

Strategi for signeringstjenesten

2017 - 2022

Difi rapport 2017:3

ISSN 1890-6583

Forord

Det er tverrpolitisk enighet om at forvaltningens kommunikasjon med innbyggere og næringsliv på sikt skal være nettbasert. Nasjonale felleskomponenter er byggeklosser som alle offentlige virksomheter skal dra nytte av når de utvikler sine digitale tjenester. De overordnede mål er «enklere møte med døgnåpen offentlig sektor, høyere kvalitet i tjenestene, økt verdiskaping og bedre beslutninger» (Regjeringen, 2013).

Difi har ansvaret for å forvalte og videreutvikle signeringstjenesten, slik at virksomhetene kan kommunisere digitalt med innbyggerne i tråd med ambisjonen om et digitalt førstevalg. Dette innebærer at tjenesten er enkel i bruk og løser virksomhetenes behov på en effektiv måte. Målet med strategien er å gi forutsigbarhet for tjenestens kunder og samarbeidspartnere med tanke på hvordan den skal utvikle seg de nærmeste årene.

Vi takker tjenestens kunder som har bidratt med gode innspill underveis.

Arbeidet er utført av Stig Hornnes og Sindre Ramung i Difi. Arbeidet er gjennomført i perioden fra og med januar til og med mars 2017.

Oslo 20. april 2017

Torgeir Strypet
avdelingsdirektør

Innhold

1	Sammendrag	1
2	Innledning	3
2.1	Formål	4
2.2	Kort beskrivelse av signeringstjenesten	4
2.2.1	Tilgjengelige signaturer	5
2.2.2	Portal og maskingrensesnitt	7
2.2.3	Støttetjenester	8
2.3	Avgrensning	10
2.4	Signeringstjenestens kunder og sluttbrukere	10
3	Mål og visjon	12
4	Strategi	14
4.1	Signeringstjenestens kontekst	14
4.1.1	E-signering for personer	14
4.1.2	Loggbasert signering	15
4.1.3	E-signering for virksomheter (forsegling)	16
4.1.4	Tidsstempling	16
4.2	Behandling av innmeldte behov	16
4.3	Strategi for signering	17
4.4	Strategi for støttetjenester	19
4.4.1	Integrerte støttetjenester	19
4.4.2	Tilleggstjenester	20
5	Videre forvaltning av strategien	21

1 Sammendrag

Signeringstjenesten *eSignering* tilbyr en tjeneste for elektronisk signatur for privatpersoner til bruk for offentlige virksomheter, i tillegg til en tjeneste for langtidsvalidering av signaturer og en tjeneste for arkivering av signerte dokumenter. Virksomhetene kan bruke signeringstjenesten via en portal hvor dokumentene lastes opp manuelt, eller de kan integrere tjenesten inn i sine egne løsninger, slik at innbyggeren bruker tjenesten i virksomhetens egen kontekst.

Signeringstjenesten skal understøtte de ulike politiske ambisjonene rundt blant annet digitalt førstevalg.

- Tilby signering med et tilstrekkelig nivå av sporbarhet og beviskraft for offentlige virksomheter og innbyggere, for de mest utbredte brukstilfellene for elektronisk signatur for privatpersoner i offentlig sektor.
- Understøtte prinsippet om digitalt førstevalg ved å effektivisere tidsbruk i offentlige virksomheter knyttet til elektronisk signatur for privatpersoner gjennom kostnadseffektiv digitalisering av manuelle arbeidsprosesser, med de formkrav som til enhver tid stilles i relevant lovverk.
- Tilby en tjeneste som er enkel, robust, pålitelig og sikker for offentlig sektor og for innbyggerne.

Med bakgrunn i disse målene har signeringstjenesten følgende visjon:

Signeringstjenesten skal tilby en effektiv tjeneste for elektronisk signatur for privatpersoner med tilstrekkelig beviskraft og sporbarhet.

Strategien deles inn i to områder som vil bli behandlet. Det største og viktigste området er strategi for signering, mens det andre området er strategi for støttetjenester. Det finnes flere støttetjenester som en del av løsningen.

Signeringstjenesten skal bidra til å sikre brukervennlige, praktiske og effektive tjenester ved å fjerne manuelle prosesser og oppnå et tilstrekkelig nivå av sporbarhet og beviskraft for elektroniske dokument. For å nå dette målet har Difi satt opp følgende delmål for tjenesten i strategiperioden:

- Signeringstjenesten skal være kostnadseffektiv utfra de behovene offentlige virksomheter har.
- Det skal være mulig å signere med utenlandske sertifikater.
- Det skal være mulig å få validert utenlandske signaturer.
- Det skal være mulig å bevise en knytning mellom personnummer og organisasjonsnummer når en person signerer på vegne av en organisasjon.
- Signeringstjenesten skal tilby e-signatur med nasjonalt ID-kort.
- Difi skal etablere en fast referansegruppe for signeringstjenesten.

Det finnes flere støttetjenester i løsningen som virksomhetene kan ta i bruk. Støttetjenestenes funksjon er å understøtte forretningsprosesser som involverer

personlig e-signatur på en effektiv måte. Difi skiller mellom integrerte støttetjenester og tilleggstenester. Integrerte støttetjenester er av en slik karakter at de er nødvendige å bruke (av funksjonelle eller juridiske årsaker) for å kunne realisere elektronisk signering for privatpersoner. Tilleggstenester bidrar til å understøtte forretningsprosesser der elektronisk signatur for privatpersoner inngår, men er ikke nødvendige (funksjonelt eller juridisk) for å kunne gjennomføre prosessen. Følgende mål er satt for støttetjenestene:

- Signeringstjenesten tilbyr støttetjenester som realiserer delprosesser som naturlig henger sammen med personlig e-signering eller administrasjon av personlig e-signering og som effektiviserer disse prosessene.
 - Effektive, sikre og praktiske administrasjonstjenester som dekker tjenesteeiernes behov.
 - Signaturvedlikehold tilbys som tilleggsteneste slik at levetiden til kryptografien i det signerte dokumentet forlenges og kan valideres over lengre tid.
 - Varsling til personer med signaturfullmakt/prokura tilbys som tilleggsteneste.

2 Innledning

Våren 2016 lanserte Difi en ny fellestjeneste for elektronisk signatur for privatpersoner til offentlige virksomheter, kjent som *eSignering*.

Mange virksomhetsprosesser i offentlig sektor involverer signatur - et behov som enten springer ut fra et lovkrav, fra en risikovurdering eller benyttes fordi signatur oppfattes som en hensiktsmessig sikkerhetsmekanisme i den aktuelle prosessen. Formålet med signaturen er å tydeliggjøre ansvar og forpliktelser hos partene som signerer og å sikre innholdet i det signerte dokumentet fra å kunne endres. Dette for å redusere risiko for at en av partene ikke vedkjenner seg innholdet i de aktuelle dokumentene. I slike virksomhetsprosesser kan elektronisk signatur som regel erstatte manuell/fysisk signatur.

Manuell/fysisk signatur er tid- og kostnadskrevende, siden dokumenter må skrives ut på papir, konvolutteres, adresseres, frankeres, postlegges, fraktes til mottaker (2-3 dager), signeres, legges i ny konvolutt, adresseres, postlegges, fraktes tilbake (2-3 dager), åpnes og skannes og til slutt arkiveres. Ved å digitalisere prosesser der manuell/fysisk signatur er nødvendig i dag, bidrar offentlige virksomheter til digitalt førstevalg. Tida fra et dokument er utstedt til det foreligger i signert form kan kortes vesentlig ned fordi man kutter postgang i begge ender av prosessen. Signeringstjenesten er etablert som en felles tjeneste for offentlig sektor for å kunne løse dette behovet hos virksomhetene¹.

