

Høringsnotat

Innhold

Innledning.....	1
I Gjennomføringsrettsaktene	2
1. Forskrift om fastsettelse av saksbehandlingsregler for samarbeid mellom medlemsstatene om elektronisk identifikasjon	3
2. Forskrift om fastsettelse av spesifikasjoner for formater for avanserte elektroniske signaturer og avanserte segl, som skal anerkjennes av offentlige organer	4
3. Forskrift om fastsettelse av tekniske minstespesifikasjoner og minstekrav til framgangsmåter for sikkerhetsnivåene for elektroniske identifikasjonsmidler	4
4. Forskrift om rammen for samvirkingsevne	5
5. Forskrift om fastsettelse av vilkår, formater og framgangsmåter for melding	6
II Rammeverk for identifikasjon og sporbarhet.....	7
III Forslag til ny forskrift om selvdeklarasjonsordninger for elektroniske tillitstjenester	9

Innledning

Kommunal- og moderniseringsdepartementet sender med dette på høring forslag til forskrifter som implementerer vedtatte gjennomføringsrettsakter til Europaparlaments- og rådsforordning (EU) 910/2014 om elektronisk identifikasjon og elektroniske tillitstjenester for elektroniske transaksjoner på det indre marked (eIDAS-forordningen).

Prop 71 LS (2017-2018) med forslag til ny lov om elektroniske tillitstjenester og om opphevelse av direktiv 1999/93/EF¹, er vedtatt i Stortinget og ble sanksjonert i statsråd 15. juni 2018. Loven trådte i kraft samme dato. Loven gjennomfører eIDAS-forordningen.

Forordningen har som formål å legge til rette for økt elektronisk samhandling mellom næringsdrivende, borgere og offentlige myndigheter på tvers av landegrensene i EU/EØS og dermed sterkere økonomisk vekst i det indre marked. Reglene om elektronisk signatur styrkes og utvides, eID reguleres og også andre typer tillitstjenester omfattes. Forordningen er todelt og regulerer gjensidig aksept av løsninger for eID og gjensidig aksept av elektronisk signatur og andre tillitstjenester.

Europakommisjonen har siden våren 2014 utarbeidet gjennomføringsrettsakter som utfyller bestemmelsene i forordningen. Til å bistå i dette arbeidet har Kommisjonen etablert "eIDAS

¹ Europaparlaments- og rådsdirektiv 1999/93/EF om en felleskapsramme for elektroniske signaturer

Expert Group" der Norge har deltatt. Norge deltar også som observatør i "eIDAS Committee", som avgir vurdering av forslagene.

Myndighet til å fastsette forskrifter som gjennomfører rettsaktene om bruk av eID og tillitstjenester i offentlig sektor, er delegert til Kommunal- og moderniseringsdepartementet.

Departementet sender på denne bakgrunn gjennomføringsrettsaktene som er delegert til Kommunal- og departementsdepartementet på høring som utkast til forskrifter. Siden gjennomføringsrettsaktene allerede er vedtatt i EU gjennomføres høringen av disse hovedsakelig av informasjonshensyn. Alle rettsaktene er foreløpig ikke tatt inn i EØS-avtaleverket. Høringen gjennomføres derfor med forbehold om den videre EØS-prosessen.

Myndighet til å fastsette forskrifter som gjennomfører rettsaktene om tillitstjenester, er delegert til Nærings- og fiskeridepartementet som sender eget høringsnotat med forslag til forskrifter. Dersom det er ønskelig, kan høringsinstansene levere et samlet høringssvar til høringsnotatene. Høringsvaret sendes da begge departementene.

Gjennomføringsrettsaktene er vedlagt i uoffisiell norsk oversettelse.

eIDAS-forordningen påvirker det norske regimet for bruk av eID i offentlig sektor. Forordningen legger også rammene for bruk av eID og PKI i andre deler av samfunnet, ikke minst for finanssektoren. Bruk av eID i offentlig sektor reguleres i dag av Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor², Kravspesifikasjon for PKI i offentlig sektor³ og Forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere⁴ (selvdeklarasjonsforskriften). Som en følge av gjennomføringen av eIDAS-forordningen og opphevelse av e-signaturloven, vil det også være behov for å endre selvdeklarasjonsforskriften. Forslag til nytt rammeverk og forslag til ny selvdeklarasjonsforskrift sendes derfor på høring samtidig med gjennomføringsrettsaktene.

Høringsnotatet er todelt. Første del omhandler gjennomføringsrettsaktene til eIDAS-forordningen. Andre del omhandler forslag til Rammeverk for identifikasjon og sporbarhet samt forslag til ny forskrift om selvdeklarasjonsordninger for elektroniske tillitstjenester.

