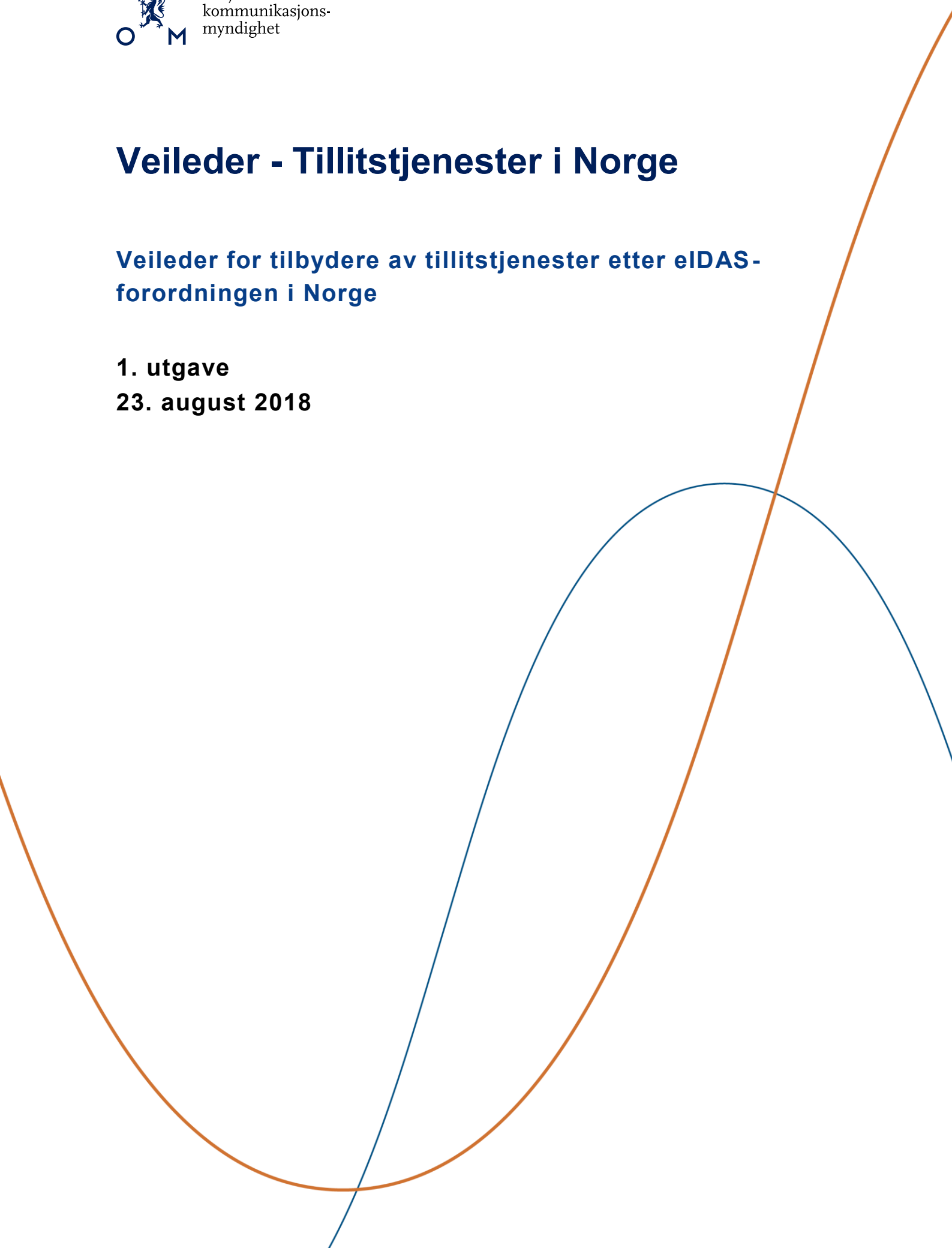
Nasjonal kommunikasjons-myndighet

Veileder - Tillitstjenester i Norge

Veileder for tilbydere av tillitstjenester etter eIDAS-forordningen i Norge

1. utgave

23. august 2018



Innholdsfortegnelse

Revisjonsliste

Revisjon	Dato	Endring/Merknad
1	23. august 2018	1. utgave

1 Innledning

Den 1. juli 2016 trådte EU-forordningen[1] om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre markedet (eIDAS-forordningen) i kraft i EUs medlemsland.

Elektronisk identifikasjon og elektroniske signaturer er en viktig forutsetning for at enkeltpersoner og bedrifter skal bruke digitale tjenester. For at et system med elektronisk identifikasjon skal fungere er det nødvendig at alle involverte parter oppfatter det sNkom sine om pålitelig. Forordningen inneholder en rettslig ramme for en type tjenester som tilbydere av elektronisk identitet og elektronisk signatur vanligvis tilbyr. Forordningen inneholder også regler for tilbyderne av slike tjenester. Målet er å øke tilliten til elektroniske transaksjoner i det indre marked ved å gi et felles grunnlag for sikker elektronisk samspill mellom bedrifter, borgere og offentlige myndigheter.

eIDAS-forordningen stiller flere krav til tilbyderne, men reglene er generelt utformet. I stedet for å gi detaljerte regler, gis det i forordningen hjemmel til at Europakommisjonen (heretter Kommisjonen) skal eller kan vedta gjennomføringsrettsakter. Disse gjennomføringsrettsaktene skal i større grad beskrive detaljerte tekniske krav og andre utfyllende regler. Kommisjonen har vedtatt de gjennomføringsrettsaktene som er obligatoriske å utarbeide i henhold til eIDAS-forordningen (se vedlegg 1).

1.1 Inkorporering av eIDAS-forordningen i Norge

Lov om gjennomføring av EUs forordning om elektronisk kommunikasjon og tillitstjenester for elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked, og samtykke til EØS-komiteens beslutning nr. 22/2018 om innlemmelse av forordningen i EØS-avtalen (lov om elektroniske tillitstjenester[2]) trådte i kraft 15. juni 2018. Loven inkorporerer eIDAS-forordningen i norsk rett. Loven skal bidra til økt elektronisk samhandling mellom næringsdrivende, innbyggere og offentlige myndigheter på tvers av landegrensene i EØS.

1.2 Gjennomføringsrettsaktene

Forordningen gir Kommisjonen hjemmel til å vedta gjennomføringsrettsakter. Flere slike rettsakter er vedtatt. Gjennomføringsrettsaktene tas inn som norske forskrifter med hjemmel i lov om elektroniske tillitstjenester.

