ALT DU TRENGER Å VITE OM eID, E-SIGNERING OG DIGITALE LOMMEBØKER

NIVLHEIM

Hei!

Veilederen du nå leser inneholder alt du trenger for å få en grunnleggende forståelse for hva **elektronisk identifikasjon** (eID) er, hvordan **elektronisk signering fungerer** og hvilke regulatoriske endringer som nå skjer med **digital lommebok**. Målgruppen er produktledere, forretningsutviklere, tjenesteutviklere, designere, arkitekter eller ledere som ønsker en detaljert forståelse for hvorfor det er forretningskritisk å kjenne sine kunder og brukere, og hvordan eID, e-signering og digital lommebok er verktøy som hjelper til med dette.

Kunnskap om dine kunder og brukere er forretningskritisk! Å vite at det er rett person som bruker din tjeneste er helt nødvendig, slik at du ikke knytter opplysninger til feil person. I verste fall kommer sensitive personopplysninger på avveie, med tilhørende sanksjoner og bøter. Når du vet med sikkerhet hvem dine kunder og brukere er, kan du også tilby skreddersydde kundeopplevelser og tjenester som er tilpasset dem. E-signering er en forlengelse av eID, ved at en person kan signere dokumenter elektronisk ved hjelp av sin eID. Digital lommebok er et konsept som lar eieren av lommeboken oppbevare digitalt innhold som eID, elektronisk signerte dokumenter, fullmakter, sertifikater, attester, betalingskort og mye mer.

Martin Koksrud Bekkelund
Daglig leder i Nivlheim

NIVLHEIM

INNHOLD

eID 5

Hva er en identitet? 5

Hva er fødselsnummer og D-nummer? 6

Hva er bruksområdene? 8

Hva er identitetsbevis og legitimasjon? 8

Hva betyr å identifisere? 9

Hva er forskjellen på identifisering og autentisering? 10

Hva er en IdP? 10

Hva er elektronisk identifikasjon? 10

Bruksområder for eID 12

Hvem er myndighet for eID i Norge? 13

Hvilke eID-er finnes i Norge? 14

Hvordan anskaffer man eID? 14

Hvordan er Norge sammenliknet med andre land? 15

Hva er ID-porten? 15

Hva er eIDAS? 16

E-signering 17

Hva er signering? 17

Hva er e-signering? 17

Hva er en signatar? 18

Hvordan fungerer elektronisk signering? 18
Hvordan utstede dokumenter som skal signeres? 19
Hva er forskjellen på forskjellige signaturmetoder? 22
Simpel, avansert og kvalifisert signatur 23
Hva er PAdES og XAdES? 23
Hvordan kontrollerer man et e-signert dokument? 25
Oppbevaring av signerte dokumenter 25
Hvordan anskaffer man e-signering? 26
Digital lommebok 27
Hva er en digital lommebok? 27
Hvem gir deg en digital lommebok? 29
Hva kan du ha i en digital lommebok? 29
Hva er bruksområdene? 30
Hva betyr en digital lommebok for tjenestetilbyderne? 30
Hvem gir deg den digitale lommeboken? 31
Når kan du få en digital lommebok? 31
Kom i gang med eid, e-signering og digital lommebok 32

NIVLHEIM

eID

Hva er en identitet?

Før vi kan snakke om en elektronisk identitet, skal vi snakke om hva en identitet er.

I følge Wikipedia[1] er identitet fra latin «det samme» og betyr grunnleggende sett «likhet» eller «det samme som». Vi kan si at en identitet både har en filosofisk og en teknisk side.

Den filosofiske siden har forgreninger også til psykologien, sosiologien, politikken og kulturen, da en identitet handler om hvem vi er, hvordan vi oppfatter oss selv og hvordan andre oppfatter oss. Vi går ikke nærmere inn i dette i denne veilederen.

Den tekniske siden er mer målbar og handler om opplysninger som forteller hvem eller hva noen eller noe er, for eksempel en persons navn, fødselsdato, kjønnsidentitet og liknende.

> “
> En identitet forteller oss hvem en person er

[1] https://no.wikipedia.org/wiki/Identitet

NIVLHEIM

Hva er fødselsnummer og D-nummer?

Et fødselsnummer[2] er en konstruksjon som er skapt for unikt å kunne identifisere enkeltpersoner. I Norge er et fødselsnummer et ellevesifret nasjonalt identitetsnummer som tildeles av den norske stat til alle landets innbyggere. Nummeret skiller enkeltpersoner fra hverandre, men kan ikke brukes til å autentisere at en person er den de påstår de er. Fødselsnummer ble innført i 1964 og administreres i dag av Skatteetaten i Folkeregisteret[3].

Fødselsnummeret er konstruert av elleve siffer, hvorav de første seks er fødselsdatoen og de siste fem et konstruert personnummer.

[2] https://www.skatteetaten.no/person/folkeregister/identitetsnummer/fodselsnummer/

[3] https://www.skatteetaten.no/person/folkeregister/om/om/

NIVLHEIM

Et D-nummer[4] er et unikt identitetsnummer, på linje med fødselsnummer, som gjerne benyttes for personer som har en midlertidig tilknytning til Norge, for eksempel midlertidig arbeid, asylsøkere, eller utenlandske statsborgere med styreverv i et norsk firma.

