Den Danske Stat Tillidstjenester

Vilkår for signaturer baseret på kvalificerede personcertifikater

Version 1.1

8. marts 2022

Indholdsfortegnelse

1. Indledning og formål 3
2. Beskrivelse af Signeringsløsningen 3
3. Kontaktinformation 4
4. Den juridiske gyldighed af en elektronisk signatur 4
5. Anvendelsesmuligheder 4
   - 5.1 Generel anvendelse 4
   - 5.2 Certifikatets gyldighedsperiode 4
   - 5.3 Spærreliste 5
6. Signaturløsningens tilgængelighed 5
   - 6.1 Signeringsløsningen 5
7. Dine forpligtelser ved afgivelse af en elektronisk signatur 5
   - 7.1 Opdaterede og korrekte oplysninger om dig 5
   - 7.2 Anvendelse af signaturgenereringsdata 5
   - 7.3 Beskyttelse af identifikationsmiddel 5
   - 7.4 Underretning af Digitaliseringsstyrelsen og spærring af certifikat 5
   - 7.5 Beskyttelse på et kvalificeret elektronisk signaturgenereringssystem (QSCD) 6
8. Forpligtelser som modtager af en signatur 6
9. Support 7
10. Digitaliseringsstyrelsens registrering af oplysninger 7
    - 10.1 Registrering af oplysninger ved afgivelse af en signatur 7
    - 10.2 Lagring af data 7
    - 10.3 Oplysninger der ikke registreres 7
    - 10.4 Offentliggørelse af certifikatet 8
11. Behandling af personoplysninger 8
    - 11.1 Privatlivspolitik 8
    - 11.2 Dataansvar 8
12. Elektronisk kommunikation 8
13. Ansvar ved afgivelse og modtagelse af en elektronisk signatur 8
    - 13.1 Ansvar for indehaver af et certifikat 8
    - 13.2 Ansvar for modtager af digitalt underskrevne data 8
    - 13.3 Ansvar ved afgivelse af tidsstempel 9
14. Ændring af vilkår 9
15. Lovvalg og tvister 9
16. Ophør af Den Danske Stat Tillidstjenester 9

1. Indledning og formål

Disse vilkår regulerer privatpersoners afgivelse af en elektronisk signatur (herefter signatur) på dokumenter og andre data hos selvbetjeningsløsninger, der er tilsluttet signeringsløsningen i NemLog-in.

Vilkårene skal accepteres i signeringsløsningen før der kan afgives en signatur.

Hvor ikke andet er anført, er er disse vilkår ligeledes gældende for udstedelsen af tidsstempler, der sammenkobles med signaturen.

Afgivelse af en signatur i signaturløsningen forudsætter at du som privatperson kan autentificere dig med dit private MitID.

Du skal behandle dit MitID i overensstemmelse med de regler og vilkår (MitID Slutbrugervilkår), der er gældende for dette og som accepteres i forbindelse med udstedelsen et MitID.

Signaturer og tidsstempler i signeringsløsningen er udstedt af Digitaliseringsstyrelsens Tillidstjenester på vegne af den danske stat.

2. Beskrivelse af Signeringsløsningen

Signeringsløsningen understøtter afgivelse af en signatur på dokumenter og anden data.

Signaturen er en kvalificeret elektronisk signatur, der er anerkendt i EU og EØS. Den danske stat 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). Den afgivne signatur har derfor retskraft i hele Europa på samme måde som en fysisk underskrift.

Når du benytter løsningen, udstedes et certifikat, der herefter indgår i signaturen. Ud over en række tekniske oplysninger indeholder certifikatet dit navn og et unikt løbenummer, og sikrer at det efterfølgende kan konstateres, at det er dig, der har afgivet signaturen.

Certifikatet kan alene anvendes til afgivelse af én signatur. Næste gang du skal afgive en signatur udstedes et nyt certifikat.

De anvendte tidsstempler er kvalificerede tidsstempler, der ligeledes er anerkendt i EU og EØS. Tidsstemplingen dokumenterer tidspunktet for afgivelse af signaturen, herunder at certifikat og de signerede data var til stede på underskriftstidspunktet

Disse vilkår er udarbejdet i overensstemmelse med Offentlig certifikatpolitik for kvalificerede personcertifikater version 1.1, der danner grundlaget for Digitaliseringsstyrelsens udstedelse af kvalificerede personcertifikater.

De kvalificerede tidsstempler, der sammenkobles med den elektroniske signatur er udstedt på baggrund af Digitaliseringsstyrelsens Offentlig politik for kvalificeret tidsstempling, version1.1.

Certifikatpolitikken, politik for tidsstempling kan læses på certifikat.gov.dk

Den detaljerede beskrivelse af tillidstjenesterne (Practice) kan læses på www.CA1.gov.dk.

