Nasjonal kommunikasjons-myndighet

Postboks 93
4791 Lillesand
www.nkom.no

Telefon: 22 82 46 00
Telefaks: 22 82 46 40
E-post: firmapost@nkom.no

Registreringsskjema for sertifikatklasse "Person-Høyt"

Jf. forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere 21. november 2005 nr. 1296.

Bruk eget vedlegg ved eventuell plassmangel i skjemafeltene. Utfylt skjema sendes:

*Per post til **Nasjonal kommunikasjonsmyndighet, Postboks 93, 4791 Lillesand**, per faks til **22 82 46 40** eller via e-post til **firmapost@nkom.no***

Registreringsskjemaet blir i sin helhet publisert på www.nkom.no. Beskrivelser av oppfyllelse av krav som er taushetsbelagt eller forretningsmessige opplysninger av sensitiv art, må derfor sendes i eget vedlegg.

OPPLYSNINGER OM LEVERANDØREN/SERTIFIKATUTSTEDER	
Leverandørens/sertifikatutstederens navn	Organisasjonsnummer
Postadresse	Telefon
Postnr/poststed	Telefaks
Land	E-post
Besøksadresse	E-post til kontaktperson
Kontaktperson	Telefon til kontaktperson
Navn på sertifikatutsteder	Dato og sted for registrering som utsteder av kvalifiserte sertifikater
Navn på sertifikatutsteder (dersom flere utstedere)	Dato og sted for registrering som utsteder av kvalifiserte sertifikater

VIKTIG INFORMASJON OM SKJEMAET

- Begrepet ”sertifikatutsteder” brukes heretter slik begrepet forstås i esignaturloven § 3 nr. 10 og omfatter også de som tilbyr andre tjenester relatert til elektronisk signatur, f.eks. PKI-leverandøren hvor sertifikatutsteder som utsteder og signerer sertifikatene er en underleverandør. ”Sertifikatutsteder” omfatter altså både begrepene ”Leverandør” og Sertifikatutsteder” slik disse begrepene er definert i ”Kravspesifikasjon for PKI i offentlig sektor” punkt 2.2.
- Når en sertifikatutsteder selvdeklarerer seg til Nasjonal kommunikasjonsmyndighet ved å fylle ut dette skjemaet, innebærer det at sertifikatutsteder erklærer overfor norske myndigheter at utstederen oppfyller kravene i den til enhver tid gjeldende versjon av ”Kravspesifikasjon for PKI i offentlig sektor”.
- Sertifikatutstederen skal oppføres på tilsynets liste over utstedere av ”Person-Høyt” sertifikater dersom kravene i forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere 21. november 2005 nr. 1296 (forskriften) § 11 er oppfylt.
- Nasjonal kommunikasjonsmyndighet vil varsle registrerte sertifikatutstedere om relevante endringer i kravspesifikasjonen for sertifikater i klassen ”Person-Høyt”. Tilsynet vil oppgi en tidsfrist på minimum 6 måneder for oppfyllelse av endrede krav og hvordan oppfyllelse av kravene eventuelt skal dokumenteres. Dersom dokumentasjon ikke er sendt innen fristen, kan sertifikatutstederen fjernes fra den publiserte listen i henhold til kravene i forskriften § 11 tredje ledd.
- Bruk av dette skjemaet for selvdeklarering er obligatorisk.
- Sertifikatutstederen skal i dette skjemaet angi hvilke tjenester som tilbys og i den sammenheng positivt angi hvilke relevante A-krav som oppfylles. Utstederen kan unnlate å oppfylle A-krav som ikke er relevante for de tjenestene som tilbys.
- Endringer i registrerte opplysninger eller forhold som påvirker opplysningene skal meldes til Nasjonal kommunikasjonsmyndighet uten ugrunnet opphold, jf. forskriften § 8.
- Utfylt skjema **vil bli publisert** på Nasjonal kommunikasjonsmyndighets hjemmeside ***www.nkom.no***. Forretningsmessige opplysninger av sensitiv art eller taushetsbelagte opplysninger må derfor oppgis i vedlegg der det spesifiseres hvilket krav det er relatert til.
- Der skjemaet ikke gir tilstrekkelig plass brukes vedlegg.

SERTIFIKATPOLICY

Sertifikatutstederens sertifikatpolicy skal vedlegges. Utstederen skal også oppi en nettadresse for hvor sertifikatpolicyen og andre relevante dokumenter finnes.
Sertifikatpolicy skal være en angivelse av sikkerhetsnivået for tjenesten og inneholde informasjon om hvordan sertifikatene skal
utstedes og behandles, og hvem som har ansvaret for sikkerheten knyttet til dette.

SERTIFIKATUTSTEDELSESPRAKSIS

Beskrivelse av sertifikatutstederens sertifikatpraksis skal vedlegges.
Sertifikatpraksis skal gi en beskrivelse av organisering og prosedyrer som utstederen og andre i dennes tjeneste benytter i forbindelse med utstedelse og administrasjon av sertifikater.

ANNEN INFORMASJON

I tillegg til overnevnte informasjon skal sertifikatutsteder, i forbindelse med denne registreringen eller så snart som mulig, gi Nasjonal kommunikasjonsmyndighet informasjon om:

- **Rutiner for IT-revisjon**

  Generell IT kontroll i selskapet, IT baserte brukersystemer som benyttes i fremstilling av sertifikater og registreringsrutiner.

  Valgt IT-revisor og tidspunkt for siste revisjon.

