

DIGITALISERINGSSTYRELSEN



Vilkår for Brugerorganisationer

Indholdsfortegnelse

Bilag	3
1 Indledning	4
2 Kontaktinformation	4
3 Definitioner.....	5
4 Tilslutning og accept af vilkår	7
4.1 Accept af vilkår	7
4.2 Registrering i det Centrale Virksomhedsregister	8
4.3 Den Bemyndigedes udpegning af Organisationsadministrator	8
4.4 Tilslutning baseret på migrering fra Nets DanID	8
5 Brugerorganisationens administratorer	8
5.1 Oprettelse af administratorer	8
5.2 Organisationsadministrator.....	9
5.3 Rettighedsadministrator.....	9
5.4 Brugeradministrator	9
6 Tilslutning og anvendelse af Lokal IdP.....	9
7 Services til Brugerorganisationer	9
7.1 Services.....	9
7.2 Oprettelse af Brugeridentiteter og erhvervelse af identifikationsmidler	9
7.3 Oprettelse af brugeridentiteter via Lokal IDM Service.....	10
7.4 Identitetssikring ved oprettelse af Brugeridentiteter	10
7.5 Certifikater til elektronisk signatur.....	10
7.6 Brugerrettighedsadministration.....	10
7.6.1 Rettigheder til Brugerorganisationens Medarbejdere	10
7.6.2 Digitale erhvervsfuldmagter	10
8 Dedikerede MitID identifikationsmidler.....	11
8.1 Anskaffelse af dedikerede MitID identifikationsmidler.....	11
8.2 Særlige regler for anskaffelse af MitID identifikationsmidler	11
9 Certifikater til elektronisk signatur.....	11
9.1 Certifikater i MitID Erhverv.....	11
9.2 Vilkår for anvendelse af certifikater	13
9.3 Generelt om Certifikater i MitID Erhverv	13
9.4 OCES-certifikater (persistente).....	13
9.5 Kvalificerede certifikater (persistente).....	13
9.6 Kvalificerede signaturer (baseret på Korttidscertifikater).....	14
9.7 Certifikatpolitikker.....	14
9.8 Validering af kvalificerede elektroniske signaturer og segl.....	14

10	Brugerorganisationens forpligtelser	14
10.1	Korrekt og opdateret information.....	14
10.2	Overensstemmelse til CVR	15
10.3	Anvendelse af procedurer og systemer	15
10.4	Sikring af korrekt tilknytning mellem Brugerorganisation og Erhvervsbrugere.....	15
10.5	Erhvervsbrugers overholdelse af vilkår	15
10.6	Anvendelse af fuldmagter	15
10.7	Behandling af Identifikationsmidler	15
10.8	Rapportering vedr. sikkerhedshændelser	16
11	Behandling af personoplysninger	16
12	Service mål og tilgængelighed.....	16
13	Support	16
14	Systemforvaltning.....	17
14.1	Digitaliseringsstyrelsens forvaltningsenhed.....	17
14.2	Suspension og spærring af Brugerorganisationen	17
15	Vederlag.....	17
15.1	Generelt.....	17
15.2	Vederlag ved migrering fra Nets DanID.....	17
15.3	Fakturering og betalingsbetingelser.....	17
16	Sletning og logning	18
17	Ændringer i rettighedsregimer	18
18	Misligholdelse og misligholdelsesbeføjelser	18
18.1	Afhjælpning	18
18.2	Generelt om ophævelse	18
18.3	Digitaliseringsstyrelsens ophævelse.....	18
18.4	Suspension af Brugerorganisationens adgang til Services	19
19	Generel suspension af adgang til Services	19
20	Ansvar og ansvarsbegrænsning.....	19
20.1	Generelt ansvar	19
20.2	Ansvar vedr. udstedelse af Særskilt MitID	20
20.3	Ansvarsbegrænsning	20
20.4	Ansvar relateret til kvalificerede certifikater	20
21	Tavshedspligt.....	20
22	Løbetid og ophør	20
22.1	Løbetid og opsigelse	20
22.2	Ændringer	20
22.3	Ophør.....	21

23	Tvister	21
23.1	Lovvalg.....	21
23.2	Tvister, mediation og voldgift.....	21
23.3	Tvister relateret til certifikater og fysiske MitID Identifikationsmidler.....	21

Bilag

Bilag 1 Vilkår og betingelser for dedikeret MitID til Erhvervsbrugere

Bilag 2 Vilkår for OCES Brugercertifikater

Bilag 3 Vilkår for OCES Organisationscertifikater

Bilag 4 Vilkår for kvalificerede brugersignaturer

Bilag 5 Vilkår for kvalificerede segl

Bilag 6 Handelsbetingelser for fysiske MitID identifikationsmidler

Bilag 7 Vilkår for anvendelse af Lokal IdP

1 Indledning

Disse vilkår regulerer Juridiske enheders tilslutning og anvendelse af MitID Erhverv som en Brugerorganisation. Juridiske enheders tilslutning til og anvendelse af MitID Erhverv er ligeledes reguleret af bekendtgørelse om MitID Erhverv og MitID Privat til Erhverv (Bkg. nr. 1778 af 01/09/2021).

I MitID Erhverv kan Juridiske enheder i rollen som Brugerorganisation oprette, administrere og anvende digitale Erhvervsidentiteter samt tilknytte og administrere Identifikationsmidler til Erhvervsbrugere. Desuden kan der tildeles og administreres rettigheder til de oprettede Erhvervsidentiteter.

MitID Erhverv er den danske nationale identitetsgarant for Erhvervsidentiteter.

En Brugerorganisationens oprettelse af Erhvervsidentiteter i MitID Erhverv giver mulighed for, at Tjenesteudbydere kan modtage information om, at der er tilknyttet en Erhvervsidentitet til det Identifikationsmiddel, der anvendes til autentifikation over for Tjenesteudbyder.

Oplysning om at der forefindes Erhvervsidentiteter, gives til Tjenesteudbydere, der er tilsluttet NemLog-in samt brokere, der har indgået en særskilt aftale med Digitaliseringsstyrelsen om modtagelse af Erhvervsidentiteter via NemLog-in.

For yderligere information om MitID Erhverv henvises til information på MitID Erhverv Portalen.

Nærværende vilkår erstatter "Vilkår for anvendelse af NemLog-in/Brugeradministration".

Alle de i vilkårene beskrevne Services er ikke nødvendigvis tilgængelige på tidspunktet for Brugerorganisationens accept af Vilkår. Brugerorganisationen skal særskilt orientere sig på MitID Erhverv Portalen for nærmere beskrivelse af, hvilke Services der er tilgængelige samt evt. tidsplaner for introduktion af nye Services.

Der hører syv bilag til vilkårene. Bilagene udgør en integreret del heraf.

