

Vedlegg til skjema for melding om kvalifisert tillitstjeneste – Kvalifisert sertifikat for nettstedsautentisering

Navnet på tilbyder av kvalifisert tillitstjeneste:
Kontaktperson (navn, e-post):
Dato:

Utfyllt vedlegg sammen med skjema for melding om kvalifisert tillitstjeneste sendes til: firmapost@nkom.no

Informasjon om samsvarsvurdering

| | |
|---|--|
| Navn på samsvarsvurderingsorgan | |
| Navn og dato på sertifikat utstedt av samsvarsvurderingsorgan | |
| Navn og dato på rapport utstedt av samsvarsvurderingsorgan | |

Informasjon om avvik

| | | |
|---|--|--|
| Totalt antall: (0-x) | Antall vesentlige avvik: (0-x) Antall mindre avvik: (0-x) | Overordnet beskrivelse av avvik avdekket av samsvarsvurderingsorgan med henvisning til relevant eIDAS-artikkel |
| Er tilbyder av tillitstjenesten kjent med andre avvik som ikke fremkommer i rapport fra samsvarsvurderingsorganet | | (ja/nei) Hvis ja, kort beskrivelse av avvik med henvisning til korrekt eIDAS-artikkel |
| Merknader til eventuelle avvik | | |

Generelle krav til kvalifiserte tilbydere av tillitstjenester – dokumentasjon

| eIDAS-artikkel | Kravbeskrivelse | Relevant standard | Relevante kapitler i policy/praksis, andre dokumenter med eventuelle merknader | Avvik (Ja/nei) | Inngående beskrivelse av hvert enkelt avvik, inkludert beskrivelse av planlagte tiltak og tidsaspekt for å lukke avviket |
|----------------|--|--|--|----------------|--|
| 5.1 | Personopplysninger skal behandles i samsvar med direktiv 95/46/EF. | EN 319 401, 7.13 (REQ 2, 5) | | | |
| 13.1 | Med forbehold for nr. 2 skal tilbydere av kvalifiserte tillitstjenester være ansvarlig for skader som forsettlig eller uaktsomt påføres en fysisk eller juridisk person på grunn av manglende overholdelse av forpliktelsene i denne forordningen. Bevisbyrden for at en ikke-kvalifisert tilbyder av tillitstjenester har handlet forsettlig eller uaktsomt, påvirker den fysiske eller juridiske personen som hevder å ha lidd skadene nevnt i første ledd. En kvalifiserte tilbyder av tillitstjenester formodes å ha handlet forsettlig eller uaktsomt, med mindre vedkommende beviser at skaden nevnt i første ledd oppsto uten at vedkommende har handlet forsettlig eller uaktsomt. | EN 319 401, 6.2 (alle REQ) 7.1.1 (REQ 1-5) | | | |
| 13.2 | Når tilbydere av tillitstjenester på behørig vis underretter sine kunder på forhånd om begrensningene som gjelder for bruken av tjenestene de leverer, og når begrensningene er | EN 319 401, 6.2 (alle REQ) 7.1.1 (REQ 6) | | | |

| | | | | | |
|------|---|--|--|--|--|
| | mulig å gjenkjenne for tredjepart, skal tilbydere av tillitstjenester ikke være ansvarlig for skader som oppstår ved slik bruk av tjenester som overskrider de angitte begrensningene. | | | | |
| 13.3 | Punkt 13.1 og 13.2 får anvendelse i samsvar med nasjonale regler for erstatningsansvar. | EN 319 401, 7.1.1 (REQ 4) | | | |
| 15 | Når det er mulig, skal tillitstjenester og sluttbrugerprodukter som benyttes ved levering av slik tjenester, gjøres tilgjengelige for personer med nedsatt funksjonsevne. | EN 319 401, 7.13 (REQ 2, 3, 4) EN 319 411-1, 6.9.3 (OVR 1) EN 319 411-2, 6.9.3 (OVR 1) | | | |
| 19.1 | Kvalifiserte og ikke-kvalifiserte tilbydere av tillitstjenester skal treffe egnede tekniske og organisatoriske tiltak for å håndtere sikkerhetsrisikoer i forbindelse med tillitstjenestene de leverer. Idet det tas hensyn til den siste teknologiske utviklingen, skal nevnte tiltak sikre at sikkerhetsnivået står i forhold til graden av risiko. Det skal særlig treffes tiltak for å forebygge og minimere virkningen av sikkerhetshendelser samt for å underrette berørte parter om skadevirkningene av slike hendelser. | EN 319 401, 5 (alle REQ) 6. 3 (alle REQ) 7 (alle REQ) EN 319 411-1, 6.4, (alle REQ) 6.5 (alle REQ unntatt 6.5.8) EN 319 411-2, 6.4 (alle OVR) 6.5 (alle OVR, unntatt 6.5.8) | | | |