[1] Europaparlamentets og rådets forordning (EU) nr. 910/2014 av den 23. juli 2014 om elektronisk identifisering og tillitstjenester for elektroniske transaksjoner på det indre marked og om oppheving av direktiv 1999/93/EF
[2] https://lovdata.no/dokument/NL/lov/2018-06-15-44

1.3 Selvdeklarasjonsordningen

Lov om elektronisk signatur av 15. juni 2001 nr. 81 § 16 a (esignaturloven, opphevet per 15. juni 2018) gir hjemmel til å etablere frivillige sertifiserings-, godkjennings- eller selvdeklarasjonsordninger for sertifikatutstedere. Formålet er å høyne sikkerhetsnivået for sertifikattjenester og dermed øke tilliten til og bruken av slike tjenester.

Ordningen med selvdeklarasjon vil ikke oppfylle kravene i forordningen for kvalifiserte tillitstjenester. Begrepet tillitstjenester er på EU-nivå uttømmende definert i forordningen. Begrepet omfatter blant annet ikke autentiseringstjenester eller krypteringstjenester, kun de kvalifiserte sertifikater som de eventuelt er basert på. For slike tjenester vil derfor en selvdeklarasjonsordning kunne bidra til å øke tilliten.

I lov om elektroniske tillitstjenester § 10 er det derfor gitt overgangsregler som innebærer at forskrifter gitt i medhold av esignaturloven gjelder inntil de blir opphevet. Forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere gjelder derfor inntil videre.

1.4 Nkom sin rolle

Nkom er i forskrift utpekt som tilsynsmyndighet og skal utføre tilsynsorganets oppgaver i henhold til eIDAS-forordningen. Nkom skal altså føre tilsyn med at tilbydere av tillitstjenester oppfyller kravene i lov om elektroniske tillitstjenester.

1.5 Nærmere om veilederen

Denne veilederen inneholder en beskrivelse av prosessen med å etablere seg som tilbyder av en kvalifisert tillitstjeneste, hva som er kravene til en ikke-kvalifisert tilbyder, hendelsesrapportering og anvendelse av ulike standarder.

Målgruppen for veilederen er først og fremst tilbydere av tillitstjenester som ønsker å etablere seg som kvalifiserte. Veiledningen er også rettet mot tilbydere av ikke-kvalifiserte tillitstjenester, relevante myndigheter og andre organer. Veiledningen er ikke bindende, men er en beskrivelse av regelverket som gjelder og den støtte som finnes i form av standarder.

2 Bakgrunn

2.1 eIDAS-forordningen og tillitstjenester

Formålet med eIDAS-forordningen er å sikre et velfungerende marked og oppnå et passende sikkerhetsnivå for elektronisk identifikasjon og tillitstjenester (artikkel 1).

Forordningen fastsetter prinsippet om et indre marked (artikkel 4). Tilbyder av tillitstjenester i en medlemsstat kan ikke hindres fra å levere slike tjenester i en annen medlemsstat av grunner fastsatt i forordningen. Signaturer og segl, og andre tillitstjenester som er i samsvar med forordningen skal være underlagt fri bevegelse på det indre markedet.

Forordningen inneholder generelle bestemmelser om tillitstjenester og kvalifiserte tillitstjenester, samt spesielle bestemmelser om elektronisk signaturer, elektroniske segl, elektroniske tidsstempler, elektroniske tjenester for registrert sending og nettstedsautentisering.
I tillegg er det bestemmelser om elektroniske dokumenter som er lagret i elektronisk form som også inneholder lyd- og videoopptak og audiovisuelle opptak.

2.1.1 Anvendelsesområde

eIDAS-forordningen regulerer ordninger for elektronisk identifikasjon som en medlemsstat har meldt og tilbydere av tillitstjenester som er etablert innen unionen (artikkel 2 nr. 1).

Forordningen gjelder imidlertid ikke for tilbydere av tillitstjenester som følger av nasjonal lovgivning eller som er avtalt mellom en avgrenset krets av deltakere, og som brukes innen ett lukket system (artikkel 2 nr. 2). I fortalens punkt 21 utdypes hva som menes med et lukket system. Der fremgår det at forordningen ikke gjelder tilbydere av tillitstjenester som brukes innen lukkede systemer med et avgrenset antall deltakere, og som ikke påvirker tredjeparter. For eksempel nevnes systemer som er opprettet i selskaper eller offentlig administrasjon for styring av interne prosedyrer. Det oppgis at bare tillitstjenester som tilbys offentligheten og som påvirker tredjeparter, bør oppfylle de krav som stilles i forordningen.

Forordningen påvirker heller ikke bestemmelser i nasjonal lovgivning eller europeisk lov som regulerer inngåelse av avtaler og deres gyldighet, eller andre juridiske eller prosessuelle reguleringer angående formelle krav (artikkel 2 nr. 3). Forordningen bør heller ikke påvirke nasjonale formkrav i offentlige registre, spesielt ikke kommersielle registre eller eiendomsregistre (fortalens punkt 21). Norsk lovgivning stiller i dag ingen krav til å bruke kvalifiserte tillitstjenester verken mellom enkelte eller mot offentlige organer.

2.1.2 Definisjoner

Artikkel 3 inneholder definisjoner.

Nedenfor er noen av dem gjengitt:

16) «tillitstjeneste» en elektronisk tjeneste som normalt tilbys mot betaling, og som består av

> a) framstilling, kontroll og validering av elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler, elektroniske tjenester for registrert sending og sertifikater knyttet til slike tjenester eller
>
> b) framstilling, kontroll og validering av sertifikater for nettstedsautentisering eller
>
> c) bevaring av elektroniske signaturer, segl eller sertifikater knyttet til slike tjenester

17) «kvalifisert tillitstjeneste» en tillitstjeneste som oppfyller gjeldende krav fastsatt i denne forordning

25) «elektronisk segl» data i elektronisk form som er lagt ved eller er logisk knyttet til andre data i elektronisk form for å sikre sistnevntes opprinnelse og integritet

33) «elektronisk tidsstempel» data i elektronisk form som knytter andre data i elektronisk form til et bestemt tidspunkt og dokumenterer at sistnevnte data eksisterte på det tidspunktet,

36) «elektronisk tjeneste for registrert sending» en tjeneste som gjør det mulig å overføre data elektronisk mellom tredjeparter, som omfatter dokumentasjon av håndteringen av de overførte dataene, herunder dokumentasjon av sending og mottak av dataene, og som beskytter overførte data mot tap, tyveri, skade eller ikke-autoriserte endringer

38) «sertifikat for nettstedsautentisering» en attest som gjør det mulig å autentisere et nettsted, og som knytter nettstedet til den fysiske eller juridiske personen som sertifikatet er utstedt til.

