Kravspesifikasjon for PKI i offentlig sektor

Versjon 2.0
Juni 2010

Innhold

1. INNLEDNING

1.1 Formål og bakgrunn

Dette dokumentet er en overordnet, funksjonell kravspesifikasjon for selvdeklarering og anskaffelse av PKI-basert eID som skal benyttes i forbindelse med elektronisk kommunikasjon med og i offentlig sektor i Norge. PKI-løsninger som benyttes i offentlig virksomhet skal oppfylle kravspesifikasjonen. Kravspesifikasjonen er hjemlet i eForvaltningsforskriften § 27. Videre er det fastsatt i forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere at krav angitt i kravspesifikasjonen skal oppfylles.

Formålet med kravspesifikasjonen er å bidra til enklere anskaffelser og felles krav til sikre og standardiserte PKI-tjenester i forvaltningen. Den enkelte virksomhet må gjøre selvstendige sikkerhets- og sårbarhetsvurderinger og avgjøre hvilke sikkerhetstjenester og hvilket sikkerhetsnivå de har behov for, i tråd med deres sikkerhetsmål og -strategi, jf. eForvaltningsforskriften [3] §§ 4 og 13. Tilsvarende krav følger av annet regelverk, bl.a. personopplysningsloven.

Kravspesifikasjonen inngår som krav for en rekke anvendelsesområder i og utenfor offentlig sektor og er på denne bakgrunn delt inn i:

- Krav til basis sertifikattjenester – dette er grunnkrav til alle PKI-løsningene som skal selvdeklareres og/eller leveres i henhold til kravspesifikasjonen.
- Krav til tjenester som er nødvendig for å realisere bruksområdene autentisering, signering og kryptering basert på en basis sertifikattjeneste.
- Krav til tilleggstjenester.

Tjenester som er nødvendig for å realisere bruksområdene autentisering, signering og kryptering kan leveres både av det offentlige selv og av sertifikatutstedere i markedet.

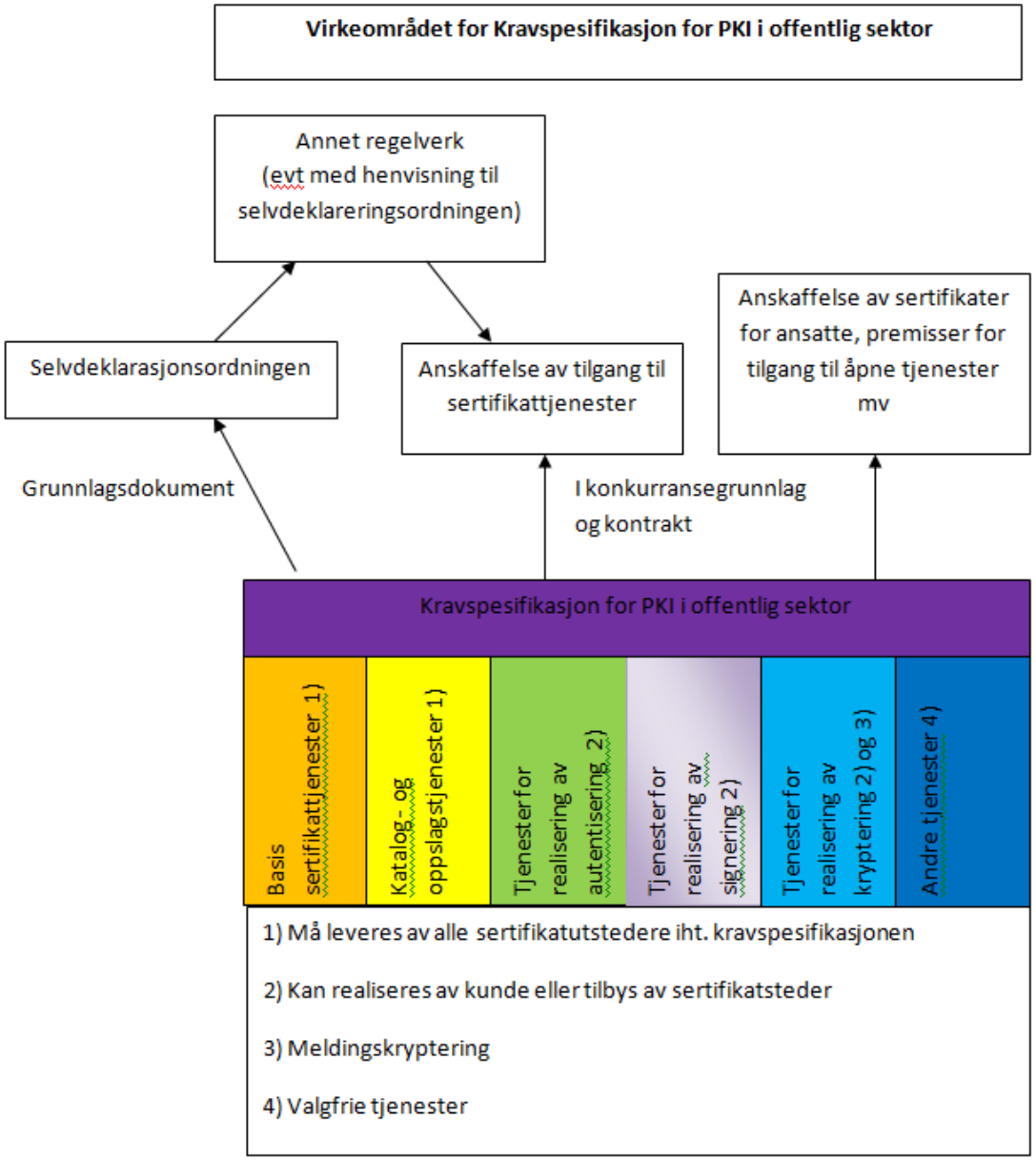
Kravspesifikasjonen er utformet slik at kravene så langt som mulig relevante internasjonale standarder samt følger anbefalingene fra SEID-prosjektet.

1.2 Kort om virkeområdet

Kravspesifikasjonen er et overordnet dokument som fastsetter hvilke felles krav til sikkerhet som må ligge i bunn for basis sertifikattjenester og øvrige tjenester som tilbys. Kravspesifikasjonen dekker bruksområdene autentisering, signering og kryptering.

Figuren nedenfor illustrerer bruksområdene som er beskrevet i kravspesifikasjonen. Figuren illustrerer også at kravspesifikasjonen understøtter selvdeklarasjonsordningen, se punkt 1.3 nedenfor. Annet regelverk baserer seg på selvdeklarasjonsordningen, eller viser til denne.

Videre inngår kravspesifikasjonen i konkurransegrunnlaget og kontrakten ved inngåelse av avtaler om tilgang til sertifikattjenester. Tilsvarende vil kravspesifikasjonen være aktuell ved kjøp av sertifikater til virksomheten eller ansatte og ved bruk av åpne tjenester. Se figuren nedenfor.



Kravspesifikasjonen stiller krav til tre typer sertifikater som er delt inn i sertifikatklassene Person-Standard, Person-Høyt og Virksomhet.. Sertifikatklassene forholder seg til de to øverste sikkerhetsnivåene i Rammeverk for autentisering og uavviselighet [13], se punktene 2.1 og 2.2.

PKI-løsninger for mobiltelefon er i ferd med å bli utbredt og kan tilby tilfredsstillende sikkerhetsnivå. Her lagres brukerens private nøkler på SIM-kortet i mobiltelefonen. Kravspesifikasjonen er ikke skrevet med tanke på mobil PKI, men den er ikke til hinder for bruk av mobil plattform hvis den kan realiseres innenfor de kravene som er stilt i kravspesifikasjonen.

1.3 Bruk av kravspesifikasjonen ved selvdeklarasjon

Selvdeklarasjonsordningen, og tilsynet med denne, skal sørge for at sertifikatutstederne oppfyller kravene i kravspesifikasjonen, jf. forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere [12]. Formålet med selvdeklarasjonsordningen er å fastslå hvilke sertifikater og sertifikattjenester som møter offentlig sektors krav innenfor de ulike tjenestene. Ordningen bidrar til forenkling av anskaffelser i både privat og offentlig sektor.

Post- og teletilsynet er utpekt som tilsynsmyndighet etter selvdeklarasjonsordningen og publiserer en liste over de utstederne som har selvdeklarert seg til tilsynet innen de ulike sertifikatklassene. Tilsynet skal publisere selvdeklarasjonsmeldingen hvor det fremgår hvilke bruksområder og hvilke tilhørende tjenester sertifikatutstederen har selvdeklarert seg for, med en beskrivelse av hvordan kravene er oppfylt. Dersom det foreligger særlige grunner, kan tilsynet gjøre unntak fra bestemmelsene i forskriften, jfr. forskriften § 9 annet ledd.

Det stilles ingen konkrete krav til sertifikatutstederens tjenester i forskriften om frivillige selvdeklarasjonsordninger for sertifikatutstedere [12]. Det følger av forskriften at sertifikatutsteder skal oppfylle alle absolutte krav (A-krav) som er relevante for aktuelle sikkerhetsprodukter og -tjenester i den sertifikatklassen utstederen deklarerer seg for. Med *aktuelle sikkerhetsprodukter og -tjenester* menes de produktene og tjenestene sertifikatutstederen velger å tilby innen den enkelte sertifikatklasse, og selvdeklarere seg for. De konkrete kravene fremgår av den til enhver tid gjeldende versjon av "Kravspesifikasjon for PKI i offentlig sektor".

Selvdeklarerte sertifikatutstedere skal levere *basis sertifikattjenester* for bruksområdene autentisering og signering med tilhørende statustjenester og oppslagstjenester. Sertifikatutstederne kan velge hvorvidt de vil levere sertifikater for bruksområdet kryptering og hvilke underliggende tjenester de vil levere. Den enkelte sertifikatutsteder kan som hovedregel velge hvilke av tjenestene beskrevet i kapittel 6-9 som skal selvdeklareres. Hvis sertifikatutstederens løsning er organisert slik at det *må* benyttes autentiserings-, signerings-, og/eller meldingskrypteringstjenester fra sertifikatutstederen selv, må også disse tjenestene selvdeklareres. Alle A-krav til tjenestene som sertifikatutstederen har selvdeklarert seg for, skal oppfylles.

Opplysninger om hvilke tjenester den enkelte sertifikatutsteder tilbyr, kan fås hos sertifikatutstederen og hos tilsynet. Det kan være hensiktsmessig at dette er tilgjengelig informasjon til brukerne gjennom fellesløsninger for tjenesteeierne. Sertifikatutstederne kan f.eks. informere om hvilke tjenester de tilbyr ved å fylle ut tabellen omtalt nedenfor under punkt 2.3.

1.4 Bruk av kravspesifikasjonen i anskaffelser

Kravspesifikasjonen er utarbeidet for å dekke krav til PKI-produkter og -tjenester for alle typer elektronisk kommunikasjon med og i offentlig sektor. Det gjelder både internt i det offentlige og mellom det offentlige og enkeltpersoner eller privat næringsvirksomhet. Siden kravspesifikasjonen skal ligge til grunn ved alle PKI-anskaffelser til offentlig sektor vil kravspesifikasjonen virke som en forvaltningsstandard og fastsette felles krav til løsningene.