- **Rutiner for lagring av relevante opplysninger om kvalifiserte sertifikater**
- **Vilkår, begrensninger og lignende i kundeavtale,** kopi av kundeavtale bør vedlegges.
- **Eventuelle sertifiseringer selskapet innehar**

NASJONAL KOMMUNIKASJONSMYNDIGHETS HJEMMESIDER

Nasjonal kommunikasjonsmyndighet vil publisere oppdatert informasjon om utstedelse av sertifikater iht. "Kravspesifikasjon for PKI i offentlig sektor" på adressen ***www.nkom.no***

Ønsker sertifikatutsteder å stå oppført med en link til egne web-sider på Nasjonal kommunikasjonsmyndighets hjemmeside (kryss av): **Ja** **Nei**

Hvis ja, fyll inn korrekt adresse:

TJENESTER SERTIFIKATUTSTEDEREN TILBYR

Sertifikatutstederen skal nedenfor krysse av for hvilke sikkerhetsprodukter og – tjenester utstederen tilbyr. Sertifikatutstederen må oppfylle alle A-krav i kravspesifikasjonen som er relevante for de aktuelle sikkerhetsprodukter og – tjenester som utstederen tilbyr.

AUTENTISERING	
SIGNERING	
MELDINGSKRYPTERING	

OPPFYLLELSE AV KRAVSPESIFIKASJON FOR PKI I OFFENTLIG SEKTOR VERSJON 2.0

Sertifikatutstederen skal oppfylle **alle A-krav til basis sertifikattjenester** og **alle A-krav til katalog- og oppslagstjenester i kravspesifikasjonen**. Utstederen skal oppfylle **alle A-krav i kravspesifikasjonen som er relevante** for de aktuelle sikkerhetsprodukter og –tjenester som utstederen tilbyr. Sertifikatutstederen skal i feltene under opplyse om oppfyllelse av A-kravene som er relevante for utstederens produkter og tjenester. En nærmere begrunnelse for hvorfor kravene ikke er relevante kan følge i vedlegg. Nasjonal kommunikasjonsmyndighet kan veilede utstederne i forhold til hvilke krav som er relevante krav. Se informasjonen på Nkoms hjemmeside eller ta kontakt med Nkom på firmapost@nkom.no merket "sertifikatklasse Person-Høyt".

A-KRAV TIL BASIS SERTIFIKATTJENESTER - må oppfylles av alle sertifikatutstedere

Krav nr.	Kravbeskrivelse	Oppfyller Ja/Nei	Dokumentasjon og henvisning til kapittel i CP/CPS	Merknad
4.1.1.1	**Sertifikat med bruksområde autentisering** eID skal inneholde sertifikat og nøkkelpar med formål autentisering (key usage "digital signature").			
4.1.1.2	**Sertifikat med bruksområde elektronisk signatur** eID skal inneholde sertifikat og nøkkelpar med formål elektronisk signatur (key usage "content commitment", tidligere navn "non-repudiation").			
4.1.1.4	**Antall sertifikater og kombinering av bruksområder** Sertifikatutsteder skal oppgi hvor mange sertifikater og nøkkelpar som inngår i en eID. Dersom forskjellige bruksområder kombineres i samme sertifikat/nøkkelpar skal dette oppgis.			
4.1.1.8	**Sertifikatprofil i henhold til SEID [10]** Alle sertifikater skal være i henhold til "Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater" [10]. Følgende avvik fra SEID sertifikatprofil tillates: For personsertifikater til personer *som ikke er registrert i Folkeregisteret*, er det ikke krav om kopling mot fødselsnummer eller D-nummer. For virksomhetssertifikater til virksomheter *som ikke er registrert i Norge*, er det ikke krav om kopling til Enhetsregisteret. Dersom disse avvikene påberopes, skal navngiving i "Subject" feltet, og spesielt bruken av "serialNumber" attributtet i "Subject", spesifiseres for disse tilfellene. Eventuelle felter, attributter og utvidelser (extensions), som er med i sertifikatet, men ikke er spesifisert i [10], skal spesifiseres.			
4.1.1.9	**Tegnsett for navn i sertifikater** Navn i sertifikater (utstedernavn og navn for sertifikatinnehaver) skal kodes med UTF-8 tegnsett [i].			
4.1.1.10	**Begrensninger knyttet til sertifikatinnehaver** Eventuelle restriksjoner (eksempelvis alder eller oppføring i Folkeregisteret) knyttet til hvem som kan være sertifikatinnehaver, skal beskrives.			

