CERTIFIKATBESKRIVNING ROTCERTIFIKAT

För Myndigheten för digitalisering och befolkningsdatas rotcertifikatutfärdare

13.9.2025

Dokumenthantering

Ägare	
Utarbetats av	Ville Aarnio (VA), Jari Pirinen (JP)
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 och datumet. Förtydligade vem som kan ansöka utfärdarcertifikat i stycke 2.2. Korrigerade OID-koderna i stycke 1. Korrigerade CA-namn i stycke 1.	15.9.2023/JP
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/JP
v 1.5	Uppdaterade versionen och datumet.	13.9.2025/JP

Innehållsförteckning

CERTIFIKATBESKRIVNING ROTCERTIFIKAT

1 Inledning

Det här dokumentet beskriver på allmän nivå hur Myndigheten för digitalisering och befolkningsdata i sin roll som rotcertifikatutfärdare går till väga vid beviljandet av certifikathierarkins DVV Gov. Root CA – G3 certifikatutfärdarens certifikat.

Detta dokument beskriver certifikatutfärdarens verksamhetskoncept på ett allmänt plan samt villkor och begränsningar för användningen av certifikatutfärdarens certifikat.

Detta dokument hänför sig till följande dokument:

Certifikatpolicy för Myndigheten för digitalisering och befolkningsdatas certifikatutfärdares certifikat, OID 1.2.246.517.1.10.301, 1.2.246.517.1.10.351 och 1.2.246.517.1.10.201.

Certifieringspraxisen för följande undercertifikat:

DVV Citizen Certificates - G4R, OID: 1.2.246.517.1.10.301.1

DVV Citizen Certificates - G4E, OID: 1.2.246.517.1.10.351.1

DVV Organisational Certificates - G4R, OID: 1.2.246.517.1.10.301.2

DVV Organisational Certificates - G4E, OID: 1.2.246.517.1.10.351.2

DVV Temporary Certificates - G3R, OID: 1.2.246.517.1.10.301.3

DVV Temporary Certificates - G3E, OID: 1.2.246.517.1.10.351.3

DVV Service Certificates - G5R, OID: 1.2.246.517.1.10.301.4

DVV Service Certificates - G5E, OID: 1.2.246.517.1.10.351.4

DVV Social Welfare and Healthcare Prof. Certificates - G2R, OID: 1.2.246.517.1.10.301.5

DVV Social Welfare and Healthcare Prof. Certificates - G2E, OID: 1.2.246.517.1.10.351.8

DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2R, OID: 1.2.246.517.1.10.301.6

DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2E, OID: 1.2.246.517.1.10.351.6

DVV Social Welfare and Healthcare Service Certificates - G3R, OID: 1.2.246.517.1.10.301.7

DVV Social Welfare and Healthcare Service Certificates - G3E, OID: 1.2.246.517.1.10.351.7

DVV Time Stamp Certificates - G2R, OID: 1.2.246.517.1.10.301.8

DVV Time Stamp Certificates - G2E, OID: 1.2.246.517.1.10.351.8

VRK Gov. CA for Citizen Certificates - G3, OID: 1.2.246.517.1.10.201.1

VRK CA for Organisational Certificates - G3, OID: 1.2.246.517.1.10.201.2

VRK CA for Service Providers - G4, OID: 1.2.246.517.1.10.201.4

VRK CA for Social Welfare and Healthcare Prof. Certs, OID: 1.2.246.517.1.10.201.5

VRK CA for Social Welfare and Healthcare Service Providers – G2, OID: 1.2.246.517.1.10.201.7

VRK CA for Time Stamp Services, OID: 1.2.246.517.1.10.201.8

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

2 Certifikatbeskrivning

2.1 Certifikatutfärdarens kontaktuppgifter

Myndigheten för digitalisering och befolkningsdata

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

00531 Helsingfors Fax +358 9 876 4369

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

Myndigheten för digitalisering och befolkningsdata (MDB) Certifikattjänster

PB 123

00531 Helsingfors

www.dvv.fi/sv

2.2 Certifikattyp, kontrollförfarande och syfte

Certifikatutfärdarens certifikat är ett certifikat beviljat av Myndigheten för digitalisering och befolkningsdata för att bevilja slutanvändarens certifikat.

Certifikatutfärdarens certifikat ansöks hos Myndigheten för digitalisering och befolkningsdata.

Innan certifikatet beviljas kontrollerar MDB certifikatsökandens uppgifter bl.a. i handelsregistret.

Förnyelse av certifikat följer samma ansökningsförfarande som den ursprungliga ansökningen.

Certifikatets kostnad är en årlig avgift enligt serviceprislistan.

Certifikatutfärdarens certifikat kan endast ansökas av parter som gjort skilt avtal med MDB.

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

2.3 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 mot en spärrlista. Med tanke på en eventuell spärrning är förlitande parter skyldiga att kontrollera certifikaten mot en spärrlista innan de godkänner dem.

2.4 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 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 certifikatet i fråga.

2.5 Förlitande parters skyldighet att kontrollera certifikat

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 förlitande parter 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.

2.6 Ansvarsbegränsningar

Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar i anslutning till produktionen av certifikattjänster regleras i skadeståndslagen (412/1974). De skadeståndsansvar som föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster gäller Myndigheten för digitalisering och befolkningsdata. 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 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.

Rotcertifikatutfärdaren 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.

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.

2.7 Tillämpliga avtal, certifieringspraxis och certifikatpolicy

Certifikatansökarens rättigheter och skyldigheter nämns i dokumenten om certifikatpolicy och certifikatpraxis. Då organisationen ansöker om certifikat godkänner den

reglerna och villkoren för användningen av certifikatet samt ansvarar för certifikatets förvaring samt för att 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.

När en certifikatutfärdare utfärdar certifikatutfärdarens certifikat är det samtidigt ett godkännande av 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.

2.8 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.

2.9 Ersättningspraxis

På Myndigheten för digitalisering och befolkningsdata tillämpas bestämmelserna i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009). Även vissa bestämmelser i skadeståndslagen (412/1974) tillämpas.

2.10 Tillämplig lagstiftning och avgörande av tvister

I lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) föreskrivs om identifierings- och betrodda tjänster. Bestämmelser om av Myndigheten för digitalisering och befolkningsdata beviljade certifikat fastställs i lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster (661/2009).

På Myndigheten för digitalisering och befolkningsdata tillämpas bestämmelserna i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009). Även vissa bestämmelser i skadeståndslagen (412/1974) tillämpas.

2.11 Granskning av certifikatutfärdarens verksamhet

Traficom har rätt att granska utfärdarens verksamhet på de villkor som anges 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.

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. Dataskyddsegenskaper som kontrolleras är bl.a. konfidentialitet, integritet och användbarhet.

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.