



Difi

Direktoratet for
forvaltning og ikt

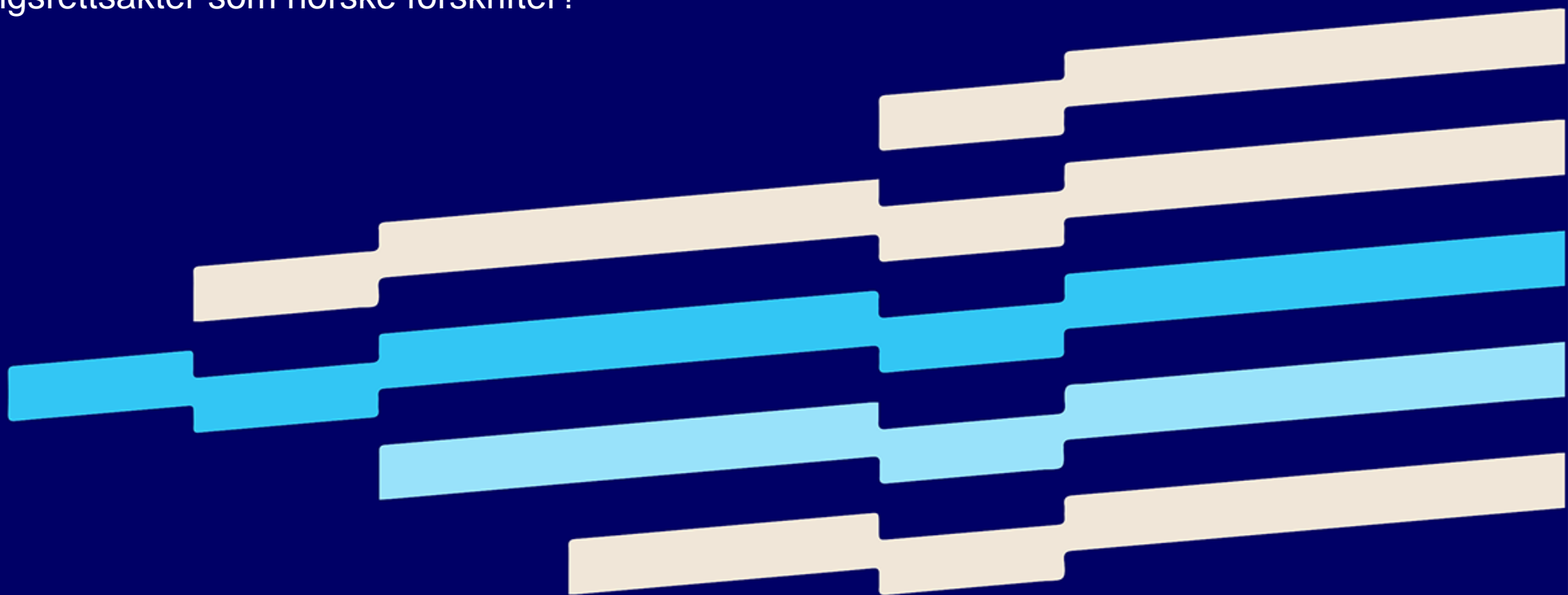
eIDAS-forskrifter og nytt e-ID-rammeverk på høring

•Nytt norsk «Rammeverk for identifikasjon og elektronisk kommunikasjon med og i offentlig sektor» og knytning av selvdeklarasjonsforskriften til nytt rammeverk – hva er status for høring om dette? Hva er status for innføring av eIDAS gjennomføringsrettsakter som norske forskrifter?

