DIGITALISERINGSSTYRELSEN

Erhverv

Bilag 3
Vilkår for OCES organisationscertifikater

Indholdsfortegnelse

1 Beskrivelse af certifikater i MitID Erhverv 3
2 Kontaktinformation 3
3 Organisationscertifikaters juridiske gyldighed 3
4 Anvendelsesmuligheder – OCES organisationscertifikat 3
4.1 Generel anvendelse 3
4.2 Navngivning af Certifikatholder i certifikatet 4
5 Tilgængelighed 4
5.1 Generelle services 4
5.2 Spærreliste 4
6 Forpligtelser ved brug af OCES-certifikater 4
6.1 Opdaterede og korrekte oplysninger 4
6.2 Forpligtelser ved afgivelse af et elektronisk segl 4
6.3 Anvendelse af nøgler 4
6.4 Offentliggørelse af certifikatet 4
6.5 Beskyttelse af privat nøgle ved generering 5
6.6 Certifikatets gyldighedsperiode 5
6.7 Underretning af Digitaliseringsstyrelsen og spærring af certifikat 5
6.8 Begrænsninger ved navngivning af Certifikatholder 5
7 Digitaliseringsstyrelsens ret til at spærre certifikater 5
8 Forpligtelser som modtager af et elektronisk segl 6
9 Support 6
9.1 Generel support 6
10 Digitaliseringsstyrelsens registrering af oplysninger 6
10.1 Registrering af oplysninger ved oprettelse og anvendelse af certifikater 6
10.2 Oplysninger der ikke registreres 7
11 Behandling af personoplysninger 7
11.1 Privatlivspolitik 7
11.2 Dataansvar 7
11.3 Registrering af oplysninger 7
12 Ophør af Den Danske Stat Tillidstjenester 7
13 Elektronisk kommunikation 7
14 Digitaliseringsstyrelsens ansvar 8
14.1 Ansvar over for Certifikatindehaver 8
14.2 Ansvar for tredjeparter 8
14.3 Ansvarsbegrænsninger 8
15 Anvendelse af OCES organisationscertifikat 8

16 Anvendelsesbegrænsninger 8
17 Ændringer til vilkår 8
18 Lovvalg og tvister 9

1 Beskrivelse af certifikater i MitID Erhverv

Disse vilkår regulerer anvendelsen af OCES organisationscertifikater udstedt af Den Danske Stat Tillidstjenester (CA1) ved Digitaliseringsstyrelsen til brug for specifikke fysiske eller logiske enheder i Brugerorganisationen. En enhed kan omfatte den samlede Brugerorganisation.

Efter udstedelsen af et organisationscertifikat knyttes dette til organisationsidentiteten i MitID Erhverv.

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

OCES organisationscertifikater er udstedt på baggrund af Digitaliseringsstyrelsens Certifikatpolitik for OCES-virksomhedscertifikater, v.7.1. Certifikatpolitikken supplerer disse vilkår og er således også gældende i forholdet mellem Certifikatindehaver og Digitaliseringsstyrelsen. Certifikatpolitikken er tilgængelig på https://certifikat.gov.dk/

Disse vilkår benytter betegnelsen organisationscertifikat for den certifikattype, der i certifikatpolitikken er benævnt virksomhedscertifikat. Certifikatpolitikkens regulering af virksomhedscertifikater er således gældende for vilkårenes organisationscertifikater.

2 Kontaktinformation

Den Danske Stat Tillidstjenester har følgende kontaktinformation:

Digitaliseringsstyrelsen

Att. Den Danske Stat Tillidstjenester

Landgreven 4

1301 København K

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

3 Organisationscertifikaters juridiske gyldighed

For et elektronisk segl baseret på et OCES organisationscertifikat, gælder der en formodning for integriteten af de data og nøjagtigheden af oprindelsen af de data, som seglet er knyttet til.

OCES-certifikater og segl afgivet på baggrund heraf er ikke anerkendt i EU, men kan i medlemslandene ikke nægtes retsvirkning og anerkendelse som bevis under retssager, alene af den grund at de er i elektronisk form, eller at den ikke opfylder kravene til kvalificerede elektroniske segl.

OCES-certifikaterne er ikke kvalificerede certifikater, og de må derfor ikke bruges i situationer, hvor kvalificerede certifikater er påkrævet.

4 Anvendelsesmuligheder – OCES organisationscertifikat

4.1 Generel anvendelse

OCES organisationscertifikater i MitID Erhverv udstedes med et tilknyttet og persistent certifikat og anvendes når en Juridisk enhed skal påføre data en elektronisk signatur med henblik på at dokumentere integritet og oprindelsen heraf.

