Notat 2002:8

Elektronisk plan- og byggesaksbehandling og krav om signatur med videre i lover og forskrifter

Rapport til ByggSøk-prosjektet skrevet på oppdrag fra Statens byggningstekniske etat

Forord

Dette notatet er Statskonsults første utredning for ByggSøk-prosjektet, på oppdrag fra Statens bygningstekniske etat. Arbeidet er gjennomført av seniorrådgiver Amund Eriksen (prosjektleder), seniorrådgiver Halvor S. Oseid og seniorrådgiver Annikken B. Seip.

Statskonsult ble av Statens bygningstekniske etat bedt om å gjennomføre en utredning om behovet for elektronisk signatur og kryptering i forhold til et av regjeringens hovedprosjekter i eNorge-planen; ByggSøk. Dette prosjektet har utviklet et første system for å fylle ut byggesøknader på internett. Systemet er under videreutvikling. Prosjektet skal legge til rette for at internett blir et verktøy for å effektivisere den kommunale plan- og byggesaksbehandlingen.

Målet med Statskonsults utredning har vært å avklare hvordan elektronisk plan- og byggesaksbehandling skal forholde seg til aktuelle rettsregler, særlig plan- og bygningslovgivningen, lov om elektroniske signaturer og forskrift om elektronisk kommunikasjon, i forhold til ByggSøk-prosjektets behov.

Oslo, Juni 2003

Guri Verne
avdelingsdirektør

Innhold

1 Bakgrunn

1.1 ByggSøk-prosjektet

Statens bygningstekniske etat og Statens kartverk gjennomfører prosjektet ByggSøk etter oppdrag fra Kommunal- og regionaldepartementet og Miljøverndepartementet. Prosjektet skal legge til rette for at Internett blir et verktøy som bidrar til å effektivisere den kommunale plan- og byggesaks-behandlingen.

ByggSøk-prosjektet har utviklet et system for å fylle ut byggesøknader på Internett. Den ferdig utfylte saken kan enten skrives ut på egen skriver og sendes kommunen i form av papirpost, eller den kan sendes elektronisk over til kommuner som kan ta i mot elektroniske søknader. Sommeren 2002 hadde fire store leverandører av kommunale saksbehandlingssystemer utviklet tilleggs-moduler til sine systemer. Kommuner som installerer denne tilleggsmodulen kan nå motta byggesøknader via Internett. Intensjonen var å gjennomføre fullskala tester av systemet i sommer/tidlig i høst. Det er forventet at flere kommuner vil bli i stand til å motta elektroniske byggesøknader i løpet av kort tid.

1.2 Bygningslovgivningen

Bygningslovgivningen har gjennomgått en ganske omfattende reform ved ikraftsettelsen av lov- og forskriftsreglene som er vedtatt i løpet av 1995 - 97. Hovedformålet med disse endringene har vært å sikre bedre kvalitet på gjen-nomføring av byggeprosessen, for derved å høyne kvaliteten på byggverk som føres opp. Dette oppnås blant blant annet ved at vesentlige deler av byggepro-sessen skal forestås av ansvarlige foretak. De ansvarlige foretak er pålagt et direkte ansvar overfor bygningsmyndighetene for de faser av tiltaket foretaket har ansvarsrett for. Retten til ansvar er knyttet opp mot kvalifikasjonskrav og krav til at foretakene har gode systemer for å oppfylle forskriftskravene. Sam-tidig skal de ansvarlige foretak dokumentere at tiltaket oppfyller kravene i bygningslovgivningen. Sikringen av dette gjennomføres ved krav til kontroll, som aktørene selv skal stå for.

De kommunale bygningsmyndighetenes og øvrige aktørers oppgaver og plikter i en byggesak er beskrevet i bestemmelser gitt i eller i medhold av *plan- og bygningsloven*. Kommunen har et overordnet ansvar for å påse at tiltaket er i samsvar med bindende arealplaner og lovens rammebestemmelser. Videre skal kommunen vurdere kvalifikasjonene og systemene til de foretak som skal være ansvarlige for gjennomføring og kontroll av den tekniske delen av prosjektet. Ved systemrevisjon og stikkprøvekontroll kan kommunen føre tilsyn med at gjennomføringen av tiltakene skjer i samsvar med de vilkår som fremgår av de tillatelser som er gitt, eller de meldinger som er akseptert, og kommunen gjen-nomfører i det hele tatt tilsyn for å sikre at regelverket blir fulgt. *Forskrift om saksbehandling og kontroll i byggesaker* (SAK) binder sammen de forskjellige

deler av byggeprosessen og aktørenes gjøremål i den. I tillegg finnes det blant annet *Forskrift om krav til byggverk og produkter til byggverk* (teknisk forskrift) (TEK) og *Forskrift om godkjenning av foretak for ansvarsrett* (GOF).

1.3 Statskonsults oppdrag

Statens bygningstekniske etat har bedt Statskonsult utrede bruk av elektronisk signatur og eventuelt behov for kryptering av dokumenter i forbindelse med plan- og byggesaksbehandlingen. Statens bygningstekniske etat peker på at det i plan- og bygningsloven (pbl.) m/forskrifter flere steder er krav om signering av dokumenter, eksempelvis i pbl. § 93b nr. 1, der søknaden skal undertegnes både av tiltakshaver og ansvarlig søker, og de aktuelle foretakene skal skrive under søknad om ansvarsrett, kontrollplan og kontrollerklæringer.

Statens bygningstekniske etat understreker sitt behov for å ha en gjennomtenkt strategi i forhold til hvordan lovens krav til signatur kan oppfylles i en elektronisk søknad. Man peker også på de nye bestemmelsene som er vedtatt om bruk av elektronisk signatur i forvaltningen, og fremhever ByggSøk-prosjektets behov for å få avklart hvordan elektronisk plan- og byggesaksbehandling skal forholde seg til bestemmelsene om elektronisk signatur, og hvilke alternative løsninger som finnes, som kan dekke prosjektets behov.

Statens bygningstekniske etat understreker også at hensikten med utredningen fra Statskonsult er å bruke den som en del av det beslutningsgrunnlaget som vil bli lagt frem for ByggSøk-prosjektets to departementer, Kommunal- og regionaldepartementet og Miljøverndepartementet. Man regner med at disse departementene vil ta beslutninger om når bruk av elektronisk signatur eventuelt er nødvendig, og hvilket sikkerhetsnivå som i så fall vil være det riktige.

Innenfor den relativt korte tiden som sto til disposisjon har Statskonsult brukt som metode å gjøre rede for aktuelle rettsregler og –hensyn på området for elektronisk kommunikasjon, med krav til underskrifter og konfidensialitet, og enkelte andre forhold som hører med. Det er tatt et generelt utgangspunkt, som plan- og byggesaksbehandlingen må forholde seg til, i tillegg til eget sektorregelverk. På denne bakgrunn er det en gjennomgang av de utvalgte og antatt mest relevante rettsregler, herunder lov om elektronisk signatur, forskrift om elektronisk kommunikasjon med og i forvaltningen, personvernregler, samt utvalgte regler fra plan- og byggesakslovgivningen. På det sistnevnte området kunne det med fordel ha vært brukt mer tid, og vært utvekslet mer informasjon med de myndigheter og prosjekter som har førstehånds kunnskaper på dette feltet. Slik utredningen nå foreligger, bærer den nok noe preg av ”skrivebordstenkning”, og uten å ha kunnet ta tilstrekkelig hensyn til alle de kunnskaper som sektormyndigheter og prosjektdeltakere i ByggSøk har. Slik sett ville det ikke være unaturlig eventuelt å følge opp dette arbeidet med nærmere dialoger, for å komme dypere inn/ned i de spørsmålene som oppstår i overgangen fra papirbasert til elektronisk basert saksbehandling og forvaltning. Dette tror vi kunne være nyttig.

2 Hva kan en oppnå med elektroniske signaturer og innholdskryptering, og med hvilken tillit?

Elektronisk signatur er et upresist og overordnet fellesbegrep som kan dekke flere metoder eller teknikker. Hvilke teknikker man skal bruke vil avhenge av hva signaturen skal brukes til, hvilken funksjon den skal dekke, og hva som gir tilstrekkelig eller tilfredstillende sikkerhet/funksjonalitet i forhold til det som kan gå galt/de feilene som kan oppstå. Elektroniske signaturer kan benyttes til å "signere" digital informasjon. Metoden kan ivareta flere av de samme funksjonene som en håndskrevet signatur i forhold til et papirdokument, og en del av dem til og med på en bedre måte. I tillegg har metoden nyttige funksjoner som den håndskrevne underskriften ikke har. Teknikken får betydning for jussen (og omvendt), blant annet i sammenhenger hvor det å "skrive under" spiller en rolle. I tillegg vil kryptering av innholdet gjøre det uleselig/uforståelig for uvedkommende, slik at krypteringen kan sies å fungere som en godt lukket konvolutt.

Ved krav om underskrift er det aktuelt å spørre:

- Hvilke funksjoner skal signaturen dekke?
- Hvilken risiko løper man hvis den aktuelle funksjonen ved signaturen faktisk ikke oppnås, er feil, eller falsk?

