Den Danske Stat Tillidstjenester

Vilkår for OCES brugercertifikater

Version 1.2.2

6. februar 2024

Indholdsfortegnelse

1 Beskrivelse af certifikater i MitID Erhverv

Disse vilkår regulerer anvendelsen af OCES brugercertifikater udstedt af Den Danske Stat Tillidstjenester (CA1) ved Digitaliseringsstyrelsen til Brugerorganisationer og deres Brugere oprettet i MitID Erhverv løsningen til brug for Brugerorganisationens Brugere. Den Danske Stat Tillidstjenester er godkendt af Digitaliseringsstyrelsen som udsteder af OCES-certifikater.

Efter udstedelsen af et brugercertifikat knyttes dette til brugeridentiteten i MitID Erhverv.

I det følgende benævnes Brugerorganisationen som Certifikatindehaver og Brugere som Certifikatholder.

OCES brugercertifikater er udstedt på baggrund af Digitaliseringsstyrelsens Certifikatpolitik for OCES-medarbejdercertifikater (Offentlige Certifikater til Elektronisk Service), v.7.2. 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 brugercertifikat for den certifikattype, der i certifikatpolitikken er benævnt medarbejdercertifikat. Certifikatpolitikkens regulering af medarbejdercertifikater er således gældende for vilkårenes brugercertifikater.

Vilkårene for udstedelse og anvendelse af OCES brugercertifikater består af to dele, der adresserer henholdsvis Certifikatindehaver (del 1) og Certifikatholder (del 2).

Brugerorganisationens accept af vilkårene omfatter begge dele og Brugerorganisationen tiltræder således også at Brugerne i rollen som Certifikatholder underlægges vilkårene i del 2.

Brugerorganisationens Brugere skal alene acceptere del 2 i forbindelse med udstedelsen af certifikatet til den enkelte Bruger.

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/

Del 1 Vilkår for Certifikatindehaver

3 Brugercertifikaters juridiske gyldighed

En elektronisk signatur afgivet med et OCES brugercertifikat har i Danmark den samme juridiske gyldighed som en almindelig fysisk underskrift.

OCES-certifikater og signaturer 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 signaturer.

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

4 Anvendelsesmuligheder – OCES brugercertifikat

4.1 Generel anvendelse

OCES brugercertifikater i MitID Erhverv er baseret på et persistent certifikater og anvendes, når en fysisk person tilknyttet en Juridisk enhed skal signere data med en elektronisk signatur, der sidestilles med en fysisk signatur.

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 brugercertifikater udstedt af Den Danske Stat Tillidstjenester.

4.2 Anvendelse af pseudonym

Certifikatindehavers Brugeradministrator fastsætter hvilken navngivning Certifikatholder fremstår med i certifikatet. Der kan anvendes pseudonym.

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 brugercertifikater

6.1 Offentliggørelse af certifikatet

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

6.2 Certifikatholders accept af vilkår

I forbindelse med udstedelse af certifikater til Certifikatholder, er Certifikatindehaver forpligtet til følgende:

- Sikre at Certifikatholder accepterer del 2 af nærværende vilkår forud for udstedelsen af certifikatet
- Etablere og dokumentere faste processer for certifikatudstedelsen og sikre at der kan føres bevis for Certifikatholders accept af vilkår

Processer og dokumentationen for Certifikatholders accept af vilkår skal på forlangende udleveres til Digitaliseringsstyrelsen.

De i del 2 indeholdte vilkår til Certifikatholdere er tilgængelige på MitID-Erhverv i en version, der er egnet til distribution hos Brugerorganisationen.

Hvis certifikater udstedes til Certifikatholder via MitID Erhverv med identifikation af Certifikatholder på baggrund af bruger-login, afkræves Certifikatholder accept af vilkår i MitID Erhverv-løsningen.

6.3 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/efterlevelseserklaeringer/

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

6.4 Certifikatets gyldighedsperiode

[CP-Krav 2.1-04]

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

6.5 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 Certifikatholders private nøgle er kompromitteret
iv. Der konstateres unøjagtigheder i eller ændringer af data, der er inkluderet i certifikatet.
v. Certifikatholder ikke længere har tilknytning til Certifikatindehaveren.
vi. 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.

7 Digitaliseringsstyrelsens ret til at spærre certifikater

[CP-krav 4.9.1-01 og afsnit 4.9 generelt]

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 en elektronisk signatur

Forud for at have tillid til et certifikat skal modtageren af en elektronisk signatur 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 en elektronisk signatur udstedt på baggrund af disse vilkår være gyldig og modtageren kan støtte ret herpå, selv om certifikatet efter afgivelsen af signaturen 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 brugercertifikater, herunder generelle forhold ved afgivelse af en elektronisk signatur 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.

10 Digitaliseringsstyrelsens registrering af oplysninger

10.1 Registrering af oplysninger ved oprettelse og anvendelse af certifikater

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

Følgende registreres:

- Certifikatindehavers grundlæggende virksomhedsoplysninger, som registreret i MitID Erhverv løsningen
- Kontaktoplysninger på administratorer
- Certifikatholders navn, UUID, e-mail og evt. CPR-nummer
- 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 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 signaturer eller hemmeligholdelse.

