



**Opnå en langsigtet
løsning med elektronisk
signatur.**

Indholdsfortegnelse.

Indledning.....	3
Kontor kombineret med hjemmearbejde	3
Hvem kan man stole på?	3
Retningslinjer for en elektronisk signatur, der opfylder de juridiske krav.	3
Udførelsen af underskrifter i dag.	4
Inden I investerer i en ny løsning.....	4
Ikke-tilpassede løsninger til offentlig administration.	4
Hvordan kravene bør stilles.	5
Lovkrav og anbefalinger	5
Forskellige niveauer af elektronisk signatur.....	5
Processen for en elektronisk signatur på avanceret niveau.....	5
Konkrete krav til en løsning med elektronisk signatur.....	6
Konvertering.....	6
Identifikation	6
Arkivering og sporbarhed.....	6
Krav til ejerskab	6
Kom godt i gang med e-signatur.	7
Tag det næste skridt i processen.	7
Deltagere	7
Dagsorden	7
En lille dybtgående undersøgelse af love og anbefalinger . .	8
Lovkrav	8
Krav til dokumenthåndtering	8
Forskellige niveauer for e-signering.	8





Indledning.

Kontor kombineret med hjemmearbejde

Der har igennem de seneste år været en tendens til i højere grad at arbejde hjemmefra. Samtidig forventes det at vores arbejde udføres på samme måde og med samme effektivitet som på kontoret. Mange af vores processer er blevet digitaliseret, og vi er ved at vænne os til de mange digitale værktøjer, som gør os i stand til at samarbejde med andre uden at være fysisk det samme sted.

I januar 2021 offentliggjorde det svenske *Netigate en undersøgelse, der viste, at 73% ønsker at kombinere arbejdsugen med hjemmearbejdsdage og dage inde på kontoret, når vi kommer på den anden side af coronapandemien. Dette blev også bekræftet efter vores egen undersøgelse i Formpipe koncernen, som blev foretaget i sensommeren 2020. Hvor op til 37% mener, at arbejdet er blevet mere effektivt, men fremhæver stadig vigtigheden og behovet for en kvalitetssikret elektronisk signatur, som det sidste led i en effektiv digital arbejdsgang.

At underskrive dokumenter er stadig en kritisk del af mange arbejdsgange. I betragtning af hvor vigtig en aktivitet det er, er det overraskende hvor lang tid det tog for digitaliseringen at få fokus på netop dette.

*Netigate (Svensk Enterprise Feedback Management)

De hidtil introducerede værktøjer til håndtering af elektroniske signaturer er blevet optimeret ud fra et brugerperspektiv. De elektroniske signaturer er blevet en langsigtet strategisk prioritering i flere forretningsgange, og vi er nødt til at sikre løsninger til vores komplekse behov.

Retningslinjer for en elektronisk signatur, der opfylder de juridiske krav.

Denne vejledning er en guide og information omkring elektronisk signatur. Heri også de juridiske krav I skal tage højde for, samt hvilke krav I skal stille for at kunne skabe langsigtede løsninger for jeres arbejdsgange. Løsningerne skal leve op til områdets krav til og samtidig skabe fleksibilitet i forretningsprocesser og systemer.

Udførelsen af digitale underskrifter i dag.



Inden I investerer i en ny løsning

Vi har underskrevet dokumenter i mange år, og det er blevet en naturlig del af vores hverdag – både privat og på arbejdspladsen.

Uden at tænke over det, så har vi i vores hverdag forskellige niveauer og udgaver af aftaler. Vi lover noget, vi aftaler noget eller vi skriver under på en aftale. Nogle gange kræves aftaler endda en autentificeret underskrift. Alt dette kan en elektronisk signatur også have - altså flere niveauer og karakterer.

Ikke-tilpassede løsninger til offentlig administration.

Det er let at underskrive elektronisk, men det kræver lidt mere at sætte sig ind i kompleksiteten bag den elektroniske signatur for at træffe den rigtige beslutning for din virksomhed og dine dokumenter. Ellers er risikoen, at du får en løsning, der ikke lever op til den aftaleindgåelse, der underskrives.