2.1 Funksjonalitet

I papirverdenen er det ofte underforstått, eller sammenhengen tilsier, hva en bestemt signatur innebærer. Vi er på en måte så vant til å skrive under, at vi ikke tenker bevisst gjennom hvilke funksjoner underskriften kan ha. Den kan ofte dekke flere funksjoner på én gang. Når man skal forflytte signering til den elektroniske verdenen, så fungerer teknologien der annerledes. Den kan som nevnt (til dels) gi samme funksjonalitet, eller annen/ny funksjonalitet, men den oppnår funksjonaliteten på en annen måte, ved en annen teknikk, naturlig nok. Ved overgang til elektroniske måter å gjennomføre blant annet underskrifter på, er det derfor viktig å vite hva man forventer å oppnå, hvilke konkrete funksjoner som skal dekkes, som et ledd i vurderingen om å ta for eksempel elektroniske signaturer i bruk. De følgende punktene kan være en sjekkliste for dette formålet:

a) **Identifiseringsfunksjon;** målet er å se hvem som signerer, med hvilket navn eller identitet. Håndskrevne signaturer er ofte uleselige, så man må ty til maskinskrevne bokstaver i tillegg for å være sikker på å bli forstått. I en elektronisk verden kan man ty til mange ulike måter å gjøre dette på, fra vanlig maskinskrevet navn (e-post, nett-skjema), til en eller annen form for elektronisk signatur (det finnes flere, blant annet PIN-kode[1], biometrisk gjenkjenning, eller

[1] PIN står for Personal Identification Number, ofte en firesifret kode som brukeren har for å identifisere seg overfor et system (typisk minibank).

digital signatur). I tillegg kan man identifisere aktuell elektronisk enhet, i form av dokument, maskin, system, nettside, prosess.

b) **Autentiseringsfunksjon;** målet er å kunne kontrollere at den som underskrev, faktisk er den som han eller hun gir seg ut for å være. I papirverdenen er det bare i spesielle situasjoner man har sett behov for dette, for eksempel i forbindelse med sjekker og lignende i banksektoren. For øvrig kan man si at håndskrevne underskrifter generelt etterprøves i liten grad, og det er sjelden noe rettslig krav om det. Tilliten baserer seg ikke på at teknikken er sikker eller lett etterprøvbar, men vi er vant til det, det er kulturelt akseptert, over lang tid, og det går stort sett bra i det praktiske liv. Tilsvarende er vi uvante med den elektronisk verden, vi har ikke innarbeidede tradisjoner, dette er nytt og ukjent og oppleves utrygt. Men nettopp i elektroniske løsninger finner vi teknikker som tilbyr en form for kontroll og trygghet som ikke finnes i papirverdenen, slik at det blir en naturlig del av det elektroniske systemet å autentisere/bekrefte at det faktisk *er* underskriveren man kommuniserer med. I tillegg kan man få bekreftet at opplysninger som identifiserer et dokument, en maskin, system, nettside, prosess, faktisk er ekte, at opplysningene stemmer.

c) **Autorisasjonsfunksjon;** handler om hva man "har fått lov til å gjøre", hvilken adgang man har til noe, enten det er rett til tilgang eller rett til å gjøre noe av juridisk bindende karakter (med fullmakter bak). Selve underskriften kan ikke si noe om hva man eventuelt er autorisert for, dette må fremgå av et underliggende forhold, - både i papirverdenen og i den elektroniske.

d) **Integritetsfunksjon;** målet er å gjøre noe som gjør det mulig å oppdage om dokumentet eller underskriften er forandret/manipulert/forfalsket i kommunikasjonen fra avsender til mottaker. I papirverdenen vil håndunderskrift (med for eksempel blått blekk) på papirdokumentet inngå i en fysisk sammenheng med arket, som gjør det mindre sannsynlig at det kan endres. Elektronisk finnes det teknikker som gjør det enkelt å oppdage denne typen endringer.

e) **Bevisfunksjon;** en signatur knyttet til et dokument kan brukes som bevis i ulike sammenhenger, bevis for at noe er gjort, hvem som har gjort det, osv. Det er styrken i beviset som blir avgjørende for om man tror på det eller ikke, enten det gjelder papir eller elektronikk, dagligliv eller i en rettssak.

d) Underskrifter brukes til å avslutte prosesser, f.eks. forhandlinger, en søknad eller et vedtak og har da en **avslutningsfunksjon.** Velkjent måte å skille mellom utkast/kladd, og det ferdige produktet. Kan ivaretas i "begge verdener".

f) En signatur kan f.eks. understreke alvoret i en handling og har da mer av en **symbolfunksjon** enn en bevisfunksjon. Kanskje mest aktuelt i papirsammenhenger?

I noen situasjoner kan man ønske at en signatur skal bekrefte det faktum at en person har vært på et gitt sted, på et tidspunkt, med intensjon om å godkjenne/-vedkjenne seg forfatterskapet av/innholdet i teksten, med intensjon om å knytte seg til en tekst skrevet av andre, osv.

I papirverdenen sjekker man ikke nødvendigvis alle disse punktene, men i en tvistesituasjon kan de til sammen styrke en påstand eller svekke den. I en elektronisk verden ønsker man med andre ord å finne teknikker som støtter opp om

det vi her kaller *sikkerhetstjenester*, som dekker mange av funksjonene ved håndunderskrift, og har andre i tillegg. PIN er én teknikk, digital signatur er en annen. De har ulik funksjonalitet og ulik grad av sikkerhet for å støtte den. Dette er nytt både for systemeierne og for brukerne. I følge den nye forskriften om elektronisk kommunikasjon med og i forvaltningen (omtales senere), er det en plikt for de forvaltningsorganer som ber brukere benytte elektronisk kommunikasjon, å veilede brukerne om hva dette går ut på, eventuelle risikosider ved det, og nøye forklare hvordan brukerne kan eller skal gå frem for å ta de aktuelle teknikkene i bruk.

I tillegg til underskriftsfunksjoner kan man ha behov for å skjule innholdet i dokumentet for uvedkommende, enten fordi det er uferdig, inneholder sensitive personopplysninger eller det er pålagt taushetsplikt for de aktuelle opplysningene. I papirverdenen er vi vant til å lime igjen konvolutter for å gjøre det utilgjengelig/uleselig for uvedkommende. I den elektroniske verden må man bruke kryptering for å oppnå det samme. Mer om dette senere.

2.2 Risikovurdering

Hva som er godt nok som signatur, vil variere med hvor sikkert/sårbart systemet er, hvilke problemer det utsettes for og hvor mye man taper hvis noe går galt. Dette må vurderes i hvert tilfelle.

Eksempler på problemstillinger som bør vurderes

Hva skal forhindres:

- at noen sender inn falsk søknad,
- at det er usant at tømreren har alle papirene i orden
- at noen signerer på vegne av andre
- at noen usant ”dokumenterer” at nabovarsel er sendt, eller at naboene har samtykket
- at noen starter å bygge uten å ha lov

Hvor uheldig er det at disse problemene kan inntreffe:

- skjer det ofte at det sendes falske søknader eller falsk dokumentasjon i forbindelse med nabovarsel/samtykke?
- hvor ofte opptrer profesjonelle på falske premisser?
- hvor mye arbeidstid og penger taper man på det?
- hvor mange rettssaker man får ved falske signaturer

Hvis det ikke er så farlig uten signatur, hva vil likevel gi søkeren en indikasjon på at han må vite at han sender inn en søknad til et offentlig kontor og opptar deres tid hvis han ikke er seriøs?

Involverer saksbehandlingen opplysninger som må holdes skjult for uvedkommende? Hvilke og hvor ofte?

Hvilke mekanismer gir systemeier akseptabel sikkerhet for at søknaden er i hht. regelverket?

2.3 Tiltak for å motvirke risiko, og oppnå ønsket funksjonalitet

2.3.1 Sikkerhetstjenester og –teknikker

For å motvirke den risiko man har vurdert som relevant, eller for å oppnå den funksjonen man er ute etter (signatur/skjule innhold, jf listen foran) kan man ta i bruk det som kalles s*ikkerhetstjenester* (som ikke må forveksles med nasjoners "hemmelige tjenester" eller lignende). Sikkerhetstjenestene det tenkes på er i hovedsak følgende: *autentisering* (gjøre det mulig å få bekreftet at oppgitt identitet stemmer), *integritet* (at endringer ikke skjer uønsket, at eventuelle endringer lar seg oppdage), *ikke-benekting* (at en ikke kan nekte for å ha gjort noe) og *konfidensialitet* (at uvedkommende ikke skal få tilgang til informasjonen). Sikkerhetstjenestene er i denne sammenhengen en overordnet betegnelse på en egenskap eller ytelse som vi ønsker eller trenger i et system, og sier ikke i seg selv noe om *hvilken teknologi som benyttes for å realisere løsningen*. Begrepet sikkerhetstjeneste brukes blant annet i forskriften om elektronisk kommunikasjon (som blir nærmere omtalt i kapittel 4). Disse tjenestene er uttrykk for behov som er relativt stabile over tid, jf oversikten over om de funksjonene man ønsker å oppnå når man bruker signatur, eller skal holde noe hemmelig/skjult.

Sikkerhetstjenester kan ivaretas av sikkerhets*teknikker* eller *–mekanismer*, som er teknikk- og tidsavhengige forhold og kan være av fysisk, organisatorisk eller logisk (systemteknisk) karakter. Av sistnevnte slag har vi de elektroniske produktene som til enhver tid er på markedet. Kryptering og elektroniske eller digitale signaturer er eksempler på slike. Fysisk og organisatorisk sikkerhet ut fra et helhetssyn i virksomheten hører med, fordi sikkerhet i bare enkelt-ledd ikke er tilstrekkelig, uansett om dette enkelt-leddet er sterkt i seg selv.

Tradisjonelt har vi løst *konfidensialitet* ved bruk av forseglede konvolutter og kurérpost, mens elektronisk kommunikasjon blir tilsvarende beskyttet ved hjelp av kryptering. Kryptering forvrenger det digitale signalet slik at bare rettmessig avsender og mottaker ser det opprinnelige innholdet i klartekst. Kryptografi er et omfattende teknologisk fagfelt, men de grunnleggende idéene er enkle.

Symmetrisk kryptering bruker to like nøkler, og egner seg godt til raskt å kryptere/dekryptere store datamengder. Men det er et alvorlig problem å få fordelt de to nøklene til bare de aktuelle deltakerne. De skal holdes strengt hemmelig, og det er upraktisk å distribuere dem til mange og/eller over store avstander.

Asymmetrisk kryptering bruker også to nøkler, men de er ulike (derav navnet), og den ene både kan og skal være offentlig tilgjengelig for alle, mens den tilhørende nøkkelen skal være hemmelig/privat. Kravet til hemmelighold av nøkkelen fra symmetrisk krypto er erstattet av et krav om at den offentlig

tilgjengelige krypteringsnøkkelen må være ekte eller autentisk, samt krav om sikre opplysninger om hvem den hører til.

Dette betyr at asymmetrisk krypto er best egnet til å løse de klassiske problemene knyttet til nøkkelfordeling. Men også her kreves det organisasjonsmessige og tekniske løsninger for å etablere den infrastrukturen som skal til for å få offentlige nøkler i bruk på en god måte. Bruk av nøkkelsertifikater og katalogtjenester er viktig for å få til dette.

I praksis er alle asymmetriske kryptosystemer for langsomme til å kryptere store mengder data eller trafikk i sanntid. Det er derfor vanlig å lage blandingssystemer, der man benytter det asymmetriske systemet til å fordele trafikknøkler som går inn i symmetrisk kryptering av selve meldingen.