> “
>
> Et fødselsnummer er en unik ID på en person

Fødselsnummer og D-nummer er den eneste nasjonale, unike identifikatoren for enkeltpersoner, og identifikatoren er å anse som konfidensiell og skal ikke deles med uvedkommende eller utveksles elektronisk over usikre kommunikasjonskanaler som e-post eller SMS. Årsaken er at fødselsnummer benyttes til en rekke formål som for eksempel å åpne bankkonto eller skaffe et mobiltelefonabonnement. Tilgang til et fødselsnummer således kan benyttes til identitetstyveri ved at personer med tilgang til fødselsnummeret kan bestille tjenester med fødselsnummeret.

Dette må du vite

Fødselsnummer og personsensitive opplysninger er underlagt regulatoriske krav til hvordan disse skal oppbevares og utveksles. Har du kontroll på hvordan slike og andre personopplysninger lagres og utveksles i din bedrift? Ta kontakt på martin@nivlheim.no eller 93055510 så hjelper jeg deg!

NIVLHEIM

Hva er bruksområdene?

Mange bedrifter og virksomheter har ofte omfattende tjenesteporteføljer med hundrevis eller tusenvis av systemer som i større eller mindre grad kommuniserer med hverandre. For tjenester som omhandler privatpersoner er det essensielt med en unik nøkkel som identifiserer personer på tvers av tjenestene, slik at man kjenner igjen personene og unngår inkonsistens i data og fragmenterte og dårlige brukeropplevelser. Et fødselsnummer kan være en slik unik ID, men det finnes også alternative identifikatorer som kan benyttes i tilfeller der man ikke kan oppbevare fødselsnummer eller D-nummer.

Dersom din bedrift har behov for å oppbevare fødselsnummer eller D-nummer i deres systemer, kreves et behandlingsgrunnlag som forklarer behovet. Skal du ha tilgang til oppslag i Folkeregisteret, kreves en egen søknad til Skatteetaten. Deretter kan oppslag gjøres direkte mot Folkeregisteret, eller gå via tredjepartsaktører som for eksempel elektroniske identifikasjonsmetoder som BankID.

Hva er identitetsbevis og legitimasjon?

Et identitetsbevis eller en legitimasjon, er et instrument — fysisk eller digitalt — som vi benytter for å dokumentere identiteten til en person. Et slikt instrument kan være et pass eller et nasjonalt ID-kort. Når denne veilederen skrives finnes det i Norge intet nasjonalt, elektronisk identitetsbevis utstedt av staten. Derimot finnes det flere godt kjente elektroniske identiteter som bygger på de fysiske, slik som BankID, Buypass og Commfides. For å få opprettet en elektronisk identitet med en av disse trenger du et pass eller et

nasjonalt ID-kort eller en annen eksisterende legitimasjon som disse utstederne aksepterer som gyldig legitimasjon.

Hva betyr å identifisere?

I følge Digitaliseringsdirektoratet[5] betyr identifikasjon «gjenkjenning som den samme», og kommer av latinsk idem, som betyr «den samme».

Å identifisere er selve prosessen med å slå fast med tilstrekkelig sikkerhet at en person er den vedkommende gir seg ut for å være. Med tilstrekkelig sikkerhet menes at konsekvensen av at identifiseringsprosessen går feil ikke er betydelig. Konsekvensen av at feil person åpner bankkonto i en annen persons navn er langt høyere enn at feil person handler en flaske vin på Vinmonopolet i en annen persons navn. Hva som er tilstrekkelig sikkerhet avgjøres av den som utfører identifiseringsprosessen, altså for eksempel banken eller Vinmonopolet. Forskjellige bransjer eller sektorer kan ha krav til hva man anser som tilstrekkelig sikkerhet. For eksempel er det i helsesektoren stilt krav om at helseopplysninger kun skal være tilgjengelig bak en eID på nivå «Høyt», tidligere kjent som «Nivå 4». Mer om sikkerhetsnivåer kan du lese i et påfølgende kapittel.

Vanlige situasjoner hvor man identifiserer seg kan være når man reiser utenlands, handler på Vinmonopolet eller åpner bankkonto.

[5] https://www.digdir.no/digital-samhandling/veileder-identifikasjon-og-sporbarhet-i-elektronisk-kommunikasjon-med-og-i-offentlig-sektor/2992

Hva er forskjellen på identifisering og autentisering?

I denne sammenheng er autentisering en del av identifiseringsprosessen, der autentisering er å verifisere en påstått identitet. Digitaliseringsdirektoratet opererer med tre forskjellige typer autentiseringsfaktorer:

- **Noe personen vet**, for eksempel et passord (kunnskapsbasert)
- **Noe personen har**, for eksempel en passordkalkulator eller en app på telefonen (besittelsesbasert)
- **Noe personen er**, for eksempel et fingeravtrykk (attributtbasert, biometrisk)

Autentiseringsfaktoren(e) må på et tidspunkt bli knyttet til en person og dennes identitet, og personen må også alene ha full råderett over autentiseringsfaktoren.

Hva er en IdP?

IdP står for «identity provider» og er en aktør eller et system som lager, vedlikeholder og administrerer identiteter og tilhørende autentiseringsmekanismer. Typisk tilbys slike tjenester elektronisk.

