

NemLog-in vilkår kvalificerede personcertifikater

Version 1.0

Version	Dato	Bemærkninger	Ansvarlig
1.0	29/9 2021	Samlet version til certificering	ACB

Indholdsfortegnelse

1.	INDLEDNING OG FORMÅL.....	3
2.	BESKRIVELSE AF SIGNERINGSTJENESTEN	3
3.	KONTAKTINFORMATION.....	2
4.	DEN JURIDISKE GYLDIGHED AF EN ELEKTRONISK SIGNATUR.....	2
5.	ANVENDELSESMULIGHEDER	3
5.1	Generel anvendelse	3
5.2	Certifikatets gyldighedsperiode	3
6.	TJENESTENS TILGÆNGELIGHED.....	3
6.1	Signeringstjenesten	3
6.2	Spærreliste	3
7.	DINE FORPLIGTELSE VED AFGIVELSE AF EN ELEKTRONISK SIGNATUR	3
7.1	Opdaterede og korrekte oplysninger om dig.....	3
7.2	Korrekte oplysninger i certifikatet.....	4
7.3	Anvendelse af nøgler	4
7.4	Beskyttelse af identifikationsmiddel.....	4
7.5	Underretning af Digitaliseringsstyrelsen og spærring af certifikat.....	4
7.6	Beskyttelse på et kvalificeret elektronisk signaturgenereringssystem (QSCD)	5
8.	FORPLIGTELSE SOM MODTAGER AF EN ELEKTRONISK SIGNATUR.....	5
9.	SUPPORT.....	6
10.	DIGITALISERINGSSTYRELSENS REGISTRERING AF OPLYSNINGER.....	6
10.1	Registrering af oplysninger ved oprettelse og anvendelse af certifikat.....	6
10.2	Hændelseslog.....	7
10.3	Lagring af data.....	7
10.4	Oplysninger der ikke registreres	7
10.5	Offentliggørelse af certifikatet	7
11.	BEHANDLING AF PERSONOPLYSNINGER.....	7
11.1	Privatlivspolitik	7
11.2	Dataansvar	7
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	8
14.	ANVENDELSESBEGRÆNSNINGER.....	8
15.	ÆNDRING AF VILKÅR.....	9
16.	LOVVALG OG TVISTER.....	9
17.	OPHØR AF DIGITALISERINGSSTYRELSENS SIGNERINGSTJENESTEN	9

1. Indledning og formål

Disse vilkår regulerer private borgeres afgivelse af en kvalificeret elektronisk signatur (elektronisk signatur) under anvendelsen af kvalificerede personcertifikater udstedt af den danske Stat via NemLog-in serviceområdet Digital Signering (signeringstjenesten) til brug i offentlige og private Selvbetjeningsløsninger.

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

Afgivelse af en elektronisk signatur forudsætter at du som bruger kan autentificere dig over for NemLog-in signeringstjenesten med et godkendt identifikationsmiddel. Dit private MitID er som udgangspunkt godkendt til anvendelse i tjenesten.

En oversigt over godkendte identifikationsmidler findes på [www.\[...\].dk](http://www[...]dk).

Du skal behandle dit MitID eller andet identifikationsmiddel i overensstemmelse med de regler og vilkår, der er gældende for dette. Regler for anvendelse af MitID følger af særskilte vilkår (MitID Slutbrugervilkår), som du skal acceptere i forbindelse med udstedelsen heraf. MitID reglerne skal også overholdes i forbindelse med anvendelse af personcertifikater til afgivelse af en elektronisk signatur.

Den elektroniske signatur er sammenkoblet med et kvalificeret tidsstempel, der præcist angiver hvornår den pågældende signatur er afgivet.

Certifikater og tidsstempel til brug for elektronisk signatur er udstedt af Digitaliseringsstyrelsens certificeringscenter på vegne af den danske stat.

[Kvalificeret Personcertifikat: CP-krav 1.4.2-03 og CP-krav 1.4.2-04, CP-krav 6.2.8-01, CP-krav 6.4.1-02]

[Kvalificeret tidsstempling: CP-krav 6.3-01, CP-krav 6.3-02]

2. Beskrivelse af Signeringstjenesten

Når du anvender et kvalificeret personcertifikat, understøtter signeringstjenesten alene afgivelse af en elektronisk signatur på elektroniske data, herunder dokumenter online hos Tjenesteudbydere, der har en aftale med NemLog-in. Det er ikke muligt at anvende tjenesten til at signere e-mails eller foretage hemmeligholdelse/kryptering.