| | | | | | |
|---------------------|--|---|--|--|--|
| 19.2 | Kvalifiserte og ikke-kvalifiserte tilbydere av tillitstjenester skal så snart som mulig og senest 24 timer etter å ha fått kjennskap til sikkerhetsbrudd eller tap av integritet som i betydelig grad påvirker tillitstjenesten eller personopplysninger som oppbevares i forbindelse med levering av tjenesten, underrette tilsynsorganet og eventuelt andre berørte organer, for eksempel vedkommende nasjonale organ for informasjonssikkerhet eller personvernmyndighet. | EN 319 401, 7.9 (alle REQ) 7.11 (alle REQ) EN 319 411-1, 6.4.8 (OVR 11, 5) EN 319 411-2, 6.4.8 (OVR 1) | | | |
| 24.2 24.2 a) | En kvalifisert tilbyder av tillitstjenester som tilbyr kvalifiserte tillitstjenester, skal: - underrette tilsynsorganet om eventuelle endringer i leveringen av sine kvalifiserte tillitstjenester, og om en eventuell hensikt om å innstille denne virksomheten; | EN 319 401, 6.1 (alle REQ) 7.12 (REQ 3) EN 319 411-1, 5.2 (alle OVR) EN 319 411-2, 5.2 (OVR 1) | | | |
| 24.2 b) | - ha personale og eventuelt underleverandører med den nødvendige sakkunnskap, pålitelighet, erfaring og kvalifikasjoner som har fått egnet opplæring med hensyn til sikkerhet og regler for vern av personopplysninger, og skal anvende administrative og forvaltningsmessige fremgangsmåter som er i samsvar med | EN 319 401, 7.1 (alle REQ) 7.2 (REQ 1, 2, 3, 13) EN 319 411-1, 6.4.4 (OVR 1), 6.9.1 (alle OVR) | | | |

| | | | | | |
|---------|--|--|--|--|--|
| | europæiske og internasjonale standarder; | EN 319 411-2, 6.4.4 (OVR 1) 6.9.1 (OVR 1) | | | |
| 24.2 c) | - når det gjelder risikoen for erstatningsansvar, jf. artikkel 13, ha tilstrekkelige økonomiske midler og/eller tegne en egnet ansvarsforsikring i samsvar med nasjonal lovgivning; | EN 319 401, 7.1.1 (REQ 4) EN 319 411-1, 6.8.2 (OVR 1) EN310 411-2, 6.8.2 (OVR 1) | | | |
| 24.2 d) | - før inngåelse av et kontraktsforhold, på en tydelig og forståelig måte opplyse enhver person som ønsker å benytte en kvalifisert tillitstjeneste, om de nøyaktige vilkårene for bruk av denne tjenesten, herunder eventuelle bruksbegrensninger; | EN 319 401, 6.2 (alle REQ) EN 319 411-1, 6.1 (DIS 4-9) 6.3.4 (OVR 1-6) 6.9.4(OVR 1-3) EN 319 411-2, 6.1 (OVR 1) 6.3.4 (alle OVR) 6.9.4 (alle OVR) | | | |
| 24.2 e) | - benytte pålitelige systemer og produkter som er beskyttet mot endringer, og sikre den tekniske sikkerheten og påliteligheten i de prosessene som støttes av disse; | EN 319 401, 7.4 (REQ 1-3) 7.5 (REQ 1) 7.7 (alle REQ) 7.8 (alle REQ) EN 319 411-1, 6.5 (OVR 1-7) | | | |

