

VILKÅR FOR KORTTIDS- BRUGERSIGNATURER

Version: 1.3

Forfatter: Digitaliseringsstyrelsen, Den Danske Stat Tillidstjenester

Udgivelsesdato: Marts 2026

Dette dokument gælder også som bilag 4 til Vilkår for Brugerorganisationer.



Indholdsfortegnelse

1. Brugersignaturer i Signeringsløsningen.....	4
2. Kontaktinformation	5
3. Brugercertifikaters juridiske gyldighed.....	7
4. Anvendelsesmuligheder –brugersignaturer	7
4.1. Generel anvendelse	7
4.2. Pseudonym.....	8
5. Tilgængelighed	8
5.1. Signeringsløsningen	8
5.2. Spærreliste	8
6. Forpligtelser ved brug af kvalificerede brugercertifikater	8
6.1. Opdaterede og korrekte oplysninger	8
6.2. Offentliggørelse af certifikatet	8
6.3. Certifikatets gyldighedsperiode	8
6.4. Spærring af certifikat.....	9
7. Forpligtelser som modtager af en elektronisk signatur	9
8. Support	10
8.1. Generel support	10
9. Behandling af personoplysninger	10
9.1. Privatlivspolitik	10
9.2. Dataansvar	10
9.3. Registrering af oplysninger	10
10. Ophør af Den Danske Stat Tillidstjenester	10
11. Elektronisk kommunikation.....	11
12. Digitaliseringsstyrelsens ansvar.....	11
12.1. Ansvar over for Certifikatindehaver.....	11
12.2. Ansvar for tredjeparter	11
12.3. Ansvarsbegrænsninger.....	11
12.4. Ansvar ved afgivelse af tidsstempel.....	11
13. Anvendelsesbegrænsninger	11
14. Ændringer til vilkår	12
15. Lovvalg og tvister	12
16. Indledning	14



16.1.	Generelle forhold	14
16.2.	Kontaktinformation.....	14
17.	Forpligtelser ved anvendelse af brugercertifikat	15
17.1.	Generelle forhold	15
17.2.	Begrænsninger i anvendelse af certifikat og nøgler	15
17.3.	Beskyttelse af identifikationsmiddel.....	15
17.4.	Opdaterede og korrekte oplysninger	15
17.5.	Beskyttelse på et kvalificeret elektronisk signaturgenereringssystem (QSCD)	16
17.6.	Spærring af certifikat.....	16
18.	Digitaliseringsstyrelsens registrering af oplysninger	16
18.1.	Registrering af oplysninger ved oprettelse og anvendelse af certifikater	16
18.2.	Oplysninger der ikke registreres	17
18.3.	Oversigt over signaturanvendelse	17
18.4.	Lagring af data.....	17
19.	Ophør af Den Danske Stat Tillidstjenester	17



1. Brugersignaturer i Signeringsløsningen

Disse vilkår regulerer erhvervsbrugeres afgivelse af en kvalificeret eller OCES elektronisk brugersignatur (elektronisk signatur) ved anvendelsen af kvalificerede brugercertifikater eller OCES brugercertifikater udstedt af Den Danske Stat Tillidstjenesters signeringsløsning til brug i offentlige og private Selvbetjeningsløsninger. Den Danske Stat Tillidstjenester er godkendt af Digitaliseringsstyrelsen som udsteder af kvalificerede certifikater jf. eIDAS-forordningen og OCES-certifikater.

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

I det følgende benævnes Brugerorganisationen som Certifikatindehaver og en Bruger som Certifikatholder.

Vilkårene er udarbejdet i overensstemmelse med Samlet offentlig certifikatpolitik for OCES og kvalificerede certifikater version 8.0, der danner grundlaget for Digitaliseringsstyrelsens udstedelse af brugercertifikater. De kvalificerede tidsstempler, der sammenkobles med den elektroniske signatur er udstedt på baggrund af den europæiske standard ETSI EN 319 421. Både certifikatpolitik og ETSI EN 319 421 er omfattet af disse vilkår.

Disse vilkår benytter betegnelsen brugercertifikat for den certifikattype, der i certifikatpolitikken er benævnt medarbejdercertifikat. Certifikatpolitikken regulerer af medarbejdercertifikater er således gældende for vilkårenes brugercertifikater og de elektroniske signaturer, der er udstedt på baggrund heraf.

Certifikatpolitikken kan læses på:

<https://certifikat.gov.dk/>

ETSI EN 319 421 kan findes på

<https://www.etsi.org/standards>

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

Vilkårene for udstedelse og anvendelse af 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 Brugere 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 i Signeringsløsningen.