—

Norstella 4.12.2018

Jon B. Holden - Difi



Innhold

- Kort om forordningen
- Forordningens rettslige status i Norge
- Høring – frist 6.-7. februar 2019
 - Gjennomføringsrettsakter, selvdeklarasjonsforskrift og nytt rammeverk
 - Høringen fra KMD
 - Rammeverket
 - Selvdeklarasjonsforskriften
 - Regelverkslandskapet
- Meldte e-ID-ordninger

Om eIDAS

- Forordning [910/2014](#)
 - EU-forordning, inntatt i norsk rett av Stortinget 15.06.2018
 - Erstatte e-signatordirektivet ([1993/93](#))
- Formål
 - Bygge tillit
 - Etablere grenseoverskridende tjenester
- Inndeling
 - **e-ID (kapittel 2, art 6-12)** – offentlig sektor
 - **Tillitstjenester (kapittel 3, art 13-45)** – hele samfunnet
 - Elektroniske dokumenter (kapittel 4, art 46)

eIDAS og Norge

- **eIDAS har trådt i kraft i EU**
 - Anerkjennelsesplikt eID fra 29. sept 2018, jf. art 51 nr 2 (og [2015/1502](#))
 - Kvalifiserte sertifikatutstedere må levere samsvarsrevisjonsrapport innen 1. juli 2017, art 51 nr 3
- **Norge har satt i kraft eIDAS-regler**
 - [Tillitstjenesteloven](#) gjelder fra 15.6.18, opphever e-signaturloven
 - Inntil videre gjelder likevel forskrifter til e-signaturloven
- **eIDAS er på vei inn i EØS**
 - Norge deltar i samarbeidsnettverket til eIDAS
 - eIDAS er besluttet innlemmet i EØS, jf. [komitebeslutning](#) 9. februar 2018
 - eIDAS tas inn i EØS-avtalen når **alle** EFTA-land har gjort nødvendige lovendringer, jf. beslutningens art 3
 - Norge (25.6.18), Liechtenstein (15.10.18), Island (**gjenstår**)
 - Fra ikrafttredelse løper 6 mnd frist for sertifikatutstedere, jf. beslutningens artikkel 1

Høring – inkl. rammeverk for e-ID



The screenshot shows the website 'Regjeringen.no' with a navigation menu including 'Tema', 'Dokument', 'Aktuelt', 'Departement', and 'Regjering'. The breadcrumb trail is 'Du er her: Forsiden • Dokument • Høring'. The main title is 'Høring - Implementering av gjennomføringsrettsakter til eIDAS-forordningen, nytt rammeverk for identifikasjon og sporbarhet og ny selvdeklarasjonsforskrift'. The date is 'Høring | Dato: 29.11.2018'. The status is 'På høring' and the deadline is 'Høringsfrist: 07.02.2019'. A section titled 'Høringsbrev' with a minus sign icon contains the reference 'Vår ref.: 18/3166-19' and the start of the text: 'Kommunal- og moderniseringsdepartementet (KMD) sender med dette på høring forslag om implementering av gjennomføringsrettsakter til'.

Regjeringen.no

Tema ▾ Dokument ▾ Aktuelt ▾ Departement ▾ Regjering ▾

Du er her: [Forsiden](#) • [Dokument](#) • [Høring](#) •

Høring - Implementering av gjennomføringsrettsakter til eIDAS-forordningen, nytt rammeverk for identifikasjon og sporbarhet og ny selvdeklarasjonsforskrift

Høring - Implementering av gjennomføringsrettsakter til eIDAS-forordningen, nytt rammeverk for identifikasjon og sporbarhet og ny selvdeklarasjonsforskrift

Høring | Dato: 29.11.2018

Status: På høring
Høringsfrist: 07.02.2019

Høringsbrev ⊖

Vår ref.: 18/3166-19

Kommunal- og moderniseringsdepartementet (KMD) sender med dette på høring forslag om implementering av gjennomføringsrettsakter til


Høring – nye forskrifter og endret rammeverk

- To høringer
 - [NFD](#) (frist 6.2.2019)
 - Tre gjennomføringsrettsakter – 2015/806 (tillitsmerket), 2015/1505 (tillitslisten), 2016/650 (kvalifiserte signatur- og seglfremstillingssystemer)
 - [KMD](#) (frist 7.2.2019)
 - Fem gjennomføringsrettsakter – 2015/296 (samarbeidsnettverk), 2015/1501 (teknisk samvirkingsevne, minste datasett), 2015/1502 (sikkerhetsnivåer e-ID), 2015/1506 (signatur- og seglformater), 2015/1984 (e-ID-meldinger)
 - Nytt rammeverk for identifikasjon og sporbarhet
 - Selvdeklarasjonsforskrift

