Statskonsultrapport 2003/14

Signaturkrav, risiko og elektroniske byggesøknader

Rapport om behovet for elektroniske signaturer i ByggSøk-systemet, skrevet på oppdrag fra Statens bygningstekniske etat

Forord

Er det i orden å sende inn byggesøknader elektronisk? Hva sier jussen? Hvilke egenskaper ved en signatur dekkes av ulike tekniske løsninger, og hvilke dekkes ikke? Hvilke risikoer er viktig å være klar over ved bruk av de forskjellige løsningene? Dette er spørsmål Statskonsult har prøvd å besvare gjennom denne rapporten.

Statskonsult ble i 2002 bedt av Statens bygningstekniske etat om å utrede behovet for elektronisk signatur og kryptering knyttet til elektroniske byggesøknader. Det elektroniske systemet for byggesøknader, ByggSøk, faller inn under regjeringens hovedprosjekter i eNorge-planen. Systemet er under utvikling, og skal legge til rette for at Internett blir et verktøy for å effektivisere den kommunale plan- og byggesaksbehandlingen.

Notatet er Statskonsults andre utredning for Statens bygningstekniske etat knyttet til bruk av elektroniske signaturer i det elektroniske systemet for byggesøknader, ByggSøk. Notatet viser at forskjellige typer elektroniske signaturer dekker regelverkets krav til underskrifter på til dels ulike måter, og at risikoen ved bruk av ulike løsninger varierer. Risikoene varierer også for systemets ulike brukere (interessenter). Målet med utredningen er å gi et bedre grunnlag for å velge type elektronisk signatur ved innsendelser av elektroniske byggesøknader.

Statskonsult står ansvarlig for det faglige innholdet i rapporten. Avdelingsdirektør Guri Verne i avdeling for informasjonsteknologi har vært prosjektansvarlig. Prosjektleder har vært Seniorrådgiver Amund Eriksen. Rapporten er skrevet av seniorrådgiverne Annikken Bonnevie Seip og Amund Eriksen. Arbeidet ble gjennomført fra november 2002 til februar 2003 og overlevert Statens bygningstekniske etat 6. mars. Denne rapporten, som ikke er en del av oppdraget, har fått noen bedre formuleringer uten at konklusjonene er endret.

Oslo, november 2003

Jon Blaalid
Direktør

Innhold

1 Sammendrag

Dette vil revolusjonere byggesøknader både for den som søker og for den som behandler. Så langt jeg kan se gir det en fantastisk oversikt på en veldig klar måte.
Førsteinntrykket fra en ansvarlig søker

ByggSøk er et elegant lite pilotsystem som hjelper søkerne med å fylle ut byggesøknader. Kommuner skal kunne ta i mot søknadsinformasjon elektronisk. Systemet klarer ikke å gi hjelp til fullstendig og korrekt informasjon for alle søknadstyper fordi mange søknader kan bli komplekse. Likevel er den elektroniske søknaden en meget god og effektiv hjelp for søkere, og som også avlaster saksbehandlerne i kommunene.

Regelverket stiller krav om underskrifter uten at det står i klartekst hva hensikten er med de ulike signaturene. Det kommer fram av intervjuene våre at regelforvalter og kommuner ønsker seg signaturer som uttrykk for at søkerne vedkjenner seg at de søker.

Det fins flere signeringsteknikker som kan dekke det vi kaller "ikke-benekting", dvs. at en søker ikke kan nekte å ha signert en søknad. De fleste teknikkene medfører enten å installere programvare for digital signatur med infrastruktur for å verifisere tilhørende digitale sertifikater, eller ved å benytte f.eks. en mobiltelefon i tillegg som sikkerhetsmekanisme. Alle varianter innenfor disse løsningene krever fungerende programvare for flere parter, god oppetid og kommunikasjon for infrastrukturen. ByggSøk er et system for allmennheten og profesjonelle utøvere. Men det er få som har nøkler og sertifikater til å lage digitale signaturer med foreløpig, og det er foreløpig få kommuner som kan behandle sertifikater og søknader elektronisk. Det er derfor ikke rimelig å anbefale at ByggSøk skal være drivkraften for åpen PKI og digitale signaturer. Men å vinne erfaring med ulike løsninger gjennom piloter, kan være fornuftig. Et alternativ kan være å lage tilgangskontroller som sikrer at alle signatarene (de som signerer) får tilgang til sin del av søknaden slik at de kan signere den. Det er en løsning som vil kreve en god del forståelse for hvordan signering kan foregå, mye tilgangslogikk og logging av det som foregår.

Vi har risikovurdert to elektroniske signaturløsninger, men vi anbefaler Statens bygningstekniske etat (BE) å overveie en enklere løsning for de nærmeste årene, nemlig den som Oslo kommune tester: Søknadene fylles ut og sendes elektronisk. Et ark skrives ut der alle signatarer kan påføre sin håndskreve underskrift og vedkjenne seg sin del av søknaden. Denne fakses kommunen og lagres elektronisk sammen med søknaden. Det oppstår få konflikter knyttet til signaturer, men i tilfelle en slik forekommer har samtlige underskrivere en kopi av søknaden, hvilket vil lette avklaringen av hva som har skjedd.

I tillegg til håndskrevet underskrift mener vi det vil være nødvendig å forbedre opplysningene til søkerne om hva de er med på når de knytter seg til en bestemt søknad. I søknaden bør det være meldinger eller felt av typen: 'Klikker du her betyr at du tar ansvar for at opplysningene er korrekte'. For å komme videre,

må man klikke i feltet. Gode veiledninger trengs uavhengig av hvilken signeringsmetode som benyttes.

For å opprettholde tilliten til ByggSøk, bør BE videreutvikle systemet ved å legge økt vekt på at dette skal skje systematisk og etter anerkjente systemutviklingsmetoder med inspeksjoner der jurister deltar. Det må utvikles en sikkerhetsstrategi og jevnlig foretas risikoanalyser, jfr. 3.6.4. Systemet må dokumenteres.

2 Mandat og mål for prosjektet

2.1 Mandat

Er det i orden å sende inn byggesøknader elektronisk? Hva sier jussen, og hva slags teknisk løsning kan brukes? Hvilken risiko foreligger? Dette er spørsmål Statskonsult har prøvd å besvare gjennom denne og en tidligere rapport. Rapportene er skrevet på bestilling fra Statens bygningstekniske etat (BE). Det er et mål for BE å ha en gjennomtenkt strategi for hvordan elektroniske byggesøknader kan oppfylle aktuelle rettslige krav og eventuelt ikke holde lavere sikkerhetsnivå enn det man har for søknader skrevet på papir, men på den annen side heller ikke et høyere og mer kostbart sikkerhetsnivå, med mindre dette er nødvendig ut fra juss og/eller risikovurderinger. Rapportene skal gi et bidrag til dette.

Statskonsult leverte den første rapporten 19.09.02 til Statens bygningstekniske etat (BE), om rettslige krav til signatur og kryptering i forhold til et av regjeringens hovedprosjekter i eNorge-planen: ByggSøk. Rapporten er publisert på ByggSøks nettside (http://byggsok.be.no/), ledsaget av denne teksten:

> ”Trenger vi digitale signaturer?
> For å kunne svare på dette trenger vi å vite hva en signatur er slik vi bruker den i dag, og slik den kan brukes i fremtiden. Derfor har vi bedt Statskonsult om en utredning om dette tema som alle snakker om, men som få kan noe om. Rapporten finner du her.”

Rapporten heter ”Elektronisk plan- og byggesaksbehandling og krav om signatur mv. i lover og forskrifter”, Statskonsult.

Metoden i den første rapporten var 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 ble tatt et generelt utgangspunkt, som plan- og byggesaksbehandlingen må forholde seg til. Det ble innledningsvis redegjort for hva en kan oppnå med elektroniske signaturer og innholdskryptering. Deretter fulgte en gjennomgang av noen utvalgte bestemmelser fra lov om elektronisk signatur, forskriften om elektronisk kommunikasjon med og i forvaltningen og personopplysningsloven med forskrift. Noen av hovedkravene til underskrift i plan- og bygningslovgivningen ble gjennomgått. I tillegg ble spørsmålet om behov for kryptering av innholdet i dokumenter vurdert (for å bevare konfidensialitet). Til slutt ble det gitt en oversikt over ulike typer av elektroniske signaturer. Denne rapporten er en oppfølging, basert på kontrakt oversendt i brev av 27.11.02 fra Statens bygningstekniske etat (BE) til Statskonsult. Den er skrevet av seniorrådgiver Annikken Seip og seniorrådgiver Amund Eriksen, og Eriksen var prosjektleder. I sluttfasen fikk vi noe bistand fra seniorrådgiver Kirsti Berg, Statskonsult og teknisk sjef Jon Ølnes, PKI Consulting Services[1].

[1] Vi diskuterte noen faktaopplysninger med Ølnes. Det har ikke påvirket innholdet og vurderingen i rapporten i noen retning. Vi har ikke funnet at det er i konflikt med at hans firma er aktør på markedet.

2.2 Mål for denne rapporten

Målet i denne rapport nr 2 er særlig å fokusere på risiko- og sårbarhetsvurdering av ByggSøks signaturtjenester/sikkerhetstjenester i forhold til de ulike rettsreglenes krav om signatur mv, samt krav om helhetlig sikkerhetstenkning hvis man tar elektronisk signatur eller andre sikkerhetstjenester i bruk, og når man har med personopplysninger å gjøre. Med sikkerhetstjenester i denne sammenhengen menes tjenester for autentisering, integritet og ikke-benekting. Begrepene er forklart i den første rapporten, og gjennomgås kort også nedenfor. ByggSøkprosjektet har utviklet et system for å fylle ut byggesøknader via Internett, hvor den ferdige søknaden enten kan skrives ut på papir og sendes på vanlig måte, eller sendes elektronisk til det økende antall kommuner som er i stand til å motta elektroniske søknader. Det er et mål i rapporten å gjennomgå krav til underskrift i plan- og bygningslovgivningen for å se hvordan underskriftskravet kan oppfylles i forbindelse med en elektronisk byggesøknad. I tillegg er det et mål å få frem relevante krav fra den nye lov om elektronisk signatur og den enda nyere forskriften om elektronisk kommunikasjon med og i forvaltningen, samt annet aktuelt regelverk.

Arbeidet skal bidra til å gi et (av flere) beslutningsgrunnlag for KRD til å velge en løsning basert på forslag fra BE.

2.3 Problemstillinger

2.3.1 Noen begreper

Begrepene nedenfor er relevante og sentrale som et grunnlag for problemstillingen i denne rapporten. De beskrives som mulige sikkerhetstjenester knyttet til datasystemer. Hva slags teknologi som benyttes for å realisere / ta tjenestene i bruk, kan variere. Ulike tekniske løsninger kan gi ulike grad av sikkerhet for å få realisert dem.

.

Autentisering er en sikkerhetstjeneste som skal sikre at opplysninger som identifiserer en enhet (person, maskin, system, nettside, prosess) virkelig stemmer. I forbindelse med utveksling av elektroniske meldinger vil bruk av autentisering sannsynliggjøre at avsenderen av en melding faktisk er den vedkommende gir seg ut for å være og dermed knytte avsenderen til meldingens innhold [1]. Behovet for autentisering varierer bla. ut fra saksbehandlingshensyn. I mange tilfeller vil det være ønskelig eller nødvendig å få etablert tilfredsstillende autentisering, f eks av hensyn til korrekt saksbehandling, personvern, økonomiske verdier, mv.

Integritet er en sikkerhetstjeneste som skal sørge for at informasjon ikke kan endres uautorisert under lagring eller transport uten at det oppdages. Hvis skade kan oppstå ved at innholdet i en melding blir endret, vil det være behov for å benytte en integritetstjeneste. Denne typen integritet for data, informasjon, melding eller dokument må ikke forveksles med informasjonens kvalitet, som er knyttet til riktigheten av de opplysninger som er formidlet. Informasjonens

integritet kan være i behold selv om opplysningene objektivt sett er uriktige, dersom det var disse opplysningene avsenderen faktisk sendte (”Shit in, shit out”) [1].

Ikke-benekting er en sikkerhetstjeneste som gir mottakeren av et dokument en rimelig grad av sikkerhet for at den angitte avsender ikke senere kan nekte å ha sendt dokumentet. Hvis avsenderen av et dokument har behov for å vite med en viss grad av trygghet at sendingen er mottatt, må imidlertid mottakeren ved en handling gi fra seg en kvittering for mottaket, slik at han eller hun ikke senere kan nekte å ha mottatt dokumentet.

2.3.2 Hovedspørsmål

I plan- og bygningslovgivningen finnes det flere krav om at byggesøknader skal skrives under av ulike aktører/roller, bl.a. tiltakshaver og ansvarlig søker. En sentral paragraf finner vi i plan- og bygningslovens §93b, nr 1, første avsnitt, der det heter at søknaden om byggetillatelse *skal undertegnes både av tiltakshaver og ansvarlig søker.* Også i forskriften om saksbehandling og kontroll i byggesaker (SAK), som utfyller loven, stilles det flere krav om underskrifter. Det er laget en rekke skjemaer for ulike typer søknader og erklæringer, som søkerne skal fylle ut og undertegne, for å ivareta kravene i regelverket.