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

3. Kontaktinformation

Digitaliseringsstyrelsen
Att. Den Danske Stat Tillidstjenester
Landgreven 4
1301 København K

Tlf. 3392 5200
info@ca1.gov.dk

CVR: 34051178

4. Den juridiske gyldighed af en elektronisk signatur

En signatur fra signaturløsningen afgivet af dig som privatperson forpligter på samme måde, som din fysiske underskrift. Det er derfor væsentligt, at du er opmærksom på, hvad du skriver under på, når du afgiver signaturen.

Signaturen har ensartet anerkendelse og ligestilles med en fysisk underskrift i alle medlemslande.

Tidsstemplet sikrer, at det kan dokumenteres hvornår signaturen blev afgivet samt hvilket dokument eller anden data der blev underskrevet på dette tidspunkt.

5. Anvendelsesmuligheder

5.1 Generel anvendelse

Signaturer med tilhørende certifikater fra signeringsløsningen kan anvendes til at afgive viljeerklæringer og til aftaleindgåelser med både private parter og offentlige organisationer.

Det er alene muligt at signere dokumenter og anden data online hos tjenesteudbydere, der er tilsluttet til signeringsløsningen. Det er ikke muligt at anvende signeringsløsningen til at signere e-mails eller til hemmeligholdelse (kryptering).

Der er ikke fastlagt begrænsninger til hvilke typer aftaler og forpligtigelser du kan indgå ved anvendelse af en signatur fra signeringsløsningen.

5.2 Certifikatets gyldighedsperiode

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

gyldighed efter afgivelsen af signaturen, er alene begrundet i tekniske hensyn til de systemer, der efterfølgende skal læse signaturen.

5.3 Spærreliste
Information om status på udstedte certifikater kan til enhver tid tilgås via signaturløsningens spærreliste på https://www.ca1.gov.dk/crls/

6. Signaturløsningens tilgængelighed

6.1 Signeringsløsningen
Signeringsløsningen og tilknyttede services er tilgængelig døgnet rundt alle årets dage.

Digitaliseringsstyrelsen er dog ikke ansvarlig for at ovenstående tilgængelighed leveres.

7. Dine forpligtelser ved afgivelse af en elektronisk signatur

7.1 Opdaterede og korrekte oplysninger om dig
Forud for afgivelse af signaturen præsenteres du i signaturløsningen for dit navn. Signeringsløsningen har denne oplysninger fra dit MitID.

Du skal sikre dig at dit navn fremstår korrekt, da det inkluderes i signaturen og det tilhørende certifikat med henblik på at dokumentere, at signaturen er afgivet af dig.

Ved din godkendelse af den pågældende signering, accepterer du samtidig certifikatet, og at de anførte oplysninger om dit navn er korrekte.

Hvis oplysningerne ikke er korrekte, skal du afbryde signeringsprocessen og opdatere dit MitID i overensstemmelse med de regler, der gælder for dette.

7.2 Anvendelse af signaturgenereringsdata
Du kan ikke anvende signaturgenereringsdata (den private nøgle) til signering af andre certifikater.

7.3 Beskyttelse af identifikationsmiddel

Du skal beskytte dit MitID og tilhørende sikkerhedsmekanismer (f.eks. kodeord og MitID App), du anvender til brug for afgivelse af signaturen, i overensstemmelse med de vilkår, der er gældende herfor således at der er taget rimelige forholdsregler for, at der ikke afgives en signatur i dit navn.

Hvis du har mistanke om at dit MitID er kompromitteret skal du suspendere eller spærre det i overensstemmelse med MitID Slutbrugervilkårene, således at det ikke uberettiget kan anvendes til at afgive en signatur i dit navn.

7.4 Underretning af Digitaliseringsstyrelsen og spærring af certifikat
Som udgangspunkt behøver du aldrig af spærre et certifikat fra signeringsløsningen.

Du er dog forpligtet til straks at underrette Digitaliseringsstyrelsen og spærre dit certifikat, hvis du konstaterer unøjagtigheder eller ændringer af data, der er inkluderet i certifikatet inden udløb af certifikatets gyldighedsperiode, jf. punkt 5.2.

Spærring af et certifikatkan skal ske via www.ca1.gov.dk. Spærring kan ske døgnet rundt. Du kan ligeledes sende anmodning om spærring med fysisk post til Digitaliseringsstyrelsens adresse som oplyst i punkt 3.

Spærring af et tidligere anvendt certifikat er igen hindring for at du kan få udsted et nyt certifikat til brug for afgivelse af en ny signatur.

Hvis du har mistanke om at dit MitID er kompromitteret, skal du spærre det i overensstemmelse med de vilkår, der er gældende herfor, således at det ikke uberettiget kan anvendes til at afgive en signatur i dit navn, jf. punkt 7.3 ovenfor.

7.5 Beskyttelse på et kvalificeret elektronisk signaturgenereringssystem (QSCD)

Signaturløsningen sikrer, at den signatur, som du afgiver genereres under en høj grad af sikkerhed og kobles til det dokument eller anden data, som du præsenteres for i selvbetjeningsløsningen.