2 Kontaktinformation

Digitaliseringsstyrelsen har følgende kontaktinformation:

Digitaliseringsstyrelsen
Landgreven 41301 København K
Tlf. 3392 5200
mitiderhverv@digst.dk
CVR: 34051178

3 Definitioner

Begreb	Definition
Administrator	<p>Administrator er en fællesbetegnelse for de administratorroller (Organisationsadministrator, Brugeradministrator og Rettighedsadministrator), der kan oprettes i MitID Erhverv.</p> <p>En administratorrolle besættes altid af en Bruger.</p>
Bemyndiget	<p>En repræsentant fra den Juridiske enhed (typiske en ledelsesrepræsentant), der formelt tilslutter enheden som Brugerorganisation i MitID Erhverv.</p> <p>Den personkreds, der kan agere i rollen som Bemyndiget afhænger af den Juridiske enheds virksomhedsform. Der henvises til MitID Erhverv Portalen for nærmere information herom.</p>
Bruger	<p>Erhvervsbruger, der er associeret med en Brugerorganisation. Det er ikke et krav, der er tale om et formelt ansættelsesforhold mellem Bruger og Brugerorganisationen.</p>
Brugeradministrator	<p>Brugeradministrator i MitID Erhverv er ansvarlig for at oprette og administrere en virksomheds Erhvervsbrugere og dertil knyttede Identifikationsmidler.</p>
Brugerdata	<p>Brugerdata er oplysninger om Erhvervsbrugerne i Brugerorganisationen og omfatter bl.a. navn, CPR-nummer, e-mail og telefonnummer samt hvilke rettigheder Erhvervsbrugerne er tildelt.</p> <p>Brugerdata tilføjes og administreres i MitID Erhverv af en brugeradministrator.</p>
Brugerorganisation	<p>En Juridisk enhed tilsluttet MitID Erhverv.</p>
Brugidentitet	<p>Elektronisk identitet udstedt til fysisk person, der er associeret med en Brugerorganisation.</p>
Certificeringscenter	<p>En fysisk person eller juridisk enhed, der som tillidstjenesteudbyder genererer, udsteder og administrerer certifikater. I eIDAS forordningen benyttes betegnelsen tillidstjenesteudbyder for denne enhed.</p> <p>Digitaliseringsstyrelsen er på vegne af den danske stat Certificeringscenter for de certifikater, der udstedes i regi af MitID Erhverv.</p>
Certifikatindehaver	<p>En fysisk eller juridisk person, der indgår aftale med Certificeringscenteret (CA) om udstedelse af certifikater til én eller flere Certifikatholdere.</p>
Certifikatholder	<p>En fysisk person eller en enhed hos en Certifikatindehaver, som i certifikatet er identificeret, som den rette anvender af den private nøgle, hørende til</p>

	den offentlige nøgle, der er givet i certifikatet, og til hvem et certifikat enten er under udstedelse eller er blevet udstedt.
Dedikeret MitID identifikationsmiddel	Se Særskilt MitID.
Digital Selvbetjeningsløsning	Et it-system hvorfra privatpersoner eller Erhvervsbrugere kan tilgå digital selvbetjening efter at have autentificeret sig.
Erhvervsbruger	En fysisk person, der er associeret med en Brugerorganisation og som er oprettet med en Brugeridentitet i MitID Erhverv.
Erhvervsidentitet	Erhvervsidentitet er en samlebetegnelse for Brugeridentitet og Organisationsidentitet. En Erhvervsidentitet har altid en CVR og RID attribut, der tilsammen muliggør unik identifikation af Erhvervsidentiteten på tværs af organisationer tilsluttet som Brugerorganisationer i MitID Erhverv.
Forvalter	Forvalter er en medarbejder hos Digitaliseringsstyrelsen eller Digitaliseringsstyrelsens leverandør, der på baggrund af administratorrettigheder kan foretage visse handlinger på vegne af en Brugerorganisation. Alle handlinger foretaget af en Forvalter på vegne af en Brugerorganisation logges, så de kan henføres til den specifikke medarbejder, der udførte dem.
Identifikationsmiddel	Et identifikationsmiddel er det middel som en bruger autentificerer sig med online. Identifikationsmidlet skal være under kontrol af den fysiske eller juridiske entitet, der har fået det udstedt.
Juridisk Enhed	Ved Juridisk enhed forstås en juridisk enhed med et cvr-nummer som fastsat i CVR-lovens § 3.
Korttid	En certifikattype, der udstedes i Signeringsløsningen, hvor den private nøgle slettes umiddelbart efter afgivelse af signaturen og hvor certifikatet udløber efter 10 dage. Korttidscertifikater kan alene anvendelse til afgivelse af en elektronisk signatur og således ikke til hemmeligholdelse og sikker e-mail.
Kvalificeret certifikat	Certifikat der er et "Kvalificeret certifikat for elektronisk signatur" eller et "Kvalificeret certifikat for elektronisk segl" som defineret i eIDAS-forordningens artikel 3 litra 15) og litra 30)
Lokal IdP	En lokal NSIS-anmeldt autentifikationsløsning tilsluttet NemLog-in, der kan autentificere Erhvervsbrugere fra en Brugerorganisation og videreformidle autentifikationssvaret gennem NemLog-in til en Tjenesteudbyder tilsluttet NemLog-in.
MitID Erhverv Portalen	Digitaliseringsstyrelsens produktsite om MitID Erhverv målrettet Brugerorganisationer på www.mitid-erhverv.dk MitID Erhverv Portalen indeholder en beskrivelse af tekniske krav til Brugerorganisationers anvendelse af MitID Erhverv samt en række underliggende politikker. Henvisning til portalen er samtidig en henvisning

	til de tekniske krav og underliggende politikker, der tilgængelige på portalen.
MitID Privat til Erhverv	Et privat MitID der anvendes til brug for repræsentation af en Juridisk enhed uden, at der er oprettet en Erhvervsidentitet i MitID Erhverv. MitID Privat til Erhverv kan alene anvendes af personer, der kan tegne en virksomhed alene.
NemLog-in	Digitaliseringsstyrelsens Identitetsbroker, hvorfra der viderefremmes autentifikation af digitale identiteter, herunder ved anvendelse af identifikationsmidler fra NemID, MitID og Lokale IdP'er.
Organisationsadministrator	Den øverste administrator i Brugerorganisationen i MitID Erhverv.
Organisationsidentitet	En Erhvervsidentitet (organisationsprofil) hvorunder der kan udstedes OCCES organisationscertifikater og Kvalificerede organisationscertifikater. Der er ikke tilknyttet en fysisk person til en Organisationsidentitet.
Persistent	En certifikattype, der udstedes i Signeringsløsningen via MitID Erhverv, kendetegnende ved at certifikatet har gyldighed på 36 måneder. Der kan afgives et ubegrænset antal signaturer eller segl på baggrund af certifikatet, der ligeledes tilbyder en flerhed af anvendelsesformer.
Rettighedsadministrator	En Rettighedsadministrator er bl.a. ansvarlig for at administrere brugerroller, rettigheder og erhvervsfuldmagter for en Brugerorganisation i MitID Erhverv.
Services	Services fra Digitaliseringsstyrelsen til brug for Brugerorganisationen, herunder Erhvervsidentiteter, certifikater, identifikationsmidler og rettighedsstyring samt de i vilkårene yderligere fastlagte forpligtelser, som Digitaliseringsstyrelsen er underlagt.
Signeringsløsningen	Digitaliseringsstyrelsens signeringsløsning, der muliggør afgivelse af signaturer og segl via Tjenesteudbydere. Signaturer og segl i signeringsløsningen er baseret på Korttidscertifikater.
Særskilt MitID	Et særskilt MitID Identifikationsmiddel udstedt til en Erhvervsbruger i Brugerorganisationen udelukkende til brug for Erhvervsbrugeren som repræsentant for Brugerorganisationen. Betegnes også Dedikeret MitID

4 Tilslutning og accept af vilkår

4.1 Accept af vilkår

Vilkårene skal på vegne af den Juridiske enhed accepteres af den Bemyndigede. Ved accept af vilkårene erklærer den Bemyndigede, at den Juridiske enhed vil efterleve vilkårene. Digitaliseringsstyrelsens forpligtelser over for Brugerorganisationen indtræder samtidig med Brugerorganisationens accept af vilkårene.

