DIGITALISERINGSSTYRELSEN

Erhverv

Bilag 5
Vilkår for kvalificerede segl

Indholdsfortegnelse

1 Kvalificerede segl i Signeringsløsningen

Disse vilkår regulerer Brugerorganisationens afgivelse af et kvalificeret elektronisk segl (segl) under anvendelsen af et kvalificeret organisationscertifikat udsted af Den Danske Stat Tillidstjenester via Signeringsløsningen til brug i offentlige og private Selvbetjeningsløsninger.

Hvor ikke andet er anført, er vilkårene ligeledes gældende for udstedelsen af kvalificerede tidsstempler, der sammenkobles med det elektroniske segl. Kvalificeret tidsstempling dokumenterer tidspunktet for afgivelse af det elektroniske segl, herunder at certifikat og de signerede data var til stede på underskriftstidspunktet.

I det følgende benævnes Brugerorganisationen som Certifikatindehaver og den enhed tilknyttet Certifikatindehaveren, der registreres og får udstedt et certifikat, benævnes Certifikatholder.

Vilkårene er udarbejdet i overensstemmelse med Offentlig certifikatpolitik for kvalificerede virksomhedscertifikater v1.1, der danner grundlaget for Digitaliseringsstyrelsens udstedelse af det kvalificerede organisationscertifikat. Certifikatpolitikken er ligeledes omfattet af vilkårene.

Disse vilkår benytter betegnelsen organisationscertifikat for den certifikattype, der i certifikatpolitikken er benævnt virksomhedscertifikat. Certifikatpolitikkens regulering af virksomhedscertifikater er således gældende for vilkårenes organisationscertifikater og de elektroniske segl, der er udstedt på baggrund heraf.

De kvalificerede tidsstempler, der sammenkobles med det elektroniske segl er udstedt på baggrund af Digitaliseringsstyrelsens offentlig politik for kvalificeret tidsstempling, v.1.0, der ligeledes er omfattet af disse vilkår.

Certifikatpolitikken, politik for tidsstempling og Digitaliseringsstyrelsen detaljerede beskrivelse af Signeringsløsningen (Certificate Practice statement) kan læses på certifikat.gov.dk.

Den Danske Stat Tillidstjenester udsteder en række andre certifikattyper til brug i erhvervsmæssig sammenhæng. Disse certifikattyper er alle underlagt særskilte vilkår.

2 Kontaktinformation

Den Danske Stat Tillidstjenester har følgende kontaktinformation:

Digitaliseringsstyrelsen

Att. Den Danske Stat Tillidstjenester

Landgreven 4

1301København K

Yderligere kontaktoplysninger findes på www.ca1.gov.dk/

3 Organisationscertifikatets juridiske gyldighed

Det kvalificerede elektroniske segl er anerkendt i EU. Den Danske Stat Tillidstjenester agerer således som kvalificeret tillidstjenesteudbyder som nærmere beskrevet i Europa-Parlamentets og Rådets forordning (EU) Nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (eIDAS forordningen).

For et kvalificeret elektronisk segl afgivet på baggrund af et kvalificeret organisationscertifikat, gælder der en formodning for integriteten af de data og nøjagtigheden af oprindelsen af de data, som det kvalificerede elektroniske segl er knyttet til. Kvalificerede segl anerkendes i alle medlemsstater.

Ved sammenkoblingen af de signerede data med et kvalificeret elektronisk tidsstempel gælder der i alle medlemslande en formodning for nøjagtigheden af den dato og det tidspunkt, som det angiver, og integriteten af de data, som dato- og tidsangivelsen er knyttet til.

4 Anvendelsesmuligheder – kvalificerede segl

4.1 Generel anvendelse

Et kvalificeret organisationscertifikat til afgivelse af et kvalificeret segl kan anvendes, når en organisatorisk enhed tilknyttet Certifikatindehaver skal signere data med henblik på at dokumentere integritet og nøjagtighed af data.

