DIGITALISERINGSSTYRELSEN

Vejledning – Tillidstjenester i Danmark

Januar 2020

2020

Indhold

1. Indledning **5**
1.1 Indarbejdelse af eIDAS-forordningen i Danmark 5
1.2 Gennemførelsesretsakterne 6
1.3 Digitaliseringsstyrelsens rolle 6
1.4 Nærmere om vejledningen 6

2. Baggrund **7**
2.1 eIDAS-forordningen og tillidstjenester 7
2.1.1 Anvendelsesområde 7
2.1.2 Definitioner 8
2.1.3 Kvalificerede tillidstjenester 8
2.1.4 Positivlisten 9
2.2 Gennemførelsesretsakter og standarder 10
2.2.1 Gennemførelsesretsakter 10
2.2.2 Standarder 10
2.2.3 Alternative standarder 10

3. Etablering af kvalificerede udbydere og kvalificerede tillidstjenester **12**
3.1 Generelt 12
3.2 Proces for at starte en kvalificeret tillidstjeneste 14
3.3 Frister 14
3.4 Digitaliseringsstyrelsens behandling af ansøgningen 14
3.5 EU-tillidsmærket for kvalificerede tillidstjenester 15

4. Krav som gælder både kvalificerede og ikkekvalificerede udbydere **16**
4.1 Erstatningsansvar og bevisbyrde 16
4.2 Sikkerhedskrav til tillidstjenesteudbydere og hændelsesrapportering 16
4.3 Tilsyn 17
4.3.1 Tilsyn med kvalificerede udbydere 17
4.3.2 Tilsyn med ikkekvalificerede udbydere 17

5. Regler for overensstemmelsesvurdering **18**
5.1 Overensstemmelsesvurdering 18
5.2 Overensstemmelsesvurderingsrapport 18

6. Krav til kvalificerede tillidstjenester **20**
6.1 Kvalificerede certifikater for elektroniske signaturer og segl 20
6.2 Kvalificeret valideringstjeneste 20
6.3 Kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer 21
6.4 Kvalificerede elektroniske tidsstempler 21
6.5 Kvalificerede elektroniske registrerede leveringstjenester 22
6.6 Kvalificerede certifikater for websteds autentifikation 22

7. Krav til IT-systemer og kvalificerede enheder for elektronisk signatur og segl **23**
7.1 Pålidelige IT-systemer 23
7.2 Krav til kvalificerede elektroniske signaturgenereringssystemer 23

8. Rapportering af sikkerhedshændelser **25**
8.1 Generelt 25
8.2 Hvilke sikkerhedshændelser skal rapporteres? 26
8.3 Anmeldelse til Digitaliseringsstyrelsen 26

9. Ophør af virksomhed **27**
9.1 Information til Digitaliseringsstyrelsen 27
9.2 Opbevaring af information 27
9.3 Offentliggørelse af spærring af certifikater og informering af berørte parter 27

10. Bilag **29**
10.1 Bilag 1 – Vedtagne gennemførelsesretsakter for tillidstjenester 29
10.2 Bilag 2 – Indhold af ansøgning 30
10.3 Bilag 3 – Digitaliseringsstyrelsens politikker 31

Vejledning for udbydere af tillidstjenester efter eIDAS forordningen i Danmark

1. Indledning

Den 1. juli 2016 trådte EU-forordningen[1] om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (eIDAS-forordningen) i kraft i EU's medlemslande.

Elektronisk identifikation og elektroniske tillidstjenester er vigtige forudsætninger for, at personer og virksomheder kan foretage elektroniske transaktioner. For at et system med elektroniske tillidstjenester – fx elektroniske signaturer – skal fungere, er det nødvendigt, at alle involverede parter opfatter det som pålideligt. Forordningen indeholder de juridiske rammer for disse elektroniske tillidstjenester. Forordningen indeholder også regler for udbyderne af sådanne tjenester. Målet er at øge tilliden til elektroniske transaktioner i det indre marked ved at give et fælles grundlag for sikker elektronisk interaktion mellem virksomheder, borgere og offentlige myndigheder.

eIDAS-forordningen stiller flere krav til udbyderne, men reglerne er overordnet udformet. I stedet for at udstikke detaljerede regler, gives der i forordningen hjemmel til, at Europa-kommissionen (herefter Kommissionen) skal eller kan vedtage gennemførelsesretsakter. Disse gennemførelsesretsakter skal i højere grad beskrive detaljerede tekniske krav og andre udfyldende regler. Kommissionen har vedtaget de gennemførselsretsakter som Kommissionen er pålagt i medfør af eIDAS-forordningen, se denne vejlednings Bilag 1.

1.1 Indarbejdelse af eIDAS-forordningen i Danmark

eIDAS-forordningen er gældende i Danmark. Forordningen er suppleret af lov nr. 617 af 8.juni 2016 om supplerende bestemmelser til forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked.

[1] 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. https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:32014R0910&from=EN

1.2 Gennemførelsesretsakterne

Forordningen giver Kommissionen hjemmel til at vedtage gennemførelsesretsakter. Flere sådanne retsakter er vedtaget. Gennemførelsesretsakterne er også gældende i Danmark. En oversigt er anført i denne vejlednings Bilag 1.

1.3 Digitaliseringsstyrelsens rolle

Digitaliseringsstyrelsen er i lov nr. 617 af 8. juni 2016 udpeget som tilsynsorgan og skal udføre tilsynsorganets opgaver i henhold til eIDAS-forordningen. Digitaliseringsstyrelsen skal altså føre tilsyn med, at udbydere af tillidstjenester opfylder kravene i forordningen.

1.4 Nærmere om vejledningen

Denne vejledning indeholder en beskrivelse af processen med at etablere sig som udbyder af en kvalificeret tillidstjeneste, samt kravene til en ikke-kvalificeret udbyder, hændelsesrapportering og anvendelse af forskellige standarder. Målgruppen for vejledningen er først og fremmest udbydere af tillidstjenester, som ønsker at etablere sig som udbydere af kvalificerede tillidstjenester. Vejledningen er også rettet mod udbydere af ikkekvalificerede tillidstjenester, relevante myndigheder og andre organer. Vejledningen er en beskrivelse af det gældende regelsæt og den støtte, som findes i form af standarder.

2. Baggrund

2.1 eIDAS-forordningen og tillidstjenester

Formålet med eIDAS-forordningen er at sikre et velfungerende marked og opnå et passende sikkerhedsniveau for elektroniske identifikationsmidler og tillidstjenester (artikel 1). Forordningen fastsætter princippet om et indre marked (artikel 4). En udbyder af tillidstjenester i en medlemsstat kan ikke hindres i at levere sådanne tjenester i en anden medlemsstat, når tjenesterne udbydes med et formål, der er omfattet af forordningen. Elektroniske signaturer, elektroniske segl og andre tillidstjenester, som er i overensstemmelse med forordningen, skal være underlagt fri bevægelighed på det indre marked. Forordningen indeholder generelle bestemmelser om tillidstjenester og kvalificerede tillidstjenester samt specielle bestemmelser om elektroniske signaturer, elektroniske segl, elektroniske tidsstempler, elektroniske tjenester for registreret leveringstjeneste og webstedsautentifikation. Desuden er der bestemmelser om elektroniske dokumenter, som er lagret i elektronisk form, som også kan indeholde lyd-og videooptagelser og audiovisuelle optagelser.