Vi har funnet følgende spørsmål som vi mener er sentrale for denne undersøkelsen:

- Hvilken fleksibilitet gir regelverket mht. signering?
- Hvor høyt sikkerhetsnivå forventes det?
- Hvis reglene gir frihetsgrader, betyr det at flere teknologiske løsninger kan dekke behovet?
- Fins det andre verdier, f.eks. økonomi, brukervennlighet og tillit, som regelforvalter bør trekke inn for å bestemme akseptabelt risikonivå ved bruk av ByggSøk?
- Hva er det som kan være uønskete hendelser ved bruk av ByggSøk?
- Hvem løper hva slags risiko når systemet ikke virker etter hensikten?
- Hva slags signeringsteknikker vil gi akseptabelt risikonivå for systemet?

Tilgrensende problemstillinger mener vi kan være:

- Hva er det som kjennetegner denne spesielle saksbehandlingen som skal utføres elektronisk?
- Individuelle vs. kollektive goder.
- Hvilke av delene som utføres elektronisk vil gi størst effekt? Hvordan måle effekt?
- Måle ressursinnsats før og nå.
- Hvilken informasjon må være riktig?

2.3.3 Grunnlaget for å bestemme akseptabel risiko

Det er flere elementer som er med på å bestemme sikkerhetsnivået som er nødvendig i ByggSøk. Med dette mener vi hvilke verdier som en vurdering skal forholde seg til, slik at det blir en akseptabel administrasjon og håndtering av informasjon. Begreper som kommer inn er bl.a. brukernes tillit til systemet og til forvaltningens rolle. Det er også spørsmål om departementets, BE’s og

kommunenes tillit til systemet. Det er spørsmål om disse får den styringen og kontrollen med søknadene som de trenger. Hvem er det som løper risikoer, BE, kommuner og/eller brukere?

Det kan lett oppstå interessekonflikter mellom partene, f.eks.

- brukernes og forvaltningsorganenes verdsetting av tid,
- opplever ansvarlig søker at det er vanskeligere å bli overlatt til et elektronisk skjema framfor å spørre kommunen?
- osv.

Akseptabel risiko vil variere med funksjonaliteten for hver signatur. Risikoen skal i tillegg håndteres, dvs. BE må opprettholde interessentenes tillit til systemet også når truslene slår til. Dette innbefatter å ha løsninger for interessenter (de som har en eller annen nytte av ByggSøk) som opplever feilsituasjoner. Det fins situasjoner og områder der det er vanskelig å si noe om risikoen.

2.4 Avgrensning av arbeidet

Det eksisterer allerede et elektronisk system der søkere kan skrive inn og lagre sin informasjon. Vi har knyttet arbeidet vårt til regelverkets krav om signering og tilhørende behov som trenger sikkerhetsmekanismer for å få til et akseptabelt risikonivå.

Stortinget vedtok 13.1 2003 at *ansvarlig søker* har ansvar for å varsle naboer og håndtere eventuelle klager fra naboer. Nabohåndteringen blir dermed en prosess som ikke går via ByggSøk, og medfører at vi ikke har sett på elektronisk kommunikasjon med naboer. Vi har ikke gått inn på problemstillingene knyttet til å hente informasjon fra GAB.

En generell risikovurdering ser etter alle trusler og sårbarheter som kan hindre systemet å virke etter intensjonene. På den ene siden forventer vi at dét arbeidet er gjort og implementert. På den andre siden kan sikkerhetstjenester, som elektronisk signatur av et eller annet slag, introdusere nye huller i helheten. Derfor har vi til en viss grad vurdert svakheter ved hele systemet. I tillegg har vi forholdt oss til at teknologien løser signaturfunksjoner på en annen måte enn måten det gjøres på med papir.

Både risikovurderingene og nytte-kostnadsanalysene har tatt utgangspunkt i at vi bare kan indikere noe for de nærmeste årene. Hvis bruk av digitale signaturer og PKI har fått stor utbredelse om tre år, så kan vurderingene bli annerledes. Innenfor oppdragets tidsramme er vi kommet et stykke ned i problemstillingen, men opplever ikke at vi har krystallklare svar på alt. Det er imidlertid vårt håp at noen av vurderingene vi legger fram i rapporten, kan brukes av oppdragsgiver BE og andre til selv å komme dypere i materien.

2.5 Arbeidsmåte

Arbeidet ble en iterativ prosess. Følgende punkter ble gjennomgått flere ganger etter hvert som forståelsen for problemstillingen økte:

- Forstå målsettingen for ByggSøksystemet og hvor signaturfunksjoner er relevante.
- Identifisere relevante rettsregler for signaturer og andre sikkerhetsbehov knyttet til signatarene
- Vurdere disse så konkret som mulig i forhold til systemet og hvilken funksjonalitet hver enkelt skal dekke.
- Vurdere likheter og forskjeller mellom papirsøknader og elektroniske søknader
- Identifisere og vurdere signaturløsninger og tilknyttede rutiner
- Foreta risikovurdering av signaturfunksjoner
- Beskrive funn og vurdere anbefalinger.

I arbeidets gang intervjuet vi interessentene rundt byggesøknader og ByggSøk-systemet: BE, Kommunal- og regionaldepartementet (KRD), systemutvikleren av ByggSøk, de som drifter systemet, Oslo og Oppdal kommuner og en ansvarlig søker. Disse hjalp oss bl.a. med å identifisere risikoområder og forstå hva som kan være akseptabel risiko.

3 Dagens situasjon

Dagens situasjon danner basis for vurdering av behovet for sikkerhet i ByggSøk.

En papirsøknad med signatur kan sees som en transformasjon av et regelverk. Feltene som skal fylles ut i hver søknad, representerer enkelte rettslige normer og krav i plan- og bygningslovgivningen.

En elektronisk søknad er også en transformasjon av det samme regelverket. Det kan være en nyttig øvelse for noen å vurdere om feltene der representerer normene på samme vis. Samtidig er det slik at elektroniske søknader ofte bør se annerledes ut. De gir muligheter for tilpasninger basert på tidligere utfylling av felter (”hoppe over felter”), prosesseringen (”ferdigutfylling”), og validering underveis. Et elektronisk søknadssystem gir i ytterste konsekvens en program-messig implementering av normer og regelsett – noe som er en utfordring i seg selv (programmereren tolker regelverket istedenfor juristen?).

3.1 Generell rettslig bakgrunn

Den generelle rettslige bakgrunnen ble det gjort rede for i den første rapporten fra Statskonsult [17]. Av pedagogiske grunner gjentar vi noe av det her. I utgangspunktet er det pr 2003 i de fleste tilfeller rettslig akseptert at krav om *undertegning* og *skriftlighet* kan ivaretas like godt elektronisk som vi hittil har vært vant til på papir. Slik rettslig aksept har dels skjedd ved lovgjennomgang, og endringer i ca 39 aktuelle lover. I forhold til lovgivningen på sitt område, har Kommunal- og regionaldepartementet uttrykkelig uttalt at kravene til skriftlig-het i bl.a. plan- bygningsloven ”*anses ikke å være til hinder for bruk av elek-tronisk kommunikasjon*”. Videre uttaler departementet at deres ”generelle tolkning er at *skriftlighet* og *signatur* må anses å være teknologinøytrale begreper, dvs at valg av teknologiform i kommunikasjon mv ikke er avgjørende for gyldigheten av innholdet”. Disse uttalelsene er hentet fra Ot.prp.nr. 108 (2000-2001) (kap. 12, side 165), som handler om å fjerne juridiske hindre for elektronisk kommunikasjon. Denne tolkningen er helt i tråd med den generelle rettsforståelsen fra de øvrige departementer, som dokumentert i Ot. prp’en og i etterfølgende dokumenter. I Besl.O.nr.19 (2001-202) (http://www.stortinget.no/-beso/beso-200102-019.html) ble lovendringene vedtatt. I tillegg er det foretatt endringer i 21 forskrifter som trådte i kraft 1. juli 2001.[2] Sentrale konklusjoner i lovendringene er at elektronisk kommunikasjon i stor grad likestilles med papirbasert kommunikasjon. Arbeidet i kartleggingsprosjektet/e-regel-

[2] Fellesproposisjonen, Ot.prp. nr 108 (2000-2001) om lov om diverse endringer i lover for å fjerne hindringer for elektronisk kommunikasjon, ble oversendt Stortinget til behandling 31. august 2001. Som følge av Stortingsvalget samme høst ble proposisjonen lagt frem på nytt for det nye Stortinget den 5. oktober 2001 som Ot.prp. nr 9 (2001-2002). I denne ble det gjort mindre justeringer/presiseringer i lovendringsforslagene.

prosjektet[3] tok utgangspunkt i en "funksjonell ekvivalens metode". Med denne modellen har man vurdert hvilke funksjoner som for eksempel begreper som skriftlig og protokoll kan ha og hvilke hensyn som må ivaretas for å åpne for elektronisk kommunikasjon.

De konklusjoner som kan trekkes etter det omfattende arbeidet i e-regel-prosjektet er i følge Nærings- og handelsdepartementet (i egenskap av prosjektleder) bl.a. følgende:

- Eksisterende regelverk er i stor grad ikke til hinder for elektronisk kommunikasjon. Hensynene bak den enkelte bestemmelsen er mulig å ivareta ved elektronisk kommunikasjon og selve lovteksten har ikke brukt begreper som stenger for elektronisk kommunikasjon.
- Begrepet "skriftlig" er nå blitt tolket til å være et teknologinøytralt begrep. Dette betyr at begrepet ikke vil være et hinder for elektronisk kommunikasjon. Dersom det i et regelverk stilles krav om "skriftlig", men det ikke er ønskelig at det kan skje elektronisk, må det heretter stilles tilleggskrav; for eksempel "skriftlig på papir".
- Normalt kan elektronisk kommunikasjon bare benyttes når mottaker har godtatt å motta meldingen på denne måten. Med godtakelse menes en frivillig erklæring om at man aksepterer å motta meldingen elektronisk. Det kan også stilles krav om at godtakelsen er uttrykkelig, hvilket påvirker beviskravet i forhold til selve godtakelsen og hva den dekker.
- Der det er viktig at dokumentet er kommet frem, stilles det krav om at "det er benyttet en betryggende metode for å sikre at dokumentet er kommet frem". For å ivareta dette kravet kan man for eksempel bruke et web-skjema eller gjøre dokumentet tilgjengelig fra et informasjonssystem for nedlasting av mottaker. Dette krav oppstilles bl.a. for elektroniske meldinger som på papir sendes som rekommandert brev.
- I mange situasjoner er det ønskelig å sikre hvem som har sendt et dokument (alternativt undertegnet en avtale) og at dokumentet ikke er blitt endret etter det er blitt sendt elektronisk. For å sikre at disse hensynene blir ivaretatt kan det oppstilles krav om at "det benyttes en betryggende metode for å autentisere avsender/avtaleinngåelsen og sikre dokumentets/avtalens innhold".

Det legges generelt sett ikke føringer i ”vanlige” lover/forskrifter for valg av hva slags teknisk løsning man må ha for å aksepteres iht. regelverket som gyldig underskrift. Er det så noen *andre* rettslige føringer på hva slags teknologivalg som skal eller bør gjøres?

I lov om elektronisk signatur, med forskrift, kan vi ikke se at det gis direkte føringer for løsninger på plan- og byggesaksområdet. Loven gir ingen pålegg om å bruke elektronisk signatur, men gir rammebetingelser for *tilbydere* av aktuelle tjenester og produkter, særlig i forhold til elektroniske signaturer på et høyt kvalitets- og sikkerhetsnivå (kalt kvalifisert elektronisk signatur). Loven slår fast at slike signaturer alltid skal sies å tilfredsstille rettslige krav om underskrift, men også elektroniske signaturer på enklere nivå kan gjøre det, iht.

[3] Se e-Regelprosjektet i regi av Nærings- og handelsdepartementet
http://www.dep.no/nhd/norsk/p10001272/eRegelprosjektet/index-b-n-a.html

loven, som er en norsk implementering av et EU-direktiv[4]. I Norge har vi følgelig både en generell rettslig aksept av elektronisk signatur i loven om elektronisk signatur, og uttrykkelige aksepter i en rekke enkeltlover gjennom de nevnte lovendringene som følge av e-regelprosjektet. Vi har nærmest fått i pose og sekk; det skal ikke være noen tvil om at elektroniske løsninger er i orden juridisk sett (på noen enkeltområder er bildet et annet, men det er annen historie).

Men er teknikken til å stole på? Vil den gjøre det vi er ute etter å få gjort, brukervennlig, raskt, effektivt og uten problemer?

Elektronisk signatur kan innebære ulike teknologivalg/metoder for å ivareta en eller flere signatur-funksjoner. Elektroniske signaturer er et fellesbegrep for eksempelvis passord, PIN-kode, biometri, eller digital signatur. Loven om elektronisk signatur definerer dette til å være ”*data i elektronisk form som er knyttet til andre elektroniske data og som brukes som autentiseringsmetode”*. Tilnærmet samme definisjon er brukt i den nye forskriften om elektronisk kommunikasjon med og i forvaltningen. Selve begrepet er følgelig omfattende, upresist, og sier i seg selv lite om kvaliteten på løsningen, styrken i den tekniske løsningen. Det finnes *flere ulike teknikker* som kan gi signeringsfunksjoner. Disse må vurderes i forhold til hva en vil oppnå, hva en skal sikre seg mot. Forskriften om elektronisk kommunikasjon med og i forvaltningen gir heller ikke noe pålegg om å ta elektroniske løsninger i bruk. Men den gir en del klare føringer hvis man tar elektroniske signaturer eller andre såkalte sikkerhets-tjenester i bruk.