En spesiell variant er det som kanskje litt villedende kalles *digitale signaturer*. Digitale signaturer er også eksempel på en teknologi innenfor området kryptering (asymmetrisk krypto), men her brukes nøklene den andre veien, det vil si på en måte som ikke skjuler innholdet. Teknikken har som hovedoppgave å realisere sikkerhetstjenester som autentisering, integritet og ikke-benekting, men ikke konfidensialitet.

Teknologien i asymmetriske systemer er en helt annen enn i de symmetriske systemene, blant annet vil kravene til nøkkellengder være helt forskjellige. En kan derfor ikke sammenligne nøkkellengder mellom DES (symmetrisk kryptoalgoritme) og RSA (asymmetrisk).[2] En god egenskap ved mange asymmetriske løsninger er at de enkelt kan skaleres opp til et ønsket sikkerhetsnivå.

For å få et digitalt signatursystem til å virke i praksis, er det nødvendig å etablere en infrastruktur som sikrer at alle parter får tilgang til de ulike nøklene som trengs. Alle skal ha tilgang til alle verifiseringsnøklene (de offentlige nøklene).

Kort oppsummert: I et *signatursystem* er det kun en person som kan signere ved hjelp av den hemmelige signeringsnøkkelen, men det er mange som kan verifisere signaturen ved hjelp av den offentlig tilgjengelige verifiseringsnøkkelen. Verifiseringen er en måte å få bekreftet at signaturen er ekte, eller få en økt sannsynlighet for dette.

Både lov om elektronisk signatur (se kapittel 3) og forskriften om elektronisk kommunikasjon (se kapittel 4) bygger på blant annet kryptering og digitale signaturer, hvor kryptografi ved hjelp av offentlig tilgjengelige nøkler, med

[2] Den amerikanske standarden for symmetrisk kryptering, DES, står for Data Encryption Standard. Den ble offentliggjort i 1975 av det som nå er NIST, National Institute of Standards and Technology, som en åpen standard for ikke-graderte formål, der en bruker to hemmelige kryptonøkler. DES er nå erstattet av AES, Advanced Encryption Standard, som føderal sektor i USA skal følge, iht Federal Information Processing Standard (FIPS) 197. RSA er en offentlig nøkkelkryptografi for signering, basert på en hemmelig signeringsnøkkel og en offentlig verifiseringsnøkkel. Den er oppkalt etter de amerikanske opphavsmennene Rivest, Shamir og Adleman. Metoden ble publisert i 1978. Både DES og RSA har siden de ble publisert fått stor utbredelse i hele verden, som de facto standarder på området. Det er ventet at AES vil få tilsvarende utbredelse og status.

hjelp fra tredjeparter, er viktige ingredienser. Men også kryptering med like nøkler kan være aktuelt.

Ved god implementering og bruk av sikkerhetsteknikker, og ivaretakelse av behovet for helhetlig sikkerhetstenkning (inkludert fysisk, organisatorisk og logisk sikring), kan det kommuniseres trygt ved hjelp av åpne og utrygge nettverk, som Internett. Men det må gjennomføres en risikovurdering for å finne det riktige sikkerhetsnivået, og mye kan gjøres uten (altfor) mye sikkerhet.

2.3.2 Hva er et sertifikat, og hvorfor trenger man det?

Når de offentlige nøklene blir viktige for det en skal oppnå, hvordan kan en vite at den offentlige nøkkelen for verifisering av en signatur, faktisk hører til den vi vil kommunisere med, og ikke noen andre? Det gis ikke noe enkelt svar på dette spørsmålet.

For å få etablert sikkerhet for at en signatur er korrekt, kan man søke hjelp hos en tredjepart (av og til flere, kanskje med litt ulike roller), som kan *bekrefte* at en bestemt offentlig nøkkel faktisk hører til en bestemt person, som altså har den tilhørende hemmelige nøkkelen i nøkkelparet. Dette forutsetter at tredjeparten kontrollerer og/eller går god for at en person er rette vedkommende (entydig navn), for eksempel ved personlig møte hvor det er fremvist akseptabelt identifikasjonsbevis. På grunnlag av dette utsteder eller lager tredjeparten de to nøklene som må til for å få til den aktuelle kommunikasjonen (krypteringen og/eller signeringen). Samtidig lages det en erklæring fra utstederen som bekrefter at *den bestemte offentlige nøkkelen hører til den identifiserte personen*. Det er denne bekreftelsen som kalles ”offentlig nøkkelsertifikat”.

Vi får altså et sertifikat eller en bekreftelse på en sammenheng, som sannsynliggjør at vi har med rett person å gjøre, i hvert fall hvis tredjeparten er til å stole på. Dette siste er et kapittel for seg, som vi ikke kan gå inn på her. I NOU 2001:10 Uten penn og blekk er det sagt mer om det, se blant annet kapitel 3.2.5. Hvilket grunnlag man har for å stole på en sertifikatutsteder og de sertifikatene som utstedes, vil variere i mange sammenhenger, ut fra ulike sikkerhetsbehov og hva som tilbys på markedet.

3 Lov om elektronisk signatur og kvalifiserte sertifikater

I Norge fikk vi i 2001 en lov om elektronisk signatur[3], som i hovedsak gir regler nettopp om sertifikatutstedere i signatursammenheng, og det loven kaller kvalifiserte elektroniske *signaturer* og sertifikater. Det er opp til de utstederne som finnes på markedet om man vil kalle sine sertifikater for *kvalifiserte*. Men *hvis* man gjør det, er det en *plikt* å følge loven med forskrifter. Da kommer sertifikatutstederen inn under et regime som skal gjøre det trygt for brukerne å kjøpe tjenester og produkter fra utstederen. Reglene i Norge er i overensstemmelse med et EU-direktiv om dette, slik at det er felles, harmoniserte regler i hele EØS-området, til glede blant annet for alle som skal kommunisere på tvers av disse landegrensene.

Loven pålegger med andre ord ikke at elektroniske signaturer skal brukes i bestemte sammenhenger, - den tilrettelegger for bruk, og stiller i hovedsak både brukere og leverandører fritt med hensyn til om de vil følge reglene eller ikke. For brukere gir loven som nevnt en ekstra "forbrukertrygghet", ved bruk av tjenester og produkter fra leverandører som har innrettet seg etter det kvalitets- og sikkerhetsnivået som loven legger opp til.

Det gjenstår imidlertid å se om de relativt få markedsaktørene på dette smale området vil finne det attraktivt å kalle sine sertifikater for kvalifiserte og dermed underlegge seg de aktuelle reglene om blant annet erstatningsansvar, kvalitetssikring av egen organisasjon og produksjon, mv. Hvis det er penger å tjene på et marked som etterspør slike løsninger, blir det selvfølgelig attraktivt. Så vidt vi vet er det bare ett firma i Norge som pr i dag (høsten 2002) kan levere kvalifiserte løsninger.

Loven om elektronisk signatur har imidlertid *to* paragrafer som gir regler som gjelder *alle* signaturer med sertifikater, enten de er kvalifiserte eller ikke. Disse gjelder følgelig også i plan- og byggesaksbehandling, hvis man tar slike signaturer i bruk. Først må vi nevne en hovedregel om kvalifiserte elektroniske signaturer, for deretter å komme frem til de ikke-kvalifiserte, i forhold til spørsmålet om de faktisk har noen rettsvirkning.

I korthet slår reglene fast at kvalifiserte signaturer *alltid* skal anses å tilfredsstille eventuelle krav i lover og annet regelverk om underskrift, men også ikke-kvalifiserte signaturer *kan* oppfylle krav om rettslig gyldighet (jf § 6), dessuten at enhver sertifikatutsteder må følge grunnleggende viktige personvernregler (gitt i § 7), og at Datatilsynet er tilsynsorgan for at reglene i § 7 overholdes. I denne paragrafen bestemmes blant annet at en sertifikatutsteder bare får innhente personopplysninger direkte fra den det gjelder, eller med uttrykkelig samtykke, og at slike opplysninger bare må brukes hvis det er absolutt

[3] Finn loven her: http://www.lovdata.no/all/nl-20010615-081.html

nødvendig i forbindelse med sertifikatet (som altså bekrefter at en bestemt offentlig nøkkel tilhører en bestemt person, virksomhet, eller lignende). Datatilsynet forvalter og fører naturlig nok tilsyn med personopplysningsloven med forskrifter, som også gjelder på plan- og byggesaksområdet, men de nevnte reglene i § 7 er spesielt rettet inn mot virksomheten til alle sertifikatutstedere, enten sertifikatene kalles kvalifisert eller ikke. Dermed får §§ 6 og 7 i loven om elektronisk signatur et virkeområde som er betydelig større på disse to punktene, mens virkeområdet for resten av loven er begrenset til utstedere av kvalifiserte sertifikater.

Hvis det i fremtiden viser seg at utviklingen skjer mest på det såkalte ikke-kvalifiserte nivået, vil loven om elektronisk signatur få mindre direkte virkning. På den annen side er det lite ved loven som hindrer markedet i å velge andre og eventuelt enklere løsninger, innenfor rammene av de to generelle §§ 6 og 7. I en tidlig fase av utviklingen for elektroniske signaturer vil det ikke være unaturlig om både forvaltningen og privat sektor, og de få sertifikatutstederne, prøver seg frem med forholdsvis enklere løsninger til mer erfaring er vunnet. Dette vil vi anta er det mest aktuelle også for det meste innenfor plan- og byggesaksbehandling, med mindre man vurderer fordelene ved kvalifiserte løsninger som så vidt store at de veier tyngre enn eventuelle ulemper, i en tidlig fase av utviklingen på dette området. Hva som nærmere ligger i kravene til kvalifiserte elektroniske signaturer fremgår av loven, samt de til enhver tid aktuelle standarder som finnes på dette området. Foreløpig finnes det en rekke ulike nyutviklete standarder som kan tas i bruk, men det vil nok ta litt tid før markedet har laget produkter i samsvar med standardene.

Uansett hvordan dette utvikler seg, vil forskriften om elektronisk kommunikasjon med og i forvaltningen[4] gi regler på selvstendig grunnlag, på en måte uavhengig av loven om elektroniske signaturer (selv om den er hjemlet i denne loven, samt i forvaltningsloven).