2.1.1 Anvendelsesområde

eIDAS-forordningen regulerer ordninger for elektronisk identifikation, som en medlemsstat har anmeldt, og udbydere af tillidstjenester, som er etableret i unionen (artikel 2, stk. 1). Forordningen gælder imidlertid ikke for udbydere af tillidstjenester, der udelukkende anvendes i lukkede systemer i henhold til national ret, eller som er aftalt mellem en afgrænset kreds af deltagere

I betragtningernes punkt 21 uddybes, hvad der menes med et lukket system. Der fremgår det, at forordningen ikke gælder udbydere af tillidstjenester, som bruges i lukkede systemer med et afgrænset antal deltagere, og som ikke påvirker tredjeparter. For eksempel nævnes systemer, som er oprettet i virksomheder eller offentlig administration for styring af interne procedurer. Det erklæres, at kun tillidstjenester, som tilbydes offentligheden, og som påvirker tredjeparter, skal opfylde de krav, som stilles i forordningen.

Forordningen påvirker heller ikke bestemmelser i national lovgivning eller europæisk lov, som regulerer indgåelse af aftaler og deres gyldighed, eller andre juridiske eller processuelle reguleringer angående formelle krav (artikel 2, stk. 3). Forordningen har heller ikke til hensigt at regulere nationale formkrav i offentlige registre, specielt ikke kommercielle registre eller ejendomsregistre (betragtningerne punkt 21).

Dansk lovgivning stiller i dag ingen krav til at anvende kvalificerede tillidstjenester hverken mellem individer eller mod offentlige organer. For udstedelse af cer-

tifikater og tidsstempler til brug i offentlige tjenester som NemID er der dog aftalemæssige krav om opfyldelse af Digitaliseringsstyrelsens politikker, se denne vejlednings bilag 3.

2.1.2 Definitioner

Artikel 3 indeholder definitioner. Nedenfor er nogen af dem gengivet:

16) «tillidstjeneste»: en elektronisk tjeneste, der normalt udføres mod betaling, og som består af

a) generering, kontrol og validering af elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler, elektroniske registrerede leveringstjenester og certifikater relateret til disse tjenester, eller
b) generering, kontrol og validering af certifikater for webstedsautentifikation, eller
c) bevaring af elektroniske signaturer, segl eller certifikater knyttet til disse tjenester

17) «kvalificeret tillidstjeneste»: en tillidstjeneste, der opfylder de krav, der er fastsat i denne forordning

25) «elektronisk segl»: data i elektronisk form, der er vedhæftet eller logisk tilknyttet andre data i elektronisk form, og som giver sikkerhed for disse tilknyttede datas oprindelse og integritet

33) «elektronisk tidsstempel»: data i elektronisk form, der forbinder andre data i elektronisk form med et bestemt tidspunkt og udgør bevis for, at disse andre data eksisterede på det pågældende tidspunkt

36) »elektronisk registreret leveringstjeneste«: en tjeneste, der gør det muligt at sende data mellem tredjeparter ad elektronisk vej og dokumenterer behandlingen af de sendte data, herunder leverer bevis for afsendelse og modtagelse af dataene, og som beskytter de sendte data mod tab, tyveri, beskadigelse og uautoriseret ændring

38) »certifikat for webstedsautentifikation«: en attestering, der gør det muligt at autentificere et websted og knytter webstedet til den fysiske eller juridiske person, som certifikatet er udstedt til.

2.1.3 Kvalificerede tillidstjenester

Artiklerne 20 til 24 indeholder specielle bestemmelser om kvalificerede tillidstjenester. En udbyder, som ønsker at tilbyde disse tjenester, skal sende en ansøgning til Digitaliseringsstyrelsen om dette. Udbyderen skal tillige medsende en

overensstemmelsesvurderingsrapport udstedt af et overensstemmelsesvurderingsorgan[2]. Overensstemmelsesvurderingsorganet gennemgår og dokumenterer udbyderens overholdelse af eIDAS-forordningens krav. Hvis Digitaliseringsstyrelsen vurderer, at udbyderen og de tillidstjenester, som udbydes, opfylder kravene i forordningen, optages de på den nationale positivliste med tildelt status som kvalificeret. Denne liste indeholder oplysninger om danske kvalificerede udbydere af tillidstjenester og de tjenester, som udbydes. Der er også en bestemmelse om tilbagekaldelse af en status som kvalificeret, hvis kravene i forordningen ikke længere er opfyldt af udbyderen.

Der gælder særlige krav for kvalificerede tjenesteudbydere, eksempelvis:

- at verificere identiteten af den person, hvortil der udstedes et kvalificeret certifikat
- personalets uddannelse/oplæring og viden
- økonomisk evne til at bære risikoen for virksomheden
- teknisk sikkerhed og pålidelige systemer
- løbende planlægning for at sikre kontinuitet i tjenesten i tilfælde af ophør af virksomheden[3].

Forordningen indeholder desuden krav om, at udbydere af kvalificerede tillidstjenester regelmæssigt og mindst hvert andet år skal vurderes af et overensstemmelsesvurderingsorgan for at verificere, at udbyderne opfylder kravene i forordningen.

2.1.4 Positivlisten

Oplysninger om kvalificerede udbydere og de kvalificerede tillidstjenester optages på den danske positivliste. Digitaliseringsstyrelsen vedligeholder positivlisten og meddeler Kommissionen, hvor positivlisten er offentliggjort. Derved gøres oplysningerne tilgængelige på Kommissionens EU Trusted List[4], som giver et centralt, ajourført og autoritativt overblik over kvalificerede tillidstjenesteudbydere i EU.

Hovedformålet med oplysningerne i positivlisten er at støtte valideringen af de sikkerhedstokens, som oprettes eller udstedes som følge af anvendelsen af en kvalificeret tillidstjeneste. Kommissionen har derfor fastlagt tekniske specifikationer og formater for positivlisten med retsakten (EU) 2015/1505. Positivlisterne skal indeholde både aktuelle og alle historiske oplysninger om de angivne tillidstjenesteudbydere fra det tidspunkt, hvor den pågældende tillidstjenesteudbyder optages på positivlisten. Positivlisten skal derfor være tilgængelig i en form, som er egnet til automatiseret behandling.

---

[2] Organet kaldes et overensstemmelsesvurderingsorgan eller en Conformity Assessment Body (CAB).
[3] Se kapitel 9. Ophør af virksomhed.
[4] Kommissionens Trusted List Browser - https://webgate.ec.europa.eu/tl-browser/#/

Kræver Digitaliseringsstyrelsen, at en kvalificeret tillidstjenesteudbyder afhjælper enhver forsømmelse af opfyldelse af kravene i eIDAS-forordningen, og hvis tjenesteudbyderen ikke handler i overensstemmelse hermed og eventuelt inden for en fastsat frist, kan Digitaliseringsstyrelsen tilbagetrække tjenesteudbyderens eller den pågældende tjenestes status som kvalificeret (artikel 20).