I Gjennomføringsrettsaktene

eIDAS-forordningen har som formål å skape et felles grunnlag for sikker elektronisk samhandling mellom borgere, virksomheter og offentlige myndigheter og dermed øke effektiviteten til offentlige og private nett-tjenester, elektronisk forretningsdrift og elektronisk handel i EU/EØS. Etter eIDAS-forordningens artikkel 12 (1) skal eID-ordninger som meldes i henhold til forordningens artikkel 9 (1) være interoperable. Videre fastsettes det i forordningens artikkel 12 (2) at det skal innføres en interoperabilitestramme som skal oppfylle visse kriterier som angis nærmere i artikkel 12 (3) og som skal omfatte nærmere

² <https://www.regjeringen.no/no/dokumenter/rammeverk-for-autentisering-og-uavviseli/id505958/>

³ <https://www.regjeringen.no/no/dokumenter/kravspesifikasjon-for-pki-i-offentlig-se/id611085/>

⁴ <https://lovdata.no/pro/#document/SF/forskrift/2005-11-21-1296>

bestemte opplysninger jf. artikkel 12 (4). Etter forordningens artikkel 12 (5) skal medlemslandene samarbeide om interoperabilitet mellom eID-ordningene som er meldt etter artikkel 9 (1) og eID-ordninger som medlemslandene har til hensikt å melde, samt om sikkerheten i eID-ordningene. Forordningens artikkel 12 (6) fastsetter nærmere hva samarbeidet skal omfatte.

1. Forskrift om fastsettelse av saksbehandlingsregler for samarbeid mellom medlemsstatene om elektronisk identifikasjon

Forskriften gjennomfører Kommisjonens gjennomføringsbeslutning (EU) 2015/296 av 24. februar 2015 om fastsettelse av saksbehandlingsregler for samarbeid mellom medlemsstatene om elektronisk identifikasjon i henhold til artikkel 12 (7) i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (eIDAS-forordningen).

Om forskriften

Formålet med forskriften er å fremme et høyt nivå av tillit og sikkerhet, som står i passende forhold til risikoen. Etter formålsbestemmelsen i artikkel 1 skal samarbeidsordningen bl.a. omfatte utveksling av opplysninger, erfaring og god praksis samt fagfellebedømmelser i forbindelse med innmelding av eID-ordninger. Forskriften fastsetter videre i kapittel 1 at samarbeidsspråket skal være engelsk (artikkel 2), og at det skal opprettes "hurtigskranker"/kontaktpunkter i hvert medlemsland for utveksling av informasjon. Kapittel II har bestemmelser om utveksling av opplysninger, erfaringer og god praksis, og det fastsettes i artikkel 4 og 5, jf. artikkel 6, at utveksling av slik informasjon skal skje gjennom "hurtigskrankene". Gjennom "hurtigskrankene" kan medlemslandene også be om flere opplysninger enn hva som fremkommer i forbindelse med innmeldingen av en eID-ordning. Kapittel III fastsetter prinsipper og prosessregler for fagfellevurderinger, og kapittel IV fastsetter at det skal etableres et samarbeidsnettverk med nærmere angitte oppgaver.

Økonomiske og administrative konsekvenser

Forskriften fastsetter enkle og klare prosedyrer for hvordan samarbeidet mellom medlemstatene skal organiseres, herunder prosedyrer og regler for samvirkningsevne og sikkerhet i elektroniske identifikasjonsordninger, og om hvordan utveksling av informasjon i forbindelse med melding og anerkjennelse av hverandres eID-ordninger og fagfellevurderinger skal skje. Opprettelsen av et samarbeidsnettverk og etablering av et kontaktpunkt i hvert medlemsland (hurtigskranke), vil bidra til høy grad av tillit og sikkerhet, og til at dette vil kunne skje på en mest mulig kostnadseffektiv og administrativt lite byrdefull måte.

Etter departementets syn vil forskriften i seg selv ikke innebære vesentlige administrative eller økonomiske konsekvenser, men den vil kunne få administrative og økonomiske konsekvenser i forbindelse med opprettelse og drift av et kontaktpunkt ("hurtigskranken") og i forbindelse med deltakelse i samarbeidsnettverket. Det er naturlig at en slik oppgave legges til Difi. Opprettelse av "hurtigskranker" i alle medlemsland vil bidra til at man enkelt og effektivt kan komme i kontakt med relevante myndigheter og organer. Utveksling av

erfaringer, opplysninger og god praksis vil bidra til utvikling av gode løsninger og samvirkningsevne. Fagfellevurderinger (peer review) vil bidra til å sikre tillit til og sikkerhet i meldte eID-ordninger.