| | | | | | |
|---------|---|---|--|--|--|
| | | EN 319 411-2, 6.5 | | | |
| 24.2 f) | - benytte pålitelige systemer til lagring av dataene den mottar, i en kontrollerbar form slik at: (i) de er offentlig tilgjengelige bare dersom det er innhentet samtykke fra personen som dataene gjelder, (ii) bare autoriserte personer kan legge inn opplysninger og gjøre endringer i de lagrede dataene, (iii) dataenes ekthet kan kontrolleres; | EN 319 401, 7.5 (alle REQ) 7.7 (alle REQ) 7.8 (alle REQ) EN 319 411-1, 6.4.3 (OVR 1, GEN 2-3) 6.4.6 (OVR 1) 6.5 (alle, unntatt 6.5.8) EN 319 411-2, 6.4.3 (OVR 1) 6.4.6 (OVR 1) 6.5 (alle, unntatt 6.5.8) | | | |
| 24.2 g) | - treffe egnede tiltak mot forfalskning og tyveri av data; | EN 319 401, 5 (alle REQ) 6.3 (alle REQ) 7.3-7.12 (alle REQ) EN 319 411-1, 6.4 (alle, unntatt 6.4.7) 6.5 (alle, unntatt 6.5.8) | | | |

| | | | | | |
|---------|--|---|--|--|--|
| | | EN 319 411-2, 6.4 (alle, unntatt 6.4.7) 6.5 (alle, unntatt 6.5.8) | | | |
| 24.2 h) | - registrere alle relevante opplysninger om data som den kvalifiserte tilbyderen av tillitstjenester har utstedt og mottatt, og sørge for at de er tilgjengelige i et rimelig tidsrom, herunder etter at virksomheten til den kvalifiserte tilbyderen av tillitstjenester er innstilt, særlig for å kunne framlegge bevis i forbindelse med rettergang og sikre kontinuitet i tjenesten. Slik registrering kan gjøres elektronisk; | EN 319 401, 7.12 (alle REQ) EN 319 411-1, 6.2.2 (REG 18, 19 eller 20) 6.3.4 (REG 7, 8,17) 6.3.8 (REQ 2) 6.4.5 (REQ 4) 6.4.6(REQ 1) 6.4.9 (alle REQ) EN 319 411-2, 6.2.2 (REG 1) 6.3.4 (OVR 1) 6.3.8 (REG 1) 6.4.5 (alle OVR) 6.4.6 (OVR 1) 6.4.9 (OVR 1) | | | |
| 24.2 i) | - ha en ajourført plan for opphør av virksomhet for å sikre kontinuitet i tjenesten i samsvar med bestemmelsene kontrollert av tilsynsorganet i samsvar med artikkel 17 nr. 4 bokstav i; | EN 319 401, 7.12 (alle REQ) EN 319 411-1, 6.4.9 (alle OVR) | | | |

| | | | | | |
|---------|--|---|--|--|--|
| | | EN 319 411-2, 6.4.9 (OVR 1) | | | |
| 24.2 j) | - sikre rettmessig behandling av personopplysninger i samsvar med direktiv 95/46/EF; | EN 319 401, 7.13 (REQ 2, 5) EN 319 411-1, 6.8.4 (alle OVR) EN 319 411-2, 6.8.4 (OVR 1) | | | |

Krav til kvalifiserte sertifikater for nettstedsautentisering – dokumentasjon

| eIDAS-artikkel | Kravbeskrivelse | Relevant standard | Relevante kapitler i policy/praksis, andre dokumenter med eventuelle merknader | Avvik (Ja/nei) | Inngående beskrivelse av hvert enkelt avvik, inkludert beskrivelse av planlagte tiltak og tidsaspekt for å lukke avviket |
|----------------|--|---|--|----------------|--|
| 24.1 | Når en kvalifiserte tilbyder av tillitstjenester utsteder et kvalifisert sertifikat for en tillitstjeneste, skal vedkommende ved hjelp av egnede midler og i samsvar med nasjonal lovgivning kontrollere identiteten til og, dersom det er relevant, eventuelle særlige egenskaper ved den fysiske eller juridiske personen som den kvalifiserte sertifikatet utstedes til. Opplysningene i første ledd skal kontrolleres av den kvalifiserte tilbyderen av tillitstjenester enten direkte eller via en tredje part i samsvar med nasjonal lovgivning: | EN 319 401, punkt 7.2 EN 319 411-1, punkt 6.2.2, 6.2.3 EN 319 411-2, punkt 6.2.2, 6.2.3 | | | |
| 24.1 a) | - ved fysisk tilstedeværelse av den fysiske personen eller en godkjent representant for den juridiske personen eller; | | | | |
| 24.1 b) | - uten fysisk tilstedeværelse ved bruk av elektroniske identifikasjonsmidler, der det før utstedelsen av det kvalifiserte sertifikatet var sikret fysisk tilstedeværelse av den fysiske | EN 319 411-1, 6.2.2 (alle REG) 6.2.3 (REG 1) | | | |