2.2 Gennemførelsesretsakter og standarder

2.2.1 Gennemførelsesretsakter

eIDAS-forordningen indeholder ikke detaljerede regler. I stedet er Kommissionen bemyndiget til at vedtage gennemførelsesretsakter for at give en mere detaljeret regulering. Alle vedtagne gennemførelsesretsakter[5] er gældende i Danmark.

De fleste gennemførelsesretsakter giver Kommissionen mulighed for at henvise til standarder på området. Hvis Kommissionen henviser til en standard, betyder det ikke, at udbydere skal overholde denne standard, men hvis standarden følges, antages det dog, at kravene i forordningen er opfyldt.

2.2.2 Standarder

Kommissionen har givet de europæiske standardiseringsorganisationer CEN og ETSI mandat (M/460)[6] til at udarbejde standarder inden for tillidstjenester. CEN og ETSI har i fællesskab udviklet et fælles sæt standarder for sikker elektronisk transaktion for e-handel og tjenester i Europa. Formålet med mandatet er at skabe betingelser for interoperabilitet og en europæisk standardramme. Disse standarder er tilpasset eIDAS-forordningen og danner grundlaget for gennemførelsesretsakterne. Standarderne har også til hensigt at lægge grundlaget for fremtidige gennemførelsesretsakter.

I mangel af gennemførelsesretsakter fra Kommissionen om anvendelse af standarder er det passende at bruge standarderne fra CEN og ETSI på området for tillidstjenester.

ENISA har offentliggjort en vejledning til brug af standarder i henhold til kravene i eIDAS-forordningen[7].

2.2.3 Alternative standarder

Alternative standarder end de, der er specificeret i Kommissionens gennemførelsesretsakter, kan bruges, så længe kravene i eIDAS-forordningen er opfyldt.

---

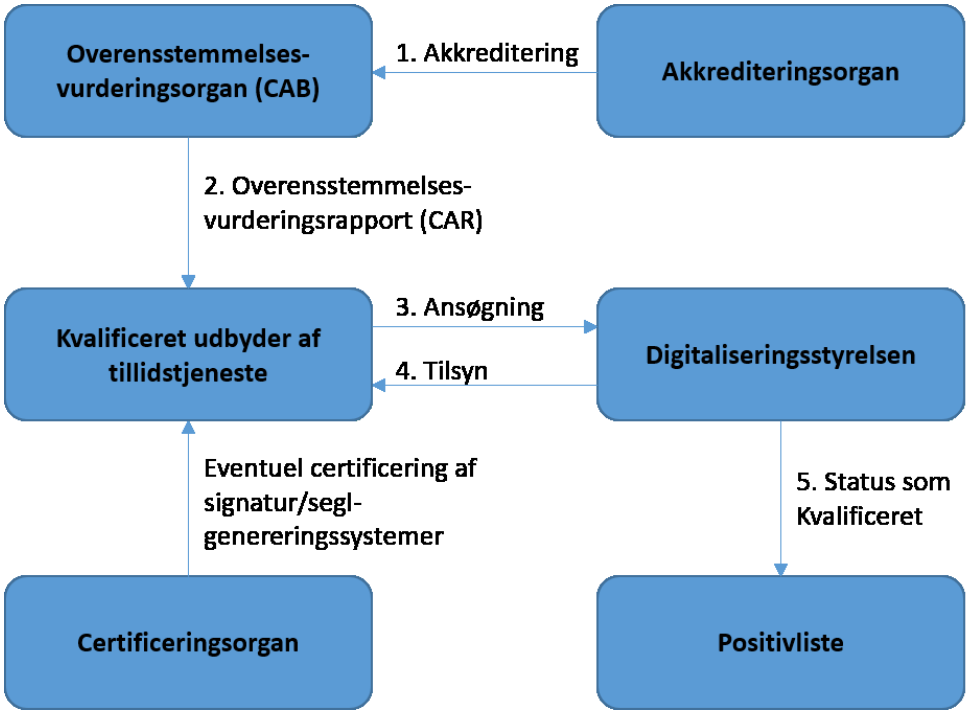
[5] Se denne vejlednings bilag 1 for en oversigt over vedtagne gennemførelsesretsakter.
[6] Se https://www.etsi.org/images/files/ECMandates/m460.pdf
[7] Se https://www.enisa.europa.eu/publications/tsp_standards_2015.

Der er dog undtagelser i henhold til muligheden for brug af alternative standarder jf. bestemmelserne i artikel 30 og 39. De standarder, der er nævnt i disse artikler, er obligatoriske for kvalificerede udbydere.

3. Etablering af kvalificerede udbydere og kvalificerede tillidstjenester

3.1 Generelt

eIDAS-forordningen indeholder krav til, hvordan en udbyder skal starte en kvalificeret tillidstjeneste. Kravene specificerer også, hvordan udbyderen og de tjenester, den udbyder, skal organiseres og fungere for at blive kvalificeret.



Kontekst for kvalificering af tillidstjenester og tillidstjenesteudbydere i Danmark

Figur 1

For at en udbyder etableret i Danmark skal kunne udbyde kvalificerede tillidstjenester, skal udbyderen:

1. Kontakte Digitaliseringsstyrelsen og melde sin hensigt.
2. Få et akkrediteret overensstemmelsesvurderingsorgan til at vurdere udbyderens overholdelse af kravene i eIDAS-forordningen.
3. Overholde forordningens regler om krav til udbydere og til de udbudte tillidstjenester[8].
4. Ansøge Digitaliseringsstyrelsen om ret til at anvende betegnelsen kvalificeret.

[8] Se kapitel 4 til og med 7.

5. Godkendes af Digitaliseringsstyrelsen som en kvalificeret udbyder af tillidstjenester, jf. artikel 21, stk. 2 med optagelse på den danske positivliste.

Processen er beskrevet i artikel 21 og illustreret i Figur 1 ovenfor. I Danmark er det Digitaliseringsstyrelsen, som skal kontrollere og vurdere, om de aktiviteter og tjenester, der udbydes, opfylder kravene i forordningen. Hvis Digitaliseringsstyrelsen fastslår, at udbyderen opfylder kravene, får udbyderen status som 'kvalificeret leverandør af tillidstjenester' og tillidstjenesten status som 'kvalificeret tillidstjeneste'.

De kvalificerede udbydere og de kvalificerede tillidstjenester skal derefter optages på den danske positivliste[9]. Til formålet har Digitaliseringsstyrelsen brug for oplysninger om udbydere, tjenester og certifikater, der skal inkluderes på positivlisten for at opfylde kravene i gennemførelsesretsakten på dette område[10].

Tillidstjenesteudbydere, der ønsker at blive kvalificeret, henvender sig til et akkrediteret overensstemmelsesvurderingsorgan, som vurderer overholdelsen af bestemmelserne i forordningen og udarbejder en overensstemmelsesvurderingsrapport. Rapporten udarbejdes for udbyderens regning. Rapporten skal udfærdiges på dansk eller engelsk[11].