Hva er elektronisk identifikasjon?

I den fysiske verden benytter vi identifikasjon for eksempel med et fysisk pass når vi reiser utenlands. Digitalt, derimot, benytter et elektronisk identitetsbevis for eksempel når vi skal legitimere oss på nett. Det kan være når du skal åpne et kundeforhold i en ny bank, logge inn på offentlige tjenester og liknende.

Enkelte elektroniske identitetsmetoder tilbyr også muligheten til å foreta elektronisk signering. Mer om det finnes lenger ned i denne veilederen under kapittelet om elektronisk signering.

Elektronisk ID i Norge kommer i tre såkalte sikkerhetsnivåer:

- Høyt
- Betydelig
- Lavt

Bakgrunnen for disse tre sikkerhetsnivåene er at de angir ulike grader av tillit til at påstanden om identitet, i en elektronisk kommunikasjon, er korrekt.

Svært forenklet kan vi si at forskjellen mellom nivåene handler om hvor sikre vi er på at den opprinnelige identifiseringsprosessen er på at personen var den personen utga seg for å være da vedkommendes eID ble utstedt. Eksempelvis måtte du sannsynligvis møte opp fysisk i banken din med et pass for å få utstedt BankID. En motsetning til dette kan for eksempel være din konto hos Google, Apple eller Facebook, som du kan bruke til å logge inn også hos andre tjenester enn bare disse. I motsetning til BankID har du aldri møtt opp noe sted og identifisert deg, så tilliten til slike brukerkontoer

> “
>
> Apple, Google og Facebook *tror de vet* hvem du er, mens BankID *faktisk vet*.

NIVLHEIM

kan ikke sammenliknes med dem som gjennomgår en sikrere identifiseringsprosess. For en detaljert gjennomgang av forskjellen på nivåene, har Digitaliseringsdirektoratet en egen side[6].

Bruksområder for eID

Bruk av elektronisk ID har en rekke bruksområder, blant annet:

- **Legitimering og signering**, på forskjellige fysiske lokasjoner eller digitalt på nett. Det kan være at du skal etablere et boliglån og i denne sammenheng både skal legitimere deg og signere lånepapirene med en elektronisk ID.

- **KYC** står for «Know Your Customer»[7] og er et sett retningslinjer og reguleringer innen bank- og finanssektoren som pålegger for eksempel en bank å forstå identiteten til sine kunder, hvor skikket kunden er til å betjene sitt kundeforhold og hvilken risiko kundeforholdet medfører.

- **AML** står for «Anti-money laundering»[8] og er et sett med retningslinjer og praksiser som bank- og finanssektoren benytter for å forebygge, oppdage og rapportere økonomisk kriminalitet generelt og hvitvasking spesielt.

---

[6] https://www.digdir.no/digital-samhandling/veileder-identifikasjon-og-sporbarhet-i-elektronisk-kommunikasjon-med-og-i-offentlig-sektor/2992

[7] https://en.wikipedia.org/wiki/Know_your_customer

[8] https://en.wikipedia.org/wiki/Anti%E2%80%93money_laundering

- **SCA** står for «Strong Customer Authentication»[9] og er et krav i EU-regulativet PSD2; «Revised Directive on Payment Services». Det stilles krav om flerfaktorautentisering ved monetære transaksjoner, en funksjon som typisk er innebygget i en elektronisk ID.

- **Onboarding**, altså prosessen med å etablere et nytt kundeforhold elektronisk, typisk at en kunde registrerer seg på nett ved hjelp av en elektronisk ID som BankID eller liknende. Det kan være å åpne et kundeforhold hos en bank.

Dette må du vite

Mange bransjer og sektorer er underlagt regulatoriske krav til hva de må vite om sine kunder. Har du kontroll på hvilke krav din bedrift er underlagt? Og er du sikker på at du oppfyller kravene? Ta kontakt på martin@nivlheim.no eller 93055510 så hjelper jeg deg.

Hvem er myndighet for eID i Norge?

I Norge er det Nasjonal kommunikasjonsmyndighet (Nkom) som regulerer tilgangen til å tilby elektronisk ID. I følge Nkom[10] er det flere lover og forskrifter regulerer krav til elektronisk legitimasjon. Det kreves en eID-

[9] https://en.wikipedia.org/wiki/Strong_customer_authentication

[10] https://nkom.no/internett/elektronisk-id-og-tillitstjenester/elektronisk-identifikasjon-eid

ordning som oppfyller kravene i selvdeklarasjonsforskriften[11], og som er oppført på en publisert liste i henhold til § 13.

Ønsker du å tilby en elektronisk ID må du benytte Nkoms selvdeklarasjonsordning og sende inn et skjema.

Hvilke eID-er finnes i Norge?

I skrivende stund finnes det fem eID-er i Norge:

- BankID
- Buypass ID på smartkort
- Buypass ID i mobil
- Commfides eID
- MinID

BankID på mobil ble avviklet 1. september 2024.

Hvordan anskaffer man eID?