3.2 Søknadsbehandling i dag

Totalt behandles det ca. 100 000 byggesaker i året i Norge, [15]. De fleste søknadene gjelder bygging/endring av privatpersoners boliger. Hovedpro-blemene er at søknadsprosessen tar lang tid i flere ledd, og at den er ’smertefull’ for søkerne fordi søknaden ofte sendes i retur som ufullstendig og søkerne må drive ’oppsøkende arbeid’ for å få tak i informasjon. Særlig store kommuner har lang behandlingstid.

Det generelle inntrykket er at søkere har problemer med å forstå hva som skal være med i søknaden. Det er ikke lett å orientere seg i regelverket for å finne ut hva som er riktig å gjøre. Det står ikke nok informasjon på søknadsskjemaet og de må henvende seg til kommunen. Det innebærer at det kan bli flere søknads-runder før kommunen aksepterer søknaden som fullstendig. Deretter avhenger saksbehandlingstiden av hvilke hjelpemidler kommunen har når den skal sjekke om all informasjon er korrekt, og selvfølgelig av at kommunen har nok kompe-tente saksbehandlere.

[4] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures, http://www.ict.etsi.fr/eessi/Documents/e-sign-directive.pdf

3.2.1 Problemer det kan være ønskelig å gjøre noe med i en elektronisk versjon

Det er ønskelig å kunne hjelpe søkerne med å få til en fullstendig søknad raskere. Det har bare med signaturer å gjøre i den grad noen krever at signatarene (de som signerer) skal være klar over / forstå hva de signerer og hvorfor.

Den elektroniske søknaden medfører at noe av søknadsarbeidet overføres til søkerne. Dvs. systemet (framfor at saksbehandler hjelper eller retter i ettertid) hjelper søkerne ved å forklare hva som menes med hver informasjon det spørres etter, enten det er felt i søknaden eller informasjon som skal være med på en tegning eller et situasjonskart. Dette kan i stor grad gjøres enklere og bedre elektronisk bl.a. ved hjelp til å verifisere gyldige verdier i et felt eller ved at det kommer fram forklaringer og lenker til aktuelt regelverk.

Det er sannsynligvis et større arbeid å lage en korrekt søknad (kravspesifikasjonens pkt 2.16 [18]). Fordi det er så mange slags søknader, vil et elektronisk system bare til en viss grad kunne sjekke om det er logisk brist i søknaden.

3.2.2 Signatarer

Signatarer er de som signerer søknadene. Vi forstår det slik at kommunens status for sjekking av signatarer er:

- Ansvarlig søker: Det sjekkes ikke hvem det er som signerer, bare om oppgitt firma eller navn har akseptabel godkjenning. Hvis ikke stoppes søknadsbehandlingen.
- Tiltakshaver sjekkes ikke, Bare at det oppgis et navn, ellers stopper behandlingen
- Naboer: kommunen sjekker om riktige naboer er varslet, men ikke om innholdet i varselet er korrekt.
- Faglig ansvarlige på ulike områder må ha godkjenning seinest ved igangsetting.

I papirverdenen undersøkes det altså om det skrevne navnet i noen tilfeller kan relateres til den rollen underskriveren har. Om signaturene på dokumentene tilhører navnet, undersøkes bare ved tvister.

3.2.3 Vurdering av dagens situasjon

De fleste vi har snakket med, gir uttykk for at det generelt er lav risiko forbundet med å bruke papirsøknader. Informasjonen er åpen og fordrer ikke konfidensialitet. Men søknadsutfylling og –behandling oppleves som frustrerende. Det går mye penger og tid med til mye ”rot”. Respekt for regler og myndigheter står på spill.

I og med at det er papirdokumenter som oversendes, skaper ikke søknadene noen risiko for andre systemer i kommunene.

3.3 Dagens ByggSøksystem

I kravspesifikasjonen for ByggSøk [18] står følgende hovedmål spesifisert:

> Hovedmål med ByggSøk er å utvikle standardiserte utvekslingsformater og beskrivelse av systemer for elektronisk behandling av og kommunikasjon via Internett i bygge og plansaker.
>
> Målet er kortere behandlingstid og bedre ressursutnyttelse i kommunene og i næringen som skal gi en reell effektivitets- og kvalitetsøkning for BA-næringen og kommunene men også tilpasset selvbyggere. I neste omgang gir dette gevinst for tiltakshaver og samfunnet.

I tillegg skal prosjektet føre til større tilgjengelighet, forutsigbarhet, tempo og åpenhet som gir bedre service for alle.

3.3.1 Det som er realisert

ByggSøksystemet er i dag en prototyp som er utviklet med åpen kildekode. Hovedingrediensene er skriptspråket PHP, MySQL og XML. Det er registrert 12 – 1300 brukere og ca. 1000 aktive byggesaker. Hver søknad tar liten plass i databasen < 1 MB. Tegninger og kart kan øke datamengden. BE har lagt seg på pdf som format for grafikk. Det regner de vil holde de nærmeste 5 årene. Systemet går på en server hos BE. All kommunikasjon med systemet skjer over internett, også spørring til andre databaser i huset. All spørring til interne og eksterne databaser skjer etter avtale og mellom IP-adresser. Det legges ikke på ekstra sikkerhet i overføringen, ettersom det er enklere å få tak i informasjonen på annet vis (ringe kommunen). Det tas vanlig backup med fjernlagring. Oppetiden er ca. 99.5%. En dag nede kan gi manglende tilgang til ca. 6000 søknader hvis alle søknader fylles ut elektronisk.[5]

Systemet driftes av 1 ½ person pluss konsulenthjelp ½ dag hver 14. dag. De har god overvåking av systemene sine. Når systemet settes i drift, skal de ha to servere for speiling og to porter til internett for å bedre tilgjengeligheten.

- Alle som har en nokså standard PC med internettilknytning, kan fylle ut en elektronisk søknad. Den lagres hos BE.
- Det er ansvarlig søker som får tilsendt bruker-ID og passord.
- Søkerne får hjelp til utfyllingen og kan endre de fleste feltene. Systemet er raskt.
- Byggefirmaer kan forberede søknadene lokalt og deretter reformatere dem og oversende dem til ByggSøk.
- Søknaden skal i teorien kunne lagres lokalt hos søker. På den måten kan den lastes opp igjen til ByggSøk for videre bearbeiding dersom kommunen returnerer den pr. post.
- Entreprenører vil etter hvert benytte interne ”fagsystemer” i søknadsskrivingen slik at all utfylling gjøres lokalt før hele søknaden ”dumpes” ned samlet til Byggsøk. Her kan det trengs definisjon av meldingsformater mm. for å representere informasjon som skal produseres lokalt og sendes inn. En søknad som er utfylt lokalt, kan også være ”ferdig signert” lokalt.

[5] 100 000 søknader/ 52 uker = 1900 nye søknader /uke * editering i 3 uker = 5700 søknader

3.3.2 Autentisering av signatarer

Følgende sjekkes i ByggSøk:

- Ansvarlig søker: hvis søker ikke har sentral godkjenning, kommer det fram skjema for å søke om lokal godkjenning.
- Faglig ansvarlige på ulike områder sjekkes mot sentralt register. Hvis vedkommende ikke står i registeret, kommer det fram skjema for å søke om lokal godkjenning. ByggSøk sjekker om foretaket har godkjenning for utførelse og/eller kontroll, men ikke hva slags oppgaver. Det er en større utfordring.
- Tiltakshaver sjekkes ikke
- Naboer sjekkes ikke

3.3.3 Saker som ikke er løst og som er relevante for tillit og risiko

- Ved å taste g.nr. og b.nr. er det lagt til rette for at informasjon om eier overføres fra GAB. Da låses den informasjonen for videre endring. Hvis informasjonen fra GAB er ufullstendig eller feil, og søkeren er klar over det, kan det frustrere søkeren at det er umulig å endre informasjonen slik at den sendes ukorrekt til kommunen. Dette er ulikt papirløsningen.
- Utskrift av ferdig utfylt søknad virker ikke like bra hos alle. Det viser seg at Acrobat har problemer med konvertering. Uerfarne søkere kan ha problemer med å se at utskriften ikke er korrekt. Da vil søkerne få søknaden i retur fra kommunen likevel. Det kan senke tilliten til systemet og forvaltningen.
- Fullstendighet. ByggSøk klarer ikke å sjekke om en søknad er fullstendig. Prosjektet har ikke tatt mål av seg til å sjekke alle muligheter. På en del områder er ikke regelverket klart, og på andre områder fins det ikke ferdige databaser med informasjon som systemet kan kontrollere søknaden mot.
- Korrekthet. ByggSøk kan i liten grad være til hjelp med å sjekke om søknaden henger logisk sammen.
- Om regelkrav til underskrift er oppfylt (jfr. bla. denne utredningen).

3.3.4 Annet

Ansvarlig søker kan ta kopi av søknaden og laste den opp for videre utfylling eller endring dersom den kommer i retur fra kommunen. Kravspesifikasjonen for ByggSøk ble laget sommeren 2002. Momenter av interesse er:

- Det er BE som godkjenner foretak og lagrer informasjonen i et register for sentralt godkjente foretak. Registeret har ikke kopling mot Brønnøysund-registrene. BE har prøvd å standardisere indetifikatoren med BR, men de har ikke lyktes helt. BE godkjenner distriktskontorer mens BR lagrer foretak på overordnet nivå. Dette skal/ønsker de å løse.
- BE har foreløpig ikke løst hvordan systemet skal framskaffe reguleringsstatus for eiendommer elektronisk.
- Noen kommuner har ikke saksbehandlingssystemer som kan motta all informasjonen fra en elektronisk byggesøknad. Disse kan (skal kunne) bruke systemet ByggSøk på elektroniske søknader som lagres i kommunen.
- I kravspesifikasjonen står det at det skal være mulig å endre i alle tidligere registrerte data før sending. Det er uklart for oss hvordan hva som skjer hvis brukerne mener at informasjonen fra GAB er feil. Brukerne bør på en eller annen måte kunne formidle at de mener informasjonen fra GAB er feil.

- Det er bare ansvarlig søker som kan endre informasjonen i søknaden. Tiltakshaver og andre kan få se sitt område og krysse av for at det har sett det. Dersom ikke-benekting er et krav, vil det være vesentlig å vite hvem som endrer i søknaden

3.3.5 Vurdering av ByggSøk som grunnlag for papirsøknad

ByggSøk kan hjelpe søkeren til en mer fullstendig utfylt søknad. Kommunene mottar bedre utfylte søknader som kan viderebehandles elektronisk.

3.4 Oppdal kommune

Oppdal kommune har valgt å starte med å hente elektroniske søknadsskjemaer for enkle byggemeldinger fra Sem og Stenersens databank. Det er en byggesøknad som bare signeres av tiltakshaver og er teknisk mye enklere enn andre byggesøknader der tiltakshaver og aktuelle ansvarlige foretak skal signere over delvis samme informasjon. Søkerne logger seg på med en digital signatur og et digital sertifikat. Sertifikatet sjekkes av ZebSign/Buypass. Ved hjelp av fødselsnummeret som er lagret i sertifikatet, hentes opplysninger knyttet til egen person som f.eks. g.nr. og bnr. fra GAB, og fylles inn i meldingen. Søkeren får altså hjelp fra bakenforliggende systemer. Men meldingen kan ikke lagres halvferdig. Den må fylles ut i én sesjon. Deretter kan meldingen signeres digitalt og oversendes kommunen. Det genereres en XML-file av meldingen og et pdf-dokument om hvem som har signert. Oppdal kommune har ikke md dette ment å løse "alle" problemstillinger knyttet til elektronisk byggesaksbehandling. Men de opplever at de får mye god erfaring i en tidlig fase av digitale signaturer.

3.5 Oslo kommune

Våre informanter i Oslo kommune opplever sterkt et behov for at formalitetene skal være i orden i en elektronisk verden. De mener at det å være seg bevisst signeringsprosessen er vesentlig. Hvor reelt behovet for signering er, er likevel uklart. Kommunen har løst problemet ved at ansvarlig søker fyller ut søknaden og oversender den elektronisk til kommunen. I tillegg skrives det ut et signeringsskjema der alle signatarer vedkjenner seg sin del av innholdet i søknaden ved at de skriver under for hånd. Dette skjemaet fakses til kommunen som lagrer det elektronisk i tilknytning til selve søknadsinnholdet.

Oslo kommune har ikke mange konflikter knyttet til signaturer. Den mener at den får til en effektiv søknadsinnhenting og nyter godt av at ansvarlig søker gjør mer av utfyllingsarbeidet uten deres hjelp. Alle signatarene kan ta vare på en utskrift av det de har signert. Ikke-benekting er godt ivaretatt.

Oslo kommune tester bruk av digitale signaturer mot ByggSøk-systemet. For autentisering av ansvarlig søker mot ByggSøk er det nå mulig å benytte sertifikater fra Skandiabanken, Buypass / Norsk Tipping (brukerne må istallere en ekstra komponent for CAPI-grensesnitt) og Postens eKurer. Testen vil

antagelig bli utvidet med EuroTrust (Verisign i DK). Det arbeides med å få til signering av søknaden.