I loven om elektronisk signatur er det mest generelle og (antatt) teknologiuavhengige begrepet brukt (altså elektronisk signatur), men det er relativt klart at det er den mer presise teknologien eller mekanismen kalt digital signatur som ligger bak loven, og dessuten direktivet fra EU, som den bygger på. Dette gjelder for det loven kaller avansert elektronisk signatur, som forskriften om elektronisk kommunikasjon også omfatter (jf identiske definisjoner). De to omtalte paragrafene med større virkeområde omfatter også andre elektroniske signaturer, som ikke bygger på digitale signaturer. Begrepet elektronisk signatur kan omfatte:

- Digital signatur,
- Biometrisk baserte teknikker med for eksempel øye/iris-gjenkjenning og fingeravtrykk,
- PIN-koder.

[4] Finn forkriften her: http://www.lovdata.no/for/sf/aa/aa-20020628-0656.html

På neste side følger en illustrasjon av sentrale begreper i loven om elektronisk signatur. Begrepene *elektronisk signatur* og *avansert elektronisk signatur* brukes også i forskriften om elektronisk kommunikasjon med og i forvaltningen, men begrepet *kvalifisert elektronisk signatur* brukes bare i loven. Statskonsult har på oppdrag fra Arbeids- og administrasjonsdepartementet laget en veiledning eller kommentar til forskriften, som er tilgjengelig på Statskonsults nettside.[5]

I forskriften om elektronisk kommunikasjon brukes disse definisjonene (§ 2):
"elektronisk signatur: data i elektronisk form som er knyttet til andre elektroniske data og som fungerer som autentiseringsmetode,
avansert elektronisk signatur: en elektronisk signatur som:

a. er 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,"

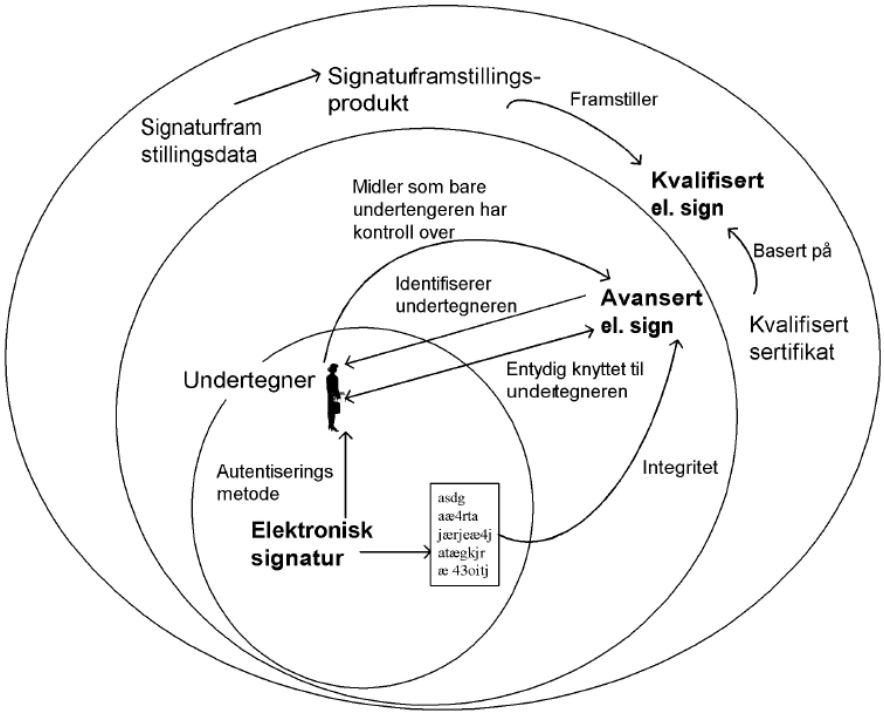
Definisjonen av elektronisk signatur her er lik/tilnærmet lik den som brukes i lov om elektronisk signatur. Merk kravet om å bruke dataene/nøklene som *autentiseringsmetode*. Det vil si som metode for å bekrefte at oppgitt identitet på person, virksomhet eller annen enhet, faktisk stemmer. Det er med andre ord dette som er kjernen i bruken av elektronisk signatur.

Definisjonen av *avansert elektronisk signatur* bygger på den første definisjonen, men legger på flere, opptrappende krav. Definisjonen er identisk med tilsvarende i lov om elektronisk signatur (§3 nr 2). Dette er i praksis en beskrivelse av krav som nettopp teknikken kalt *digital signatur* (med infrastruktur) kan tilfredsstille. Den innebærer en høyere grad av sikkerhet enn den vanlige, elektroniske signaturen, med ivaretakelse av de funksjonene som nevnes i bokstavene a – d i § 2 nr 2.

Se figuren nedenfor for en illustrasjon av økende krav i forholdet mellom "vanlig" elektronisk signatur, avansert elektronisk signatur og kvalifisert elektronisk signatur. Begrepene som brukes er definert i loven, og er nærmere kommentert i den nevnte veiledningen, se forrige fotnote.

[5] I veiledningen kan man bl.a. se nærmere om forståelsen av begrepene i forskriftens kapittel 2 om definisjoner
http://www.statskonsult.no/prosjekt/Veiledningtileforskrift/kapittel_1/p2/p2.htm

Illustrasjon til lov om
elektronisk signatur
17.9.02 ABS



4 Hovedtrekk i forskriften om elektronisk kommunikasjon med og i forvaltningen

Forskriften er som nevnt hjemlet i en ny § 15a i forvaltningsloven, og i lov om elektronisk signatur § 5. Det er imidlertid (foreløpig) ikke foreslått å stille særskilte krav til kvalifiserte elektroniske signaturer, eller bruk av slike, ved kommunikasjon med og i offentlig sektor, slik det er adgang til etter lov om elektronisk signatur § 5.

En veiledning til forskriften er lagt ut på Statskonsults nettsider, som nevnt foran på oppdrag fra Arbeids- og administrasjonsdepartementet. Forskriften er vedtatt for to års levetid, og vil automatisk utgå på dato (1.7.04) hvis den ikke uttrykkelig fornyes. Denne "solnedgangsregelen" er en understrekning av at departementet alvorlig vil vurdere hvordan forskriften virker i praksis, og fange opp eventuelle endringsbehov. Om det så blir fornyelse eller opphør, vil tiden vise. Reaksjoner til forskriften (og veiledningen) vil derfor være verdifulle, ikke minst fra et konkret område som plan- og byggesaksbehandling, som gjennom blant annet ByggSøk-prosjektet vinner verdifull erfaring fra elektronisk saksbehandling og kommunikasjon som angår hele landet. Statskonsult oppfordrer ByggSøk til å gi sine reaksjoner, på godt og vondt, til hvordan forskriftens ulike regler oppleves. Utviklingen på området for elektroniske forvaltningsløsninger går fort, og ByggSøk-prosjektet kan eventuelt bidra positivt til den videre utviklingen av forskriften på dette området.

4.1 Forskriftens formål og anvendelsesområde

Forskriften gjelder for elektronisk kommunikasjon mellom forvaltningen og publikum og for elektronisk saksbehandling og kommunikasjon i forvaltningen (§ 1 nr. 2). Forskriften gjelder derimot ikke elektronisk kommunikasjon mellom private parter (for eksempel to naboer, i forbindelse med nabovarsel). Hele forvaltningen omfattes; stat, fylkeskommuner og kommuner. Forskriften gjelder med andre ord også i forhold til plan- og byggesaker, i tillegg til andre regler, eksempelvis forvaltningsloven og personopplysningsloven.

4.2 Alminnelige regler om elektronisk saksbehandling og tilrettelegging for elektronisk kommunikasjon

Innenfor rammen av relevant sektorlovgivning, plan- og byggesakslovgivningen, får det enkelte forvaltningsorgan/den enkelte kommune stor grad av frihet til selv å velge i hvilken grad, og eventuelt hvordan, de vil legge til rette for elektronisk kommunikasjon. Publikum som vil kommunisere elektronisk med forvaltningen/kommunen må etter reglene benytte den fremgangsmåten som forvaltningsorganet har tilrettelagt for eller gitt anvisning på, f.eks. at all

kommunikasjon i forbindelse med et forvaltningsområde skal foregå via en eller flere bestemte nettsider, jf. § 4.

Henvendelser som ikke er underlagt spesielle krav til form eller fremgangsmåte i, eller i medhold av, lov eller forskrift, og som forvaltningsorganet heller ikke har stilt andre krav til, f.eks. ved å kreve bruk av en særskilt papirblankett eller angitt en spesiell nettside, kan rettes til forvaltningsorganets generelle elektroniske adresse, jf. § 3. Dette kan være en nettside for alminnelige henvendelser til organet eller en e-postadresse.

Det enkelte forvaltningsorgan kan stille krav om at bestemte sikkerhetstjenester skal benyttes hvis det kommuniseres elektronisk med forvaltningsorganet. Slike krav kan fastsettes individuelt eller generelt, f.eks. for et forvaltningsområde (plan- og byggesaker) eller for en eller flere bestemte typer saker (nabovarsel) eller henvendelser (taushetsbelagte opplysninger, eller sensitive personopplysninger). Valg av sikkerhetstjenester skal være i henhold til organets sikkerhetsstrategi, jf. om § 11 nedenfor. På områder der det finnes krav til form eller fremgangsmåte som kan oppfylles ved hjelp av elektronisk kommunikasjon, har forvaltningsorganet en plikt etter reglene til å gi anvisning på hvilken fremgangsmåte og hvilke sikkerhetstjenester som kan eller skal benyttes for å oppfylle kravene, jf. § 4 nr. 5. Et eksempel kan være at loven krever at det skal benyttes en "… betryggende metode som autentiserer avsender …" e.l., jf. Ot.prp. nr. 108 (2000-2001) om fjerning av juridiske hinder mv, jf. e-regelprosjektet.

Forskriften inneholder videre bestemmelser om behandlingsmåten for henvendelser som ikke tilfredsstiller de krav som er stilt i eller i medhold av forskriften (§ 6), om betingelsene for når og hvordan underretning om vedtak og forhåndsvarsling kan skje i elektronisk form (§ 7), samt bestemmelser om bruk av elektronisk kommunikasjon i forbindelse med klage over enkeltvedtak (§ 8), innsyn i opplysninger og dokumenter (§ 9) og høring av forskrifter mv.(§ 10). Det er også gitt bestemmelser om arkivering av avansert elektronisk signatur og andre autentiseringsmekanismer (§ 26).