4.1.1.11	**Begrensninger i sertifikatenes anvendelsesområde** Eventuelle restriksjoner på anvendelse av sertifikater, og spesielt betingelser knyttet til hvem som kan være sertifikatmottaker, skal beskrives.			
4.1.2.1	**Registrering som utsteder av kvalifiserte sertifikater** Før en sertifikatutsteder kan selvdeklareres for Person-Høyt etter forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere [12], skal det dokumenteres at utstederen er registrert som utsteder av kvalifiserte sertifikater etter esignaturloven [2] § 18, eller at registermelding for utstedelse av kvalifiserte sertifikater er sendt.			
4.1.2.2	**Kvalifiserte sertifikater** Det skal oppgis hvilke sertifikater i en eID som er merket som kvalifisert sertifikat.			
4.1.2.3	**Kvalifisert sertifikat for signering** Sertifikat som inneholder bruksområdet signering skal være et kvalifisert sertifikat og merkes som dette.			
4.1.2.4	**Sertifikatpolicy for sertifikater merket kvalifisert** Sertifikatpolicy for kvalifiserte sertifikater skal tilfredsstille kravene til QCP (Qualified Certificate Policy) i ETSI TS 101 456 [a], eventuelt også kravene til QCP+ dersom det tilbys kvalifisert signatur.			
4.1.2.5	**Sertifikatpolicy for sertifikater som ikke er merket kvalifisert** Krav i sertifikatpolicy som gjelder sertifikater som ikke er merket kvalifisert, skal tilfredsstille kravene til NCP+ (extended Normalized Certificate Policy) i ETSI TS 102 042 [b].			
4.2.1	**Tilgang til sertifikatutsteders offentlige nøkler** Nødvendige utstedersertifikater (rotsertifikater) for verifisering av utstedte sertifikater skal være allment (åpent) tilgjengelige og distribueres på en sikker og tillitvekkende måte. Prosedyre for distribusjon skal dokumenteres.			
4.3.1.1	**Styringssystem for informasjonssikkerhet** Sertifikatutsteder skal ha et formalisert og dokumentert styringssystem for informasjonssikkerhet (ISMS), eksempelvis som definert i ISO/IEC 27001. Styringssystemet skal som minimum omfatte den delen av organisasjonen og de prosessene som inngår i leveransen av basis eID/sertifikattjeneste som definert i kapittel 4.			
4.3.1.2	**Risikovurdering og risikohåndtering** Sertifikatutsteder skal regelmessig gjennomføre en metodisk risikovurdering for å evaluere risiko, samt beslutte sikringskrav og sikringstiltak. Risikovurderingen skal som minimum utføres årlig, og resultatet av denne, samt tilhørende tiltak for risikohåndtering skal på forespørsel gjøres tilgjengelig for tilsynsmyndighet.			
4.3.1.3	**Valg av sikringstiltak** Sikringstiltak for informasjonssikkerhet skal velges på basis av gjennomført risikovurdering og skal som minimum være i henhold til ISO/IEC 27002:2005.			

4.4.1.1	**Nøkkelgenerering – sertifikatutstederens nøkler** Nøkkelgenerering for sertifikatutsteders egne nøkler skal foregå i henhold til en veldokumentert prosess, og det skal dokumenteres at prosessen har vært fulgt (”nøkkelseremoni”). Prosessen skal inkludere sertifisering av sertifikatutstederens offentlige nøkler gjennom egensignerte sertifikater og eventuelt også sertifikater fra utstedere på høyere nivå i hierarkier.			
4.4.1.2	**Sertifikatinnehavers nøkler og sertifikater** Styrke og levetid for sertifikater og nøkler skal være i henhold til ETSI TS 102 176 -1 [s]. Sertifikatutsteder skal spesifisere algoritme, nøkkellengde og levetid for nøkler og sertifikater for sertifikatinnehaverne. Det skal spesifiseres i hvilken grad nøkler kan gjenbrukes ved fornyelse av sertifikater.			
4.4.1.3	**Levetid for sertifikatutsteders egne nøkler og sertifikater** Levetid for sertifikatutsteders egne nøkler og sertifikater (for signering av sertifikater og statusinformasjon) skal være i henhold til ETSI TS 102 176-1 [s]. Sertifikatutsteder skal spesifisere algoritme, styrke og levetid for nøkler som brukes av sertifikatutstederen selv, og for sertifikater (egensignerte og andre) for slike nøkler.			
4.4.1.4	**Krav til kryptografisk styrke for sertifikatutsteder** Sertifikatutsteders hashalgoritme og offentlig-nøkkel algoritme med tilhørende nøkkellengde for signering av sertifikater og statusinformasjon (CRL, OCSP) skal være i henhold til krav i ETSI 102 176-1 [s].			
4.4.1.5	**Sikkerhetskopi av private nøkler for dekryptering** Sertifikatutsteder skal oppgi om det tas sikkerhetskopi av private nøkler for dekryptering, og om dette gjøres for alle slike nøkler eller som et frivillig tilbud til sertifikatinnehaverne. Sikkerhetskopi av private nøkler for dekryptering skal ikke forekomme dersom disse nøklene også har andre bruksformål (autentisering og/eller signering). Dersom det tas sikkerhetskopi, skal det beskrives hvordan sikkerhetskopien oppbevares og sikres. Betingelser for tilgang til sikkerhetskopien skal beskrives.			
4.4.2.1	**Nøkkelgenerering – sertifikatinnehaverens nøkler** Sertifikatutsteder skal garantere at prosesser for nøkkelgenerering for sertifikatinnehavernes nøkler oppfyller kravene i esignaturloven [2] § 11, 1. og 3. ledd. Dette skal gjelde for nøkler som genereres av sertifikatutsteder, av programvare eller utstyr levert av sertifikatutsteder (for eksempel i et smartkort under brukerens kontroll) eller av programvare eller utstyr levert av andre (for eksempel smartkort fra annen leverandør).			
4.4.2.2	**Kvalitet på kryptoutstyr** Følgende utstyr skal oppfylle krav til FIPS PUB 140-2 [p] nivå 3 eller høyere, eller tilsvarende standarder (se ETSI TS 101 456 [a] avsnitt 7.2.1 og 7.2.2): a) Utstyr for generering og lagring/bruk av sertifikatutsteders egne, private nøkler. b) Utstyr for generering av nøkler for sertifikatinnehavere når dette gjøres slik at private nøkler etterpå må skrives til lager for sertifikatinnehaverens private nøkler (for eksempel nøkler som genereres i spesielt utstyr, og så skrives til smartkort).			