Certifikaterne tilbyder en høj grad af funktionalitet og fleksibilitet i anvendelsen og kan både anvendes til autentifikation (over for tjenester, der specifikt tillader dette), signering af e-mails og til hemmeligholdelse (kryptering).

Der er ikke fastlagt begrænsninger til hvilke typer aftaler og forpligtigelser der kan indgås ved anvendelse af OCES organisationscertifikater udstedt af Den Danske Stat Tillidstjenester (CA1).

4.2 Navngivning af Certifikatholder i certifikatet

Certifikatindehavers brugeradministrator fastsætter hvilken navngivning Certifikatholder fremstår med i certifikatet.

5 Tilgængelighed

5.1 Generelle services

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

Digitaliseringsstyrelsen er dog 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 spærreliste på www.ca1.gov.dk/tilbagekald-certifikater/.

6 Forpligtelser ved brug af OCES-certifikater

6.1 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.

Certifikatindehaver er forpligtet til at spærre certifikatet, hvis de registrerede oplysninger ændrer sig i certifikatets levetid, jf. punkt 6.7 nedenfor.

6.2 Forpligtelser ved afgivelse af et elektronisk segl

Forud for afgivelse af et elektronisk segl skal Certifikatindehaver kontrollere indholdet af certifikatet, og sikre at anvendelsen sker inden for de begrænsninger, der måtte fremgå heraf. Ved godkendelsen af den pågældende seglgenerering, accepteres samtidig certifikatet og indholdet heri.

6.3 Anvendelse af nøgler

Den private nøgle må ikke anvendes til signering af andre certifikater.

Den private nøgle skal beskyttes i overensstemmelse med det i punkt 6.5 anførte.

6.4 Offentliggørelse af certifikatet

Certifikatindehavers Brugeradministrator træffer beslutning om, hvorvidt certifikater fra MitID Erhverv skal offentliggøres i Den Danske Stats Tillidstjenesters offentlige certifikatdatabase (LDAP søgetjeneste), hvor det kan fremsøges af tredjepart.

6.5 Beskyttelse af privat nøgle ved generering

Certifikatindehaver er forpligtet til at etablere det fornødne teknisk grundlag og administrative kontroller til at sikre, at den private nøgle genereres sikkert og under kontrol af certifikatholder.

Certifikatholders nøgler skal genereres ved hjælp af en algoritme som opfylder profilkravene anført i Certificate Profiles på https://www.ca1.gov.dk/practice/.

Som en del af det tekniske grundlag og de administrative kontroller skal Certifikatindehaver sikre, at Certifikatholder til stadighed kan have egenkontrol over egen nøgle.

Der henvises til punkt 7 for nærmere krav til dokumentation af Certifikatindehavers tekniske grundlag og administrative kontroller.

6.6 Certifikatets gyldighedsperiode

Certifikatet har en gyldighedsperiode på 36 måneder. Efter udløb må certifikatet ikke længere anvendes.

6.7 Underretning af Digitaliseringsstyrelsen og spærring af certifikat

Certifikatindehaver skal straks spærre certifikatet, hvis nedenstående forhold opstår inden udløb af certifikatets gyldighedsperiode:

i. Adgangen til den private nøgle er mistet, herunder at den er stjålet eller potentielt kompromitteret.
ii. Certifikatholders egenkontrol med den private nøgle er mistet på grund af kompromittering af aktiveringsdata (fx PIN kode).
iii. Der er vished eller mistanke om, at Certifikatholderens private nøgle er kompromitteret
iv. Der konstateres unøjagtigheder i eller ændringer af data, der er inkluderet i certifikatet.
v. Certifikatindehaverens konkurs eller ophør af virksomhed

Anvendelse af den private nøgle skal ophøre hvis den konstateres kompromitteret eller der foreligger mistanke herom, efter anmodning om spærring, notifikation om spærring eller efter udløb af certifikat med undtagelse af anvendelse relateret til dekryptering af data. Den private nøgle må dog altid anvendes som grundlag for autentifikation med henblik på at gennemføre en spærring.

Spærring af et certifikat udføres i MitID Erhverv løsningen.

Spærring af et tidligere anvendt certifikat er ikke til hindring for at der kan udstedes et nyt certifikat til Certifikatholder.

6.8 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 forvekslelig 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 Digitaliseringsstyrelsens ret til at spærre certifikater

Digitaliseringsstyrelsen er berettiget til ensidigt at spærre et certifikat, såfremt Digitaliseringsstyrelsen får vished for eller mistanke om, at Certifikatindehaver eller Certifikatholder handler i strid med fastlagte forpligtelser eller at Digitaliseringsstyrelsen i øvrigt får vished eller mistanke om, at den private nøgle er kompromitteret eller ødelagt.