2. Forskrift om fastsettelse av spesifikasjoner for formater for avanserte elektroniske signaturer og avanserte segl, som skal anerkjennes av offentlige organer

Forskriften gjennomfører Kommisjonens gjennomføringsbeslutning (EU) 2015/1506 av 8. september 2015 om fastsettelse av spesifikasjoner for formater for avanserte elektroniske signaturer og avanserte segl, som skal anerkjennes av offentlige organer i henhold til artikkel 27 (5) og artikkel 37 (5) i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester til bruk for elektroniske transaksjoner på det indre marked (eIDAS-forordningen)

Om forskriften

Forskriften skal sikre at attester som er signert med avansert signatur kan brukes i et annet medlemsland. Når dokumenter vedlegges avansert signatur må det aksepteres at andre medlemsland bruker andre formater. Når offentlig forvaltning/offentlige virksomheter krever avanserte signaturer på et dokument, så skal signaturer som foreligger i et av formatene XAdES, CAdES eller PAdES som angitt i forskriften, anerkjennes. I tillegg gjelder anerkjennelsesplikten for andre formater hvis medlemslandet tilbyr en valideringstjeneste som oppfyller nærmere angitte vilkår som fremgår av forskriften.

Økonomiske og administrative konsekvenser

Forskriften vil bidra til en mer enhetlig bruk av avanserte signaturer og det vil bli enklere å lage signeringsløsninger for offentlige dokumenter som kan brukes i utlandet. For de som krever avanserte signaturer vil håndtering og validering av ulike formater innebære en økt kostnad. Standardisering vil imidlertid kunne skape et europeisk marked som forenkler bruk av signaturer i de angitte formatene.

3. Forskrift om fastsettelse av tekniske minstespesifikasjoner og minstekrav til framgangsmåter for sikkerhetsnivåene for elektroniske identifikasjonsmidler

Forskriften gjennomfører Kommisjonens gjennomføringsforordning (EU) 2015/1502 av 8. september 2015 om fastsettelse av tekniske minstespesifikasjoner og minstekrav til framgangsmåter for sikkerhetsnivåene for elektroniske identifikasjonsmidler i henhold til artikkel 8 (3) i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (eIDAS-forordningen).

Om forskriften

Etter eIDAS-forordningen skal det for eID-ordninger som er meldt etter forordningens artikkel 9 (1) angis hvilket av tillitsnivåene 'lav', 'betydelig' eller 'høy' eID-ene tilfredsstillers. Formålet med gjensidig anerkjennelse av eID-er på tvers av medlemslandene er å gjøre det mulig for innbyggerne i EU/EØS å kunne bruke sine nasjonale eID-er på tvers av landegrensene. Siden medlemslandene har forskjellige eID-ordninger, er det nødvendig med en mekanisme for å gjøre dem sammenlignbare og sikre samvirkeevne. Forskriften løser en del av denne utfordringen ved å beskrive tillitsnivåene.

Forskrift om tillitsnivåer inneholder detaljerte kriterier til de tre tillits-/sikringsnivåene 'lav', 'betydelig' og 'høy', som gjør det mulig for medlemslandene å vurdere sine egne eID-ordninger opp mot teknologinøytrale nivåbeskrivelser som ikke er låst til bestemte tekniske standarder eller løsninger.

Muligheten for å gjenkjenne personen i norske tjenester forutsetter imidlertid også at personen er identifisert på en entydig måte og er gjenkjennbar i norske systemer. For å oppnå dette kreves det noe tilleggskompetanse i Folkeregisteret og i ID-porten.

Økonomiske og administrative konsekvenser

Forskriften beskriver minimumskrav til tillitsnivåene og nærmere kriterier for oppfyllelse av minimumskravene. Dette skal sikre at ulike løsninger kan oppfylle fastsatte nivåer. Forskriften utfylles av forskrift om samarbeid og fagfellevurderinger (peer review) (gjennomføringsbeslutning 2015/296). For å sikre godt samspill mellom norske og europeiske tillitsnivåer revideres nå rammeverket for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. Det vises til omtale i del II av dette høringsnotatet. Det vil påløpe kostnader i forbindelse med tilrettelegging for gjenkjenning av personer som benytter meldte eID-ordninger i norske løsninger hvor anbefalt løsning for hvordan slik tilrettelegging kan skje er kostnadsberegnet til 16 millioner i forventede investeringskostnader og en årlig forvaltningskostand på 8 millioner kroner. Denne tilretteleggingen mellom Folkeregisteret og ID-porten er ikke ferdigstilt, men Difi har utviklet grensesnittet til ID-porten. Det vil være behov for revurdering av kostnadsestimatene i lys av dette. .

4. Forskrift om rammen for samvirkingsevne

Forskriften gjennomfører Kommisjonens gjennomføringsforordning (EU) 2015/1501 av 8. september 2015 om rammen for samvirkeevne i henhold til artikkel 12 (8) i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (eIDAS-forordningen).

Om forskriften

Etter artikkel 12 (2) i eIDAS-forordningen skal det innføres krav til samvirkeevne for å sikre samvirke mellom nasjonale eID-ordninger som er meldt etter forordningens artikkel 9 (1). Denne forskriften fastsetter tekniske og operasjonelle krav til samvirkeevne.