2.1.3 Kvalifiserte tillitstjenester

Artiklene 20 til 24 inneholder spesielle bestemmelser om kvalifiserte tillitstjenester. En tilbyder som ønsker å tilby slike tjenester, skal sende en melding til tilsynsmyndigheten (Nkom) om dette. Tilbyderen skal også sende en samsvarsvurderingsrapport utstedt av et samsvarsvurderingsorgan[3]. Dersom tilbyderen og de tillitstjenestene som tilbys oppfyller kravene i eIDAS-forordningen, føres den opp på en nasjonal liste (tillitsliste) med tildelt status som kvalifisert. Denne listen inneholder opplysninger om kvalifiserte tilbydere av tillitstjenester

[3] Organet omtales som samsvarsvurderingsorgan eller Conformity Assessment Body (CAB)

og de tjenestene som tilbys. Det er også en bestemmelse om tilbakekalling av en status som kvalifisert, dersom kravene i forordningen ikke lenger er oppfylt av tilbyderen.

For kvalifiserte tilbydere av tillitstjenester gjelder spesielle krav, for eksempel:

- kontroll av identiteten til den som et kvalifisert sertifikat utstedes til
- personellets utdanning/opplæring og kunnskap
- økonomisk evne til å bære risikoen for virksomheten
- teknisk sikkerhet og pålitelige systemer
- løpende planlegging for å sikre kontinuitet i tjenesten i tilfelle opphør av virksomheten[4].

Forordningen inneholder også krav til at tilbydere av kvalifiserte tillitstjenester jevnlig (annethvert år) skal vurderes av akkrediterte organer for å kontrollere at tilbyderne oppfyller kravene i forordningen.

2.1.4 Overgangsbestemmelser

Da lov om elektroniske tillitstjenester trådte i kraft, opphørte direktiv 1999/93/EF, direktivet om elektroniske signaturer (esignaturdirektivet)[5]. Det samme gjaldt den norske esignaturloven.

Artikkel 51 i eIDAS-forordningen inneholder visse overgangsbestemmelser. Elektroniske signaturer og kvalifiserte sertifikater til fysiske personer utstedt etter esignaturdirektivet skal betraktes som kvalifiserte tjenester i henhold til eIDAS-forordningen.

2.2 Gjennomføringsrettsaker og standarder

2.2.1 Gjennomføringsrettsakter

eIDAS-forordningen inneholder ikke detaljerte regler. I stedet er Kommisjonen gitt hjemmel til å fastsette gjennomføringsrettsakter for å gi mer detaljert regulering. Som nevnt ovenfor blir disse gjennomføringsrettsaktene innført som norske forskrifter med hjemmel i lov om elektroniske tillitstjenester.

De fleste gjennomføringsrettsaktene tillater Kommisjonen å henvise til standarder på området. Hvis Kommisjonen refererer til en standard, betyr det ikke at tilbydere må overholde denne standarden, men følges standarden antas det at kravene i forordningen er oppfylt.

[4] Se kapittel 9

[5] Europaparlamentets og rådets direktiv 1999/93/EF av den 13. desember 1999 om en fellesskapsramme for elektroniske signaturer

2.2.2 Standarder

Kommisjonen har gitt de europeiske standardiseringsorganisasjonene CEN og ETSI et standardiseringsoppdrag (mandat M/460[6]) med å utvikle standarder innen tillitstjenester. CEN og ETSI har i samarbeid utviklet et felles sett av standarder innen sikker elektronisk transaksjon for e-handel og tjenester i Europa. Formålet med mandatet er å skape betingelser for interoperabilitet og et europeisk standard-rammeverk. Disse standardene er tilpasset eIDAS-forordningen og utgjør grunnlaget for gjennomføringsrettsaktene. Standardene har også til hensikt å legge grunnlaget for fremtidens gjennomføringsrettsakter.

I påvente av Kommisjonens implementering av gjennomføringsrettsakter om bruk av standarder, er det hensiktsmessig å bruke standardene fra CEN og ETSI på området for tillitstjenester.

ENISA har publisert en veiledning for bruk standarder opp mot kravene i eIDAS-forordningen[7].

2.2.3 Alternative standarder

Alternative standarder enn de som er påpekt i Kommisjonens gjennomføringsrettsakter kan brukes, så lenge kravene i eIDAS-forordningen er oppfylt.

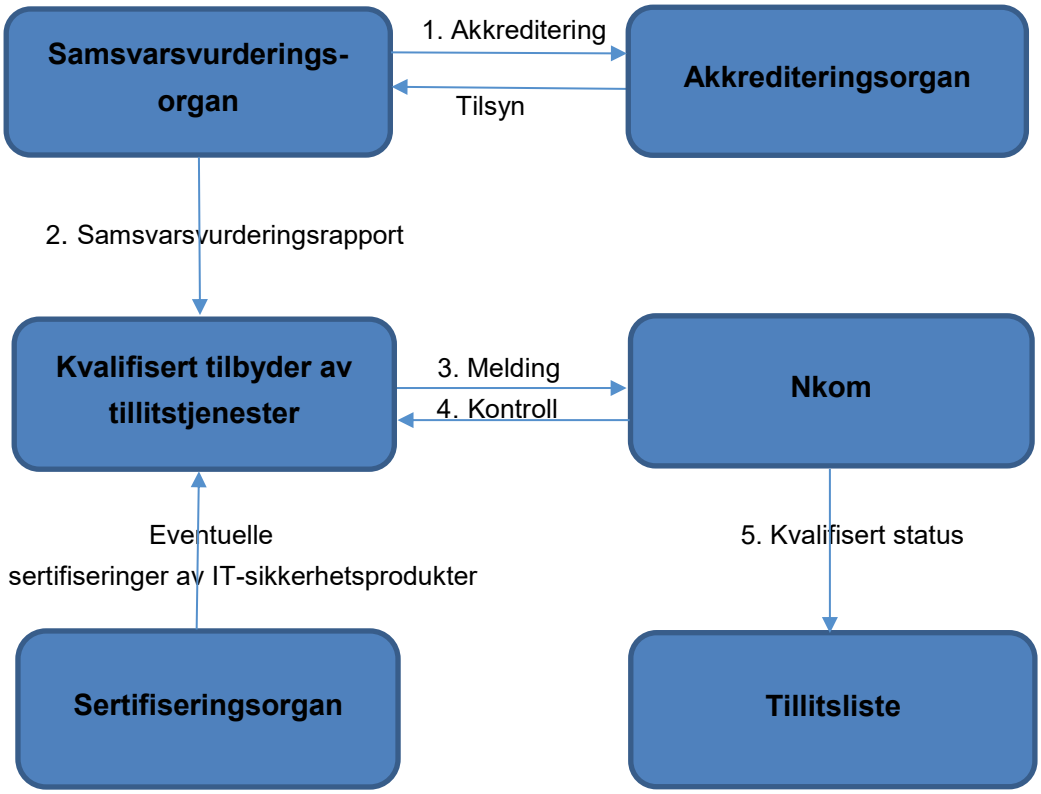
Det er imidlertid unntak fra muligheten for å bruke alternative standarder jf. bestemmelsene i artikkel 30 og 39. De standardene som utpekes i disse artiklene er obligatoriske for kvalifiserte tilbydere å følge.