Spærring kan i visse tilfælde ske efter fastlagte processer, herunder i tilfælde af Certifikatindehavers navneskifte eller ophør af virksomhed.

Digitaliseringsstyrelsen er i øvrigt berettiget til at spærre certifikater af sikkerhedsmæssige grunde eller hvis der konstateres tekniske fejl relateret til udstedelse af certifikatet, der har betydning for certifikatets korrekte anvendelse.

8 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 - dvs. ikke opført på Den Danske Stat Tillidstjenesters 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, jf. punkt 1.

Med mindre andre forhold tilsiger andet, vil et elektronisk segl udstedt på baggrund af disse vilkår være gyldig og modtageren kan støtte ret herpå, 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.

9 Support

9.1 Generel support

Supporthenvendelser vedr. udstedelse af 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 www.mitid-erhverv.dk/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.

10 Digitaliseringsstyrelsens registrering af oplysninger

10.1 Registrering af oplysninger ved oprettelse og anvendelse af certifikater

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

Følgende registreres:

- Certifikatindehavers grundlæggende virksomhedsoplysninger, som registreret i MitID Erhverv
- Kontaktoplysninger på administratorer
- Certifikatholders navn, UUID og e-mail
- Tidspunktet for udstedelse af certifikatet

- Alle interaktioner med MitID Erhverv relateret til certifikatet
- Oplysninger relateret til efterfølgende spærring og suspension af certifikatet.

Hvis Digitaliseringsstyrelsen nedlægger sin CA-tjeneste, er Digitaliseringsstyrelsen berettiget til at videregive registrerede oplysninger til tredjemand i overensstemmelse med det i punkt 12 anførte.

Alle data relateret til Certifikatindehaver og Certifikatholder opbevares i syv (7) år fra tidspunktet for udløb eller spærring af certifikatet.

10.2 Oplysninger der ikke registreres

Digitaliseringsstyrelsen registrerer ikke oplysninger om den løbende anvendelse af certifikatet, herunder anvendelse af certifikatet til afgivelse af elektroniske segl eller hemmeligholdelse.

11 Behandling af personoplysninger

11.1 Privatlivspolitik

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

11.2 Dataansvar

Digitaliseringsstyrelsen er dataansvarlig for de personoplysninger som behandles i MitID Erhverv i forbindelse med certifikatanvendelsen. NNIT A/S og Nets Dan ID A/S er databehandler for Digitaliseringsstyrelsen.

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

Personoplysninger slettes efter løbende år + 7 år.

11.3 Registrering af oplysninger

Digitaliseringsstyrelsens registrering og behandling af oplysninger, herunder personoplysninger ved registrering af Certifikatholdere og den efterfølgende brug af certifikater fremgår af punkt 9.1.

12 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.

13 Elektronisk kommunikation

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

Certifikatindehaver har i MitID Erhverv mulighed for at tilmelde sig en særlig informationsservice hos Digitaliseringsstyrelsen, der giver mulighed for information via mobil, herunder push-notifikationer.

14 Digitaliseringsstyrelsens ansvar

14.1 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 handlet forsætligt eller uagtsomt.

14.2 Ansvar for tredjeparter

Digitaliseringsstyrelsen er over for den, der med rimelighed forlader sig på et elektronisk segl fra Digitaliseringsstyrelsen, 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.

14.3 Ansvarsbegrænsninger

Digitaliseringsstyrelsens ansvar efter punkt 14.1 og punkt 14.2 over for både Certifikatindehaver og tredjeparter i det omfang disse parter 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.

15 Anvendelse af OCES organisationscertifikat

Certifikatindehavers anvendelse af OCES organisationscertifikater skal ske i overensstemmelse med det nedenfor anførte.

Nøgleparret må kun anvendes i overensstemmelse med fastlagt tilladt brug og ikke uden for eventuelle begrænsninger, der er meddelt Certifikatindehaver og Certifikatholder.

Certifikatindehaver er forpligtet til at beskytte den private nøgle og forhindre uautoriseret brug heraf. Dette skal bl.a. ske ved at iagttage følgende:

a) at valg af kodeord sikrer, at de ikke umiddelbart kan gættes ved kendskab til Certifikatholder,
b) at der tages rimelige forholdsregler, for at beskytte de sikkerhedsmekanismer, der sikrer den private nøgle mod kompromittering, ændring, tab og uautoriseret brug og
c) at hemmeligholde kodeord, så andre ikke får kendskab til disse.

Certifikatindehaver skal i forbindelse med udstedelse og efterfølgende anvendelse af den private nøgle sikre at dette sker på en sådan måde, at egenkontrollen med nøglen bibeholdes.

16 Anvendelsesbegrænsninger

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

17 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.

18 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.