Kravspesifikasjonen dekker bruksområdene autentisering, signering og kryptering. Hver anskaffelse av PKI-løsninger behøver imidlertid ikke benytte hele kravspesifikasjonen. Den enkelte tjenesteeier må vurdere hvilke bruksområder og tjenester de har behov for, for å oppnå

et bestemt sikkerhetsmål. Kravspesifikasjonen vil inngå i konkurransegrunnlaget i forespørselen hvor det presiseres hvilke deler av kravspesifikasjonen som ønskes besvart i tilbudet, og eventuelt hvilke tilleggskrav som stilles. Kravspesifikasjonen er anvendelig for ulike anskaffelsesmodeller.

2. OMFANG OG FORUTSETNINGER

2.1 Sertifikatklasser

Kravspesifikasjonene er inndelt i tre sertifikatklasser. Nedenfor fremgår en kort redegjørelse av de ulike klassene:

***Person-Standard**:* Et personsertifikat for en bestemt fysisk person som entydig identifiseres i sertifikatet.

***Person-Høyt**:* Et personsertifikat for en bestemt fysisk person som entydig identifiseres i sertifikatet. Person-Høyt er basert på kvalifiserte sertifikater, jf. esignaturloven § 4.

Virksomhet: Et virksomhetssertifikat for en enhet (virksomhet) som entydig identifiseres i sertifikatet.

For sertifikatklassen Virksomhet avgjør virksomheten hvordan sertifikatet skal benyttes, eksempelvis om det skal brukes av en fysisk person autorisert av virksomheten eller en prosess under virksomhetens kontroll, for eksempel en server. Det kan utstedes flere virksomhetssertifikater for samme bruksområde til en og samme virksomhet.

2.2 Sikkerhetsnivåer

Ved utarbeidelsen av versjon 1.02 av kravspesifikasjonen ble det identifisert tre sikkerhetsnivåer, to for privatpersoner og et for virksomheter. Den første versjonen av kravspesifikasjonen, versjon 1.02, bygget på disse tre sikkerhetsnivåene: ”Person-Høyt”, ”Person-Standard” og ”Virksomhet”.

I april 2008 publiserte Fornyings- og administrasjonsdepartementet ”Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor” [13] hvor det brukes 4 sikkerhetsnivåer. Disse 4 sikkerhetsnivåene har etter hvert blitt innarbeidede begreper i offentlig sektor. Sikkerhetsnivåene i kravspesifikasjonen forholder seg til de to øverste sikkerhetsnivåene i rammeverket: nivå 3 og 4. ”Person-Standard” er tilpasset krav til nivå 3, og ”Person-Høyt” er tilpasset krav til nivå 4.

Når det gjelder ”Virksomhet”, er de kravene som ble stilt i kravspesifikasjon versjon 1.02, i utgangspunktet ikke tilstrekkelige til å oppfylle krav til nivå 4, samtidig som kravene er strengere enn det som er minimumskravene til nivå 3. Kravene til ”Virksomhet” i kravspesifikasjon versjon 1.02 kan oppfylles av ”softsertifikater” som ikke tilfredsstiller krav til ikke-kopierbarhet av autentiseringsfaktorer gitt av nivå 4 i rammeverket. Slike virksomhetssertifikater er i dag utbredt i markedet. Rammeverket bruker likevel virksomhetssertifikater som eksempel på løsninger som *kan* tilfredsstille krav til nivå 4. For å

oppnå forutsigbarhet er det viktig at virksomhetssertifikater kan relateres til nivåene i rammeverket.

Kravspesifikasjonen stiller fremdeles krav til én sertifikatklasse for virksomhetssertifikater. Minimumskravene til klassen "Virksomhet" tilfredsstiller kravene til sikkerhetsnivå 3 i rammeverket.

Dette er imidlertid ikke til hinder for at sertifikatinnehavere, for eksempel innenfor lukkede brukergrupper som Norsk Helsenett, kan etablere tilleggskrav og særlige løsninger for håndtering av slike virksomhetssertifikater som gjør det forsvarlig å benytte disse også på nivå 4. Det samme gjelder virksomhetssertifikater som oppfyller krav 4.1.4.2 om oppbevaring av nøkler på elektronikkomponenter (B-krav).

For virksomhetssertifikater som brukes av automatiserte prosesser under virksomhetens kontroll er krav 4.1.4.1 ikke *alene* tilstrekkelig til å oppfylle de forutsetninger som ligger til grunn i rammeverket for å kunne benyttes på sikkerhetsnivå 4 (jf. krav til ikke-kopierbarhet av autentiseringsfaktorer). Dette er imidlertid ikke til hinder for at virksomheten ved hjelp av egne tiltak kan oppnå så godt vern mot kopiering og misbruk at et slikt sertifikat kan benyttes på sikkerhetsnivå 4.

Nedenfor oppstilles eksempler på krav til slike tiltak som virksomheten selv, og ikke sertifikatutsteder, må oppfylle. Sertifikatutsteder kan pålegge sertifikatinnehaver slike krav gjennom sertifikatpolicy. Kravene skal sikre at det angjeldende IT-systemet har tilstrekkelig sikkerhet mot kopiering og misbruk av sertifikatet, og at det er strengt kontrollert hvilke prosesser som har tilgang til virksomhetssertifikat (se eForvaltningsforskriften [3] § 21).

Eksempler på krav virksomheten selv må oppfylle:
Sertifikatinnehaver skal installere virksomhetssertifikat kun i IT-systemer som er under sertifikatinnehaverens kontroll.
Sertifikatinnehaver skal implementere tilstrekkelige mekanismer for å kontrollere tilgang til og bruk av private nøkler. Dette skal skje i henhold til sertifikatinnehavers dokumenterte sikkerhetsstrategi (se eForvaltningsforskriften § 21, punkt 1).
Sertifikatinnehaver skal logge all bruk av private nøkler, inkludert hvilken prosess som har initiert bruken (se eForvaltningsforskriften § 21, punkt 1).
Sertifikatinnehaver skal installere og beskytte private nøkler slik at bare autorisert personell kan administrere sertifikat og tilgang til private nøkler.
Med mindre private nøkler er lagret i elektroniske komponenter, skal lagring av private nøkler gjøres kryptert.
Med mindre private nøkler er lagret i elektroniske komponenter, skal det benyttes kryptering ved overføring av virksomhetssertifikat mellom IT-systemer hos sertifikatinnehaver.
Aktivering av private nøkler skal kreve bruk av aktiveringskode. Aktiveringskode kan gis ved oppstart av IT-system, ved pålogging av administrator, ved oppstart av prosess eller ved hver enkelt bruk. Aktiveringskode kan kun lagres (caches) tilknyttet IT-system eller prosesser dersom aktiveringskode er tilstrekkelig beskyttet mot kopiering eller misbruk.

Det fremgår av tabellen nedenfor hvordan sertifikatklassene Person-Høyt og Person-Standard tenkes brukt.

ANVENDELSER FOR SERTIFIKATKLASSER	**Autentisering**	**Signering (ikke-benektning)**	**Mottak av krypterte opplysninger**
Person-Høyt - oppfyller sikkerhetsnivå 4 i Rammeverk for autentisering og uavviselighet	Transaksjoner der det er behov for stor grad av sikkerhet om avsenders identitet, for eksempel i forbindelse med tilgang til særlig følsomme opplysninger, eller der skaden ved kompromittering er stor.	Transaksjoner der det er behov for stor grad av sikkerhet om koblingen mellom innhold og avsenders identitet, eller der skaden ved kompromittering av koblingen er stor.	Dokumenter osv. som inneholder særlig følsomme opplysninger, eller når skaden ved kompromittering er stor.
Person-Standard - oppfyller sikkerhetsnivå 3 i Rammeverk for autentisering og uavviselighet	Transaksjoner der det er behov for rimelig grad av sikkerhet om avsenders identitet, eller der skaden ved kompromittering er middels stor.	Transaksjoner der det er behov for rimelig grad av sikkerhet om koblingen mellom innhold og avsenders identitet, eller der skaden ved kompromittering av koblingen er middels stor.	Dokumenter osv. som ikke inneholder særlig følsomme opplysninger, og der skaden ved kompromittering ikke er stor.

Tabellen nedenfor viser sertifikatklassene med et utvalg egenskaper som må være oppfylt for de respektive klassene:

SERTIFIKAT KLASSE	Registrerings- og utleveringsprosedyre	Krav til navnestruktur og innhold	Krav til beskyttelse av private nøkler
Person-Høyt	Sertifikat med formål elektronisk signatur skal være et *kvalifisert sertifikat* og andre sertifikater skal være på samme kvalitetsnivå. Sertifikatutsteder skal oppfylle registrerings- og utleveringsprosedyrer som følger av dette, herunder bl.a. krav om personlig fremmøte.	Navnestruktur og sertifikatinnhold skal følge kravene i esignaturloven [2] § 4, med de presiseringer som følger av "Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater"[10].	Tilgang til private nøkler skal kreve minimum to-faktor autentisering, hvorav den ene faktoren er noe brukeren er i fysisk besittelse av. Brukeren skal godkjenne hver operasjon som involverer private nøkler ved å autentisere seg. Private nøkler må aldri finnes i klartekst i registre som kan kompromitteres eller på annen måte gi opphav til misbruk.
Person-Standard	Sertifikatutsteder skal oppfylle kravene i esignaturloven [2] §§ 10 til 16 samt forskrift om krav til utsteder av kvalifiserte sertifikater mv. [4] § 3. Det skal sikres en rimelig grad av trygghet for at utlevering av nøkler og/eller tilhørende tilgangskoder /passord og sertifikat skjer til riktig person. Utlevering skal enten skje ved utsendelse pr post til registrert adresse eller elektronisk utstedelse basert på eksisterende autentiseringsmekanisme, som gir minst like god trygghet for korrekt mottager som post til registrert adresse.	Sertifikatet skal oppfylle kravene til kvalifiserte sertifikater i esignaturloven [2] § 4 annet ledd bokstav b til j. Navnestruktur og sertifikatinnhold skal ellers følge "Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater" [10].	Tilgang til private nøkler skal kreve autentisering. Brukeren skal selv ha mulighet til å velge/ bestemme om hver operasjon som involverer private nøkler skal godkjennes. Private nøkler må minimum lagres kryptert.