Det er tatt inn et krav om at forvaltningsorgan som mottar henvendelser i elektronisk form skal gi *bekreftelse* til avsender om at en henvendelse er mottatt (§ 5). Bestemmelsen er tatt inn for å unngå usikkerhet hos publikum med hensyn til hvorvidt en henvendelse er mottatt eller ikke og for å forebygge uheldige virkninger av tekniske eller andre feil som måtte føre til at en melding ikke kommer frem som forutsatt.

Det er også tatt inn en ny bestemmelse om oppbevaring og utlevering av sertifikater og bekreftede meldinger mv.(§ 27). Bestemmelsen innebærer at publikum, i forbindelse med en begjæring om innsyn i dokumenter som er signert med avansert elektronisk signatur, ikke skal kunne avspises med tilgang til dokumentets innhold, men også skal få tilgang til sertifikater og andre opplysninger som er nødvendige for verifisering av signaturen dersom den som begjærer innsyn ber om det.

Forvaltningsorganet skal også sørge for at publikum om nødvendig kan få tilgang til dokumentenes innhold i en annen form som gjør det mulig å dokumentere innholdet også overfor tredjepart. Dette kan f.eks. være i form av en elektronisk melding som er signert av forvaltningsorganets arkiv, etter at den er bekreftet og konvertert i henhold til forskriftens § 26, eller i form av en bekreftet papirutskrift dersom tredjepart f.eks. ikke kan behandle en signert elektronisk melding.

4.3 Krav til utarbeiding av sikkerhetsstrategi og koordinering av forvaltningens sikkerhetstjenester

Forvaltningsorgan som benytter eller ønsker å benytte sikkerhetstjenester for elektronisk kommunikasjon i sin saksbehandling skal utarbeide en strategi for informasjonssikkerhet i virksomheten ("sikkerhetsstrategi"), jf. § 11. Sikkerhetsstrategien vil være grunnlaget for blant annet krav til bruk av sikkerhetstjenester i henhold til § 4. Sikkerhetsstrategien skal utarbeides i henhold til anerkjente prinsipper for informasjonssystemers sikkerhet, eksempelvis relevante norske standarder på området (jf NS-ISO/IEC 17799 Utgave 1, 2001 Informasjonsteknologi - Administrasjon av informasjonssikkerhet). Det er i bestemmelsen angitt en del forhold som sikkerhetsstrategien skal inneholde.

Det er gitt hjemmel i forskriften til å utpeke et organ med koordineringsansvar for forvaltningens bruk av sikkerhetstjenester for elektronisk kommunikasjon, jf. § 28. Dette er ikke gjort ennå (høsten 2002). Organet skal utarbeide krav til løsninger som anses hensiktsmessige for forvaltningens bruk av elektronisk kommunikasjon i ulike situasjoner og på ulike områder. Koordineringsorganet skal også vurdere hvorvidt sikkerhetsløsninger som er tilgjengelige i markedet tilfredsstiller de krav organet har stilt. Hensikten er å sikre samvirke mellom løsninger i ulike forvaltningsorgan og å lette anskaffelsesprosessen for det enkelte organ ved å gjøre krav og vurderinger tilgjengelige. Hensikten er også å sikre forvaltningsorganene fleksibilitet og utvikling i markedet ved at det kan velges mellom ulike løsninger. Koordineringsorganet kan også iverksette andre koordinerende tiltak.

4.4 Anskaffelse og bruk av tjenester for sikring av autentisering, ikke-benekting, integritet og konfidensialitet

Forskriften inneholder videre bestemmelser om bruk av sertifikat som identifiserer forvaltningsorgan og ikke den enkelte saksbehandler ("virksomhetssertifikat") (§§ 12 og 13), om anskaffelse av utstyr og data til ansatte for bruk av sikkerhetstjenester (§ 24), om veiledning av ansatte og publikum (§§ 17 og 20), om restriksjoner på bruk av sertifikat mv.(§ 14), om krav til oppbevaring og bruk av signaturfremstillingsdata og dekrypteringsdata mv.(§ 15) samt varslingsplikt ved tap eller mistanke om misbruk av slike data (§ 16).

Det er tatt inn en bestemmelse om adgang til å hindre bruk av sertifikat mv. i forvaltningssammenheng dersom en person misbruker sine signaturfremstillingsdata eller adgangen til å kommunisere elektronisk med forvaltningen (§ 19). Det er også tatt inn bestemmelser om innholdskryptering mv. (§§ 21 til 23).

Det er kommet til en bestemmelse om krav til kontroll av sertifikater og tilbaketrekkingslister (§ 18). Bestemmelsen gjelder på områder der det er krav om bruk av avansert elektronisk signatur. Der det måtte finnes et slikt krav i lovgivningen, eller der et slikt krav er fastsatt av forvaltningsorganet, antas det å være et reelt behov for å oppnå den sikkerhet som en avansert elektronisk signatur kan gi. Det er derfor stilt krav til kontroll om at signaturen kan verifiseres, at sertifikatet er egnet for den aktuelle anvendelse og at det er utstedt av en sertifikatutsteder som er anerkjent av koordineringsorganet eller kan aksepteres i henhold til forvaltningsorganets sikkerhetsstrategi.

Det skal også kontrolleres at relevante sertifikater fortsatt er gyldige og ikke trukket tilbake. Hvor oppdaterte opplysningene om sertifikatets status bør være kan variere fra område til område, men skal fremgå av forvaltningsorganets sikkerhetsstrategi, f.eks. om det skal sendes forespørsel til sertifikatutsteder om oppdaterte opplysninger ved hver verifisering, eller om det kan benyttes tilbaketrekkingslister som oppdateres f.eks. daglig.

For henvendelser der det er benyttet annen sikkerhetsteknikk enn avansert elektronisk signatur, må nødvendige kontroller vurderes i forhold til sikkerhetsbehovet på det aktuelle området. Dette bør fremgå av forvaltningsorganets sikkerhetsstrategi.

5 Hva kreves generelt i henhold til personopplysningslov og -forskrift?

Fra 1. januar 2001 trådte en ny lov og forskrift om behandling av personopplysninger i kraft, med bakgrunn blant annet i EU's personverndirektiv fra 1995. Reglene skal bidra til å beskytte mot krenkelse av personvernet, ved at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, som loven sier omfatter blant annet personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger. Personopplysninger defineres som opplysninger og vurderinger som kan knyttes til en enkeltperson. En del av opplysningene i forbindelse med plan- og byggesaksbehandling kan nok knyttes til enkeltperson/tiltakshaver, og området omfattes også av personvernreglene.

Den nye loven går i hovedsak bort fra fokus på konsesjon (bortsett fra for sensitive opplysninger) og over til et system med plikt for de behandlingsansvarlige til å sende melding til Datatilsynet om hva slags behandling av personopplysninger man vil ha, *før* man starter å behandle slike opplysninger.

Reglene slår fast at personopplysninger bare kan behandles hvis den opplysningene gjelder enten har samtykket, eller det er gitt adgang ved lov, eller det er nødvendig av andre grunner (som nevnes uttrykkelig og punktvis i lovens § 8). Ved byggesaksbehandling må plan- og byggesakslovgivningen anses å gi adgang til i utgangspunktet å innhente og behandle de personopplysningene som er nødvendige for saksbehandlingen i henhold til loven, men personvernets regler utfyller, ikke minst i forhold til hvordan personopplysningene skal behandles.

Samtykke krever at den registrerte "frivillig, uttrykkelig og informert" i en erklæring godtar behandling av opplysninger om seg selv.

Særlover kan gi eget lovgrunnlag for å behandle personopplysninger. Særlover kan også gi regler som er overlappende med personopplysningslovens, av og til med henvisning til hvilke av personopplysningslovens regler som uttrykkelig skal gjelde i tillegg til særlovens, eller at særloven slår fast at personopplysningsloven gjelder som utfyllende regler til særloven, så langt det passer.

Det personopplysningsloven nevner (i § 8) som nødvendige grunner for å behandle personopplysninger er blant annet et behov for å oppfylle en avtale med den som registreres, eller for å ivareta vitale interesser for vedkommende, for at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse, for å ivareta oppgaver av allmenn interesse, eller utøve offentlig myndighet. De nevnte vilkårene gjelder all behandling av personopplysninger (jf § 8).

I tillegg kommer mer detaljerte regler for behandling av sensitive personopplysninger (jf § 9). Hva som er sensitive opplysninger fremgår av § 2, nr 8, og omfatter blant annet opplysninger om rase, politisk eller religiøs oppfatning, opplysninger om straffbare forhold, opplysninger om helseforhold, seksuelle

forhold eller medlemskap i fagforeninger. Disse opplysningstypene er neppe særlig aktuelle i forbindelse med plan- og byggesaker.

Det slås fast visse grunnkrav (jf § 11), som den behandlingsansvarlige må oppfylle. En behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysninger, og hvilke hjelpemidler som skal brukes. Behandlingen må for det første være tillatt etter §§ 8 og 9, dessuten må opplysningene bare brukes i forhold til uttrykkelig angitte formål som er saklig begrunnet, ikke brukes senere til formål som er uforenlig med det opprinnelige formålet (med mindre samtykke innhentes). Opplysningene må videre være tilstrekkelige, relevante, korrekte og oppdatert, og ikke lagres lenger enn det som er nødvendig ut fra formålet.

Ved innsamling av personopplysninger fra den registrerte eller andre, ved bruk av personprofiler og ved automatiserte avgjørelser, foreligger det informasjonsplikt om en rekke forhold, samt innsynsrett for den registrerte.

Det er gitt egne regler for bruk av fødselsnummer (§12), for informasjonssikkerhet (§13) og for internkontroll (§14). For informasjonssikkerhet skal den behandlingsansvarlige og databehandleren sørge for det som kalles "tilfredsstillende informasjonssikkerhet". Dette skal oppnås ved planlagte og systematiske tiltak for å sikre konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Både de aktuelle informasjonssystem og sikkerhetstiltak skal dokumenteres, og dokumentasjonen skal være tilgjengelig for medarbeidere, Datatilsynet og Personvernnemda. Det skal også påses at andre som får tilgang til personopplysningene i forbindelse med saksbehandlingen, oppfyller kravene til tilfredsstillende informasjonssikkerhet.