Hvis du har en tjeneste hvor du ønsker å ta i bruk en eID, trenger du å anskaffe en slik løsning enten fra tilbyderen eller via en forhandler. Tilbyderen leverer normalt selve basistjenesten, mens forhandlere gjerne tilbyr verdiøkende tilleggsfunksjonalitet. Hva du velger avhenger av hvilken arbeidsprosess du skal putte løsningen inn i. Ta kontakt på martin@nivlheim.no eller 93055510 så hjelper jeg deg med anskaffelsen.

[11] https://lovdata.no/dokument/SF/forskrift/2019-11-21-1578

Hvordan er Norge sammenliknet med andre land?

Norge kan sies å være blant de land som er aller lengst fremme i hele verden når det gjelder utbredelse og bruk av eID. Av en befolkning på litt over fem millioner mennesker, er det mer enn 4,6 millioner som har en eID[12].

I EU arbeides det for at både eID og en digital lommebok skal kunne benyttes på tvers av landegrensene innenfor unionen. Dette inkluderer også Norge, og erfaringene herfra benyttes inn i arbeidet i EU. Mer om den digitale lommeboken følger i et eget kapittel i denne veilederen.

Hva er ID-porten?

ID-porten utvikles, vedlikeholdes og driftes av Digitaliseringsdirektoratet og skal sikre innbyggerne i Norge innlogging til offentlige nettjenester eller til nettjenester som tilbyr tjenester på vegne av offentlig sektor.

ID-porten er, som navnet indikerer, en slags samling med flere eID-er, hvor den som skal logge inn kan velge å benytte den eID man selv har. Digitaliseringsdirektoratet har fremforhandlet egne priser med eID-tilbyderne som inngår i ID-porten. For den som tilbyr tjenester for offentlig sektor, er det langt mer økonomisk attraktivt å benytte ID-porten for innlogging og signering, enn å inngå en avtale med en eID-tilbyder direkte. For å benytte ID-porten som innloggingsmetode, er det et krav at tjenestene som det skal logges inn til utføres på vegne av offentlig sektor i Norge.

[12] https://www.norge.no/nb/digital-borgar/elektronisk-id

Hva er eIDAS?

eIDAS står for «electronic IDentification, Authentication and trust Services» og er en EU-forordning som har som formål å styre eID-er og tilhørende tillitstjenester for elektroniske transaksjoner. Tilbydere av slike tjenester må forholde seg til eIDAS-forordningen. Mer om eIDAS finnes hos Nkom[13]. eIDAS er retningsgivende for all videreutvikling av eID og tilhørende tillitstjenester i Norge.

[13] https://nkom.no/internett/elektronisk-id-og-tillitstjenester/eidas-forordningen

E-SIGNERING

Hva er signering?

I etymologien kommer ordet signere fra det latinske verbet «signare» som betyr «sette merke på» eller «merke», til det latinske substantivet «signum» som betyr «tegn» eller «merke».

I praktisk bruk betyr å signere å avgi et unikt og personlig tegn eller merke ved det vi kaller å undertegne eller underskrive, altså at vi skriver vårt eget navn på en måte som er unik og som binder vår aksept til det vi signerer på.

Typisk signerer vi et dokument for å inngå en avtale eller for å dokumentere autentisiteten til et dokument. Det kan være å inngå en låneavtale med en bank, der partene som inngår avtalen signerer det med sin underskrift. Det kan også være å utarbeide en fremtidsfullmakt der fullmaktsgiver og vitner signerer dokumentet for å dokumentere dens autentisitet.

Hva er e-signering?

Elektronisk signering har samme betydning som å signere noe fysisk, men at man gjør det ved hjelp av et elektronisk instrument. Typisk skjer dette ved at man benytter sin elektroniske identitet til å fortelle hvem man er, for så å koble denne identiteten til et merke som påføres et elektronisk dokument med tilstrekkelig grad av sikkerhet. Med tilstrekkelig grad av sikkerhet mener vi at måten en slik elektronisk signatur utføres på gir tilstrekkelig grad av sikkerhet for at den som utfører signeringen er den vedkommende gir seg ut

for å være, og for at prosessen skjer uten utilbørlig påvirkning, og at resultatet antas å være rettsgyldig.

Hva er en signatar?

En signatar er den personen som setter sin signatur på et dokument, enten det er fysisk eller elektronisk.

Hvordan fungerer elektronisk signering?

Konseptet om elektronisk signering fremstår enkelt, men fra et teknisk perspektiv er elektronisk signering en komplisert prosess. Når du benytter din elektroniske ID så utleveres det et digitalt sertifikat fra ID-en som så knyttes til dokumentet som skal signeres, og som så krypteres på en måte som gjør at det ikke kan endres. Dette digitale sertifikatet inneholder informasjon om signataren, slik som blant annet navn, fødselsdato eller fødselsnummer, og det er eID-utstederens garanti for at signataren er den signataren gir seg ut for å være. Det påføres et digitalt sertifikat for hver signatar som signerer.

En konsekvens av dette er at kryptografien blir kompleks og at størrelsen på et dokument målt i bits og bytes vokser kraftig.

