# Hur man uppnår en långsiktig lösning med elektronisk underskrift.

Formpipe.

# Innehållsförteckning.



Formpipe.

# Inledning.

## Kontor kombinerat med distans

Det har under många år funnits en trend där vi i allt högre grad jobbar mer på distans och förväntar oss att vårt arbete ska kunna genomföras på samma sätt och med samma effektivitet som på kontoret. Många processer har digitaliserats där vi börjat vänja oss vid digitala verktyg på jobbet och att kunna samarbeta med andra utan att vara på samma plats.

En aktivitet som är en kritiskt del i många affärsprocesser är signering. Det är förvånande hur lång tid det tagit innan denna aktivitet i processen satts i fokus för digitalisering med tanke på hur viktig den är.

Under januari 2021 publicerade Netigate en undersökning som visar att 73% vill kombinera jobb på distans och på arbetsplatsen efter pandemin. Något som även bekräftades efter vår undersökning som genomfördes efter sommaren 2020. Där hela 37 % anser att arbetet effektiviserats men belyser vikten och behovet av en kvalitetssäker elektronisk underskrift.

De verktyg som tidigare införts för att hantera elektroniska underskrifter har varit optimerade ur ett användarperspektiv. Nu när elektroniska underskrifter har blivit en långsiktig strategisk fråga för olika typer av verksamhetsprocesser behöver vi kravställa lösningar för att de ska tillgodose ett komplext behov.

### Vem kan man lita på?

Den 16 februari publicerade Infrastrukturdepartementet sin utredningen om betrodda tjänster, rubricerat som "Vem kan man lita på? – Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen (SOU 2021:9)". Denna del omfattade elektroniska underskrifter och andra relaterade betrodda tjänster.

I delbetänkandet har utredarna gått igenom nuvarande lagstiftning under eIDAS-förordningen och sammanfattat denna på ett lättförståeligt sätt som indirekt också gör den enklare att uppfylla. Det innehåller också tankar för framtida lagstiftning inom området. Exempel från delbetänkandet är förtydligandet av underskrift och stämpel, där underskrifter alltid är personliga, det vill säga knutna till en individ. Medan en stämpel är kopplad till en juridisk person såsom ett företag.

### Riktlinjer för en elektronisk underskrift som uppfyller lagkraven.

Vi har tagit fram denna guide för att informera kring elektroniska underskrifter, de lagkrav som finns inom området och hur ni behöver ställa krav för att kunna skapa långsiktiga lösningar. Dessa lösningar behöver leva upp till krav för underskrifter och samtidigt vara lätta och smidiga att använda kopplat till olika verksamhetsprocesser och system.

Formpipe.

# Utförandet av underskrifter idag.

## Säkerställ innan upphandling.

Signera har vi gjort sen urminnes tider. Det är en naturlig del av vår vardag både privat och på jobbet. Utan att vi tänker på det har vi i vår vardag olika nivåer av avtal eller överenskommelser, vi säger att vi ska något, lovar eller skriver under ett avtal. Ibland krävs till och med bevittnad underskrift. Även elektroniska underskrifter kan ha olika tyngd.

### Ej anpassade lösningar för offentlig förvaltning.

Att signera elektroniskt är enkelt, men att sätta sig in i komplexiteten bakom den elektroniska underskriften, för att kunna fatta rätt beslut, för er verksamhet och era handlingar, kräver lite mer. Risken är annars att ni skaffar en lösning som levererar ett löfte när ni behöver ett underskrivet avtal.

Många lösningar på marknaden är användarvänliga men levererar en underskrift som inte är möjlig att bevara över tid, och att det kan vara svårt att bevisa vem som signerat och att det är korrekt gjort.

För vår traditionella hantering av undertecknade dokument finns ett regelverk från kommunallagen, riksarkivet, egna dokumenthanteringsplaner eller arkivhänvisningar. Motsvarande finns för elektroniska underskrifter och man behöver även relatera detta till den traditionella hanteringen för att säkerställa rätt hantering.

Tyvärr är många lösningar på marknaden inte byggda för offentlig förvaltning vilket gör att krav som finns inte uppfylls. Nedan belyser vi några viktiga punkter att tänka på vid en kravställning gällande e-underskrifter och vi kommer även i slutet av detta dokument fördjupa oss i de lagar och rekommendationer som finns inom elektroniska underskrifter.