3.6 Utgangspunkt for arbeidet

3.6.1 Identifikasjon av signeringsfunksjoner

I hht. lov om elektronisk signatur, kan man bruke mange slags teknikker for å få til en elektronisk signatur. Kravet i loven for å kalle noe en elektronisk signatur er at man bruker den tekniske løsningen som 'autentiseringsmetode'. Man kan bruke f.eks.

- digitale signaturer, som benytter asymmetrisk kryptografi,
- en brukerident og et passord, slik at bare den som kjenner passordet får tilgang til søknaden,
- en PIN slik det brukes når man oversender selvangivelsen.

Det er kanskje ikke vanlig å tenke slik ennå, men vi har sett på brukerident og passord som en signeringsteknikk som loven om elektronisk signatur definerer som en elektronisk signatur. Vi er klar over at BE bruker brukernavn og passord som tilgangsmekanisme til de enkelte søknaden og ikke ser på det som en generell metode for elektronisk signatur.

Når det i et regelverk er krav om at det skal benyttes en signatur, er det sjelden utdypet hvilken funksjonalitet signaturen har. På et papir ser en signatur likedan ut enten den identifiserer signataren eller den knytter ham til et byggeansvar. Det er ikke nødvendigvis tilfelle i en elektronisk verden. En digital signatur vil alltid være forskjellig. Men hvis man tenker på brukerident og passord som en elektronisk signatur, kan den lages lik ved hver bruk. Det er flere som har prøvd å framstille signaturenes ulike funksjoner [8], [9]. Noen eksempler er:

a) I **identifiseringsfunksjon** ligger det at signaturen knytter et dokument til innehaveren av signaturen. De personlige elementene i den håndskrevne signaturen er med på å fastslå identiteten til underskriveren.
b) I **bevisfunksjonene** ligger det at en underskrift på et dokument kan brukes som bevis for noe, f.eks. en handling mellom parter og eventuelt i en rettssak.
c) En underskrift har **autentiseringsfunksjon** ved at den står under et dokuments innhold.
d) En signatur kan f.eks. understreke alvoret i en handling og har da mer av en **symbolfunksjon** enn en bevisfunksjon.
e) Underskrifter brukes til å avslutte prosesser, f.eks. forhandlinger og har da en **avslutningsfunksjon.**
f) Den sosiale verdien ved signering kan kalles en **seremonifunksjon**.
g) Ved en **vedkjenningsfunksjon** har signataren en intensjonen om å knytte seg til en tekst skrevet av andre eller en selv.

Signaturfunksjoner kan løses teknisk med ulike metoder, dvs. ulike teknikker vil dekke funksjonene i varierende grad. For å finne en akseptabel løsning må man se helheten i problemet.

3.6.2 Papir vs. Elektronikk

Når man går fra papirteknologi (søknadsskjemaer) til den elektroniske verdenen, og sender en byggesøknad via nettet, må man på noen områder ta i bruk teknikker som er spesielle for den nye teknologien. F.eks. er det enkelt på papir at ansvarlig søker fyller ut alle felt, og at tiltakshaver signerer etterpå. På en elektronisk søknad må man finne løsninger slik at tiltakshaver ikke kan benekte å ha signert, også kalt ikke-benekting, hvis det er en annen som har fylt ut feltene i søknaden.

3.6.3 Bruk av digitale signaturer

Bruk av digitale signaturer på en byggesøknad vil sannsynligvis bli dyrt og krevende hvis mekanismen skal bli gjort tilgjengelig for hele den voksne befolkningen og de ikke har den fra før. Det blir billigere totalt sett hvis søkerne har utstyret fra før. Momenter som bør tas i betraktning er:

- Kommunenes mottakssystemer må kunne validere sertifikater, og kunne benytte informasjon i sertifikatene inne i egne saksbehandlingssystemer.
- Brukerne må til en viss grad forstå, kunne installere system for og kunne bruke nøkler og sertifikater.
- Det er fra flere hold uttrykt ønske om at innholdet i sertifikatene og sertifikatformatene bør standardiseres på tvers i forvaltningen der det er nytte-kostnadseffektivt. Slike vurderinger av standardiseringsbehov kan ta tid og forsinke hvert enkelt prosjekt hvis de må vente på hverandre.
- ByggSøksystemet må holde et generelt sikkerhetsnivå som hindrer sikkerhetsbrudd på områder som en digital signatur er knytet til. Dette gjelder også for elektroniske signaturer og enklere former for sikkerhetsteknikker.
- BE og kommuner som ønsker å motta elektroniske søknader, må skaffe seg kompetanse innen informasjonssikkerhet for å kunne forstå og drifte bruken av digitale signaturer.

Det fins alternativer innenfor dette området. ByggSøk kan validere sertifikatene, men da må BE ta ansvaret for arkivering av logger osv. På den andre siden kommer mange kommuner til å måtte håndtere digitale signaturer og sertifikater i andre sammenhenger. Da vil de få en infrastruktur som kan gjenbrukes for bl.a. byggesøknader.

Det er derfor ønskelig å vurdere rimeligere alternativer som likevel sikrer lover og forskrifters hovedhensikter på akseptabel måte. Noen forvaltningssystemer som kommuniserer med befolkningen klarer seg med PIN-kode for autentisering/signering. Det anses å oppfylle deres lovkrav, jfr. selvangivelsen. Vi må undersøke om endrete rutiner eller annet til sammen kan gi samme virkning som en signatur. Logging og tilknyttede prosedyrer kan bli viktig for slike løsninger.

3.6.4 Strategi for helhetlig informasjonssikkerhet

Som nevnt gir forskriften om elektronisk kommunikasjon med og i forvaltningen ikke noe pålegg om å ta elektroniske løsninger i bruk. Men den gir en del klare føringer *hvis* man tar elektroniske signaturer eller andre såkalte

sikkerhetstjenester i bruk, eller ønsker å ta dem i bruk. Da pålegger forskriften forvaltningsorganer at de *på forhånd* må utarbeide sikkerhetsmål og –strategi, slik at man skal tenke signatur-sikkerhet i et helhetlig perspektiv som et ledd i den generelle informasjonssikkerheten i virksomheten. Det er videre pålegg i forskriften om å utarbeide slik strategi på grunnlag av anerkjente prinsipper for virksomheters håndtering av informasjonssikkerheten (§ 11, nr 1 og 2). Anerkjente prinsipper er ofte nedfelt i standarder. En meget viktig standard på dette området er BS 7799:1999 – British Standard 7799. Den er også blitt norsk og internasjonal standard (NS-ISO/IEC 17799 Utgave 1, 2001 Informasjonsteknologi - Administrasjon av informasjonssikkerhet (ISO/IEC 17799:2000) / Information technology - Code of practice for information security management (ISO/IEC 17799:2000). Virksomheter kan derved utvikle, implementere og måle virksomhetens sikkerhetsarbeid og rutiner. BS 7799 er basert på den beste nåværende praksis innen arbeidet med informasjonssikkerhet både i England og i mange andre land. Den ligger til grunn for en norsk ordning for frivillig sertifisering av informasjonssikkerheten i organisasjoner, forvaltet av Norsk Akkreditering, se under I*nformasjonssikkerhet* på nettsiden deres: http://www.justervesenet.no/na/. Se også rapporten Elektroniske signaturer – Myndighetsroller og regulering av tilbydere av sertifikattjenester http://odin.dep.no/nhd/norsk/publ/rapporter/024005-994081/index-dok000-b-n-a.html.

I den grad personvernhensyn gjør seg gjeldende i byggesaker, må personvernlovgivningen følges. Det vises til den første rapporten fra Statskonsult for en nærmere omtale, men først og fremst til Datatilsynets egne nettsider (se http://www.datatilsynet.no). Her skal vi bare minne om at den behandlingsansvarlige har plikt til å lage og systematisk vedlikeholde sikkerhetsmål- og strategi, herunder gjennomføre risikovurdering knyttet til behandlingen av personopplysninger, før behandling av personopplysninger gjøres (personopplysningsloven § 13 og -forskriften kapittel 2). I praksis betyr dette å legge den britiske ”best-practice” standarden til grunn, BS 7799 nevnt over, eller tilsvarende norsk versjon.

Det er med andre ord sterke grunner til å få tak i og sette seg inn i denne standarden, som grunnlag for sitt eget arbeid på området sikkerhetsstrategi og risikovurderinger, der hele virksomhetens håndtering av informasjonssikkerhet er objekt for vurdering. Dermed kan risikovurderinger i det små (signaturer) sees i et mer helhetlig perspektiv (hele virksomheten), for å unngå åpenbart svake ledd i kjeden.

4 Tekniske løsninger for ulike signatur-funksjoner

En signaturfunksjon kan realiseres elektronisk på ulike måter avhengig av hvilken teknikk man velger. Teknikkene vil dekke en slik funksjon i ulik grad.

Teknikken asymmetrisk kryptering, som digitale signaturer benytter, og tilhørende sertifikater og infrastruktur, gir vanligvis en lav risiko for at det er feil person som kopler seg til et system. Teknikken med bruker-ID og passord vurderes til å gi en høyere risiko for at feil person kan kople seg til. En teknikk for å dekke funksjonen å vedkjenne seg å ha signert et bestemt dokument, vil ofte være tjent med å ha med spørsmål eller påminnelse om at. 'Nå signerer du søknad om ansvarsrett for elektrikerarbeid'.

I tillegg til teknikker kommer altså en eller annen form for infrastruktur, rutiner, påminnelser og hvordan et mottakende system skal benytte/bruke en bestemt signaturfunksjon. Arbeid som ofte må utføres av det mottakende systemet, er

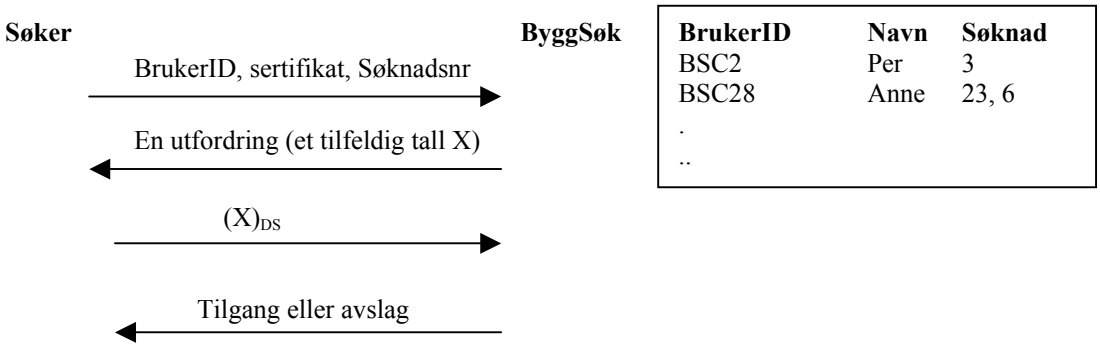
- Autentisere signataren mot et offentlig register slik at det er 'riktig' navn som er knyttet til signaturen. Dette kan kreve en bakenforliggende kopling til det signaturen gjelder. Eksempler er at det er riktig nabo eller at det er en godkjent rørlegger som signerer.
- Verifisere selve 'signaturen'. Det kan være å beregne en digital signatur eller verifisere godkjente brukernavn og passord.

4.1 Digitale signaturer

Digitale signaturer bruker asymmetrisk kryptering som teknikk[6]. I og med at den teknikken kan brukes til mange ting, må ByggSøk gjøre søkeren spesielt oppmerksom på at 'nå signerer du og vedkjenner deg innholdet i søknaden', der det er aktuelt. Den asymmetriske krypteringsteknikken kan eventuelt brukes av ansvarlig søker eller andre til å logge seg på ByggSøk for å fylle ut en bestemt søknad eller en del av den.

Ved et tenkt eksempel kan vi anta at ansvarlig søker vil benytte en digital signatur i stedet for passord til å autentisere seg overfor ByggSøk. ByggSøk har opprettet en tabell med søkeres navn, bruker-ID og søknadsnumre hver søker kan få tilgang til. Søkeren mottar en bruker-ID og aktuelle søknadsnumre via e-post fra BE og skal i gang med utfyllingen. Da kan bruk av digital signatur for autentisering fungere på følgende måte.

[6] *Digital signatur* brukes ofte synonymt med teknikken asymmetrisk kryptering. Men asymmetrisk kryptering kan også brukes til f.eks. autentisering og kryptering av data. Vi mener at det ikke er nødvendig å forstå teknikken asymmetrisk kryptering for å lese denne rapporten.



Figur 1 Pålogging til et system vha. digital signatur

Søkeren sender brukerident: BSC2, et sertifikat der navnet "Per" står og vil ha tilgang til søknad nr. 3. ByggSøk må undersøke i sin tabell om den innsendte BrukerID-en har samme navn i sertifikatet som det som står i tabellen. Hadde det stått. "Per Bjørn" i sertifikatet, ville henvendelsen blitt avvist. Hvis navnet stemmer, sjekker ByggSøk med sertifikatutstederen om sertifikatet er gyldig. Deretter signerer søkeren et tilfeldig tall X som ByggSøk må verifisere om er ekte eller ikke. Hvis signaturen er ekte og riktig søknadsnr. er knyttet til brukeridenten, får søkeren tilgang. En variant av denne teknikken testes i Oslo kommune.