Signeringsløsningen kan alene anvendes til afgive et kvalificeret elektronisk segl online via tjenesteudbydere, der er tilmeldt løsningen. Som følge heraf kan certifikatet til seglet f.eks. ikke anvendes til at signere mails via en e-mailklient eller til hemmeligholdelse (kryptering).

Segl i Signeringsløsningen baserer sig på kryptografiske nøgler, der genereres til lejligheden i et centralt kvalificeret signaturgenereringssystem (QSCD) og den private nøgle slettes umiddelbart efter generering af hvert enkelt elektronisk segl.

Segl og organisationscertifikater er ikke til brug for autentifikation. Selve autentifikationen over for en tjenesteudbyder håndteres af Brugerens eID identifikationsmiddel.

Elektroniske segl udstedes i LTV format.

Der er ikke fastlagt begrænsninger til hvilke typer aftaler og forpligtigelser der kan indgås ved anvendelse af organisationscertifikater udstedt af Den Danske Stat Tillidstjenester.

4.2 Navngivning af Certifikatholder i certifikatet

Certifikatindehavers Brugeradministrator fastsætter hvilken navngivning Certifikatholder fremstår med i certifikatet.

5 Tilgængelighed

5.1 Signeringsløsningen

Alle Digitaliseringsstyrelsens Services relateret til udstedelse og validering af certifikater er tilgængelige døgnet rundt alle årets dage.

Digitaliseringsstyrelsen er ikke ansvarlig for at ovenstående tilgængelighed leveres.

5.2 Spærreliste

En oversigt over spærrede certifikater kan til enhver tid tilgås via Den Danske Stat Tillidstjenesters (CA 1) spærreliste på www.ca1.gov.dk/tilbagekald-certifikater/.

6 Forpligtelser ved brug af kvalificerede organisationscertifikater

6.1 Offentliggørelse af certifikatet

Der sker ingen offentliggørelse af certifikater udstedt via Signeringsløsningen. Det enkelte certifikat eksisterer alene indlejret i det elektroniske segl.

6.2 Certifikatets gyldighedsperiode

Certifikatet har en gyldighedsperiode på 10 dage. Den tekniske løsning sikrer dog, at det ikke er muligt at generere flere segl på baggrund af samme certifikat.

Certifikatets forlængende gyldighed efter afgivelsen af seglet, er alene begrundet i tekniske hensyn til de systemer, der efterfølgende skal læse seglet. Spærring af certifikat

6.3 Spærring af certifikat

Signeringsløsningen sletter den private nøgle tilhørende certifikatet umiddelbart efter afgivelse af det kvalificerede elektroniske segl, hvorfor certifikatet ikke kan anvendes som grundlag for et nyt segl. Der påhviler derfor ikke en pligt for Certifikatindehaver eller Certifikatholder til at spærre certifikatet selv om der efterfølgende måtte opstå en situation, der hvis den havde fundet sted forud for anvendelsen af certifikatet, ville have begrundet en spærring.

6.4 Begrænsninger ved navngivning af Certifikatholder

Den konkrete navngivning af Certifikatholder, jf. punkt 4.2, må ikke være af en sådan karakter, at det kan være forveksleligt med et varemærke. Digitaliseringsstyrelsen kan i øvrigt pålægge Certifikatindehaver at ophøre med anvendelsen af konkret navngivning, såfremt Digitaliseringsstyrelsen vurderer, at anvendelsen kan være krænkende.

7 Forpligtelser som modtager af et elektronisk segl

Forud for at have tillid til et certifikat skal modtageren af et elektronisk segl sikre sig følgende:

- At certifikatet er gyldigt og ikke spærret på signeringstidspunktet - dvs. ikke opført på Den Danske Stat Tillidstjeneste (CA 1) spærreliste,
- At det formål, certifikatet søges anvendt til, er passende i forhold til evt. anvendelsesbegrænsninger i certifikatet samt
- At anvendelsen af certifikatet i øvrigt er passende i forhold til niveauet af sikkerhed, som er beskrevet i disse vilkår og den underlæggende certifikatpolitik for certifikatet, jf. punkt 1.