Når et dokument signeres elektronisk så benyttes det kryptografiske metoder som anses som beste praksis på det tidspunktet som dokumentet signeres. Over tid, derimot, ser vi at kryptografiske metoder svekkes ved at det kan bli mulig å dekryptere innholdet når datamaskinene får mer regnekraft. Dersom man har behov for å oppbevare elektronisk signerte

dokumenter over lengre tid, det kan være lånedokumenter med lang løpetid eller testamenter, så bør man ha en prosess for å gjennomføre såkalt automatisk resignering av dokumentene. Det vil si at man påfører et nytt lag med nyere kryptografi utenpå det eksisterende dokumentet, på en måte som ikke ødelegger det opprinnelige innholdet. Man kan enten bygge sin egen resigneringsprosess, eller man kan benytte en tredjepart som utfører slike tjenester, og da blir dette gjort automatisk og på en måte som ikke involverer opprinnelige signatarer.

Hvordan utstede dokumenter som skal signeres?

Elektronisk signering er enkelt og lett tilgjengelig på nett både for privatpersoner og for bedrifter. Det betyr at man trenger ikke utvikle sin egen signeringstjeneste, men kan med fordel kjøpe dette fra en leverandør.

Som privatperson er det mange bruksområder for elektronisk signering. Det kan være ved eierskifte av bil eller utleie av hus og hytter.

Som bedrift er det også mange bruksområder for elektronisk signering. Det kan være inngåelse av kontrakter mellom bedrifter eller mellom bedrifter og privatpersoner.

Å få et dokument signert deles gjerne inn i tre steg i det som kalles en signeringsprosess:

1. Utarbeide dokument som skal signeres
2. Sende dokument til signering og få det signert
3. Distribuere og lagre signert dokument

Steg 1: Utarbeidelse av dokument

Enten man er en privatperson eller en bedrift så må dokumentet utarbeides. Dette kan gjøres i alt fra et vanlig tekstbehandlingsprogram som Microsoft Word eller Google Docs eller Apple Pages, men det kan også skje i mer spesialiserte programmer som et saksbehandlingssystem i bedriften. Når dokumentet er ferdig utarbeidet, produseres det som oftest en PDF som skal ivareta både den visuelle fremstillingen av dokumentet, men også innholdet, slik at gjenkjenningseffekten ivaretas så signatarer i fremtiden vedkjenner seg dokumentet. Denne delen av signeringsprosessen skjer som oftest i bedriftens egne saksbehandlingssystemer, men det finnes også spesialiserte verktøy som tar hånd om dokumentutarbeidelse, for eksempel utarbeidelse av kontrakter i såkalte *Contract Lifecycle Management*-systemer (CLM).

Steg 2: Sende dokumentet til signering og få det signert

Når dokumentet er ferdig produsert som en PDF skal det lastes opp til en signeringstjeneste som ivaretar selve signeringsprosessen. Dokumentet kan lastes opp i nettleseren dersom man er en privatperson eller en liten bedrift, men det kan også lastes opp maskinelt via et API[14] dersom man er en større bedrift og ønsker å ekspedere dokumentet rett fra saksbehandlingssystemet. Denne delen av signeringsprosessen skjer som oftest ved at dokumentet sendes fra bedriftens systemer til et eksternt system som for eksempel kjører som en tjeneste (SaaS[15]) i skyen.

[14] https://en.wikipedia.org/wiki/API

[15] https://en.wikipedia.org/wiki/Software_as_a_service

Steg 3: Distribuere og lagre signert dokument

Når dokumentet er lastet opp til signeringstjenesten må man angi informasjon om blant annet hvem som skal signere, når det er signeringsfrist, om det endelige dokumentet skal inneholde fødselsnummer eller bare fødselsdato, hvordan signatarer skal bli varslet om et dokument til signering, informasjon om tittel og innhold, med mer. Deretter låses dokumentet slik at det ikke kan endres straks det gjøres tilgjengelig for signatarene. Når den enkelte signatar signerer dokumentet påføres tidligere omtalte digitale sertifikater, og det endelige dokumentet produseres straks siste signatar har signert. Denne delen av signeringsprosessen kan enten utføres av signeringstjenesten man har valgt, dersom den har slik funksjonalitet, eller man kan ta hånd om den selv. En del signeringstjenester har funksjonalitet for å arkivere og distribuere signerte dokumenter til dem som har signert. Det er fordeler og ulemper med begge deler, og det avhenger av hvilke behov du har i din signeringsprosess.

Signeringsprosessen kan ofte bli omfattende og komplisert, avhengig av hvor mange dokumenter som skal flettes sammen og hvor mange personer som skal signere dokumentet og ha tilgang til det etterpå.

Dette må du vite

Å bygge en prosess fra utarbeidelse av dokumenter til endelig signert dokument er omfattende og det stilles regulatoriske krav til lagring og utveksling av data gjennom prosessen. Har du kontroll på din signeringsprosess? Eller lurer du på hvor du skal starte? Ta kontakt på martin@nivlheim.no eller 93055510, så hjelper jeg deg!

NIVLHEIM

Hva er forskjellen på forskjellige signaturmetoder?

Det finnes forskjellige måter å signere på. Kanskje har du fått en SMS der det står «Svar 'JA' på denne meldingen for å signere!», eller du har kanskje signert et dokument med pekefingeren på nettbrettet eller telefonen. Kanskje har du også brukt din eID, kanskje BankID, til å signere et dokument fra banken.