Formpipe.

# Hur krav bör ställas.

## Lagkrav och rekommendationer

En bra utgångspunkt när det gäller elektroniska underskrifter är att de ska stödja ett dokuments livstid, från det att det ska skrivas under tills dess att det ska gallras eller långtidslagras. Användaren ska inte behöva fundera på underskriftens giltighet, om den kan valideras, om informationen lagras i rätt format eller att hanteringen följer de regler som finns kring underskrifter, dokumenthantering och personuppgifter.

Lagkrav och rekommendationer kring elektroniska underskrifter, signeringstjänster och långtidslagring finns på både svensk och europeisk nivå. eIDAS-förordningen reglerar lagkraven kring elektroniska underskrifter vilket beskrivs i stycket **“**Fördjupning i lagar och rekommendationer**”.**

I den svenska kontexten har DIGG rekommendationer kring e-underskrift, bland annat med skisser och specifikationer hur den rent tekniska lösningen bör fungera. De har däremot inte rekommendationer kring själva e-tjänsten för elektronisk underskrift.

Riksarkivet lämnar föreskrifter och allmänna råd gällande långtidsbevarande av information, vilket bland annat omfattar dokumentformat men även hantering av elektroniska underskrifter.

### Olika nivåer för elektronisk underskrift

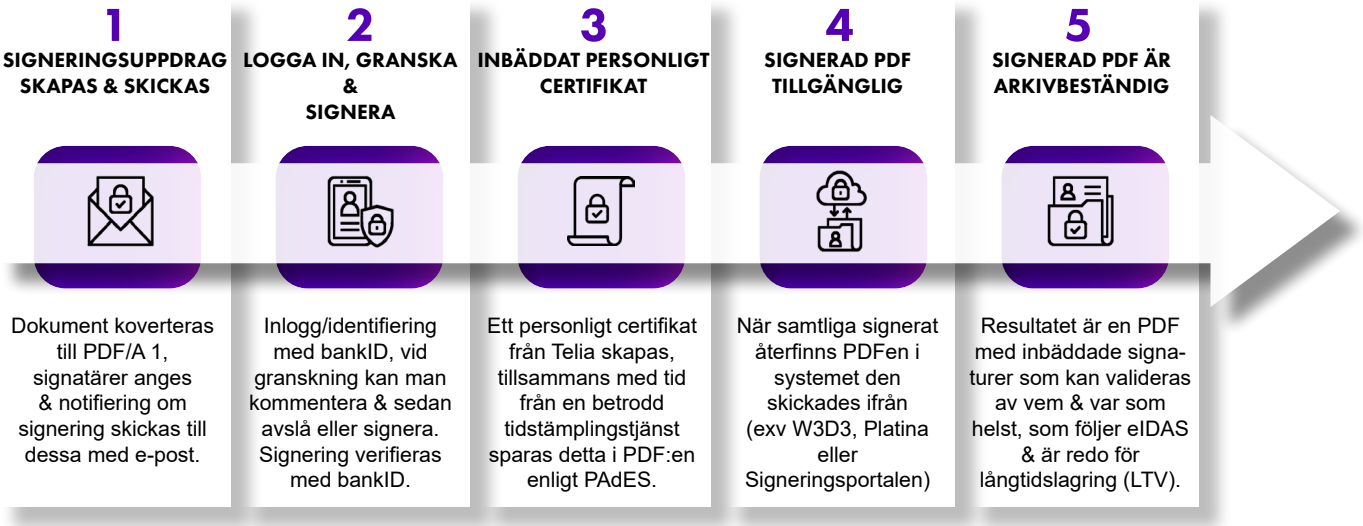
Det finns tre olika nivåer av elektronisk underskrift:

- Elektronisk underskrift
- Avancerad elektronisk underskrift
- Kvalificerad elektronisk underskrift

De olika nivåerna finns mer i detalj beskrivna under rubriken **“**Olika nivåer för e-signering**”** längre ner i detta dokument.

## Processen för en elektronisk underskrift på avancerad nivå.

### SIGNERINGSFLÖDE.




Formpipe.

## Konkreta krav på en lösning för en elektronisk underskrift.

Nedan följer några viktiga, konkreta krav kring användbarhet och regelefterlevnad som behöver ställas på en modern lösning för e-underskrift.