SERTIFIKAT KLASSE	Registrerings- og utleveringsprosedyre	Krav til navnestruktur og innhold	Krav til beskyttelse av private nøkler
Virksomhet	Sertifikatutsteder skal oppfylle kravene i esignaturloven [2] §§ 10 til 16 samt forskrift om krav til utsteder av kvalifiserte sertifikater mv. [4] §§ 3 og 7. Det skal være mulig å entydig identifisere virksomheten ved at sertifikatet utstyres med organisasjonsnummer fra Enhetsregisteret i henhold til SEID sertifikatprofil [10]. Det skal sikres at utlevering av nøkler med tilhørende tilgangskoder/passord og sertifikat skjer til en person som har rett til å motta dette på vegne av virksomheten. (dette kan være for eksempel en person med fullmakt fra daglig leder, forretningsfører, innehaver eller tilsvarende kontaktperson i selskapet). Forholdet skal kunne dokumenteres. Virksomheten skal pålegges å loggføre hvilke personer eller prosesser som benytter sertifikatet.	Sertifikatet skal oppfylle kravene til kvalifiserte sertifikater i esignaturloven [2] § 4 annet ledd bokstav b til j. Navnestruktur og sertifikatinnhold skal følge "Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater" [10]. Sertifikatet skal inneholde virksomhetens organisasjonsnummer.	Det skal være mulig å realisere tilgangskontroll til private nøkler. Virksomheten skal selv ha mulighet til å velge/bestemme om hver operasjon som involverer private nøkler skal godkjennes. For virksomhetssertifikater som brukes av automatiserte prosesser skal det spesifiseres og kontrolleres hvilke prosesser som kan bruke private nøkler. Private nøkler må minimum lagres kryptert.

Denne kravspesifikasjonen bygger på disse sertifikatklassene og sikkerhetsnivåene. Dersom det ikke eksplisitt fremgår noe annet, gjelder kravene for alle sertifikatklasser.

Det er strengere sikkerhetskrav til løsninger med kvalifisert elektronisk signatur, se punkt 7.7. En kvalifisert signatur er ifølge esignaturloven en avansert signatur basert på et kvalifisert sertifikat og fremstilt av et godkjent sikkert signaturfremstillingssystem. Et godkjent sikkert signaturfremstillingssystem må enten være godkjent av et utpekt norsk organ eller godkjent av et tilsvarende organ utpekt i et annet EØS-land, eller så må signaturfremstillingssystemet være i samsvar med standarder utpekt av EU Kommisjonen. Kommisjonen har utpekt standarden CWA 14169 [j] som krav til sikre signaturfremstillingssystem.

Kravspesifikasjonen viser til krav i esignaturloven og forskrift om krav til utsteder av kvalifiserte sertifikater mv. som også gjelder for Person-Standard og Virksomhet. Kravene i esignaturloven – med unntak av kravene i lovens §§ 6 og 7 – gjelder i utgangspunktet kun for *kvalifiserte sertifikater* (dvs. Person-Høyt) og først og fremst for *utstedere* av kvalifiserte sertifikater. Selv om denne kravspesifikasjonen viser til krav i esignaturloven med forskrift for Person-Standard og Virksomhet, vil kravene hovedsaklig ha en avtalerettslig virkning. Esignaturlovens regler om tvangsmulkt i § 20 kommer til anvendelse ved uriktig erklæring om selvdeklarering. Tilsynet kan ilegge tvangsmulkt med hjemmel i selvdeklarasjonsforskriften § 13, jf. esignaturloven §§ 16a og 20.

2.3 Forklaring til inndelingen av krav

Kravspesifikasjonens inndeling og grupperingen av krav er basert på en tjenesteorientert tilnærming. Denne inndelingen skal legge til rette for at sertifikatutstedere kan selvdeklarere seg med de tjenester som støttes av de aktuelle sertifikatene, og at offentlige etater enkelt skal kunne sette sammen kravene til de tjenester de har behov for. Ved anskaffelsen kan etaten benytte et skjema hvor de fyller ut hvilke bruksområder og tjenester de ønsker. Samme skjema kan sertifikatutstederne fylle ut for, på en lettfattelig måte, å vise hvilke tjenester de tilbyr. Nedenfor følger en forenklet tabell for hvilke sertifikatklasser og tilhørende bruksområder og tjenester som etterspørres, og henvisning til hvor i kravspesifikasjonen kravene til tjenestene fremgår. Det må fylles ut en tabell for hver av sertifikatklassene.

Sertifikatklasse	**Bruksområde**	**Tjenester**	**Krav**
[ ] Person-Standard *eller* [ ] Person-Høyt *eller* [ ] Virksomhet	[ ] Autentisering [ ] Signering [ ] Kryptering	**[ ] Basis sertifikattjenester** [ ] Vedlikehold og tilbakekalling [ ] Brukerstøtte [ ] RA for norske borgere [ ] RA for utenlandske personer [ ] RA for virksomhetssertifikat **[ ] Katalog- og oppslagstjenester** **[ ] Autentiseringstjenester** [ ] Kanalsikkerhet **[ ] Signeringstjenester** [ ] Brukerdialog - brukskvalitet **[ ] Krypteringstjenester** **[ ] Kvalifisert signatur** [ ] Langtidslagring utover 10 år [ ] Tidsstempling	Kap. 4 og 5 Kap. 4.8 Kap. 4.9 Kap. 4.5.1 og 4.5.2 Kap. 4.6 Kap. 4.5.3 Kap. 5 Kap. 6 Kap. 6 Kap. 7 Kap. 7.5 Kap. 4.4 og 8 Kap. 7.6 Kap. 9.2 Kap. 9.1

Sertifikatutstedere må levere basis sertifikattjenester for bruksområdene autentisering og signering. Sertifikatutsteder kan velge hvorvidt de vil levere sertifikater for bruksområdet kryptering og hvilke tjenester de vil selvdeklarere seg for. Bruksområdet kryptering og det valgte settet av tjenester omtales som *Valgfritt* under punkt 2.4. Dersom sertifikatutstederens løsning er organisert slik at det *må* benyttes autentiserings-, signerings-, og/eller meldingskrypteringstjenester fra sertifikatutstederen selv, må også disse tjenestene selvdeklareres. Det er viktig å merke seg at en basis eID/sertifikattjeneste må ligge til grunn, uansett om denne leveres av samme sertifikatutsteder som for en deltjeneste, eller av en annen leverandør. Det er mulig, dersom en leverandør ønsker det, å selvdeklarere seg kun for en eller flere av tjenestene i tredje kolonne (eller funksjonalitet for å realisere en slik tjeneste). Dette forutsetter at disse deklareres med referanse til en eller flere basis sertifikattjenester som tjenesten støtter. ”Leverandøren” vil i denne forstand være en tilbyder av andre tjenester relatert til elektronisk signatur som omfattes av begrepet ”sertifikatutsteder” slik dette er definert i esignaturloven § 3 nr. 10.

Hovedtyngden av kravene er samlet i kapitlene 4 og 5, som omhandler basis sertifikattjenester, og som utgjør den grunnleggende tjenesten for levering av eID. Her er det samlet krav som dekker registrering og nødvendig legitimasjonskontroll av sertifikatinnehaver, fremstilling og forvaltning av sertifikatet, og krav til etablering av katalog- og statustjenester. Tjenester for *tilgang* til katalog- og statustjenester skal leveres av sertifikatutstederen. Enkelte av tjenestene kan i tillegg leveres av andre.

Krav til tjenester som *muliggjør* autentisering, signering og/eller kryptering er beskrevet i separate kapitler som egne tjenestekategorier.

Inndelingen av kravsett er som følger:

- **Krav til basis eID/sertifikattjeneste**
  Krav som dekker registrering av sertifikatinnehaver, fremstilling og forvaltning av sertifikatet og krav til etablering av kataloger og statustjenester.
- **Krav til katalog og oppslagstjenester**
  Krav som dekker hvordan man får tilgang til sertifikatinformasjon og hva det gis tilgang til av informasjon.
- **Krav til autentisering**
  Krav som dekker autentiseringsfunksjonalitet og hvordan autentisering kan bidra til å realisere informasjonssikring i form av kanalsikkerhet.
- **Krav til signeringstjenester**
  Krav til bl.a. avansert- og kvalifisert signatur.
- **Krav til kryptering**
  Krav til meldingskryptering
- **Krav til tilleggstjenester**

Kravene for basis sertifikattjenester vil altså dekke alle krav knyttet til fremstilling av selve sertifikatet, men også krav bl.a. om at utsteder *har tilgjengelig* katalog og statusinformasjon for sertifikatene. De detaljerte kravene til *hvordan* man får tilgang til informasjonen, og *hva* man får tilgang til vil imidlertid fremgå under kapittelet om katalog og oppslagstjenester.

2.4 Forklaring til kravtabellen

I de påfølgende kapitler er det benyttet tabeller med nummererte krav.
I disse tabellene inngår en kolonne for kategorier (Kat) hvor det benyttes følgende koder:

A:	Absolutt krav	- betyr at kravet skal tilfredsstilles.
B:	Betinget krav	- betyr at kravet bør tilfredsstilles.
V:	Valgfritt krav	- benyttes om bruksområde og tjenester som sertifikatutsteder ikke må levere, men som de kan velge hvorvidt de ønsker å selvdeklarere seg for.

Koden *Valgfritt krav* brukes om bruksområdet meldingskryptering og om tjenester som sertifikatutstederne selv velger hvorvidt de ønsker å tilby og selvdeklarere seg for. Dette er tjenester som brukerstedene også kan tilby selv eller som de kan velge å anskaffe fra andre sertifikatutstedere/leverandører. Andre leverandører kan velge å selvdeklarere seg for disse tjenestene, men det er altså valgfritt, se punkt 2.3.

Videre er det en egen kolonne "Svar fra leverandør". I denne kolonnen skal sertifikatutstederen fylle inn:

J:	Ja	- Betyr at kravet er oppfylt (og at løsningen inngår i tilbudets/kontraktens pris).
N:	Nei	- Betyr at kravet ikke er oppfylt.
F:	Forbehold	Her skal det gis et nummer som refererer til en spesifikk beskrivelse av forbeholdet. Det skal fylles inn "**NA"** i denne kolonnen dersom kravet ikke er relevant for leveransen.

For krav merket som V (Valgfritt), betyr:

J:	Ja	- At sertifikatutstederen tilbyr bruksområdet eller tjenesten.