Dette dokumentet beskriver signeringstjenestens visjon og strategi for de neste fem årene. Målgruppen for dokumentet er nåværende kunder, fremtidige kunder og personer med ansvar for tjenesteutvikling i eller på vegne av offentlige virksomheter. Sammen med tre-årige roadmaps som viser en grov overordnet utviklingsplan og årlige handlingsplaner gir dette signeringstjenestens brukere trygghet og forutsigbarhet for videre utvikling.

Strategien beskriver den retningen signeringstjenesten vil utvikles i perioden 2017-2022. De behov som kundene har meldt inn og vurderingen av disse har vært førende for utforming av strategien. I strategien beskrives også signeringstjenestens visjon, hvor strategien vil ligge til grunn for å nå denne. Det kan oppstå behov for endringer i perioden. Dette vil hovedsakelig oppstå som følge av:

- Nye politiske vurderinger og endringer i regelverk som påvirker tillitstjenester som signeringstjenesten
- Teknologiutvikling
- Innovasjon hos kundene

Strategien tar ikke stilling til i hvilke virksomhetsprosesser elektronisk signatur bør inngå, siden dette medfører strategiske og arkitekturmessige vurderinger som strekker seg utover signeringstjenesten som produkt.

¹ Posten anslår at samfunnsøkonomisk gevinst pr elektronisk signerte dokument er 50 kr sammenlignet med manuell/fysisk signatur.

2.1 Formål

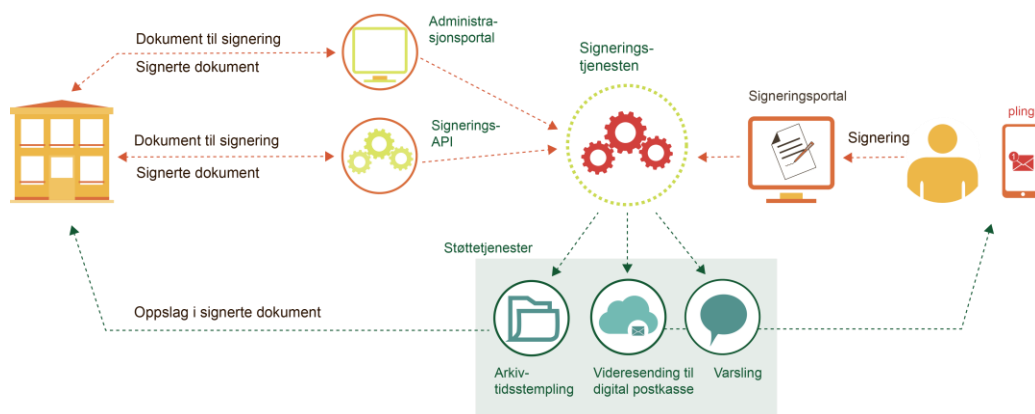
Strategien for signeringstjenesten skal bidra til at de overordnede målene og visjonen nås. Målene og visjonen er utarbeidet i samarbeid med virksomheter som bruker tjenesten. Strategien skal også bidra til at kundene opplever forutsigbarhet og åpenhet i utviklingen av signeringstjenesten. Dette er også viktig for andre interessenter, slik som andre felleskomponentforvaltere og Skate. Åpenhet i utviklingen av felleskomponenter er viktig for å sikre at løsningene i størst mulig grad utfyller hverandre og i minst mulig grad overlapper hverandre. Målet er at strategien skal bidra til dette på en god måte.

Skate har etablert en strategi for nasjonale felleskomponenter med tilhørende handlingsplan². Strategien legger opp til at felleskomponentene skal samordnes mer på tvers og koordineres slik at felleskomponentene inngår i stadig nye løsninger og støtter opp om en felles arkitektur³. Signeringstjenesten er laget for å kunne integreres i offentlige virksomheters tjenester, og slik bidra til at virksomhetene kan digitalisere sine tjenester på en effektiv måte.

2.2 Kort beskrivelse av signeringstjenesten

Signeringstjenesten tilbyr en tjeneste for elektronisk signatur for privatpersoner til bruk for offentlige virksomheter, i tillegg til en tjeneste for langtidsvalidering av signaturer og en tjeneste for arkivering av signerte dokumenter. Virksomhetene kan bruke signeringstjenesten via en portal hvor dokumentene lastes opp manuelt, eller de kan integrere tjenesten inn i sine egne løsninger, slik at innbyggeren bruker tjenesten i virksomhetens egen kontekst.

Posten er leverandør av signeringstjenesten. Signicat er underleverandør og fungerer som tiltrodd tredjepart som bevitner og garanterer for autentisiteten til signeringen fremstilt i signeringstjenesten.



Figur 1 Signeringstjenesten

² <https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/skate/veikart/strategi>

³ <https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/nasjonal-arkitektur>

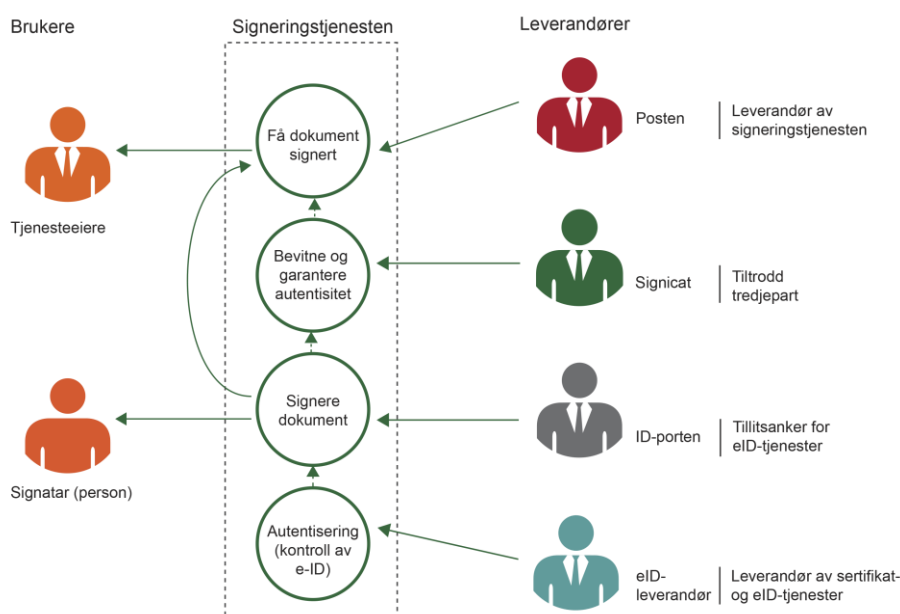
2.2.1 Tilgjengelige signaturer

Da tjenesten ble etablert var det kun avansert signatur som var tilgjengelig i løsningen. I januar 2017 ble signeringstjenesten utvidet til å omfatte elektronisk signatur, som i tjenesten er omtalt som autentisert signatur. Formålet med utvidelsen var å tilby et supplement til avansert e-signatur som legger til rette for at innbyggere som ikke har eID på sikkerhetsnivå 4 eller som foretrekker andre eID-produkt i ID-porten enn BankID/Buypass kan signere med disse, samtidig som at kostnadene for transaksjoner som ikke nødvendigvis krever avansert e-signatur reduseres.

2.2.1.1 Autentisert e-signering

En autentisert e-signatur er en signatur fremstilt på grunnlag av en autentisering i ID-porten på minimum sikkerhetsnivå 3 eller 4. Dokument og bevis fra signeringsseremonien (inkludert autentiseringen) forsegles av en tiltrodd tredjepart (Signicat). I tjenesten for autentisert e-signering er ID-porten tillitsanker for eID-tjenestene som benyttes for å autentisere signatøren. eID-leverandøren er ansvarlig for selve autentiseringen.