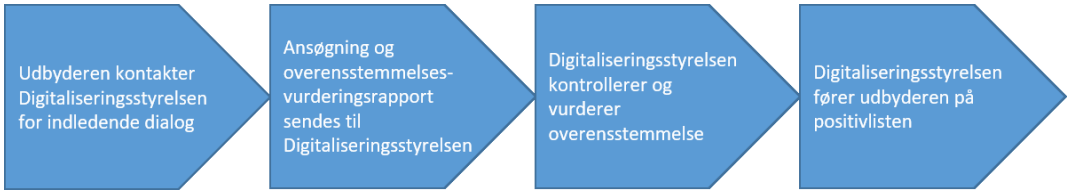
Det indre marked betyder, at udbyderen kan vælge et overensstemmelsesvurderingsorgan, der er akkrediteret i et andet EU-medlemsland. Kommissionen har opført alle godkendte overensstemmelsesvurderingsorganer på en liste[12]. Der er i øjeblikket ingen akkrediterede overensstemmelsesvurderingsorganer i Danmark. Der er indgået en aftale mellem Digitaliseringsstyrelsen og DANAK om etablering af en ordning for akkreditering af danske overensstemmelsesvurderingsorganer. Hermed er der mulighed for, at der i nær fremtid kan findes danske overensstemmelsesvurderingsorganer på listen.

---

[9] https://en.digst.dk/digitisation/eid/trusted-list/.
[10] Se bilag 2 til denne vejledning for mere information.
[11] Se mere om krav til ansøgningens indhold i denne vejlednings Bilag 2.
[12] https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation

3.2 Proces for at starte en kvalificeret tillidstjeneste

For at starte en kvalificeret tillidstjeneste skal udbyderen sende en ansøgning sammen med overensstemmelsesvurderingsrapporten til Digitaliseringsstyrelsen. Digitaliseringsstyrelsen vil kontrollere, om tillidstjenesteudbyderen og de tillidstjenester, som vedkommende udbyder, overholder forordningens krav. Hvis kravene er opfyldt, vil udbyderen og dens tjenester blive opført på den danske positivliste med status som kvalificeret.



Proces for at starte en kvalificeret tillidstjeneste i Danmark

Figur 2

Forud for den formelle proces anbefaler Digitaliseringsstyrelsen, at udbyderen kontakter Digitaliseringsstyrelsen så tidligt som muligt og inden ansøgning med henblik på at forberede processen og undgå tilbageløb.

3.3 Frister

Det følger af forordningen (artikel 21 stk. 2), at hvis Digitaliseringsstyrelsen ikke afslutter kontrollen af overensstemmelsesvurderingsrapporten inden for tre måneder efter, at rapporten er modtaget, skal Digitaliseringsstyrelsen underrette udbyderen om dette. Digitaliseringsstyrelsen angiver årsagen til forsinkelsen, og hvornår kontrollen antages at være afsluttet.

3.4 Digitaliseringsstyrelsens behandling af ansøgningen

Digitaliseringsstyrelsens behandling af ansøgningen består af en kontrol af overensstemmelsesvurderingsrapporten og de øvrige dokumenter, som ansøgningen består af. Kontrollen skal sikre, at Digitaliseringsstyrelsen kan bekræfte, at udbyderen og tillidstjenesterne opfylder alle kravene i forordningen og de relaterede gennemførelsesretsakter.

Der kan findes mere information om dette på Digitaliseringsstyrelsens hjemmeside, www.digst.dk og i Bilag 2 til denne vejledning.

3.5 EU-tillidsmærket for kvalificerede tillidstjenester

Udbydere af kvalificerede tillidstjenester er berettiget til at benytte EU-tillidsmærket, se figur 3. EU-tillidsmærket for kvalificerede tillidstjenester skal benyttes på en måde, som gør det muligt at vise tydeligt, hvilke kvalificerede tjenester tillidsmærket gælder for. EU-tillidsmærket er defineret og brugen af det reguleret i gennemførelsesretsakten (EU) 2015/806[13].

Figur 3 EU-tillidsmærket

[13] Kommissionens gennemførelsesforordning (EU) 2015/806 af 22. maj 2015 om specifikationer for udformningen af EU-tillidsmærket for kvalificerede tillidstjenester: https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:32015R0806&from=EN

4. Krav som gælder både kvalificerede og ikkekvalificerede udbydere

Visse bestemmelser i forordningen gælder for alle udbydere. Både kvalificerede og ikkekvalificerede udbydere er omfattet af kravene til erstatningsansvar og bevisbyrde (artikel 13) og sikkerhedskrav til tillidstjenesteudbydere (artikel 19). I punkt 35 i forordningens præambel fremgår det, at formålet med forordningen er at sikre, at både kvalificerede og ikkekvalificerede udbydere har en vis grad af sikkerhed i deres forretninger og i de tjenester, de udbyder. Desuden gælder et krav om, at tillidstjenester og de slutbrugerprodukter, der bruges til levering af disse tjenester, gøres tilgængelige for handicappede, når det er muligt (artikel 15).

4.1 Erstatningsansvar og bevisbyrde

Bestemmelsen i artikel 13 om erstatningsansvar og bevisbyrde gælder for både kvalificerede og ikkekvalificerede udbydere af tillidstjenester. Alle udbydere er ansvarlige for skader, der forsætligt eller uagtsomt påføres en fysisk eller juridisk person på grund af manglende overholdelse af forskrifterne.

For ikkekvalificerede udbydere hviler bevisbyrden for forsæt eller forsømmelighed hos den fysiske eller juridiske person, der hævder at have lidt et tab. For de kvalificerede udbydere gælder en såkaldt omvendt bevisbyrde. Det vil sige, at tillidstjenesteudbyderen beviser, at tabet ikke har fundet sted som følge af mangler i deres tillidstjenester.

Regler om erstatningsansvar anvendes i overensstemmelse med national lovgivning. Dette betyder, at ud over bestemmelserne i artikel 13 finder dansk rets almindelige regler om erstatningsansvar anvendelse.

4.2 Sikkerhedskrav til tillidstjenesteudbydere og hændelsesrapportering

Kravene i forordningen om sikkerhed i henhold til artikel 19, stk. 1 gælder både kvalificerede og ikkekvalificerede udbydere af tillidstjenester. Alle tillidstjenesteudbydere skal træffe passende tekniske og organisatoriske foranstaltninger til at styre de sikkerhedsmæssige risici i forbindelse med de tillidstjenester, de udbyder. Under hensyn til den seneste teknologiske udvikling skal disse foranstaltninger garantere et sikkerhedsniveau, der svarer til risikoens omfang.

Tillidstjenesteudbyderne bør navnlig tage skridt til at forhindre og minimere virkningen af sikkerhedsrelaterede hændelser og underrette de berørte parter om de negative virkninger af sådanne hændelser.

Dette betyder, at udbydernes sikkerhedsarbejde skal udføres langsigtet, kontinuerligt og systematisk, og at der skal være en klar rollefordeling. Eksempler på foranstaltninger og støtte til dette arbejde er beskrevet i standarder som ETSI EN 319 401. Denne standard identificerer, hvilke politikker, der kan kræves, og henviser til ISO/IEC 27002:2013.

