

Elektronisk signering:

# eIDAS blir norsk lov

eIDAS – en forordning om eID og elektroniske tillitstjenester blir norsk lov og det nye rammeverket utvides til å omfatte flere typer elektroniske tillitstjenester. En Kvalifisert Elektronisk Signatur skal etter forordningen ha samme rettsvirkning i offentlig sektor som en håndskrevet signatur – i alle EU-land.



Sivilingeniør  
Carl H. Pedersen  
Partner i Maestro Soft

Anerkjennelsesplikten gjelder imidlertid ikke for privat sektor. Private aktører har derfor fortsatt formfrihet til selv å fastsette både avtale- og signeringsform. Forordningen oppfordrer likevel privat sektor til å benytte det samme rammeverket.

## eIDAS erstatter esignaturloven

eIDAS – Forordning om eID og elektroniske tillitstjenester: Europaparlaments- og Rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og opphevelse av direktiv 1999/93/EF.

Formålet med forordningen er å legge til rette for økt elektronisk samhandling mellom næringsdrivende, borgere og offentlige myndigheter på tvers av landegrensene i EU/EØS og på den måten bidra til sterkere økonomisk vekst i det indre marked.

Samtidig vises det til at det tidligere direktivet om elektronisk signatur (direktiv 1999/93/EF, esignaturloven) ikke har vært det verktøyet man hadde håpet på for å sikre grensekryssende elektroniske transaksjoner. Forordningen erstatter esignaturloven og både styrker og utvider dette regelverket betraktelig.

Den nye loven trådte i kraft 15. juni 2018.

## Elektronisk identifisering i Norge

Elektronisk identifisering og signering blir stadig mer vanlig. Særlig bruk av MinID og BankID som autentisering til ulike tjenester både innenfor og utenfor bankrelaterte tjenester oppleves som helt vanlig. ID-porten som forvalter pålogging til offentlige tjenester, har opplevd en betydelig økning hvert år siden oppstart i 2008. Antall innlogginger til ID-porten i 2018 kommer trolig til å overstige 120 millioner transaksjoner, (kilde: [www.difi.no/rapporter-og-statistikk/nokkeltall-og-statistikk/digitalisering/id-porten-antall-innlogginger](http://www.difi.no/rapporter-og-statistikk/nokkeltall-og-statistikk/digitalisering/id-porten-antall-innlogginger)) og BankID rapporterer om ca. 600 millioner transaksjoner fra 3,7 millioner unike brukere.



Trolig er Norge et foregangsland når det kommer til utbredelse og anvendelse av elektronisk ID. Vi har en banksektor som har samarbeidet om å etablere en tjeneste for PKI-basert elektronisk identifisering og signering (BankID) og som samtidig er villig til å innta en rolle som ID-leverandør for andre aktører, både offentlige og private. Samtidig har vi som nevnt både ID-porten og Altinn som i dag åpner for elektronisk tilgang til mer enn 1100 nettjenester fra over 600 offentlige virksomheter (kilde: <https://no.wikipedia.org/wiki/ID-porten>).

## eIDAS-forordningen omfatter flere typer tillitstjenester

Mens dagens regelverk regulerer elektronisk identifisering og signering, vil det nye rammeverket utvides til å omfatte flere typer elektroniske tillitstjenester (elektroniske segl, elektronisk tidsstempling, elektronisk meldingsutveksling, sertifikater for websideautentisering og lagringstjenester for esignatur og elektroniske segl).

eIDAS-rammeverket definerer tillitsnivåene lav, betydelig og høy, for de ulike tjenestene. Dette betyr at de fire norske sikkerhetsnivåene må konsolideres slik at de harmoniserer med de europeiske. I praksis benyttes nivå 3

(MinID) og 4 (BankID, Buypass, Commfides) som trolig vil tilsvare henholdsvis Betydelig og Høy. I tillegg omtales tjenestene som Kvalifisert når tjenesten er notifisert og underlagt periodisk tilsyn av nasjonale myndigheter. I praksis betyr dette at tilbydere av kvalifiserte tillitstjenester må få utført en kontroll av et samsvarsvurderingsorgan («conformity assessment body») og melde dette til Nasjonal Kommunikasjonsmyndighet (NKOM) før tjenesten kan bli godkjent som en kvalifisert tjeneste fra tilbyderen.

Pr. mai 2018 er det 189 tilbydere av Kvalifiserte Sertifikater for elektronisk signatur i EU/EØS, hvorav ni i Norge



*En Kvalifisert Elektronisk Signatur har samme rettsvirkning som en håndskrevet signatur, og skal regnes som Kvalifisert Elektronisk Signatur i alle EU-land.*

(BankID (6), Buypass, Commfides og Equinor/Statoil) (se <https://webgate.ec.europa.eu/tl-browser/#/>). Merk at verken Sverige eller Danmark ennå har tilbydere av Kvalifiserte Sertifikater for elektronisk signatur.