3. BEGREPSAVKLARINGER, FORKORTELSER OG REFERANSER

3.1 Begrepsavklaringer

Autentisering	Autentisering er å verifisere påstått identitet. Autentisering kan baseres på forskjellige autentiseringsfaktorer.
D-nummer	Når en innvandret person skal få tildelt fødselsnummer, gis det ofte først et midlertidig D-nummer. For utlendinger som har lovlig opphold i Norge, brukes dette i forbindelse med skatt og offentlige tjenester. D-nummeret er ellevesifret, og består av modifisert fødselsdato og et femsifret nummer. Fødselsdatoen modifiseres ved at det legges til 4 på det første sifferet: En person født 1. januar 1980 får dermed 410180, mens en som er født 31. januar 1980 får 710180. Det femsifrede tallet gis ikke i serier, men tildeles fortløpende.
eID, elektronisk ID	En PKI-basert eID består av ett eller flere sertifikater med tilhørende private nøkler, der sertifikatene er utstedt samlet og identifiserer samme sertifikatinnehaver. Dersom det er flere sertifikater/nøkkelpar, vil disse ha forskjellige bruksområder

	(autentisering, signering eller kryptering).
Fødselsnummer	Et fødselsnummer er et ellevesifret registreringsnummer som tildeles av den norske stat til alle landets innbyggere. De seks første sifrene angir fødselsdato og de fem siste utgjør personnummeret. Fødselsnummeret er en unik identifikasjon av en enkeltperson. For tilgang til tjenester er fødselsnummer å betrakte som et navn og ikke et passord – det skal aldri gis tilgang til tjenester basert på bare kjennskap til fødselsnummer. Alle som er bosatt i Norge og innført i Folkeregisteret, har enten et fødselsnummer eller et D-nummer. Ifølge personopplysningsloven kan fødselsnummer kun brukes når det er saklig behov og når det er umulig å oppnå tilfredsstillende identifikasjon ved bruk av andre metoder, som for eksempel navn, adresse, fødselsdato, medlems- eller kundenummer.
Integrasjonspakke	En programvaremodul, som kan kalles av applikasjoner for å utføre funksjonalitet knyttet til elektronisk ID og e-signatur.
Katalogtjeneste	I PKI-sammenheng vil katalogtjenesten systematisere, oppbevare og gjøre tilgjengelig sertifikater, CRL-er og eventuelt annen informasjon fra en sertifikatutsteder.
Kryptering	En prosess som fører til forvrenging av innholdet i et dokument eller annet datagrunnlag slik at bare bestemte mottakere kan få det fram og lese det. Normalt skjer kryptering i henhold til faste algoritmer der egne parametere, krypteringsnøkkel og dekrypteringsnøkkel, er bestemmer hvordan innholdet forvrenges og bringes tilbake til klartekst. For symmetriske algoritmer er krypteringsnøkkel og dekrypteringsnøkkel den samme. For offentlig-nøkkel algoritmer, kan innhold som er kryptert med offentlig nøkkel dekrypteres med tilsvarende privat nøkkel[1], og omvendt. Krypteringsnøkler kan være forhåndsavtalt eller utveksles gjennom en protokoll mellom sender og mottakere.
Kanalsikkerhet	Kanalsikring ved oppsett av en sikker kommunikasjonskanal tilbyr kryptering og integritetsbeskyttelse av innhold mellom endepunktene for kanalen. Utenom endepunktene i begge ender er innholdet i ubeskyttet klartekst. Konfidensialitetssikring kan realiseres gjennom at Sluttbrukeren autentiserer seg over en kryptert kommunikasjonskanal og at meldinger deretter transporteres over kanalen.
Meldingskryptering	Metode for sikring av konfidensialitet hvor meldinger krypteres av senderen ved ”point of origin” og kun kan dekrypteres av den tiltenkte mottageren. Meldingskryptering, slik begrepet benyttes i dette dokumentet, realiseres ved at det krypteres en melding til sertifikatinnehaver, det vil si *innehaveren av et krypteringssertifikat og tilhørende dekrypteringsnøkkel*. Der hvor dette dokumentet kun bruker begrepet ”kryptering”, skal dette forstås som meldingskryptering.
Organisasjonsnummer	Ni sifre som ikke er informasjonsbærende, og som identifiserer en registreringsenhet eller en underenhet i Enhetsregisteret.
Personsertifikat	Et sertifikat hvor sertifikatinnehaver er en fysisk person
PKI	”Public Key Infrastructure” – infrastruktur for offentlig- nøkkel-

[1] Det finnes offentlig-nøkkel algoritmer som ikke støtter slik kryptering, men disse er ikke i vanlig bruk.

	kryptografi er en teknologi for å utstede, administrere og bruke elektronisk ID og e-signatur basert på en standardisert krypteringsteknologi.
Registreringsautoritet (RA)	Samler inn de data som er nødvendige i forbindelse med utstedelse av sertifikat. Registreringsautoriteten kontrollerer og verifiserer den kommende sertifikatinnehaverens identitet og formidler de nødvendige data til sertifikatutstederen.
Registrert adresse	Adresse registrert i Folkeregisteret.
Registreringsenhet i Enhetsregisteret	Juridisk person, enkeltpersonforetak eller annen enhet som registreres i Enhetsregisteret. For en registreringsenhet registreres det daglig leder, forretningsfører, innehaver eller tilsvarende kontaktperson i Enhetsregisteret.
Sertifikat	Et sertifikat er en kopling mellom en offentlig nøkkel, identifikasjon (navn) for sertifikatinnehaveren, og eventuelt annen informasjon. Ved signaturer er den offentlige nøkkelen signaturverifikasjonsdata, og navn i sertifikatet. Sertifikatet er signert av sertifikatutsteder, som med dette innestår for at sertifikatets innhold er korrekt.
Sertifikatinnehaver	Den personen som rettmessig disponerer et sertifikat, dvs. den som utpekes i sertifikatet som innehaver av den offentlige nøkkelen i sertifikatet, og som disponerer den private nøkkelen tilhørende sertifikatet.
Sertifikatmottaker	Den som forholder seg til innholdet i et sertifikat i forbindelse med autentisering, kryptering eller verifisering av signatur.
Sertifikatutsteder (CA)	En fysisk eller juridisk person som utsteder sertifikater (CA). I denne kravspesifikasjonen er sertifikatutsteder alltid en juridisk person.
Sertifiseringsordning	Enhver ordning der en tredjepart skriftlig bekrefter at en sertifikatutstеders produkter, prosesser eller tjenester oppfyller spesifiserte krav, og der sertifikatutsteder ikke er berettiget til å utøve de rettighetene som sertifiseringen gir før vedkommende har mottatt tredjeparts bekreftelse.
Standard	Dokument til felles og gjentatt bruk, fremkommet ved konsensus og vedtatt av et anerkjent organ, som gir regler eller retningslinjer for eller karakteristiske trekk ved aktiviteter eller resultantene av dem. Hensikten er å oppnå en optimal orden i en gitt sammenheng.
Særlig følsomme opplysninger	Opplysninger som er sensitive i henhold til personopplysningsloven og/eller oppfattes som særlig følsomme i henhold til annet regulativ/retningslinjer. Inkluderer virksomhetsopplysninger av særlig sensitiv karakter.
Tjenesteeier	Virksomhet som er tilbyder av elektroniske tjenester. Dette inkluderer tjenester på web, virksomhet med integrasjon av elektronisk meldingsutveksling i interne systemer eller der standard e-post brukes til slik utveksling.
Underenhet	Bedrift m.v. som tildeles eget organisasjonsnummer og registreres i Enhetsregisteret. For en underenhet registreres det ikke daglig leder, forretningsfører, innehaver eller tilsvarende kontaktperson, men det registreres knytning til en overordnet registreringsenhet i Enhetsregisteret.
Valideringstjeneste	Forsvarlig bruk av eID forutsetter at tjenesteeier har forvisset seg

	om at sertifikatet er egnet for den aktuelle bruk, og at det ikke er trukket tilbake. På grunn av de praktiske vanskeligheter med å innhente den nødvendige informasjon om sertifikattjenestens egnethet for tjenesteeiers formål, kan det være behov for en valideringstjeneste som på sertifikatmottakers (tjenesteeiers) vegne utfører oppgaven.
Virksomhetssertifikat	Sertifikat som identifiserer en registreringsenhet eller en underenhet i Enhetsregisteret. Videre i dette dokumentet benyttes virksomhet som fellesbegrep for registreringsenhet og underenhet.

3.2 Forkortelser

CA	Certification Authority (Sertifikatutsteder)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List (Tilbakekallingsliste)
CWA	CEN Workshop Agreement
ETSI	European Telecommunications Standards Institute
J2EE	Java 2 Platform, Enterprise Edition (Programmeringsstandard)
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
LRA	Lokal RegistreringsAutoritet
NCP	Normalized Certificate Policy
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PKI	Public Key Infrastructure (Infrastruktur for offentlige nøkler)
PKCS	Public Key Cryptography Standard
QCP	Qualified Certificate Policy
RA	RegistreringsAutoritet
RFC	Request For Comment (dokumentserie med spesifikasjoner fra IETF, noen RFC dokumenter har status som ”Internet standard”)
RSA	Rivest, Shamir and Adleman (offentlig-nøkkel krypto algoritme)
SEID	Samarbeid om elektronisk ID og signatur
S/MIME	Secure/Multipurpose Internet Mail Extension (Protokoll for sikker E-Post)
SSL	Secure Socket Layer (protokoll for sikker kommunikasjons, brukes bl.a. for web tjenester over https)
TLS	Transport Layer Security (protokoll for sikker kommunikasjonskanal, videreutvikling av SSL)
TS	Technical Specification
TSA	Tiltrodd ekstern tidsstemplingstjeneste (I henhold til ETSI TS 102 023 er en TSA å betrakte som en ”certification service provider”.)

3.3 Refererte standarder

Den sist oppdaterte versjonen av standardene skal gjelde for denne kravspesifikasjonen.

[a] ETSI TS 101 456 – Policy requirements for certification authorities issuing qualified certificates
[b] ETSI TS 102 042 - Policy requirements for certifications authorities issuing public key certificates
[c] ETSI TS 101 733 - Electronic Signature Formats
[d] ETSI TS 101 903 - XML Advanced Electronic Signatures (XAdES)
[e] PKCS #7 –The cryptographic message syntax standard
[f] X.509 - The Directory: Public-key and attribute certificate frameworks
[g] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[h] RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
[i] RFC 3629 – UTF-8 – a transformation format of ISO 10646
[j] CWA 14169 – Secure Signature-Creation Devices
[k] CWA 14170 – Security Requirements for Signature Creation Systems
[l] CWA 14171 – Procedures for Electronic Signature Verification
[m] PKCS #11 – Cryptographic Token Interface Standard
[n] CMS – Certificate Management Messages (RFC 2797)
[o] AICPA/CICA – WebTrust Program for Certification Authorities
[p] FIPS PUB 140-2 (2001) – Security Requirements for Cryptographic Modules
[q] ISO/IEC 27001:2005 Information technology – Security techniques – information security management systems – Requirements
[r] RFC 1777 - Lightweight Directory Access Protocol
[s] ETSI TS 102 176-1 – Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash Functions and Asymmetric Algorithms
[t] RFC 5246 -The Transport Layer Security (TLS) Protocol
[u] RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
[v] ETSI TS 102 023 - Policy Requirements for Time-Stamping Authorities (TSAs)

3.4 Refererte dokumenter

[1] NOU 2001:10 Uten penn og blekk
[2] Lov 15. juni 2001 nr. 81 om elektronisk signatur (esignaturloven)
[3] Forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
[4] Forskrift 15. juni 2001 nr. 611 om krav til utsteder av kvalifiserte sertifikater mv.
[5] Europaparlaments- og rådsdirektiv 1999/93/EF av 13. desember 1999 om en fellesskapsramme for elektroniske signaturer
[6] Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).
[7] Forskrift 15. desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften)
[8] Lov 6. mars 2009 nr. 11 om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven)
[9] Forskrift 13. mars 2009 nr. 302 om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsforskriften)
[10] SEID-prosjektet, Anbefalte sertifikatprofiler for personsertifikater

og virksomhetssertifikater, versjon 1.01, september 2004.
[11] SEID-prosjektet, Grensesnitt for tilgang til Oppslagstjenester, (godkjent desember 2004)
[12] Forskrift 21. november 2005 nr. 1296 om frivillige selvdeklarasjonsordninger for sertifikatutstedere.
[13] Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. Retningslinjer fra Fornyings- og administrasjonsdepartementet, april 2008.
[14] Forskrift 9. november 2007 nr. 1268 om folkeregistrering.
[15] Lov 20. juni 2008 nr. 42 om forbud mot diskriminering på grunnlag av nedsatt funksjonsevne (diskriminerings- og tilgjengelighetsloven)
[16] Referansekatalog for IT-standarder i offentlig sektor, versjon 2.0, 25.6.2009.