### Konvertering

En e-signeringslösning bör kunna konvertera de dokument som ska signeras inför signeringen. Ett grundkrav bör vara att alla de vanliga dokumenttyperna som Google Docs, Microsoft Office, PDF, bilder med mera kan konverteras till bevarandeformat av en lösning för elektronisk underskrift. Undersök vilka verktyg och system din organisation använder och ta med i kravställningen för att e-signeringlösningen skall kunna ta emot dokument även från dessa. Anledningen till att e-signeringslösningen bör konvertera dokument inför signering är för att signaturen bland annat intygar att dokumentet inte har förändrats efter signering. Skulle dokumentet behöva konverteras senare inför arkivering kommer dokumentet och dess signaturer förändras och signaturen i och med det förstöras. Detta gäller även om dokumentet är en PDF i annat format än PDF/A.

### Identifiering

För att vara säkra på att rätt person ser och signerar dokumenten behöver användaren identifieras. DiGG rekommenderar en e-legitimation med minst tillitsnivå tre. Exempel på en sådan e-legitimation är BankID.

### Arkivering och spårbarhet

För att uppnå enkelhet för ett signerat dokument bör vissa kriterier vara uppfyllda. Till exempel bör signaturerna vara personliga och inbäddade i dokumentet samt att de ska vara validerbara när som helst i efterhand. När underskrifterna är inbäddade innebär det att dokumentet alltid är att betrakta som ett original och det kommer bara att utgöra ett arkivobjekt. Med ett personligt certifikat bäddas underskriften in i en PDF i enlighet med den standard som eIDAS förordar (PAdES) och när man också använder LTV-nivån av denna standard valideras signaturen vid signeringstillfället och informationen sparas i dokumentet. Då uppfyller man också kraven både från Riksarkivet och eIDAS och har en avancerad underskrift med hög spårbarhet och som är arkivbeständig. Se stycket om fördjupning i lagar och rekommendationer för mer information om arkivering och PAdES.

### Krav på ägarskap

Hur och var man lagrar information är för många en viktig fråga. Den är viktig att ta hänsyn till även vid val av en tjänst för e-underskrifter. Ställ krav på ägarskap av all information kring underskrifter. Kravet representerar egentligen två saker, dels att säkra att ingen information utan användarens kännedom lämnar myndighets-/verksamhetsgränsen, men också att all information är enkel att kontrollera och spåra. Loggar och signeringsinformation ska alltid finnas tillgänglig inom organisationen. Om ni väljer att lagra den själva slipper ni ta ställning till cloud-act och schrems-II.





Formpipe.

# Att sätta igång med e-underskrift.

## Ta nästa steg i processen.

Val av lösning är en långsiktigt strategiskt viktig fråga och bör drivas centralt kopplat till hela verksamhetens långsiktiga behov.

Ett första steg för er som inte hunnit börja med e-signering är så klart att ta reda på mer, frågor som behöver besvaras kan vara:

- Hur funkar e-underskrivna dokument ihop med arkivet?
- Kan jag lita på elektroniska underskrifter?
- Är lösningar för e-underskrift informationssäkra?

En grund till detta finns nedan men om ni vill ha ytterligare stöd i er kunskapsinhämtning kan Formpipe erbjuda hjälp med det via en partner. Kontakta oss gärna på info@formpipe.com så berättar vi mer.

För er som har kommit lite längre i processen och önskar införa elektroniska underskrifter kan snarare frågorna som behöver besvaras handla mer om förankring internt och hur man kan komma igång. Frågor som dessa är viktiga att besvara:

- Vad vill vi uppnå med elektroniska underskrifter?
- Är juridik, kansli, IT och arkiv med på noterna?
- Vilka dokument/processer börjar vi igång med?
- Hur går vi vidare?

Oavsett om hur långt ni kommit i er utveckling föreslår vi en workshop som så klart är specifik för er.

Förslag på deltagare och agendapunkter finns nedan. Målet för workshopen kan vara att signeringslösningen blir förankrad internt och att det finns en grov plan för fortsatt arbete.

### Deltagare

Alla intressenter såsom juridik, registratur, arkiv, IT och tilltänkt förvaltare bör vara med på workshoppen. De är exempel på funktioner som behöver förstå och acceptera den lösning som väljs.