Den elektroniske signatur er en kvalificeret signatur, der er anerkendt i EU. 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.

Personcertifikaterne i tjenesten, har karakter af éngangscertifikater, der oprettes specifikt til afgivelse af én elektronisk signatur. Efter afgivelse af signaturen slettes de signaturgenereringsdata (herunder den private nøgle), der er knyttet til certifikatet og certifikatet kan herefter ikke bruges igen. For at sikre at den elektroniske signatur kan modtages og læses af en bred portefølje af systemer udløber certifikatet dog først efter 30 dage. Næste gang du har behov for at afgive en elektronisk signatur oprettes et nyt certifikat med tilhørende nye signaturgenereringsdata.

Disse vilkår er udarbejdet i overensstemmelse med Offentlig certifikatpolitik for kvalificerede personcertifikater v1.0, der danner grundlaget for Digitaliseringsstyrelsens udstedelse af kvalificerede personcertifikater. Vilkårene omfatter også certifikatpolitikken for kvalificerede certifikater.

De kvalificerede tidsstempler, der sammenkobles med den elektroniske signatur 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 signeringstjenesten (Certificate Practice statement) kan læses på certifikat.gov.dk.

Digitaliseringsstyrelsen CA udsteder en række andre certifikattyper til brug i erhvervsmæssig sammenhæng. Disse certifikattyper er alle underlagt særskilte vilkår.

[Kvalificeret Personcertifikat CP-krav 1.4.2-03 og 1.4.2-04]

[Kvalificeret tidsstempling: CP-krav 6.3-02]

3. Kontaktinformation

Digitaliseringsstyrelsen har følgende kontaktinformation:

Digitaliseringsstyrelsen
Landgreven 4
1301 København K

Tlf. 3392 5200
[...][@digst.dk](mailto:info@digst.dk)

CVR: 34051178

4. Den juridiske gyldighed af en elektronisk signatur

En elektronisk signatur fra Signatortjenesten forpligter på samme måde som hvis du skrev under med din fysiske underskrift. Det er derfor væsentligt at du er opmærksom på, hvad du skriver under på, når du afgiver signaturen.

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

5. Anvendelsesmuligheder

5.1 Generel anvendelse

[Kvalificeret Personcertifikat CP-krav 2.1-03, 9.8-1 og CP-krav 1.4.2-04 og eIDAS art. 13]

En kvalificeret elektronisk signatur fra Signatortjenesten kan anvendes, når en fysisk person skal signere data med en kvalificeret elektronisk signatur, der sidestilles med en fysisk underskrift og som har ensartet anerkendelse i alle medlemslande.

Signeringstjenesten kan alene anvendes til afgive en elektronisk signatur online via de tjenesteudbydere, der er tilmeldt tjenesten. Dette betyder at certifikatet til signaturen f.eks. ikke kan anvendes til at signere mails via en e-mailklient eller til hemmeligholdelse (kryptering).

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

5.2 Certifikatets gyldighedsperiode

[Kvalificeret Personcertifikat CP-krav 2.1-04]

Certifikatet har en gyldighedsperiode på 30 dage. Idet den private nøgle tilhørende certifikatet slettes i forbindelse med afgivelse den elektroniske signatur er det ikke muligt at generere flere signaturer på baggrund af samme certifikat. Certifikatets forlængende gyldighed efter afgivelsen af den elektroniske signatur og sletning af den private nøgle, er alene begrundet i tekniske hensyn til de systemer, der efterfølgende skal læse signaturen.

6. Tjenestens tilgængelighed

6.1 Signeringstjenesten

Tjenesten er tilgængelig døgnet rundt alle årets dage.

Digitaliseringsstyrelsen er dog ikke ansvarlig for at ovenstående tilgængelighed leveres.

Information om driftsstatus kan tilgås på www.digst.dk/[...].

6.2 Spærreliste

[Kvalificeret Personcertifikat CP-krav 2.1-03, CP-krav 4.10-02]

Information om status på udstedte certifikater kan til enhver tid tilgås via Tjenestens spærreliste på [www\[..\].dk](http://www[..].dk). Spærrelisten er tilgængelig døgnet rundt alle årets dage.