Den Bemyndigede skal varetage en sådan rolle i Brugerorganisationen, der muliggør repræsentation af Brugerorganisationen over for Digitaliseringsstyrelsen, herunder i forhold til accept af vilkår.

4.2 Registrering i det Centrale Virksomhedsregister

Det er forudsætning for oprettelse som Brugerorganisation i MitID Erhverv, at den Juridiske enhed er registreret i det Centrale Virksomhedsregister (CVR).

4.3 Den Bemyndigedes udpegning af Organisationsadministrator

Som en del af tilslutningsprocessen skal den Bemyndigede udpege minimum én Organisationsadministrator, jf. pkt. 5.2. Ved udpegningen erklærer den Bemyndigede sig samtidig indforstået med, at Organisationsadministratoren på Brugerorganisationens vegne har mandat til at udføre de for Organisationsadministrator fastsatte opgaver, herunder fungere som kontaktpunkt for Digitaliseringsstyrelsen i forhold til meddelelse om opdatering af vilkår og i øvrigt over for Digitaliseringsstyrelsen indgå bindende aftaler i MitID Erhverv på vegne af Brugerorganisationen, jf. herom bl.a. punkt 5.2 og punkt 22.2.

Den Bemyndigede har mulighed for at udpege sig selv som Organisationsadministrator.

4.4 Tilslutning baseret på migrering fra Nets DanID

Hvis Brugerorganisationen tilsluttes som led i en migrering fra NemID Medarbejdersignatur-løsningen hos Nets DanID, kan der efter accept af nærværende vilkår og accept af migrering ske en overførsel af alle eller udvalgte medarbejdere til MitID Erhverv.

Som led i migreringen oprettes medarbejdere registreret i NemID Medarbejdersignatur-løsningen som Brugeridentiteter i MitID Erhverv og vil ved overførslen være i en midlertidig suspenderet tilstand.

Det er Organisationsadministrators ansvar at kontrollere, at alle overførsler er gennemført korrekt, hvorefter Organisationsadministrator udvælger de brugerregistreringer, der skal oprettes som Brugeridentiteter. Den formelle oprettelse som Brugeridentitet sker på baggrund af en accept fra den enkelte Bruger, der samtidig informeres om flytningen af personoplysninger fra Nets DanID til MitID Erhverv.

Der henvises til punkt 15 for en nærmere beskrivelse af priser for oprettelse af Brugerorganisationen ved migrering fra NemID medarbejdersignatur-løsningen.

5 Brugerorganisationens administratorer

5.1 Oprettelse af administratorer

Den daglige administration af Brugerorganisationen sker ved tre administratorer:

- Organisationsadministrator
- Rettighedsadministrator
- Brugeradministrator

De af Brugerorganisationen udpegede administratorer må ikke være straffet for forhold, der gør dem uegnet til at udføre hvervet som administrator.

For at kunne optræde som administrator er det en forudsætning, at den pågældende Bruger er registreret som Erhvervsbruger hos Brugerorganisationen.

Det er i øvrigt Brugerorganisationens ansvar, at udpegning af administratorer sker i overensstemmelse med Brugerorganisationens interne tegningsregler.

5.2 Organisationsadministrator

Organisationsadministratoren er efter udnævnelse den øverste repræsentant for Brugerorganisationen i MitID Erhverv. Brugerorganisationen skal sikre, at den altid er repræsenteret af mindst én Organisationsadministrator med tilknytning til den Juridiske enhed. Hvis den Juridiske enhed, f.eks. på baggrund af en opsigelse, ikke længere er repræsenteret ved en Organisationsadministrator, vil der være behov for, at en Bemyndiget for Brugerorganisationen udpeger en ny Organisationsadministrator.

Kravene til verifikation af en Bemyndiget med henblik på udpegning af en ny Organisationsadministrator, svarer til kravene ved den oprindelige tilslutning af den Juridiske enhed.

Organisationsadministrator er ansvarlig for at udpege øvrige administratorer samt for at opsætte virksomhedsdata og administrationspræferencer i MitID Erhverv.

Organisationsadministrator har mulighed for at udpege sig selv i rollen som rettighedsadministrator og Brugeradministrator, ligesom der kan være personsammenfald mellem de øvrige administratorer.

5.3 Rettighedsadministrator

Rettighedsadministrator kan tildele og administrere rettigheder til de registrerede Erhvervsidentiteter, og kan tillige udpege andre Rettighedsadministratorer med tilsvarende rettigheder.

5.4 Brugeradministrator

Brugeradministrator opretter Erhvervsidentiteter i form af Brugeridentiteter og Organisationsidentiteter, som tilknyttes den Juridiske enheds CVR-nummer.

Ved oprettelse af en Erhvervsidentitet specificerer Brugeradministrator, hvorvidt oprettelsen vedrører en Brugeridentitet eller en Organisationsidentitet, og om der skal knyttes et certifikat eller Identifikationsmiddel til identiteten.

Ved oprettelsen af Brugeridentiteter, skal Brugeradministrator tage stilling til, hvilket identifikationsmiddel der skal tilknyttes, jf. punkt 7.2.

6 Tilslutning og anvendelse af Lokal IdP

Brugerorganisationen har via MitID Erhverv mulighed for at tilslutte en Lokal IdP til NemLog-in med henblik på at tilknytte identifikationsmidler herfra til de Brugeridentiteter, der er oprettet i MitID Erhverv, således at disse Identifikationsmidler kan benyttes til autentifikation over for Tjenesteudbydere.

Tilslutning og anvendelse af en Lokal IdP sker på baggrund af de i bilag 7 anførte vilkår.

7 Services til Brugerorganisationer

7.1 Services

Via MitID Erhverv har Brugerorganisationen adgang til en række Services. Disse er beskrevet nedenfor i punkt 7.2 til punkt 7.3.

7.2 Oprettelse af Brugeridentiteter og erhvervelse af identifikationsmidler

Brugerorganisationen kan oprette Brugeridentiteter for fysiske personer, der som Erhvervsbrugere kan repræsentere Brugerorganisationen over for tredjeparter.