Der findes mange brugervenlige løsninger på markedet, men på trods af det understøtter få af dem langtidsarkivering og transparens til at gennemskue hvem der har skrevet under og om dette er gjort korrekt. Gennem den traditionelle håndtering af underskrevne dokumenter skal der ikke kun tages højde for egne interne dokumentstyrings-regler, men også for de regler, der udstedes fra myndighederne og rigsarkivet. Dette er vigtigt at tage med i jeres overvejelser, så I sikrer korrekt håndtering af elektronisk signatur. Desværre er mange løsninger på markedet ikke designet til offentlig administration, hvilket betyder, at gældende krav ikke er opfyldt.

På næste side belyser vi nogle vigtige punkter, som du skal huske på, når du stiller krav til e-signaturer, og vi vil også dykke ned i de love og anbefalinger, der findes til elektroniske signaturer i slutningen af dette dokument.

Hvordan kravene bør stilles.

Lovkrav og anbefalinger

Et godt udgangspunkt, når det kommer til elektroniske signaturer er, at de skal understøtte et dokumentets levetid, fra det tidspunkt, hvor det skal underskrives, indtil det skal fjernes eller langtidsopbevares. Brugeren skal ikke være nødt til at tænke på signaturens gyldighed, om den kan valideres, om oplysningerne er gemt i det korrekte format, eller om håndteringen følger de regler, der findes vedrørende underskrifter, dokumenthåndtering og personfølsomme data.

Juridiske krav og anbefalinger vedrørende elektroniske signaturer, signeringstjenester og langtidsopbevaring er tilgængelige på både dansk og europæisk niveau. eIDAS-forordningen regulerer de lovmæssige krav til elektroniske signaturer, som er beskrevet i afsnittet "En dybtgående undersøgelse af love og anbefalinger".

Digitaliseringsstyrelsen har klare anbefalinger til e-signaturer, herunder skitser og specifikationer for, hvilket format underskriften skal understøtte. De har dog ikke anbefalinger vedrørende selve e-tjenesten til elektroniske signaturer.

Rigsarkivet udsteder regler og generel rådgivning vedrørende langsigtet opbevaring af information, som inkluderer dokumentformater, men også håndtering af elektroniske signaturer.

Forskellige niveauer af elektronisk signatur

Der er tre forskellige niveauer af elektronisk signatur:

- Elektronisk underskrift
- Avanceret elektronisk underskrift
- Kvalificeret elektronisk underskrift

De forskellige niveauer er beskrevet mere detaljeret under overskriften "Forskellige niveauer for e-signering" senere i dette dokument.

Processen for en elektronisk signatur på avanceret niveau

UNDERSKRIFTSFLOW

1
DER OPRETTES OG
SENDES EN UNDER-
SKRIFTSOPGAVE



Dokumentet konverteres til PDF/A 1, underskrivere angives og meddelelse om underskrift sendes til dem via Digital post eller e-mail

2
LOG IND.
GENNEMSE OG
UNDERSKRIV



Login/identifikation med NemID (Kommande MitID), hvorefter du kan afvise eller underskrive dokumentet som vises. Signering bekræftes med NemID (MitID)

3
INDLEJRET PERSONLIGT
CERTIFIKAT



Et personligt certifikat oprettes sammen med tidspunkt fra en betroet tidsstempeltjeneste, dette gemmes i PDF'en i henhold til PAdES

4
UNDERSKREVET PDF ER
TILGÆNGELIG



Når alle har underskrevet, findes PDF-filen i det system, den blev sendt fra (fx Acadre eller Signeringsportalen)

5
UNDERSKREVET PDF ER
ARKIVRESISTENT



Resultatet er en PDF med indlejrede signaturer, der kan valideres af alle og hvor som helst, der følger eIDAS og er klar til langtidsopbevaring (LTV)

Konkrete krav til en løsning med elektronisk signatur.

På denne side nævnes nogle vigtige, konkrete krav til brugervenlighed og overholdelse, der skal placeres på en moderne løsning til e-signatur.