### Anerkjennelsesplikt for offentlige tjenester

Det er i første omgang offentlige tjenester som berøres av det nye regelverket. Når offentlig sektor krever identifisering eller signering med notifisert elektronisk ID, skal den offentlige tjenestetilbyderen også anerkjenne identifisering eller signaturer med utenlandsk eID på lik linje med de norske ID-løsningene.

Det er ikke dermed sagt at alle europeere er autorisert for å benytte de offentlige norske tjenestene, men ID-porten må støtte identifisering av personer utenfor Norge så lenge de har en elektronisk ID utstedt av en notifisert ID-løsning på samme nivå eller høyere, tilsvarende kravet til de norske ID-løsningene i tjenesten. Utenlandske personer må likevel få norsk d-nummer og koble dette til sin elektroniske ID før de kan bli autorisert for faktisk bruk av norske tjenester.

Det betyr heller ikke at nordmenn umiddelbart får tilgang til offentlige tjenester i andre europeiske land med sin BankID. Det kan kun skje dersom landets offentlige tjenesteeier stiller

krav om bruk av notifisert eID. Tilsvarende må man også få et midlertidig personnummer i det aktuelle landet før tjenestene kan tas i bruk.

### Offentlig vs. privat sektor

Det er ikke sikkert at eIDAS-forordningen stod øverst på ønskelisten til offentlig sektor i Norge. Det kan virke som om anerkjennelsesplikten skaper flere problemer enn den løser, særlig for Difi og ID-porten som må integrere seg mot en rekke andre eIDAS-noder i Europa. Samtidig er det ca. 1,6 millioner personer med aktive d-nummer i Norge, som allerede har mulighet til å anskaffe elektronisk ID fra norske ID-leverandører og benytte seg av norske offentlige tjenester på den måten.

Privat sektor har imidlertid ikke den samme tilgangen til de offentlige ID-portalene, og samhandling mellom private aktører foregår heller ikke via et rammeverk for strukturerte data som det offentlige gjør med skjema-definisjoner og innrapportering via Altinn. Privat sektor er likevel i mange situasjoner lovpålagt å foreta både legitimering, signering og alderskontroll. Kunde kontroll i henhold til hvitvaskingsloven er et eksempel som i stor grad følger de samme reglene i Europa, og eIDAS gjør det mulig for en person å legitimere seg elektronisk på et nivå som kan anerkjennes som tilfredsstillende ved etablering av kunde forhold i hele Europa.

De offentlige tjenestene anvender i liten grad elektronisk signering. Fordi man først identifiserer seg ved pålogging til ID-porten, krever de fleste tjenestene bare at man trykker på en knapp som det står «Signer og send inn» for å forplikte seg, selv om ikke dette er elektronisk signering etter eIDAS-rammeverket. Riktignok likestiller forordningen elektronisk underskrift bare med en håndskrevet underskrift, men en Kvalifisert Elektronisk Signatur (QESign) er likevel et langt kraftigere verktøy for privat sektor enn en håndskrevet underskrift. Nettopp fordi en signatur ikke bare autentiserer signatørene, men også tidfester og sikrer dokumentinnholdet, har man oppnådd samme sikkerhet og dataintegritet som avkrevs i det offentlige på høyeste sikkerhetsnivå. Samtidig kan signerte dokumenter kopieres, sendes på e-post, lagres på alt fra minnepinner til skytjenester både innenfor og utenfor sikre nettverk, og likevel ivareta det autentiske innholdet og de påførte signaturene.

### Rettsvirkning for elektronisk signatur

Ifølge forordningen skal en Kvalifisert Elektronisk Signatur ha samme rettsvirkning som en håndskrevet signatur (EU910/2014, Art. 25, pkt. 2), og skal regnes som Kvalifisert Elektronisk Signatur i alle EU-land.

Anerkjennelsesplikten gjelder imidlertid ikke for privat sektor. Private aktører har derfor fortsatt formfrihet til selv å fastsette både avtale- og signeringsform. Forordningen oppfordrer likevel privat sektor til å benytte det samme rammeverket. Når offentlige tjenester ikke kan kreve høyere sikkerhetsnivå enn Kvalifisert Elektronisk Signering (EU910/2014, Art 17, pkt. 3), kan dette være en rettesnor også for privat sektor.

### Når digitale signaturer er gyldige

Etter norsk lov (Lov om avslutning av avtaler, om fuldmagt og om ugyldige viljeseerklæringer [avtaleloven]) er det partene selv som fastsetter på hvilken måte de ønsker å forplikte seg til en avtale, og en muntlig avtale kan derfor være like bindende som en skriftlig med digital signatur. Juridisk gyldighet er heller et spørsmål om hvorvidt det kan sannsynliggjøres at partene hadde til hensikt å forplikte seg til en avtale. I denne sammenhengen vil signatur være én faktor, men også det at partene har etterlevd en avtale over tid, kan bidra til å sannsynliggjøre at avtalen fortsatt forplikter partene.