4.2 Andre aktuelle signerings- og sikkerhetstjenester

Teknikken asymmetrisk kryptering kan benyttes fra PC-er eller f.eks. fra mobiltelefoner der sertifikater allerede fins som sikkerhetsmekanisme.

4.2.1 Bruker-ID og passord.

Den som har mottatt bruker-ID og passord, skal sikres å få tilgang til en eller flere søknader. Administrator for ByggSøk setter tilgangsrettigheter – hva eieren skal kunne lese og hva eieren eventuelt skal kunne bearbeide. En tiltakshaver skal kunne lese alle søknader, men kanskje bare kunne endre felt som er knyttet til eget navn. En rørlegger skal bare ha tilgang til informasjonen som angår ham og skal bare kunne endre felt som er knyttet til hans ansvarsområde.

Den vanlige måten å tenke på denne teknikken på, er at den autentiserer en bruker. I hht. definisjonen i lov om elektronisk signatur kan bruker-ID og passord betraktes som en elektronisk signatur, og regelforvalter kan bestemme at det skal brukes på denne måten i en bestemt sammenheng, jfr. 5.2.7.

4.2.2 Knytte sammen en bruker-ID, en signatar og en rolle.

En person som skal signere elektronisk på del av en byggesøknad, må være registrert i ByggSøk før signeringen kan foregå fordi det må opprettes tilgang til informasjonen. I papirverdenen trengs det intet slikt forarbeid.

Hvem som helst kan sende inn en byggesøknad. ByggSøk trenger derfor ikke å identifisere søkeren ytterligere, men sender bruker-ID og passord til den e-postadressen en framtidig søker oppgir.

Derimot kan det være vesentlig for andre interessenter at en som skal signere deler av en søknad, er "rette vedkommende". Kommuner kan ønske å identifisere en signatar som elektriker på elektronisk vis for å effektivisere saksbehandlingen. Det kan kreve opprettelse av og elektronisk kontakt med oversikter over godkjente profesjoner. Lovgiverne ønsker at søknadsprosessen har en viss kvalitet og mener at det f.eks. hjelper å sjekke ansvarlig rørlegger mot det sentrale registeret. Ut fra det kan kanskje systemet akseptere å sende en egen bruker-ID og passord til rørleggeren som skal utføre et arbeid og signere deler av søknaden til e-postadressen som er oppgitt i det registeret. Tilsvarende gjelder for andre profesjoner.

Det blir mye vanskeligere hvis den som har rolle som nabo, skal signere elektronisk. Hvordan skal man vite at en oppgitt e-postadresse (donald@online.no) tilhører riktig nabo (gnr 3, bnr. 15, Kari Halden)? Foreløpig er e-postadresser en flyktig affære som det ikke er rimelig å stadig skulle oppdatere i f.eks. GAB-registeret.

5 Risikovurdering

5.1 Analysegrunnlaget

5.1.1 Risiko

Utgangspunkt for risikovurderingen er at det ikke er et mål å ha høyere sikkerhet elektronisk enn for papirsøknader med mindre regelverk eller risikovurdering tilsier det [15]. Vi tok derfor utgangspunkt i sikkerhetskravene ved bruk av papirsøknader. I og med at papir og elektronikk er to ulike teknologier, løses 'sikkerhetsproblemene' på ulike måter. Bl.a. er egenskaper som håndskrevne underskrifter har, forskjellig fra elektroniske og digitale signaturer. Sammenlikningen blir derfor haltende og kan bare aksepteres på et grovt nivå. Vi har brukt verdiene lav, middels og høy for både risiko, sannsynlighet og kostnader.

Det fins flere måter å definere risiko, se kap.7 Ordbok. Risiko er i stor grad en subjektiv forståelse der man balanserer

- uønskete hendelser som kan inntreffe,
- oppfatningen av 'fare' ved hver hendelse og
- egen tilbøyelighet til å ta en risiko i forhold til hva man kan oppnå eller tape [2].

Interessenter rundt ByggSøk må f.eks. vurdere:

- Hva galt kan skje hvis jeg signerer og sender denne meldingen ut fra det jeg vet og kan om datasystemet?
- Hva gir mest arbeid for kommunen: å motta falske elektroniske søknader eller falske papirsøknader?

Objektene for risikovurderingen har vært de funksjonene som signaturkravene i regelverket kan sies å ha. I tillegg er det mange steder i regelverket det ikke er krav om signatur, men der det ligger under at aktørene knytter seg til ett eller annet tilsynelatende udefinert ansvar. Disse aspektene har vi også prøvd å vurdere ettersom sikkerheten i det elektroniske systemet blir uinteressante hvis det er fullt av huller på andre områder enn signering.

Vi har i hovedsak valgt å risikovurdere signaturteknikkene (signeringstjenestene) digital signatur med eventuelle meldinger om at 'nå signerer du' mot det ByggSøk bruker i dag: bruker-ID og passord (som her betraktes som en elektronisk signatur) med eventuelle meldinger i tillegg. Disse teknikkene eksemplifiserer ulike nivåer for sikkerhet og hva de kan bidra med mot ulike uønskede hendelser. Det fins mange signeringsteknikker for elektronisk signatur. De spenner over så ulike teknikker som engangspassord og PKI-basert pålogging til et system[7]. Men en nytte-kostnadsvurdering må ta hensyn til både utgifter, inntekter og mulig risiko de ulike interessentene løper ved å

[7] Om forståelse av forskjellene på digital og elektronisk signatur, se Statskonsults første rapport om emnet [17]

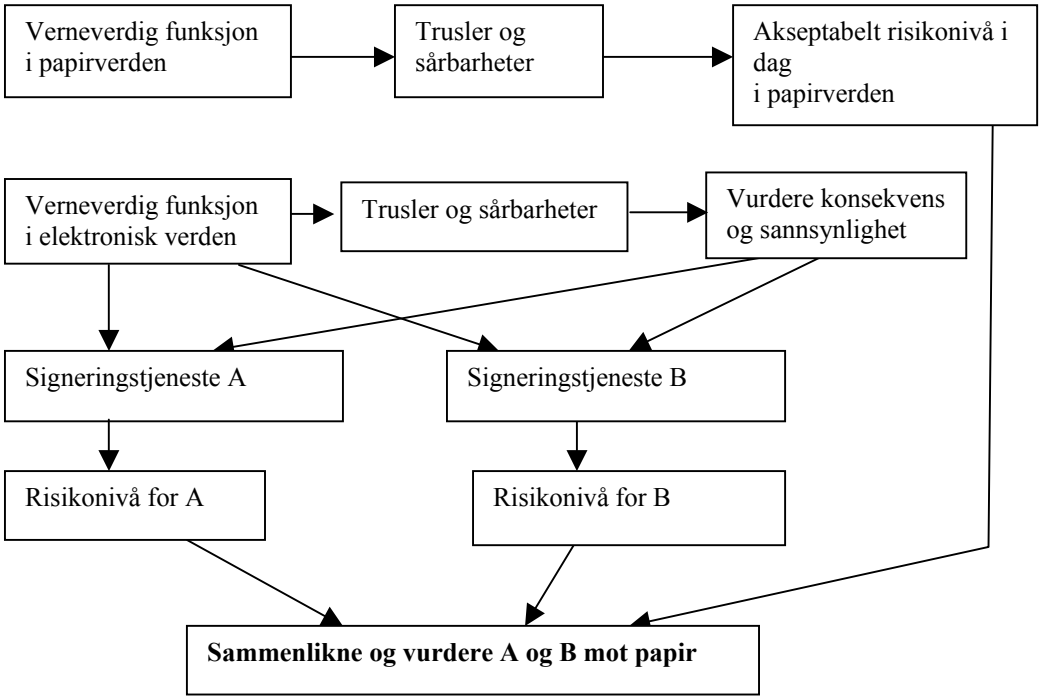
bruke de forskjellige teknikkene. Det bør bli en helhetsvurdering av hva som er optimalt.

Oslo kommune har f.eks. valgt at ansvarlig søker skal fakse håndskrevne underskrifter i tillegg til en elektronisk oversendelse av søknadsinnholdet. Den har vi tatt opp til slutt i vurderingen fordi det er en blandingsløsning.

5.1.2 Framgangsmåte for risikovurderingen

Vi startet med en vurdering av trusler og sårbarheter som papirsøknadene er gjenstand for, og fikk en forståelse for hva som er akseptabelt risikonivå for dem, se Figur 2 Risikovurdering.

Etter å ha funnet aktuelle signeringsfunksjoner, så vi etter trusler og sårbarheter mot disse i det elektroniske systemet, og vurderte mulige konsekvenser.
En signeringstjeneste A, f.eks. digital signatur, kan redusere visse uønskede konsekvenser, f.eks. lette identifiseringen av en ansvarlig søker som ikke har riktig kompetanse i forhold til byggesaken. En annen signeringstjeneste B, f.eks. bruker-ID og passord, kan også lette identifiseringen, men neppe gi samme lave risikonivå. Avslutningsvis vurderte vi risikonivåer for papirsøknader mot risikonivåene de ulike signeringstjenestene ga.

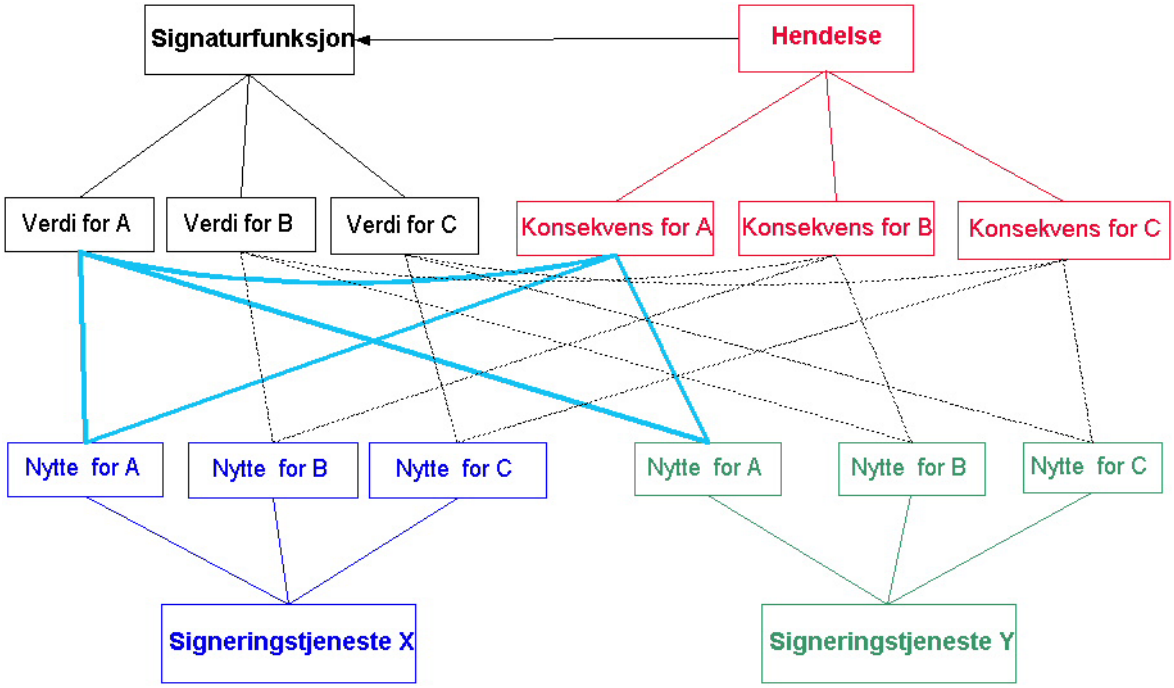


Figur 2 Risikovurdering

Det kan se lett ut å foreta risikovurdering av et slikt lite system der det ikke er krav om konfidensialitet. Vi har hatt stort utbytte av å gå ordentlig inn i risikovurderingen. En offentlig institusjon kan sjelden se bare på egne behov. Den må vurdere hva regelverket uttrykker, hvilke ulike behov publikum,

regelforvaltere, saksbehandlere, mottakere av informasjonen og andre har opp mot hverandre.

Da vi gikk dypere ned i vurderingen så vi mange eksempler på at de ulike interessentene har ulik nytte av ulike signaturfunksjoner, jfr. Figur 3 Risikoanalyse for flere interessenter. En signaturfunksjon, som å autentisere ansvarlig søker, har én verdi for kommunen (A) og kanskje en annen verdi for tiltakshaver (B). Dersom det skjer en uønsket hendelse i ByggSøksystemet slik at f.eks. autentiseringen av ansvarlig søker ikke kan gjennomføres på det aktuelle tidspunktet, kan det få ulike konsekvenser for kommunen og for tiltakshaver. Signeringstjeneste X kan redusere uønskete konsekvenser for kommunen, men kanskje ikke for tiltakshaver. Derimot kan signeringstjeneste Y redusere risikoen for begge.



Figur 3 Risikoanalyse for flere interessenter

Den tykke (blå) streken viser vurderingen for interessent A, hvilke verdier A ser for en bestemt signaturfunksjon, konsekvensene for A ved en uønsket hendelse og nytten A kan ha av signeringstjeneste X i forhold til signeringstjeneste Y. Disse betraktningene må veies mot hverandre og sees i forhold til konsekvensene for andre interessenter. Regelforvalter må deretter bestemme signeringsteknikk for hver signatar.