[6] http://www.etsi.org/images/files/ECMandates/m460.pdf
[7] https://www.enisa.europa.eu/publications/tsp_standards_2015

3 Etablering av kvalifiserte tilbydere og kvalifiserte tillitstjenester

3.1 Generelt

eIDAS-forordningen inneholder krav til hvordan en tilbyder skal starte opp en kvalifisert tillitstjeneste. Kravene angir også hvordan tilbyderen og tjenestene den tilbyr skal innrettes for å kunne kalles kvalifisert.



For at tilbydere skal kunne tilby kvalifiserte tillitstjenester kreves det at de:

1. engasjerer et akkreditert samsvarsvurderingsorgan for vurdering av samsvar med kravene i eIDAS-forordningen.
2. overholder forordningens regler om krav til tilbydere og til tillitstjenestene som tilbys[8].
3. melder til Nkom at de ønsker å starte opp en eller flere kvalifiserte tillitstjenester.
4. blir godkjent av Nkom som kvalifisert tilbyder for tillitstjenester, jf. artikkel 21 nr 2.

[8] Se kapittel 4-7

Prosessen beskrives i artikkel 21. Her beskrives det at Nkom skal kontrollere virksomheten og tjenestene som tilbys at de oppfyller kravene i forordningen. Dersom Nkom fastslår at tilbyderen oppfyller kravene skal den gis status som kvalifisert tilbyder av tillitstjenester og kvalifisert status for tillitstjenestene.

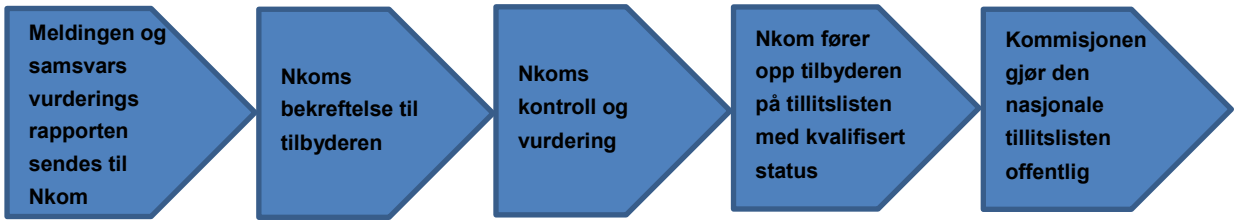
De kvalifiserte tilbyderne og de kvalifiserte tillitstjenestene skal deretter føres opp på Norges tillitsliste[9] (Trusted List).

Nkom vil ha behov for informasjon om tilbydere, tjenester og sertifikater som skal inkluderes på tilitslisten for å oppfylle kravene i gjennomføringsrettsaken på dette området[10].

Tjenestetilbydere som ønsker å bli kvalifisert må henvende seg til et akkreditert organ for å vurdere om bestemmelsene i forordningen overholdes. Det er per i dag ingen akkrediterte organer i Norge. Det er noen organer som er akkreditert i Europa, og flere som er i ferd med å bli akkreditert. Spørsmål om akkrediterte organer i Norge kan stilles til Norsk Akkreditering. Det indre markedet innebærer at tilbyderen kan henvende seg til et organ for samsvarsvurdering som er akkreditert i et annet medlemsland i EU.

3.2 Prosess for å starte en kvalifisert tillitstjeneste

For å starte en kvalifisert tillitstjeneste må tilbyderen sende en melding sammen med samsvarsvurderingsrapport til Nkom. Nkom vil vurdere samsvarsvurderingsrapporten og ta stilling til om tilbyderen av kvalifisert tjenester oppfyller kravene i forordningen eller ikke. Hvis kravene er oppfylt blir tilbyderen og deres tjenester ført opp på nasjonal tillitsliste med tildelt kvalifisert status.



[9] https://www.nkom.no/teknisk/tillitstjenester/kvalifiserte-tilbydere/tillitsliste
[10] Kommisjonens gjennomføringsrettsakt (EU) 2015 av 8. september 2015 om fastsettelse av tekniske spesifikasjoner og formater vedrørende tillitslister i henhold til artikkel 22 nr. 5

3.3 Frister

Det fremgår av forordningen (artikkel 21 nr. 2) at dersom ikke Nkom sin kontroll av samsvarsvurderingsrapporten er gjort innen tre måneder fra rapporten ble sendt inn, skal Nkom informere tilbyderen om dette. Nkom skal angi grunnen til forsinkelsen og når kontrollen antas å være sluttført.

3.4 Nkom sin behandling av varselet

Nkom sin behandling av varselet består dels av en kontroll av rapporten fra samsvarsvurderingen, og dels av ytterligere kontroller som Nkom anser nødvendig for å kunne bekrefte at tilbyderen og tillitstjenestene oppfyller samtlige krav i forordningen og tilhørende gjennomføringsrettsaker. Mer informasjon er tilgjengelig på Nkom sine nettsider[11].