7. Dine forpligtelser ved afgivelse af en elektronisk signatur

[Kvalificeret Personcertifikat: CP, afsnit 4.0 og CP-krav 4.5.1-01, CP-krav 4.4.1-01]

7.1 Opdaterede og korrekte oplysninger om dig

Du skal sikre, at oplysninger om dig, der udgør grundlaget for udstedelsen af et certifikat, er korrekte og fyldestgørende på tidspunktet for afgivelse af en elektronisk signatur. Signeringstjenesten modtager

oplysninger om dig fra det identifikationsmiddel, f.eks. MitID, som du anvender i forbindelse med autentifikation overfor tjenesten. Du bliver præsenteret for oplysningerne forud for afgivelse af signaturen.

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

7.2 Korrekte oplysninger i certifikatet

[Kvalificeret Personcertifikat CP-krav 4.5.1-01, CP-krav 4.4.1-01]

Forud for afgivelse af en signatur skal du kontrollere indholdet af certifikatet. Du skal i denne forbindelse sikre dig, at anvendelsen sker inden for de begrænsninger, der måtte fremgå heraf. Ved din godkendelse af den pågældende signering, accepterer du samtidig certifikatet og indholdet heri.

7.3 Anvendelse af nøgler

[Kvalificeret Personcertifikat: CP-krav 4.5.1-01]

Du må ikke anvende den private nøgle til signering af andre certifikater.

[I praksis er det teknisk umuligt af komme i konflikt med kravet grundet tjenestens tekniske indretning. Bestemmelsen er alene medtaget for at sikre Compliance til certifikatpolitikken. Ud fra et forbrugerjuridisk synspunkt burde bestemmelsen udgå, da den skaber tvivl og er irrelevant]

7.4 Beskyttelse af identifikationsmiddel

[Kvalificeret Personcertifikat: CP-krav 4.5.1-01 –De dele, der beskriver beskyttelse af nøgler. Må nødvendigvis rette sig mod identifikationsmidlet]

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

7.5 Underretning af Digitaliseringsstyrelsen og spærring af certifikat

Dit MitID anvendes til at autentificere dig over for signeringstjenesten. Det er derfor vigtigt at du beskytter det i overensstemmelse med vilkårene for MitID, dvs. beskytter de udstedte identifikationsmidler, f.eks. din MitID App eller tokens og spærre disse, hvis der foreligger eller er mistanke om misbrug.

[Kvalificeret Personcertifikat: CP-krav 4.5.1-01, litra b og krav 2.1-04]

Du er forpligtet til straks at underrette Digitaliseringsstyrelsen og spærre dit certifikat hvis nedenstående opstår inden udløb af certifikatets gyldighedsperiode:

- i. Din adgang til private nøgle er mistet, herunder at den er stjålet eller potentielt kompromitteret.

- ii. Din egenkontrol med den private nøgle er mistet på grund af kompromittering af aktiveringsdata (fx PIN kode).
- iii. Du konstaterer unøjagtigheder eller ændringer af data, der er inkluderet i certifikatet.

Den private nøgle må ikke anvendes efter at du har fået mistanke om kompromittering bortset fra evt. autentifikation i forbindelse med spærring.

Spærring af et certifikat kan ske via [www.\[...\].dk](http://www[...]dk) eller hos [Support] på telefon [...]. 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 ikke til hindring for at du kan få udstedt et nyt certifikat til brug for afgivelse af en ny elektronisk signatur.

Hvis du har mistanke om at dit identifikationsmiddel 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 elektronisk signatur i dit navn.

7.6 Beskyttelse på et kvalificeret elektronisk signaturgenereringssystem (QSCD)

[Kvalificeret Personcertifikat: CP-krav 4.5-01, litra f og g]

Digitaliseringsstyrelsen sikrer 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 NemLog-in signeringstjenesten. Det er således alene er dig, der har kontrollen med den private nøgle og certifikat ved afgivelse af en elektronisk signatur.

8. Forpligtelser som modtager af en elektronisk signatur

[Kvalificeret Personcertifikat: CP-krav 2.1-03 og 05.]

[Kvalificeret tidsstempling: Cp-krav 6.6-01]

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 CA's 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 denne CP.

Inden et tidsstempel accepteres skal modtageren af elektronisk 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 elektronisk signatur være gyldig og modtageren kan støtte ret på den, selv om certifikatet efter afgivelsen af signaturen er udløbet eller spærret.

Digitaliseringsstyrelsen har indsat nærmere information i Certifikatet om anvendelsen heraf. Informationen kan læses via [PDS – se ETSI A.2].