4.4.2.3	**Beskyttelse av sertifikatinnehavers private nøkler** Sertifikatinnehaveres private nøkler skal lagres i egne elektronikkomponenter (for eksempel smartkort) på en slik måte at nøklene ikke kan leses, kopieres eller endres. Tilgang til private nøkler skal kreve to faktorer: Fysisk besittelse av en komponent som ikke er kopierbar, og en statisk (eller dynamisk) faktor som heller ikke er kopierbar (for eksempel et passord som sertifikatinnehaver må huske). Brukeren skal godkjenne hver operasjon som involverer private nøkler ved å autentisere seg. Elektronikkomponenter skal minst tilfredsstille krav i FIPS 140-2 eller en tilsvarende standard som er relevant for det aktuelle produktet. Sertifikatutstederen skal fremlegge dokumentasjon på hvordan kravene er oppfylt.			
4.5.1.1	**Dokumentasjon av registrering og utstedelsesprosess** For utstedelse av sertifikater skal minimum følgende beskrives, og det skal spesifiseres hvilke oppgaver som utføres av RA-rollen, og hvilke som utføres av sertifikatutsteder: Hvor og hvordan sertifikatinnehaverens nøkkelpar genereres, distribueres og installeres. Hvordan registrering av sertifikatsøknad skjer, herunder hvordan personopplysninger kontrolleres, og om det innhentes samtykke til offentliggjøring av sertifikat i henhold til esignaturloven [2] § 14 annet ledd bokstav b. Rutine for utstedelse av sertifikater, herunder hvor og hvordan sertifikatsøkeren får utlevert sertifikat jfr. esignaturloven [2] § 13 og medfølgende forskrift [4] § 7. Tid fra søknad er levert til sertifikat kan utleveres skal oppgis. Alle disse funksjonene skal være tilstrekkelig dekket i sertifikatpolicy og sertifikatpraksis, og beskrivelsen kan derfor gis i form av referanse til relevante deler av disse dokumentene.			
4.5.1.2	**Organisering av RA-tjenesten** RA-tjenesten skal organiseres i henhold til kravene i esignaturloven [2] med forskrift [4] og ETSI TS 101 456 [a].			
4.5.1.3	**RA som underleverandør** Sertifikatutsteder skal spesifisere hvilke underleverandører som har avtale med sertifikatutsteder om levering av RA-tjenester. Sertifikatutsteder skal også spesifisere om det er mulig for andre underleverandører å kunne ha rollen som RA (for eksempel en offentlig virksomhet), og i tilfelle hvilke betingelser som gjøres gjeldende.			
4.5.1.4	**Tekniske og organisatoriske løsninger for RA** Sertifikatutsteder skal beskrive hvilke krav som stilles til en RA innen følgende områder, og hvordan det kontrolleres at disse kravene er oppfylt: Utstyr (maskinvare og programvare) for RA, Hvordan RA autentiseres overfor sertifikatutstederen, Krav til opplæring og eventuelt andre krav til RAs personell, Krav til fysisk sikkerhet, IT-sikkerhet og organisatorisk sikkerhet for RA.			

4.5.1.5	**Dokumentasjonskrav ved utstedelse av sertifikatet** Sertifikatutsteder skal ved utstedelse av sertifikater kreve at sertifikatsøkeren fremviser legitimasjonsdokument som oppfyller kravene til hvitvaskingsforskriften [9] § 5 første ledd. Sertifikatutsteder er ansvarlig for å påse at RA-tjenesten oppfyller disse kravene.			
4.5.1.6	**Registrering, oppbevaring og sletting av opplysninger** Sertifikatutsteder har ansvar for å registrere, lagre og slette opplysninger etter krav i hvitvaskingsloven [8] § 8 første og annet ledd og § 22 og hvitvaskingsforskriften [9] § 17.			
4.5.1.7	**Personlig oppmøte, geografisk nærhet** Personlig oppmøte skal kunne skje i tilstrekkelig geografisk nærhet for alle aktuelle sertifikatsøkere bosatt i Norge. Geografisk spredning av RA-aktører skal beskrives. Eventuelle RA-tjenester for personer bosatt i utlandet skal også beskrives.			
4.5.1.8	**Validering mot Folkeregisteret** For personer som er registrert i Folkeregisteret, skal opplysninger kunne valideres mot Folkeregisteret.			
4.6	**RA-tjeneste for Personsertifikater for utenlandske personer uten D-nummer** Det skal angis om sertifikatutstederen leverer denne tjenesten. I så fall gjelder kravet nedenfor, 4.6.1.	**Leveres:**	**Ja**	**Nei**
4.6.1	**Dokumentasjonskrav, registrering, oppbevaring og sletting av relevante opplysninger** Kontroll og registrering av opplysninger om utenlandske personer uten D-nummer må følge samme krav som krav til rekvirering av D-nummer i forskrift om folkeregistrering [14]. Innsamlede opplysninger skal oppbevares og slettes iht. bestemmelsene i hvitvaskingsloven § 22 og hvitvaskingsforskriften § 17.			
4.7.1.1	**Plattformuavhengighet** Løsningen skal ikke binde sertifikatinnehaver til én plattform med hensyn til for eksempel operativsystem eller nettleser. Det skal spesifiseres hvilken maskinvare sertifikatinnehaver kan benytte (PC, MAC, PDA osv.). Det skal spesifiseres behov for eventuelle grensesnitt mot utstyr (seriell port, USB osv.). Det skal beskrives behov for installasjon av maskinvare (for eksempel kortleser).			
4.7.1.2	**Universell utforming** Løsningen skal oppfylle krav til universell utforming iht. lov 20. juni 2008 nr. 42 om forbud mot diskriminering på grunnlag av nedsatt funksjonsevne (diskriminerings- og tilgjengelighetsloven) [15] § 11, innen de frister som er fastsatt i eller med hjemmel i loven.			
4.7.1.4	**Installasjon av basis programvare for tilgang til eID** Sertifikatutsteder skal oppgi om spesifikk programvare for tilgang til eID (for eksempel for tilgang til smartkort på en PC) må installeres fast i sertifikatinnehavers systemer. Systemkrav (operativsystemer som støttes mv.) for programvaren skal oppgis.			