Til brug herfor anvender Digitaliseringsstyrelsen et såkaldt kryptografisk modul (QSCD), hvorefter signaturgenereringsdata forbliver under din kontrol under signeringsprocessen.

8. Forpligtelser som modtager af en signatur

Forud for at have tillid til et certifikat skal modtageren af en signatur fra signeringsløsningen sikre sig følgende:

- At certifikatet er gyldigt og ikke spærret - dvs. ikke opført på certificeringscenterets 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 certifikatpolitikken, jf. punkt 2.

Inden et tidsstempel accepteres skal modtageren af en signatur 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 en signatur fra signeringsløsningen være gyldig og modtageren kan støtte ret herpå, selv om certifikatet efter afgivelsen af signaturen er udløbet eller spærret.

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

Supporthenvendelser vedr. signering, herunder tekniske problemer ved afgivelse af signatur, skal rettes til den tjenesteudbyder, der er ansvarlig for selvbetjeningsløsningen, hvori du skal underskrive et dokument eller anden data.

10. Digitaliseringsstyrelsens registrering af oplysninger

10.1 Registrering af oplysninger ved afgivelse af en signatur

Når du afgiver en signatur og der oprettes et certifikat registrer Digitaliseringsstyrelsen en række oplysninger om dig, certifikatet og hvilken tjenesteudbyder, signaturen har været anvendt hos.

Følgende registreres:

- Tidspunkt for signering
- Dit navn (fornavn og efternavn)
- Din alder
- Det sikringsniveau (Level Of Assurance) du er autoriseret med over for tjenesten
- CPR/session UUID
- Referencetekst
- SAML assertion

10.2 Lagring af data

Digitaliseringsstyrelsen gemmer data om dig og din anvendelse af Signaturer og certifikater fra signaturløsningen i syv (7) år fra tidspunktet for afgivelse af en signatur. Oplysninger om de accepterede vilkår ved anvendelsen gemmes ligeledes.

Opbevaring sker af hensyn til oprettelse af et højt niveau for privatlivsbeskyttelse, efterforskning og anvendelse som bevismateriale, f.eks. i retssager. Alle data relateret en signatur slettes løbende, når syvårs fristen for certifikatets udløbsdato nås.

10.3 Oplysninger der ikke registreres

Digitaliseringsstyrelsen registrerer ikke oplysninger om hvilket dokument eller andre data du har signeret i signaturløsningen.

10.4 Offentliggørelse af certifikatet
Certifikater fra Certificeringscenteret for den Danske Stat offentliggøres ikke i et offentligt tilgængeligt register. Certifikatet eksisterer alene indlejret i signaturen.

11. Behandling af personoplysninger

11.1 Privatlivspolitik
Du kan i Digitaliseringsstyrelsens privatlivspolitik (www.digst.dk) læse hvilke oplysninger Digitaliseringsstyrelsen indsamler, opbevarer og behandler om dig i forbindelse med udstedelse af certifikater og afgivelse af signaturer.

11.2 Dataansvar
Digitaliseringsstyrelsen er dataansvarlig for dine personoplysninger som behandles i signeringsløsningen. Nets Dan ID A/S er databehandler for Digitaliseringsstyrelsen.

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

Personoplysninger slettes efter 7 år.

12. Elektronisk kommunikation

Ved accept af disse vilkår gives der samtidig samtykke til at Digitaliseringsstyrelsen i forbindelse med drift af signeringsløsningen kan henvende sig til dig via e-mail. Henvendelser kan f.eks. vedrøre driftsrelateret information, sikkerhedsrelaterede forhold, ændringer og ophør.

13. Ansvar ved afgivelse og modtagelse af en elektronisk signatur

13.1 Ansvar for indehaver af et certifikat
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.

13.2 Ansvar for modtager af digitalt underskrevne data
Digitaliseringsstyrelsen er over for den, der med rimelighed forlader sig på en kvalificeret elektronisk signatur fra signaturløsningen, 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.

Digitaliseringsstyrelsens ansvar over for erhvervsdrivende og offentlige myndigheder 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.

13.3 Ansvar ved afgivelse af tidsstempel

Det ovenfor under punkt 13.1 og punkt 13.2 anførte er ligeledes gældende for Digitaliseringsstyrelsens afgivelse af tidsstempler.

14. Ændring af vilkår

Digitaliseringsstyrelsen har ret til uden varsel at ændre disse vilkår. Såfremt der foretages ændringer, vil du blive bedt om at acceptere opdaterede vilkår næste gang, du ønsker at afgive en signatur.

15. Lovvalg og tvister

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

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

16. Ophør af Den Danske Stat Tillidstjenester

Hvis Digitaliseringsstyrelsen nedlægger de tillidstjenester der udbydes på vegne af Den Danske Stat, er styrelsen berettiget til at videre give alle registrerede oplysninger til en tredjepart med henblik på at denne kan indtræde i de forpligtelser, som Digitaliseringsstyrelsen har efter disse vilkår.