolleras med hjälp av Valviras centralregister över yrkesutbildade personer inom hälso- och sjukvården (Terhikki) eller i centralregistret för yrkesutbildade personer inom socialvården (Suosikki). Certifikat kan användas för stark autentisering av en person, kryptering av information och elektroniska signaturer. Certifikaten får användas obegränsat i enlighet med sitt syfte i administrativa tillämpningar och tjänster eller sådana tillämpningar och tjänster som tillhandahålls av en enskild organisation.

Yrkescertifikat för social- och hälsovården används för elektronisk identifiering av certifikatinnehavaren och för elektroniska signaturer, dvs. för att garantera äktheten, integriteten och oavvisligheten hos digitala dokument eller andra uppgifter (exempelvis anteckningar i patienthandlingar, elektroniska recept).

Loggdata relaterat till utfärdande och spärrning av certifikat lagras minst sju (7) år efter certifikatets giltighetstid.

2.3 Certifikatens tillförlitlighet

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 certifikaten användas i andra informationssystem inom social- och hälsovården och apoteksväsendet.

Syftet med ett certifikat anges i certifikatpolicyn och certifieringspraxisen. Ett certifikat får användas enbart i avsett syfte.

Förlitande parter ska kontrollera att giltighetstiden för ett certifikat som ska användas inte har gått ut via en OCSP-tjänst eller att certifikatet inte har upptagits på någon

spärrlista. Förlitande parter kan inte uppriktigt lita på ett certifikat, om de inte har kontrollerat certifikatet mot en spärrlista eller via en OCSP-tjänst. Med tanke på en eventuell spärrning är förlitande parter skyldiga att kontrollera certifikaten mot en spärrlista eller via en OCSP-tjänst innan de godkänner dem.

I förlitande parters ansvar ingår att för de egna datasystemens del försäkra sig om att certifikaten används för de syften som anges i certifikatpolicyn. För att säkerställa att certifikaten används för rätt syfte kan förlitande parter åberopa en hänvisning till certifikatpolicyn i certifikatet.

Förlitande parter ska kontrollera att de tillämpningar som används uppfyller kraven i certifikatpolicyn.

2.4 Certifikatinnehavarens skyldigheter

Yrkesutbildade personer inom social- och hälsovården ska förbinda sig att följa certifikatpolicyn när de ansöker om och använder yrkescertifikat för social- och hälsovården. Certifikatinnehavaren svarar för att de uppgifter som anges vid ansökan om certifikatet är korrekta.

Certifikatinnehavaren svarar för användningen av aktivkortet, de rättshandlingar som företas med stöd av kortet och deras ekonomiska följder.

Yrkesutbildade personer inom social- och hälsovården 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.

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

Yrkesutbildade personer inom social- och hälsovården ska meddela spärrtjänsten:

- om certifikatkortet försvinner eller om de misstänker missbruk

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

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.

Kortinnehavaren kan byta PIN-koderna och öppna låsta PIN-koder med aktiveringskoden som kortinnehavaren fått. Om aktiveringskodsbrevet har kommit bort, gör kortinnehavaren en ny beställning av aktiveringskodsbrevet på registreringsstället.

2.5 Förlitande parters skyldighet att kontrollera giltigheten för certifikat

I förlitande parters ansvar ingår att, innan ett certifikat godkänns, kontrollera att certifikatet gäller och inte har upphävts.

Förlitande parter svarar för att certifikatets status kontrolleras via en OCSP-tjänst eller mot gällande spärrlistor. Ett certifikat är inte tillförlitligt, om inte den förlitande parten har kontrollerat spärrade certifikat på följande sätt:

1. Förlitande parter ska kontrollera spärrlistans certifikatkedja och autenticitet med stöd av utfärdarens digitala signatur.

2. Förlitande parter ska kontrollera spärrlistans giltighetstid för att försäkra sig om att spärrlistan gäller.

3. Certifikat (publika nycklar) kan lagras lokalt i förlitande parters system, men giltighetstiden bör kontrolleras innan certifikaten godkänns.