Af artikel 19, stk. 2, fremgår det, at kvalificerede og ikkekvalificerede tillidstjenesteudbydere, der konstaterer et brud på sikkerheden eller tab af integritet, som har en væsentlig indvirkning på den udbudte tillidstjeneste eller de berørte personoplysninger, hurtigst muligt og under alle omstændigheder inden for 24 timer efter at være blevet opmærksomme på forholdet skal underrette Digitaliseringsstyrelsen og eventuelt andre relevante organer som fx. Datatilsynet.

Alle udbydere har tillige pligt til at underrette en fysisk eller juridisk person, der er blevet påvirket negativt af en hændelse.

Mere om rapportering af sikkerhedshændelser i kapitel 8.

4.3 Tilsyn

Digitaliseringsstyrelsens rolle som tilsynsorgan er beskrevet i forordningens artikel 17 stk. 3. Tilsynet omfatter både kvalificerede og ikkekvalificerede udbydere af tillidstjenester, som er etableret i Danmark.

4.3.1 Tilsyn med kvalificerede udbydere

Tilsyn med kvalificerede udbydere involverer både forebyggende aktiviteter og retrospektiv kontrol for at sikre, at udbydere og deres tjenester opfylder kravene i forordningen (artikel 17, stk. 3, litra a).

4.3.2 Tilsyn med ikkekvalificerede udbydere

For ikkekvalificerede udbydere fremgår det af forordningen (artikel 17, stk. 3, litra b), at tilsynsorganet skal gribe ind, når det underrettes om, at en ikkekvalificeret tjenesteudbyder eller en tillidstjeneste, den tilbyder, ikke opfylder kravene i forordningen, der gælder for ikkekvalificerede udbydere.

5. Regler for overensstemmelsesvurdering

5.1 Overensstemmelsesvurdering

Udbydere af tillidstjenester, der har til hensigt at levere kvalificerede tillidstjenester, skal rapportere dette til Digitaliseringsstyrelsen i overensstemmelse med artikel 21 i forordningen.

Samtidig med anmeldelsen indsender udbyderen en overensstemmelsesvurderingsrapport, der udføres af et akkrediteret overensstemmelsesvurderingsorgan. Anmeldelse og ansøgning skal udfærdiges på dansk eller engelsk[14].

Digitaliseringsstyrelsen kontrollerer rapporten og vurderer derefter, om udbyderen og de tillidstjenester, den tilbyder, opfylder kravene i forordningen. Kravene til kvalificerede udbydere af tillidstjenester er beskrevet i artikel 24.

Kommissionen kan ved hjælp af gennemførelsesretsakter bestemme referencenummeret for standarder for akkreditering af overensstemmelsesvurderingsorganer og for regler for overensstemmelsesvurdering (artikel 20, stk. 4).

Når det gælder overensstemmelsesvurderinger, vil det være hensigtsmæssigt at anvende standarden ETSI EN 319 403, der er i overensstemmelse med generelle krav og politikker fra standarden ETSI EN 319 401.

5.2 Overensstemmelsesvurderingsrapport

Udbydere af tillidstjenester, der ønsker status som kvalificeret, skal levere en overensstemmelsesvurderingsrapport med ansøgningen til Digitaliseringsstyrelsen. Rapporten skal vise, at både udbyderen og dennes tillidstjenester opfylder kravene i forordningen.

Kommissionen kan ved hjælp af gennemførelsesretsakter bestemme referencenummeret for standarder for rapportering af overensstemmelsesvurderingen, men Kommissionen har besluttet, at disse ikke skulle fastlægges på nuværende tidspunkt.

Overensstemmelsesvurderingsrapporten vil være en vigtig del af Digitaliseringsstyrelsens kontrol med, om en enkelt udbyder og dens tjenester betragtes som kvalificerede. Det skal derfor fremgå af rapporten, om kravene i forordningen er opfyldt, og hvorledes de overholdes. Rapporten i sin helhed skal tilgå Digitaliseringsstyrelsen.

---

[14] Se mere om krav til ansøgningens indhold i denne vejlednings Bilag 2

I mangel af en gennemførelsesretsakt, der kræver anvendelse af visse standarder, vil det være hensigtsmæssigt, at rapporten om overensstemmelsesvurdering som minimum indeholder de oplysninger, der er specificeret i ETSI EN 319 403.

6. Krav til kvalificerede tillidstjenester

6.1 Kvalificerede certifikater for elektroniske signaturer og segl

Forordningens artikel 25 og 35 specificerer retsvirkningerne af elektronisk signatur og elektronisk segl. Det fremgår af artikel 26 og 36, hvilke krav der stilles, for at en elektronisk signatur eller et elektronisk segl anses for at være avanceret.

En kvalificeret elektronisk signatur eller et kvalificeret elektronisk segl, som defineret i artikel 3, er en avanceret signatur eller segl baseret på et kvalificeret certifikat og oprettet ved hjælp af en kvalificeret elektronisk signaturgenereringsenhed. Artikel 27 og 37 regulerer medlemsstaternes forpligtelser til at acceptere elektroniske signaturer og segl fra andre medlemsstater.

For at et certifikat kan betragtes som kvalificeret, skal det opfylde kravene i artikel 28 og 38 og forordningens bilag I. Certifikatet er ikke underlagt flere krav end dem, der er anført i forordningen. Hvis et kvalificeret certifikat er spærret, skal det betragtes som ugyldigt fra det tidspunkt, hvor der anmodes om spærring. Status kan ikke efterfølgende ændres, så certifikatet igen kan betragtes som gyldigt.

Kommissionen har udarbejdet en gennemførelsesretsakt om formatet til avancerede elektroniske signaturer og segl[15].

Kommissionen kan ved hjælp af gennemførelsesretsakter bestemme referencenummeret for standarder for kvalificerede certifikater, der understøtter elektroniske underskrifter og segl.

I mangel af en beslutning om gennemførelse af retsakter vil det være hensigtsmæssigt at anvende standarderne ETSI EN 319 411-1 og ETSI EN 319 411-2.

6.2 Kvalificeret valideringstjeneste

Artikel 3, stk. 41, definerer validering som processen for at kontrollere og bekræfte gyldigheden af en elektronisk signatur eller et elektronisk segl. I henhold til artikel 32 i forordningen skal processen med validering af en kvalificeret elektronisk signatur bekræfte gyldigheden af en kvalificeret elektronisk signatur. Det forudsættes, at certifikatet, der understøtter signaturen på signeringstidspunktet,

---

[15] KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2015/1506
af 8. september 2015 om fastlæggelse af specifikationer vedrørende formater for avancerede elektroniske signaturer og avancerede segl, som skal anerkendes af offentlige myndigheder i henhold til artikel 27, stk. 5, og artikel 37, stk. 5. Https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:32015D1506&from=EN.

er et kvalificeret certifikat for elektronisk signatur, der opfylder kravene i forordningens bilag.

Systemet, der bruges til at validere den kvalificerede elektroniske signatur, skal give brugeren af tjenesten det korrekte resultat af valideringsprocessen. Systemet skal også gøre det muligt for brugeren af tjenesten at opdage eventuelle problemer relateret til sikkerheden.

Det følger af artikel 33, at en kvalificeret valideringstjeneste for kvalificerede elektroniske signaturer alene kan leveres af en kvalificeret tillidstjenesteudbyder.