| | | | | | |
|---------|---|--|--|--|--|
| | personen eller en godkjent representant for den juridiske personen, og som oppfyller kravene fastsatt i artikkel 8 med hensyn til sikkerhetsnivåene «betydelig» eller «høyt» eller; | EN 319 411-2, 6.2.2 (alle REG) 6.2.3 (alle REG) | | | |
| 24.1 c) | - ved hjelp av et sertifikat for en kvalifisert elektronisk signatur eller et kvalifisert elektronisk segl utstedt i samsvar med bokstav a) eller b) eller; | EN 319 411-1, 6.2.2 (alle REG) 6.2.3 (alle REG) EN 319 411-2, 6.2.2 (alle REG) 6.2.3 (alle REG) | | | |
| 24.1 d) | - ved bruk av andre identifikasjonsmetoder anerkjent på nasjonalt plan som garanterer pålitelighet som tilsvarer fysisk tilstedeværelse. Et samsvarvurderingsorgan skal bekrefte at garantiene er likeverdige. | EN 319 411-1, 6.2.2 (alle REG) 6.2.3 (alle REG) EN 319 411-2 6.2.2 (alle REQ) 6.2.3 (alle REG) | | | |
| 24.2 | En kvalifiserte tilbyder av tillitstjenester skal: | EN 319 411-1, 6.1 (alle DIS) | | | |
| 24.2 k) | - dersom kvalifiserte tilbydere av tillitstjenester utsteder sertifikater, etablere og oppdatere en sertifikatdatabase. | EN 319 411-2, 6.1 (OVR 1) | | | |
| 24.3 | Dersom en kvalifisert tilbyder av tillitstjenester som utsteder kvalifiserte sertifikater, beslutter å tilbakekalle et sertifikat, skal den registrere tilbakekallingen i sin sertifikatdatabase og offentliggjøre sertifikatets status som | EN 319 411-1, 6.2.4 (alle REV) 6.3.9 (alle REV og CSS) EN 319 411-2, 6.2.4, (REV 1) | | | |

| | | | | | |
|---------------|--|--|--|--|--|
| | tilbakekalt i god tid, og i alle tilfeller innen 24 timer etter mottak av anmodningen. Tilbakekallingen skal tre i kraft umiddelbart etter at den er offentliggjort. | 6.3.9 (REV 1) | | | |
| 24.4 | Med hensyn til artikkel 24 nr. 3 skal kvalifiserte tilbydere av tillitstjenester som utsteder kvalifiserte sertifikater, informere eventuelle tjenestebrukere om gyldigheten av eller status som tilbakekalt for kvalifiserte sertifikater som er utstedt av dem. Slike opplysninger skal minst gjøres tilgjengelig for hvert enkelt sertifikat, når som helst og utover sertifikatets gyldighetsperiode på en automatisert måte som er pålitelig, gratis og effektiv. | EN 319 411-1, 6.3.10 (alle CSS) EN 319 411-2, 6.3.10 (alle CSS) | | | |
| 45.1 | Kvalifiserte sertifikater for nettstedsautentisering skal oppfylle kravene fastsatt i vedlegg IV. | | | | |
| Vedlegg IV | Kvalifiserte sertifikater for nettstedsautentisering skal inneholde: | EN 319 411-1, 6.6.1 (alle GEN) | | | |
| Vedlegg IV a) | - en angivelse, som minst er i en form som er egnet for automatisert behandling, om at sertifikatet er utstedt som et kvalifisert sertifikat for nettstedsautentisering; | EN 319 411-2, 6.6.1 (GEN 1, 2) EN 319 412-5, 4.2.1, 4.2.3 | | | |
| Vedlegg IV b) | - et datasett som på en utvetydig måte representerer den kvalifiserte tilbyderen av tillitstjenester som utsteder de kvalifiserte sertifikatene, som minst | EN 319 411-1, 6.6.1 (alle GEN) | | | |