5.1.3 Risikoer i en elektronisk verden

Det er vesentlig for søkernes tillit til byggesøknadsprosessen at papirsøknader og elektroniske søknader behandles likt av kommunene. Det innebærer bl.a. at

søkerne må føle seg trygge på at de ikke mister noen steg i søknadsprosessen når ByggSøk "bygger opp" den elektroniske søknaden.

De ulike interessentene kan ofte ha ulike vurderinger av hva som er vesentlig for dem i tilfelle en uønsket hendelse inntreffer. Uønskede hendelser kan være

- at en ansvarlig utførende påstår og signerer på at han har større kompetanse enn det som er dokumentert,
- at ikke alle naboene varsles,
- at ikke kommunen har tid til å verifisere alle innkomne opplysninger.

En risikovurdering må derfor se på alle interessentenes interesser i forhold til hver enkelt større uønskete hendelse, og hvilke teknikker som reduserer risikoene til akseptable nivåer. En offentlig institusjon skal ikke se bruken av systemet bare fra egen side, men ta hensyn til hvilken nytte og hvilken risiko alle aktuelle aktører kan oppleve ved at det systemet blir brukt. Vanligvis vil bare en slik forståelse gjøre at systemet tas i bruk i stort omfang.

Ulike signaturløsninger koster forskjellig for de forskjellige aktørene. Det er f.eks. dyrt å legge til rette for at allmennheten skal ta i bruk digitale signaturer i 'alle' sammenhenger. Mens det kan være rimeligere å la noen brukergrupper teste det. Det vil også være dyrt for kommunene hvis de skal verifisere alle slags sertifikater og benytte sertifikatinformasjonen inn i egne saksbehandlingssystemer. På den annen side er bruker-ID og passord billig for alle, men hvis noe galt skjer, kan det bli dyrt i hvert enkelt tilfelle og det kan tenkes at det ikke gir god nok sikkerhet totalt sett.

I alle tilfeller må kommunene legge til rette for å kunne motta elektroniske søknader på en forsvarlig måte.

5.1.4 Analyseobjekter

Hovedobjektet for analysen vår er de funksjonene som regelkravene om signatur står for. Som tidligere nevnt fins det ikke så mange krav om signering av byggesøknader i regelverket. Det står ingenting uttrykkelig om hva hensikten/funksjonaliteten med signaturene er. Det står en del om ansvar og opplysningsplikt som ikke er knyttet til signering direkte. Ett spørsmål er om det er vesentlig å kunne bevise at rette vedkommende har signert og dermed plassere ansvaret, eller om det er viktigst at noen har signert, f.eks. for at søknaden i det hele tatt kan behandles. Hvis det i mange av tilfellene bare er at en eller annen signerer, så kan det bli et internt oppgjør i firmaet hvis noen har signert på gale premisser.

Lov om elektronisk signatur stiller ikke krav om at elektronisk signatur må brukes, se første rapport [17]. Den åpner for at *enhver* elektronisk signatur kan være rettslig gyldig. Med elektronisk signatur mener loven 'noe' som brukes som *autentiseringsmetode.* Plan- og bygningsloven med forskrifter gir heller ikke anvisning på noen bestemt måte å 'undertegne' på. Rettslig sett er det følgelig åpent for mange signeringsmekanismer. Disse dekker begrepet signering på ulike måter. Det er derfor aktuelt å se på signeringsmekanismer/-

teknikker sammen med rutiner rundt signeringssituasjonene. Et eksempel er at i tillegg til en elektronisk signatur, enten den er digital eller noe annet, så bør det komme fram en melding til signataren om at 'nå må du være klar over hva du gjør'. Ved signering på papir er man klar over at man signerer og har en viss forståelse for hva det innebærer i hvert enkelt tilfelle. Det kan være vanskeligere ved elektronisk søknadsutfylling. Hvis systemet ikke utrykkelig sier fra om at nå signerer du, så kan signataren unngå å oppfatte det og bli ansvarlig for noe uten å vite det.

Vi har også sett på noen generelle risikoaspektene ved å sende inn en elektronisk søknad i forhold til regelverkets intensjoner.

5.1.5 Roller og interessenter

I plan- og bygningsloven, *pbl* [13], og forskriften til plan- og bygnigsloven om saksbehandling og kontroll, *SAK* [12], har vi funnet følgende roller knyttet til signering og det å påta seg et ansvar ved innsendelse av en byggesøknad:

AS	Ansvarlig søker	AUF	Ansvarlig utførende
TH	Tiltakshaver	AK	Kontrollansvarlig
AP	Ansvarlig prosjekterende	AF	Ansvarlig foretak
ASam	Ansvarlig samordner		

Ansvarlig foretak er, slik vi forstår det, et overordnet begrep for AS, AP, ASam, AUF og AK.

Vi ser fire større roller som skiller seg fra hverandre i søknadsprosessen.

Tiltakshaver eier oftest tomta der noe skal bygges og er dermed en viktig interessent rundt bruken av ByggSøk. Tiltakshaver forstår neppe alt som står i søknadene, og tilslutter seg tiltaket på en overordnet måte. Det kan tenkes at det er en feil tolkning fra vår side og at det er tiltakshaver som har det egentlige ansvaret. Det kommer ikke fram i loven hvilket ansvar tiltakshaver påtar seg ved å signere, men det er klart at han kan bli skadelidende hvis søknadene ikke er korrekte og fullstendige.

Ansvarlig søker er profesjonell aktør på en annen måte enn tiltakshaver. Han har ansvar for hele søknadsprosessen og for at søknaden er korrekt og fullstendig i forhold til kravene i regelverket. Det er et stort ansvar. Det er viktig at søkeren er klar over både ansvaret og straffeansvaret som følger med.

Ansvarlig søker og de andre aktørene som opptrer i regelverket har det til felles, at de har kompetanse på områder som er vesentlige for å gjennomføre byggeprosessen. "De andre" aktørene har bare ansvar for sin avgrensete del av søknaden og gjennomføringen av byggeprosessen. De må bli gjort klar over ansvaret ved å signere uriktig. Dette skiller alle disse aktørene fra tiltakshaver, som vanligvis har andre forutsetninger for å forstå innholdet i byggesøknaden.

Kommunene som mottar søknader elektronisk. De må kunne ta i mot dem, sjekke ekthet og kunne bruke informasjonen videre innover i egne systemer

Det fins i tillegg følgende interessenter rundt byggesøknaden:

- Regelforvalter, KRD, som er opptatt av at systemet gjenspeiler regelverket.
- Statens byggtekniske etat, BE, som eier og drifter datasystemet ByggSøk
- Systemutviklerne som lager systemet.
- Naboer og gjenboere

5.1.6 Signaturfunksjoner

Byggesøknader skal undertegnes. En del steder i pbl står det ikke noe om signering av dokumenter. I stedet kan det stå 'skriftlig', 'påta seg ansvar', 'søke', 'forplikte seg'. Dette er uttrykk som vi forbinder med signering på papir og der det er rimelig å finne brukbare elektroniske signaturteknikker som kan dekke de samme funksjonene på en tilsvarende måte.

Særlig 'underskrive', 'forplikte seg' og å 'påta seg ansvar' er uttrykk i regelverket som det er naturlig å forbinde med ikke-benekting, dvs. at man ikke kan frasi seg å ha knyttet seg til søknaden. Det innebærer at både den som skal signere en søknad og den som mottar søknaden, er interessert i at det er riktig signatar. En som påtar seg et ansvar, skal ikke ha støtte for å hevde at han ikke har gjort det. Og mottakeren av søknaden skal kunne føle seg trygg på at signataren har påtatt seg ansvaret. Ikke-benekting kan realiseres som en sikkerhetstjeneste som genererer og sanker bevis for hendelser[8]. Hvor sterke bevisene regnes for å være, vil variere med hva slags teknikker og rutiner som benyttes. Hvor vesentlig det er å sanke slike bevis, vil avhenge av hvem som trenger dem og hva de skal brukes til. Det kan likevel tenkes at *ikke-benekting* ikke er på linje med de andre signaturfunksjonene. Det å ikke kunne nekte for noe, kan gjelde i forhold til både identifisering, autentisering, ansvar osv.

'Gi opplysninger', 'vise fordeling av ansvar' og 'sørge for' kan være svakere uttrykk som ikke behøver å være knyttet til ikke-benekting. Hvis det mangler informasjon om noe ved byggeprosessen, som signataren kan ha utelatt ut fra manglende forståelse for hva en fullstendig søknad skal inneholde, så vet kommunen ut fra de andre søknadspapirene hvem den skal henvende seg til.

Vi mener at følgende signaturfunksjoner er aktuelle i forhold til ByggSøk:

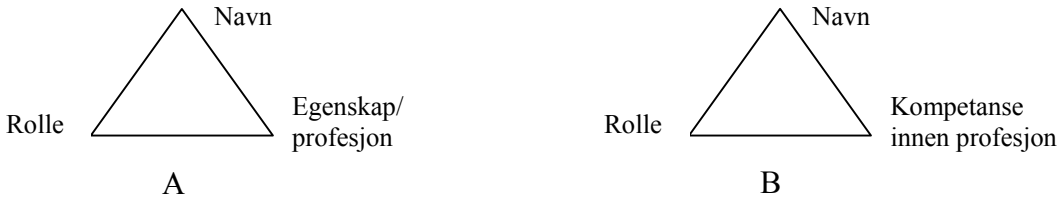
Identifisere I denne sammenhengen definerer vi det til å 1) få fram et navn på en person eller foretak, 2) knytte et navn til en rolle, f.eks. Kari Buer er *tiltakshaver*, Agra Prosjektering er *ansvarlig søker*, Ove Meyer er *ansvarlig utførende* på et område.

Autentisere Å verifisere at noe er fullt ut ekte og pålitelig [1]. Det kan gjelde f.eks. dokumenter, personer eller egenskaper. Når man har knyttet et navn til en rolle (identifisering, betraktes ofte som del av autentisering), trenger ByggSøk å verifisere at rolleinnehaveren har riktig egenskap i forhold til rollen. Rollen *tiltakshaver* har egenskapen å være eier av en tomt, mens rollen *ansvarlig foretak* har ulike profesjoner som egenskap, f.eks. arkitekt, rørlegger eller snekker, se
Figur 4 A. I begge tilfellene sjekker man ekthet vha. en tiltrodd tredjepart (i dette tilfellet nedre høyre hjørne i trekanten). Tomteeierskap sjekkes via GAB, mens

[8] ISO/IEC FCD 13888-1, 2002: *to generate, collect, maintain, make available and verify evidence concerning a claimed event or action in order to resolve disputes about the occurrence of the event or action.*

profesjoner sjekkes via sentralt godkjenningsregister eller gjennom lokal godkjenning ved å kontrollere tilsendte vitnemål osv.

Ved søknad om f.eks. ansvarsrett innenfor et område, vil autentiseringen/-sjekkingen av ekthet gå dypere. Da vurderer kommunen om kompetansen innen profesjonsområdet er dekkende for det som skal utføres, se Figur 4 B. (Kommunen autentiserer autorisasjonen.) Eksempel på den type autentisering er å gå inn i sentralt godkjenningsregister og sjekke om rørleggeren har lov til utføre den type rørleggerarbeid som står beskrevet i søknaden.



Figur 4 Autentisering

Ansvar Knytte en oppgitt identitet til et bestemt innhold (tiltakshaver, ansvarlig søker, prosjekterende avgir en viljeserklæring, påtar seg et bestemt ansvar for å utføre noe).

Opplyse Knytte en oppgitt identitet til et bestemt innhold (tiltakshaver, ansvarlig søker, prosjekterende som går god for opplysninger/fakta/vurderinger). Å påta seg et ansvar og å gi opplysninger om saksforhold kan etter vår mening gi ulike risiko-vurderinger. Noen gale opplysninger kan sikkert skape alvorlige problemer og gi straffeansvar, men plan- og byggingsloven påpeker særlig straffeansvar i forhold til utførelsen av arbeidet en aktør påtar seg. Vi mener derfor at det er fornuftig å se ansvar og opplysningsplikt hver for seg selv om det sannsynligvis er en glidende overgang mellom dem.

Vedkjenningsfunksjon I dette tilfellet er det å forstå at man knytter seg til en byggesøknad. Det kan sees som en overordnet funksjon ved det å signere noe, og det henger etter vår mening sammen med begrepet ikke-benekting. Når man signerer og vedkjenner seg noe, skal det være vanskelig å unndra seg. I papirverdenen er man som oftest klar over at man blir med på noe når man signerer. Det må tydeliggjøres på en elektronisk søknad.

Avslutningsfunksjon Man markerer at søknaden er ferdigskrevet/ikke lenger er et uferdig utkast. Handlingen gir kommunen grunnlag for å akseptere søknaden som korrekt utfylt i hht. kravene i regelverket, for dermed å starte søknadsbehandlingen.

5.1.7 Kopling av regelverk og signeringsfunksjoner

Tabellen nedenfor viser hver enkelt paragraf der det står noe om å undertegne eller å påta seg et ansvar. Vi analyserte regelteksten for å identifisere hvilke funksjoner som er knyttet til den og hver enkelt rolle. Dette har så dannet grunnlaget for risikoanalysen.