Konvertering

En løsning til e-signering skal kunne konvertere de dokumenter, der skal underskrives, før de underskrives. Et grundlæggende krav bør være, at alle de almindelige dokumenttyper såsom Google Docs, Microsoft Office, PDF, billeder og mere kan konverteres til bevaringsformat ved hjælp af en elektronisk signaturløsning. Undersøg hvilke værktøjer og systemer din organisation bruger og medtag dette i kravspecifikationen, så e-signeringsløsningen også kan modtage dokumenter fra disse.

Årsagen til, at e-signeringsløsningen skal konvertere dokumenter inden signering, er, at signaturen blandt andet bekræfter, at dokumentet ikke er ændret efter underskrivelsen. Hvis dokumentet skal konverteres senere inden arkivering, ændres dokumentet og dets underskrifter, og signaturen ødelægges som et resultat. Dette gælder også, hvis dokumentet er en PDF i et andet format end PDF/A.

Identifikation

For at være sikker på, at den rigtige person ser og underskriver dokumenterne, skal brugeren identificeres. Her anbefaler flere digitaliseringsmyndigheder en e-identifikation med mindst tillidsniveau tre. Et eksempel på en sådan e-identifikation er NemID (MitID).

Arkivering og sporbarhed

For at opnå enkelhed for et underskrevet dokument skal visse kriterier være opfyldt. For eksempel skal underskrifterne være personlige og indlejrede i dokumentet, og de skal kunne valideres når som helst efterfølgende. Når signaturene er indlejret, betyder det, at dokumentet altid kan betragtes som en original. Med et personligt certifikat er signaturen indlejret i en PDF i overensstemmelse med den standard, der anbefales af eIDAS (PADES), og når du også bruger LTV-niveauet for denne standard, valideres signaturen på tidspunktet for underskrivelsen, og informationen gemmes i dokumentet.

Derfor opfylder du også kravene til både Rigsarkivet og eIDAS og har en avanceret signatur med høj sporbarhed, som er arkivresistent. Se afsnittet om dybdegående undersøgelse af love og anbefalinger for mere information om arkivering og PADES.

Krav til ejerskab

Hvordan og hvor man skal opbevare information er et vigtigt spørgsmål for mange. Det er vigtigt at tage dette i betragtning, når du vælger en e-signatortjeneste. Stil krav til ejerskab af al information omkring underskrifter. Kravet repræsenterer faktisk to ting, for det første at sikre, at ingen information uden brugerens viden forlader grænsen for myndigheds-/virksomhedsgrænsen, men også at al information er let at kontrollere og spore.

Kom godt i gang med e-signatur.

Tag det næste skridt i processen.

Valg af løsning er et langsigtet, strategisk vigtigt emne og skal drives centralt og kobles til de langsigtede behov i hele virksomheden.

Det første skridt for dem af jer, der ikke har haft tid til at få indlejret e-signering i jeres arbejdsgang, er selvfølgelig at få mere viden. Spørgsmål der skal besvares, kan være:

- Hvordan fungerer e-signerede dokumenter sammen med arkivet?
- Kan jeg stole på elektroniske signaturer?
- Er e-signaturløsninger sikre?

Årsagen til dette findes nedenfor, men hvis du vil have yderligere support i din viden-indsamling, kan Formpipe tilbyde hjælp med det via en partner. Du er også velkommen til at kontakte vores Market Manager Silje Berg på silje.berg@formpipe.com, så kan hun fortælle dig mere.

For dem af jer, der er kommet lidt længere i processen og ønsker at indføre elektroniske signaturer, kan de spørgsmål, der skal besvares, måske mere handle om forankring internt og hvordan man kommer i gang. Spørgsmål som disse er vigtige at besvare:

- Hvad vil vi opnå med elektroniske signaturer?
- Hvilke dokumenter/processer starter vi med?
- Hvordan kommer vi videre?

Uanset hvor langt du er kommet i din proces, foreslår vi en workshop, der naturligvis er specifik for dig.