En autentisert e-signatur vil ikke ha like sterk beviskraft som en avansert e-signatur i signeringstjenesten, siden dokumentet ikke signeres med innbyggerens privatnøkkel, men baserer seg på en autentisering med innbyggerens eID (eID på sikkerhetsnivå 3 eller PKI-basert eID på nivå 4), som så knyttes til dokumentet av en tiltrodd tredjepart. Siden det finnes svært få tilfeller hvor det kreves en avansert signatur, vil autentisert e-signatur med tilnærmet samme beviskraft være tilstrekkelig for de aller fleste brukstilfeller. Den autentiserte signaturen er dessuten enklere for innbygger, fordi den gjør det mulig å bruke alle de ulike eIDene som tilbys gjennom ID-porten. Det innebærer blant annet at det er mulig å signere ved hjelp av mobiltelefon. Samtidig blir kostnadene for den enkelte virksomhet betydelig lavere.



Figur 2 Autentisert e-signering

2.2.1.2 Avansert e-signering

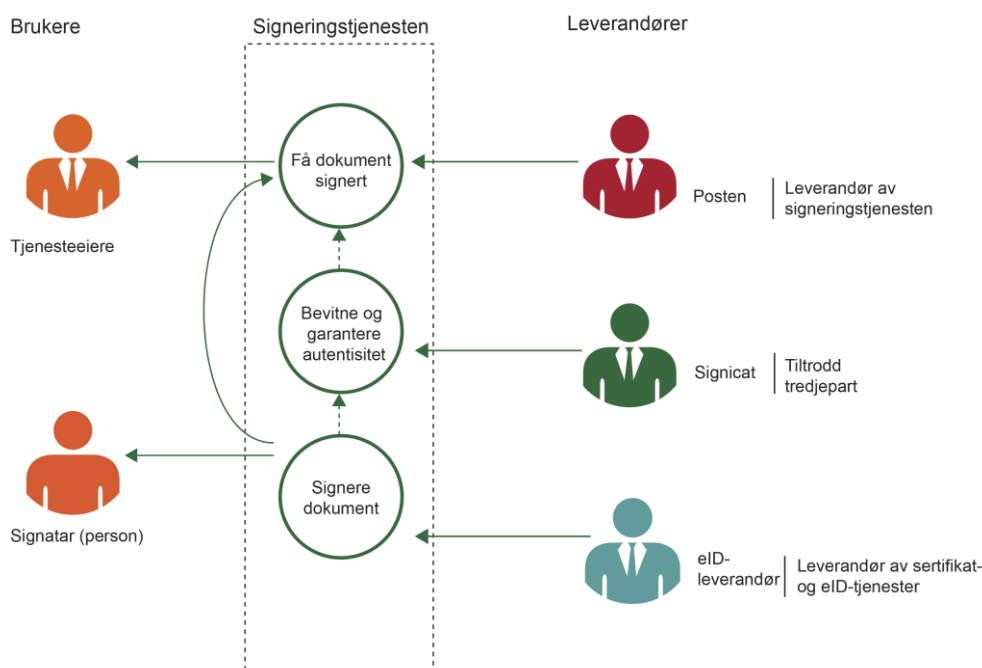
Avansert elektronisk signatur er en kryptografisk sjekksum generert over et dokument. Sjekksommen fremstilles ved hjelp av sertifikatnehaverens privatnøkkel. Sjekksommen kan valideres ved bruk av sertifikatnehaverens offentlige nøkkel.

e-signaturlova (§ 3, punkt 2) definerer avansert elektronisk signatur som en elektronisk signatur som

- a) entydig knyttet til undertegneren,
- b) kan identifisere undertegneren,
- c) er laget ved hjelp av midler som bare undertegneren har kontroll over, og
- d) er knyttet til andre elektroniske data på en slik måte at det kan oppdages om disse har blitt endret etter signering

I tjenesten for avansert e-signering er eID-leverandøren ansvarlig for kontroll av signatarens identitet og muliggjør e-signering med signatarens sertifikat.

Løsningen for avansert e-signering benytter kvalifiserte sertifikat. Lov om elektronisk signatur (e-signaturloven) fastsetter blant annet krav til kvalifiserte sertifikater og utstedere av disse. Løsningen er integrert med BankID og Buypass, som er tilbydere av kvalifiserte sertifikater (se www.nkom.no). Når signering gjøres med signeringsnøkler tilhørende disse sertifikatene, oppfyller signeringstjenesten e-signaturlovens krav til avansert elektronisk signatur.



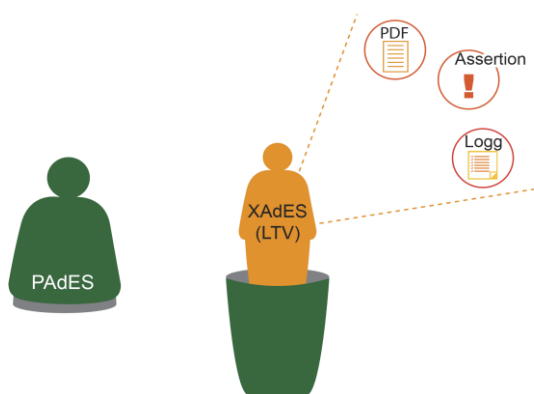
Figur 3 Avansert e-signering

2.2.1.3 Felles for autentisert og avansert e-signering

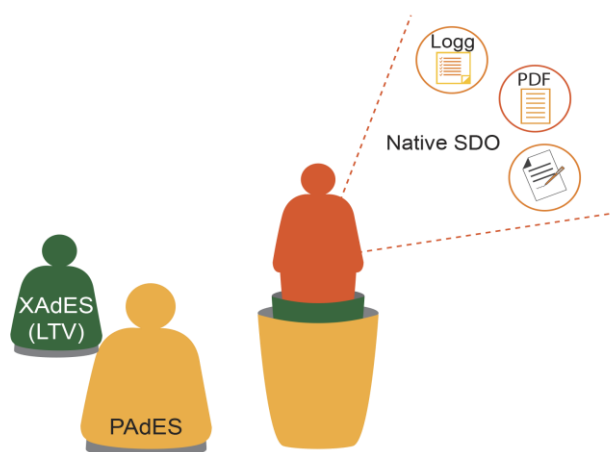
e-Signatur i signeringstjenesten er langtidvaliderbar (LTV). Det signerte dokumentet med logg og signeringskontekst er realisert i XAdES-format

(signert XML). XAdES er et integrert vedlegg til en PAdES (signert PDF). PAdES er en representasjon av det signerte dokumentet som skal gjøre det lettere å lese, validere og arkivere. PAdES er deklart i arkivkompatibelt format og kan arkiveres direkte.

Signaturen (identifikasjon, logg og signert dokument) bevitnes og forsegles av Posten (PAdES) og Signicat (XAdES) som tiltrudde tredjeparter.