[11] https://www.nkom.no/teknisk/tillitstjenester/eidas/eidas-forordning

4 Krav som dekker både kvalifiserte og ikke-kvalifiserte tilbydere

Visse bestemmelser i forordningen gjelder alle tilbydere. Det vil si også tilbydere som ikke er kvalifiserte i henhold til forordningen. Både kvalifiserte og ikke-kvalifiserte tilbydere omfattes av kravene om erstatningsansvar (artikkel 13) og sikkerhet (artikkel 19). I fortalen punkt 35 fremgår det at formålet med reguleringen er å forsikre seg om at også de ikke-kvalifiserte tilbyderne har en viss grad av sikkerhet i sine virksomheter og i de tjenestene som de tilbyr.

4.1 Erstatningsansvar (artikkel 13)

Bestemmelsen i artikkel 13 om erstatningsansvar gjelder for både kvalifiserte og ikke-kvalifiserte tilbydere av tillitstjenester. Alle tilbydere har ansvar for skade som forsettlig eller uaktsomt er påført en fysisk eller juridisk person på grunn av manglende overholdelse av forordningens krav.

For ikke-kvalifiserte tilbydere hviler bevisbyrden for forsett eller uaktsomhet på den fysiske eller juridisk person som hevder å ha blitt påført et tap. For de kvalifiserte tilbyderne gjelder en såkalt omvendt bevisbyrde. Det vil si at det er tilbyder som må godtgjøre at tapet ikke er oppstått som følge av mangler ved deres tillitstjenester.

Regler om erstatningsansvar skal anvendes i samsvar med nasjonal lovgivning. Det innebærer at i tillegg til bestemmelsene i artikkel 13 er det norske regler om erstatningsansvar som gjelder.

4.2 Sikkerhetskrav og hendelsesrapportering (artikkel 19)

Kravene i forordningen om sikkerhet i henhold til artikkel 19 nr. 1 både kvalifiserte og ikke-kvalifiserte tilbydere av tillitstjenester. Alle tjenestetilbydere skal treffe hensiktsmessige tekniske og organisatoriske tiltak for å håndtere sikkerhetsrisikoen til de tillitstjenestene som tilbys. Sikkerhetsnivået må stå i forhold til graden av risiko og ta hensyn til teknologiutviklingen.

Det må treffes tiltak for å forhindre og minimere sikkerhetshendelser, og informere berørte parter om hendelser og dens konsekvenser.

Dette vil bety at tilbydernes sikkerhetsarbeid skal utføres langsiktig, kontinuerlig og systematisk, og at det skal være en klar rollefordeling. Eksempler på handlinger og støtte i dette arbeidet er beskrevet i standarder som ETSI EN 319 401. Denne standarden utpeker hvilke policy dokumenter som kan være nødvendig og refererer til ISO/IEC 27002: 2013.

Artikkel 19 nr. 2 sier at alle tilbydere, kvalifiserte og ikke-kvalifiserte, så snart som mulig og senest innen 24 timer skal rapportere sikkerhets- eller integritetshendelser til Nkom. Dette gjelder hendelser som i betydelig grad påvirker tillitstjenesten som tilbys, eller de personopplysninger som fremgår. Alle tilbyderne har videre en plikt til å varsle en fysisk eller juridisk person som har blitt negativt påvirket på grunn av inntruffet hendelse.

Mer om rapportering av sikkerhetshendelser i kapittel 8.

4.3 Tilsyn (artikkel 17)

Nkom sin rolle som tilsynsmyndighet er beskrevet i artikkel 17 nr. 3. Tilsynet omfatter, som nevnt ovenfor, både kvalifiserte og ikke-kvalifiserte tilbydere av tillitstjenester som er etablert i Norge.

4.3.1 Tilsyn med kvalifiserte tilbydere

Tilsyn med kvalifiserte tilbydere innebærer både forebyggende aktiviteter og kontroller i ettertid for å se til at tilbyderne og deres tjenester oppfyller forordningens krav (artikkel 17 nr. 3 bokstav a).

4.3.2 Tilsyn med ikke-kvalifiserte tilbydere

Når det gjelder ikke-kvalifiserte tilbydere fremgår det av forordningen (artikkel 17 nr. 3 bokstav b) at Nkom skal agere når myndigheten mottar opplysninger om at en ikke-kvalifisert tjenestetilbyder, eller en tillitstjeneste som den tilbyr, ikke oppfyller kravene i forordningen som gjelder ikke-kvalifiserte tilbydere.

5 Regler for samsvarsvurderingen

5.1 Samsvarsvurdering

Tilbydere av tillitstjenester som har til hensikt å levere kvalifiserte tillitstjenester skal melde om dette til Nkom i henhold til forordningen artikkel 21.
Tilbyderen må samtidig med meldingsskjema sende inn en samsvarsvurderingsrapport som er utført av et akkreditert samsvarsvurderingsorgan.

Nkom vil da sjekke at tilbyderen og tillitstjenestene som de tilbyr oppfyller kravene i forordningen. Kravene som stilles til de kvalifiserte tilbyderne av tillitstjenester fremgår av artikkel 24.

Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenummer for standarder for akkreditering av organer for samsvarsvurderinger, og for regler om samsvarsvurderinger (artikkel 20 nr. 4).

Når det gjelder samsvarsvurderinger vil det være hensiktsmessig å bruke europeisk standard ETSI EN 319 403 som går på generelle krav og policy-standarden ETSI EN 319 401.

5.2 Samsvarsvurderingsrapport

Tilbydere av tillitstjenester som vil ha status som kvalifiserte må levere en samsvarsvurderingsrapport sammen med meldingen til Nkom. Rapporten skal vise at både kravene til tilbyderen og deres tillitstjenester er i samsvar med lov om elektroniske tillitstjenester.

Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenummer for standarder for rapport om samsvarsvurderingen, men Kommisjonen har bestemt at disse ikke skal etableres på nåværende tidspunkt.

Samsvarsvurderingsrapporten vil være en viktig del av Nkom sin kontroll av om en tilbyder og dens tjenester er å anse som kvalifiserte. Det må derfor framgå av rapporten at kravene i forordningen er oppfylt og hvordan de skal etterleves.

I fravær av gjennomføringsrettsakt som pålegger bruk av bestemte standarder vil det være hensiktsmessig at rapporten om samsvarsvurdering minst inneholder informasjonen spesifisert i ETSI EN 319 403.