Inden et tidsstempel accepteres skal modtageren af et elektronisk segl sikre sig følgende:

- at tidsstemplet er korrekt signeret, og at den private nøgle, der bruges til at signere tidsstemplet, ikke er blevet markeret som kompromitteret på kontroltidspunktet,
- Være opmærksom på eventuelle begrænsninger for brugen af tidsstemplet angivet i tidsstempelpolitikken og
- Andre forholdsregler, der er angivet i aftaler eller lignende.

Med mindre andre forhold tilsiger andet, vil et elektronisk segl udstedt på baggrund af disse vilkår være gyldig og modtageren kan støtte ret på det, selv om certifikatet efter afgivelsen af seglet er udløbet eller spærret.

Signerede dokumenter kan valideres i Digitaliseringsstyrelsens valideringstjeneste på adressen https://validering.ca1.gov.dk/

Detaljeret information om modtagerens forpligtelser fremgår af PKI Disclosure Statement, der er tilgængelig på www.ca1.gov.dk/pds. Digitaliseringsstyrelsen har desuden indsat nærmere information i certifikatet om anvendelsen heraf, herunder henvisning til PKI Disclosure Statement.

8 Support

8.1 Generel support

Supporthenvendelser vedr. kvalificerede organisationscertifikater, herunder generelle forhold ved afgivelse af et elektronisk segl og anvendelse af certifikater kan rettes til MitID Erhverv Support på telefon +45 33980020 eller via kontaktformular http://www.mitid-erhverv.dk/support/kontakt.

Digitaliseringsstyrelsen leverer ikke support relateret til tekniske forhold, herunder installation af software og etablering af kontroller og processer hos Certifikatindehaver.

Certifikatindehaver har mulighed for at indgå en supportaftale med Nets DanID A/S, jf. beskrivelser herom i vilkår for Brugerorganisationer. En supportaftale giver mod betaling af vederlag mulighed for at rekvirere teknisk support, herunder som hastesupport.

9 Behandling af personoplysninger

9.1 Privatlivspolitik

Certifikater fra Digitaliseringsstyrelsen er omfattet af Digitaliseringsstyrelsens Privatlivspolitik for MitID Erhverv. Privatlivspolitikken er tilgængelig på https://www.mitid-erhverv.dk/info/losning/privatlivspolitik/.

9.2 Dataansvar

Digitaliseringsstyrelsen er dataansvarlig for de personoplysninger som behandles i Signeringsløsningen i forbindelse med certifikatanvendelsen. NNIT A/S og Nets DanID A/S er databehandler for Digitaliseringsstyrelsen.

Behandlingen af personoplysninger er underlagt databeskyttelsesreglerne, herunder databeskyttelsesforordningen og databeskyttelsesloven.

Personoplysninger slettes efter løbende år +7 år.

9.3 Registrering af oplysninger ved oprettelse og anvendelse af certifikater

Digitaliseringsstyrelsen opbevarer en række oplysninger ved registrering af Certifikatindehaver og Certifikatholdere og den efterfølgende brug af certifikater.

Følgende registreres:

- Tidspunktet for signering/udstedelse af certifikatet
- Certifikatindehavers grundlæggende virksomhedsoplysninger, som registreret i MitID Erhverv
- Det NSIS sikringsniveau (Level Of Assurance) Certifikatholder er autoriseret med over for tjenesten
- Session UUID
- Referencetekst
- Tekniske oplysninger relateret til autentifikationen (SAML assertion)
- Certifikatholders navn, UUID og e-mail

Alle data relateret til Certifikatindehaver og Certifikatholder opbevares i syv (7) år.

9.4 Oplysninger der ikke registreres

Den Danske Stat Tillidstjenester registrerer ikke oplysninger om hvilket dokument eller hvilke data, der er signeret under anvendelse af certifikatet.