### Agenda

- Signering - hur funkar det?
    - *Vad händer tekniskt, hur ser ett signerat dokument ut, kan vi förlita oss på signaturerna och lösningen i sig?*
- Hur säkras dokument och signering från signering till långtidslagring?
    - *Informationssäkerhet, personuppgifter, loggning, validering*
- Vilka dokument ska vi börja med?
    - *Identifiera lågt hängande frukt. Vilka volymer finns, vad är krångligt, finns dokument för många underskrifter med långa ledtider.*
- Planera för implementation i verksamheten.
    - *Så sätter vi igång!*

Formpipe.

# En liten fördjupning i lagar och rekommendationer.

### Lagkrav

EIDAS-förordningen reglerar de lagkrav som finns kring elektroniska underskrifter oavsett om det är den enklaste nivån som bara benämns som en elektronisk underskrift men framför allt de mer tillförlitliga underskrifter som definieras som avancerad och kvalificerad underskrift. För att se vilka krav som ställs hänvisas till en standard,  PAdES, definierad via ETSI. När en lösning följer dessa blir resultatet en avancerad underskrift. Se mer information under nivåer av e-underskrifter.

### Nationella rekommendationer

För just Sverige har DIGG tagit fram rekommendationer kring den underskriftstjänst som tekniskt  behandlar hashvärdet för dokumentet och vad som krävs av ingående information såsom vilken nivå av tillförlitlighet en användares e-legitimation måste ha. Här finns också skisser och specifikationer hur lösningen bör skilja på tjänst för signering och tjänst för identifiering med mera. Men det är alltså inte e-tjänsten som användaren ser som DIGG i allmänhet skriver om.

### Krav kring dokumenthantering

Riksarkivet reglerar vilka kriterier som finns för långtidsbevarande gällande dokumentformat för bevarande, och kring elektroniska underskrifter*. I en rapport** från 2015 finns en förklaring kring hur och vilken information om signaturen som ska sparas för att kunna validera signaturen långt senare. Här hänvisar man också till PAdES. Riksarkivet har tagit fram en rapport med  uppdaterade skrivningar som ytterligare befäster logiken under punkt 3.1 i rapporten ovan. Rapporten kommer efter remiss att finnas tillgänglig hos Riksarkivet.

### Olika nivåer för e-signering.

eIDAS* beskriver tre olika nivåer av elektroniska underskrifter. Först definierar man elektronisk underskrift, det inkluderar egentligen all form av digital underskrift utan att specificeras mycket närmare.

Men man konstaterar i artikel 25 att “En elektronisk underskrift får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att underskriften har elektronisk form eller inte uppfyller kraven för kvalificerade elektroniska underskrifter.” och det är viktigt att ha med sig. Dock är en enkel form av elektronisk underskrift som tex en inklistrad scannad namnteckning mycket svår att verifiera, framför allt i efterhand. Som alternativ kan man istället erbjuda en annan lösning som passar det egna organisationen bättre för att slippa hantera de enklaste formerna av e-underskrifter.

I artikel 26 i eIDAS förordningen skriver man om avancerad elektronisk underskrift och krav kring den, där fokus ligger på koppling till undertecknaren. Man skriver sedan i artikel 27, punkt 5 att man ska fastställa referensformat för avancerade elektroniska underskrifter. Detta gör man i kommissionens genomförandebeslut 2015/1506 där man i bilagan hänvisar till tekniska specifikationer för signaturer för PDF dokument vilket är PAdES och den beskrivs i en ETSI standard. I denna standard tydliggörs också olika nivåer av PAdES och för bevarande över tid bör en lösning uppfylla kraven för LTV/LTA nivå.

I själva eIDAS förordningen definierar man även kvalificerad elektronisk underskrift ytterligare, bland annat krävs kvalificerade certifikat och en särskild anordning för skapande av kvalificerade underskrifter. I dagsläget finns ingen myndighet eller liknande i Sverige som kräver kvalificerad underskrift.

EIDAS förordningen skriver också om stämplar och det är motsvarigheten till signatur men för en juridisk person dvs ett företag. Detta innebär i förlängningen att om du i en PDF ser ett företag i signaturpanelen istället för de personer som ska ha signerat dokumentet så är det inte en handling signerad med en avancerad underskrift utan i bästa fall en enklare form av elektronisk underskrift stämplad med en avancerad stämpel vilket inte är samma sak.