4. KRAV TIL BASIS SERTIFIKATTJENESTER

En eID består av ett eller flere sertifikater med tilhørende private nøkler, der sertifikatene er utstedt samlet og identifiserer samme sertifikatinnehaver. Dersom det er flere sertifikater/nøkkelpar, vil disse ha forskjellige bruksområder (autentisering, signering, kryptering). En eID bør for brukeren framstå som en enhet. Det vil si at brukeren ikke aktivt trenger å velge hvilket sertifikat eller hvilken nøkkel som skal brukes for en gitt operasjon. For utstedelse av eID vil det imidlertid kunne være noe forskjellige krav til sertifikater for ulike formål. Denne kravspesifikasjonen inneholder derfor både overordnede krav til eID og spesifikke krav for sertifikater for forskjellige bruksområder.

4.1 Sertifikater, bruksområder og sertifikatpolicy

En eID består av ett eller flere sertifikater og nøkkelpar med forskjellige bruksområder. Denne kravspesifikasjonen gjelder tre bruksområder: Autentisering, signering og kryptering.

Følgende anbefalinger gis:

- Det er sterkt anbefalt å tilby alle tre bruksområder, men en eID som kun tilbyr autentisering og signering, kan selvdeklareres. Flere anvendelser for kommunikasjon med og i offentlig sektor vil imidlertid trenge meldingskryptering, og en eID som ikke støtter kryptering, kan ikke brukes for slike anvendelser.
- Det er sterkt anbefalt å ha separate nøkkelpar og sertifikater for hvert bruksområde. I noen land i Europa er det et absolutt krav for kvalifiserte sertifikater at bruksområdet elektronisk signatur skal ha et eget sertifikat/nøkkelpar. Det er sikkerhetsmessige årsaker til at også bruksområdet kryptering bør ha et eget sertifikat/nøkkelpar. Kravspesifikasjonen forholder seg imidlertid til SEID-prosjektets anbefalte sertifikatprofiler [10] som tillater sertifikater og nøkkelpar som dekker flere bruksområder.
- Det er sterkt anbefalt at eID-er skal være tilgjengelig over åpne, standardiserte grensesnitt for bruk med tredjeparts programvare og til standard protokoller som TLS/SSL og S/MIME e-post. Det er likevel mulig å selvdeklarere løsninger med begrensinger i tilgang og anvendelsesområder. Dette kan bli innskjerpet i framtidige versjoner av kravspesifikasjonen.

4.1.1 Generelle krav, alle sertifikattyper

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
4.1.1.1	**Sertifikat med bruksområde autentisering** eID skal inneholde sertifikat og nøkkelpar med formål autentisering (key usage ”digital signature”).	A			
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”).	A			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
4.1.1.3	**Sertifikat med bruksområde kryptering** eID skal inneholde sertifikat og nøkkelpar som kan brukes til meldingskryptering (key usage ”key encipherment” eventuelt også ”key agreement” og/eller ”data encipherment”).	B			
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.	A			
4.1.1.5	**Separering av bruksområder** Bruksområdene autentisering, signatur og kryptering skal ha separate sertifikater og nøkkelpar.	B			
4.1.1.6	**Bruk til autentisering i TLS/SSL** eID skal kunne brukes til brukersideautentisering i TLS/SSL-protokollen [t] (extended key usage ”client authentication”).	B			
4.1.1.7	**Bruk til sikring av epost** eID skal kunne brukes til sikring av epost (extended key usage ”email protection” satt i relevante sertifikater, eventuelt også e-postadresse inkludert i relevante sertifikater).	B			
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[2]: • 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[3]. Eventuelle felter, attributter og utvidelser (extensions), som er med i sertifikatet, men ikke er spesifisert i [10], skal spesifiseres.	A			
4.1.1.9	**Tegnsett for navn i sertifikater** Navn i sertifikater (utstedernavn og navn for sertifikatinnehaver) skal kodes med UTF-8 tegnsett [i].	A			
4.1.1.10	**Begrensninger knyttet til sertifikatinnehaver** Eventuelle restriksjoner (eksempelvis alder eller oppføring i	A			

[2] Begrunnelsen for avvikene er at denne kravspesifikasjonen ikke skal *hindre* en sertifikatutsteder i å utstede sertifikater internasjonalt etter samme policy som benyttes for norsk personsertifikat eller virksomhetssertifikat. Dette innebærer *ikke* noe krav om å skulle tilby sertifikater til andre enn sertifikatinnehavere registrert i Norge.

[3] Det anbefales å bruke REID (Registered Entity ID) for organisasjonsnummer for virksomheter i dette tilfellet da dette gir en unik identifikator også internasjonalt. Se http://www.brreg.no/porvoo13/documents/reid_unique_company_identifier.pdf.

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
	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.	A			

4.1.2 Tilleggskrav for Person-Høyt

For Person-Høyt gjelder følgende krav til sertifikatpolicy:

- Et sertifikat som inneholder bruksområdet elektronisk signatur, *skal* være et kvalifisert sertifikat, og merkes som dette.
- Sertifikater som ikke innholder dette bruksområdet, *kan* merkes som kvalifisert sertifikat i henhold til SEID sertifikatprofil [10].

I en del europeiske land er EUs esignaturdirektiv [5] tolket slik at det *kun* er sertifikater med bruksområdet signatur som kan være kvalifiserte, og disse sertifikatene skal ikke ha andre bruksområder i tillegg. Denne tolkningen er akseptabel, og kravspesifikasjonen stiller derfor ikke krav om at andre sertifikater enn de med formål signering skal være kvalifiserte.

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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.	A			
4.1.2.2	**Kvalifiserte sertifikater** Det skal oppgis hvilke sertifikater i en eID som er merket som kvalifisert sertifikat.	A			
4.1.2.3	**Kvalifisert sertifikat for signering** Sertifikat som inneholder bruksområdet signering skal være et kvalifisert sertifikat og merkes som dette.	A			
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.	A			
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].	A			

4.1.3 Tilleggskrav for Person-Standard

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
4.1.3.1	**Sertifikatpolicy** Sertifikatpolicy for Person-Standard skal tilfredsstille kravene til LCP (Lightweight Certificate Policy) i ETSI TS 101 042 [b].	A			

4.1.4 Tilleggskrav for Virksomhetssertifikat

Nedenfor oppstilles krav til policy for virksomhetssertifikater. Som redegjort for under punkt 2.2 defineres A-kravene til virksomhetssertifikater å være på sikkerhetsnivå 3 Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor [13].

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
4.1.4.1	**Sertifikatpolicy** Sertifikatpolicy skal tilfredsstille kravene til NCP (Normalized Certificate Policy) i ETSI TS 101 042 [b].	A			
4.1.4.2	**Sertifikatpolicy, nøkkellagring i elektronisk komponent** Sertifikatpolicy skal tilfredsstille kravene til NCP+ (extended Normalized Certificate Policy) i ETSI TS 101 042 [b].	B			
4.1.4.3	**Disponering av virksomhetssertifikat** Sertifikatpolicy skal pålegge sertifikatinnehaver å loggføre hvilke personer (hvis sertifikat brukes under personlig kontroll) eller IT-systemer og prosesser som benytter virksomhetssertifikatet.	A			

4.2 Tilgang til sertifikatutsteders offentlige nøkler

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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.	A			
4.2.2	**Sertifisering for enkel tilgang til utstedersertifikater** Sertifikatutsteder skal være sertifisert etter Web Trust for Certification Authorities [o], eller ha samsvarserklæring med ETSI TS 101 456 [a] eller annen ordning som muliggjør spredning av utstedersertifikater i standarddistribusjoner av operativsystemer, nettlesere og annen programvare.	B			

4.3 Informasjonssikkerhet

4.3.1 Generelle krav, alle sertifikattyper

Det stilles ikke krav til at sertifikatutsteder skal være sertifisert etter utpekte standarder, men en sertifisering eller gjennomført tredjepartsrevisjon vil være en måte å dokumentere overfor tilsynet at sertifikatutstederen oppfyller kravene for selvdeklarasjonen.

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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.	A			
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.	A			
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.	A			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
4.3.1.4	**Sertifisering av styringssystem for informasjonssikkerhet** Sertifikatutsteders styringssystem for informasjonssikkerhet skal være sertifisert etter ISO/IEC 27001:2005 [q]. En sertifisering skal minimum omfatte organisasjon for operativ drift av maskin- og programvare for sertifikatutstedelse. Sertifikatutsteder skal kunne fremlegge gyldig ISO/IEC 27001 sertifikat.	B			
4.3.1.5	**Samsvarserklæring** Sertifikatutsteder skal fremlegge ekstern revisjonsrapport vedrørende oppfyllelse av krav til sertifikatpolicy på nivå QCP/QCP+ [b], eventuelt også NCP/NCP+ eller LCP [c]. Dokumentasjon av gjennomførte revisjoner skal ikke være eldre enn to år.	B			

4.4 Krav til kryptografi og kryptoutstyr

4.4.1 Generelle krav, alle sertifikattyper

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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.	A			
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.	A			
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.	A			
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].	A			
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.	A			

4.4.2 Tilleggskrav for Person-Høyt

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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).	A			
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).	A			
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.	A			

4.4.3 Tilleggskrav for Person-Standard

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
4.4.3.1	**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	A			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
	andre (for eksempel smartkort fra annen leverandør).				
4.4.3.2	**Kvalitet på kryptoutstyr** Utstyr for generering og lagring/bruk av sertifikatutsteders egne, private nøkler skal oppfylle krav til FIPS PUB 140-2 [p] nivå 2 eller høyere eller tilsvarende standarder (se ETSI TS 102 042 [b] avsnitt 7.2.1 og 7.2.2).	A			
4.4.3.3	**Beskyttelse av sertifikatinnehavers private nøkler** Tilgang til private nøkler skal kreve autentisering (oppfylt ved pålogging til IT-system). Brukeren skal selv ha mulighet til å velge/bestemme om hver operasjon som involverer private nøkler, skal godkjennes. Private nøkler må minimum lagres kryptert.	A			

4.4.4 Tilleggskrav for Virksomhet

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
4.4.4.1	**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).	A			
4.4.4.2	**Kvalitet på kryptoutstyr** Følgende utstyr skal oppfylle krav til FIPS PUB 140-2 [p] nivå 3 eller høyere, eller tilsvarende standarder (se ETSI TS 102 042 [b] 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 elektronikkomponent for lagring av sertifikatinnehaverens private nøkler (for eksempel nøkler som genereres i spesielt utstyr, og så skrives til smartkort).	A			

4.5 RA-tjenester

Sertifikatutsteder har ansvaret for at RA-tjenester og utstedelsesprosess for sertifikater utføres etter kravene til angjeldende sertifikatklasse, også der sertifikatutsteder benytter underleverandører til RA-tjenester.