Forordningen fastsetter tekniske minimumskrav, minstekrav til personidentifikasjonsdata, felles operasjonelle standarder og referanser til tillitsnivåer og mulighet for sammenligning av disse.

Kravene til samvirkeevne tar sikte på å være teknologinøytrale og skal ikke forskjellsbehandle mellom spesifikke nasjonale tekniske løsninger for eID innenfor et medlemsland. De skal følge europeiske og internasjonale standarder så langt det er mulig, lette gjennomføringen av prinsippet om innebygget personvern (privacy by design) og skal sikre at personopplysninger behandles i overensstemmelse med personvernforordningen.⁵

Økonomiske og administrative konsekvenser

Forordningen etablerer felles krav, slik at man i praksis skal kunne koble til eID-ordninger fra de forskjellige medlemslandene, for å kunne muliggjøre samvirke.

I all hovedsak vil konsekvensene av rettsakten innebære nødvendig teknisk tilrettelegging i ID-porten. I tillegg vil det eventuelt være behov for tilpasning i folkeregisteret for å gjenkjenne minimum datasett dersom man skal kunne ta ut gevinstene ved gjennomføring av forordningen. Dette omtales også ovenfor.

5. Forskrift om fastsettelse av vilkår, formater og framgangsmåter for melding

Forskriften gjennomfører Kommisjonens gjennomføringsbeslutning (EU) 2015/1984 av 3. november 2015 om fastsettelse av vilkår, formater og framgangsmåter for melding i henhold til artikkel 9 (5) i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (eIDAS-forordningen).

Om forskriften

Forskriften fastsetter nærmere vilkår, prosedyrer og formater for melding av eID-ordninger. Melding er frivillig, men er en grunnleggende forutsetning for gjensidig anerkjennelse av eID-ordninger på tvers av landegrensene i EU/EØS. Forskriften skal sikre en enhetlig bruk av meldingsskjemaer. Etter eIDAS-forordningens artikkel 9 skal alle medlemslandene ved melding av en eID-ordning, gi Kommisjonen en nærmere beskrivelse av ordningen slik det er beskrevet i artikkel 9 (1).

Etter forordningens artikkel 9 (5) kan Kommisjonen ved hjelp av gjennomføringsrettsakter fastlegge vilkår, formater og prosedyrer for melding i henhold til forordningens artikkel 9 (1). Disse gjennomføringsrettsaktene vedtas etter undersøkelsesprosedyren i artikkel 48 (2), jf. artikkel 5 i forordning (EU) nr. 182/2011 om generelle regler og prinsipper for hvordan medlemsstatene skal kontrollere Kommisjonens utøvelse av gjennomføringsbestemmelser.

⁵ Forordning 2016/679 General Data Protection Regulation (GDPR)

Gjennomføringsbeslutningens artikkel 2 fastsetter at meldingen skal sendes inn på engelsk, med unntak av bilagsdokumenter dersom dette medfører en urimelig byrde. Artikkel 3 fastsetter at meldingen skal skje elektronisk og gir nærmere spesifikasjoner om prosedyre og formater. Artikkel 4 fastsetter at Kommisjonen må bekrefte mottakelsen av meldingen elektronisk. Artikkel 5 regulerer i hvilke tilfeller Kommisjonen kan be om tilleggsopplysninger eller nærmere avklaringer. Artikkel 6 fastsetter at meldingen først anses som utfylt når eventuelle tilleggsopplysninger eller avklaringer er sendt Kommisjonen.

Økonomiske og administrative konsekvenser

Forskriften kan innebære kostnader i forbindelse med oversettelse av dokumentasjon som inngår i en melding av norske eID-ordninger. Samtidig forenkler arbeidet med fagfelle vurderinger av andre land ordninger ved at dokumentasjon skal foreligge på engelsk.

Det er frivillig å melde en eID-ordning, men enklere gjenbruk av eID-er forventes å føre til økt anvendelse av digitale selvbetjeningsløsninger både nasjonalt og på tvers i EU/EØS. Følgelig vil det kunne innebære betydelige samfunnsøkonomiske gevinster og kostnadsbesparelser. Forskriften fastsetter enkle og klare prosedyrer for hvordan meldingen skal skje, noe som vil bidra til at meldingen skjer på en mest mulig kostnadseffektiv og administrativt lite byrdefull måte.