Dersom det ikke er snakk om en gjensidig avtale mellom to parter, men selskapsdokumentasjon som årsregnskap, styreprotokoller, fullmakter og revisjonsberetning, vil dokumentets gyldighet i større grad hvile på signaturene i dokumentet. En kvalifisert elektronisk signatur er tilnærmet umulig å forfalske og gir oss først og fremst en teknisk gyldighet som langt overgår håndskrevne underskrifter.

### Hvordan man vet at et dokument er elektronisk signert i tråd med forordningen

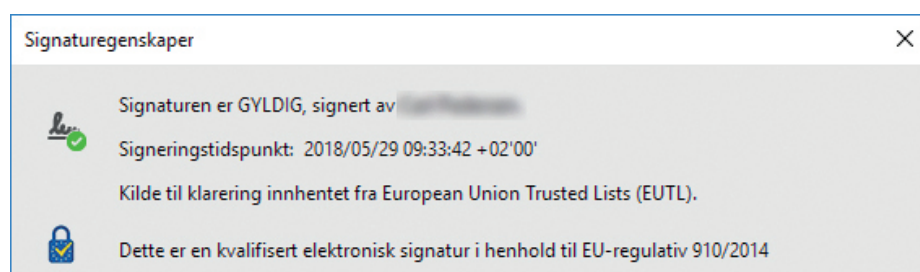
Elektroniske dokument- og signaturformater som skal anerkjennes av offentlige myndigheter, reguleres av Kommisjonens gjennomføringsbeslutning (EU) 2015/1506 av 8. september 2015.

Gjennomføringsrettsakten omfatter flere formater, blant annet PAdES, XAdES, og CAAdES. Medlemsland kan også benytte andre formater gitt at det

etableres en valideringstjeneste for formatet. Felles for de nevnte formatene er at de benytter Avansert Elektronisk Signering. Særlig PAdES (PDF med Avansert Elektronisk Signatur) kan både leses og valideres gratis i vanlig PDF-leser. Adobe Acrobat Reader har god støtte for både visning og validering av PAdES dokumenter, herunder validering i henhold til tillitstjenestene i EU (EUTL). Også andre PDF-lesere støtter visning av PAdES dokumenter, men kan være noe umodne i forhold til valideringsfunksjonaliteten.

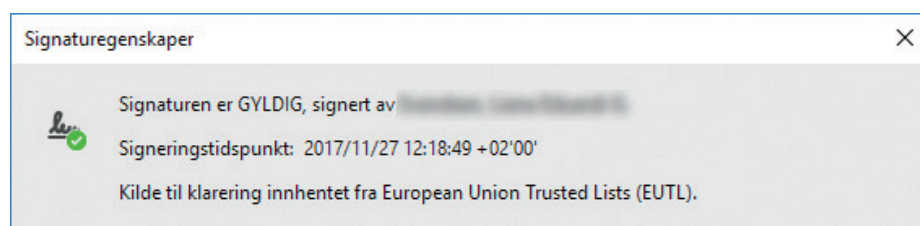
### Autentisering – valideringsfunksjon i pdf

Hvordan vet man at et dokument er autentisk med gyldige signaturer i tråd med forordningen? For PDF-dokumenter utføres dette relativt enkelt ved å benytte valideringsfunksjonen i PDF-leseren. Dersom denne viser at signaturen er gyldig, signert av forventet person, og at signaturen er i henhold til EU-regulativ 910/2014, har man et dokument og en signatur som følger retningslinjene i forordningen til punkt og prikke. Bildet under viser Signaturegenskaper for en Kvalifisert Elektronisk Signatur (med sertifikat fra QuoVadis EU Issuing Certification Authority G4).



### Gyldige norske løsninger

De norske eID-løsningene (BankID, Buypass, og Commfides) valideres også som gyldige og klarerte i henhold til EUTL, men mangler foreløpig betegnelsen Kvalifisert etter EU-regulativ 910/2014. Bildet under viser Signaturegenskaper for PAdES med norsk BankID-signatur.



De nevnte norske eID-løsningene er allerede registrert i EUTL som kvalifiserte sertifikatutstedere, og vil også kunne oppnå Kvalifisert nivå på signering etter at forordningen trer i kraft slik at de også kan nyte godt av rettsvirkning utenfor Norge.

### På-vegne-av-signaturer

Enkelte eID-løsninger støtter ennå ikke ekte PAdES (for eksempel svensk BankID og danske NemID), eller tilbyr bare ren identifisering (for eksempel nederlandske iDIN).

En tilnærming i slike tilfeller er at signaturportalen velger å tilby en løsning som signerer med et virksomhetssertifikat på vegne av personen som kanskje bare har foretatt en ren identifisering med den aktuelle eID-løsningen. Selv om dette kan fremskaffe et teknisk gyldig PAdES format, mangler likevel sertifikatet til signaturen i signaturen. Denne teknikken gjør det likevel mulig å signere digitalt uavhengig av styrken til den underliggende eID-løsningen. Slike på-vegne-av-signaturer er imidlertid ikke en del av rammeverket i eIDAS-forordningen, men kan være tilstrekkelig og gyldig i privat sektor der man er fri til å anerkjenne ulike signaturvarianter.