Ved bruk av elektroniske "hjelpemidler", gjelder i tillegg egne regler i kapittel 2 i personvernforskriften, hvis det er nødvendig å sikre konfidensialitet, tilgjengelighet og integritet for opplysningene for å hindre fare for tap av liv og helse, økonomisk tap, eller tap av anseelse og personlig integritet (§ 2-1). En sentral regel er at den behandlingsansvarlige må gjennomføre en risikovurdering knyttet til behandlingen av personopplysningene, avstemme risikoen i forhold til et sikkerhetsnivå for akseptabel risiko som den behandlingsansvarlige selv har fastsatt på forhånd, samt iverksette nødvendige sikkerhetstiltak. Alt dette skal skje *før* behandlingen av personopplysninger settes i gang.

Sikkerhetsbestemmelsene angir krav til det styringssystemet den enkelte behandlingsansvarlige må etablere for å oppnå tilfredsstillende informasjonssikkerhet. Et viktig element i dette systemet er kravet om sikkerhetsledelse, som innebærer blant blant annet. en plikt til å utarbeide sikkerhetsmål og –strategi, samt ha jevnlige revurderinger av disse ved gjennomganger fra ledelsens side og ved sikkerhetsrevisjoner.

Det stilles krav egnet til organisering, personell, taushetsplikt, fysisk sikring og sikring av konfidensialitet, tilgjengelighet og integritet. Dessuten til sikkerhet hos andre virksomheter, ved at den behandlingsansvarlige bare kan overføre personopplysninger elektronisk til den/de kommunikasjonspartner og andre som tilfredsstiller kravene i forskriften.

I forhold til sikring mot uautorisert innsyn slås det fast i § 2-11 at det er et krav til kryptering eller sikring på annen måte, hvis overføring skjer ved hjelp av medium som er utenfor den behandlingsansvarliges fysiske kontroll, "når konfidensialitet er nødvendig". I denne forbindelse har Datatilsynet supplert med en anbefaling om en viss krypteringsstyrke, tilsvarende DES 128, nærmere omtale på www.datatilsynet.no, under temaet informasjonssikkerhet. Se også omtalen foran om symmetrisk og asymmetrisk krypto.

Det sentrale her blir å vurdere om det foreligger personopplysninger i plan- og byggesaksbehandlingen som faller inn under formuleringen i § 2-11, om når "konfidensialitet er nødvendig". Dette må vurderes og finnes ut av i forbindelse med, eller som et resultat av, den pålagte risikovurderingen som skal gjennomføres, se forskriftens § 2.4 Risikovurdering. Av denne fremgår det en plikt til å formulere et sikkerhetsmål, lage en sikkerhetsstrategi mv.

6 Kravet til underskrift i plan- og bygningslovgivningen

6.1 Plan- og bygningsloven § 93b

Plan- og bygningsloven (plbl.) § 93b krever at søknaden skal undertegnes av tiltakshaver og ansvarlig søker. Spørsmålet blir da om dette kan sies å være et formkrav som kan være til hinder for bruk av elektronisk signatur.

I bygningsloven av 18. juni 1965 nr 7 var det ikke oppstilt noe krav om underskrift. Derimot var det et krav om skriftlighet, se dennes § 94. Kravet til underskrift ser ut til å ha kommet med endringene i 1985, uten at vi har vært i stand til å finne noen begrunnelse for underskriftskravet. Heller ikke i forbindelse med lovendringene i 1995 har vi vært i stand til å identifisere noen begrunnelse for kravet om underskrift.

I forbindelse med alle departementenes gjennomgang av eget regelverk i det såkalte eRegelprosjektet[6] uttalte Kommunal- og regionaldepartementet at "KRDs generelle tolking er at "skriftlighet" og "signatur" må anses å være teknologinøytrale begreper, dvs valg av teknologiplattform i kommunikasjon mv ikke er avgjørende for gyldigheten av innholdet."[7] Regelforvalteren konkluderte med at i forhold til plan- og bygningsloven var dette et regelverk som allerede åpnet for elektronisk kommunikasjon. Vi legger derfor denne konklusjonen til grunn.

I juridisk teori har underskriften vanligvis vært knyttet til følgende funksjoner:

- Identifikasjon av utsteder av dokumentet; altså hvem underskriveren er,
- godtgjøre at opplysningene i dokumentet er gitt av underskriveren,
- indikasjon på endelighet; først når avtalen er ferdigforhandlet skal den underskrives, og
- vanskeliggjøre manipulering ved at en knytter underskriften til dokumentet sikrer seg mot senere forsøk på endring av dokumentet.

I tillegg kan kravet om underskrift sies å ha en varslingsfunksjon, ved at underskriveren varsles om at en, ved sin underskrift, bindes til rettshandelen.

Underskrift er også bundet til tradisjon og vane. Selv om det kanskje ikke eksisterer noe formelt krav om underskrift har man allikevel påført sin signatur.

En mer utførlig fremstilling om hensynene bak kravet om underskrift finnes i en prosjektrapport utgitt av Nærings- og handelsdepartementet kalt Kartlegging av

[6] www.dep.no/nhd/norsk/p10001272/eRegelprosjektet/index-b-n-a.html

[7] Se Ot.prp. nr. 108 (2000-2001) kapittel 12.2, side 165 annen spalte.

bestemmelser i lover, forskrifter og instrukser som kan hindre elektronisk kommunikasjon[8]

6.2 Hvilke hensyn kan tenkes å være relevante på plan- og bygningslovens side?

Identifikasjon av avsender vil finnes i feltoppsettet på de standardiserte skjemaene på en byggesøknad jf SAK[9] § 32a (NBR nr. 5174) slik at denne funksjonen trer i bakgrunnen i denne sammenheng. Likeså er egenskapen om indikasjon på endelighet heller ikke så fremtredende i forhold til et dokument som kun fremstilles av en part og med hans folk. Mer fremtredende er egenskapen om å vanskeliggjøre manipulering. Dette vil være viktig for både sender og mottaker av dokumentet. Likeledes vil varslingsfunksjonen om at underskriveren ved sin underskrift binder seg til de avgitte opplysningene i søknadsdokumentet være fremtredende. Dette fordi loven har regler om straffeansvar for forseelser etter loven og forskrifter[10] gitt i medhold av denne. Reaksjoner utenfor plan- og bygningsloven kan i noen tilfeller være aktuelle, f.eks. straffeloven § 166 om uriktige opplysninger og kapitlene 3 a (foretaksstraff) og 18 (dokumentfalsk). Av denne grunn vil det også være viktig å være rimelig sikker på å få verifisert identiteten til avsenderen(e) (autentisere) fordi søkeren(e) altså kan pådra seg straffeforfølgning.

6.3 Hva slags elektroniske sikkerhetsløsninger vil være aktuelle for å tilfredstille kravet til plbl. § 93b og SAK § 12?

Lov om elektronisk signatur[11] sier § 6, om rettsvirkningene av elektroniske signaturer, at kvalifisert elektronisk signatur vil "Dersom det i lov, forskrift eller på annen måte er oppstilt krav om underskrift for å få en bestemt rettsvirkning og disposisjonen kan gjennomføres elektronisk, oppfyller en kvalifisert elektronisk signatur alltid et slikt krav.

Dette betyr at når man anvender en kvalifisert elektronisk signatur for å signere en byggesøknad, vil dette alltid gi den ønskede rettsvirkning. De nærmere vilkår for at en elektronisk signatur kan kalles kvalifisert følger av loven om elektronisk signatur. Se for øvrig fremstillingen av dette ovenfor.

[8] http://odin.dep.no/nhd/norsk/publ/rapporter/024011-220007/index-dok000-b-n-a.html

[9] Forskrift 1997-01-22 34 om saksbehandling i byggesaker

[10] SAK, GOF 1997-01-22 35 om godkjenning av foretak for ansvarsrett, TEK 1997-01-22-33 Forskrift om krav til byggverk og produkter til byggverk

[11] lov 2001-06-15 81

Så vidt vi vet er det ennå ingen som tilbyr kvalifisert signatur i det norske markedet.[12]

Den andre setningen i bestemmelsen i § 6 sier: En elektronisk signatur som ikke er kvalifisert, kan oppfylle et slikt krav. ”

Setningen nøyer seg altså med å fastslå at andre typer elektroniske signaturer enn de kvalifiserte kan oppfylle et slikt krav. Dette vil bero på en konkret vurdering.

Elektroniske signaturer anses å være et meget vidtfavnende begrep. I forarbeidene til loven om elektronisk signatur sies det i spesialmotivene til § 3 nr 1. at : ”Elektronisk signatur skal omfatte alle former for elektroniske autentiseringsmetoder og er således et meget vidt begrep.”[13]

En PIN-kode kan altså anses som en elektronisk signatur etter loven. Om bruken av denne typen signatur kan oppnå den samme rettsvirkning som en håndskreven underskrift vil bygge på en konkret vurdering av den angjeldende sikkerhetsløsning. I siste instans vil det være domstolen som foretar denne vurderingen.

Norsk sivilprosess bygger på prinsippet om fri bevisføring og fri bevisvurdering. Dette innebærer at partene kan føre ethvert bevis de finner hensiktsmessig og at dommeren etter en samvittighetsfull prøvelse av hele saken avgjør hvilket faktum, som ut fra en sannsynlighetsvurdering, skal legges til grunn for pådømmelsen. Domstolen skal i en sivil sak legge til grunn det faktum som fremstår som mest sannsynlig.[14]

I en straffesak øker beviskravene. Ved tvil om faktum, for eksempel om hvilke typer opplysninger som er avgitt og det er faktisk tvil om dette, skal denne tvilen komme tiltalte til gode.

Med utgangspunkt i prinsippet om fri bevisføring kan også elektroniske dokumenter og signaturer legges frem som bevis. Dette slås fast i Justisdepartementets brev. De anfører også at ”Vi antar at utskrifter av elektroniske dokumenter i kombinasjon med sakkyndige erklæringer om at det er anvendt tekniske metoder med høy bevisverdi, vil ha stor overbevisningskraft.” Dette vil også gjelde for elektroniske signaturer. Domstolen vil vurdere både de teknologiske, organisatoriske og de juridiske aspektene i den konkrete sak. Jo mer avansert teknologi og jo mer gjennomførte og sikre organisatoriske systemer for tilgang,

[12] Vi tar et forbehold om at firmaet ZebSign AS, eid av Telenor og Ergo Group muligens har registrert seg overfor Post- og teletilsynet som tilbyder av kvalifiserte elektroniske signaturer. Se her om krav om registrering i forskriften til lov om elektronisk signatur (FOR 2001-06-15 81) § 2.