11 Behandling af personoplysninger

11.1 Privatlivspolitik

Certifikater fra Den Danske Stat Tillidstjenester udstedt via MitID Erhverv er omfattet af Digitaliseringsstyrelsens Privatlivspolitik for MitID Erhverv. Privatlivspolitikken 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 DanID 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 22.

12 Ophør af Den Danske Stat Tillidstjenester

Hvis Den Danske Stat Tillidstjeneste ophører med at udstede brugercertifikater, er Den Danske Stat Tillidstjeneste 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 Stat Tillidstjenester.

13 Elektronisk kommunikation

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

Den Danske Stat Tillidstjenesters kommunikation vedr. anvendelsen af certifikater sker som udgangspunkt elektronisk til Certifikatindehavers Organisationsadministrator og Brugeradministrator.

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 en elektronisk signatur fra Digitaliseringsstyrelsen, erstatningsansvarlig for tab efter dansk rets almindelige regler.

For de i Certifikatpolitikkens krav 9.6.1-04 anførte forhold er Digitaliseringsstyrelsen ansvarlig for tab, medmindre Digitaliseringsstyrelsen kan godtgøre, at styrelsen ikke har handlet forsætligt eller uagtsomt.

14.3 Ansvarsbegrænsninger

Digitaliseringsstyrelsens ansvar efter punkt 14.1og 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 Anvendelsesbegrænsninger

Der er ikke fastlagt anvendelsesbegrænsninger for OCES brugercertifikater fra Den Danske Stat Tillidstjenester, jf. dog punkt 4 om begrænsninger i den tekniske anvendelse af certifikater.

16 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.

17 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 Den Danske Stat Tillidstjenester skal indbringes for Københavns Byret.

Del 2 Vilkår for Certifikatholder

18 Indledning

18.1 Generelle forhold

Disse vilkår regulerer anvendelsen af OCES brugercertifikater der udstedes af Den Danske Stat Tillidstjenester ved Digitaliseringsstyrelsen.

Vilkår skal accepteres af Bruger (Certifikatholder) forud for udstedelse af OCES brugercertifikatet. Udstedelsen sker på vegne af den Brugerorganisation (Certifikatindehaver), som Certifikatholder er tilknyttet.

Vilkårene er godkendt af Certifikatindehaver, der desuden har accepteret generelle vilkår for anvendelse af OCES brugercertifikater fra Digitaliseringsstyrelsen.

Efter udstedelsen af et brugercertifikat knyttes dette til Certifikatholders Brugeridentitet i MitID Erhverv.

18.2 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/

19 Anvendelse af OCES brugercertifikat

Certifikatholders anvendelse af OCES brugercertifikat sker på vegne af Certifikatindehaver i overensstemmelse med de mellem parterne fastlagte aftaler, herunder evt. ansættelsesvilkår.

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

Certifikatholder er forpligtet til at beskytte den private nøgle, så kompromittering, ændring, tab og uautoriseret brug forhindres. Der skal således tages rimelige forhold ved beskyttelse af sikkerhedsmekanismer, herunder valg og beskyttelse af kodeord. Certifikatholder skal altid hemmeligholde kodeord, så andre ikke får kendskab hertil.

Certifikatholder 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.

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

20 Forpligtelse ved brug af OCES brugercertifikater

20.1 Opdaterede og korrekte oplysninger

Certifikatholder 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.

Certifikatholder er forpligtet til at spærre certifikatet, hvis de registrerede oplysninger ændrer sig i certifikatets levetid, jf. punkt 20.3 nedenfor.

20.2 Forpligtelser ved afgivelse af en elektronisk signatur

Forud for afgivelse af en elektronisk signatur skal Certifikatholder kontrollere indholdet af certifikatet og sikre at anvendelsen sker inden for de begrænsninger, der måtte fremgå heraf. Ved godkendelsen af den pågældende signering, accepteres samtidig certifikatet og indholdet heri.

20.3 Spærring af certifikat

Certifikatholder skal straks sikre at certifikatet spærres, 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.

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. Certifikatholder må dog altid anvende den private nøgle som grundlag for autentifikation med henblik på at gennemføre en spærring.

Certifikatholders forpligtelse efter denne bestemmelse til at sikre spærring af certifikatet kan opfyldes ved straks at rette henvendelse til Certifikatindehavers Brugeradministrator, der spærrer certifikatet i MitID Erhverv løsningen.

21 Digitaliseringsstyrelsens ret til at spærre certifikater

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

22 Digitaliseringsstyrelsens registrering af oplysninger

22.1 Registrering af oplysninger ved oprettelse og anvendelse af certifikater

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

Følgende registreres:

- Certifikatindehavers grundlæggende organisationsoplysninger, som registreret i MitID Erhverv
- Kontaktoplysninger på administratorer
- Certifikatholders navn, UUID, e-mail og evt. CPR-nummer
- Tidspunktet for udstedelse af certifikatet
- Alle interaktioner med MitID Erhverv relateret til certifikatet
- Oplysninger relateret til efterfølgende spærring og suspension af certifikatet.

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

22.2 Oplysninger der ikke registreres

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

23 Ophør af certifikattjeneste

Hvis Den Danske Stat Tillidstjenester ophører med at udstede brugercertifikater, er Den Danske Stat Tillidstjenester 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 Stat Tillidstjenester.