| | | | | | |
|---------------|--|--|--|--|--|
| | <p>inneholder opplysninger om hvilken medlemsstat tjenestetilbyderen er etablert i, og:</p> <ul style="list-style-type: none"> - for en juridisk person: navn og når det er relevant, registreringsnummer oppført i offisielle registre - for en fysisk person: personens navn; | <p>EN 319 411-2, 6.6.1 (GEN 1, 2)</p> <p>EN 319 412-2, 4.2.3</p> <p>CABForum BR, 7.1.4.1</p> | | | |
| Vedlegg IV c) | <ul style="list-style-type: none"> - for fysiske personer: minst navnet på personen som sertifikatet er utstedt til, eller et pseudonym, der pseudonymet er tydelig angitt dersom et slikt brukes, - for juridiske personer: minst navnet på den juridiske personen som sertifikatet er utstedt til, og eventuelt registreringsnummeret oppført i offisielle registre; | <p>EN 319 411-1, 6.6.1 (alle GEN)</p> <p>EN 319 411-2, 6.6.1 (GEN 1, 2)</p> <p>CABForum BR, 7.1.4.2.2</p> <p>CABForum EV, 9.2.1</p> | | | |
| Vedlegg IV d) | <ul style="list-style-type: none"> - adresseopplysninger, herunder minst opplysninger om by og stat, til den fysiske eller juridiske personen som sertifikatet er utstedt til, og eventuelt som angitt i offisielle registre; | <p>EN 319 411-1, 6.6.1 (alle GEN)</p> <p>EN 319 411-2, 6.6.1 (GEN 1,2)</p> <p>EN 319 412-2, 4.3.11, 4.4.1, 4.2.5</p> <p>CABForum BR, 7.1.4.2.2</p> | | | |

| | | | | | |
|------------------|--|---|--|--|--|
| | | CABForum EV, 9.2.5, 9.2.7 | | | |
| Vedlegg IV e) | - domenenavnet eller -navnene som drives av den fysiske eller juridiske personen som sertifikatet er utstedt til; | EN 319 411-1, 6.6.1 (alle GEN) EN 319 411-2, 6.6.1 (GEN 1,2) CABForum BR, 7.1.4.2.1 CABForum EV, 9.2.2 | | | |
| Vedlegg IV f) | - opplysninger om når sertifikatets gyldighetsperiode starter og utløper; | EN 319 411-1, 6.6.1 (alle GEN) EN 319 411-2, 6.6.1 (GEN 1,2) RFC 5280 | | | |
| Vedlegg IV g) | - sertifikatets identifikasjonskode, som må være entydig for den kvalifiserte tilbyderen av tillitstjenester; | EN 319 411-1, 6.6.1 (alle GEN) EN 319 411-2, 6.6.1 (GEN 1,2) EN 319 412-4 RFC 5280 | | | |
| Vedlegg IV h) | - den avanserte elektroniske signaturen eller det avanserte elektroniske seglet til den utstedende kvalifiserte tilbyderen | EN 319 411-1, 6.6.1 (alle GEN) | | | |

| | | | | | |
|---------------|---|--|--|--|--|
| | av tillitstjenester; | EN 319 411-2, 6.6.1 (GEN 1,2) RFC 5280 | | | |
| Vedlegg IV i) | - opplysninger om hvor sertifikatet som støtter den avanserte elektroniske signaturen eller det avanserte elektroniske seglet nevnt i bokstav h), er gratis tilgjengelig; | EN 319 411-1, 6.6.1 (alle GEN) EN 319 411-2, 6.6.1 (GEN 1,2) CABForum BR, 7.1.2.3 c) RFC 5280 | | | |
| Vedlegg IV j) | - opplysninger om hvor tjenestene som Kan brukes for å få kjennskap til det kvalifiserte sertifikatets gyldighetsstatus, befinner seg. | EN 319 411-1, 6.6.1(alle GEN) EN 319 411-2, 6.6.1 (GEN 3) CABForum BR, 7.1.2.3 b) og c) CABForum EV, 9.7 4) RFC 5280 | | | |