Om det på grund av störningar i systemet eller tjänsten inte går att få tillgång till en giltig spärrlista, får certifikatet inte godkännas. Om en förlitande part ändå godkänner certifikatet, sker det på partens eget ansvar.

2.6 Friskrivningsklausul och ansvarsbegränsningar

De friskrivningsklausuler som ingår dels i avtalen mellan certifikatutfärdaren och certifikatutfärdarens avtalsparter, dels i de krav som certifikatutfärdaren särskilt ställer på certifikatinnehavare och organ som använder certifikatsystemet är bindande för utfärdarens avtalsparter, certifikatinnehavaren och de organ som använder certifikatsystemet på samma sätt som de friskrivningsklausuler och ansvarsbegränsningar som ingår i certifikatpolicyn.

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.

Certifikatutfärdaren svarar inte för eventuella skador som orsakas av att PIN-koden, aktiveringskoden eller certifikatinnehavarens privata nycklar röjs, om inte avslöjandet direkt har orsakats av utfärdarens omedelbara åtgärder.

Certifikatutfärdarens ansvar gentemot certifikatinnehavare och förlitande parter omfattar högst de direkta skador som har åsamkats dem, om skadan beror på utfärdarens omedelbara åtgärder.

Certifikatutfärdaren svarar inte för indirekta skador eller följdskador som orsakas certifikatinnehavaren. Utfärdaren svarar inte heller för eventuella indirekta skador eller följdskador som orsakas förlitande parter eller andra avtalsparter till certifikatinnehavaren.

Certifikatutfärdaren ansvarar inte för funktionen i de allmänna teleförbindelserna eller datanäten, till exempel Internet, eller för att en rättshandling inte kan utföras på grund av att certifikatinnehavarens utrustning eller kortläsare inte fungerar eller för att certifikatet används i strid med sitt syfte.

Certifikatutfärdaren svarar inte för skador som orsakas av force majeure, till exempel: strejk, eldsvåda, krig, uppror, konfiskering, valutarestriktioner, myndighetsåtgärder, lagstiftning och myndighetsbestämmelser, störningar i telekommunikation, eller dylika signifikanta och ovanliga orsaker oberoende av certifikatutfärdaren.

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. Certifikatinnehavare eller förlitande parter ska i sådana fall svara för egna kostnader och utfärdaren är inte skyldig att ersätta certifikatinnehavare eller förlitande parter för kostnader som orsakas av utvecklingsarbetet.

Certifikatutfärdaren ansvarar inte för ett fel i en nättjänst eller en applikation avsedd för slutanvändare som använder certifikatet eller för kostnaderna för detta fel.

Certifikatinnehavarens ansvar för användningen av ett certifikat upphör när innehavaren eller en företrädare för innehavarens organisation har anmält till spärrtjänsten de uppgifter som är nödvändiga för att spärra certifikatet och efter att ha fått ett meddelande om spärrningen från den funktionär som tagit emot samtalet. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats föreligga skäl för anmälan.

2.7 Avtal, certifieringspraxis och certifikatpolicy

De rättigheter, ansvar och skyldigheter som berör certifikatutfärdaren och certifikatinnehavaren fastställs i certifikatpolicyn. Genom att underteckna certifikatansökan förbinder sig en yrkesutbildad person inom social- och hälsovården att iaktta användarvillkoren för certifikatet. Gällande användarvillkor lämnas till den yrkesutbildade personen i samband med överlämnandet av certifikatet.

Genom sin underskrift förbinder sig yrkesutbildade personer inom social- och hälsovården att omedelbart meddela spärrtjänsten, om certifikatkortet försvinner eller om de misstänker att det förekommer eller kan förekomma missbruk.

Med de registrerare som är auktoriserade av certifikatutfärdaren ingår utfärdaren ett avtal av vilket framgår bägge parters rättigheter, ansvar och skyldigheter.

Certifikatutfärdaren kan ingå avtal med förlitande parter eller andra parter. Av avtalen ska tydligt framgå bägge parters rättigheter, ansvar och skyldigheter. Certifikatutfärdaren ska upprätta nödvändiga avtal med leverantörer och delleverantörer av certifieringstjänster.