II Rammeverk for identifikasjon og sporbarhet

eIDAS-forordningen påvirker det norske regimet for bruk av eID i offentlig sektor. Bruk av eID i offentlig sektor reguleres i dag av "Rammeverk for autentisering og uavviselighet ved elektronisk kommunikasjon med og i offentlig sektor", "Kravspesifikasjon for PKI i offentlig sektor" og selvdeklarasjonsforskriften. Denne reguleringen legger også rammene for bruk av eID og PKI i andre deler av samfunnet, ikke minst for finanssektoren. eID-ordningene på høyeste sikkerhetsnivå etter dagens rammeverk har inntil nå vært regulert av e-signaturloven med tilhørende forskrifter, bl.a. selvdeklarasjonsforskriften.

eIDAS-forordningen erstatter e-signatordirektivet. For norsk rett innebærer dette at Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester)⁶ erstatter Lov om elektronisk signatur (e-signaturloven) (opphevet) og vil påvirke e-ID-bruk nasjonalt. Virkeområdet for loven er kraftig utvidet i forhold til e-signaturloven, både ved at forordningen definerer flere tillitstjenester og ved at den i motsetning til i dag, regulerer bruk av e-ID i offentlig sektor.

Dagens rammeverk definerer fire sikkerhetsnivåer for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. På høyeste sikkerhetsnivå kreves det at

⁶ <https://lovdata.no/dokument/NL/lov/2018-06-15-44>

det benyttes løsninger som er deklartert i henhold til offentlige krav. Dette reguleres av selvdeklarasjonsforskriften. Dagens rammeverk forutsetter et selvdeklarasjonsregime for eID-er på høyeste sikkerhetsnivå. Leverandører av sertifikattjenester kan i dag melde inn løsninger som oppfyller Kravspesifikasjon for PKI i offentlig sektor til Nasjonal kommunikasjonsmyndighet (Nkom). Selvdeklarasjonsforskriften åpner for deklarasjon av sertifikatklassene Person høy, Person standard og Virksomhet, basert på Kravspesifikasjon for PKI i offentlig sektor. Selv om rammeverket i seg selv er teknologinøytralt, har selvdeklarasjonsforskriften bare anerkjent PKI-baserte løsninger.

Rammeverket har fungert godt i 10 år. Både utbredelse og bruk av elektroniske identitetsbevis har økt vesentlig i løpet av disse årene. Departementet foreslår å revidere dagens Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, både for å tilpasse den til forordningen og for at det skal være bedre tilpasset dagens behov.

Departementet foreslår å knytte de norske eID-nivåene opp mot eIDAS-forordningens tillitsnivåer og utvide omtalen av sporbarhetstjenester mm. Videre foreslår departementet å revidere begrepsbruken for å gjøre den mer treffende og tilpasset forordningen. Forslaget til revidert rammeverk er teknologinøytralt, og selvdeklarasjonsordningen foreslås endret slik at den ikke lenger forutsetter bruk av PKI⁷ for å oppnå høyeste sikkerhetsnivå. De norske eID-nivåene vil dermed i likhet med eIDAS-nivåene ikke lenger forutsette bruk av PKI. Departementet foreslår derfor å oppheve Kravspesifikasjon for PKI som forvaltningsstandard.

Dagens rammeverk knytter legitimasjonskravene på høyeste sikkerhetsnivå til hvitvaskingsregelverket. Departementet foreslår å videreføre en slik knytning i utkastet til nytt rammeverk. Etter vår vurdering er trusselbildet for bruk av eID i offentlig sektor sammenlignbart med utfordringene knyttet til hvitvasking, slik at legitimasjonskravene i hvitvaskingsforskriften har overføringsverdi og kan gjenbrukes i rammeverket. Dessuten vil gjenbruk av disse reglene legge til rette for effektiv ressursbruk ved at de samme løsningene kan brukes både i offentlig og privat sektor.

Vi gjør oppmerksom på at hvitvaskingsreglene nylig er endret. I ny forskrift fremgår legitimasjonskravet av forskriftens § 4-3, jf. tidligere forskrifts § 7. Ved større endringer av hvitvaskingsforskriften må legitimasjonskravet i rammeverket vurderes på nytt.

De viktigste endringene i det reviderte rammeverket er:

- Språk og begrepsbruk er harmonisert med eIDAS-forordningen for å gi en helhetlig regulering av området. Vi har også supplert med enkelte nye norske begreper.
- Omtale av risiko er kortet ned. Rammeverket refererer til Difis veiledning i internkontroll.

⁷ Public key infrastructure (PKI) er en måte å sikre kommunikasjon på ved hjelp av elektroniske nøkler. Avsender og mottaker har hver sine nøkler som henger sammen parvis, en hemmelig privat nøkkel og en publisert offentlig nøkkel som lagres hos en tiltrodd tredjepart. Slike nøkkelpar kalles ofte asymmetriske nøkler.