[13] Ot.prp. nr.82, kap.15, side 48.

[14] Se mer om dette i Brev fra Justisdepartementet til Nærings- og handelsdepartementet 05.05.99, vedlagt som vedlegg 4 i Kartleggingsrapporten http://odin.dep.no/nhd/norsk/publ/rapporter/024011-220007/index-dok000-b-n-a.html. Brevet er også inntatt i Ot.prp. nr. 82 (1999-2000) Om lov om elektroniske signaturer, pkt. 8.10 side 37.

anvendelse og vedlikehold av sikkerhetsløsningene - herunder bruk av logger, jo høyere er sannsynligheten for at domstolen vil finne bevist hvilke opplysninger som er avgitt og hvem som har avgitt dem.

6.4 Hva slags teknologisk nivå er nødvendig for å kunne avgi en elektronisk byggesøknad med elektronisk signatur i forhold til plan- og bygningsloven § 93b og SAK § 12?

Noen av de sentrale hensynene bak underskrift er nevnt tidligere i dette notatet. Dette var hensynet til identifikasjon av underskriver/avsender og godtgjøring av at opplysningene var gitt av underskriveren. Videre skulle underskriften hindre manipulering av innholdet i dokumentet ved at en knytter sammen dokumentet og underskriften. Til sist nevnte vi at underskriveren varsles om at en, ved sin underskrift, bindes til det som uttrykkes i dokumentet, enten dette er en viljeserklæring, enkeltvedtak eller uttrykk for andre rettslig bindende utsagn.

Vi skal gjennomgå dette mer konkret, og gi eksempel på et teknisk og regulatorisk system som etter vår mening til sammen vil sikre at hensynet bak underskrift blir tilstrekkelig ivaretatt. Vi skal også antyde noe om hvor sterke krav som må stilles for å verifisere identiteten til avsenderen.

Med bruk av elektroniske skjemaer slik SAK § 32a gir adgang til, samt bestemmelsens mulighet til å kreve dette, vil en maskinelt kunne sikre at alle relevante opplysninger er fylt ut og at de vedleggene som man krysser av for, virkelig er vedlagt søknaden. NBR nr. 5174 har strukturert disse opplysningene på en god måte. Er inntastingen av opplysninger enten ufullstendig eller ikke komplett, kan et system gi melding tilbake om de korreksjoner som må gjøres.

I vanlige nettbankløsninger får man opp et skjermbilde hvor de inntastede opplysninger fremkommer og en blir bedt om å bekrefte, eventuelt korrigere de viste opplysningene. Dette er en måte å sikre at opplysningene blir registrert slik de var ment fra avgiver. Ved å måtte bekrefte at de avgitte opplysningene er korrekte, har en sikret sammenknytningen av en oppgitt identitet og de avgitte opplysninger.

En byggesøknad skal undertegnes av både ansvarlig søker og av tiltakshaver. Ansvarlig søker vil være kjent for bygningsmyndigheten gjennom den sentrale eller lokale godkjenningsordningen, jf GOF § 4 og kap. V. I systemer der avgiver av opplysningene er kjent for myndigheten er det ikke nødvendig med bruk av avansert PKI-teknologi. Det er her nok å vise til Skattedirektoratets (SKD) system for elektroniske selvangivelser og Toll- og avgiftsdirektoratets (TAD) TVINN system. SKD anvender en firesifret PIN-kode som er fortrykt på utsendelsen av den papirbaserte selvangivelsen den enkelte skatteyter mottar i posten. TAD benytter en 8-sifret kode som gis til den enkelte deklarant (importør, speditør mv) etter en prekvalifisering der både deklarantens utstyr og kunnskap om regelverket testes. Det er her grunn til å nevne at i forhold til begge

disse myndighetene er feilaktige eller manglende opplysninger straffesanksjonert.

Ved å knytte en unik identifikator til den enkelte registrerte i det sentrale/lokale godkjenningsregisteret, vil denne identifikatoren kunne benyttes i det elektroniske byggesøknadssystemet.

Den enkelte tiltakshaver vil vanligvis ikke være kjent for byggemyndigheten. Antakelig vil det være ansvarlig søker som forestår utfyllingen av søknaden og som da kan identifisere seg mot systemet med en unik identifikator. Personopplysninger om tiltakshaver, herunder elektronisk postadresse kan gis av ansvarlig søker. Slike systemer vil ved registrering for eksempel av en byggesak generere et saksnummer. Saksnummer samt eventuelt et engangspassord kan så formidles av systemet til tiltakshaver, som så skal identifisere seg overfor systemet og kontrollere/korrigere de relevante opplysninger. Først når tiltakshaver har registrert seg i systemet er søknaden komplett. Hvis vedkommende "tiltakshaver" mottar en oppfordring om dette, og mener at dette ikke er noe som angår ham, har han all grunn til å varsle bygningsmyndigheten om dette.

Plan- og bygningslovens system legger opp til at ansvar for opplysninger om et tiltak knyttes direkte opp mot hver enkelt aktør. Dette vil være et viktig incitament for at korrekte opplysninger gis av den enkelte aktør. Lovens system vil derfor etter vår oppfatning medvirke til at opplysningene som gis er korrekte.

Som en konklusjon mener vi at et teknisk system som beskrevet ovenfor og et gjennomtenkt samvirke med den eksisterende plan- og bygningslovgivingen er en av sikkert flere mulige løsninger som vil kunne oppfylle lovens krav til underskrift.

Et ytterligere moment vil være at de interne administrative og tekniske rutinene rundt systemet er tilfredstillende. Det vises her til beskrivelsen om sikkerhetsbestemmelsene i personopplysningsloven foran. Momenter som hvem som har tilgang til systemet, tilgang til å korrigere lagrede opplysninger, samt sikre aktivitetslogger er her relevante.

6.5 Plan- og bygningsloven §§ 94 og 95b Nabovarsel

I § 94 pkt 3. stilles det krav om at naboer og gjenboere skal varsles. Det nærmere kravet er at søknaden skal inneholde gjenparter av varselbrevene samt kvitteringer for at brevene er sendt. Etter praksis betyr dette kvitteringer for sending av rekommanderte brev eller der tiltakshaver eller en representant for denne oppsøker den enkelte nabo og ved dennes påtegning dokumenterer at varsel er mottatt. NBR nr. 5155 kan benyttes til dette. Ved delte søknader skal dette skje i forbindelse med søknad om rammetillatelse i følge Tyréns kommentarutgave til plan- og bygningsloven.

Alternativt til varsel er naboens skriftlige godkjennelse av tiltaket. Dette kan gjøres på det ovenfor nevnte NBR-skjema ved å krysse av i godkjennings-

rubrikken og undertegne. Dette er i alle tilfeller nødvendig i forbindelse med søknad om tillatelse til enkle tiltak etter § 95b.

Dette vil være mer problematisk å gjennomføre i et elektronisk system. Fortsatt vil det være mange som vil vegre seg for å måtte avgi erklæringer i elektronisk form. De er heller ikke lovpålagt å gjøre dette. Selvsagt kan de tilbys å aksessere bygningsmyndighetenes saksbehandlingssystem og bekrefte at de er varslet, eventuelt at de godkjenner tiltaket. Imidlertid vil dette ikke være nok hvis ikke alle naboer/gjenboere gjennomfører dette.

Alternativt kan tiltakshaver/ansvarlig søker anvende det tradisjonelle papirdokumentet og innhente kvitteringer om varsel eller godkjennelser på vanlig måte. Dokumentene kan så skannes og oversendes bygningsmyndigheten i elektronisk form. Lovens system hviler på at den enkelte søker er ansvarlig for opplysningens godhet. Det vises her også til Rt. 1962.105 som er gjengitt i Tyréns kommentarutgave til plan- og bygningsloven[15] side 360.

Det kan her være grunn til å vurdere en lovendring som ytterligere tydeliggjør tiltakshavers ansvar i forbindelse med uriktig eller manglende oppfyllelse av varslingsplikten overfor naboene.

[15] Carl Wilhelm Tyrén: Plan- og bygningsloven, 4. utgave Tano Aschehoug 2000.

7 Er det behov for å kryptere innholdet i dokumenter?

Spørsmålet om kryptering henger sammen med spørsmålet om det er behov for å ivareta konfidensialitet i hele eller deler av plan- og byggesaksbehandlingen. Det kommer an på hvilken type opplysninger som inngår i saksbehandlingen, og hvilke rettsregler som gjør seg gjeldende. Ved elektronisk behandling og kommunikasjon av opplysninger som skal beskyttes mot uvedkommendes innsyn (bevare opplysningenes konfidensialitet), kan kryptering være ett av flere relevante sikkerhetstiltak, og i spesielle tilfeller finnes det rettslig pålegg om det.

Vi begynner i den andre enden av skalaen, med offentlighetsloven, som slår fast at alle saksdokumenter i forvaltningen *skal* være offentlige, bortsett fra i de tilfellene hvor det er gjort unntak fra dette i lov eller i medhold av lov. Det er så vidt vi vet ikke gjort slike unntak i plan- og byggesakslovgivningen. Tvert i mot er det der pålegg om å drive aktiv opplysningsvirksomhet overfor offentligheten om planleggingsvirksomheten etter loven. I byggesaker gjelder de vanlige reglene i offentlighetsloven og i forvaltningsloven, samt reglene i personopplysningsloven, jf omtalen av personvernreglene foran.

Vi tror ikke det er grunn til å fremstille de vanlige reglene om offentlighet og partsoffentlighet for denne utredningens formål. Det er nok å vise til dem, og understreke at de gjelder fullt ut på området for plan- og byggesaker, inkludert plikten til å vurdere meroffentlighet, selv om et tilfelle *kan* unntas offentlighet.

Av generell taushetsplikt finner vi regler i straffeloven i §§ 90, 91, og 91a. Disse gjelder opplysninger som kan skade rikets sikkerhet hvis de blir kjent for uvedkommende, og dels politiske og personlige opplysninger som kan skade Norges interesser eller volde fare for enkeltpersoners liv, helse, helbred, frihet og eiendom. Disse bestemmelsene om taushetsplikt og straff retter seg mot alle. Slike opplysninger er vel imidlertid neppe ofte å se på plan- og byggesaksområdet.

Straffelovens § 121 retter seg mot alle som er ansatt i eller utfører tjenester eller arbeid for stat eller kommune. Paragrafen gjør det straffbart å krenke taushetsplikt som følger av lov eller gyldig instruks.