Figur 4 PAdES autentisert e-signatur



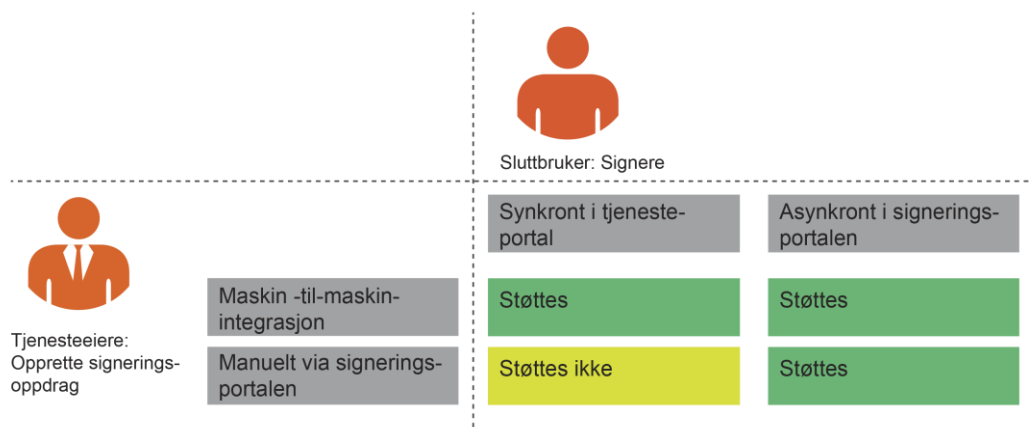
Figur 5 PAdES avansert e-signatur

2.2.2 Portal og maskingrensesnitt

Signeringstjenesten kan brukes enten via et portalgrensesnitt eller et maskingrensesnitt.

Portalgrensesnittet gjør det mulig for en virksomhet å ta i bruk signeringstjenesten uten å gjøre noen tekniske integrasjoner. Dokumentene som skal signeres lastes manuelt inn i portalen, og innbygger må logge inn i portalen for å få tilgang til dokumentene og signere dem. Portalgrensesnittet kan brukes i de tilfeller hvor signeringen er initiert av virksomheten. Dette kalles asynkron signering. Dvs. at innbyggeren ikke er i en aktiv dialog med virksomheten som utstedte signeringsoppdraget når han signerer dokumentet. Dette er en enkel og effektiv måte å komme i gang med signeringstjenesten, og passer bra for mindre volumer.

Maskingrensesnittet krever en teknisk integrasjon mellom virksomheten og signeringstjenesten. Ved å gjøre dette innbygger forholde seg til virksomhetens portal, og signeringstjenesten vil oppleves som en integrert del av virksomhetens tjeneste. Når en virksomhet har tatt i bruk maskingrensesnittet er det også mulig for en innbygger å signere et dokument på vei inn, for eksempel en søknad. Dette kalles synkron signering, altså at innbygger signerer som en del av den aktive dialogen innbyggeren har med virksomheten som utsteder signeringsoppdraget.



Figur 6 Bruksscenario for Signeringstjenesten

2.2.3 Støttetjenester

I tillegg til å tilby en tjeneste for signering, har Difi i avtalen med Posten flere tilleggstjenester som virksomhetene kan velge å benytte seg av. Dette er støttetjenester som naturlig henger sammen med personlig e-signering og således støtter oppunder signeringstjenesten.

2.2.3.1 Administrasjon

Signeringstjenesten tilbyr tjenesteeiere to grensesnitt for administrasjon, ett for maskin-til-maskin-integrasjoner og ett integrasjonsfritt portalgrensesnitt. Begge grensesnittene tilbyr samme funksjonalitet til brukerne.

Maskin-til-maskingrensesnittet er et REST-grensesnitt basert på to vegs TLS sikret vha. virksomhetssertifikat. Portalgrensesnittet er sikret med tilgangsstyring på personnivå (virksomheten autoriserer selv personer som skal ha tilgang) med autentisering på sikkerhetsnivå 4.

Sentraladministratoren Difi, administrer virksomhetenes tilgang og metadata via et webgrensesnitt med avgrenset personlig tilgang gjennom autentisering på sikkerhetsnivå 4.

2.2.3.2 Varsling

Varslingsfunksjonalitet er ansett å være nødvendig for å kunne realisere asynkron signering på en hensiktsmessig måte. Målet med tjenesten er å

- Tilby varsling om dokumenter til signering i asynkrone bruksscenarier

- Bidra til at avsenderen oppfylder varslingsplikten iht. eForvaltningsforskriftens § 8
- Tilby integrert oppslag mot Kontakt- og reservasjonsregisteret (KRR) slik at avsenderne slipper å etablere hver sine integrasjoner/forretningsprosesser for varsling

Bruk av varslingsfunksjonaliteten er aktuelt for de to bruksscenariene med asynkron signering. I begge disse tilfellene vil sluttbrukeren logge seg inn i signeringstjenesten manuelt for å gjennomføre signeringen. Det er en forutsetning at brukeren får beskjed om dette, enten direkte fra tjenesteeieren eller fra signeringstjenesten. Dersom tjenesteeierne skal håndtere dette selv, vil det kunne gi en varierende brukeropplevelse. For det synkrone bruksscenariet der signeringstjenesten brukes som en del av tjenesteeiers egen flyt vil det ikke være behov for varsling. Varsling er i dag en integrert del av tjenesten for asynkron e-signering.

Signeringstjenesten tilbyr varsel på både SMS og e-post. Varsel sendes enten til brukerens kontaktinformasjon fra KRR, eller til tjenesteeiers spesifiserte kontaktinformasjon.

Signeringstjenesten tilbyr påminnelsesvarsling dersom bruker etter en spesifisert tid ikke har fullført eller kansellert signeringsoppdraget.

Varsling er tilgjengelig både for API- og portalbrukere.

For dokumenter der signatøren ikke skal signere som privatperson, men som representant for en virksomhet registrert i enhetsregisteret, skal det ikke gjøres oppslag i KRR jf. eForvaltningsforskriftens § 8. I disse tilfellene kan tjenesteeieren overstyre data fra KRR - både i API og i portal.

2.2.3.3 Videre sending av signerte dokumenter til digital postkasse

Tjenesten tilbyr videre sending av signerte dokumenter til innbyggerens digitale postkasse. På denne måten får innbyggeren tilgang til

- Sikker oppbevaring av signerte dokument i personlig arkiv
- Ved multesignataroppdrag får han tilgang til dokumentet signert av alle parter, ikke bare seg selv

For tjenesteeieren kan gevinstene oppsummeres slik:

- Slipper å tilby arkivfunksjonalitet til innbyggeren som signerer
- Slipper å selv etablere prosess for videre sending av signerte dokument til innbyggeren sin digitale postkasse

Personer som har aktiv postkasse får signerte dokument sendt dit. Også dokument med multesignatur (dvs. som er signert av flere) blir sendt til aktive postkasser når alle partene har signert. Slik får signatørene ett dokument i postkassa som inneholder alle partene sine signaturer.

Brukere som ikke har postkasser og som ikke er reservert eller mangler kontaktinfo i KRR, får info om at de kan opprette postkasse og få ettersendt det signerte dokumentet. Hvis ikke gir signeringstjenesten innbyggeren muligheten til å laste ned dokumentet til sin egen enhet. Nedlasting er også tilgjengelig for brukere med aktiv digital postkasse, om de har behov for det.

Tjenesteeieren kan unnta et dokument fra videresending til digital postkasse ved å oppgi at dokumentet signeres i kraft av en rolle, stilling eller ansvar (altså ikke som privatperson). Så lenge videresendingstjenesten er en tilleggstjeneste, kan tjensteeierne si nei til bruk.

2.2.3.4 Arkiv og langtidvalidering

Arkivtjenesten som tilbys er et skybasert arkiv som for arkivering av signerte dokument som skal arkivsigneres (langtidspreserveres). Tjenesten benytter samme datalager som signeringstjenesten for øvrig, men tilbyr lagring av dokumentene inntil 50 år (mot 30 dager ellers). Tjenesten for langtidvalidering gjør at virksomhetene kan overlate den operative delen av signaturvedlikeholdet til signeringstjenesten. Ved bruk av tjenestene for arkiv og langtidvalidering er det altså signeringstjenesten som sørger for at dokumentene som er sjekket inn i arkivet blir periodisk arkivsignert av en tidsstemplingsautoritet og så lagret på nytt i arkivet.