- Omtalen av løsninger for å sikre dokumentasjon er utvidet og det gis eksempler på hvordan nye tillitstjenester kan tilfredsstille behovet. Begrepsbruken er endret og klargjør at tiltakene vil gi ulike grader av tillit.
- Sikkerhetsnivåene for eID tar utgangspunkt i sikkerhetsnivåene i eIDAS-forordningen. Det stilles krav både til identitetspåstanden (individualiseringen) og autentiseringens styrke.
- Kravsettet for eID er vesentlig utvidet, ved at det bygger på eIDAS-kravene. Det gis nå omfattende, teknologinøytrale beskrivelser på alle sikkerhetsnivåer for identifikasjon.
- Kravspesifikasjon for PKI i offentlig sektor avvikles.
- Identifikasjonspåstanden skal entydig kunne knytte personen til en norsk identifikator som finnes i folkeregisteret (p.t. fødselsnummer eller d-nummer).
- Rammeverket omtaler ikke lenger autentisering av virksomheter. Dette behovet forutsettes håndtert gjennom tillitstjenester for elektroniske segl (tidligere kalt virksomhetssignaturer). Dette gjelder både identifikasjon av nettsteder og andre systemløsninger.

Departementet tar sikte på at nytt rammeverk kan erstatte eksisterende rammeverk fra ikrafttredelsesdatoen, dvs. at det ikke legges opp til overgangsregler. For å gjøre det helt klart at alle eksisterende e-ID-er på nivå 4 også tilfredsstiller krav til nytt nivå høyt, er dette eksplisitt presisert i rammverkets punkt 3.3.4.1.

Økonomiske og administrative konsekvenser

Forslag til revidert rammeverk vil tilrettelegge for mer enhetlig bruk av løsninger for identifikasjon og sporbarhet. I en overgangsfase vil det påløpe kostnader fordi leverandørene må forholde seg til et nytt kravsett. For øvrig vil ikke det reviderte rammeverket innebære vesentlige økonomiske eller administrative konsekvenser. Det reviderte rammeverket legger til rette for innovasjon og mer hensiktsmessige løsninger, noe som vil gi gevinster på sikt.

III Forslag til ny forskrift om selvdeklarasjonsordninger for elektroniske tillitstjenester

Innledning

Som angitt ovenfor under II om Rammeverk for identifikasjon og sporbarhet, foreslår departementet at muligheten til selvdeklarasjon for eID-løsninger videreføres, men at dette gjøres mot det teknologinøytrale kravsettet som fremgår av forslaget til nytt rammeverk.

Forslag til ny selvdeklarasjonsforskrift åpner for at man kan selvdeklare eID-løsninger på nivå 'Lav', 'Betydelig' eller 'Høy' iht. nytt rammeverk. Dette gjelder både eID-løsninger som baserer seg på kvalifiserte sertifikater, og løsninger som på annen måte oppfyller kravene.

Dagens selvdeklarasjonsforskrift⁸, som muliggjør selvdeklarasjon for etterlevelse av sertifikatklassene i Kravspesifikasjon for PKI i offentlig sektor, foreslås opphevet.

Flere forskrifter henviser til dagens selvdeklarasjonsforskrift. Når forslag til ny selvdeklarasjonsforskrift nå gjøres mer teknologinøytral, må det vurderes hvordan henvisninger til forskriften bør videreføres. I forslag til ny forskrift vil selvdeklarasjon gjelde eID-nivåer, ikke sertifikatklasser.

Mange av regelverkene som viser til selvdeklarasjonsordningen, brukes i dag om innloggingskravet i web-baserte løsninger. Der vil formodentlig en henvisning til selvdeklarte eID-løsninger være dekkende. For regelverk som viser til innsendingsløsninger, hvor dokumenter sendes inn elektronisk signert av signatøren fra signatørens egne systemer, bør det vurderes hvordan sporbarhetskravet skal opprettholdes. Rammeverkets omtale av to sporbarhetsnivåer kan være et utgangspunkt.

Forskrifter med slike henvisninger er gjengitt nedenfor med forslag til endringer.

Om forslaget til revidert forskrift om selvdeklarasjon

Forskriften er nesten likelydende med nåværende selvdeklarasjonsforskrift, med den forskjell at selvdeklarasjon nå knyttes opp mot nytt rammeverk for identifikasjon og sporbarhet (Rammeverket), og ikke mot Kravspesifikasjon for PKI i offentlig sektor (som foreslås opphevet).

Slik departementet ser det, vil lov om tillitstjenester og det nye rammeverket for identifikasjon og sporbarhet gjøre det unødvendig å opprettholde en felles Kravspesifikasjon for PKI i offentlig sektor. Departementet vil vurdere å gjøre relevante tekniske standarder, som i dag henviser til kravspesifikasjonen, til anbefalte standarder i Referanse katalogen for IT-standarder⁹.

I den grad det er behov for å spesifisere at sertifikatbaserte løsninger skal benyttes, kan dette skje ved å henvise til sertifikater som utstedes av kvalifiserte tilbydere av tillitstjenester og som tilfredsstiller kravene i Lov om tillitstjenester. Dersom det også er behov for en klar knytning til norske identitetsnumre (fødselsnummer, d-nummer eller organisasjonsnummer), kan dette kreves eksplisitt eller ved å henvise til relevante standarder som SEID-profilene¹⁰.