Brugeren af tillidstjenesten skal kunne modtage resultatet af valideringsprocessen på en automatisk måde, der er pålidelig, effektiv og signeret eller forseglet af udbyderen af den kvalificerede valideringstjeneste.

Kommissionen kan ved hjælp af gennemførelsesretsakter bestemme referencenumre for standarder for validering af kvalificerede elektroniske signaturer samt standarder for kvalificerede valideringstjenester.

I mangel af en beslutning om gennemførelse af retsakter vil det være hensigtsmæssigt at anvende ETSI EN 319 102-1.

6.3 Kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer

Det følger af forordningens artikel 34, at en kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer kun må stilles til rådighed af en kvalificeret tillidstjenesteudbyder, der anvender procedurer og teknologier, der gør det muligt at forlænge pålideligheden af den kvalificerede elektroniske signatur ud over den teknologiske gyldighedsperiode.

Kommissionen kan ved hjælp af gennemførelsesretsakter bestemme referencenumre for standarder for kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer.

I mangel af en beslutning om gennemførelsesretsakter vil det være hensigtsmæssigt i forhold til AdES-signaturformater at anvende LTV/LTA-klasser efter ETSI EN 319 102, herunder tidsstempling efter ETSI EN 319 421.

6.4 Kvalificerede elektroniske tidsstempler

Ifølge forordningens artikel 42 skal kvalificerede elektroniske tidsstempler forbinde dato og tidspunkt med data på en sådan måde, at det med rimelighed udelukker muligheden for at ændre data, uden at det kan opdages. Tidsstemplerne skal bygge på en præcis tidskilde forbundet med koordineret universaltid (UTC).

Tidsstemplet skal være forsynet med den kvalificerede tillidstjenesteudbyders avancerede elektroniske signatur eller forseglet med dennes avancerede elektroniske segl eller med en anden tilsvarende metode.

Kommissionen kan ved hjælp af gennemførelsesretsakter bestemme referencenumre for standarder for forbindelsen af dato og tidspunkt med data og for brug af nøjagtige tidskilder.

I mangel af en beslutning om en gennemførelsesretsakt vil det være passende at anvende ETSI EN 319 421.

6.5 Kvalificerede elektroniske registrerede leveringstjenester

Det følger af forordningens artikel 44, at kvalificerede elektroniske registrerede leveringstjenester skal udbydes af en eller flere kvalificerede tillidstjenesteudbydere. Kvalificerede elektroniske registrerede leveringstjenester skal med en høj grad af tillid sikre identifikation af modtageren. De sikrer forud for levering af data identifikation af modtageren. De kontrollerer adressatens identitet, inden de leverer data. Afsendelse og modtagelse af data skal beskyttes af en kvalificeret udbyders avancerede elektroniske signatur eller avancerede elektroniske segl på en måde, så det er umuligt at ændre data uden at det opdages. Hvis det er nødvendigt at ændre data, for at de kan sendes eller modtages, angives dette klart over for afsenderen og modtageren af data. Dato og tidspunkt for afsendelse, modtagelse og en eventuel ændring af data angives ved hjælp af et kvalificeret elektronisk tidsstempel.

Kommissionen kan ved hjælp af gennemførelsesretsakter bestemme referencenumre for standarder for afsendelse og modtagelse af data.

I mangel af en beslutning om en gennemførelsesretsakt vil det være hensigtsmæssigt at anvende ETSI EN 319 521 eller ETSI EN 319 531, alternativt ETSI TS 102 640-3.

6.6 Kvalificerede certifikater for webstedsautentifikation

Det følger af forordningens artikel 45, at kvalificerede certifikater for webstedsautentifikation skal opfylde kravene i forordningens bilag IV.

Kommissionen kan ved hjælp af gennemførelsesretsakter bestemme referencenumre for standarder for kvalificerede certifikater for webstedsautentifikation. Et kvalificeret certifikat for webstedsautentifikation, der opfylder disse standarder, formodes at overholde kravene i bilag IV. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

I mangel af en beslutning om en gennemførelsesretsakt vil det være passende at bruge ETSI EN 319 411-1 og ETSI EN 319 411-2.

7. Krav til IT-systemer og kvalificerede enheder for elektronisk signatur og segl

eIDAS-forordningen kræver, at kvalificerede tillidstjenesteudbydere anvender pålidelige it-systemer. For at der kan produceres en kvalificeret elektronisk signatur eller et kvalificeret elektronisk segl, kræves anvendelse af en certificeret enhed.

7.1 Pålidelige IT-systemer

En kvalificeret tillidstjenesteudbyder, der tilbyder kvalificerede tillidstjenester, skal bruge pålidelige systemer og produkter under deres aktiviteter (artikel 24, stk. 2, litra e og f).

Der er lignende krav til pålidelige produkter, kaldet HSM (Hardware Security Module), der bruges til opbevaring eller generering af krypteringsnøgler i overensstemmelse med det tidligere gældende direktiv om elektroniske signaturer (EU) 1993/93.

Kommissionen kan ved hjælp af gennemførelsesretsakter opstille standarder for pålidelige systemer og produkter.

I mangel af en beslutning om gennemførelse af retsakter vil det være hensigtsmæssigt at anvende ETSI EN 419 211, ETSI EN 419 221, ETSI EN 419 231 og ETSI EN 419 241.

7.2 Krav til kvalificerede elektroniske signaturgenereringssystemer

Kvalificerede elektroniske signaturgenereringssystemer skal opfylde kravene i forordningens bilag II, jf. forordningens artikel 29.

Kommissionen kan ved hjælp af gennemførelsesretsakter opstille standarder for kvalificerede elektroniske signaturgenereringssystemer.

Kravene til de organer, der skal certificere overensstemmelsen mellem de kvalificerede elektroniske signaturgenereringssystem, er anført i artikel 30. Der er i øjeblikket intet certificeringsorgan i Danmark. En udbyder, der ønsker at tilbyde kvalificerede elektroniske signaturer, kan bruge et signaturgenereringssystem, der er certificeret af et certificeringsorgan i en anden EU-medlemsstat.

Kommissionens gennemførelsesretsakt om standarder for sikkerhedsvurdering af it-sikkerhedsprodukter (EU) 2016/650 blev vedtaget 25. april 2016[16].

Kommissionen bemyndiges til at vedtage delegerede retsakter i overensstemmelse med artikel 47 om specifikke kriterier, der skal opfyldes af de udpegede certificeringsorganer, der er omhandlet i artikel 30, stk. 1.

Det følger af forordningens artikel 31, at medlemsstaterne underretter Kommissionen om signaturfremstillingssystemer, der er certificeret i medlemsstaterne. På dette grundlag udarbejder Kommissionen en liste over certificerede systemer[17].

Det følger af artikel 39, at lignende certificeringskrav også gælder for kvalificerede elektroniske seglfremstillingssystemer.

Gennemførelsesretsakten oplister de standarder, der skal anvendes på kvalificerede systemer. Standarderne er anført i bilaget til gennemførelsesretsakten.