Alt dette er hva vi kaller signaturmetoder. Det er stor forskjell på signaturmetodene, både hvordan de fungerer men også i den innebygde sikkerheten. Å svare «JA» på en melding gir ingen garanti for at den som svarer er den vedkommende gir seg ut for å være. Heller ikke det å påføre en signatur med en pekefinger på et nettbrett. Dette fordi det ikke er en kobling mellom identiteten til den som utfører handlingen og det endelige sluttresultatet, men også fordi det endelige sluttresultatet heller ikke kan inneholde et digitalt sertifikat som med tilstrekkelig sikkerhet slår fast identiteten til signataren og dokumentets autentisitet.

Dette betyr derimot ikke at mindre sikre signaturmetoder er uegnet i bruk. Det betyr bare at den som skal ha noe signert må vurdere risiko. Hva er sannsynligheten for at feil person signerer noe, og hva er konsekvensen? Det har langt større konsekvenser at feil person signerer på et lånedokument fra banken, enn om feil person signerer for utlevering av en pakke fra Temu verdt 100,- kroner.

Som oftest gjør man lite feil ved å velge det vi kaller en sterkere signaturmetode. Dette må ses opp mot risiko og brukeropplevelsen i

signeringsprosessen. Sterkere signaturmetoder er ofte mer omfattende å gjennomføre og koster mer.

Simpel, avansert og kvalifisert signatur

Når man snakker om signaturmetoder kan det være nyttig å vite om at det bak disse signaturmetodene benyttes forskjellig teknologi for å ivareta sikkerheten og autentisiteten. Man vil i denne sammenheng komme over:

Elektronisk signatur, ofte kalt simpel signatur. Dette er en signaturmetode der man knytter informasjon om en person til det som signeres. Det kan være å svare «JA» på en SMS eller påføre signatur med pekefingeren på et nettbrett.

Avansert elektronisk signatur. Dette er PKI-basert signering ved hjelp av en elektronisk ID.

Kvalifisert elektronisk signatur. Det samme som avansert, men med krav til både det digitale sertifikatet som utstedes og til hvordan sertifikatet oppbevares.

Hva er PAdES og XAdES?

Som nevnt tidligere produseres det et endelig dokument når alle signatarer har signert dokumentet. Ofte kan dette være en PDF som både er lesevennlig, som inneholder informasjonen i dokumentet, og som også holder på all kryptografien. Denne PDF-varianten kalles en PAdES (PDF Advanced Electronic Signatures) og er en

ISO-standard som en utvidelse av PDF. Med denne standarden kan man produsere PDF-dokumenter som både kan holde avanserte elektroniske signaturer, samt kvalifiserte elektroniske signaturer.

Dersom man åpner en PAdES i en PDF-leser med rett funksjonalitet, vil man kunne lese ut de elektroniske signaturene og verifisere at dokumentet er autentisk. En slik leser kan være Adobe Acrobat Reader[16].

Fordelen med en PAdES er at det er en komplett pakke som inneholder alt du trenger i ett og samme dokument.

Ulempen med PAdES er at størrelsen målt i bits og bytes ofte er stor. For bedrifter med mange dokumenter som skal oppbevares over lang tid, vil størrelsen ha en kostnad når det skal lagres. Derfor ser man i slike tilfeller ofte på alternative måter å oppbevare signerte dokumenter på.

XAdES står for «XML Advanced Electronic Signatures» og er, svært forenklet, en del av et rammeverk som skal holde på avanserte (ikke kvalifiserte) elektroniske signaturer frikoblet fra dokumentet som er signert. En egenskap ved XAdES er at signerte dokumenter vil være gyldige i lang tid, også dersom kryptografien til det signerte dokumentet blir brutt. Resultatet er et XML-format som inneholder inneholder både signaturen og tilhørende data, slik som informasjon om dokumentet, tidsstempler, med mer. Utført riktig er XAdES rettskraftig i henhold til eIDAS-forordningen.

[16] https://get.adobe.com/reader/

Fordelen med XAdES er blant annet at det er plassbesparende og maskinlesbart. Ved å bruke såkalt «detached XAdES» kan man holde data separert fra selve signaturen, og heller pakke dette sammen ved behov, som igjen bidrar til å holde lagringskostnadene nede.

Ulempen med XAdES er at man som et menneske ikke kan åpne en XAdES på samme måte som en PAdES og lese innholdet.

Hvordan kontrollerer man et e-signert dokument?

Som nevnt kan man benytte Adobe Acrobat Reader til å kontrollere et signert dokument. BankID har en detaljert beskrivelse[17] som forklarer hvordan man benytter Reader til å gjennomgå dokumentet.

Oppbevaring av signerte dokumenter

Som en bedrift trenger man et system for å oppbevare signerte dokumenter. For små bedrifter med få og enkle dokumenter, kan det være tilstrekkelig å oppbevare signerte PDF-dokumenter på PAdES-formatet på et sikkert filsystem som det tas sikkerhetskopi av. Det kan være i Microsoft SharePoint eller Google Workspace. Derfra er det lett for et menneske å åpne dem, lese dem og gjøre seg kjent med innholdet.