Regelverk som henviser til dagens selvdeklarasjonsforskrift

Det er i dag en rekke forskrifter som stiller krav om at det skal benyttes løsninger som er selvdeklarte i henhold til forskrift om selvdeklarasjon av sertifikatutstedere. Departementet

⁸ <https://lovdata.no/pro/#document/SF/forskrift/2005-11-21-1296>

⁹ <https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/standarter/referanse katalogen>

¹⁰ https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/seid_leveranse_1_-_v1.02.pdf

foreslår at henvisningene i regelverk som viser til selvdeklarasjonsforskriften, oppdateres ved at *sertifikatklasse Person Høy* erstattes med *eID-nivå HØY*, *sertifikatklasse Person Standard* erstattes med *eID-nivå Betydelig* og henvisninger til *sertifikatklasse Virksomhet* erstattes med *kvalifiserte sertifikater for juridiske personer*.

Departementet er ikke kjent med at det er stilt krav om avanserte signaturer eller segl i forskrifter som i dag viser til dagens selvdeklarasjonsforskrift. Departementet presiserer at opplistingen nedenfor ikke nødvendigvis er komplett.

Departementet ber høringsinstansene være spesielt oppmerksom på at dersom det stilles krav om å benytte avanserte signaturer eller segl, så må man også akseptere signaturer og segl i PAdES, XAdES, CAdES og eventuelt andre formater eller metoder, jf. gjennomføringsrettsakt 2015/1506 som utfyller eIDAS-forordningens artikkel 27 nr. 5 og artikkel 37 nr. 5, og som er omtalt ovenfor. Vi minner også om at terminologien i Lov om tillitstjenester avviker noe fra terminologien i e-signaturloven ved at det som før kaltes virksomhetssignatur, nå omtales som elektroniske segl.

Når det gjelder anskaffelsesforskriften § 22-5, som omtales nedenfor, så benytter forskriften allerede betegnelsen elektroniske segl og er således i tråd med terminologien i Lov om tillitstjenester. Forslag til endringer gjelder derfor kun oppdatering av henvisninger til forskrifter som implementerer gjennomføringsrettsaktene til eIDAS-forordningen.

Departementet foreslår endringer i følgende forskrifter:

Forskrift om tinglysing § 3 annet ledd ¹¹ skal lyde:

Når det i eller i medhold av tinglyssingsloven er krav om underskrifter på dokumentet, skal det ved elektronisk tinglysing av dokumenter benyttes eID-tjeneste på nivå Høy som oppfyller kravene i *forskrift dd.mm.åååå nr. xx om frivillige selvdeklarasjonsordninger* § 3, og som er oppført på publisert liste i henhold til § 11 første ledd i nevnte forskrift. Ved bruk av slike elektroniske sertifikater stilles det ikke krav til vitnebekreftelser.

Forskrift om tiltak mot hvitvasking og terrorfinansiering mv. § 6¹² skal lyde:

Gyldig legitimasjon for fysiske personer er eID-tjeneste som oppfyller kravene i *forskrift dd.mm.åååå nr. xx om frivillige selvdeklarasjonsordninger* § 3 og som er oppført på publisert liste i henhold til § 11 første ledd i nevnte forskrift.

Forskrift om forsvars- og sikkerhetsanskaffelser § 7-3 første ledd bokstav a¹³ skal lyde:

- a. den elektroniske signaturen *må være basert på eID-tjeneste på nivå Betydelig eller Høy, og som oppfyller kravene i forskrift xx.xx.åååå nr. xx om frivillige selvdeklarasjonsordninger* § 3 eller

¹¹ <https://lovdata.no/SF/forskrift/1995-11-03-875/§3>

¹² <https://lovdata.no/SF/forskrift/2009-03-13-302/§6>

¹³ <https://lovdata.no/SF/forskrift/2013-10-04-1185/§7-3>

4 og er oppført på publisert liste i henhold til § 11 første ledd i nevnte forskrift. *Alternativt må det benyttes elektronisk signatur eller segl basert på kvalifisert sertifikat fra en tilbyder av elektroniske tillitstjenester som oppfyller kravene i lov av 15. juni 2018 nr. 44 om elektroniske tillitstjenester.*

Oppdragsgiver skal alltid akseptere elektroniske signaturer eller segl som oppfyller kravene til utenlandsk kvalifisert sertifikat i forordning (EU) nr. 910/2014 artikkel 14, dersom tilbudet er elektronisk signert av en utenlandsk statsborger,

Forskrift om behandling av opplysninger i politiet og påtalemyndigheten § 36 fjerde ledd¹⁴ skal lyde:

Gyldig legitimasjon for fysiske personer er *eID-tjeneste* som oppfyller *kravene til nivå Høy* i forskrift dd.mm.åååå nr. xx om *frivillig selvdeklarasjonsordninger* § 3 og som er oppført på publisert liste i henhold til § 11 første ledd i nevnte forskrift.