9.5 Oversigt over signaturanvendelse

Det er muligt i MitID Erhverv at tilgå en log over alle anvendelser af Signeringsløsningen.

9.6 Lagring af data

Alle data relateret til Certifikatindehaver og Certifikatholder, herunder anvendelse af signeringsløsningen opbevares i syv (7) år.

Hvis Signaturløsningen ophører inden for 7 års perioden vil data fortsat blive lagret og kan tilgås af kompetente myndigheder og andre parter, der kan have en retlig interesse heri.

10 Ophør af Den Danske Stat Tillidstjenester

Hvis Den Danske Stat Tillidstjenester ophører med at udstede OCES organisationscertifikater, er styrelsen berettiget til at videre give alle registrerede oplysninger til en anden juridisk enhed, herunder en offentlig myndighed eller et offentligretligt organ, som får til opgave at varetage den fortsatte forvaltning med eller ophør af Den Danske Stats Tillidstjenester.

11 Elektronisk kommunikation

Den Danske Stat Tillidstjenester kan i forbindelse med drift af tjenesten kontakte Certifikatindehaver via e-mail. Henvendelser kan f.eks. vedrøre driftsrelateret information, sikkerhedsrelaterede forhold, ændringer og ophør.

Digitaliseringsstyrelsens kommunikation vedr. anvendelsen af certifikater sker som udgangspunkt til Certifikatindehavers Organisationsadministrator og Identitetsadministrator.

12 Digitaliseringsstyrelsens ansvar

12.1 Ansvar over for Certifikatindehaver

Digitaliseringsstyrelsen er efter dansk rets almindelige regler erstatningsansvarlige for manglende opfyldelse af disse vilkår, herunder for tab, der skyldes at Digitaliseringsstyrelsen har begået fejl i forbindelse med registrering, udstedelse og spærring af certifikatet.

Digitaliseringsstyrelsen er forpligtet til at løfte bevisbyrden for ikke at have forsætligt eller uagtsomt.

12.2 Ansvar for tredjeparter

Digitaliseringsstyrelsen er over for den, der med rimelighed forlader sig på et kvalificeret elektronisk segl fra Signeringsløsningen, erstatningsansvarlig efter dansk rets almindelige regler, medmindre Digitaliseringsstyrelsen kan løfte bevisbyrden for ikke at have handlet forsætligt eller uagtsomt, herunder at certifikatet ikke er anvendt i overensstemmelse med de i certifikatet indeholdte retningslinjer.

Omfattet af Digitaliseringsstyrelsens ansvar er tab, der skyldes at Digitaliseringsstyrelsen har begået fejl i forbindelse med registrering, udstedelse og spærring af certifikatet.

12.3 Ansvarsbegrænsninger

Digitaliseringsstyrelsens ansvar over for både Certifikatindehaver og tredjeparter i det omfang disse er juridiske personer, herunder offentlige myndigheder og offentlige organisationer, er i alle tilfælde begrænset til 100.000 kr. for hver tabsgivende begivenhed og er i alle tilfælde maksimeret til 100.000 kr. årligt. Ved en tabsgivende begivenhed anses alle forhold, der udspringer af samme fortsatte eller gentagne ansvarspådragende forhold.

12.4 Ansvar ved afgivelse af tidsstempel

Det ovenfor under punkt 12.1til punkt 12.3 er ligeledes gældende for Digitaliseringsstyrelsens afgivelse af tidsstempler.

13 Anvendelsesbegrænsninger

Der er ikke fastlagt anvendelsesbegrænsninger for kvalificerede organisationscertifikater fra Digitaliseringsstyrelsen, jf. dog punkt 4 om begrænsninger i den tekniske anvendelse af certifikater.

14 Anvendelse af kvalificeret virksomhedscertifikat

14.1 Generelle forhold

Certifikatholders anvendelse af et kvalificeret organisationscertifikat til afgivelse af et kvalificeret segl sker på vegne af Certifikatindehaver i overensstemmelse med de mellem parterne fastlagte aftaler.