9. Support

Supporthenvendelser vedr. signeringstjenesten, herunder tekniske problemer ved afgivelse af en elektronisk signatur skal rettes til [Det centrale Supporttilbud].

Du kan finde detaljerede oplysninger om tjenesten på [www\[...\]dk](http://www[...]dk)

[Åbningstider.]

[Intern bemærkning: Bemærk at der er en forvaltningsretlig vinkel på ovenstående]

10. Digitaliseringsstyrelsens registrering af oplysninger

[Kvalificeret Personcertifikat CP-krav 4.4.1-09]

10.1 Registrering af oplysninger ved oprettelse og anvendelse af certifikat

Når du opretter og anvender et certifikat registrerer Digitaliseringsstyrelsen en række oplysninger om dig, certifikatet og den efterfølgende anvendelse.

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

Hvis du er anonym, sker der ingen registrering af dit navn.

10.2 Hændelseslog

[Kvalificeret Personcertifikat CP-krav 2.1-03 og krav 5.8-06]

Alle dine handlinger i forbindelse med afgivelse af signaturer registreres i en hændelseslog, hvor du bl.a. har adgang til at kontrollere hvor din signatur have været anvendt. Hændelsesloggen er tilgængelig på [www\[...\].dk](http://www[...].dk). Du logger på hændelsesloggen med det identifikationsmiddel, som du anvendte til brug for autentifikation over for signeringstjenesten.

10.3 Lagring af data

[Kvalificeret Personcertifikat CP-krav 5.5.2-01, krav 4.4.1-13, CP-krav 5.8-06]

Digitaliseringsstyrelsen gemmer data om dig og din anvendelse af certifikater i Signatortjenesten i syv (7) år fra tidspunktet for afgivelse af en signatur. Oplysninger om de accepterede vilkår for anvendelse af certifikater 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 til en bestemt anvendelse af et certifikat slettes løbende, når syvårs fristen for certifikatets udløbsdato nås.

10.4 Oplysninger der ikke registreres

Digitaliseringsstyrelsen registrerer ikke oplysninger om hvilket dokument eller hvilke data du har underskrevet.

10.5 Offentliggørelse af certifikatet

[Kvalificeret Personcertifikat CP-krav 4.4.1-09]

Certifikater fra NemLog-in Digital signering offentliggøres ikke i et offentligt tilgængeligt register. Certifikatet eksisterer alene indlejret i den elektroniske signatur.

11. Behandling af personoplysninger

[Kvalificeret Personcertifikat CP-afsnit 9.4, CP-krav 9.4.5-01]

11.1 Privatlivspolitik

Du kan i NemLog-in Privatlivspolitikken ([www\[...\].dk](http://www[...].dk)) læse hvilke oplysninger Digitaliseringsstyrelsen indsamler, opbevarer og behandler om dig i forbindelse med udstedelse af certifikater og afgivelse af elektronisk signatur.

11.2 Dataansvar

Digitaliseringsstyrelsen er dataansvarlig for dine personoplysninger som behandles i NemLog-in Signeringstjenesten. 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 tjenesten 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

[Kvalificeret Personcertifikat: CP-krav 9.61-03, -04 og 9.8-01]

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 NemLog-in Signaturtjenesten, 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. Anvendelsesbegrænsninger

[Kvalificeret Personcertifikat: CP-krav 9.8-02, EIDAS-artikel 13, stk. 2]

De kvalificerede personcertifikater fra Digitaliseringsstyrelsen er til brug for anvendelse i forbindelse med afgivelse af viljeerklæringer og aftaleindgåelser med både private parter og offentlige organisationer.

Afgivelse af den elektroniske signatur skal ske via Signaturtjenesten.

Der er ikke fastlagt anvendelsesbegrænsninger for Kvalificerede personcertifikater, der udstedes af Digitaliseringsstyrelsen.

15. 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 afgiver en elektronisk signatur.

[Kvalificeret Personcertifikat: CP-krav 4.6.3-03]

16. Lovvalg og tvister

[Kvalificeret Personcertifikat: CP-krav 9.13-01]

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

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

17. Ophør af Digitaliseringsstyrelsens signeringstjenesten

[Kvalificeret Personcertifikat: CP-krav 4.4.1-09]

Hvis Digitaliseringsstyrelsen nedlægger sin CA-tjeneste, 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.