Brugerorganisationen skal knytte ét af følgende Identifikationsmidler til Brugeridentiteten:

- Erhvervsbrugerens private MitID Identifikationsmiddel
- Et Særskilt MitID Identifikationsmiddel
- Et Identifikationsmiddel fra en Lokal IdP (forudsætter, at Brugerorganisationen har tilknyttet en Lokal IdP og udsteder identifikationsmidler herfra)

Tilknytning af Erhvervsbrugerens private MitID identifikationsmiddel til Brugeridentiteten kan alene ske, hvis både Brugerorganisationen og Erhvervsbrugeren har samtykket hertil (det dobbelte frivillighedsprincip). Accepten fra Erhvervsbrugeren skal være baseret på et individuelt samtykke indhentet af Brugerorganisationen.

Som led i udstedelsen af et Særskilt MitID identifikationsmiddel skal Erhvervsbrugeren acceptere de i bilag 1 vedlagte vilkår fra MitID.

Brugerorganisationens anskaffelse af MitID identifikationsmidler sker i overensstemmelse med det i punkt 8 anførte.

7.3 Oprettelse af brugeridentiteter via Lokal IDM Service

Brugerorganisationen kan oprette Erhvervsbrugere og vedligeholde rettigheder hertil i MitID Erhverv via en tilsluttet Lokal IdM løsning. Nærmere krav til integration af IdM-løsningen findes på MitID Erhverv Portalen.

7.4 Identitetssikring ved oprettelse af Brugeridentiteter

Oprettelsen af en Brugeridentitet forudsætter at den pågældende Bruger identitetssikres og autentificeres som en fysisk person med en NSIS anmeldt eID, der kan modtages af MitID Erhverv. Det anvendte eID skal som minimum understøtte en autentifikation på NSIS sikringsniveau betydelig. MitID og NemID kan anvendes som grundlag for identitetssikring.

7.5 Certifikater til elektronisk signatur

Brugerorganisationen har i MitID Erhverv mulighed for at oprette og administrere certifikater til elektronisk signatur.

De nærmere bestemmelser om certifikater er beskrevet i punkt 9.

7.6 Brugerrettighedsadministration

7.6.1 Rettigheder til Brugerorganisationens Medarbejdere

En Brugerorganisation kan tildele og administrere rettigheder til egne Brugeridentiteter med henblik på anvendelse af Offentlige Selvbetjeningsløsninger.

7.6.2 Digitale erhvervsfuldmagter

En Brugerorganisation kan anvende MitID Erhverv til at tildele rettigheder (såkaldte erhvervsfuldmagter) til en Brugerorganisation eller en Erhvervsbruger i en anden Brugerorganisation med et andet CVR-nummer.

Erhvervsfuldmagten gives til specifikke offentlige selvbetjeningsløsninger.

8 Dedikerede MitID identifikationsmidler

8.1 Anskaffelse af dedikerede MitID identifikationsmidler

MitID Identifikationsmidler kan bestilles af Brugerorganisationen via MitID Erhverv. Brugerorganisationens køb af MitID identifikationsmidler sker med Nets DanID A/S som aftalepart i overensstemmelse med de i Bilag 6 anførte vilkår. Digitaliseringsstyrelsen er ikke part i aftaler om anskaffelse af MitID identifikationsmidler.

8.2 Særlige regler for anskaffelse af MitID identifikationsmidler

MitID Identifikationsmidler må alene anskaffes til Brugerorganisationens egne Brugere. Der må ikke købes ind på vegne af tredjepart. Videresalg af Identifikationsmidler er ikke tilladt.

9 Certifikater til elektronisk signatur

9.1 Certifikater i MitID Erhverv

Brugerorganisationen har i MitID Erhverv mulighed for at oprette og administrere certifikater til elektronisk signatur. Certifikater i MitID Erhverv har karakter af Persistente certifikater.

Herudover kan Erhvervsbrugere benytte deres Brugeridentitet til at afgive elektroniske signaturer og elektroniske segl i Digitaliseringsstyrelsens Signeringsløsning. Certifikater i Signeringsløsningen følger modellen Korttid.

Certifikater og tidsstempel til brug for elektronisk signatur er udstedt af Den Danske Stats Tillidstjenester (CA1), der leveres af Digitaliseringsstyrelsen. Via MitID Erhverv er der samlet adgang til følgende certifikater udstedt af Den Danske Stats Tillidstjenester (CA1):

ID	Certifikater og signaturtyper	Karakteristika
A	OCES organisationscertifikat (Persistent) Udstedt efter certifikatpolitikken for OCES virksomhedscertifikater, jf. punkt 9.7.	Certifikat til anvendelse for elektronisk signatur til virksomheder. Der knyttes ingen personnavne til certifikatet. Et organisationscertifikat bruges af maskiner og programmer, der skal kommunikere sikkert på vegne af en virksomhed. Med en virksomhedssignatur har modtageren garanti for, at der kommunikeres med den virksomhed, som fremgår af certifikatet. Et OCES organisationscertifikat og tilhørende private nøgle kan ligeledes anvendes til signering af e-mails og til kryptering af data
B	OCES brugercertifikat (Persistent) Udstedt efter certifikatpolitikken for OCES medarbejdercertifikater, jf. punkt 9.7.	Certifikat til anvendelse for elektronisk signatur til fysiske personer tilknyttet Juridiske enheder. OCES brugercertifikater kan anvendes, når fysiske personer skal signere elektronisk og skal identificere sig som tilknyttet en given organisation. Et OCES brugercertifikat og tilhørende private nøgle kan anvendes til signering af e-mails og til kryptering af data.

ID	Certifikater og signaturtyper	Karakteristika
C	<p>Kvalificeret brugersignatur (Korttid)</p> <p>Udstedt efter certifikatpolitikken for kvalificerede medarbejdercertifikater, jf. punkt 9.7.</p>	<p>Certifikat til anvendelse for kvalificerede elektroniske signaturer til fysiske personer tilknyttet Juridiske enheder.</p> <p>Brugercertifikater kan anvendes, når en fysisk person tilknyttet en Juridisk enhed skal signere data med en kvalificeret elektronisk signatur, der sidestilles med en fysisk underskrift.</p> <p>En kvalificeret elektronisk signatur baseret på et Korttidscertifikat kan ikke anvendes til signering af e-mails eller anvendes til kryptering af data.</p> <p>De afgivne signaturer baserer sig på ikke-persisterede private nøgler. Dvs. de underliggende kryptografiske nøgler genereres til lejligheden i et centralt kvalificeret signaturgenereringssystem (QSCD) og den private nøgle slettes umiddelbart efter generering af hver enkelt elektronisk signatur.</p>
D	<p>Kvalificeret brugercertifikat udstedt på et lokalt kvalificeret signaturgenereringssystem (QSCD) (persistent)</p> <p>Udstedt efter certifikatpolitikken for kvalificerede medarbejdercertifikater, jf. punkt 9.7.</p>	<p>Certifikat til anvendelse til kvalificerede elektroniske signaturer til fysiske personer tilknyttet Juridiske enheder.</p> <p>Brugercertifikater kan anvendes, når en fysisk person tilknyttet en Juridisk enhed skal signere data med en kvalificeret elektronisk signatur, der sidestilles med en fysisk signatur.</p> <p>Et kvalificeret brugercertifikat udstedt på et lokalt QSCD kan anvendes til signering af e-mails og til kryptering af data.</p> <p>Signaturer baserer sig på en privat nøgle, der er beskyttet af et lokalt kvalificeret signaturgenereringssystem (QSCD).</p>
E	<p>Kvalificeret segl (Korttid)</p> <p>Udstedt efter certifikatpolitikken for kvalificerede virksomhedscertifikater, jf. punkt 9.7.</p>	<p>Certifikat til anvendelse for kvalificerede elektroniske segl til Juridiske enheder. Der knyttes ingen personnavne til certifikatet.</p> <p>Kvalificerede segl kan anvendes, når en Juridisk enhed skal påføre data et kvalificeret elektronisk segl, der sidestilles med en fysisk signatur</p> <p>Et kvalificeret segl baseret på et Korttidscertifikat kan ikke anvendes til signering af e-mails eller anvendes til kryptering af data.</p> <p>De afgivne segl baserer sig på ikke-persisterede private nøgler. Dvs. de underliggende kryptografiske nøgler genereres til lejligheden i et centralt kvalificeret signaturgenereringssystem (QSCD) og den private nøgle slettes umiddelbart efter generering af hver enkelt elektronisk signatur.</p>

