MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

Certifikatbeskrivning

för Myndigheten för digitalisering och befolkningsdatas servicecertifikat samt social- och hälsovårdens servicecertifikat.

15.9.2023

Kuusela Minna

15.9.2023

Dokumenthantering

Ägare	
Utarbetats av	Ville Aarnio, Sanni Kytölä, Minna Kuusela
Granskats av	
Godkänts av	Mikko Pitkänen

Versionshantering

versions nr	vad som har gjorts	datum/person
v 1.0	Version 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	29.9.2022/SK
v 1.3	Uppdaterade versionen	15.9.2023/MK

Kuusela Minna

15.9.2023

Innehållsförteckning

Kuusela Minna

15.9.2023

Certifikatbeskrivning

1 Certifikatbeskrivning

Myndigheten för digitalisering och befolkningsdata

PB 123 (Fågelviksgränden 2) Tfn +358 295 535 001

00531 Helsingfors

FO-nummer: 0245437-2 kirjaamo@dvv.fi

Myndigheten för digitalisering och befolkningsdata (MDB) Certifikattjänster

PB 123

00531 Helsingfors

www.dvv.fi/sv

2 Certifikattyp, kontrollförfarande och syfte

Servicecertifikat är ett certifikat som beviljas av Myndigheten för digitalisering och befolkningsdata och som används för att autentisera serviceleverantörens service eller tjänst.

Servicecertifikat ansöks genom Myndigheten för digitalisering och befolkningsdatas elektroniska tjänst, E-tjänster: asiointi.dvv.fi

När ett certifikat utfärdas kontrollerar MDB sökandens uppgifter. Det utfärdade certifikatet levereras till kunden i enlighet med avtalet.

Innan ett certifikat utfärdas ska organisationen ha ett registrerat konto i Myndigheten för digitalisering och befolkningsdatas webbtjänst, E-tjänster. Organisationsdata för kontot för E-tjänster hämtas från FODS-företags och organisationsdatasystemet. Användaren ska identifiera sig starkt för att kunna logga in på organisationskontot för E-tjänster. En ny användare behöver en inbjudan från en användare i organisationen för att få åtkomst till organisationens konto. Användaren ska identifiera sig varje gång hen loggar in på kontot. En servicecertifikatansökan kan enbart inlämnas när du är inloggad. I samband med ansökan lämnas in en fullmakt, ifall den som ansöker om certifikatet (ADB-kontaktperson o.d.) agerar på uppdrag av ett företag eller en organisation.

Om det servicecertifikat som beställs har ett domännamn eller en IP-adress, kontrollerar Myndigheten för digitalisering och befolkningsdata, i samband med behandlingen av ansökan, sökandens rätt att använda domännamnet antingen i ett

tillgängligt internetbaserat offentligt register, genom kontroll av DNS/TXT, eller någon annan godtagbar metod. På samma sätt kontrolleras IP-adressens ägare i offentliga register. Myndigheten för digitalisering och befolkningsdata utfärdar endast servercertifikat för IP-adresser eller domäner som används för offentligrättsliga ändamål.

All organisationsdata som kommer på certifikatet, kontrolleras på FODS-företags och organisationsdatasystemet, eller på Patent- och registerstyrelsens Virre-register. OID:n som kommer på Social- och hälsovårdens servicecertifikat, kontrolleras på FPA:s nationella Kanta-kodtjänst, som upprätthålls av Institutet för hälsa och välfärd.

När certifikatbegäran behandlas, testas den offentliga nyckeln gentemot kända svagheter med ett mjukvaruverktyg.

Servercertifikat utfärdas för högst 12 månader och andra servicecertifikat för högst 24 månader.

Förnyelse av certifikat följer samma ansökningsförfarande som den ursprungliga ansökningen. Certifikatets kostnad är en årlig avgift enligt serviceprislistan. Kunderna debiteras inte för social- och hälsovårdens servicecertifikat.

Servicecertifikaten kan användas för identifiering av såväl den offentliga förvaltningens som den privata sektorns tjänster. Med hjälp av servicecertifikatet kan den som utnyttjar tjänsten försäkra sig om att tjänsteleverantören är pålitlig.