Dokumenter som kommer i kategorien ”unntatt offentlighet” etter offentlighetsloven, men som ikke er taushetsbelagte, kan sies å befinne seg i en gråsone mellom et potensielt, men vagt uttrykt konfidensialitetsbehov og et noe klarere sikkerhetsbehov knyttet til integritet og tilgjengelighet. Kryptering er neppe et nødvendig tiltak, men kan vurderes der det er mye om å gjøre.

I forvaltningslovens § 13 heter det at enhver som utfører tjeneste eller arbeid for et forvaltningsorgan, har plikt til å hindre at andre får adgang eller kjennskap til

det han i tjenesten eller arbeidet får vite om "noens personlige forhold" eller konkurranseutsatte opplysninger som en bedrift trenger å holde hemmelige.

Forvaltningsloven krever at "dokumenter og annet materiale som inneholder opplysninger undergitt taushetsplikt, skal forvaltningsorganet oppbevare på betryggende måte". Hva som faktisk er betryggende, sier ikke loven noe om. Den setter normen og retningen.

I statlig sektor er det gitt en konkret instruks for hva som anses som betryggende, beskyttelsesinstruksen[16]. Den gir, sammen med sikkerhetslovens forskrift om informasjonssikkerhet, omfattende regler for hvordan taushetsplikten konkret skal ivaretas. Den statlige instruksen gjelder kun i staten, men sikkerhetsloven med forskrifter gjelder også kommunene. Dermed faller kommune-Norge utenfor deler av denne regelgivningen.

Skadevurderingen i beskyttelsesinstruksen er knyttet til hvorvidt det "vil kunne skade" eller "vil kunne forårsake betydelig skade for det offentliges interesser, en bedrift, institusjon eller enkeltperson" at dokumentets innhold blir kjent for uvedkommende. Dette utløser i så fall en plikt til å beskytte, slik reglene sier.

Etter ordlyden er det derfor naturlig å legge til grunn at alle dokumenter som er underlagt taushetspliktregler i staten i henhold til forvaltningsloven og tilsvarende lovverk, skal behandles etter reglene i beskyttelsesinstruksen.

Dersom en har behov for beskyttelse av både integritet og konfidensialitet, kan digital signatur kombineres med påfølgende kryptering av innholdet i dokumentet eller informasjonen (innholdskryptering). Valg av tjenester må gjøres ut fra den verdien informasjonen har og de truslene eller mulighetene vi står overfor.

Så vidt vi kan forstå er det *ikke behov* for å kryptere innholdet i plan- og byggesaker, ettersom de neppe inneholder opplysningstyper som er underlagt taushetsplikt. Hvis opplysningene skal følge hovedregelen om offentlighet i forvaltningen, som vi antar de generelt må, er det selvfølgelig heller ikke behov for kryptering for å skjule innholdet. Ved behov for å beskytte opplysningenes integritet, kan imidlertid kryptering være et tiltak å vurdere.

I forhold til personopplysninger og eventuelt behov for kryptering, viser vi til gjennomgangen over.

[16] FOR 1972-03-17 nr 3352: Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter. Se § 12, som sier at dokumenter gradert etter beskyttelsesinstruksen skal elektronisk behandles i samsvar med nærmere identifiserte regler i sikkerhetslovens forskrift om informasjonssikkerhet, og eventuelt følge reglene om dokumenter gradert BEGRENSET.

8 Typer av elektroniske signaturer

Her kommer en liste med sikkerhetsmekanismer og kjente sterke og svake sider ved dem. Den viser at det fins mange måter og nivåer å sikre signaturfunksjonalitet på.

8.1 Digital signatur med nøkkel og sertifikat i chip

Denne mekanismen gir som kjent best sikkerhet for identifisering, autentisering, integritet og uavviselighet. Den krever integrasjon med systemene på baksiden, en vel utbygd infrastruktur og store investeringer både for brukere og systemeier. En åpen PKI vil kreve ekstra mye. For å skaffe erfaringer uten å investere for mye, kan systemeier starte med en avgrenset brukergruppe, f.eks. større byggefirmaer, som vil bruke systemet mye og gi tilbakemeldinger. Systemet bør i så fall bare akseptere bestemte sertifikatutstedere og installasjoner bare på bestemte PC-konfigurasjoner.

8.2 Digitale signaturer med nøkler og sertifikater i PC

Denne mekanismen kan brukes for de samme tjenestene, men den gir vanligvis lavere sikkerhet. (MS lager noen sikrere mekanismer nå, men det kan tenkes at de har andre baksider.) Den er sannsynligvis lettere å installere hos brukerne. Systemeier må vurdere hvor vesentlig det er å hindre at familiemedlemmer eller kolleger (hvis det installeres på jobb) kan skaffe seg tilgang til søknaden.

8.3 PIN – koder

Disse brukes for eksempel til enkle selvangivelser. Det gir en sikkerhet for at noen på selvangivelsens adresse har tatt inn posten og sendt inn årets selvangivelse. Sannsynligvis er det lav risiko for at mange vil forfalske selvangivelsen til en i familien.

8.4 PIN/passord

I dag sender søknadssystemet i ByggSøk brukeridentitet og passord til den oppgitte e-postadressen. Om systemet vurderer om adressen er fornuftig eller om den aksepteres som ok uten å sjekke den, vet vi ikke. Ett alternativ er å sende passordet til en mobiltelefon med samme navn og adresse som søkeren. Det krever en tiltrodd tredjepart, for kommunen må i tilfelle sjekke hos Telenor at nummer og navn stemmer. Det koster penger og blir sikkert belastet brukeren. Et annet alternativ er å hente adressen hos folkeregisteret og sende passordet dit.

8.5 SSL (Secure Sockets Layer)

Kan gi konfidensiell overføring til kommunen. Men det gir ikke signatur i og med at kommunens tjener vanligvis ikke autentiserer avsender. Men det kan gjøres ved kombinasjon med andre tjenester, f.eks. PIN/passord. Konfidensialitet kan løses ved en signert sesjonsnøkkel, enten SSL eller standard digitale signaturer. Hvis det ikke er en sesjonsnøkkel, kan sikkerheten lett bli lav.

8.6 Andre ting å tenke på

De som bruker systemet, bør oppleve det og signeringen som *brukervennlig,* og at det letter og ikke hemmer arbeidet deres. Hvis det å signere er en større operasjon som man ikke husker fra gang til gang, vil mange brukere falle fra. PIN er greit hvis man husker den. SSL følger med de fleste PC-er, men autentiserer vanligvis ikke sluttbrukeren. Om digitale signaturer er brukervennlige, vil avhenge av om det er lett eller vanskelig å installere systemet, om man husker hvordan man får tak i signeringsnøkkelen fra gang til gang osv.

Systemeier må eventuelt vurdere *hvor stor del av søkerne* som skal bruke elektronisk søknadsskjema. Det er ofte slik at spesialtilfeller kan bli dyre og at det er mest økonomisk å behandle dem manuelt. Eksempler på slike søkere kan være utenlandske søkere, gamle mennesker som ikke er så flinke med PC, og som trenger ekstra tilrettelegging. Det kan også være slik at det lønner seg å starte med brukere som søker byggeløyve ofte, større firmaer, arkitekter, tømrere osv. Dersom borgere ikke kjenner språkbruken i byggesøknader, kan det kreve mye veiledning og veldig brukervennlige systemer. Hvis borgerne ikke skal bruke digitale signaturer til noe annet enn å søke ombygging hvert 20de år, så vil de sannsynligvis oppleve det som et unødvendig og for stort skritt å installere eller å kople sertifikatet til søknadssystemet til at de ser seg tjent med det. Dermed kan det bli store utgifter for kommunen med for få brukere.

Ved overgang til elektronisk verden kan det tenkes at *signaturene skal plasseres andre steder* i søknadsbehandlingen. Det kan f.eks. tenkes at det er mer vesentlig å få en signatur når det gis løyve for byggestart enn ved søknadsinnsending.

Supplerende lesning til denne utredningen kan være *Veiledning til forskrift om elektronisk kommunikasjon med og i forvaltningen*, som Statskonsult har skrevet på oppdrag fra Arbeids- og administrasjonsdepartementet. Veiledningen er bare publisert elektronisk, og finnes på denne nettsiden: http://www.statskonsult.no/prosjekt/Veiledningtileforskrift/index.htm . Selve forskriften som veiledningen er til, finnes på Lovdata: www.lovdata.no/for/sf/aa/aa-20020628-0656.html.

Til slutt nevner vi også en nettside med oversikt over noen standardiserings-organisasjoner og standarder, som også er aktuelle i forhold til spørsmål rundt elektronisk signatur/PKI, og NOSIP, som er en forvaltningsstandard for IT-kommunikasjon. NOSIP er et fundament for å lage en helhetlig og velfungerende IT-infrastruktur innenfor offentlig forvaltning, med relevante krav også for elektronisk signatur/ PKI. Se
http://www.statskonsult.no/prosjekt/standsekr/index.htm

REFERANSER

Tittel:	Elektronisk plan- og byggsaksbehandling og krav om signatur med videre i lover og forskrifter
Forfatter(e):	Amund Eriksen, Annikken B. Seip, og Halvor S. Oseid
Statskonsults notatnummer:	2002:8
Prosjektnummer:	816
Prosjektnavn:	Elektronisk plan- og byggsaksbehandling og krav om signatur med videre i lover og forskrifter
Prosjektleder:	Amund Eriksen
Oppdragsgiver(e):	Statens bygningstekniske etat
Resymé:	Utredningen går gjennom krav til signatur og konfidensialitet på plan- og byggesaksområdet, i forhold til elektronisk saksbehandling. Den gir generell oversikt over funksjoner som kan ivaretas ved signatur og konfidensialitet, rettslige utgangspunkter for dette, samt konkrete vurderinger av behovene i forhold til relevant regelverk.
Arbeidsområde:	☐ Styring og resultatorientering ☐ Omstilling og organisasjonsformer ☒ Informasjonsteknologi ☐ Kommunikasjonsutvikling ☐ Internasjonalisering ☐ Lederskapsutvikling
Emneord:	Signatur, konfidensialitet/offentlighet, elektronisk plan- og byggesaksbehandling, elektronisk signatur og kryptering.
Dato:	20.6.03
Sider:	33
Utgiver:	Statskonsult Postboks 8115 Dep 0032 OSLO