Forslag til deltagere og dagsordenspunkter findes til højre. Målet med workshoppen kan være, at signering-løsningen er forankret internt, og at der eksisterer en overordnet plan for fortsat arbejde.

Deltagere

Alle interessenter såsom sagsbehandlere, ESDH-ansvarlige, digitaliseringskonsulenter, IT, Arkiv og tilsigtede forvaltere kan være til stede på workshoppen. De er eksempler på funktioner, der skal forstå og acceptere den valgte løsning.

Dagsorden

- **Signering - hvordan virker det?**
 - *Hvad sker der teknisk, hvordan ser et underskrevet dokument ud, kan vi stole på underskrifterne og selve løsningen?*
- **Hvordan er den integreret til Acadre?**
 - *Effektivisering, arbejdsgang og bedre service til borgeren*
- **Hvordan sikres dokumenter og underskrifter fra underskrift til langtidsoptagelse?**
 - *Informationssikkerhed, personlige data, logning, validering*
- **Med hvilke dokumenter skal vi begynde?**
 - *Identificer de lavthængende frugter. Hvilke mængder der er tilgængelige, hvad der er kompliceret, er der dokumenter med mange underskrifter med lange leveringstider.*
- **Plan for implementering i virksomheden**
 - *Lad os komme igang!*



En lille dybdegående undersøgelse af love og anbefalinger.

Lovkrav

eIDAS-forordningen regulerer de eksisterende juridiske krav til elektroniske signaturer, uanset om det er det enkleste niveau, der kun omtales som en elektronisk signatur, eller om det er de mere pålidelige signaturer, der defineres som avancerede og kvalificerede signaturer. For at se, hvilke krav der er fremsat, henvises til en standard, PAdES, defineret via ETSI. Når en løsning følger disse, er resultatet en avanceret signatur. Se mere information under niveauer af e-signaturer.

Forskellige niveauer for e-signering.

eIDAS beskriver tre forskellige niveauer af elektroniske signaturer. Først definerer man en elektronisk signatur, der faktisk inkluderer alle former for digital signatur uden at være specificeret mere detaljeret. Imidlertid hedder det i artikel 25, at "En elektronisk signatur ikke kan nægtes retsvirkning eller gyldighed som bevis i retssager, alene fordi signaturen er i elektronisk form eller ikke opfylder kravene til kvalificerede elektroniske signaturer," og det er vigtigt at huske på. Imidlertid er en simpel form for elektronisk signatur, såsom en indsat scannet signatur, meget vanskelig at kontrollere, især bagefter. Som et alternativ kan man i stedet tilbyde en anden løsning, der passer bedre til den enkelte organisation for at undgå at håndtere de enkleste former for e-signaturer.

I artikel 26 i eIDAS-forordningen skriver man om avancerede elektroniske signaturer og krav omkring dem, hvor fokus er på forbindelse til underskriveren. Artikel 27, stk. 5, bestemmer derefter, at der skal oprettes referenceformater for avancerede elektroniske signaturer. Dette gøres i Kommissionens gennemførelsesafgørelse 2015/1506, hvor man i bilaget henviser til de tekniske specifikationer for signaturer til PDF-dokumenter, som er PAdES, og det er beskrevet i en ETSI-standard. Denne standard præciserer også forskellige niveauer af PAdES, og med henblik på opbevaring over tid skal en løsning opfylde kravene til LTV/LTA-niveau.

Selve eIDAS-forordningen definerer også yderligere kvalificerede elektroniske signaturer, herunder kvalificerede certifikater og en særlig anordning til oprettelse af kvalificerede signaturer. På nuværende tidspunkt er der ingen myndighed eller lignende i Danmark, der kræver en kvalificeret underskrift. EIDAS-forordningen skriver også om stempler, og det svarer til en underskrift, men for en juridisk person, dvs. en virksomhed. På lang sigt betyder det, at hvis du i en PDF ser et firma i signaturpanelet i stedet for de personer, der skulle have underskrevet dokumentet, er det ikke et dokument, der er signeret med en avanceret signatur, men i bedste fald en enklere form for elektronisk signatur stemplet med et avanceret stempel som ikke er det samme.