Certifikatansökan och de allmänna användarvillkoren bildar tillsammans det avtal som ingås med certifikatsökanden. Användarvillkoren ingår i certifikatpolicydokumenten.

I ansökningshandlingen och i anvisningarna ska tydligt anges att certifikatsökanden genom sin underskrift bekräftar att de givna uppgifterna är korrekta och godkänner att ett certifikat skapas och publiceras.

Myndigheten för digitalisering och befolkningsdata ska utarbeta en särskild certifieringspraxis för varje typ av certifikat som den beviljar. Certifieringspraxisen hänför sig till certifikatpolicyn, som består av mer allmänna regler och anvisningar och är gemensam för alla certifikat oberoende av i vilket tekniskt medium certifikatet är lagrat. Certifieringspraxisen beskriver närmare hur certifikatpolicyn tillämpas på olika tekniska plattformar.

Både certifikatpolicyn och certifieringspraxisen finns på adressen https://dvv.fi/sv/certifikatpolicydokument.

2.8 Integritetsskydd

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.

För certifikattjänsternas del har certifikatutfärdaren gett ut särskilda uppförandekoder som följer personuppgiftslagen.

2.9 Skadestånd

Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar i anslutning till produktionen av certifikattjänster fastställs i det tjänsteavtal som ingåtts med certifikatsökanden. Myndigheten för digitalisering och befolkningsdata omfattas av de skadeståndsansvar som föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster och i lagen om elektronisk kommunikation i myndigheternas verksamhet. Vidare tillämpas lämpliga delar av skadeståndslagen (412/1974) och lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003).

2.10 Tillämplig lag

På social- och hälsovårdens certifikattjänster tillämpas Finlands lag. Eventuella meningsskiljaktigheter som gäller certifikattjänsterna för social- och hälsovården ska i första hand avgöras genom förhandlingar mellan parterna. Om ingen lösning kan nås, behandlas meningsskiljaktigheterna av tingsrätten på certifikatutfärdarens hemort i Finland.

I lagen om stark autentisering och betrodda elektroniska tjänster föreskrivs om identifiering med verktyg för stark autentisering och om betrodda elektroniska tjänster som är baserade på signeringscertifikat. Om certifikat utfärdade av Myndigheten för digitalisering och befolkningsdata föreskrivs i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården, i lagen om elektroniska recept och i lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster (304/2019).

Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar i anslutning till produktionen av certifikattjänster fastställs i det tjänsteavtal som ingåtts med certifikatsökanden. Myndigheten för digitalisering och befolkningsdata omfattas av de skadeståndsansvar som föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster och i lagen om elektronisk kommunikation i myndigheternas verksamhet. På verksamheten tillämpas även vissa bestämmelser i skadeståndslagen (412/1974).

2.11 Granskning och godkännande av certifikatutfärdarens verksamhet

Traficom, som utövar tillsyn över dem som utfärdar signeringscertifikat, har rätt att granska utfärdarens verksamhet på de villkor som anges i lagen om stark autentisering och betrodda elektroniska tjänster.

Certifikatutfärdaren har rätt att granska sina tekniska leverantörer i enlighet med de rutiner som finns inskrivna i de leveransavtal som har ingåtts med leverantörerna. Granskningar ska utföras minst en gång om året och alltid när en ny avtalsperiod inleds.

Med hjälp av granskningarna klarläggs om leverantörerna följer avtalen och beaktar kraven i informationssäkerhetsstandarderna. Som regel bedöms de tekniska leverantörerna med stöd av standarden ISO 27001 och Traficoms föreskrifter.

Granskningarna utförs av Myndigheten för digitalisering och befolkningsdatas datasäkerhetschef eller av en utomstående inspektör som har anlitats av ämbetsverket och som är specialiserad på auditering av tekniska leverantörer av certifikattjänster. Granskningarna ska genomföras med beaktande av de åtta delområdena inom informationssäkerheten. Egenskaper som granskas är konfidentialitet, integritet och tillgänglighet.

Granskningarna omfattar de föreskrifter om informationssäkerhet som Traficom meddelat utfärdaren.