4.7.1.5	**Bruk av Java applets og lignende** Sertifikatutsteder skal oppgi om Java applets eller liknende teknologier brukes for tilgang til eID. Systemkrav (operativsystemer som støttes mv.) for programvaren skal oppgis.			
4.7.1.7	**Vedlikehold av programvare** Prosedyrer for vedlikehold av programvare og oppdatering av installert programvare (der dette er relevant) skal beskrives.			
4.7.1.8	**Lisenser** Alle nødvendige lisenser for programvare med mer skal være dekket av sertifikatutstederens avtale med sertifikatinnehaver.			
4.7.1.9	**Sikkerhet og systeminnstillinger hos sertifikatinnehaver** Dersom tilgang til eID krever spesielle innstillinger for sikkerhet på sertifikatinnehavers utstyr (for eksempel konfigurasjon av brannmurer), skal dette oppgis.			
4.7.2.2	**Spesifikasjon av integrasjonspakker** Dersom sertifikatutsteder (eventuelt gjennom samarbeidspartnere) tilbyr integrasjonspakker for sertifikatmottakere, gjelder følgende krav. Det skal oppgis om integrasjonspakke er nødvendig for å kunne være sertifikatmottaker (se forrige krav). Det skal spesifiseres hvilke integrasjonspakker som tilbys, for eksempel integrasjonspakker for Tjenesteeier og integrasjonspakker for PC-miljø. For hver integrasjonspakke skal det oppgis hvilke grensesnitt (for eksempel PKCS#11 [m] og Microsoft CAPI) som støttes. Systemkrav for programvaren skal oppgis. Dette gjelder operativsystemer som støttes, og eventuelt også krav til programmiljø (for eksempel J2EE, .Net med mer).			
4.7.2.3	**Vedlikehold av programvare** Dersom integrasjonspakker tilbys, skal prosedyrer for vedlikehold av programvaren og oppdatering av installert programvare beskrives.			
4.7.2.4	**Dokumentasjon for integrasjonspakker** Dersom integrasjonspakker tilbys skal det finnes tilstrekkelig dokumentasjon til at en programmerer med generell kompetanse uten kjennskap til grensesnittet skal kunne benytte det.			
4.7.2.5	**Eksempelkode** Dersom integrasjonspakker tilbys skal det finnes kompilerbar eksempelkode som viser bruk av alle funksjoner i applikasjonens programmeringsspråk.			
4.7.2.6	**Lisenser for Tjenesteeier** Alle lisenser på integrasjonspakker og eventuelle andre nødvendige programlisenser skal være dekket av brukerstedsavtale (individuell avtale eller avtale som omfatter flere Tjenesteeiere i offentlig sektor) mellom sertifikatutsteder og sertifikatmottaker.			
4.8.1.1	**Tilbakekalling av sertifikater** Sertifikatutstederen skal levere en tjeneste for tilbakekalling av sertifikater. Sertifikatene skal kunne kalles tilbake på bakgrunn av en skriftlig, telefonisk eller elektronisk henvendelse med tilstrekkelig autentisering. Tjenesten skal være tilgjengelig 24 timer i døgnet alle døgn i året. Det skal fremgå hvem som kan kreve sertifikat tilbakekalt, og hvilke mekanismer som finnes for å beskytte mot feilaktig tilbakekalling.			

4.8.1.2	**Hendelser som krever tilbakekalling** Sertifikatutsteder skal på eget initiativ kalle tilbake (ev. suspendere) sertifikatene som et minimum: Ved kompromittering, herunder ved mottatt melding om tap av privat nøkkel. Sertifikatutsteder avdekker eller har rimelig grunn til å tro at viktig informasjon i sertifikatet er feilaktig.			
4.8.1.3	**Fornyelse av sertifikater** Sertifikatutsteder skal levere en tjeneste for å fornye sertifikater og nøkler f.eks. ved utløp av gyldighetstid, tilbakekalling av sertifikat eller tap av nøkkelbærer/beskyttelsesmekanisme. Det skal spesifiseres hvordan denne tjenesten tilbys sertifikatinnehaveren. Tjenesten skal kunne tilby automatisk initiering av fornyelse. Sertifikatutsteder skal spesifisere sin leveransetid for fornyelse av sertifikater.			
4.9.1	**Dokumentasjon av brukerstøtte** For brukerstøtte (”helpdesk”) funksjonen skal minimum følgende beskrives: Tjenesten. Dens organisering. Hvilke oppgaver som løses som 1. linje og 2. linje oppgaver. Om henvendelser ifm. tilbaketrekning av sertifikater skal gjøres til brukerstøtte, eller om det skal gjøres ved henvendelse til en separat tjeneste. Eskaleringsrutiner for support henvendelser. Responstid; dvs. hvilke svartider som det legges opp til. Hvordan sertifikatinnehaver får tilgang til tjenesten, om det er via telefon, elektronisk post eller web-grensesnitt. Hvordan brukerstøtte for sertifikatinnehavere kan integreres med brukerstøtte for applikasjoner som de benytter.			
4.9.2	**Drift av brukerstøtte** Det skal tilbys en brukerstøttefunksjon som skal gi direkte assistanse på norsk til Kunden. Brukerstøttetjenesten skal også dekke programvare og maskinvare levert til sertifikatinnehaver som del av tjenesten. (Dette kravet gjelder brukerstøtte for sertifikatinnehaver, applikasjonsutvikler og drift.)			
4.9.4	**Brukerstøtte for applikasjonsutviklere** Det skal tilbys en brukerstøtteordning for applikasjonsutviklere som benytter programgrensesnitt for å integrere PKI funksjonalitet. Denne tjenesten skal beskrives.			
A-KRAV TIL KATALOG- OG OPPSLAGSTJENESTER - må oppfylles av alle sertifikatutstedere				
5.2.1	**Tilbakekallingslister – regelmessig utstedelse** Sertifikatutsteder skal utstede nye CRLer iht. X.509 [f] regelmessig minst hver 24. time. Frekvens for CRL-utstedelse skal framgå av sertifikatpolicy. CRL skal være i henhold til RFC 5280 [g]. CRLer skal kunne gjøres tilgjengelige for parter som har behov for tilgang.			
5.2.4	**Begrensninger i tilgang** Eventuelle begrensninger i tilgang til CRL skal oppgis. Dersom det er begrensninger på tilgang, skal metode for tilgangskontroll til CRL beskrives.			