4.5.1 RA-tjeneste for Person-Høyt sertifikater

Sertifikatutsteder er ansvarlig for at det tilbys RA-tjenester som etablerer tilstrekkelig tiltro til sertifikatinnehavers identitet, jf. esignaturloven [2] med forskrift [4]. Det er vesentlig at enhver kontakt med sertifikatsøkere som krever fysisk tilstedeværelse, kan utføres i tilstrekkelig geografisk nærhet til sertifikatsøkeren slik at prosessen med å skaffe til veie sertifikatet ikke oppfattes som en unødvendig stor hindring.

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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.	A			
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].	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.	A			
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	A			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
	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.	A			
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]	A			
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.	A			
4.5.1.8	**Validering mot Folkeregisteret** For personer som er registrert i Folkeregisteret, skal opplysninger kunne valideres mot Folkeregisteret.	A			

4.5.2 RA-tjeneste for Person-Standard sertifikater

Utstedelse av Person-Standard sertifikater krever ikke personlig oppmøte. Utstedelse kan derfor foregå basert på andre mekanismer for å sikre at sertifikatet utstedes til riktig person. Dette kan være basert på allerede etablerte kundeforhold med mottaker, utsendelse til registrert adresse i Folkeregisteret, utsendelse av aktiveringsdata til registrert mobiltelefon og andre metoder som sertifikatutsteder anser å være tilstrekkelig for utstedelsesprosessen.

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
4.5.2.1	**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 nøkkelpar genereres, distribueres og installeres. • Hvordan registrering av sertifikatsøknad skjer, herunder hvordan personopplysninger kontrolleres, om det innhentes samtykke til offentliggjøring av sertifikat, og hvordan opplysninger lagres. • Rutine for utstedelse av sertifikater, herunder hvor og hvordan sertifikatsøkeren får utlevert sertifikat. Tid fra	A			

[4] For offentlige utstedere er det et lovarbeid i gang om offentlig utstedt eID.

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
	søknad er levert til sertifikat kan utleveres skal oppgis. Som eksempel kan utlevering skje ved utsendelse per post til registrert adresse i Folkeregisteret eller ved elektronisk utstedelse basert på eksisterende autentiseringsmekanisme, som gir minst like god trygghet for korrekt mottager som post til registrert adresse. 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.				
4.5.2.2	**Organisering av RA-tjenesten** RA-tjenesten skal organiseres i henhold til kravene til LCP i ETSI TS 102 042 [b].	A			
4.5.2.3	**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.	A			
4.5.2.4	**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, logisk og organisatorisk sikkerhet for RA.	A			
4.5.2.5	**Elektronisk registrering og distribusjon** Det skal angis om og i så fall beskrives hvordan leverandøren kan tilby en RA-tjeneste som baseres på gjenbruk av eksisterende autentiseringsløsninger.	A			

4.5.3 RA-tjeneste for Virksomhetssertifikater

Utstedelse er basert på personlig fremmøte av person med fullmakt ved førstegangs utstedelse.

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
4.5.3.1	**Dokumentasjon av registrering og utstedelsesprosess** For utstedelse av sertifikater skal minimum følgende beskrives, og det skal spesifiseres hvilke oppgaver som utføres av RA-	A			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
	rollen, og hvilke som utføres av sertifikatutsteder: • Hvor og hvordan nøkkelpar genereres, distribueres og installeres. • Hvordan registrering av sertifikatsøknad skjer, herunder hvordan personopplysninger kontrolleres, hvordan kontroll av mottakers autorisasjon til å motta sertifikatet (fullmakt) gjøres, og hvordan opplysninger lagres. • Rutine for utstedelse av sertifikater, herunder hvor og hvordan sertifikatsøker får utlevert sertifikat. Tid fra søknad er levert til sertifikat kan utleveres skal oppgis. Alle disse funksjonene skal være tilstrekkelig dekket i CP og CPS, og beskrivelsen kan derfor gis i form av disse.				
4.5.3.2	**Organisering av RA-tjenesten** RA-tjenesten skal organiseres i henhold til kravene til NCP i ETSI TS 102 042 [b].	A			
4.5.3.3	**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.	A			
4.5.3.4	**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, IT-messig og organisatorisk sikkerhet for RA.	A			
4.5.3.5	**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.	A			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
4.5.3.6	**Entydig identifisering av registreringsenhet (virksomhet).** Det skal være mulig å entydig identifisere en registreringsenhet. Dette skal sikres ved at sertifikatutsteder sikrer at utlevering av nøkler og sertifikat kun skjer til autorisert representant for sertifikatinnehaver (fullmakt fra daglig leder, forretningsfører, innehaver eller tilsvarende kontaktperson i selskapet)[5] og at sertifikatet utstyres med registreringsenhetens (virksomhetens) organisasjonsnummer fra Enhetsregisteret i henhold til "Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater" [10].	A			
4.5.3.7	**Entydig identifisering av underenhet** Det skal være mulig å entydig identifisere en underenhet. Dette skal sikres ved at sertifikatutsteder sikrer at utlevering av nøkler og sertifikat kun skjer til autorisert representant for sertifikatinnehaver (fullmakt fra daglig leder, forretningsfører, innehaver eller tilsvarende kontaktperson i overordnet registreringsenhet)[6] og at sertifikatet utstyres med underenhetens organisasjonsnummer fra Enhetsregisteret i henhold til "Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater" [10].	A			

4.6 RA-tjeneste for Personsertifikater for utenlandske personer

Sertifikatutsteder bør tilby en RA-tjeneste for utenlandske personer uten D-nummer for sertifikater av typen Person-Høyt og/eller Person-Standard som legger til rette for registrering av relevante opplysninger. Kravet tilrettelegger for implementering av tjenestedirektivets artikkel 6 pkt. 1a og artikkel 8 pkt. 1, ved at sertifikatutsteder kontrollerer og registrerer utenlandske sertifikatsøkere slik at registrerte opplysninger senere kan benyttes som grunnlag for en eventuell elektronisk rekvirering og utstedelse av D-nummer. RA-tjenesten kan, på sertifikatutsteders vegne, verifisere informasjon om den som bestiller sertifikat og kvalitetssikre informasjon som skal legges inn i sertifikatene.

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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.	V			
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	A			

[5] Dette kan begrenses til de personer/roller som er registrert i Enhetsregisteret.
[6] Dette kan begrenses til de personer/roller som er registrert i Enhetsregisteret.

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
	D-nummer i forskrift om folkeregistrering[14]. Innsamlede opplysninger skal oppbevares og slettes iht. bestemmelsene i hvitvaskingsloven § 22 og hvitvaskingsforskriften § 17.				

4.7 Krav til programvare

Sertifikatinnehavers tilgang til en eID krever normalt spesialtilpasset programvare, for eksempel drivere for smartkort og lesere og tilgang til datastrukturer på kortet. Programvare kan installeres permanent i sertifikatinnehavers systemer, eller det kan brukes løsninger basert på Java applets eller tilsvarende teknologier. Programvaren vil normalt tilby grensesnitt, fortrinnsvis som definert i åpne standarder, for integrasjon av PKI løsningene med applikasjoner som for eksempel e-post og nettleser for en sluttbruker, eller fagsystemer for en virksomhet.

4.7.1 Programvare hos sertifikatinnehaver

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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).	A			
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.	A			
4.7.1.3	**Støtte for "tynne klienter"** Løsningen skal kunne støtte bruk av "tynne klienter" (Citrix terminalserver og lignende) hos sertifikatinnehaver.	B			
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.	A			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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.	A			
4.7.1.6	**Integrasjon med tredjeparts programvare** Sertifikatutstederen skal tilby en eller flere løsninger som på en enkel måte gjør PKI-funksjonaliteten tilgjengelig for 3. parts programvare hos sertifikatinnehaveren. Løsningene skal støtte standard grensesnitt som PKCS#11 [m] og Microsoft CAPI. Det skal oppgis hvilke grensesnitt (standard eller ikke standard) som støttes. Systemkrav (operativsystemer som støttes mv.) for programvaren skal oppgis.	B			
4.7.1.7	**Vedlikehold av programvare** Prosedyrer for vedlikehold av programvare og oppdatering av installert programvare (der dette er relevant) skal beskrives.	A			
4.7.1.8	**Lisenser** Alle nødvendige lisenser for programvare med mer skal være dekket av sertifikatutstederens avtale med sertifikatinnehaver.	A			
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.	A			

4.7.2 Programvare hos sertifikatmottaker

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
4.7.2.1	**Sertifikatmottaker skal ikke trenge integrasjonspakke** En sertifikatmottaker skal kunne motta og behandle sertifikater uten annen tilrettelegging enn gjennom konfigurasjon av sine eksisterende systemer, for eksempel installasjon av sertifikatutsteders rotsertifikat og konfigurasjon av tilgang til OCSP-tjeneste og eventuelt tilgang til CRL og katalog.	B			
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).	A			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
	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.	A			
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.	A			
4.7.2.5	**Eksempelkode** Dersom integrasjonspakker tilbys skal det finnes kompilerbar eksempelkode som viser bruk av alle funksjoner i applikasjonens programmeringsspråk.	A			
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.	A			
4.7.2.7	**Lisenser for sluttbrukere** Dersom integrasjonspakker for sluttbrukere tilbys (for å muliggjøre at en innehaver av et personsertifikat også skal kunne ta rollen som sertifikatmottaker), skal lisenser være dekket av sertifikatutstederens avtale med sertifikatinnehaver.	B			

4.8 Vedlikehold og tilbakekalling av sertifikater

4.8.1 Generelle krav, alle sertifikattyper

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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	A			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
	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.	A			
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.	A			

4.8.2 Tilleggskrav for Virksomhet

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
4.8.2.1	**Tilbakekalling av virksomhetssertifikater** Sertifikatutsteder skal påse at endringer av en virksomhetens tilstand i Enhetsregisteret som påvirker virksomhetens virksomhetssertifikat, skal medføre tilbakekalling av virksomhetssertifikatet senest 10 virkedager etter innføringen i Enhetsregisteret. Som minimum gjelder dette ved: • Endringer i sertifikatinnehavers organisasjon, for eksempel som følge av nedleggelse. • Endring av knytning til overordnet registreringsenhet for virksomhetssertifikater som identifiserer underenheter.	A			

4.9 Brukerstøtte

Når ikke annet er spesifisert, menes med brukerstøtte assistanse til bruker av PKI tjenesten (sertifikatinnehaver).