Følgende forkortelser benyttes:

AS	Ansvarlig søker	AUF	Ansvarlig utførende
TH	Tiltakshaver	AK	Kontrollansvarlig
AP	Ansvarlig prosjekterende	AF	Ansvarlig foretak
ASam	Ansvarlig samordner	pbl	Plan- og bygningsloven
SAK	forskriften til plan- og bygningsloven om saksbehandling og kontroll		

Tabell 1 Regel, rolle og funksjon

Paragraf	Regeltekst	Rolle	Funksjon
Pbl §81, 86 a, pkt. b, SAK §20, 21	Undertegne	TH	Autentisere
§ 93 b 1	Undertegne	TH	Autentisere
Pbl § 93 b 1	Undertegne	AS	Identifisere og autentisere
§ 97 4	Skifte av tiltakshaver	TH	Autentisere
	All søknad om ansvarsrett	AF	Autentisere
SAK 14 2	Ansvar for del av prosjektering	AP	Ansvar
§ 93b 1	Ansvar for innholdet av sin del av prosjekteringen	AP	Ansvar
SAK 14	Ansvar for kontrollplan og kontrollform for utførelse	AP	Ansvar
§ 97 1, SAK §14 6	Ansvar for kontrollplan med kontrollform for utførelse	AF	Ansvar
SAK § 15 2	Ansvar for samordning	ASam	Ansvar
§ 93 b 1	Knytte seg til søknaden	TH	Ansvar
§ 29 2	Kontrollerklæring	AK	Ansvar
pbl § 93 b 1	Påta seg å være bindeledd	AS	Ansvar
§ 98 2	Søke ansvarsrett for utførelse	AUF	Ansvar
§ 94 1	Søknad om ansvarsrett for utførelse og kontroll	?	Ansvar
pbl §81, 86 a, pkt. b, SAK §20, 21	Ta ansvar for at tiltaket følger aktuelle krav	TH	Ansvar
SAK § 15 2	Ta ansvar for utførelse av sin del	AUF	Ansvar
§ 94 3	Ta ansvar for å varsle naboer	AS	Ansvar
pbl §81, 86 a, pkt. b, SAK §20, 21, og pbl § 93 b 1	Signere søknad	TH	Avslutte
pbl § 93 b 1	Signere søknad	AS	Avslutte
pbl § 93 b 1	Signere prosjektoppdeling	AP	Avslutte
SAK § 14 3	Forpliktelse til å la utføre kontroller for prosjektering	TH	Forplikte?
§ 94 1	Gi alle opplysninger for at kommunen kan ta standpunkt	AS	Opplyse
§ 93 b 1	Gi nødvendige opplysninger for å kunne utføre kontroll	TH	Opplyse
pbl § 93 b 1	Gi nødvendige opplysninger for å kunne utføre kontroll	AS	Opplyse
§ 94 2	Opplyse at saken er lagt fram for annen myndighet	AS	Opplyse
pbl § 93 b 1	Samordne søknaden	AS	Opplyse
pbl § 93 b 1, SAK 14 4	Sørge for all dokumentasjon om	AS	Opplyse?

Paragraf	Regeltekst	Rolle	Funksjon
	hvorledes alle relevante krav skal oppfylles		
pbl § 93 b 1, SAK 14 1	Søke lokal godkjenning	AS	Opplyse
§ 98 2, SAK §§ 14 1, 15 4	Søke godkjenning	AUF	Opplyse
§ 98 3, SAK § 15 4	Søknad godkjenning	ASam	Opplyse
§ 93b 2, SAK § 14 1, § 15 4	Søke godkjenning	AP	Opplyse
§ 93b 2	Søke godkjenning	AF	Opplyse
§ 93b 2, SAK § 14 1	Søke godkjenning for aktuelt oppdrag	AF	Opplyse
pbl §81, 86 a, pkt. b, SAK §20, 21	Ta ansvar for at alle nødvendige opplysninger er gitt	TH	Opplyse
pbl § 93 b 1, SAK 14 2	Vise prosjekteringsoppdelingen	AS	Opplyse
SAK § 15 2	Vise fordeling av ansvar for samordning og utførelse	AS	Opplyse
SAK § 15 3, 4	Erklære at detaljprosjekteringen er kontrollert	AF	Vedkjenne
§ 93 b 1	Signere	TH	Vedkjenne
pbl § 93 b 1	Signere	AS	Vedkjenne
§ 97 4	Skifte av tiltakshaver	TH	Vedkjenne

De ulike interessentene har ulike interesser av hver enkelt signatur, jfr. Figur 3 Risikoanalyse for flere interessenter. Et ansvarlig foretak kan oppleve søknads-prosessen med all informasjon som skal avleveres, som omstendelig. Mens regelforvalter, kommuner og tiltakshaver opplever at de får bedre oversikt og ansvarsplassering i forhold til arbeidet som skal utføres

5.1.8 Aktuelle signeringsteknikker

Vi så på tre hovedmåter å signere på i forhold til ByggSøk:

- **Digitale signaturer** med sertifikater og med meldinger som presiserer hva signeringen gjelder.
- ByggSøks nåværende bruk av **bruker-ID og passord**, med eventuelt ekstra meldinger med avkrysningsboks som presiserer hva ”signeringen” gjelder (her i ” ” fordi det ikke er så lett å assosiere denne teknikken med håndskreven underskrift).
- **Oslo kommunes variant**. Søknaden sendes elektronisk uten underskrift. Alle aktørene signerer for hånd på et ark der de påtar seg ansvaret for sin del av søknaden. Arket fakses kommunen og lagres elektronisk.

Vi har risikovurdert de to første fordi de begge er elektroniske teknikker.

Oslo kommunes variant kombinerer elektronikk og papir, og gir etter vår vurdering et akseptabelt risikonivå. Den er en rimelig løsning, for alle parter. Den sinker ikke søknadsbehandlingen nevneverdig. Den gir en god form for knytning mellom oppgitt ID og søknaden, med ansvar som følger med, og i tillegg gir den god støtte for ikke-benekting. Alle aktørene kan oppbevare hver sin utgave av det de har signert.

5.2 Risikovurdering av signaturfunksjoner

Da vi gjennomførte risikovurderingen så vi på:

- Roller med aktuelle signeringsfunksjoner i lys av regelverket og verdivurdering for ulike interessenter
- Uønskede hendelser, hvem som kunne tenkes å utføre dem, hva som kunne tenkes å skje, sannsynligheten for at de ville opptre
- Konsekvenser for ulike aktører hvis hendelsen inntreffer
- To ulike signeringsteknikker, hva hver kan bidra med mot den uønskede hendelsen og hva de eventuelt ikke kan bidra med, en grov kostnadsvurdering og en risikovurdering i forhold til signeringsteknikken
- Vurdering

En sammenstilling av vurderingene for ulike signaturfunksjoner følger nedenfor. Et utdrag av selve vurderingen er i Vedlegg 1.

5.2.1 Identifisering og autentisering

Vi har sett på funksjoner som vurderes ut fra type regelkrav: identifisering og autentisering av tiltakshaver, ansvarlig søker og andre ansvarlige foretak.

Kommunen trenger å vite hvem som står bak en søknad, bl.a. som et kriterium for i det hele tatt å starte saksbehandlingen.

Uønskete hendelser kan være at det er ikke oppgitt navn, eller at noen feilaktig utgir seg for å være tiltakshaver eller ansvarlig søker.

Verken teoretisk eller i praksis antas dette å hende ofte (lav sannsynlighet). Hvis det derimot skjer, vil det kunne ha uheldige konsekvenser, dels prosess-økonomisk for selve saksbehandlingen, dels for dem som påføres den konkrete feilen. En kan tenke seg utførte arbeider på feil tomt. Tilsvarende kan det være fare for vedtak på feil grunnlag (for eksempel om riving). I begge tilfeller kan hovedproblemet være av privatrettslig karakter, men det vil også være fare for tap av anseelse for det offentlige som eventuelt ikke har hindret feilen, selv om det rettslig sett ikke skulle være en del av deres ansvar. En ansvarlig søker kan få svekket tillit i kommunen eller i bransjen/markedet. Tidlig identifisering og autentisering er av verdi rent prosessøkonomisk (færre sendinger frem og tilbake, med unødvendig ressursbruk og frustrasjon på både sender- og mottakersiden).

Ved å ta i bruk *digital signatur* som tilgangsmekanisme vil man få meget god identifisering generelt (forutsatt god kontroll ved tildeling av sertifikat). Man vil også kunne få en meget god autentisering av navn, på tiltakshaver og ansvarlig søker. Den digitale signaturen vil ikke i seg selv kunne si om en person har rollen som tiltakshaver eller ikke. Det må fremgå på annen måte, av det elektroniske søknadsskjemaet (som i dag). Den digitale signaturen kan heller ikke gi noen kopling mellom tiltakshaver og opplysninger om hvem som

eier tomten. Den koplingen må kommunen finne på annet vis ved å se på navn på andre sakspapirer, så som informasjon fra GAB-registeret.

For ansvarlig søker kan man imidlertid lage en kobling mot ByggSøks bruker-identifikasjon og et søknadsnummer, og dermed skaffe bekreftelse på om oppgitt identitet (også) har rollen som ansvarlig søker. I tillegg (og uavhengig av digital signatur) vil kontroll mot sentralt godkjenningsregister gi svar på om den oppgitte identitet er registrert som ansvarlig foretak eller ikke. Risikoen knyttet til funksjonene identitet og autentisitet vil være lav ved bruk av digital signatur.

Ved å ta i bruk *bruker-ID og passord* (som ByggSøk bruker i dag) kan man få en god identifisering og autentisering. Også for denne signaturteknikken må eventuelt rollene som tiltakshaver og ansvarlig søker fremgå på andre måter enn ved selve signaturteknikken, på tilsvarende måte som for digital signatur nevnt over. Autentisering av *tiltakshaver* er neppe nødvendig. Det fins tiltakshavere som starter bygging der de ikke har lov, men det er så få saker at det kan løses manuelt i de kommunene det oppstår. Vi kan ikke se at det gir stor risiko å ikke autentisere tiltakshaver. På dette området bør det derfor holde med bruker-ID og passord dersom tiltakshaver skal ha tilgang til den elektroniske søknaden.

For *ansvarlig søker* kan bruker-ID og passord være knyttet til sentralt godkjenningsregister. Autentisering av ansvarlig søker er avhengig av registrering i et tilgjengelig godkjenningsregister.

Hvis passordet blir tilgjengelig for uvedkommende eller en utro tjener, vil sikkerheten være kompromittert. Dette er et kjent forhold i mange sammenhenger hvor passord og lignende brukes. Vi vurderer imidlertid at konsekvensene, sammenholdt for alle interessenter, knyttet til fusk eller feil ved funksjonene identitet og autentisitet, vil være lave ved bruker-ID og passord.

Vi har gjort tilsvarende vurderinger i forbindelse med identifisering og autentisering av andre ansvarlige foretak (ansvarlig prosjekterende, utførende og kontrollerende).

Dersom identiteten til et *ansvarlig foretak* ikke lar seg autentisere, kan søknaden returneres. Det vil kunne oppfattes som byråkrati av noen av foretakene. Men den problemstillingen er ikke vanskeligere elektronisk enn for papirsøknader. Etter vår vurdering gir det en viss risiko for forsinkelse eller feil i saksbehandlingen hvis ikke ansvarlige foretak identifiseres og autentiseres. Men behovet for autentisering varierer og må sees i sammenheng med ansvaret som foretaket knytter seg til ellers i søknaden.

5.2.2 Ansvarsfunksjon

I mange paragrafer fremgår det hvilket ansvar de ulike aktørene har. Ansvar som er uttrykt i regelverket, står der uansett måten det signeres på, og uansett hvor bevisst signataren er i det øyeblikket signeringshandlingen foretas. Rettsvillfarelse er ikke lett å påberope seg som unnskyldning for ikke å følge (eller ikke ha skjønt) regelverket og ansvaret som ligger i det. Men underskriften kan

sies å være regelverkets måte å kople det enkelte individ, med sin rolle, til den enkelte byggesøknad og -sak (med underliggende regelverk og ansvar).

Foretak som skal ha ansvar for utførelse eller kontroll påtar seg straffeansvar i hht. regelverket. Dette kan være områder kommunen kan ønske å forfølge i ettertid hvis det skjer noe galt i byggeprosessen. Særlig påtar *ansvarlig søker* seg et stort ansvar. Uønskede hendelser kan være at signatar påberoper seg større kompetanse enn han har godkjenning for, eller at han sender ufullstendig utfylling av ansvarsoppgaver. Dette er derfor et område der både kommune og tiltakshaver kan være interessert i egenskapen ikke-benekting. Det regnes for vanskeligere å benekte å ha signert med en digital signatur enn hvis det brukes bruker-ID og passord. Uavhengig av signeringsteknikken vil det hjelpe for søknadsutfyllingen og for søknadsbehandlingen hvis signatar blir gjort utrykkelig oppmerksom på ansvaret han påtar seg. Det kan gjøres ved at man ikke kommer videre før man har klikket på et felt som sier 'Ja, jeg forstår at jeg påtar meg ansvar på dette området!'.