Utkast til nytt rammeverk – e-ID

- Struktur
 - Forklaring 3.1-3.2, definisjoner 3.3, eksempler 3.4, veiledning 3.5
- Ny terminologi: *identifikasjon*, dvs. både autentiseringen (tilliten) og krav til identitetspåstanden.
- Definisjon av sikkerhetsnivåer for e-ID – kapittel 3.3
 - Norske, autonome nivåer, bygger på eIDAS-beskrivelser med tilpasninger
 - Krav om offentlig kontroll
 - Generelt krav om *sikker og entydig* knytning til person i folkeregisteret, 3.3.1.1
 - Presiseringer
 - Lavt/betydelig
 - Kan oppfylle kravet til å «besitte et bevis» ved bruk av folkeregisteret e.a. eks. kontaktregisteret, 3.3.2.1/3.3.3.1.
 - Høyt
 - Krav til id-bevis henviser til hvitvaskingsreglene, jf. dettes forskrift [§ 4-3](#)
 - Selvdeklart e-ID på nivå 4 er ok

Utkast til nytt rammeverk - sporbarhet

- Struktur
 - 4.1 forklaring, 4.2 definisjon, 4.3 eksempler, 4.4 veiledning
- Ny terminologi:
 - fra uavviselighet til sporbarhet 
 - klargjør risikobasert utgangspunkt
- Definisjoner 4.2
 - Nivå 1 – rutiner og logger
 - Nivå 2 – bruk av tilstrekkelig uavhengig tredjepart
- Mange teknikker kan brukes, ulike særtrekk
 - Bl.a. nye tillitstjenester, se 4.1.4-4.1.6

Utkast til ny selvdeklarasjonsforskrift

- Bygger på [forskriften av 2005](#)
 - Henvisninger til kravspesifikasjon PKI -> henvisning til rammeverket
- §§ 3, 4 og 5 endres
 - Sertifikatutsteder -> tilbyder av e-ID-tjeneste
 - Sertifikatklasse person standard (etc) -> e-ID-nivå betydelig

Regelverk som henviser til dagens selvdeklarasjonsforskrift

- Utgangspunkt – endre fra
 - sertifikatklasse Person Høy -> e-ID-nivå høy
 - sertifikatklasse Person Standard -> e-ID-nivå betydelig
 - sertifikatklasse Virksomhet -> kvalifiserte sertifikater for juridiske personer

Oppsummering mht. rettslig landskap



Regelverket i går (til 14.06.2018)

- Rammeverk for aut. og uavv.
 - 4 autentiseringsnivåer
 - Høyeste nivå skal være underlagt tilsyn iht. selvdeklarasjonsforskriften (=krav om PKI)
- E-signaturloven
 - Forskriftshjemmel § 16 og 16a
 - Forskrift om krav til utstedere av kvalifiserte sertifikater
 - Selvdeklarasjonsforskriften
 - Deklarere sertifikater iht. kravspesifikasjon PKI

Regelverket nå (fra 15.06.2018)

- Rammeverk for aut. og uavv.
 - 4 autentiseringsnivåer
 - Høyeste nivå skal være underlagt tilsyn iht. selvdeklarasjonsforskriften (=krav om PKI)
- ~~E-signaturloven~~ **Lov om elektroniske tillitstjenester**
 - **Viderefører eksisterende forskrifter, jf. § 10**
 - Forskrift om krav til utstedere av kvalifiserte sertifikater
 - Selvdeklarasjonsforskriften
 - Deklarere sertifikater iht. kravspesifikasjon PKI
 - **EU-forskrifter, bl.a. 2015/1502 med krav til e-ID**

Regelverket i morgen (etter høring)