Digitaliseringsstyrelsen er ikke part i sådanne aftaler og er ikke ansvarlig for den konkrete anvendelse af organisationscertifikatet.

14.2 Begrænsninger i anvendelse af certifikat og nøgler

Certifikatets nøglepar må kun anvendes i overensstemmelse med fastlagt tilladt brug og ikke uden for eventuelle begrænsninger, der er meddelt Certifikatindehaver og Certifikatholder, herunder at den private nøgle ikke må anvendes til signering af andre certifikater.

Forud for afgivelse af et segl er Certifikatindehaver forpligtet til at kontrollere indholdet af certifikatet, herunder med henblik på at kontrollere, om anvendelsen sker inden for de begrænsninger, der måtte fremgå heraf. Ved godkendelse af den pågældende signering, accepteres samtidig certifikatet og indholdet heri.

14.3 Beskyttelse af identifikationsmiddel

Certifikatholder skal beskytte det identifikationsmiddel (f.eks. MitID) og tilhørende sikkerhedsmekanismer (f.eks. kodeord), der anvendes til brug for afgivelse af et elektronisk segl, i overensstemmelse med de vilkår, der er gældende herfor således at der er taget rimelige forholdsregler for, at der ikke afgives et elektronisk segl i Certifikatholders navn.

Hvis der er mistanke om at det identifikationsmiddel, der anvendes til brug for autentifikation over for Signaturtjenesten, er kompromitteret skal dette identifikationsmiddel spærres i overensstemmelse med de vilkår, der er gældende herfor, således at det ikke uberettiget kan anvendes til at afgive et elektronisk segl i Certifikatholders navn.

14.4 Opdaterede og korrekte oplysninger

Certifikatindehaver skal sikre at oplysninger, der udgør grundlaget for udstedelsen af et certifikat, er korrekte og fyldestgørende på tidspunktet for udstedelsen af certifikatet. Oplysningerne præsenteres som led i udstedelsesprocessen og baserer sig på de oplysninger, der i forvejen er registreret i MitID Erhverv.

Hvis oplysningerne ikke er korrekte, er Certifikatindehaver forpligtet til at afbryde signeringsprocessen.

14.5 Beskyttelse på et kvalificeret elektronisk signaturgenereringssystem (QSCD)

Signeringsløsningen sikrer for Certifikatindehaver at den private nøgle, der udstedes sammen med certifikatet, bliver genereret og alene kan benyttes til kryptografiske handlinger inden for det sikrede

kryptografiske modul (QSCD) i Signeringsløsningen. Det er således alene Certifikatindehaver, der har kontrollen med den private nøgle og certifikat ved afgivelse af et elektronisk segl.

14.6 Spærring af certifikat

Signeringsløsningen sletter den private nøgle tilhørende certifikatet umiddelbart efter afgivelse af det kvalificerede elektroniske segl, hvorfor certifikatet ikke kan anvendes som grundlag for et nyt segl. Der påhviler derfor ikke en pligt for Certifikatholder til at spærre certifikatet selv om der efterfølgende måtte opstå en situation, der hvis den havde fundet sted forud for anvendelsen af certifikatet, ville have begrundet en spærring.

15 Ændringer til vilkår

Digitaliseringsstyrelsen kan ændre vilkårene med et varsel på 3 måneder.

Såfremt ændringer af Digitaliseringsstyrelsen vurderes væsentlige af hensyn til driftsmæssige forhold, herunder sikkerhed, kan ændringer gennemføres med kortere varsel, herunder med virkning fra meddelelsestidspunktet.

16 Lovvalg og tvister

Retsforholdet ifølge disse vilkår og fortolkning heraf afgøres efter dansk ret.

Enhver tvist, der måtte udspringe af brugen af certifikater udstedt af Digitaliseringsstyringsstyrelse skal indbringes for Københavns Byret.