5.2.8	**Arkivering av tilbakekallingslister for Person-Høyt og Virksomhet** Sertifikatutsteder skal arkivere utstedte CRLer i minst 10 år. Sertifikatutsteders rutiner for arkivering av CRLer skal beskrives.			
5.3.1	**OCSP-tjeneste** Ved tilbakekalling av sertifikater skal informasjon gjøres tilgjengelig uten ugrunnet opphold, men senest 1 time etter at sertifikatutsteder fikk kunnskap om forholdet, ved hjelp av en OCSP-tjeneste som definert i RFC 2560 [h].			
5.3.2	**Begrensninger i tilgang** Eventuelle begrensninger i tilgang til OCSP-tjenesten skal oppgis. Dersom det er begrensninger på tilgang, skal metode for tilgangskontroll til OCSP-tjenesten beskrives.			
5.3.4	**Ytelse på OCSP-tjeneste** Oppslag i OCSP-tjeneste skal gi svar innen 1 sekund (uavhengig av belastning). Målepunkt er grensesnitt mot offentlig nett.			
5.3.5	**Tilgjengelighet av OCSP-tjeneste** OCSP-tjenesten skal være tilgjengelig 24 timer i døgnet alle dager året rundt. OCSP-tjenesten skal minimum ha en oppetid på 99,5 % i snitt over et år. Maksimal sammenhengende nedetid skal være 3 timer. Sertifikatutstederen skal dokumentere hvordan oppetid måles og opprettholdes.			
5.4	**Tilgang til katalogtjenester** Det skal angis om det leveres katalogtjenester. I så fall gjelder kravene nedenfor, 5.4.2 til 5.4.8.	**Leveres:**	**Ja**	**Nei**
5.4.2	**Skjema og søkemuligheter** Skjema for ldap-katalog skal dokumenteres. Det skal også dokumenteres hvilken informasjon det er mulig å søke på i katalogen.			
5.4.4	**Samtykke til tilgjengeliggjøring** Personsertifikatene skal være offentlig tilgjengelige bare i de tilfellene der sertifikatinnehaveren har gitt sitt samtykke, jf. esignaturloven § 14 annet ledd bokstav b).			
5.4.5	**Begrensninger i tilgang** Eventuelle begrensninger i tilgang til katalogen skal oppgis. Dersom det er begrensninger på tilgang, skal metode for tilgangskontroll til katalogen beskrives.			
5.4.7	**Ytelse på katalogoppslag** Katalogtjenesten skal returnere svar innen maks 1 sekund per oppslag (uavhengig av belastning). Målepunkt er grensesnitt mot offentlig nett.			
5.4.8	**Tilgjengelighet av katalogtjeneste** Katalogtjenesten skal være tilgjengelig 24 timer i døgnet alle dager i året. Tjenesten skal ha en tilstrekkelig høy oppetid i snitt over et år. Maksimal sammenhengende nedetid skal være 3 timer. Sertifikatutstederen skal dokumentere hvordan oppetid måles og opprettholdes.			