ID	Certifikater og signaturtyper	Karakteristika
F	Kvalificeret organisationscertifikat udstedt på et lokalt kvalificeret seglgenereringssystem (QSCD) (Persistent)	<p>Certifikat til anvendelse for kvalificerede elektroniske segl til Juridiske enheder. Der knyttes ingen personnavne til certifikatet.</p> <p>Kvalificerede segl kan anvendes, når en Juridisk enhed skal påføre data et kvalificeret elektronisk segl med henblik på at dokumentere integritet og oprindelsen heraf.</p> <p>Et kvalificeret organisationscertifikat kan anvendes til signering af e-mails og til kryptering af data.</p> <p>Signaturer baserer sig på private nøgler, der er beskyttet af et lokalt kvalificeret signaturgenereringssystem (QSCD).</p>

9.2 Vilkår for anvendelse af certifikater

Specifikke vilkår for hver enkelt type certifikat og signatur, jf. punkt 9.1 ovenfor indgår som bilag til disse vilkår. Erhvervsbrugeren skal i rollen som Certifikatholder særskilt acceptere udvalgte dele af vilkårene forud for udstedelsen af persistente brugercertifikater i MitID Erhverv og forud for afgivelse af kvalificerede signaturer og segl i Signaturløsningen. De specifikke vilkår kan indeholde nærmere bestemmelser om Brugerorganisationens indhentelse af accept fra Erhvervsbrugeren ved udstedelse af certifikater.

9.3 Generelt om Certifikater i MitID Erhverv

Elektronisk signatur, baseret på et kvalificeret certifikat, 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). En elektronisk signatur afgivet på baggrund af Kvalificerede certifikater har retskraft i hele Europa på samme måde som en fysisk underskrift. For et elektronisk segl afgivet på baggrund af et kvalificeret organisationscertifikat, gælder der en formodning for integriteten af de data og nøjagtigheden af oprindelsen af de data, som det kvalificerede elektroniske segl er knyttet til. Kvalificerede segl anerkendes i alle medlemsstater.

Elektroniske signaturer baseret på et OCES-certifikat er baseret på den statslige OCES-standard. Den afgivne signatur har i Danmark retskraft svarende til en fysisk underskrift. I resten af Europa har signaturen retskraft efter nationale bestemmelser, men kan ikke nægtes retsvirkning alene af den grund, at den er i elektronisk form. Digitale signaturer baseret på et OCES-certifikat har karakter af en avanceret elektronisk signatur efter eIDAS forordningen.

9.4 OCES-certifikater (persistente)

OCES organisationscertifikat (ID A) og OCES brugercertifikat (ID B) kan bestilles og efterfølgende administreres i MitID Erhverv.

Brugerorganisationen er som Certifikatindehaver ansvarlig for at behandling af certifikaterne sker i overensstemmelse med vilkårene herfor og i de tilhørende certifikatpolitikker, jf. punkt 9.7.

9.5 Kvalificerede certifikater (persistente)

Kvalificerede certifikater i form af og kvalificerede brugercertifikater (ID D) og kvalificerede organisationscertifikater (ID F) i persistent form kan bestilles og efterfølgende administreres i MitID Erhverv.

Adgangen til at bestille kvalificerede certifikater er underlagt særlige krav relateret til de systemer og processer, der danner grundlag for håndtering af kvalificerede certifikater, herunder generering og opbevaring af private nøgler. Disse krav fremgår af særskilte vilkår.

Persistente kvalificerede brugercertifikater og persistente kvalificerede organisationscertifikater forventes at være tilgængelige i MitID Erhverv ultimo 2022. Nærværende vilkår vil blive opdateret i overensstemmelse hermed.

9.6 Kvalificerede signaturer (baseret på Korttidscertifikater)

Elektroniske signaturer og elektroniske segl baserede på kvalificerede brugercertifikater (ID D) og kvalificerede organisationscertifikater (ID E) i Korttid kan anvendes i Signeringsløsningen, såfremt en Digital Selvbetjeningsløsning efterspørger en kvalificeret elektronisk signatur eller et kvalificeret elektronisk segl.

9.7 Certifikatpolitikker

Vilkårene for certifikater, der kan tildeles og administreres i MitID Erhverv, er baseret på følgende certifikatpolitikker:

- Certifikatpolitikken for kvalificerede virksomhedscertifikater, version 7.1 (ID A)
- Certifikatpolitik for OCES-medarbejdercertifikater, version 7.1 (ID B)
- Certifikatpolitikken for kvalificerede medarbejdercertifikater, version 1.1 (ID C og D)
- Certifikatpolitik for OCES-virksomhedscertifikater, version 1.1 (ID E og F)

Certifikatpolitikkerne og Digitaliseringsstyrelsen detaljerede beskrivelse af Signeringsløsningen (Certificate Practice statement) kan læses på henholdsvis certifikat.gov.dk og ca1.gov.dk.

Som anført i punkt 9.1 benyttes i MitID Erhverv og i certifikatvilkårene en anden navngivning af certifikater, end hvad der fremgår af certifikatpolitikkerne.

9.8 Validering af kvalificerede elektroniske signaturer og segl

Digitaliseringsstyrelsens stiller en kvalificeret valideringstjeneste til rådighed for validering af kvalificerede elektroniske signaturer og elektroniske segl.

Valideringstjenesten kan benyttes til validering af kvalificerede signaturer og segl afgivet baggrund af certifikater udstedt fra Digitaliseringsstyrelsens Certificeringscenter.

Brug af valideringstjenesten er underlagt særskilte vilkår.

10 Brugerorganisationens forpligtelser

10.1 Korrekt og opdateret information

Brugerorganisationen er ansvarlig for, at de data, der registres om Brugerorganisationen og dens medarbejdere er korrekte og holdes opdaterede. Derudover er Brugerorganisationen ansvarlig for at sikre, at brugerrettigheder for Medarbejdere og administratorer er i overensstemmelse med de faktiske forhold, herunder Brugerorganisationens interne regler for ansvar og bemyndigelse.