Arkivtjenesten er ikke NOARK-kompatibel. Det betyr at tjenesteeierne også må arkivere de signerte dokumentene i sine NOARK-arkiver.

2.3 Avgrensning

Denne produktstrategien er en strategi for hvordan signeringstjenesten skal utvikle seg de neste fem årene. Det er ikke en strategi for hvordan den enkelte virksomhet skal ta i bruk signeringstjenesten og tilpasse egne systemer, som er kundenes eget ansvar.

I arbeidet med produktstrategien har det kommet innspill om å utvide tjenesten til å også inkludere signering med virksomhetssertifikater. Det vil være en utvidelse av formålet med dagens tjeneste, som er å tilby signering med personsertifikater. Det er også usikkert hvilke behov en slik tjeneste skulle dekke, og det er eventuelt nødvendig å gjøre vurderinger av arkitektur på tvers av offentlige virksomheter før man kan ta stilling til en slik tjeneste. Et slikt bruksområde er trolig heller ikke dekket av de avtalene Difi har inngått med Posten. En slik utvidelse er derfor ikke behandlet i denne strategien.

2.4 Signeringstjenestens kunder og sluttbrukere

Signeringstjenesten tilbyr en tjeneste for elektronisk signatur for privatpersoner for offentlige virksomheter. Tjenestens kunder er:

- Tilsyn, ombud eller direktorat
- Fylkeskommune, kommune, eller kommunale etater
- Offentlig eide selskap som bare leverer tjenester til det offentlige

- Offentlige virksomheter og andre virksomheter som utfører oppgaver på vegne av, og som delvis eller helt er finansiert av det offentlige

Kundegruppen består dermed av alt fra store statlige virksomheter til små kommunale enheter og private virksomheter. Disse har ulike forutsetninger, men har alle sammen et behov for digital kommunikasjon med innbyggere.

3 Mål og visjon

I «Digital agenda for Norge— IKT for vekst og verdiskaping» (Meld. St. 23 (2012–2013)) gav Stortinget sin tilslutning til målsetningen om et digitalt førstevalg. Dette innebærer blant annet at det offentlige skal tilby elektroniske tjenester til innbyggerne. Som en del av meldingen lå det føringer om at ID-porten skulle «videreutvikles til også å tilby elektronisk signering og kryptering. Elektronisk signering vil gjøre det mulig å kommunisere elektronisk der hvor det i dag må signeres på papir.» Disse føringene lå til grunn for etableringen av en felles offentlig tjeneste for avansert e-signatur.

Oppfølgingen av denne meldingen kom i form av stortingsmelding 27 (2015-2016) *Digital Agenda for Norge* hvor Stortinget peker på at digitalt førstevalg skal styrkes og at innbyggeren aktivt må velge manuelle alternativer til digital kommunikasjon. Digital agenda har følgende hovedprioriteringer som er relevant for signeringstjenesten:

- Brukeren i sentrum
- Effektiv digitalisering av offentlig sektor
- Godt personvern og god informasjonssikkerhet

Signeringstjenesten søker å ivareta alle disse aspektene i løsningen.

- Det skal være enkelt for innbyggerne å signere et dokument som en virksomhet har tilgjengeliggjort. Signeringstjenesten gjør bruk av andre nasjonale fellesløsninger der det er relevant, slik som Kontakt- og reservasjonsregisteret for gjenbruk av innbyggers digitale kontaktinformasjon og digital postkasse for utsending av ferdig signerte dokumenter. Signeringstjenesten har også en tett kopling mot ID-porten, både som autentisering av innbygger og for å realisere autentisert signatur. Dette skaper en helhetlig tjeneste for innbyggeren.
- Signeringstjenesten kan inngå som en integrert del av virksomhetens tjenester. På denne måten kan signeringstjenesten utfylle eksisterende løsninger hos virksomhetene, og bidra til at offentlig sektor kan tette et gap i digitaliseringen på en effektiv måte. En fellestjeneste er også prisgunstig.
- Signeringstjenesten har kontinuerlig fokus på risiko og sårbarhet for å sikre godt personvern og god informasjonssikkerhet.

Behovet for en felles offentlig tjeneste for elektronisk signatur er også dokumentert i flere offentlige strategier.

- Utkast til *Nasjonal eID-strategi*⁴ legger opp til at felles behov knyttet til autentisering og signering skal løses gjennom ID-porten og signeringstjenesten. Strategien legger videre opp til brukervennlig og gratis autentisering og signering med e-ID (mål 2.1).
- *Strategien for ID-porten*⁵ peker på at signeringstjenesten skal bidra til å sikre brukervennlige, praktiske og effektive tjenester ved å fjerne manuelle prosesser og oppnå et tilstrekkelig nivå av sporbarhet og beviskraft for elektroniske dokument.

⁴ Utkastet ligger per mars 2017 til behandling i Kommunal- og moderniseringsdepartementet.

⁵ [Strategi for ID-porten 2015-2020, Difi-rapport 2014:6](#)

- I *Difi sin strategi* for perioden 2017-2020⁶ heter det at Difi skal løse felles utfordringer som krever samordnet innsats. Difi har et spesielt ansvar for å være endringsagent innenfor digitaliseringsområdet og eksempel på hvordan digitalisering kan bidra til effektivisering og realisering av gevinster.

Signeringstjenesten skal understøtte de ulike politiske ambisjonene på følgende måte:

- Tilby signering med et tilstrekkelig nivå av sporbarhet og beviskraft for offentlige virksomheter og innbyggere, for de mest utbredte brukstilfellene for elektronisk signatur for privatpersoner i offentlig sektor.
- Understøtte prinsippet om digitalt førstevalg ved å effektivisere tidsbruk i offentlige virksomheter knyttet til elektronisk signatur for privatpersoner gjennom kostnadseffektiv digitalisering av manuelle arbeidsprosesser, med de formkrav som til enhver tid stilles i relevant lovverk.
- Tilby en tjeneste som er enkel, robust, pålitelig og sikker for offentlig sektor og for innbyggerne.

Med bakgrunn i målene har signeringstjenesten følgende visjon:

Signeringstjenesten skal tilby en effektiv tjeneste for elektronisk signatur for privatpersoner med tilstrekkelig beviskraft og sporbarhet.

⁶ <https://www.difi.no/om-difi/difis-strategi>

4 Strategi

I arbeidet med strategien er det kommet innspill fra flere virksomheter omkring tjenestens videre utvikling. Difi sitt hovedinntrykk er imidlertid at tjenesten allerede i stor grad dekker det funksjonelle behovet hos virksomhetene. For Difi sin del er det et viktig prinsipp at våre felleskomponenter skal ha et klart definert og avgrenset bruksområde, og løse helt konkrete oppgaver for virksomhetene. Med dette til grunn er strategien like viktig med tanke på hva den sier at tjenesten ikke skal løse som hva den skal løse av ulike behov som kan finnes.

Strategien deles inn i to områder som vil bli behandlet. Det største og viktigste området er strategi for signering, mens det andre området er strategi for støttetjenester. Det finnes flere støttetjenester som en del av løsningen.

4.1 Signeringstjenestens kontekst

Signeringstjenesten er en sikker tjeneste som gjør det mulig å digitalisere arbeidsprosesser som krever en signatur for personer. I et større landskap av sikkerhets- og tillitstjenester er signeringstjenesten en av flere som fyller ulike funksjoner. Bevisene som produseres i de nevnte sikkerhets- og tillitstjenestene inngår i en lengre kjede av bevis. F.eks. er det for Lånekassen nødvendig å avkreve autentisering og signatur når det inngås lånekontrakter, men i tillegg verifiserer man også at kontonummeret låntakeren oppga tilhører samme person som ble autentisert ifm. avtaleinngåelsen.