For større bedrifter trenger man ofte et mer spesialisert arkiv for oppbevaring av signerte dokumenter. Det finnes enkle arkivløsninger som oppbevarer dokumentene, gjennomfører resignering automatisk, og som lar deg søke igjennom metadata som tittel og signatar. Det finnes også mer avanserte

[17] https://bankid.no/en/help/how-to-check-signatures

arkivløsninger som spesialiserer seg på å søke i innholdet i dokumentene, samt i å forstå innholdet. Denne typen arkivløsninger leser dokumentene maskinelt og tilbyr styringsinformasjon bedriftsledere kan ta beslutninger basert på. Enkelte tilbyr også løsninger for maskinlæring og kunstig intelligens, der man kan stille spørsmål til løsningen for eksempel som følger: «Hvor mange kontrakter har vi som løper ut ved nyttår?» Eller «Hvor mange kontrakter har vi som ikke oppfyller utlånsforskriften?».

Hvordan anskaffer man e-signering?

Hvis du har en tjeneste hvor du ønsker å ta i bruk e-signering, trenger du å anskaffe en slik løsning enten fra tilbyderen eller via en forhandler. Tilbyderen leverer normalt selve basistjenesten, mens forhandlere gjerne tilbyr verdiøkende tilleggsfunksjonalitet. Hva du velger avhenger av hvilken arbeidsprosess du skal putte løsningen inn i. Ta kontakt på martin@nivlheim.no eller 93055510 så hjelper jeg deg med anskaffelsen.

Dette må du vite

Det finnes en diger skog av mer eller mindre egnede verktøy for e-signatur. Et verktøy som fremstår som billig og brukervennlig, kan for din bedrift være feil valg fordi det ikke oppfyller de kravene din bedrift er stilt overfor. Jeg har evaluert e-signaturverktøy for kunder og hjulpet dem med å velge rett verktøy for jobben. Lurer du på hvor du skal starte? Ta kontakt på martin@nivlheim.no eller 93055510, så hjelper jeg deg!

DIGITAL LOMMEBOK

Den 29. februar 2024 vedtok EU innføring av eIDAS versjon 2.0[18]. Der versjon 1.0 av forordningen ikke levde opp til forventningene om en grensekryssende bruk av elektronisk ID, introduserer versjon 2.0 bruk av en digital lommebok som sikrer eieren av lommeboken tilgang til sikker elektronisk ID og tillitstjeneister som kan brukes i hele EU og EØS.

En digital lommebok i EU-sammenheng er et konseptuelt begrep som i skrivende stund ikke har noen fungerende implementasjoner ennå. Det vil si at det er pågående utviklingsarbeid som skal lede frem til en app på telefonen.

Det finnes flere varianter av digitale lommebøker, fra de mer kjente som Apple Pay og Google Wallet, til dem som kun oppbevarer kryptovaluta. I denne veilederen konsentrerer vi oss om arbeidet som skjer i regi av EU og hvordan det påvirker norske virksomheter og privatpersoner.

Hva er en digital lommebok?

Konseptet om en digital lommebok er at den skal fungere som en digital ekvivalent til den fysiske lommeboken mange av oss har dratt rundt på i mange år. I tillegg vil den digitale lommeboken kunne romme mer enn hva vi normalt har dratt med oss i den fysiske lommeboken.

[18] https://www.europarl.europa.eu/news/en/press-room/20240223IPR18095/meps-back-plans-for-an-eu-wide-digital-wallet

Målet med en digital lommebok er å gi eieren av lommeboken en plass å oppbevare betalingskort, identitetskort og dokumenter av særskilt høy verdi, slik at eieren kan benytte dette på tvers av landegrensene i EU og EØS. Vi kommer straks tilbake med eksempler på innhold.

For at en digital lommebok skal fungere etter intensjonen, er det vesentlig at eieren av lommeboken har fullt eierskap både til appen og til innholdet, slik at det ikke kan trekkes tilbake, manipuleres eller endres av andre. Eksempelvis skal ikke en flyktning oppleve at ens pass blir trukket tilbake av staten vedkommende flykter fra.

I tillegg til å oppbevare innhold av særskilt høy verdi, skal lommeboken også kunne tilby funksjonalitet for identifisering og elektronisk signering av dokumenter, og potensielt også gjennomføre betaling.

> “
>
> En digital lommebok har du på telefonen og den inneholder kort og dokumenter av særskilt høy verdi

NIVLHEIM

Hvem gir deg en digital lommebok?

Det er staten som skal tilby en digital lommebok, og den skal være gratis for alle. Gjennom eIDAS-forordningen versjon 2.0 forplikter staten å sørge for at alle har tilgang til en universelt utformet digital lommebok og at den inneholder en elektronisk ID på nivå høyt.

Hva kan du ha i en digital lommebok?

En digital lommebok skal som nevnt kunne holde forskjellige typer innhold som er av særskilt høy verdi for eieren. Dette kalles attesterte attributter (Qualified Electronic Attestation of Attributes — QEAA) og er digitale bevis som blir utstedt og validert av tjenestetilbydere, og legges inn i lommeboken på en måte som gjør at de kan vises frem, deles og verifiseres ved behov. Den som mottar eller blir forevist innholdet med slike attesterte attributter kan få bekreftet at bevisene er ekte og at den som fremviser dem er den vedkommende gir seg ut for å være.