Forskrift om elektronisk kommunikasjon med namsmannen og Statens innkrevingssentral i saker etter tvangsfullbyrdelsesloven og i saker for forliksrådet § 8¹⁵ skal lyde:

Når det i eller i medhold av tvangsfullbyrdelsesloven eller tvisteloven er krav om underskrift på dokumenter, skal det ved elektronisk kommunikasjon etter forskriften her benyttes elektronisk signatur som *er basert på en eID-tjeneste på nivå Høy eller Betydelig*, og som er oppført på publisert liste i henhold til § 11 første ledd i forskrift dd.mm.åååå nr. xx om *frivillige selvdeklarasjonsordninger*. *Det kan alternativt benyttes elektronisk signatur eller segl basert på sertifikat fra kvalifisert tilbyder av tillitstjenester som oppfyller kravene i lov av 15. juni 2018 nr. 44 om elektroniske tillitstjenester.* Statens innkrevingssentral fastsetter hvilken sertifikatklasse som skal benyttes for de enkelte dokumenttyper og brukere.

Forskrift om elektronisk kommunikasjon med og i forvaltningen § 36¹⁶ tredje og fjerde ledd skal lyde:

Koordineringsorganet kan bestemme at det under tjeneste for forvaltningsorganer kun skal benyttes sertifikater fra *tilbydere av tillitstjenester* som har inngått rammeavtale om levering av slike tjenester til forvaltningen eller som er anerkjent av koordineringsorganet.

Koordineringsorganet kan bestemme at det ved elektronisk kommunikasjon med og i forvaltningen bare skal benyttes *eID-tjenester* som er oppført på liste publisert i henhold til forskrift dd.mm.åååå nr. xx om *frivillige selvdeklarasjonsordninger* § 11 første ledd.

Forskrift om offentlige anskaffelser § 22-5¹⁷ fjerde og femte ledd skal lyde:

(4) Når oppdragsgiveren krever bruk av elektronisk signatur, skal han godta avanserte elektroniske signaturer som er understøttet av et kvalifisert sertifikat som er utstedt av et organ som er oppført på en liste over *tilbydere av tillitstjenester i henhold til lov av 15. juni 2018 nr. 44 om elektroniske tillitstjenester.*

¹⁴ <https://lovdata.no/SF/forskrift/2013-09-20-1097/§36-4>

¹⁵ <https://lovdata.no/SF/forskrift/2010-06-25-977/§8>

¹⁶ <https://lovdata.no/SF/forskrift/2004-06-25-988/§36>

¹⁷ <https://lovdata.no/SF/forskrift/2016-08-12-974/§22-5>

(5) Oppdragsgiveren kan etter en risikovurdering kreve bruk av avansert elektronisk signatur. Når oppdragsgiveren krever bruk av en slik signatur eller elektronisk segl, skal kravene til formater for signaturen eller seglet være basert på formater som er fastsatt i *forskrift dd.mm.åååå nr. xx om fastsetting av spesifikasjoner vedrørende formater for avanserte elektroniske signaturer og avanserte segl, som skal anerkjennes av offentlige myndigheter*. Oppdragsgiveren skal iverksette de tiltakene som er nødvendige for å kunne behandle formatene teknisk. Oppdragsgiveren kan velge å godta andre formater for signaturer og segl som han er i stand til å validere på grunnlag av opplysningene i signaturen, seglet eller tilknyttet informasjon.

Høringsfrist

Høringssvar sendes inn via lenke på Kommunal- og moderniseringsdepartementets nettside (lenke). Høringssvarene vil bli offentliggjort.

Høringsfrist: xx.xx.xxx

Med hilsen

Vedlegg:

1. Kommisjonens gjennomføringsbeslutning (EU) 2015/296 av 24. februar 2015 om fastsettelse av saksbehandlingsregler for samarbeid mellom medlemsstatene om elektronisk identifikasjon
2. Kommisjonens gjennomføringsforordning (EU) 2015/1501 av 8. september 2015 om rammen for samvirkingsveve
3. Kommisjonens gjennomføringsforordning (EU) 2015/1502 av 8. september 2015 om fastsettelse av tekniske minstespesifikasjoner og minstekrav til framgangsmåter for sikkerhetsnivåene for elektroniske identifikasjonsmidler
4. Kommisjonens gjennomføringsbeslutning (EU) 2015/1506 av 8. september 2015 om fastsettelse av spesifikasjoner for formater for avanserte elektroniske signaturer og avanserte segl, som skal anerkjennes av offentlige organer
5. Kommisjonens gjennomføringsbeslutning (EU) 2015/1984 av 3. november 2015 om fastsettelse av vilkår, formater og framgangsmåter for melding
6. Forslag til Rammeverk for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor
7. Forslag til ny forskrift om frivillige selvdeklarasjonsordninger