Brugerorganisationen er ligeledes ansvarlig for berigtigelse af evt. fejlregistreringer og for at oplyse Medarbejdere om den foretagne registrering, herunder i henhold til oplysningspligten i fastsat i databeskyttelsesforordningens artikel 13.

Brugerorganisationen er som led i ovenstående ligeledes forpligtet til at registrere kontaktoplysninger samt sikre den løbende opdatering heraf.

Ophører en Erhvervsbrugers tilhørsforhold til Brugerorganisationen, skal Brugerorganisationen straks nedlægge den pågældende Erhvervsbrugers Brugeridentitet og spærre evt. tilknyttede certifikater.

Ved nedlæggelsen af en Brugeridentitet spærres automatisk dedikerede Identifikationsmidler til hørende Brugeridentiteten og associationer mellem en brugeridentitet og et privat identifikationsmiddel fjernes.

10.2 Overensstemmelse til CVR

Brugerorganisationen er forpligtet til at sikre, at der er overensstemmelse mellem registreringen af den Juridiske enhed i CVR og registreringen i MitID Erhverv. Visse ændringer i Brugerorganisationens registrering i CVR vil automatisk blive overført til MitID Erhverv, herunder virksomhedsstatus, jf. desuden punkt 14.2 om konsekvenser ved ændring i virksomhedsstatus.

10.3 Anvendelse af procedurer og systemer

Brugerorganisationen skal anvende betryggende administrative og ledelsesmæssige procedurer, der understøtter Brugerorganisationens og Medarbejdernes aktiviteter og i rimeligt omfang beskytter mod angreb og påvirkning fra uvedkommende.

Brugerorganisationen skal i denne sammenhæng sikre instruktion af Medarbejdere om korrekt anvendelse af Brugeridentiteter, Identifikationsmidler og Certifikater.

Efter anmodning fra en Erhvervsbruger skal Brugerorganisationen spærre dedikerede Identifikationsmidler og fjerne association mellem en Erhvervsbruger og private Identifikationsmidler.

10.4 Sikring af korrekt tilknytning mellem Brugerorganisation og Erhvervsbrugere

Brugerorganisationen indestår for tilknytningen mellem Brugerorganisationen og de associerede Erhvervsbrugere, herunder Administratorer. Brugerorganisationen skal vedligeholde organisatoriske og ledelsesmæssige procedurer for at sikre dette.

10.5 Erhvervsbrugers overholdelse af vilkår

Brugerorganisationen er ansvarlig for at Erhvervsbrugere, herunder Administratorer, overholder de regler og procedurer, som de er underlagt i henhold til disse vilkår samt vilkår og betingelse for MitID, jf. punkt 7.2.

10.6 Anvendelse af fuldmagter

Hvis Brugerorganisationen eller en Erhvervsbruger heri repræsenterer en fysisk person eller en Juridisk enhed, skal det sikres, at repræsentationen sker i overensstemmelse med den beskrevne fuldmagt. Erhvervede fuldmagter skal afmeldes, når grundlaget for fuldmagten ikke længere er til stede.

10.7 Behandling af Identifikationsmidler

Brugerorganisationen skal sikre, at processer og systemer, der understøtter håndtering af Erhvervsidentiteter og identifikationsmidler skaber sikkerhed og fortrolighed samt tilstrækkelig beskyttelse mod misbrug og angreb.

Brugerorganisationen er ansvarlig for at informere alle Erhvervsbrugere om, at de er ansvarlige for at overholde de til enhver tid gældende regler for opbevaring og brug af udstedte identifikationsmidler, herunder MitID og skal sikre processuelle og organisatoriske rammer, der understøtter Erhvervsbrugers opfyldelse heraf.

Omfattet af Erhvervsbrugers forpligtelser er:

- Enheder og applikationer hvorpå Identifikationsmidler anvendes skal holdes opdaterede og sikre.
- Sikker og forsvarlig opbevaring af bruger-id, adgangskoder og identifikationsmiddel, således at andre ikke kan få adgang til at bruge dem.
- Streng fortrolighed i forhold til adgangskoder, herunder forbud mod at skrive disse ned.
- Anvendelse af "Password Manager" applikation (program til at gemme adgangskoder i) til at opbevare information om bruger-id, din adgangskode etc. må alene ske såfremt den pågældende applikation yder tilstrækkelig beskyttelse mod at tredjemand adgang til den opbevarede information.
- Identifikationsmidler er personlige og må ikke anvendes af andre.

Det er Brugerorganisationens ansvar, at egne processer og systemer understøtter de forpligtelser, som Erhvervsbrugere er underlagt ved anvendelsen af specifikke identifikationsmidler.

10.8 Rapportering vedr. sikkerhedshændelser

Brugerorganisationen er forpligtet til straks at give meddelelser til Digitaliseringsstyrelsen, hvis der konstateres sikkerhedshændelser eller angreb mod MitID Erhverv eller andre services fra Digitaliseringsstyrelsen.

Brugerorganisationen er særskilt ansvarlig for at indberette brud på persondatasikkerheden til Datatilsynet i medfør af persondataforordningens artikel 33, og er forpligtet til parallelt med opfyldelse af sine forpligtelser efter artikel 33 at informere Digitaliseringsstyrelsen, såfremt bruddet relaterer sig til Services.

11 Behandling af personoplysninger

Digitaliseringsstyrelsen er dataansvarlig for MitID Erhverv og sikrer at driften og kontrollen hermed sker i overensstemmelse med de persondataretlige regler.

Brugerorganisationen er dataansvarlig for egen behandling af Personoplysninger i MitID Erhverv og ansvarlig for at have den fornødne hjemmel til at videregive og behandle personoplysninger om Brugerorganisationens Medarbejdere, herunder Administratorer.

12 Servicemål og tilgængelighed

Medmindre andet specifikt er anført, er alle Services i MitID Erhverv omfattet af disse vilkår tilgængelige døgnet rundt alle årets dage.

Digitaliseringsstyrelsen er ikke ansvarlig for manglende tilgængelighed af Services, f.eks. grundet driftsforstyrrelser hos Digitaliseringsstyrelsen eller hos tredjemand hvor Services ønskes anvendt.

13 Support

Digitaliseringsstyrelsen yder support til Brugerorganisationen via Det Samlede Supporttilbud i Erhvervsstyrelsens Kundecenter.

Brugerorganisationen kan desuden rekvirere teknisk support hos Nets DanID A/S til de på MitID Erhverv Portalen anførte priser.

Der henvises til en nærmere beskrivelse af support på MitID Erhverv Portalen.

14 Systemforvaltning

14.1 Digitaliseringsstyrelsens forvaltningsenhed

Digitaliseringsstyrelsens forvaltningsenhed har som Forvalter af MitID Erhverv en række administrative privilegier til at agere på vegne af Brugerorganisationen i MitID Erhverv.