6 Krav til kvalifiserte tillitstjenester

6.1 Kvalifiserte sertifikater for elektronisk signaturer og segl

Artikkel 25 og 35 i forordningen angir hvilken rettslig virkning elektronisk signatur og et elektronisk segl har. Det følger av artikkel 26 og 36 hvilke krav som stilles for at en signatur og et segl ansees som avanserte.

En kvalifisert signatur eller segl, som definert i artikkel 2, er en avansert signatur eller segl basert på et kvalifisert sertifikat og opprettet ved hjelp av et signaturfremstillingsenhet. Artikkel 27 og 37 regulerer medlemslandenes forpliktelser til å godta elektroniske signaturer og segl fra andre medlemsland.

For at et sertifikat kan anses som kvalifisert, skal det være i samsvar med kravene i artikkel 28 og 38, og vedlegg 1 i forordningen. Sertifikatet skal ikke omfattes av flere krav enn det som fremgår av forordningen. Dersom et kvalifisert sertifikat sperres skal de anses som ugyldig fra det tidspunktet en forespørsel om sperring skjer. Statusen skal ikke kunne endres i ettertid, slik at sertifikatet igjen kan anses som gyldig.

Kommisjonen har utarbeidet en gjennomføringsrettsakt om formatet for avanserte elektroniske signaturer og segl[12].

Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenummer for standarder for kvalifiserte sertifikater som støtter elektroniske signaturer og segl.

I fravær av et vedtak om gjennomføringsrettsakter vil det være hensiktsmessig å bruke ETSI EN 319 411-1 og ETSI EN 319 411-2.

6.2 Kvalifisert valideringstjeneste

I artikkel 3 nr. 41 defineres validering som prosessen med å kontrollere og bekrefte at en elektroniske signatur eller et elektronisk segl, er gyldig.

I henhold til artikkel 32 i forordningen skal prosessen for validering av en kvalifisert elektronisk signatur bekrefte gyldigheten av en kvalifisert elektronisk signatur. Det forutsettes at sertifikatet som støtter signaturen på signeringstidspunktet, var et kvalifisert sertifikat for elektronisk signatur som oppfyller kravene i vedlegg 1 i forordningen.

[12] Kommisjonens gjennomføringsrettsakt (EU) 2015/1506 av 8. september 2015 om fastsettelse av spesifikasjoner vedrørende formater for avanserte elektroniske signaturer og avanserte segl, som skal anerkjennes i henhold til artikkel 27 nr. 5 og artikkel 37 nr. 5

Systemet som brukes for å validere den kvalifiserte elektroniske signaturen, skal gi tjenestebrukeren det riktige resultatet av valideringsprosessen. Systemet skal også gjøre det mulig for tjenestebrukeren å oppdage eventuelle problemer knyttet til sikkerheten.

Det følger av artikkel 33 at en kvalifisert valideringstjeneste for kvalifiserte elektroniske signaturer bare kan leveres av en kvalifisert tilbyder av tillitstjenester.

De som bruker tjenesten må kunne motta resultatet av valideringsprosessen på en automatisk måte som er pålitelig, effektiv og signert eller seglet av tilbyderen av den kvalifiserte valideringen tjenesten.

Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenummer for standarder for validering av kvalifiserte elektroniske signaturer, samt standarder for kvalifiserte valideringstjenester.

I fravær av et vedtak om gjennomføringsrettsakter vil det være hensiktsmessig å bruke ETSI EN 319 102-1.

6.3 Kvalifisert tjeneste for bevaring av kvalifiserte elektroniske signaturer

Det følger av artikkel 34 i forordningen at en kvalifisert tjeneste for bevaring av kvalifiserte elektroniske signaturer bare kan leveres av en kvalifisert tilbyder av tillitstjenester. Det må benyttes fremgangsmåter og teknologi som gjør det mulig å forlenge påliteligheten til den kvalifiserte elektroniske signaturen, utover den teknologiske gyldighet.

Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenummer for standarder for kvalifisert tjeneste for bevaring av kvalifiserte elektroniske signaturer.

I fravær av et vedtak om gjennomføringsrettsakter vil det være hensiktsmessig å bruke ETSI EN 319 521.

6.4 Kvalifiserte elektroniske tidsstempler

Ifølge forordningens artikkel 42 skal kvalifiserte elektroniske tidsstempler binde dato og tid til data på en slik måte at endringer kan oppdages. Tjeneste for tidsstempler skal basere seg på en riktig tidskilde som er koblet til koordinert universell tid (UTC). Tidsstemplet skal være signert med en avansert elektronisk signatur eller segl fra en kvalifisert tilbyder, eller alternativt gjennom en annen metode som gir tilsvarende beskyttelse.

Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenummer for standarder for å knytte dato og tidspunkt til data og for nøyaktige tidskilder.

I fravær av et vedtak om gjennomføringsrettsakt vil det være hensiktsmessig å bruke ETSI EN 319 421.

6.5 Kvalifiserte elektroniske tjenester for registrert sending

Ifølge artikkel 44 i forordningen skal kvalifiserte elektroniske tjenester for registrert sending tilbys av en kvalifiserte tilbydere av tillitstjenester. Kvalifiserte elektroniske tjenester for registrert sending skal med høy grad av pålitelighet sikre avsenderens identitet. De vil kontrollere adressatens identitet før dataene leveres. Forsendelse og mottak av data skal sikres gjennom en avansert elektronisk signatur eller segl fra en kvalifisert tilbyder på en måte som utelukker muligheten for at data endres uten at det er mulig å oppdage. Eventuelle endringer gjort i informasjonen som trengs for å sende eller motta dataene, skal tydelig fremgå for avsenderen og adressaten til dataene. Dato og klokkeslett for sending, mottak og eventuelle endringer i data, må spesifiseres gjennom et kvalifisert elektronisk tidsstempel.

Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenummer for standarder for sending og mottak av data.

I fravær av et vedtak om gjennomføringsrettsakt vil det være hensiktsmessig å bruke ETSI EN 319 511. Siden denne standarden er ennå ikke publisert kan ETSI TS 102 640-3 være en egnet standard å bruke.

6.6 Kvalifisert sertifikat for nettstedsautentisering

I henhold til artikkel 45 skal kvalifiserte sertifikater for nettstedsautentisering oppfylle kravene fastsatt i forordningens vedlegg IV.

Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenummer for standarder for kvalifiserte sertifikater for nettstedsautentisering.

I fravær av et vedtak om gjennomføringsrettsakt vil det være hensiktsmessig å bruke ETSI EN 319 411-1 og ETSI EN 319 411-2.

7 Krav til pålitelige IT-systemer og kvalifiserte enheter for signaturer og segl

eIDAS-forordningen stiller krav til at kvalifiserte tilbydere av tillitstjenester bruker pålitelige IT-systemer. For at en kvalifisert signatur eller segl skal kunne fremstilles kreves det at en sertifisert enhet brukes.

7.1 Pålitelige IT-systemer

En kvalifisert tilbyder som tilbyr kvalifiserte tillitstjenester skal bruke pålitelige systemer og produkter i deres virksomhet (artikkel 24 nr. 2 bokstav e og f).

Det finnes tilsvarende krav til pålitelige produkter i så kalt HSM (Hardware Security Module), som brukes til lagring eller generering av krypteringsnøkler i henhold til det tidligere gjeldende esignaturdirektivet.

Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette standarder for pålitelige systemer og produkter.

I fravær av et vedtak om gjennomføringsrettsakter vil det være hensiktsmessig å bruke ETSI EN 419 211, ETSI EN 419 221, ETSI EN 419 231 og ETSI EN 419 241.

7.2 Krav til kvalifiserte elektroniske signaturfremstillingssystemer

Kvalifiserte elektroniske signaturfremstillingssystemer skal oppfylle kravene fastsatt i vedlegg II, jf. forordningens artikkel 29.

Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette standarder for kvalifiserte elektroniske signaturfremstillingssystemer.

Kravene til de organene som skal sertifisere ordningen fremgår av artikkel 30. I Norge er det Nasjonal sikkerhetsmyndighet (NSM) v/SERTIT som vil kunne ha rollen som norsk sertifiseringsorgan, dersom det viser seg å være et behov, jf. Prop. 71 LS (2017-2018). Per i dag finnes det ikke noen sertifiseringsorgan i Norge. En tilbyder som ønsker å tilby kvalifisert elektronisk signatur, kan benytte seg av et signaturfremstillingssystem som er sertifisert av et sertifiseringsorgan i et annet medlemsland.

Kommisjonens gjennomføringsrettsakt om standarder for sikkerhetsvurdering av

IT-sikkerhetsprodukter ble vedtatt [13] og trådte i kraft 25. april 2016. Gjennomføringsrettsakten indikerer at per i dag ikke er noen standarder for systemer som tillater at krypteringsnøkler lagres eller genereres for serverbasert signering. I stedet henvises det til den alternative prosedyren i henhold til forordningens artikkel 30 nr. 3 bokstav b, som innebærer at et tilsvarende sikkerhetsnivå er nødvendig og at Kommisjonen skal bli informert om prosedyren.

Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 47 om fastsettelse av spesifikke kriterier som skal oppfylles av de utpekte sertifiseringsorganene som nevnt i artikkel 30 nr. 1.

Forordningens artikkel 31 fastsetter at medlemsstatene skal underrette Kommisjonen om signaturfremstillingssystemer sertifisert i medlemslandene. På grunnlag av meldinger skal Kommisjonen opprette en liste over sertifiserte systemer.

Av artikkel 39 følger det at tilsvarende krav for sertifisering gjelder også for kvalifiserte elektroniske seglfremstillingssystemer.

Gjennomføringsrettsakten inneholder standarder som skal anvendes for kvalifiserte systemer. Disse standardene er oppført i vedlegget til gjennomføringsrettsakten.

[13] Kommisjonens gjennomføringsrettsakt (EU) 2016/650 av 25. april 2016 om fastsettelse av standarder for sikkerhetsvurderinger av kvalifiserte signatur- og seglfremstillingssystemer i henhold til artikkel 30 nr. 3 og 39 nr. 2

8 Rapportering av sikkerhetshendelser

8.1 Generelt

I henhold til artikkel 19 skal både kvalifiserte og ikke-kvalifiserte tilbydere av tillitstjenester rapportere de sikkerhetshendelser eller tap av integritet som i betydelig grad påvirker den tillitstjenesten, eller personlig data, som brukes i tjenesten.

I tillegg skal tilbyderne underrette både fysiske og juridiske personer som hendelsen har hatt negativ innvirkning på. Som tilsynsmyndighet har Nkom en plikt til å gi et årlig sammendrag av rapporterte sikkerhetshendelser til EUs Byrå for nettverk og informasjonssikkerhet (ENISA).

I henhold til artikkel 19 nr. 4 har Kommisjonen rett til å vedta gjennomføringsrettsakter som fastsetter format og prosedyrer, med tidsfrister for rapportering av sikkerhetshendelser, men dette arbeidet er ikke planlagt på nåværende tidspunkt. Imidlertid har ENISA arbeidet med anbefalinger om rapportering av sikkerhetshendelser. Anbefalingene er rettet mot tilsynsmyndighetene og beskriver hvilke hendelser som tilsynsmyndigheten er pålagt å rapportere til ENISA.

De hendelser som er anbefalt fra ENISA[14] skal rapporteres til Nkom. Tilbydere må derfor i det minste rapportere de hendelser og de opplysninger som omfattes av avsnitt 3 i ENISA sin anbefaling.

Nkom har i skjema for varsel av sikkerhetshendelser[15] gitt veiledning for hvilke hendelser som skal rapporteres.

8.2 Hvilke sikkerhetshendelser skal varsles?

Alle sikkerhetshendelser som tilbyder av tillitstjenester vurderer til å ha betydelig påvirkning på tillitstjenester eller personopplysninger, skal varsles. Tilbydere av tillitstjenester skal kun rapportere sikkerhetshendelser som omfatter systemer eller prosesser som er under tilbyderens kontroll. I de tilfeller hvor kjernefunksjonalitet blir ivaretatt av en tredjepart, er tilbyderen av tillitstjenester ansvarlig for å varsle om sikkerhetshendelser som forekommer i tredjeparts systemer eller prosedyrer.

For å vurdere hvorvidt en sikkerhetshendelse har betydelig påvirkning på tillitstjenester eller

[14] Forslag til rammeverk for rapportering av sikkerhetshendelser jf. artikkel 19
[15] Varsel- sikkerhetshendelse innen tillitstjenester

personopplysninger, brukes skalaen som er vist i tabellen nedenfor. Sikkerhetshendelser som er av alvorlighetsgrad 3 eller høyere, skal varsles.