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/



Den Danske Stat Tillidstjenester

Del 1

Vilkår for Certifikatindehaver



3.Brugercertifikaters juridiske gyldighed

Den Danske Stat Tillidstjenester agerer som 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, som ændret ved Europa-Parlamentets og Rådets forordning (EU) Nr. 2024/1183 af 11. april 2024 om ændring af forordning (EU) nr.910/2014 for så vidt angår fastlæggelse af den europæiske ramme for digital identitet. elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (eIDAS forordningen). Afgivne kvalificeret brugersignatur har retskraft i EU og EØS på samme måde som en fysisk underskrift. Afgivne OCES brugersignatur har i Danmark retskraft på samme måde som en fysisk underskrift. OCES brugersignaturer afgivet på baggrund heraf er ikke nødvendigvis 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 brugersignaturer.

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 tidsstemplet angiver, og integriteten af de data, som dato- og tidsangivelsen er knyttet til.

4.Anvendelsesmuligheder – brugersignaturer

4.1.Generel anvendelse

Et brugercertifikat kan anvendes, når en fysisk person tilknyttet en Juridisk enhed skal signere data med en elektronisk signatur, der sidestilles med en fysisk underskrift og som skal have ensartet anerkendelse i alle medlemslande, jf. punkt 3.

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

Brugersignaturer i Signeringsløsningen baserer sig på kryptografiske nøgler, der genereres til lejligheden i et centralt kvalificeret signaturgenereringssystem (QSCD). Den private nøgle slettes umiddelbart efter generering af hver enkelt elektronisk signatur.

Brugersignaturer og brugercertifikater er ikke til brug for Autentifikation. Selve autentifikationen over for en tjenesteudbyder håndteres af Brugerens eID identifikationsmiddel.

Signaturer udstedes i LTV format.

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



4.2.Pseudonym

Certifikatindehavers brugeradministrator fastsætter hvilken navngivning Certifikatholder fremstår med i certifikatet. Der kan anvendes Pseudonym.

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 spærreliste på:

www.ca1.gov.dk/tilbagekald-certifikater

6.Forpligtelser ved brug af kvalificerede brugercertifikater

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 baserer sig på de oplysninger, der i forvejen er registreret i MitID Erhverv.

6.2.Offentliggørelse af certifikatet

Der sker ingen offentliggørelse af certifikater udstedt via Signeringsløsningen. Certifikatet eksisterer alene indlejret i signaturen.

6.3.Certifikatets gyldighedsperiode

Certifikatet har en gyldighedsperiode på enten 12 timer eller 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 begrundet i tekniske hensyn til de systemer, der efterfølgende skal læse signaturen.



Den Danske Stat Tillidstjenester

6.4. Spærring af certifikat

Idet Signeringsløsningen sletter den private nøgle tilhørende certifikatet umiddelbart efter afgivelse af den elektroniske signatur, og certifikatet derfor ikke kan anvendes som grundlag for en ny signatur, påhviler der 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.

7. 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 på signeringstidspunktet - dvs. ikke opført på Den Danske Stat Tillidstjenesters (CA 1) respektive spærrelistes,
- 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 elektronisk signatur sikre sig følgende:

- At tidsstemplet er korrekt signeret med et gyldigt certifikat,
- 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 udstedt på baggrund af disse vilkår være gyldig, og modtageren kan støtte ret på den, selv om certifikatet efter afgivelsen af signaturen er udløbet eller spærret.

Signerede dokumenter kan valideres i Digitaliseringsstyrelsens valideringstjeneste på adressen:

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.

Den Danske Stat beskriver forhold omkring spærringsinformation, herunder periode for tilgængelighed, information ved kompromittering af udsteders nøgler samt adgang til spærringsinformation ved ophør af tjenesten, i afsnit 4.9 og afsnit 4.10 i gældende Certifikatpraksis, der er tilgængelig på:

<https://www.ca1.gov.dk/efterlevelseserklæringer/>



Den Danske Stat Tillidstjenester

8.Support

8.1.Generel support

Supporthenvendelser vedr. 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:

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 IN Groupe Denmark 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:

www.mitid-erhverv.dk/privatlivspolitik

9.2.Dataansvar

Digitaliseringsstyrelsen er dataansvarlig for de personoplysninger, som behandles i Signeringsløsningen og MitID Erhverv i forbindelse med certifikatanvendelsen. AEVEN A/S og IN Groupe Denmark A/S er databehandler for Digitaliseringsstyrelsen.

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

Personoplysninger slettes efter løbende år + syv (7) år.

9.3.Registrering af oplysninger

Digitaliseringsstyrelsens registrering og behandling af oplysninger, herunder personoplysninger ved registrering af Certifikatholdere og den efterfølgende brug af certifikater fremgår af punkt 18.

10.Ophør af Den Danske Stat Tillidstjenester



Den Danske Stat Tillidstjenester

Hvis Den Danske Stat Tillidstjenester ophører med at udstede brugercertifikater, er Den Danske Stat Tillidstjenester berettiget til at videregive alle registrerede oplysninger til en tredjepart med henblik på at denne kan indtræde i de forpligtelser, som Den Danske Stat Tillidstjenester har efter disse vilkår.