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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.	A			
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.)	A			
4.9.3	**Utrykningstjeneste** Sertifikatutsteder skal tilby utrykningstjenester i tilknytning til brukerstøtte-tjenesten. Det skal spesifiseres hvilke områder slike tjenester tilbys for og hvilken Responstid som vil gjøres gjeldende. (Dette kravet gjelder brukerstøtte for sertifikatinnehaver, applikasjonsutvikler og drift.)	B			
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			

5. KRAV TIL OPPSLAGSTJENESTER OG KATALOG

5.1 Statustjenester og sertifikatkataloger

For å ta i bruk PKI-tjenestene er det nødvendig med statustjenester som svarer på om et sertifikat er tilbakekalt. Dette er tjenester som er tilgjengelig i sann tid fra sertifikatutsteder. Kravene i dette kapitlet inkluderer derfor ytelseskrav. Verdiene som er oppgitt i disse kravene, er normalt å betrakte som minimumsverdier. Andre ytelseskrav kan brukes ved konkrete anskaffelser basert på kravspesifikasjonen.

OCSP-tjeneste for sertifikatstatus er obligatorisk. Statustjeneste i form av CRL er sterkt anbefalt og kan bli gjort obligatorisk i framtidige versjoner av denne kravspesifikasjonen. Det er krav om at CRL skal utstedes, men ikke obligatorisk krav om publisering.

Det er i tillegg krav om oppslagstjeneste for fødselsnummer knyttet til personsertifikater.

Katalogtjeneste for publiserte sertifikater kan være ønskelig, og er anbefalt for sertifikater med bruksområdet kryptering.

Sertifikatutstederen skal beskrive hvordan katalogtjenestene er organisert og drevet og hvordan disse er tenkt levert, herunder minimum:

- Den aktuelle katalogstruktur samt hvilke søkeparametre som kan anvendes.
- Om det er etablert noen form for mekanisme for aksesskontroll og hvordan denne fungerer.

5.2 Statustjeneste ved CRL

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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.	A			
5.2.2	**Tilbakekallingslister – utstedelse ved tilbakekalling** Ved tilbakekalling av sertifikater skal dette medføre utstedelse av en oppdatert CRL uten ugrunnet opphold, men senest 3 timer etter at sertifikatutsteder fikk kunnskap om forholdet.	B			
5.2.3	**Publisering av tilbakekallingslister** Siste tilbakekallingsliste skal minimum være tilgjengelig over http og/eller ldap [r]. Eventuelt andre grensesnitt for tilgang skal spesifiseres.	B			
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.	A			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
5.2.5	**Ekstra distribusjonspunkter** I enkelte sammenhenger vil det være uhensiktsmessig å hente CRL fra en tjeneste på Internett. Sertifikatutsteder skal derfor kunne legge til rette for distribusjon av CRL fra flere distribusjonspunkter. (Merk at det ikke er krav om å publisere URI for slike alternative distribusjonspunkter i sertifikatene.)	B			
5.2.6	**Tilgjengelighet av statustjeneste ved CRL** Tjeneste for tilgang til CRL 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.	B			
5.2.7	**Ytelse for tilgang til statustjeneste ved CRL** Tiden det tar å laste ned en CRL er en funksjon av størrelsen av CRL og båndbredden på forbindelsen. Sertifikatutstederen skal beskrive hvordan CRLer er tilgjengeliggjort og godtgjøre at valgt løsning gir tilfredsstillende ytelse.	B			
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.	A			
5.2.9	**Arkivering av tilbakekallingslister for Person-Standard** Sertifikatutsteder skal arkivere utstedte CRLer i minst 10 år. Sertifikatutsteders rutiner for arkivering av CRLer skal beskrives.	B			

5.3 Statustjeneste ved OCSP

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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].	A			
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.	A			
5.3.3	**Ekstra aksesspunkter** I enkelte sammenhenger vil det være uhensiktsmessig å bruke en OCSP-tjeneste på Internett. Sertifikatutsteder skal derfor kunne legge til rette for alternative OCSP-tjenester. (Merk at det ikke er krav om å publisere URI for slike alternative tjenester i sertifikatene.)	B			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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.	A			
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.	A			
5.3.6	**Arkivering av OCSP-svar** Sertifikatutsteder skal arkivere alle OCSP-svar i minst 10 år. Sertifikatutsteders rutiner for arkivering av OCSP-svar skal beskrives.	B			

5.4 Tilgang til katalogtjenester

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
5.4	**Tilgang til katalogtjenester** Det skal angis om det leveres katalogtjenester. I så fall gjelder kravene nedenfor.	V			
5.4.1	**Sertifikatkatalog for utstedte sertifikater** Sertifikatutsteder skal tilby katalog over utstedte sertifikater. Katalogen skal være tilgjengelig ved hjelp av ldap v3[7] [r]. Spesifiser eventuelle andre grensesnitt til katalogen.	B			
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.	A			
5.4.3	**Ekstra distribusjonspunkter for katalog** I enkelte sammenhenger vil det være uhensiktsmessig med tilgang på katalog fra en tjeneste på Internett. Sertifikatutsteder skal derfor kunne legge til rette for katalogtilgang fra flere distribusjonspunkter.	B			
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).	A			
5.4.5	**Begrensninger i tilgang** Eventuelle begrensninger i tilgang til katalogen skal oppgis. Dersom det er begrensninger på tilgang, skal metode for	A			

[7] Eller nyere versjoner når disse er allment brukt i markedet.

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
	tilgangskontroll til katalogen beskrives.				
5.4.6	**Kobling til organisasjonsnummer** For Virksomhetssertifikater skal det spesifiseres hvordan søk i katalogen kan vise kobling mellom sertifikat og organisasjonsnummer.	A			
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.	A			
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.	A			

5.5 Tilgang til oppslagstjenester

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 Oppslagstjenester”[11] samt at utlevering av fødselsnummer/D-nummer skal være i henhold til personopplysningsloven [6] § 12 og personopplysningsforskriften [7] § 10-2. Tjenesten skal beskrives.	A			
5.5.2	**Oppslagstjeneste for unik identifikator i sertifikat** Sertifikatutsteder skal tilby en tjeneste som gjør det mulig for autoriserte parter å knytte et fødselsnummer/D-nummer til et sertifikat, gjennom spørring på fødselsnummer og retur av enten sertifikat(er) eller unik identifikator som kodet i ”serialNumber” attributtet i sertifikatinnehaverens navn i sertifikatet.	B			

5.6 Felles tilgang til statustjenester

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
5.6.1	**Tilgang til sertifikatstatus** Det skal legges til rette for et felles punkt for tilgang til sertifikatstatusinformasjon (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.	A			

5.7 Vedlikehold av katalog og oppslagstjenester

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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.	A			
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. Sertifikatutstederen skal også tilby en varslingstjeneste for å varsle slike hendelser.	A			
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 kvalifiserte sertifikater § 3, jf. esignaturloven § 14.	A			

6. KRAV TIL AUTENTISERINGSTJENESTER

Autentiseringstjenester skal gjøre det mulig for sertifikatinnehaver å få tilgang til elektroniske tjenester ved bruk av PKI baserte teknikker. Tjenesteeier skal på sin side få verifisert brukerens identitet, med et spesifisert og forstått nivå av tiltro (autentisering).

PKI-basert autentisering foregår ved en protokoll der sertifikatinnehaveren signerer en utfordring fra motparten (for eksempel et tilfeldig tall sendt fra en Tjenesteeier) med privat nøkkel, og denne signaturen verifiseres med sertifikatet. Selv om en kan tenke seg at autentisering etterfølges av kommunikasjon over en åpen kanal, vil en i praksis alltid ønske å bruke en sikker kommunikasjonskanal dersom sikkerhetsbehovene krever en PKI-basert autentisering.

Sikker kommunikasjonskanal i denne sammenhengen etableres med TLS/SSL-protokollen. TLS/SSL krever autentisering av tjenersiden med SSL serversertifikat (dette er ikke dekket av denne kravspesifikasjonen), og en sikker kanal kan settes opp initiert av tjenersiden alene (ensidig TLS).

Autentisering også av brukersiden (tosidig TLS) er valgfritt i TLS/SSL protokollen. Det er sterkt anbefalt at eID skal kunne brukes til tosidig TLS. Dette gir høynet sikkerhet (bl.a. beskyttelse mot "mannen i midten angrep") siden begge ender autentiseres integrert med oppsettet av den sikre kommunikasjonskanalen. Scenarier for bruk er:

- Pålogging til en Tjenesteeier der personsertifikat (eller virksomhetssertifikat) brukes til TLS-brukerautentisering.
- Oppsett av sikker kommunikasjonskanal mellom IT-systemene til to virksomheter (privat-offentlig eller offentlig-offentlig) der "brukerautentisering" gjøres med virksomhetssertifikat.

For pålogging er et alternativt scenario, som dekkes av denne kravspesifikasjonen, at Tjenesteeier setter opp en ensidig TLS-kanal og at brukeren etterpå autentiseres gjennom en egen protokoll.

En sikker kommunikasjonskanal tilbyr konfidensialitet og integritetsbeskyttelse av innhold mellom endepunktene for kanalen. Utenom endepunktene i begge ender kan innholdet være i ubeskyttet klartekst. Dersom innholdet går gjennom en kjede av kanaler, vil innholdet være ubeskyttet i alle mellomliggende noder. Det er derfor viktig å vurdere når kanalsikkerhet med PKI-basert autentisering av bruker er tilstrekkelig, og når en har behov for ytterligere sikkerhetsmekanismer, dvs. meldingssikkerhet (meldingskryptering).

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
6.1	**Autentiseringstjenester** Det skal angis om det leveres autentiseringstjenester. I så fall gjelder kravene nedenfor.	V			
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.	A			
6.1.2	**Kanalbinding for autentisering** Dersom den PKI-baserte protokollen utføres etter oppsett av en (ensidig) TLS/SSL-kanal, skal det beskrives hvordan autentiseringen av sluttbruker koples til den sikre kanalen (hindre "man in the middle" angrep).	A			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
6.1.3	**Behov for spesiell programvare, sertifikatinnehaver** Dersom autentiseringsprotokollen medfører behov for installasjon av programvare i sertifikatinnehavers systemer, eventuelt bruk av Java applet eller tilsvarende teknologi, skal dette oppgis. Slik programvare skal ansees som en del av programvarepakker for å ta i bruk en eID, og skal være underlagt krav spesifisert i 4.8.1.	B			
6.1.4	**Behov for spesiell programvare, sertifikatmottaker** Dersom autentiseringsprotokollen medfører behov for installasjon av programvare i sertifikatmottakers systemer, eventuelt bruk av Java applet eller tilsvarende teknologi, skal dette oppgis. Slik programvare skal ansees som en del av programvarepakker for å ta i bruk en eID, og skal være underlagt krav spesifisert i 4.7.2.	B			

7. KRAV TIL SIGNERINGSTJENESTER

Avansert elektronisk signatur er en kryptografisk sjekksum over en avgrenset mengde data (melding, dokument), der:

- Sjekksummen lages ved hjelp av sertifikatinnehavers private nøkkel merket med bruksområdet signering
- Sjekksummen kan verifiseres ved bruk av sertifikatinnehavers tilsvarende offentlige nøkkel, og
- Resultatet pakkes som et signert dataobjekt (SDO).

Det er sterkt anbefalt at eID skal være tilgjengelig over åpne grensesnitt for integrasjon med tredjeparts programvare (se krav i 4.7.1). Dette kapitlet gir derfor generelle krav til signeringsapplikasjoner uavhengig av om applikasjonen er levert av sertifikatutsteder eller andre.