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

3 Certifikatens tillförlitlighet

Syftet med ett certifikat anges i certifikatpolicyn och certifieringspraxisen för varje enskild typ av certifikat samt i certifikatet. Ett certifikat får användas enbart i avsett syfte. Förlitande parter ska kontrollera att giltighetstiden för ett certifikat som ska användas inte har gått ut och att certifikatet inte har upptagits på någon spärrlista. Förlitande parter kan inte uppriktigt lita på ett certifikat, om de inte har kontrollerat certifikatets giltighet. Med tanke på en eventuell spärrning är förlitande parter skyldiga att kontrollera certifikaten mot en spärrlista innan de godkänner dem.

Offentliga uppgifter som publicerats av utfärdaren finns på utfärdarens webbplats. De konfidentiella uppgifterna i certifikatsystemet är sparade i utfärdarens egna, konfidentiella dataförråd. Utfärdarens data arkiveras i enlighet med gällande arkivbestämmelser. Man fäster särskild uppmärksamhet vid hanteringen av personuppgifter och Myndigheten för digitalisering och befolkningsdata har publicerat särskilda regler för produktionen av certifikattjänster i enlighet med personuppgiftslagen. Utfärdaren har även berett en registerbeskrivning för hanteringen av personuppgifter inom varje delområde inom certifikatsystemet i enlighet med personuppgiftslagen.

Vid arkivering tillämpas som allmän lag bestämmelserna i arkivlagen (831/1994). Rätten till inhämtande av information fastställs i lagen om offentlighet i myndigheternas

verksamhet (621/1999). Vid arkiveringen av certifikat tillämpas för en del dessutom bestämmelserna om arkivering i lagstiftningen om elektronisk kommunikation. Uppgifterna i certifikatregistret ska förvaras i 10 år från tidpunkten då certifikaten upphört att gälla.

4 Certifikatinnehavarens skyldigheter

Syftet med ett certifikat anges i certifikatpolicyn och certifieringspraxisen för varje enskild typ av certifikat samt i certifikatet. Ett certifikat får användas enbart i avsett syfte.

Certifikatinnehavaren (serviceleverantören) ansvarar för att de uppgifter som uppges då man ansöker om certifikatet är riktiga.

Certifikatinnehavaren ska förvara sin privata nyckel i en säker miljö och sträva efter att förhindra att den privata nyckeln förkommer, råkar i händerna på utomstående, ändras eller används av obehöriga.

Certifikatinnehavaren ska omedelbart informera certifikatutfärdaren om man misstänker att certifikatinnehavarens privata nyckel har röjts. Då spärrar utfärdaren servicecertifikatet i fråga.

Anmälan görs utan dröjsmål elektroniskt på organisationens eget konto, från vilket servicecertifikatet ursprungligen har beställts, på E-tjänster. Om detta inte är möjligt, ska anmälan göras per e-post till Myndigheten för digitalisering och befolkningsdatas registratorskontor kirjaamo@dvv.fi.

5 Förlitande parters skyldighet att kontrollera certifikat

Den part som litar på servicecertifikatet är skyldig att säkerställa att certifikatet används enligt användningssyftet.

Den förlitande parten ska iaktta certifikatpolicyn och certifieringspraxisen.

Den förlitande parten kan i god tro lita på servicecertifikatet efter att parten kontrollerat att certifikatet är i kraft och inte finns på spärrlistan. Certifikatets giltighet kan också kontrolleras i en statusinformationstjänst, OCSP, i realtid. Förlitande parter svarar för kontrollen av gällande spärrlistor. Ett certifikat är inte tillförlitligt, om inte den förlitande parten har kontrollerat de spärrade certifikaten på det sätt som beskrivs nedan.

En förlitande part som kopierar en spärrlista från registret, ska försäkra sig om spärrlistans äkthet genom att kontrollera den elektroniska signaturen för den som har signerat spärrlistan. Dessutom ska den förlitande parten kontrollera spärrlistans giltighetstid.

Om det på grund av funktionsstörningar i utrustningen eller registertjänsten inte är möjligt att få tillgång till den senaste spärrlistan från registret, bör certifikatet inte godkännas, i fall giltighetstiden för den senast erhållna spärrlistan har gått ut. Alla

godkännanden av certifikat efter att giltighetstiden har gått ut sker på den förlitande partens egen risk.

6 Ansvarsbegränsningar

Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar i anslutning till produktionen av certifikattjänster bestäms i gällande serviceavtal och i skadeståndslagen (412/1974). Myndigheten för digitalisering och befolkningsdata svarar inte för eventuella skador som orsakas av att certifikatinnehavarens privata nyckel har röjts, om inte avslöjandet direkt har orsakats av Myndigheten för digitalisering och befolkningsdatas åtgärder.