11. 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.

Kommunikation vedr. anvendelsen af certifikater sker som udgangspunkt til Certifikatindehavers Organisationsadministrator og Brugeradministrator.

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

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

12.3. Ansvarsbegrænsninger

Digitaliseringsstyrelsens ansvar efter punkt 12.1 og 12.2 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 12.1 til punkt 12.3 er ligeledes gældende for Digitaliseringsstyrelsens afgivelse af tidsstempler.

13. Anvendelsesbegrænsninger



Den Danske Stat Tillidstjenester

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

14.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 meddelelsetidspunktet.

15.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



16. Indledning

16.1. Generelle forhold

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

Brugercertifikaterne udstedes til Erhvervsbrugere i rollen som Certifikatholder, der af Erhvervsbrugerens Brugerorganisation (benævnt Certifikatindehaver), har fået rettigheder til at afgive brugersignaturer via Signeringsløsningen.

Vilkår skal accepteres af Certifikatholder forud for udstedelse af et brugercertifikat til brug for afgivelse af en kvalificeret signatur i Signeringsløsningen. Udstedelsen sker på vegne Certifikatindehaver, som Certifikatholder er tilknyttet.

Vilkårene er godkendt af Certifikatindehaver, der desuden har accepteret generelle vilkår for anvendelse af brugercertifikater fra Den Danske Stat Tillidstjenester.

Yderligere information om anvendelse af en erhvervsidentitet til afgivelse af signaturer, er tilgængelig på:

[MitID-Erhverv.dk](https://mitid-erhverv.dk)

16.2. 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



Den Danske Stat Tillidstjenester

17. Forpligtelser ved anvendelse af brugercertifikat

17.1. Generelle forhold

Certifikatholders anvendelse af et brugercertifikat til afgivelse af en elektronisk signatur sker på vegne af Certifikatindehaver i overensstemmelse med de mellem disse parter fastlagte aftaler, herunder evt. ansættelsesvilkår.

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

17.2. 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 Certifikatholder, herunder at den private nøgle ikke må anvendes til signering af andre certifikater.

Forud for afgivelse af en elektronisk signatur er Certifikatholder 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.

17.3. Beskyttelse af identifikationsmiddel

Certifikatholder skal beskytte det identifikationsmiddel og tilhørende sikkerhedsmekanismer (f.eks. kodeord), der anvendes til brug for afgivelse af en elektronisk signatur, i overensstemmelse med de vilkår, der er gældende herfor. Certifikatholder skal på denne baggrund tage rimelige forholdsregler for, at der ikke afgives en elektronisk signatur i Certifikatholders navn.

Hvis der er mistanke om at det identifikationsmiddel, der anvendes til brug for autentifikation over for signaturløsningen, 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 en elektronisk signatur i Certifikatholders navn.

17.4. 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.

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



17.5. Beskyttelse på et kvalificeret elektronisk signaturgenereringssystem (QSCD)

Signeringsløsningen sikrer for Certifikatholder, 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 Certifikatholder, der har kontrollen med den private nøgle og certifikatet ved afgivelse af en elektronisk signatur.

17.6. Spærring af certifikat

Signeringsløsningen sletter den private nøgle tilhørende certifikatet umiddelbart efter afgivelse af den kvalificerede elektroniske signatur, hvorfor certifikatet ikke kan anvendes som grundlag for en ny signatur. 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.

18. Digitaliseringsstyrelsens registrering af oplysninger

18.1. 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:

- Tidspunktet for signering/udstedelse af certifikatet
- Certifikatindehavers virksomhedsoplysninger, som registreret i MitID Erhverv
- Det NSIS sikringsniveau (Level Of Assurance) Certifikatholder er autoriseret med over for tjenesten
- Level of Identity Proofing (LoIP), jf. ETSI TS 119 461
- Session UUID
- Referencetekst
- Tekniske oplysninger relateret til autentifikationen (SAML assertion)
- Certifikatholders navn (alternativt synonym), UUID og e-mail.

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



18.2. Oplysninger der ikke registreres

Digitaliseringsstyrelsen registrerer ikke oplysninger om hvilket dokument eller hvilke data, der er signeret under anvendelse af certifikatet.

18.3. Oversigt over signaturanvendelse

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

18.4. Lagring af data

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

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

19. Ophør af Den Danske Stat Tillidstjenester

Hvis Den Danske Stat Tillidstjenester ophører med at udstede brugercertifikater, er Den Danske Stat Tillidstjenester berettiget til at videregive alle registrerede oplysninger til en anden juridisk enhed, herunder en offentlig myndighed eller et offentligt organ, som får til opgave at varetage den fortsatte forvaltning med eller ophør af Den Danske Stat Tillidstjenester.