5.5.1	**Oppslagstjeneste for fødselsnummer og D-nummer** Sertifikatutsteder skal tilby en oppslagstjeneste som gjør det mulig for autoriserte parter å knytte sertifikat til fødselsnummer/D-nummer Tjenestene skal være i henhold til "Grensesnitt for tilgang til Oppslags-tjenester"[11] samt at utlevering av fødselsnummer/D-nummer skal være i henhold til personopplysningsloven [6] § 12 og personopplys-ningsforskriften [7] § 10-2. Tjenesten skal beskrives.			
5.6.1	**Tilgang til sertifikatstatus** Det skal legges til rette for et felles punkt for tilgang til sertifikatstatusin-formasjon (OCSP eller CRL som beskrevet i kap. 5) for forvaltningen, slik at oppslag kan gjøres av hvilken som helst virksomhet i offentlig sektor. Slikt oppslag skal ikke kreve installasjon av programvare som er spesifikk for sertifikatutstederen.			
5.7.1	**Planlagt nedetid** Dersom sertifikatutstederen har behov for å oppdatere, revidere eller vedlikeholde tjenesten skal dette avtales med Kunden innen rimelig tid før gjennomføring av arbeidet. Slikt arbeid skal fortrinnsvis foregå mellom kl. 01:00 til 04:00 lørdag, søndag eller mandag. Avtalt nedetid regnes ikke som manglende oppetid. Periodiske driftsprosedyrer som for eksempel sikkerhetskopiering skal ikke medføre avtalt nedetid. Planlagt nedetid skal ikke overstige 3 timer pr. kalendermåned.			
5.7.2	**Driftsinformasjon** Driftsinformasjon som er av betydning for sertifikatmottakere, som planlagt nedetid, feilsituasjoner osv. skal være tilgjengelig på eget nettsted. Nettstedet skal være tilgjengelig for sertifikatmottakere. Serti-fikatutstederen skal også tilby en varslingstjeneste for å varsle slike hendelser.			
5.7.3	**Opphør av sertifikatutsteders tjeneste eller virksomhet** Sertifikatutsteder skal beskrive om, og i tilfelle hvordan, sertifikater og statusinformasjon planlegges vedlikeholdt dersom sertifikatutsteders tjeneste eller virksomhet opphører, se forskrift om utstedere av kvalifi-serte sertifikater § 3, jf. esignaturloven § 14.			
A-KRAV TIL AUTENTISERINGSTJENESTER – må oppfylles av sertifikatutstederen hvis autentiseringstjenester leveres				
6.1	**Autentiseringstjenester** Det skal angis om det leveres autentiseringstjenester. I så fall gjelder kravene nedenfor, 6.1.1 til 6.1.2.	**Leveres:**	**Ja**	**Nei**
6.1.1	**PKI-basert autentisering** eID skal kunne brukes i en PKI-basert protokoll for autentisering. For andre protokoller enn TLS/SSL skal protokollen dokumenteres, og det skal godtgjøres at den gir tilstrekkelig sikkerhet.			
6.1.2	**Kanalbinding for autentisering** Dersom den PKI-baserte protokollen utføres etter oppsett av en (ensi-dig) TLS/SSL-kanal, skal det beskrives hvordan autentiseringen av sluttbruker koples til den sikre kanalen (hindre "man in the middle" angrep).			

A-KRAV TIL SIGNERINGSTJENESTER – må oppfylles av sertifikatutstederen hvis signeringstjenester leveres				
7.1	**Signeringstjenester** Det skal angis om sertifikatutstederen leverer signeringstjenester. I så fall gjelder relevante kravene nedenfor, 7.1.1 til 7.1.5.	**Leveres:**	**Ja**	**Nei**
7.1.1	**Støtte for standard signaturformater** Signerte dataobjekter skal være i henhold til et etablert standardformat som en med rimelighet kan forvente at mottaker skal kunne håndtere. Eksempler er XML DSIG, PKCS #7 [e], CMS [n], PDF, XAdES (ETSI TS 101 733 [c]), CAdES (ETSI TS 101 903 [d]) og SEID SDO signeringsformat.			
7.1.2	**Universell utforming** Løsningen skal oppfylle krav til universell utforming iht. lov 20. juni 2008 nr. 42 om forbud mot diskriminering på grunnlag av nedsatt funksjonsevne (diskriminerings- og tilgjengelighetsloven) [15] § 11, innen de frister som er fastsatt i eller med hjemmel i loven.			
7.1.3	**Sertifikater i SDO** SDO skal minimum inneholde sertifikatet til den som har signert, eventuelt alle sertifikater i sertifikatstien opp til rotsertifikatet.			
7.1.5	**Åpen signaturvalidering** Signerte dokumenter skal kunne verifiseres av en vilkårlig mottaker i offentlig sektor uten krav til installasjon av spesifikk programvare for eID som er brukt ved signering. Verifisering skal være mulig med programvare valgt av mottakeren, og skal kun kreve konfigurering av mottakerens systemer (installasjon av sertifikatutsteders rotsertifikat og konfigurering av tilgang til OCSP-tjeneste og/eller CRL-tjeneste).			
7.2.1	**Bruk av privat nøkkel** Ved signering av informasjon skal det sikres at sertifikatinnehaver må godkjenne hver operasjon som involverer bruk av privat nøkkel med PIN, passord eller tilsvarende.			
7.5.1	**Brukervennlighet** Alle brukergrensesnitt skal oppfattes som enkle og brukervennlige. Der det er etablert de facto standarder for brukerdialog eller brukergrensesnitt skal disse kunne brukes, for eksempel vil relevante standarder kunne publiseres i Referansekatalog for IT-standarder i offentlig sektor [16]. Alle brukerdialoger skal tilby norsk språk.			
7.5.2	**Språk** Alle brukerdialoger skal tilby norsk språk.			
7.5.3	**Hjelpetekst** Det skal finnes eller være mulig å legge inn hjelpetekst på norsk i tilknytning til alle brukerdialoger.			
7.5.4	**Brukerveiledning** Det skal forefinnes veiledning av installasjon og bruk på norsk.			