Medmindre der forligger særlige omstændigheder, herunder af sikkerhedsmæssig karakter, vil Digitaliseringsstyrelsen alene udføre handlinger på baggrund af et konkret samtykke, herunder i forbindelse med en supportsag.

14.2 Suspension og spærring af Brugerorganisationen

Digitaliseringsstyrelsen modtager information om den Juridiske Enheds virksomhedsstatus fra CVR. Adgangen til MitID Erhverv og anvendelse af Erhvervsidentiteter og særskilte MitID til Erhverv vil blive suspenderet hvis virksomhedsstatus ændres til følgende:

- Under tvangsopløsning,
- Under konkurs
- Under rekonstruktion
- Under reasumering

Suspensionen kan ophæves ved en gentilslutning af Brugerorganisationen ved en Bemyndiget udpeget efter gældende regler, hvilket indebærer, at Brugerorganisationen igen kan tilgå MitID Erhverv.

Alle certifikater tilhørende Brugerorganisationen vil blive spærret i forbindelse med ovennævnte ændring i virksomhedsstatus. Et spærret certifikat kan ikke genaktiveres. Hvis Brugerorganisationen efter en afsluttet suspension fortsat har behov for at anvende certifikater, skal disse anskaffes på normal vis via MitID Erhverv.

Hvis Brugerorganisationen markeres som ophørt i CVR-registeret, spærrer Digitaliseringsstyrelsen straks alle Erhvervsidentiteter, certifikater og Særskilte MitID identifikationsmidler til erhvervsbrug. Det er herefter ikke muligt at genåbne Brugerorganisationen.

15 Vederlag

15.1 Generelt

Brugerorganisationen betaler de på MitID Erhverv Portalen anførte vederlag for anvendelse af MitID Erhverv, herunder i forhold til oprettelse af Brugeridentiteter, anskaffelse af certifikater og rekvirering af MitID identifikationsmidler.

15.2 Vederlag ved migrering fra Nets DanID

Brugerorganisationer der oprettes som led i en migrering fra NemID Erhverv til MitID Erhverv, jf. punkt 4.4, har mulighed for at overføre sine aktive NemID Erhvervsbrugere til MitID Erhverv og oprette disse brugere som Erhvervsidentiteter uden at betale vederlag herfor.

15.3 Fakturering og betalingsbetingelser

Der faktureres månedligt efter forbrug.

Fakturering foretages gennem Nets DanID A/S, der ligeledes håndterer de praktiske forhold vedr. betalinger og efterreguleringer.

Brugerorganisationen skal foretage betaling senest tredive (30) dage efter modtagelse af en faktura. For betalinger, der modtages efter forfaldsdagen, er Digitaliseringsstyrelsen berettiget til morarenter efter rentelovens sats.

16 Sletning og logning

Brugerdata opbevares i MitID Erhverv indtil de slettes af Brugerorganisationens administratorer.

Der foretages logning af, hvilke handlinger, Brugerorganisationens Erhvervsbrugere og administratorer foretager i MitID Erhverv. Loggen har som formål at dokumentere, hvem der på et givet tidspunkt har udført specifikke handlinger, og har været tildelt specifikke rettigheder. Loggen udleveres kun til personer, der kan godtgøre at være berettigede til at få udleveret logoplysninger.

Oplysninger i loggen slettes årligt efter udløb af pågældende år + 5 år. Oplysninger relateret til certifikater slettes efter 7 år fra tidspunktet for afgivelse af en signatur.

17 Ændringer i rettighedsregimer

Digitaliseringsstyrelsen underretter Brugerorganisationen, når Offentlig myndigheder etablerer nye rettigheder, herunder til erstatning for eksisterende rettigheder.

Tildeling af nye rettigheder til Brugere sker på baggrund af godkendelse fra Rettighedsadministrator.

18 Misligholdelse og misligholdelsesbeføjelser

18.1 Afhjælpning

Parterne er forpligtet til uden ugrundet ophold efter, at den anden part skriftligt har reklameret at foretage afhjælpning af fejl og mangler ved partens forpligtelser.

18.2 Generelt om ophævelse

Både Brugerorganisationen og Digitaliseringsstyrelsen kan ophæve aftalen, der følger af disse vilkår, såfremt den anden part i væsentlig grad har misligholdt sine forpligtelser, herunder særligt i forhold til sikkerhed, og som ikke uden ugrundet ophold har afhjulpet det eller de pågældende forhold.

Digitaliseringsstyrelsen kan derudover ophæve aftaleforholdet, hvis Brugerorganisationen bliver erklæret konkurs, indgiver konkursbegæring eller indleder rekonstruktionsbehandling, i det omfang konkurslovens regler ikke er til hinder derfor.

Ophævelsen har virkning fra det tidspunkt, hvor meddelelsen om ophævelse kommer frem og for de Services, der i tid ligger herefter.

Paterne kan ophæve aftalen som nærmere beskrevet i hhv. punkt 18.2 og punkt 18.3.

Digitaliseringsstyrelsen kan desuden i overensstemmelse med punkt 18.4 og punkt 19 suspendere Brugerorganisationens adgang til Services.

18.3 Digitaliseringsstyrelsens ophævelse

Digitaliseringsstyrelsen er berettiget til at ophæve Tilslutningsaftalen såfremt ét eller flere af følgende forhold gør sig gældende:

- Brugerorganisationen misligholdelser sin afrapporteringsforpligtelse relateret til sikkerhedshændelser.

- Digitaliseringsstyrelsen kan med føje konstatere at Brugerorganisationens anvendelse af Services har en sådan karakter, at det indebærer en risiko for kompromittering af MitID Erhverv eller tilknyttede infrastrukturer, herunder MitID.
- Manglende overholdelse af gældende lovgivning, herunder databeskyttelsesloven.
- Brugerorganisationen udviser en adfærd, der i væsentligt omfang har en negativ påvirkning eller er egnet til at skabe mistillid eller på anden måde negativt at påvirke Slutbrugernes opfattelse af MitID Erhverv og/eller tilknyttede infrastrukturer, herunder MitID-løsningen.
- Brugerorganisationen leverer ikke revisionserklæringer til brug for dokumentation af Brugerorganisationens overholdelse af krav fastlagt i NSIS-standard (alene gældende såfremt Brugerorganisationen har tilsluttet en Lokal IdP).

Ophævelse efter dette punkt kan dog først ske efter at Digitaliseringsstyrelsen skriftligt har påtalt det pågældende forhold over for Brugerorganisationen med en rimelig frist til udbedring heraf og dette ikke er sket inden for fristen.

18.4 Suspension af Brugerorganisationens adgang til Services

Digitaliseringsstyrelsen har adgang til at suspendere Brugerorganisationens adgang til Services omfattet af disse vilkår, såfremt Brugerorganisationen efter Digitaliseringsstyrelsens vurdering i væsentligt omfang ikke opfylder det i vilkårene fastlagte, eller i øvrigt anvender Services eller MitID på en sådan måde, at de er til skade for infrastrukturens sikkerhed og omdømme.

Et varsel efter punkt 18.3 ovenfor kan ligeledes suppleres af en suspension.