I de neste avsnittene følger en beskrivelse av ulike typer sikkerhets- og tillitstjenester som inngår i samme landskapet som signeringstjenesten.

4.1.1 E-signering for personer

Formålet med e-signering for personer er å sikre informasjonsintegritet og ikke-benekting knyttet til et dokument, i de tilfellene der det er risiko for at en av partene kan nekte å vedstå seg innholdet i dokumentet og det derfor er behov for å kunne etterprøve signatarens knytning til dokumentets innhold over tid.

E-signering i sin alminnelighet er i e-signaturloven definert som «data i elektronisk form som er knyttet til andre elektroniske data og som brukes som autentiseringsmetode». Dette kan i prinsippet være enten en autentiseringstransaksjon som er knyttet til loggdata på en slik måte at loggdataene fungerer som bevis på at signataren hadde som intensjon å signere et gitt dokument, eller det kan være en autentisering påfulgt av en kryptografisk signatur som forseglar et dokument. Selv om begrepet e-signering reint juridisk også kan omfatte en logget autentiseringstransaksjon, ønsker vi i denne strategien å skille mellom e-signering og loggbasert signering:

- *E-signering* forstår vi i denne strategien som en kryptografisk signatur generert over et dokument, der den kryptografiske sjekksummen fremstilles ved hjelp av privatnøkkel tilknyttet et virksomhetssertifikat eller personsertifikat.
- *Loggbasert signering* forstår vi som en «signatur» bestående av loggdata som beviser at det har funnet sted en autentisering av

signataren og at vedkommende har utvist en intensjon om å signere et spesifikt dokument (f.eks ved at han har klikket på en knapp med teksten «jeg signerer dokumentet x»).

Det er tre hovedgrunner til hvorfor det offentlige trenger e-signatur.

- Det er påkrevd ved lov: Krav om e-signatur er i liten grad påkrevd ved lov i dag. Det utelukker imidlertid ikke at dette kan bli tilfelle på et senere tidspunkt. Ved inngåelse av finansavtaler er det krav om at det skal benyttes en «betryggende metode for å autentisere inngåelsen av en avtale» (jf. Finansavtaleloven § 8, 2 ledd bokstav b). Lånekassen har for sin del vurdert autentisert signatur til å være tilstrekkelig for å ivareta dette kravet.
- Det er behov for en tilstrekkelig sikker mekanisme for å inngå forpliktelser: Signeringstjenesten skal skape tillit mellom parter ved å fungere som en tiltrodd tredjepart. For det offentlige er det viktig at innbyggeren har bekreftet sine forpliktelser gjennom å signere, mens det for innbyggeren er viktig å kunne vise til hva som faktisk er signert.
- Det er hensiktsmessig for å digitalisere en prosess: Slik som ved inngåelse av kontrakter, som i dag ofte sendes på papir frem og tilbake mellom flere ulike parter.

Signeringstjenesten er en fellestjeneste som hele offentlig sektor kan, men ikke er pålagt å benytte. Det finnes også andre skybaserte signeringstjenester i markedet. Signeringstjenesten tilbyr både avansert e-signatur og autentisert e-signatur, men tilbyr ikke loggbasert signering.

4.1.2 Loggbasert signering

Formålet med loggbasert signering er å kunne slå fast identiteten til signataren og sikre en viss grad av uavviselighet mht. innholdet i et signert dokument. Loggbasert signatur kan fremstilles med ulike autentiseringsmekanismer i kombinasjon med integritetssikrede logger.

ID-porten er felleskomponent for kontroll og formidling av eID. Det finnes også andre autentiseringsmekanismer med stor utbredelse, f.eks. FEIDE eller integrerte autentiserings- og tilgangsstyringsmoduler i sak- og arkivsystemene. Uavviseligheten knyttet til det signerte dokumentet vil da påvirkes av styrken til autentiseringsmekanismen og sikkerhetsnivået på eIDen som blir autentisert. Altinns signeringsløsning, som brukes bl.a. for selvangivelsen, eller sak-/arkivsystemenes signeringsfunksjon for utgående dokument, er eksempler på løsninger for loggbasert signering.

Fordi loggbasert signering ikke medfører forsegling av dokumentet, kan denne typen signaturer egne seg i de tilfellene der det er begrenset risiko for at signataren ikke vedstår seg innholdet i det signerte dokumentet.

4.1.3 E-signering for virksomheter (forsegling)

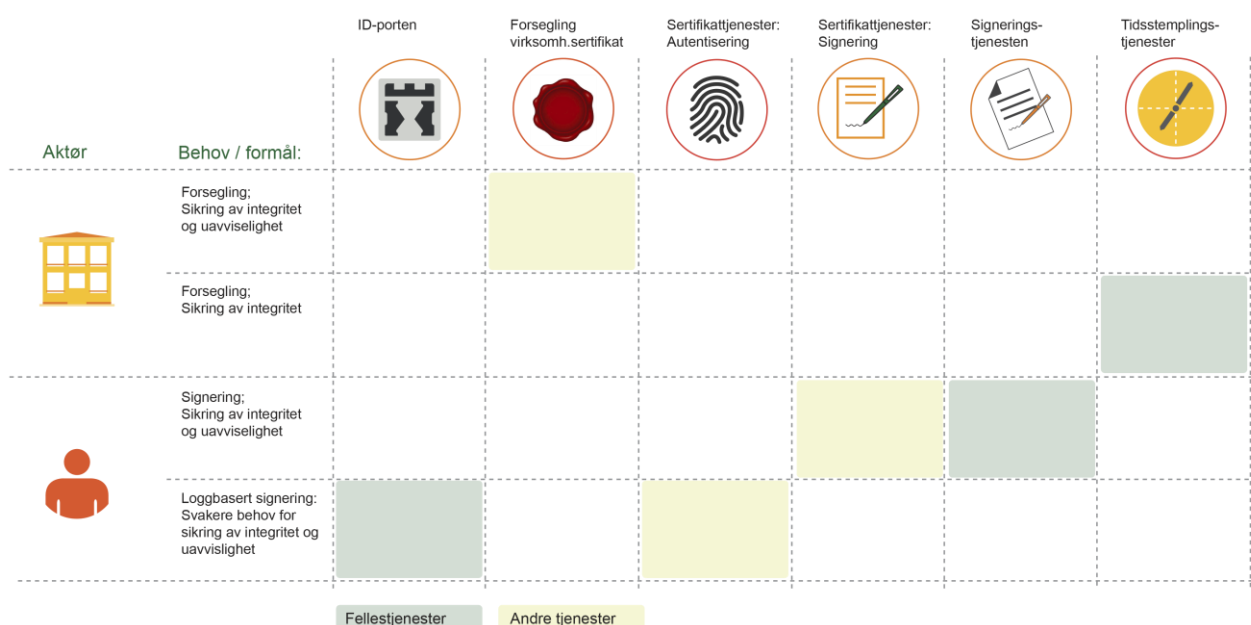
Formålet med e-signering for virksomheter (forsegling) er å sikre integriteten og uavviselighet knyttet til et dokument. Ulikt e-signering for personer, er det virksomhetenes identitet som autentiseres og sertifikatet til virksomheten som benyttes til å forsegle dokumentet. Uavviseligheten knytter seg således til virksomheten og ikke til en person. Et eksempel på signeringsløsning for virksomheter er Statens kartverks tjeneste for tinglysing.