---

[16] KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2016/650 af 25. april 2016 om fastlæggelse af standarder for sikkerhedsvurdering af kvalificerede signa-tur- og seglgenereringssystemer, jf. artikel 30, stk. 3, og artikel 39, stk. 2. https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016D0650&from=EN

[17] Listen findes på adressen: https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

8. Rapportering af sikkerhedshændelser

8.1 Generelt

I henhold til artikel 19 skal både kvalificerede og ikkekvalificerede tillidstjenesteudbydere rapportere sikkerhedshændelser eller tab af integritet, der har væsentlig indvirkning på tillidstjenesten eller de persondata, der behandles i tjenesten. Rapporteringen skal ske til Digitaliseringsstyrelsen og til andre relevante myndigheder, fx Datatilsynet[18] og CFCS[19]. Rapporteringen skal ske hurtigst muligt og under alle omstændigheder inden for 24 timer efter, at udbyderen er blevet opmærksom på hændelsen.

Når det er sandsynligt, at et brud på sikkerheden eller tab af integritet vil krænke den fysiske eller juridiske person, som har modtaget tillidstjenesten, skal tillidstjenesteudbyderen også hurtigst muligt underrette den fysiske eller juridiske person om bruddet på sikkerheden eller tab af integritet.

Hvor det er relevant, og navnlig hvis et brud på sikkerheden eller tab af integritet berører to eller flere medlemsstater, skal Digitaliseringsstyrelsen informere tilsynsorganerne i andre berørte medlemsstater og ENISA, European Network and Information Security Agency.

Digitaliseringsstyrelsen skal også informere offentligheden eller kræve, at tillidstjenesteudbyderen gør det, hvis det fastslår, at det er i offentlighedens interesse, at et brud på sikkerheden eller tab af integritet offentliggøres.

Desuden har Digitaliseringsstyrelsen som tilsynsorgan en pligt til at give et årligt resumé af rapporterede sikkerhedshændelser til ENISA.

I henhold til artikel 19, stk. 4 har Kommissionen ret til at vedtage gennemførelsesretsakter, der fastlægger format og procedurer med frister for rapportering af sikkerhedshændelser, men dette arbejde er ikke planlagt på nuværende tidspunkt.

ENISA har dog udarbejdet anbefalinger til rapportering af sikkerhedshændelser. Anbefalingerne er rettet mod tilsynsorganerne og beskriver de begivenheder, som tilsynsorganet har pligt til at rapportere til ENISA. Hændelserne, der er specificeret af ENISA[20], skal rapporteres til Digitaliseringsstyrelsen. Udbydere skal derfor som minimum rapportere hændelser og levere de oplysninger, som beskrevet i afsnit 3 i ENISA's anbefaling.

---

[18] https://www.datatilsynet.dk/anmeld-brud-paa-persondatasikkerheden/
[19] https://fe-ddis.dk/cfcs/underretning/Pages/default.aspx
[20] Rammeværk for hændelsesrapportering for eIDAS artikel 19. Se https://www.enisa.europa.eu/publications/article19-incident-reporting-framework

8.2 Hvilke sikkerhedshændelser skal rapporteres?

Alle sikkerhedshændelser, som en udbyder af tillidstjenester vurderer til at have betydelig påvirkning af sikkerheden i tillidstjenester eller persondata, skal anmeldes til Digitaliseringsstyrelsen. Udbydere af tillidstjenester skal kun rapportere sikkerhedshændelser, der involverer systemer eller processer, der er under udbyderens kontrol. I tilfælde, hvor kernefunktionalitet leveres af en tredjepart, er tillidstjenesteudbyderen ansvarlig for at rapportere sikkerhedshændelser, der opstår i tredjepartssystemer eller -procedurer.

I vurderingen af, om en sikkerhedshændelse har en betydelig påvirkning på tillidstjenester og persondata, lægger Digitaliseringsstyrelsen følgende betragtninger til grund. En sikkerhedshændelse skal indberettes til Digitaliseringsstyrelsen, hvis mindst en af følgende betingelser er opfyldt:

- Hvis mere end én fysisk eller juridisk person er berørt
- Hvis et antal enkeltbegivenheder har samme årsag
- Hvis sikkerhedshændelsen afslører en sårbarhed, som potentielt kan berøre større antal fysiske eller juridiske personer
- Hvis sikkerhedshændelsen omfatter samfundskritiske funktioner eller andre tillidstjenesteudbydere.

Denne vejledning er baseret på ENISA's rammer for sikkerhedshændelser.

8.3 Anmeldelse til Digitaliseringsstyrelsen

Rapporter om sikkerhedshændelser sendes via e-mail til tilsyn_eIDAS@digst.dk. Digitaliseringsstyrelsen vil bekræfte alle modtagne rapporter.

9. Ophør af virksomhed

Forordningen opstiller krav til, hvad en kvalificeret udbyder af tillidstjenester skal gøre, hvis den ønsker at ophøre med virksomheden.

9.1 Information til Digitaliseringsstyrelsen

En udbyder er forpligtet til at informere Digitaliseringsstyrelsen om eventuelle ændringer i driften af de kvalificerede tillidstjenester, hvis udbyderen ønsker at indstille udbuddet af tillidstjenesten eller at ophøre med virksomheden.

Allerede ved opstart af virksomheden skal udbyderen fremlægge en plan for virksomhedens ophør for Digitaliseringsstyrelsen for at opnå kvalificeret status.

Reglerne for ophør af virksomhed skal garantere kvalificerede tillidstjenesters bæredygtighed og holdbarhed og sikre brugernes tillid til disse tjenesters kontinuitet. Derfor gælder forpligtelserne for de kvalificerede udbydere i relativt lang tid efter, at den kvalificerede tillidstjeneste er ophørt.

9.2 Opbevaring af information

Det følger af forordningens artikel 24, stk. 2, litra h), at en kvalificeret udbyder af tillidstjenester skal registrere og holde alle relevante oplysninger tilgængelige, som den har produceret eller modtaget i en rimelig periode. I artiklen hedder det endvidere, at registreringen af informationen kan ske elektronisk.

Relevante oplysninger nævnt ovenfor kan være aftaler og dokumentation, som ligger til grund for udstedelse af hvert enkelt certifikat. Det er vigtigt, at sådanne oplysninger bevares, fordi der kan opstå juridiske spørgsmål, fx om det kan bevises, at en kvalificeret elektronisk signatur eller et kvalificeret elektronisk segl tidligere har været gyldigt. Det kan også tænkes, at der stilles spørgsmål til, hvordan en person blev identificeret, da et certifikat blev udstedt af udbyderen.

9.3 Offentliggørelse af spærring af certifikater og informering af berørte parter

Det følger af forordningens artikel 24, stk. 3, at hvis en kvalificeret udbyder af kvalificerede certifikater beslutter at spærre et certifikat, skal spærringen registreres i udbyderens certifikatdatabase og offentliggøres. I artiklen hedder det, at dette skal ske i god tid og inden for 24 timer, efter at udbyderen har modtaget anmodningen om spærring.

Det følger også af artikel 24, stk. 4, at en kvalificeret udbyder i disse situationer skal informere alle interesserede parter om, at de kvalificerede certifikater har status som spærret.