Digitaliseringsstyrelsen skal give et rimeligt og så vidt muligt 14 dages varsel til Brugerorganisationen med henblik på, at det pågældende forhold kan bringes til ophør.

En suspendering for adgangen til MitID Erhverv kan i ekstraordinære tilfælde ske med kortere eller uden varsel, såfremt hensyn til infrastrukturens integritet, øvrige Brugerorganisationer, eller Offentlige myndigheder gør det nødvendigt, eller såfremt den pågældende anvendelse udgør en væsentlig sikkerhedsrisiko. Digitaliseringsstyrelsen skal i alle tilfælde konkret begrunde beslutningen om suspendering.

Ved en suspension er Brugerorganisationen udelukket fra at anvende sine erhvervsidentiteter, indtil Digitaliseringsstyrelsen genopretter tilslutningen eller udnytter sine øvrige beføjelser efter disse vilkår, herunder retten til ophævelse eller bekendtgørelse om MitID Erhverv og MitID Privat til Erhverv (Bkg. nr. 1256 af 07/09/2022).

19 Generel suspension af adgang til Services

Digitaliseringsstyrelsen kan foretage en generel suspension af Brugerorganisationens adgang til Services, såfremt dette er begrundet i driftsmæssige forhold, herunder af hensyn til opretholdelse af et højt sikkerhedsniveau.

Suspension vil i videst muligt omfang blive varslet over for Brugerorganisationen.

20 Ansvar og ansvarsbegrænsning

20.1 Generelt ansvar

Parterne er erstatningspligtige i henhold til dansk rets almindelige regler og i henhold til det i dette punkt anførte.

Digitaliseringsstyrelsen er ikke i noget tilfælde ansvarlig for driftstab, avancetab, følgeskader eller andet indirekte tab. Tab relateret til suspension og spærring i henhold til punkt 18 og punkt 19, har karakter af indirekte tab.

Digitaliseringsstyrelsen er ikke ansvarlig for evt. tab som følge af manglende tilgængelighed af Services, herunder opfyldelse af de på MitID Erhverv Portalen fastlagte servicemål.

20.2 Ansvar vedr. udstedelse af Særskilt MitID

Digitaliseringsstyrelsen er erstatningsansvarlig for fejlregistreringer i forbindelse med udstedelse af Særskilt MitID, som følge af manglende overholdelse af de procedurer og forholdsregler ved registrering og indrulling og support, der er gældende ift. administration og ophør af MitID-løsningen, medmindre Digitaliseringsstyrelsen kan godtgøre, at Nets DanID A/S ikke har lavet fejl eller forsømmelser.

20.3 Ansvarsbegrænsning

Parternes samlede erstatningsansvar er 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.

Ovenstående begrænsning er kun gældende, såfremt misligholdelsen ikke kan henføres til grov uagtsomhed eller forsætlige forhold hos parterne.

20.4 Ansvar relateret til kvalificerede certifikater

Ovenstående punkt 20.1 regulerer ikke Digitaliseringsstyrelsens ansvar som udsteder af kvalificerede certifikater, der i det hele er reguleret af særskilte vilkår.

21 Tavshedspligt

Parterne, herunder medarbejdere, underleverandører, konsulenter med flere, skal iagttage ubetinget tavshed med hensyn til oplysninger modtaget fra den anden Part i forbindelse med modtagelse af Services og opfyldelse af krav relateret til disse vilkår, og forudsat oplysningerne vedrører den pågældende Parts forretningshemmeligheder, koncepter, relationer og andre fortrolige oplysninger. Parterne skal i særlig grad sikre fortrolighed om personoplysninger, tekniske integrationer og sikkerhedsrelaterede emner.

For Digitaliseringsstyrelsens personale gælder reglerne for ansatte i den offentlige forvaltning. Konsulenter og andre, der bistår styrelsen, pålægges tilsvarende forpligtelse med hensyn til oplysninger om Leverandørens forhold, som gælder for Leverandøren med hensyn til Kundens forhold.

Tavshedspligten gælder også efter ophør af vilkårene, uanset om disse er ophævet, opsagt eller på anden vis bortfaldet.

22 Løbetid og ophør

22.1 Løbetid og opsigelse

Vilkårene træder i kraft ved Brugerorganisationens accept og løber indtil de opsiges af én af parterne.

Hver af parterne kan opsige vilkårene med 3 måneders varsel

22.2 Ændringer

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.

Digitaliseringsstyrelsen kan uden varsel ændre de i Bilag 1 anførte vilkår og betingelser for MitID til Erhvervsbrugere. Ved ændringer vil Brugerorganisationen blive informeret herom, og Erhvervsbrugeren vil blive afkrævet accept ved anvendelsen af Erhvervsbrugers MitID identifikationsmiddel.

Tilføjelse af nye Services eller funktionaliteter i MitID Erhverv og særlige vilkår knyttet hertil, der ikke påvirker de eksisterende funktionalitet og driftsmæssige forhold hos Brugerorganisationen kan ske uden varsel. Ved Brugerorganisationens ibrugtagning af sådanne Services eller funktionaliteter betragtes evt. særlige vilkår samtidig som accepteret.

Ændringer vil blive meddelt Organisationsadministrator eller via Digital Post. Efter udløb af varslet vil de opdaterede vilkår være gældende.

22.3 Ophør

Aftalen ophører på tidspunktet for udløb af opsigelsesvarslet, jf. punkt 22.1. Enkelte Services kan tillige lukkes tidligere, såfremt Digitaliseringsstyrelsen træffer beslutning herom. Sådanne nedlukninger vil blive varslet som en ændring.

På tidspunktet for aftalens ophør spærres Brugerorganisationen og alle certifikater, der er udstedt gennem MitID Erhverv.

23 Tvister

23.1 Lovvalg

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

23.2 Tvister, mediation og voldgift

Såfremt der måtte opstå tvister mellem Parterne, skal Parterne først forsøge at løse uoverensstemmelserne ved gensidige og loyale forligsforhandlinger.

Alle tvister og uoverensstemmelser, som direkte eller indirekte måtte udspringe af disse vilkår, skal med endelig og bindende virkning afgøres ved voldgift i Det Danske Voldgiftsinstitut i henhold til instituttets regler og efter dansk ret. Stedet for voldgiftsretten er i København.

Hver Part udpeger en voldgiftsmand, mens voldgiftsrettens formand udnævnes af instituttet, såfremt de af Parterne udpegede voldgiftsmænd ikke inden 14 dage efter deres udnævnelse er blevet enige om en formand.

Har én af Parterne ikke inden 30 dage efter at have indgivet eller modtaget underretning om begæring af voldgift udpeget en voldgiftsmand, udpeges denne af instituttet i overensstemmelse med ovennævnte regler.

Dette punkt 23.2 skal dog ikke være til hinder for, at Parterne indbringer sager om overtrædelse af disse vilkår for domstolene med henblik på iværksættelse af foreløbige retsskridt.

23.3 Tvister relateret til certifikater og fysiske MitID Identifikationsmidler

Tvister relateret til certifikater og køb af fysiske MitID Identifikationsmidler håndteres som anført i Bilag 2 til Bilag 6.