7.5.7	**Bevisste aksjoner** Brukeren skal få tydelig varsel om at hun er i ferd med å foreta en signering. Bruker skal kunne velge å avbryte signeringen.			
7.5.8	**"What You See Is What You Sign" (WYSIWYS)** Det skal være samsvar mellom hva bruker ser og hva hun signerer. Det skal dokumenteres hvordan dette prinsippet tilfredstilles.			
7.5.9	**Responstid** Tiden for autentisering og signering skal ta maks tre sekunder (med fratrekk av tiden bruker benytter for å gi inn PIN).			
7.6	**Kvalifiserte signaturer** Det skal angis *om* sertifikatutstederen leverer kvalifiserte signaturer. I så fall gjelder kravene nedenfor, 7.6.1 til 7.6.4.	**Leveres:**	**Ja**	**Nei**
7.6.1	**Sikkert signaturframstillingssystem** Signaturframstillingssystem skal fylle kravene til sikkert signaturfremstillingssystem, jfr. esignaturloven § 9.			
7.6.2	**Bruk av privat nøkkel** Ved signering av informasjon skal det sikres at sertifikatinnehaver må godkjenne hver operasjon som involverer bruk av privat nøkkel med PIN, passord eller tilsvarende.			
7.6.3	**Krav til signaturfremstillingsapplikasjon** Hashalgoritme for signering skal være i henhold til krav for nivå standard i ETSI TS 102 176-1 [s]. Dersom dette medfører behov for skifte av hashalgoritme, skal plan for overgang til ny algoritme spesifiseres. Det skal videre dokumenteres hvorvidt løsningen samsvarer med kravene og anbefalingene i CWA 14170 [k]. Hvert punkt 1-17 under Annex A, A1 skal kommenteres. Følgende punkter i CWA 14170 [k] skal i tillegg dokumenteres: Hvis informasjonselementer knyttet til signeringen (autentiseringskode, nøkler, dokument, attributter, hashverdi) overføres over Internet eller mellom ulike plattformer, skal dette beskrives med angivelse av hvordan integritet, konfidensialitet og fullstendighet sikres (jf. pkt. 7.3 i CWA 14170) Beskriv hvordan sikkerhetskravene til autentisering i pkt. 11.8 i CWA 14170 tilfredsstilles. Beskriv hvordan det sikres at signaturattributter ikke skal kunne endres i forhold til det brukeren eller systemet har valgt. Beskriv hvilke advarsler brukeren får dersom signaturattributter inneholder skjult tekst. Dersom programvaren inneholder en egen modul for å presentere undertegners dokument/data eller leverer programvare for å analysere undertegners dokument/data for å finne skjulte koder og data som er skjult for undertegner, skal det angis hvilke formater (Data Content Type) som programvaren kan vise/analysere. Beskriv hvilke advarsler som gis dersom dokumentet inneholder skjulte koder (for eksempel makroer) eller dersom ikke alle deler av dokumentet kan vises.			

7.6.4	**Signaturverifisering** Dersom programvare som i pkt. 7.1.4 tilbys, skal sertifikatutsteder dokumentere hvorvidt løsninger for å framvise og verifisere signerte data samsvarer med krav i CWA 14171 [I]. Herunder hvorvidt løsningen kan: Presentere dokumentet slik det ble framvist under signering Varsle bruker om eventuelt dynamisk innhold i dokumentet Tydelig vise status for signaturverifikasjon Sikre at data brukt for å verifisere signatur samsvarer med data som vises for den som verifiserer Sikre at riktig og gyldig (på signaturtidspunkt) sertifikat benyttes til signaturverifikasjon Sikre at sikkerhetsrelevante endringer oppdages.			
A-KRAV TIL MELDINGSKRYPTERING – må oppfylles av sertifikatutstederen hvis meldingskryptering leveres				
8.1	**Meldingskryptering** Det skal angis om sertifikatutsteder leverer eID som kan brukes til meldingskryptering. I så fall gjelder kravene nedenfor, 8.1.1 til 8.1.3.	**Leveres:**	**Ja**	**Nei**
8.1.1	**Kryptering av meldinger med senderens programvare** Sertifikat merket for kryptering skal være tilgjengelig for bruk i programvare valgt av senderen. En sender i offentlig sektor skal ikke trenge å installere spesifikk programvare eller å ha egen avtale med sertifikatutsteder for å utføre kryptering til en sertifikatinnehaver.			
8.1.2	**Tilgjengeliggjøring av sertifikat** Det skal legges til rette for tilgjengeliggjøring av krypteringssertifikater enten Ved at sertifikatinnehaver skal kunne publisere sitt krypteringssertifikat som en del av en samtykketjeneste (jf. krav 5.4.4) eller Ved at det gis tilgang til katalog over utstedte sertifikater, se krav 5.4.1, 5.4.2 og 5.5.2.			
8.1.3	**Dekryptering** Det skal legges til rette for dekryptering ved enten At sertifikatinnehaver kan nå privat nøkkel for dekryptering over åpne grensesnitt for integrasjon med tredjeparts programvare for dekryptering hos sertifikatinnehaver. (Eventuelle betingelser knyttet til slik integrasjon skal oppgis). eller At sertifikatutsteder leverer programvare for dekryptering, eventuelt med samarbeidspartnere. Dersom programvare leveres av sertifikatutsteder (eventuelt med samarbeidspartnere), skal dette ansees som en del av programvarepakker for å ta i bruk en eID, og skal være underlagt krav spesifisert i 4.7.1.			

SERTIFIKATUTSTEDERENS UNDERSKRIFT	
Undertegnede bekrefter herved å oppfylle alle relevante krav oppgitt som absolutte (A-krav) for sertifikatklassen "Person-Høyt" i "Kravspesifikasjon for PKI i offentlig sektor", som er beskrevet ovenfor, og at opplysninger gitt på dette skjemaet er korrekte. Undertegnede er oppmerksom på at det vil/kan bli krevd gebyr i henhold til forskriften § 14 og forskrift om gebyr til Nasjonal kommunikasjonsmyndighet av 20. mars 2000 § 3.	
Dato	Sted
Underskrift av signaturberettiget hos sertifikatutsteder	
(Gjenta underskriften her med maskinskrift)	