E-signering for virksomheter (forsegling) egner seg i de tilfellene der det er vesentlig å sikre at en virksomhet vedstår seg innholdet i et dokument og sikre at ikke innholdet i dokumentet kan ha blitt endret etter forsegling.

4.1.4 Tidsstempling

Formålet med tidsstempling er å bevise at et dokument eksisterte på et bestemt tidspunkt og at dokumentet ikke er endret etter at tidsstempelet ble påført. Tidsstempelet er en kryptografisk forsegling av et dokument som påføres av en tiltrodd tidsstemplingsautoritet.

Uavviseligheten er i mindre grad ivaretatt med tidsstempling, all den tid tidsstempelet som påføres dokumentet ikke inneholder noen signatur som gjør det mulig å bevise at en part har utført en handling eller vedstår seg innholdet i dokumentet.



Figur 7 Signeringstjenestens «systemlandskap»

4.2 Behandling av innmeldte behov

Alle virksomheter som benytter signeringstjenesten kan komme med ønsker til endret innhold og funksjonalitet. Innbyggerne kan også fremme endringsønsker og behov gjennom Difis brukerstøtte. I tråd med føringene i Digital agenda om brukeren i sentrum er det ønskelig at man i tillegg til mottak av endringsønsker også aktivt innhenter endringsønsker fra innbyggerne, for eksempel ved å

gjennomføre brukerundersøkelser om tilfredshet, forventinger og endringsønsker.

Difi gjennomgår innmeldte behov og anbefaler og prioriterer behovene innenfor gjeldende strategi og budsjett. Styringsrådet for Difis felleskomponenter skal brukes som høringsinstans for foreslåtte utviklingsplaner.

For status på innmeldte og vurderte behov se vedlegg.

4.3 Strategi for signering

Begrunnelsen fra dagens tjenesteeiere for å bruke signeringstjenesten er hensynet til å ha en tilstrekkelig sikker mekanisme for å inngå forpliktelser og fordi det er en hensiktsmessig tjeneste for å digitalisere manuelle prosesser. Difi opplever at det i svært liten grad er juridiske krav som er årsaken til at signeringstjenesten ønskes brukt, og har for eksempel ikke funnet noen eksempler på at det kreves en avansert elektronisk signatur i noe eksisterende norsk lovverk. Kompleksitet påvirker pris, noe som også var en utløsende faktor for at Difi realiserte autentisert signatur som er vesentlig billigere for offentlige virksomheter. I tillegg til å opprettholde dagens alternativer kan det være aktuelt for Difi å se på mulighetene for å realisere alternativer i tjenesten som er enda enklere, og som dermed vil være enda rimeligere i bruk. Dette må imidlertid ses i sammenheng med hva slags behov som skal løses hos virksomhetene, og hvilke andre tilgjengelige tjenester som finnes som eventuelt kunne løst behovet. Dersom en autentisering og logging av denne i realiteten er det som trengs, vil det for eksempel være unødvendig å utvide signeringstjenesten i denne retningen.

Gjennom eIDAS-forordningen vil det kunne komme nye krav som signeringstjenesten må ta hensyn til. Forordningen trådte i kraft i januar 2017, og regulerer blant annet elektronisk signatur på tvers av landegrensene i Europa. Difi har per i dag ikke identifisert krav som treffer tjenesten i dag, men det kan ikke utelukkes at enkelte ting vil inntreffe på sikt.

- Dette gjelder først og fremst knyttet til validering av utenlandske signaturer.
 - Anerkjennelsesplikten gjelder likevel kun der hvor vi i Norge krever avansert signatur. Så vidt Difi er kjent med er dette ikke tilfelle i Norge nå i dag.
 - Det er ikke en plikt at vi også må legge til rette for signering med utenlandske sertifikater.

Difi ønsker likevel å se på hvordan signeringstjenesten kan integreres med den europeiske infrastrukturen og hvordan man kan tilby autentisert e-signatur med ID-portens løsning for autentisering på tvers av landegrensene. Motivasjonen er å legge til rette for både signering med utenlandske sertifikater og for å kunne validere utenlandske signaturer. Dette vil være et behov som treffer flere offentlige virksomheter, blant annet i Universitets- og Høgskolesektoren.

Signeringstjenesten skal dekke de vanligste bruksscenarioene for offentlige virksomheter knyttet til signering for privatpersoner. Difi opplever at tjenesten i stor grad gjør dette allerede, men det har kommet innspill som Difi mener kan

være relevante å gå videre med. Dette gjelder spesielt rundt det å signere på vegne av en virksomhet. Det er ingen hindringer for å kunne signere på vegne av en virksomhet i dag, men med et personlig sertifikat og uten at signeringstjenesten håndterer knytningen mellom fødselsnummeret og organisasjonsnummeret. Difi har som ambisjon i strategiperioden å få med denne knytningen med som en del av beviset som lages i signeringstjenesten. Det innebærer at det vil gjøres et oppslag i relevant register som inneholder informasjon om signaturfullmakt/prokura for en virksomhet. Det er imidlertid noe usikkerhet knyttet til om informasjonen finnes, og om den har tilstrekkelig kvalitet til å kunne brukes. Dette vil bli vurdert før eventuell realisering.

Difi ønsker å etablere en fast referansegruppe for signeringstjenesten. En fast referansegruppe vil være verdifullt for videreutvikling av tjenesten, og vil samtidig kunne være et forum for å diskutere elektronisk signatur blant offentlige virksomheter.

Følgende behov rundt bruk av signeringstjenesten er identifisert i dialogen med tjenestens kunder:

- Signeringstjenesten må tilby tjenester som er kostnadseffektive i bruk.
- Det er behov for å kunne bevise knytning mellom en person og en virksomhet i de tilfeller hvor personen signerer på vegne av virksomheten.
- Det er behov for å legge til rette for signering med utenlandske sertifikater og validering av utenlandske signaturer.
- Det er ønskelig at det etableres en fast referansegruppe for signeringstjenesten.

Hovedmål:

Signeringstjenesten skal bidra til å sikre brukervennlige, praktiske og effektive tjenester ved å fjerne manuelle prosesser og oppnå et tilstrekkelig nivå av sporbarhet og beviskraft for elektroniske dokument

Delmål	Oppfølging
Signeringstjenesten skal være kostnadseffektiv utfra de behovene offentlige virksomheter har.	<ul style="list-style-type: none"> • Vurdere enklere og mer kostnadseffektive metoder for signering som tilfredsstillende kravene fra virksomhetene.
Det skal være mulig å signere med utenlandske sertifikater.	<ul style="list-style-type: none"> • Tilby autentisert e-signering med europeisk eID basert på ID-portens løsning for autentisering på tvers av landegrensene. • Vurdere å tilby e-signering gjennom infrastrukturen for signering med europeiske sertifikater (EUs DSS-løsning for framstilling og validering av europeiske e-signaturer).

Det skal være mulig å få validert utenlandske signaturer.	<ul style="list-style-type: none"> • Etablere en kopling mot den europeiske infrastrukturen for validering av utenlandske e-signaturer (EUs DSS-løsning).
Det skal være mulig å bevise en knytning mellom personnummer og organisasjonsnummer når en person signerer på vegne av en organisasjon.	<ul style="list-style-type: none"> • Etablere en integrasjon mot rolle- og rettighetsregister.
Signeringstjenesten skal tilby e-signatur med nasjonalt ID-kort	<ul style="list-style-type: none"> • Etablere integrasjon med signeringsmiljø for nasjonalt ID-kort for framstilling av avansert e-signatur. • Tilby autentisert e-signatur med nasjonalt ID-kort med autentisering i ID-porten.
Difi skal etablere en fast referansegruppe for signeringstjenesten	

4.4 Strategi for støttetjenester

Det finnes flere støttetjenester i løsningen som virksomhetene kan ta i bruk. Støttetjenestenes funksjon er å understøtte forretningsprosesser som involverer personlig e-signatur på en effektiv måte.