Alvorlighetsgrad og omfang:

1. Ingen påvirkning
2. Ubetydelig påvirkning: Tilbyders ressurser er berørt, men ingen påvirkning på tjenestene
3. Betydelig påvirkning: Mindre andel av kunder/tjenester er berørt
4. Stor påvirkning: Stor andel av kunder/tjenester er berørt
5. Katastrofe: Hele organisasjonen og alle kunder/tjenester er berørt

En sikkerhetshendelse som kun omfatter en enkelt kunde skal i utgangspunktet ikke varsles. Unntakene for dette er som følger:

- Dersom det oppstår et større antall enkelthendelser med utspring i, eller som kan relateres til samme årsak.
- Dersom sikkerhetshendelsen avdekker en sårbarhet som potensielt kan føre til at et større antall kunder kan bli berørt.
- Dersom hendelsen omfatter kunder med samfunnskritiske funksjoner eller andre tilbyderes tjenester.

Denne veiledningen er basert på ENISA sitt rammeverk for sikkerhetshendelser (se fotnote 14).

8.3 Rapportering til Nkom

Rapporter om sikkerhetshendelser sendes via e-skjema på Altinn.no[16]. Nkom vil bekrefte alle mottatte rapporter. Mer informasjon om hendelsesrapportering er tilgjengelig på Nkom sine nettsider[17].

[16] Varsel- sikkerhetshendelse innen tillitstjenester
[17] https://www.nkom.no/teknisk/tillitstjenester/eidas/rapportering-av-sikkerhetshendelser

9 Opphør av virksomheten

Forordningen inneholder også krav til hva en kvalifisert tilbyder av tillitstjenester bør gjøre hvis de ønsker at virksomheten skal opphøre.

9.1 Informasjon til Nkom

En tilbyder er pålagt å informere Nkom om eventuelle endringer i driften av de kvalifiserte tillitstjenester, eller om tilbyderen ønsker å avslutte virksomheten.

Allerede ved oppstarten av virksomheten skal tilbyderen presentere en plan for virksomhetens opphør til Nkom for å få status som kvalifisert.
Reglene om opphør av virksomhet skal sikre kontinuiteten av kvalifiserte tillitstjenester. Derfor gjelder forpliktelser for de kvalifiserte tilbyderne i relativt lang tid etter den kvalifiserte tillitstjenesten har opphørt. Den som ønsker å bli kvalifisert tilbyder av tillitstjenester må derfor allerede ved oppstarten av tjenesten ha en langsiktig plan og ressurser for det tilfellet at virksomheten skulle opphøre.

9.2 Oppbevaring av informasjon

Artikkel 24 nr. 2 h i eIDAS-forordningen sier at en kvalifisert tilbyder av tillitstjenester skal registrere og holde tilgjengelig all relevant informasjon som den har produsert eller tatt imot i en passende tidsperiode. Artikkelen sier videre at registreringen av opplysningene kan gjøres elektronisk.

Relevant informasjon som nevnt ovenfor kan være avtaler og dokumentasjon som ligger til grunn for hver enkelt utstedelse av et sertifikat. Det er viktig at slik informasjon blir bevart fordi det kan oppstå juridiske spørsmål om man kan bevise at en kvalifisert elektronisk signatur eller segl har vært gyldig tilbake i tid. Det kan også tenkes at det stilles spørsmål ved hvordan en person ble identifisert da et sertifikat ble utstedt av tilbyderen.

På bakgrunn av dette, samt hensyn til den generelle begrensningsperiode i norsk lov, anses det som rimelig å bevare de aktuelle opplysningene i minst ti år fra gyldighetsdatoen til sertifikatet.

9.3 Offentliggjøre tilbakekalling av sertifikater og informere berørte parter

Det fremgår av artikkel 24 nr. 3 i eIDAS-forordningen at dersom en kvalifisert tilbyder av kvalifiserte sertifikater bestemmer seg for å tilbakekalle et sertifikat, skal tilbakekallingen

registreres i tilbyderens sertifikatdatabase og offentliggjøres. Artikkelen sier at dette skal skje i god tid, og innen 24 timer, etter at avgjørelsen om tilbakekallingen ble gjort.

Det følger også av artikkel 24 nr. 4 at en kvalifisert tilbyder i slike situasjoner skal informere eventuelle berørte parter om at de kvalifiserte sertifikater har status som opphevet.

Videre skal informasjonen gjøres tilgjengelig på en automatisert måte som er pålitelig, gratis og effektiv, jf. artikkel nr. 24 nr. 4. Informasjonen bør holdes tilgjengelig til det utstedte sertifikatet er utløpt.

10 Vedlegg

10.1 Vedlegg 1 - Vedtatte gjennomføringsrettsakter for tillitstjenester

Gjennomføringsrettsakt (EU) 2015/806	Artikkel 23 nr. 3	Kommisjonens gjennomføringsrettsakt (EU) 2015/806 av 22. mai 2015 om fastsettelse av spesifikasjoner vedrørende EU-tillitsmerke for kvalifiserte tillitstjenester
Gjennomføringsrettsakt (EU) 2015/1505	Artikkel 22 nr. 5	Kommisjonens gjennomføringsrettsakt (EU) 2015 av 8. september 2015 om fastsettelse av tekniske spesifikasjoner og formater vedrørende tillitslister i henhold til artikkel 22 nr. 5
Gjennomføringsrettsakt (EU) 2015/1506	Artikkel 27 nr. 5 Artikkel 37 nr. 5	Kommisjonens gjennomføringsrettsakt (EU) 2015/1506 av 8. september 2015 om fastsettelse av spesifikasjoner vedrørende formater for avanserte elektroniske signaturer og avanserte segl, som skal anerkjennes i henhold til artikkel 27 nr. 5 og artikkel 37 nr. 5
Gjennomføringsrettsakt (EU) 2016/650	Artikkel 30 nr. 3 Artikkel 39 nr. 2	Kommisjonens gjennomføringsrettsakt (EU) 2016/650 av 25. april 2016 om fastsettelse av standarder for sikkerhetsvurderinger av kvalifiserte signatur- og seglfremstillingssystemer i henhold til artikkel 30 nr. 3 og 39 nr. 2