Eksempler på dette kan være, men er ikke begrenset til:

- Betalingskort
- Identitetskort
- Pass
- Førerkort
- Vitnemål
- Attester, for eksempel
- Fødselsattester
- Vigselsattest

- Bostedsattest
- Arbeidsgiverattester
- Lånedokumenter
- Kontrakter og signerte dokumenter
- Fullmakter
- Resepter

Hva er bruksområdene?

Som innehaver av en digital lommebok er målet at du skulle kunne gjennomføre oppgaver du ellers ville gjort med en mengde fysiske papirer, dokumenter og beviser. Det kan være å åpne en bankkonto, få utskrevet resepter eller fremvist vitnemål.

Et mål er at du kun skal måtte utlevere den informasjonen som er nødvendig for å utføre den oppgaven du skal gjøre der og da, gjennom det eIDAS omtaler som «Selektive Disclosure». Det vil for eksempel si at Vinmonopolet ikke trenger fullt fødselsnummer for å selge deg en flaske vin, de trenger kun fødselsdatoen din. Videre skal du kunne bruke den digitale lommeboken for innlogging til forskjellige nettjenester, og også her er målet at du ikke skal gi fra deg mer informasjon enn nødvendig når du oppretter en konto og logger inn, slik at personvernet ditt styrkes.

Hva betyr en digital lommebok for tjenestetilbyderne?

I praksis medfører eIDAS 2.0 at alle som leverer tjenester som krever innlogging for eksempel med BankID eller Buypass må legge til rette for identifisering og innlogging med en digital lommebok der det er eieren av

lommeboken som utleverer opplysningene og ikke banken eller en annen tredjepart. Dette må sies å styrke personvernet ved at ikke banken eller en annen tredjepart får kunnskap om når personopplysninger blir benyttet. Eksempelvis er det ikke nødvendig for banken å vite at du har logget inn på et nettapotek eller identifisert deg på Vinmonopolet.

Hvem gir deg den digitale lommeboken?

Som nevnt er det staten som har ansvaret for at du får en digital lommebok, men akkurat som at det innen områdene ID og signering er underleverandører av denne funksjonaliteten, kan vi se for oss at vi får en digital lommebok fra tredjepartsaktører som oppfyller kravene fra staten.

Når kan du få en digital lommebok?

EU-vedtaket innebærer at alle EU-land må tilby en digital lommebok innen to år. For Norges del er det sannsynlig at vi vil se en digital lommebok et år eller to senere, altså i 2026 eller 2027[19].

Dette må du vite

Har du kontroll på hvordan du skal ta betalt med digital lommebok i din bedrift? Eller hva din bedrift kan putte oppi en slik lommebok? Eller om din bedrift blir underlagt regulatoriske krav når en digital lommebok innføres i din bransje? Ta kontakt på martin@nivlheim.no eller 93055510, så hjelper jeg deg!

[19] https://www.digdir.no/media/4741/download

NIVLHEIM

KOM I GANG MED EID, E-SIGNERING OG DIGITAL LOMMEBOK

Kanskje lurer du på hvordan bruk av eID kan bidra til å øke kvaliteten på tjenestene som din bedrift tilbyr, eller hvordan elektronisk signering kan gi konkurransefortrinn? Eller kanskje du lurer på hvordan digital lommebok kommer til å påvirke din bedrift og hvilke tiltak du må gjøre?

I mer enn 10 år har jeg veiledet bedrifter i problematikken om eID, e-signering og digital lommebok, slik at de blir trygge på hvordan de skal forholde seg til disse fagområdene. Nå hjelper jeg gjerne deg! Trykk på den grønne knappen under for en uforpliktende prat, eller kontakt meg på martin@nivlheim.no eller 93055510.

Jeg kan veilede i ett eller flere av disse fagområdene og jeg har et stort nettverk med dyktige mennesker som hjelper deg med tilstøtende områder, enten det er sikkerhetsrådgivere, advokater, utviklere eller driftere.

Mer informasjon om Nivlheim finner du på nivlheim.no hvor du også finner andre veiledere, podcaster, nyhetsbrev, med mer.

Jeg trenger hjelp med eID, e-signering eller digital lommebok

NIVLHEIM

RETTIGHETER

Denne veilederen er skrevet av Martin Koksrud Bekkelund i Nivlheim AS. Veilederen (kalt Verket) er omfattet av åndsverklovens bestemmelser. Verket er tilgjengelig under lisensen *Creative Commons Attribution-NonCommercial-NoDerivs 4.0 International*[20]. Det innebærer at du har lov til å dele, kopiere og spre Verket under forutsetning av at du krediterer opphavet med en lenke til https://www.nivlheim.no/, at du ikke bruker materialet i kommersiell sammenheng, og at du ikke bruker hele eller deler av Verket inn i dine egne produksjoner. Kommersiell sammenheng betyr at du ikke kan selge det, men bruke det i en kommersiell bedrift for å lære av innholdet.

EKSTERNE VERK BENYTTET I VEILEDEREN

Forsidebilde av Leon Lønsetteig. Filtype-ikoner av IconMarketPK.

DOKUMENTHISTORIKK

Versjonsnummer	Publiseringsdato
1.0	

[20] https://creativecommons.org/licenses/by-nc-nd/4.0/

NIVLHEIM