Hovedmål:

Signeringstjenesten tilbyr støttetjenester som realiserer delprosesser som naturlig henger sammen med personlig e-signering eller administrasjon av personlig e-signering og som effektiviserer disse prosessene.

4.4.1 Integrerte støttetjenester

Enkelte støttetjenester er av en slik karakter at de er nødvendige å bruke (av funksjonelle eller juridiske årsaker) for å kunne realisere elektronisk signering for privatpersoner. Eksempler på dette er administrasjon av signeringsoppdrag og varsling om dokument til signering i asynkrone signeringsprosesser, der eForvaltningsforskriften § 8 pålegger avsender å varsle innbyggeren vha. kontaktinformasjon fra Kontakt- og reservasjonsregisteret.

Siden de integrerte støttetjenestene er nødvendige for signeringsprosessen eller administrasjonen av signeringsoppdrag, er disse standardtjenester som enten er obligatoriske (administrasjonstjenester) eller som brukerstedene aktivt må overstyre dersom de ikke skal benyttes (varsling av innbygger).

For at tilleggstjenestene skal fylle sin tiltenkte funksjon, må de være effektive, sikre og brukervennlige. Administrasjonstjenestene videreutvikles med tanke på forbedring av eksisterende prosesser.

Delmål for integrerte støttetjenester:

Delmål	Oppfølging
Effektive, sikre og praktiske administrasjonstjenester som dekker tjenesteeiernes behov.	<ul style="list-style-type: none"> Vurdere ny funksjonalitet som gir mer effektive og praktiske og minst like sikre administrasjonstjenester

4.4.2 Tilleggstjenester

Signeringstjenestens tilleggstjenester bidrar til å understøtte forretningsprosesser der elektronisk signatur for privatpersoner inngår, men er ikke nødvendige (funksjonelt eller juridisk) for å kunne gjennomføre prosessen.

Dagens tilleggstjenester er videresending av signert kopi til digital postkasse og langtidslagring av signerte dokumenter.

Enkelte virksomheter har behov for å sikre integriteten og valideringsdataene til et signert dokument over lengre tid enn det kryptografien som er benyttet tillater. Disse har bruk for signaturvedlikehold.

Signeringstjenesten vil utvides med funksjonalitet for innhenting og forsegling av signatarens signeringsfullmakt/prokura som en del av beviset i LTV-SDO. Formålet er å dokumentere et øyeblikksbilde av fullmakten en person har på vegne av virksomheten han representerer, slik at informasjonen er lett tilgjengelig for bevisføring på et senere tidspunkt. Når utvidelsen realiseres, vil signeringstjenesten være bedre rustet til å understøtte prosesser der signatar signerer på vegne av en virksomhet. Det vil da være ønskelig å utgreie om det er grunnlag for å også etablere en tjeneste for varsling av personer med signaturfullmakt/prokura. Dette krever altså tilgang til en datakilde som inneholder opplysninger om slike fullmaktsforhold, noe som mangler i dag.

Delmål for tilleggstjenester:

Delmål	Oppfølging
Signaturvedlikehold tilbys som tilleggstjeneste slik at levetiden til kryptografien i det signerte dokumentet forlenges og kan valideres over lengre tid.	<ul style="list-style-type: none"> Langtidspreservering (signaturvedlikehold) etableres som tilleggstjeneste
Varsling til personer med signaturfullmakt/prokura tilbys som tilleggstjeneste.	<ul style="list-style-type: none"> Det skal utredes om det er grunnlag for en varslingstjeneste rettet mot personer med signaturfullmakt/prokura.

5 Videre forvaltning av strategien

Videre forvaltning av strategien skal skje i henhold til beslutningsprosessen for arbeid med visjon og strategi for signeringstjenesten som er fastsatt av Difi. Beslutningsprosessen er styrende for signeringstjenesten og skal brukes som grunnlag for å:

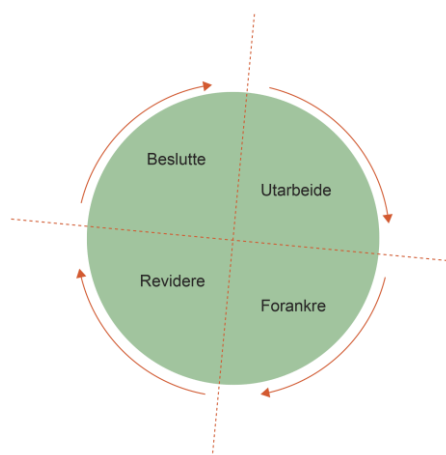
- Utarbeide og beslutte visjon og strategi.
- Revidere visjon og strategi ved fastsatte intervaller eller hendelser.

Beslutningsprosessen for visjon og strategi består av tre definerte prosesser:

1. **Visjonsprosess**
Visjonsprosessen skal gjennomføres hvert 5 – 10 år eller ved vesentlige endringer i signeringstjenestens rammebetingelser.
2. **Strategiprosess**
Prosessen skal gjennomføres hvert 3 – 5 år, ved endrede rammebetingelser eller ved identifisert behov for nye eller endrede tjenester.
3. **Utviklings- og tiltaksplanprosess**
Gjennomføres årlig i henhold til endringsstyringsprosess for Difis felleskomponenter og etter innspill fra registerets brukere som beskrevet i 4.1. Prosessen skal etablere konkrete utviklings- og tiltaksplaner som skal sikre oppfyllelse av de konkrete mål som er definert i signeringstjenestens strategi.

Visjons- og Strategiprosessene gjennomføres som en fire stegs prosess som indikert i Figur.

Det vil, avhengig av omfang av revisjon etter første forankring, kunne være behov for å gjenta stegene «forankre» og «revidere» inntil det oppnås tilstrekkelig samstemmighet som kan danne grunnlag for en endelig beslutning.



Figur 8: Prosesstegene

Det er Difis ledelse som har besluttende myndighet både for visjon, strategi samt de ulike tiltak og utviklingsplaner.

Referanseark for Difi

Tittel på rapport:	Strategi for Signeringstjenesten
DIFIs rapportnummer:	2017:3
Forfatter(e):	Stig Hornnes, Sindre Ramung
Evt. eksterne samarbeidspartnere:	
Prosjektnummer:	17-8
Prosjektnavn:	Produktstrategi signeringstjenesten
Prosjektleder:	Stig Hornnes
Prosjektansvarlig avdeling:	IDU
Oppdragsgiver(e):	
Resymé/omtale:	<p>Signeringstjenesten eSignering tilbyr en tjeneste for elektronisk signatur for privatpersoner til bruk for offentlige virksomheter, i tillegg til en tjeneste for langtidsvalidering av signaturer og en tjeneste for arkivering av signerte dokumenter. Virksomhetene kan bruke signeringstjenesten via en portal hvor dokumentene lastes opp manuelt, eller de kan integrere tjenesten inn i sine egne løsninger, slik at innbyggeren bruker tjenesten i virksomhetens egen kontekst.</p> <p>Strategien beskriver den retningen signeringstjenesten vil utvikles i perioden 2017-2022. De behov som kundene har meldt inn og vurderingen av disse har vært førende for utforming av strategien. I strategien beskrives også signeringstjenestens visjon, hvor strategien vil ligge til grunn for å nå denne.</p>
Emneord:	Elektronisk signatur, e-signatur, e-signering
Totalt antall sider til trykking:	0
Dato for utgivelse:	20.04.2017
Utgiver:	DIFI Postboks 8115 Dep 0032 OSLO www.difi.no