Desuden skal informationerne stilles til rådighed på en automatiseret måde, der er pålidelig, gratis og effektiv, jf. artikel 24, stk. 4. Oplysningerne skal som minimum for et certifikat ad gangen være automatisk og gratis tilgængelige til enhver tid og ud over gyldighedsperioden på pålidelig og effektiv vis.

10. Bilag

10.1 Bilag 1 – Vedtagne gennemførelsesretsakter for tillidstjenester

Gennemførelsesretsakt	*Reference til eIDAS-forordningen*	*Gennemførelsesretsaktens navn*
Gennemførelsesretsakt (EU) 2015/806	Artikel 23, stk. 3	KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2015/806 af 22. maj 2015 om specifikationer for udformningen af EU-tillidsmærket for kvalificerede tillidstjenester
Gennemførelsesretsakt (EU) 2015/1505	Artikel 22, stk. 5	KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2015/1505 af 8. september 2015 om fastlæggelse af tekniske specifikationer og formater for positivlister i henhold til artikel 22, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked
Gennemførelsesretsakt (EU) 2015/1506	Artikel 27, stk. 5 Artikel 37, stk. 5	KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2015/1506 af 8. september 2015 om fastlæggelse af specifikationer vedrørende formater for avancerede elektroniske signaturer og avancerede segl, som skal anerkendes af offentlige myndigheder i henhold til artikel 27, stk. 5, og artikel 37, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked

Gennemførelsesretsakt (EU) 2016/650	Artikel 30, stk. 3 Artikel 39, stk. 2	KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2016/650 af 25. april 2016 om fastlæggelse af standarder for sikkerhedsvurdering af kvalificerede signatur- og seglgenereringssystemer, jf. artikel 30, stk. 3, og artikel 39, stk. 2, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked

10.2 Bilag 2 – Indhold af ansøgning

Ansøgning om optagelse på positivlisten skal indeholde den information, der er anført i dette bilag. Ansøgningen skal udfærdiges på dansk eller engelsk. Det sætter Digitaliseringsstyrelsen i stand til at vurdere og kontrollere, om den ansøgende udbyder af en tillidstjeneste opfylder eIDAS-forordningens krav jf. forordningens artikel 17.

Ansøgningen skal indeholde dokumentation som følger:

- Produktbeskrivelse til slutbrugere, herunder beskrivelse af ansvarsbegrænsning
- Den fulde overensstemmelsesvurderingsrapport
- Detaljeret beskrivelse af hvordan udbyder overholder de enkelte krav nævnt i ETSI EN 319 401 afsnit 5, 6, og 7.
- Dokumentation for overholdelse af ISO27002 eller anden internationalt anerkendt standard for informationssikkerhed.
- En plan for ophør af de udbudte tillidstjenester
- En plan for afhjælpning af mindre afvigelser
- Dokumentation for ansvarsforsikring eller bankgaranti i overensstemmelse med ansvarsbegrænsning i produktbeskrivelsen

Hertil skal ansøgningen indeholde dokumentation som følger afhængigt af tillidstjenestens art:

- For udstedere af kvalificerede certifikater: Certifikatpolitikker, rodcertifikat(er), Certificate Practice Statement
- For udbydere af kvalificeret tidsstemplingstjeneste: Tidsstemplingspolitik og evt. tidsstemplingspraksis, hvis en sådan er udarbejdet.
- For udbydere af kvalificerede elektroniske leveringstjenester: Leveringspolitik, dokumentation for overholdelse af forordningens artikel 44.

- For udbydere af kvalificerede opbevaringstjenester af kvalificerede signaturer og segl: Politik for opbevaring
- For udbydere af kvalificerede valideringstjenester af kvalificerede signaturer og segl: Valideringspolitik

10.3 Bilag 3 – Digitaliseringsstyrelsens politikker

Digitaliseringsstyrelsen har udviklet og vedligeholder en række politikker for kvalificerede og ikkekvalificerede tillidstjenester til brug i offentlige tjenester.

OCES certifikatpolitikker

I 2003 blev de første politikker for "Offentlige Certifikater til Elektroniske Services (OCES)" offentliggjort. OCES-certifikater er ikkekvalificerede certifikater og findes fremadrettet til fysiske personer associeret med juridiske enheder (OCES-medarbejder, MOCES) og juridiske enheder (OCES-virksomhed, VOCES). Frem til overgangen til MitID og NemLog-in3 gælder tillige person certifikat til NemID (POCES) og funktionscertifikat (FOCES)

OCES certifikatpolitikkerne[21] er fra version 7.0 i overensstemmelse med ETSI EN 319 401 og ETSI EN 319 411-1.

Udbydere, der ønsker at udstede OCES-certifikater, skal anvende Digitaliseringsstyrelsens OCES-certifikatpolitikker og skal have indgået en aftale om udstedelse med Digitaliseringsstyrelsen inden udstedelse af certifikater.

Kvalificerede certifikatpolitikker

Digitaliseringsstyrelsen har udviklet og vedligeholder tre certifikatpolitikker for udstedelse af kvalificerede certifikater. Disse kan anvendes til udstedelse af kvalificerede certifikater til hhv. fysiske personer, fysiske personer associeret med juridiske enheder og juridiske enheder.

De kvalificerede certifikatpolitikker er i overensstemmelse med ETSI EN 319 401, ETSI EN 319 411-1 og ETSI EN 411-2.

Udstedere af kvalificerede certifikater kan vælge at benytte disse certifikatpolitikker, men har i øvrigt frihed til selv at udvikle egne certifikatpolitikker, når blot disse lever op til krav i eIDAS forordningen inklusive implementerende gennemførelsesretsakter.

[21] Se https://www.nemid.nu/dk-da/om-nemid/historien_om_nemid/oces-standarden/ eller https://certifikat.gov.dk/

Kvalificeret tidsstemplingspolitik
Digitaliseringsstyrelsen har desuden udviklet og vedligeholder en tidsstemplingspolitik[22] for udstedelse af kvalificerede tidsstempler.

Denne kvalificerede tidstemplingspolitik er i overensstemmelse med ETSI EN 319 401 og ETSI EN 319 421.

Udbydere af kvalificerede tidsstempler kan vælge at benytte denne tidsstemplingspolitik, men har i øvrigt frihed til selv at udvikle egne tidsstemplingspolitikker, når blot disse lever op til krav i eIDAS-forordningen inklusive implementerende gennemførelsesretsakter.

Revisionsvejledning
I forbindelse med ovenstående politikker, er der udviklet revisionsvejledninger til henholdsvis certifikatpolitikker og tidsstemplingspolitikker. Disse vejledninger giver mulighed for en struktureret håndtering af udformning af overensstemmelsesrapporter for både udbyderen og overensstemmelsesvurderingsorganet.

Samme model for revision anvendes desuden for NSIS-anmeldelser, hvilket bør forenkle arbejdet for udbydere, der både anmelder NSIS-løsninger og tjenester baseret på en af ovenstående politikker.

Hvis en udbyder vælger selv at udvikle kvalificerede politikker, kan man med fordel anvende revisionsvejledningen som inspiration.

[22] Se https://certifikat.gov.dk/

digst.dk