Myndigheten för digitalisering och befolkningsdatas ansvar gentemot certifikatinnehavare och förlitande parter omfattar högst de direkta skador som har orsakats dem, om skadan beror på Myndigheten för digitalisering och befolkningsdatas omedelbara åtgärder, dock högst 15 procent av certifikatfaktureringen under de föregående tre månaderna (MDB:s andel).

Myndigheten för digitalisering och befolkningsdata svarar inte för indirekta skador eller följdskador som har orsakats certifikatinnehavaren. Myndigheten för digitalisering och befolkningsdata svarar inte heller för eventuella indirekta skador eller följdskador som orsakas förlitande parter eller andra avtalsparter för certifikatinnehavaren.

Myndigheten för digitalisering och befolkningsdata ansvarar inte för de allmänna dataförbindelsernas eller datanätens, såsom internets, funktion.

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.

Vid fel i en nättjänst eller applikation som hänför sig till ett certifikat avsett för slutanvändare svarar utfärdaren inte för användningen av certifikatet eller för de kostnader som det orsakar användaren.

Certifikatinnehavarens ansvar för användningen av certifikatet upphör då denne eller en representant för certifikatinnehavarens organisation har meddelat certifikatutfärdaren de uppgifter som behövs för att spärra certifikatet. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats att skäl för anmälan föreligger.

7 Tillämpliga avtal, certifieringspraxis och certifikatpolicy

Certifikatansökarens rättigheter och skyldigheter nämns i dokumenten om certifikatpolicy och certifieringspraxis. Sökanden av ett servicecertifikat bekräftar genom sin underskrift när ansökan lämnas in, att de givna uppgifterna är korrekta och godkänner att ett certifikat skapas och publiceras. Samtidigt godkänner sökanden de

bestämmelser och villkor som gäller användningen av servicecertifikatet och förbinder sig att sörja för förvaringen av servicecertifikatet samt anmäla eventuellt missbruk.

Certifikatutfärdaren och registreraren och andra leverantörer på olika delområden inom certifikattjänsterna har ingått ett avtal som obestridligen uttrycker varje parts rättigheter, ansvar och skyldigheter.

Då utfärdaren beviljar servicecertifikatet godkänner utfärdaren samtidigt certifikatansökan.

Myndigheten för digitalisering och befolkningsdata ska publicera en certifikatpolicy och en certifieringspraxis för de certifikat som den har beviljat. Certifikatpolicyn beskriver förfaranden, användarvillkor och ansvarsfördelning för den aktuella certifikattypens del liksom andra aspekter på certifikatanvändningen. Certifieringspraxisen beskriver närmare hur certifikatpolicyn tillämpas på produktionen av certifikat.

Såväl certifikatpolicyn som certifieringspraxisen finns på https://dvv.fi/sv/certifikatpolicydokument.

8 Integritetsskydd

Vid behandlingen av certifikatinnehavarens uppgifter ska certifikatutfärdaren och registreraren iaktta principerna om god informationshantering och datasekretess. Särskild vikt ska fästas vid en omsorgsfull behandling av personuppgifter. För certifikattjänsternas del har Myndigheten för digitalisering och befolkningsdata gett ut särskilda uppförandekoder som följer personuppgiftslagen.

9 Tillämplig lagstiftning, avgörande av tvister och ersättningspraxis

Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar i anslutning till produktionen av certifikattjänster bestäms i gällande serviceavtal och i skadeståndslagen (412/1974). Myndigheten för digitalisering och befolkningsdata omfattas också av kraven i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009).

10 Granskning av certifikatutfärdarens verksamhet

Traficom, som är kvalitetssäkrare, har rätt att granska utfärdarens verksamhet på villkor som bestämts i lagen om stark autentisering och betrodda elektroniska tjänster. Myndigheten för digitalisering och befolkningsdata har rätt att granska sina tekniska leverantörer i enlighet med de rutiner som finns inskrivna i de leveransavtal som har ingåtts med leverantörerna. Granskningar utförs 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. I regel utvärderas tekniska leverantörer i enlighet med standarden ISO 27001.

Kuusela Minna

15.9.2023

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.

Vid granskningarna bedöms policyn och tillämpningsanvisningarna i relation till hela verksamheten inom certifikatorganisationen och certifikatsystemet. Myndigheten för digitalisering och befolkningsdata ansvarar för att tillämpningsanvisningarna är förenliga med certifikatpolicyn.