Tredjepartsleverandører av signeringsprogramvare *kan* selvdeklarere sin programvare i henhold til disse kravene.

Resultatet av en signeringsoperasjon skal være SDO på standardformat. Mottaker av SDO skal ikke trenge å installere spesifikk programvare for å håndtere verken SDO-formatet eller validering av sertifikater for signaturer.

7.1 Generelle signeringskrav

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
7.1	**Signeringstjenester** Det skal angis *om* sertifikatutstederen leverer signeringstjenester. I så fall gjelder relevante krav i dette kapittelet.	V			
7.1.1	**Støtte for standard signaturformater**	A			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
	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[8].				
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.	A			
7.1.3	**Sertifikater i SDO** SDO skal minimum inneholde sertifikatet til den som har signert, eventuelt alle sertifikater i sertifikatstien opp til rotsertifikatet.	A			
7.1.4	**Sertifikatutsteders programvare, sertifikatinnehaver** Hvis *sertifikatutsteder* leverer programvare eller tjeneste for signering (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.	B			
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).	A			
7.1.6	**Sertifikatutsteders programvare, sertifikatmottaker** Hvis *sertifikatutsteder* leverer programvare eller tjeneste for verifisering av et signert dokument (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 4.7.2. Merk at krav 7.1.5 sier at slik programvare ikke skal være nødvendig.	B			

[8] Merk at SEID signeringsformat og noen av formatene spesifisert i XAdES og CAdES er lagringsformater mer enn utvekslingsformater. Det er derfor mer aktuelt å bruke andre, basisformater for utveksling og heller bygge XAdES, CAdES eller SEID SDO på mottakersiden i forbindelse med arkivering.

7.2 Signeringskrav for Person-Høyt

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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.	A			
7.2.2	**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.	B			
7.2.3	**Signaturverifikasjon** Det skal dokumenteres hvorvidt løsninger for å framvise og verifisere signerte data samsvarer med krav i CWA 14171 [l].	B			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
	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.				

7.3 Signeringskrav for Person-Standard

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
7.3.1	**Bruk av privat nøkkel** Brukeren skal selv ha mulighet til å velge om hver operasjon som involverer bruk av privat signeringsnøkkel, skal godkjennes.	A			

7.4 Signeringskrav for Virksomhet

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
7.4.1	**Bruk av privat nøkkel** Ved signering av informasjon der bruk av privat nøkkel er kontrollert av en person, skal det sikres at sertifikatinnehaver må godkjenne hver operasjon som involverer bruk av privat nøkkel med PIN, passord eller tilsvarende.	A			

7.5 Brukskvalitet

Dersom løsningen inkluderer brukerdialoger, gjelder følgende krav:

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
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]	A			
7.5.2	**Språk**	A			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
	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.	A			
7.5.4	**Brukerveiledning** Det skal forefinnes veiledning av installasjon og bruk på norsk.	A			
7.5.5	**Tilpasning av brukerdialog** Brukerdialoger i forbindelse med signering skal kunne tilpasses. For eksempel kan den inneholde referanser til dokumentet som signeres.	B			
7.5.6	**Samsvar med grafisk profil** Det skal være mulig å tilpasse grafisk profil på autentiserings- og signeringsdialoger slik at de samsvarer med applikasjonens profil.	B			
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.	A			
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.	A			
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).	A			

7.6 Kvalifiserte signaturer

7.6	**Kvalifisert signatur** Det skal angis *om* sertifikatutstederen leverer kvalifiserte signaturer. I så fall gjelder kravene nedenfor.	V			
7.6.1	**Sikkert signaturframstillingssystem** Signaturframstillingssystem skal fylle kravene til sikkert signaturfremstillingssystem, jfr. esignaturloven § 9.	A			
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.	A			
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.	A			

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 [l]. 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.				

8. KRAV TIL MELDINGSKRYPTERING

I kravspesifikasjonen omhandles krav til to metoder for PKI-basert konfidensialitetssikring: Kanalsikring/kanalkryptering og meldingskryptering.

De to metodene kan begge dekke flere ulike behov og har også store forskjeller i måten løsningen implementeres på og hvilke tekniske egenskaper de har. For et gitt formål må det identifiseres behov og vurderes hvilken type løsning som er mest hensiktsmessig.

Dette kapitlet omhandler kun krav til meldingskryptering. (Krav i forbindelse med kanalkryptering er gitt i sammenheng med autentiseringsfunksjoner i kap. 6).

Meldingskryptering (også kalt ende-til-ende kryptering, dokumentkryptering eller permanent kryptering) beskriver en metode for sikring av konfidensialitet hvor meldinger krypteres av senderen ved ”point of origin” og kun kan dekrypteres av den tiltenkte mottageren. Meldingskryptering realiseres gjennom at senderen krypterer en melding ved hjelp av offentlig nøkkel fra mottakerens sertifikat (som må være merket slik at denne bruken er tillatt). Meldingen kan da kun dekrypteres av sertifikatinnehaveren ved bruk av den private dekrypteringsnøkkelen tilsvarende sertifikatet som ble brukt. Meldingen er kryptert ikke bare ved overføring over nettverk, men også under lagring i mellomliggende systemer.

De fleste offentlige virksomheter behandler i en eller flere deler av sin virksomhet personopplysninger og/eller taushetsbelagte opplysninger. Behandling av slike opplysninger omfattes av taushetsplikten i forvaltningsloven, unntaksbestemmelser i offentlighetsloven, bestemmelser i personopplysningsloven og bestemmelser i andre lover. Når slike opplysninger overføres elektronisk kan det være behov for å sikre konfidensialitet ved hjelp av meldingskryptering.

Det er valgfritt hvorvidt meldingskryptering leveres etter denne kravspesifikasjonen. Anvendelser som krever meldingskryptering, vil ikke kunne ta i bruk eID-er som ikke støtter disse kravene.

Programvare for kryptering og dekryptering kan leveres av sertifikatutsteder (eventuelt med samarbeidspartnere) eller av tredjeparts programvareleverandører.

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
8.1	**Meldingskryptering** Det skal angis om sertifikatutsteder leverer eID som kan brukes til meldingskryptering. I så fall gjelder kravene nedenfor.	V			
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.	A			
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.	A			
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.	A			

8.1.4	**Kryptert e-post** Det skal være mulig å bruke eID til kryptering (sertifikat) og dekryptering (privat nøkkel) av e-post på S/MIME v3 format. Eventuelle begrensninger og forutsetninger for slik bruk skal oppgis.	B			
8.1.5	**Krav til kryptostyrke for symmetrisk krypto** Programvare for kryptering og dekryptering skal bruke NIST AES symmetrisk kryptoalgoritme med nøkkellengde minimum 128 bits. Merk at oppfyllelse av dette kravet i tredjeparts programvare er utenfor sertifikatutsteders kontroll.	B			

9. TILLEGGSTJENESTER

9.1 Tidsstempling

For løsninger som er avhengige av ”sterk” ikke-benekting, kan det være ønskelig med tidsstempling fra en tiltrodd, ekstern tidsstemplingstjeneste (TSA). I henhold til ETSI TS 102 023 [v] er en TSA å betrakte som en ”certification service provider” som definert i esignaturdirektivet [5]. Sertifikatutsteder kan levere en slik tjeneste som en tilleggstjeneste.

Det er også mulig for andre enn sertifikatutstedere å levere tidsstemplingstjenester. I tilfelle er anbefalt løsning at TSAens sertifikater utstedes av en sertifikatutsteder og helst med et separat tillitsanker (ref. krav 9.1.4).

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
9.1	**Tidsstempling** Det skal angis om det leveres tidsstemplingstjeneste. I så fall gjelder kravene nedenfor.	V			
9.1.1	**Grensesnitt mot tidsstemplingstjeneste** Grensesnitt mot tidsstemplingstjenesten skal være i henhold til TSP [u].	A			
9.1.2	**Policy for tidsstemplingstjeneste** Policy for tidsstemplingstjenesten skal være i overensstemmelse med ETSI TS 102 023 [v].	A			
9.1.3	**Sikkerhetsorganisasjon** Krav gitt i 4.3.1 i denne kravspesifikasjonen gjøres gjeldende.	A			
9.1.4	**Separat tillitsanker** TSA [v] skal ikke være underlagt samme rotsertifikat som noen sertifikatutsteder.	B			
9.1.5	**Tilgjengelighet av TSA-sertifikater** Aktuelle rotsertifikater og TSAens egne sertifikater skal være allment (åpent) tilgjengelige og distribueres på en sikker og tillitvekkende måte. Prosedyre for distribusjon skal dokumenteres.	A			

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
9.1.6	**TSAs sertifikat, format** Format på TSAs sertifikat skal spesifiseres. Sertifikatet skal støtte bruksområdet signering. Sertifikatet skal i tillegg være merket med extended key usage id-kp-timeStamping.	A			
9.1.7	**TSAs sertifikat som virksomhetssertifikat** TSAs sertifikat for signering av tidsstempler skal være et virksomhetssertifikat i henhold til denne kravspesifikasjonen.	B			
9.1.8	**Begrensning i anvendelse av TSAs sertifikat** TSAs sertifikat for signering av tidsstempler skal ikke brukes til andre formål.	A			
9.1.9	**Krav til kryptografi og kryptoutstyr** Krav gitt i avsnitt 4.4.1 og 4.4.2 i denne kravspesifikasjonen gjøres gjeldende. Det vil si at en TSA skal ha kryptosikkerhet tilsvarende en sertifikatutsteder på nivå Person-Høyt.	A			
9.1.10	**Nøyaktighet av tidsstempler** Tidsstempler skal ha en nøyaktighet på 1 sekund eller bedre. (Krav gitt av ETSI TS 102 023 [v].)	A			
9.1.11	**Nøyaktighet av klokker** Kilder for synkronisering av klokker og garantert nøyaktighet av klokker brukt i tjenesten skal oppgis.	A			
9.1.12	**Synkronisering mot Justervesenet** Alle klokker i systemet skal være synkronisert basert på tid fra Justervesenets Atomur eller ha tilsvarende nøyaktighet.	B			
9.1.13	**Validering over tid** Det skal sikres at tidsstempler skal kunne valideres i 10 år etter at tidsstemplet ble utstedt. Dette gjelder uavhengig av om tjenesten fortsatt er operativ på dette tidspunktet. Prosedyrer for å sikre dette skal beskrives.	A			

9.2 Langtidslagring utover 10 år

Krav nr	Kravbeskrivelse	Kat	Svar fra lev.		
			J	N	F
9.2	**Langtidslagring** Det skal angis om det leveres tjeneste for langtidslagring. I så fall gjelder kravene nedenfor.	V			
9.2.1	**Langtidslagring** Tilbakekallingslister skal oppbevares i minimum 30 år. Sertifikater skal oppbevares i minimum 30 år i tillegg til sertifikatets levetid.	A			
9.2.2	**Langtidslagring utover 30 år** Det skal være mulig å inngå avtale om lagring utover 30 år.	A			