- Rammeverk for **identifikasjon og sporbarhet**
 - **3 identifikasjonsnivåer**, basert på [2015/1502](#) med tilpasning
 - **Alle** nivåer skal være underlagt tilsyn iht. selvdeklarasjonsforskriften. **Teknologinøytrale e-ID-krav.**
- ~~E-signaturloven~~ [Lov om elektroniske tillitstjenester](#)
 - **Gamle forskrifter oppheves, nye vedtas**
 - ~~Forskrift om krav til utstedere av kvalifiserte sertifikater~~
 - **Endret** selvdeklarasjonsforskrift
 - Deklarere **e-ID** iht. Rammeverk for identifikasjon og sporbarhet
 - **EU-forskrifter, bl.a.**

Regelverket i morgen - kortform (e-ID)

- Rammeverk for **identifikasjon**

- **3 identifikasjonsnivåer**

-

Teknologinøytrale e-ID-krav.

- ~~E-signaturloven~~ **Lov om elektroniske tillitstjenester**

- Selvdeklarasjonsforskrift

- Deklarere **e-ID** iht. Rammeverk **for identifikasjon**

Meldte e-ID- ordninger



Meldte e-ID-ordninger - [oversikt](#)

- Meldte e-ID-ordninger fra
 - Tyskland (høyt, september 2017)
 - Estland (høyt, 6 løsninger)
 - Italia (lavt, betydelig, høyt)
 - Kroatia (høyt)
 - Luxembourg (høyt)
 - Spania (høyt)
- Flere har sommer 2018 vært gjennom fagfelleevaluering
 - Belgia (høyt)
 - Portugal (høyt)
- Én gjennomgår fagfelleevaluering nå
 - Storbritannia (lavt, betydelig)

**Tillegg – basert på
spørsmål**



Revisjonskravet for e-ID – krav til revisor?

- Kravet i [2015/1502](#)
 - **2.4. Management and organisation**
 - All participants providing a service related to electronic identification in a cross-border context (“providers”) shall have in place documented information security management practices, policies, approaches to risk management, and other recognised controls so as to provide assurance to the appropriate governance bodies for the electronic identification schemes in the respective Member States that effective practices are in place. Throughout section 2.4, all requirements/elements shall be understood as commensurate to the risks at the given level.
 - **2.4.7 Compliance and audit**
 - **... HIGH**
 - 1. The existence of periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.
 - 2. Where a scheme is directly managed by a government body, it is audited in accordance with the national law.
- [Veiledning](#) fra Kommisjonen
 - Til 2.4.7 HIGH pkt 1
 - This requirement can be fulfilled by an audit/certification according to ISO/IEC 27007.

Om tillit til det teknologinøytrale e-ID-regimet

- eIDAS gir rettslig likestilling mellom e-ID med og uten pki
 - E-ID-nivåene i eIDAS kap 2 er teknologinøytralt definerte – likestiller e-ID-er, uavhengig av om eller hvordan pki brukes
 - Krav om likebehandling av europeiske og norske e-ID-ordninger
- Tilsynet er uforandret
 - Fortsatt selvdeklarasjon, nå på alle nivåer (før kun nivå 4)
 - NKOM kan kreve tilleggsinfo og revisjonsrapporter, [utkastet](#) til § 10
- Kravsettet er vesentlig utvidet
 - Eksisterende rammeverk
 - én tabell med tre krav for hvert av nivåene 1-3, kravspesifikasjon pki for nivå 4
 - Utkast til nytt rammeverk
 - Vesentlig rikere kravsett på nivå 1-3, sammenlignbar på nivå 4
 - Nivåkrav beskrevet i 16 tabeller (2015/1502), hver med krav til nivåene + norsk tilpasning
 - Dels mer omfattende, dels mindre detaljerte krav enn kravspek pki.
 - Suppleres med veiledning til 2015/1502 og erfaring fra europeiske fagfellevurderinger

Kvalifiserte virksomhetssertifikater eller virksomhetssertifikater fra kvalifiserte tillitstjenestetilbydere?

- Høringsnotatet bruker begge alternativer, vurder gjerne endringsbehov. Se
 - S 12: [§ 7-3](#) første ledd bokstav a
 - ...elektronisk signatur eller segl basert på kvalifisert sertifikat fra en tilbyder av elektroniske tillitstjenester...
 - S 13: [§ 8](#)
 - ... 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...