5.2.3 Opplysningsfunksjon

Regelverket krever mange opplysninger som grunnlag for å saksbehandle byggesaken. Men det er i stor grad opplysninger som man gir etter beste skjønn, og mange av dem kan ettersendes uten at søknadsprosessen stopper. ByggSøk er, som tidligere nevnt, ikke laget slik at søker får veiledning til fullstendig og korrekt søknadsutfyllelse. Vi ser derfor ikke mangel på korrekte opplysninger som en, generelt, stor risiko. Likevel kan opplysninger om feil kompetanse være regelbrudd. Også her ser vi behov for en uthevet melding om at man skal gi opplysningene som kreves. Underskriften er neppe noe avgjørende eller viktig bindeledd mellom signatar og opplysningsplikten iht. reglene.

5.2.4 Vedkjenningsfunksjon

Vedkjenningsfunksjonen kan sees som en overordnet varsling til signatar om at nå vedkjenner du deg noe. Kommune og tiltakshaver er spesielt opptatt av at *ansvarlig kontrollerende* og *ansvarlig utførende* vedkjenner seg arbeidet som skal gjøres. Dårlig utført arbeid, kan derfor resultere i reaksjoner, privatrettslige eller fra kommunen. En annen trussel kan være en som gir seg ut for å være *tiltakshaver* uten å være det, og deretter utfører byggearbeider på tiltakshavers tomt. Det kan føre til privatrettslig tvist eller til at kommunen krever riving av bygget. Risikoen for denne typen hendelser vet vi at er tilstede. Teknikker for ikke-benekting kan derfor være ønskelig. I alle fall trenger signataren et varsel om alvoret i handlingen.

Hvis egenskapen *ikke-benekting* er vesentlig ved signeringssituasjonen, så gir digitale signaturer den mest forsvarlige elektroniske løsningen. Den kan brukes for alle som signerer sin del av søknaden. Informasjonen som man skal ved-kjenne seg og ikke bør kunne benekte, knyttes vha. kryptografiske teknikker til den digitale signaturen for hver enkelt signatar. Bruker-ID og passord kan gi en viss grad av ikke-benekting for ansvarlig søker dersom ByggSøk utvikles slik at bare ansvarlig søker kan fylle ut alle feltene. Det vil være på et langt lavere

sikkerhetsnivå i og med at det er enklere å knekke et passord enn en digital signatur. "Signatur" ved hjelp av bruker-ID og passord knyttes ikke til innformasjonen man skal vedkjenne seg på samme måte som en digital signatur knytter sammen teksten og eieren av den private signeringsnøkkelen.

Ikke-benekting for alle signatarer via bruker-ID og passord vil bli for komplekst å administrere for de mange ulike søknadstypene. De forskjellige ansvarlige foretakene skal signere over til dels samme tekst i en og samme søknad, og det er vanskelig å finne og administrere mekanismer som gir trygghet for at ansvarlig kontrollør ikke har endret teksten som ansvarlig søker har skrevet inn.

5.2.5 Avslutningsfunksjon

Ansvarlig søker skal signere hele søknaden. Det er et tegn på at søknaden er ferdig utfylt og at den er klar for saksbehandling i kommunen. Andre signatarer avslutter også sine deler av søknaden med signatur. En uønsket hendelse for alle interessentene er at søknaden likevel ikke er ferdig utfylt. Det vil det fortsatt være risiko for med et elektronisk søknadssystem uavhengig av signeringsteknikken. Men konsekvensen er bare at søknaden sendes i retur og gir lenger behandlingstid/prosess.

5.2.6 Risiko knyttet til ByggSøk-system generelt

Papirutgaven av en byggesøknad er én måte å operasjonalisere teksten i lovverket på. Et skjema med felter gjør det lettere for brukerne å etterleve reglene, og lettere for kommunen å administrere sakene iht. reglene. Noen steder kan vi ikke se at det eksisterer krav om signatur i regelverket, men det kan være naturlig å gjennomføre intensjonen i teksten ved å kreve underskrifter. På noen av søknadsskjemaene er det knyttet krav til underskrifter som vi ikke finner eksplisitt i regelverket.

Et elektronisk byggsøkesystem kan lett bli en annen måte å operasjonalisere regelverket på. De to søkemåtene skal eksistere i parallell over flere år, og utviklerne må passe på at ingen av dem avviker vesentlig fra intensjonene i regelverket. Det er en stor risiko for at de vil avvike fra hverandre siden de operasjonaliserer regelverket på ulike måter blant annet pga. ulik teknologi. Signatarene skal sikres at de bare signerer det de skal signere i hht. regelverket.

Én trussel kan være at sentrale krav i regelverket representeres feil i systemet og at signatar dermed får feil veiledning ved søknadsutfylling. Dette er en kjent problemstilling for alle som spesifiserer og utvikler datasystemer i hht. et regelverk. Det mest anerkjente mottiltaket mot unøyaktig systemutvikling, er å følge aksepterte systemutviklingsmetoder med inspeksjoner mellom de ulike fasene, med deltakelse også av juridiske eksperter, og å dokumentere systemet.

Et annet risikomoment er om man klarer å sikre at signaturmekanismene ikke er sterkere, mer komplekse eller dyrere enn nødvendig. Hvis noe av dette er tilfelle, kan det bli en dyr og ressurskrevende løsning for alle interessenter, jfr. f.eks. punkt 3.6.3. Det beste mottiltaket er å jevnlig foreta risikovurderinger,

slik BE gjør nå på signaturområdet, for å finne akseptabelt risikonivå ut fra den kunnskapen man har på det tidspunktet vurderingen gjennomføres.

5.2.7 Kan departementet bestemme hvordan signaturfunksjonene skal ivaretas?

På papirsøknadene signerer de ulike aktørene diverse vedlegg, kanskje flere enn regelverket strengt tatt tilsier. Men signaturene ser like ut for hver signatar. Ved gjennomgang av regelverket har vi sett at aktørene knytter seg til søknaden på ulike måter, ved å gi opplysninger om noe, ved å påta seg ansvar for noe som skal gjøres eller ved å påta seg rollen som tiltakshaver. Dette kan løses teknisk på forskjellige måter avhengig av hvor alvorlig hver tilknytning er og hvilken risiko man løper ved hver tilknytning.

Juridisk blir det derfor et spørsmål om regelverket tillater hver aktør å signere én gang, med 'sterkeste signaturmekanisme' over all informasjonen som angår aktøren, eller om det må brukes ulike signaturmekanismer for hver del av søknaden. SAK § 32a har teksten: *Departementet kan fastsette blanketter ved søknad og melding. Blankett fastsatt av departementet kan kreves brukt.* Dette kan tolkes som en hjemmel for departementet til å fastsette en elektronisk blankett, som på enkel og effektivt vis tilfredsstiller de kravene plan- og byggingslovgivningen setter. Man kan f.eks. vurdere å åpne for en svakere elektronisk mellomløsning. Det kan være slik at en del av en søknad ikke trenger ikke-benektning vha. digitale signaturer og at for den delen kan signataren f.eks. krysse av i en boks at han har det navnet som står skrevet i klartekst.

5.2.8 Kostnadsvurderinger

Kostnadene ved å benytte digitale signaturer i ByggSøk-systemet vil sannsynligvis bli høyere for de fleste interessentene enn ved bruk av enklere signaturteknikker. Hvis derimot sertifikater og digitale signaturer er tatt i bruk eller kan tas i bruk mot andre systemer, både på myndighets- og brukersiden, vil kostnadsbildet for en slik løsning også kunne bli annerledes for byggesøknader.

Kostnadene ved løsninger for bruker-ID og passord er generelt lave. BE må holde à jour bruker-ID og passord for ByggSøk, og eventuelt en kopling til et sentralt godkjenningsregister. For tiltakshaver eller ansvarlig søker (signatar) vil det ikke påløpe kostnader. Men de må huske sine brukernavn og passord.

6 Funn og anbefalinger

I risikovurderingen splittet vi opp regelkravene i ulike signaturfunksjoner, og så hvordan de slo ut på ulike måter for ulike interessenter. I et elektronisk byggesøknadssystem, så vil en signatar (kanskje avhengig av rolle) bare signere på én måte for sin del av byggesøknaden, vs. at for hver rolle bør det lages bare én signeringstjeneste som dekker interessentenes behov optimalt.

6.1 Uønskede hendelser som ofte kan inntreffe

Risikovurderingen vår indikerer at følgende uønskede hendelser særlig kan inntreffe:

- Søknaden har ufullstendige opplysninger av ulike slag
- Opplysningene er feil eller ukorrekte
- Det er ikke riktig signatar som har signert
- Signatar er ikke klar over ansvaret ved å signere søknaden.

Alle fire kan være resultat av en ukonsentrert utfylling av søknaden eller resultat av en villet handling. Det blir derfor en videre vurdering om når en feil oppfattes som brudd på regelverk. Uavhengig av signeringsteknikken som velges, bør signataren gjøres oppmerksom på hva han gjør, f.eks. ved å måtte klikke på en av de følgende meldingene for å komme videre:

- ’Har du kontrollert at du har fylt ut alt du skal i søknaden?’
- ’Er opplysningene du har gitt så korrekte som du får til?’
- ’Er du <fornavn> <etternavn> som signerer denne delen av søknaden?’
- ’Er du klar over ansvaret du påtar deg for denne delen av søknaden?’
- eller lignende.

I og med at ByggSøk ikke kan klare å gi veiledning som sikrer fullstendig og korrekt utfylling, blir dette bare hjelpetekster for søkerne. Det vil fortsatt forekomme retur av søknader fra kommunene. Men vi anser hjelpetekstene for å være bevisstgjørende for signatarene og effektivitetsfremmende for saksbehandlingen.

6.2 Når er egenskapen ikke-benekting viktig?

Ikke-benekting, å ikke kunne nekte for / avvise å ha signert en bestemt del av en byggesøknad, er en egenskap ved signeringsfunksjonen som er viktig for noen kombinasjoner av roller og informasjonsinnholdet man signerer i forhold til. Sikkerhetsmessig er det særlig viktig der partene ikke kjenner hverandre og derved ikke har grunn til å ha tillit til hverandre. Dersom kommunen kjenner f.eks. ansvarlig søker fra før, er det mer vesentlig å autentisere signataren.

Våre informanter ga uttrykk for at det sjelden er viktig med ikke-benekting knyttet til *tiltakshaver*, siden problemer som eventuelt oppstår forekommer sjelden og kan behandles individuelt. Derimot er det viktig for saksbehandlingen i kommunene å knytte ikke-benekting til *ansvarlig søkers* signatur. Det vil minske ekstraarbeidet i kommunen.

Behovet for ikke-benekting for *ansvarlige foretak* har vi inntrykk av at varierer med rollen og informasjonsinnholdet. Vi har inntrykk av at det særlig er viktig for *ansvarlig utførende* av større arbeider og for *ansvarlig kontrollerende* av utført arbeid.

6.3 Papirsøknader og elektroniske søknader

Kommunene må kunne motta både papirsøknader og elektroniske søknader en del år framover. Det er derfor vesentlig at søknadene som leveres elektronisk og på papir ikke gir signatarene ulikt ansvar, dvs. de må begge representere teksten i regelgrunnlaget så godt som mulig. Vi har funnet at det er flere underskrifter på papirsøknadene enn det regelverket tilsynelatende krever[9]. I tillegg er det noen steder knyttet tekst om ansvar ved å signere. Dermed står regelforvalter friere til å velge underskriftskrav i det elektroniske skjemaet, og til å nyttiggjøre seg den nye teknologien ved tilpassing av signaturkravene til intensjonene i regelverket. Systemer i offentlig sektor er avhengige av at befolkningen som skal bruke dem har tillit til dem. Et godt grunnlag for å få til det er systemutvikling etter anerkjente metoder, sikkerhetsstrategier og risikovurderinger.

6.4 En mer effektiv byggesaksbehandling

I en startfase bør man etter vår mening vurdere å følge Oslo kommunes løsning med håndskrevne underskrifter som fakses til kommunen og lagres elektronisk der sammen med selve søknaden. Selve den elektroniske søknadsutfyllingen er en god og effektiv hjelp for ansvarlig søker selv om ikke alle kommuner er klare til å motta søknader elektronisk. Kommunene mottar bedre utfylte søknader som de dermed kan viderebehandle raskere i egne systemer. Dette mener vi vil gi en optimal effekt de nærmeste årene før digitale signaturer eller annen teknologi tas i bruk på flere områder.

Vi ser et behov for ikke-benekting særlig overfor ukjente ansvarlige foretak som skal utføre en del av byggingen eller kontrollere det som bygges. Den sikreste måten å realisere det på, er ved hjelp av digitale signaturer. Men det er ikke opplagt at regelforvalter eller kommunene mener de trenger det sikkerhetsnivået. En kommune kan bli kjent med foretaket i løpet av søknadsprosessen. Vi antar at det er uaktuelt for BE eller kommunene å bruke ByggSøk som drivkraft for å ta digitale signaturer i bruk. Men det kan gi nyttig erfaring for

[9] F.eks. pbl § 99 om ferdigattest og SAK §33 om å bekrefte kontroll.

kommuner å starte ett eller flere pilotprosjekter for signatarer som allerede har digitale signaturer og sertifikater i bruk på andre områder.

7 Ordbok

Akseptkriterier: Kriterier basert på forskrifter, standarder, erfaring og/eller teoretisk kunnskap som legges til grunn for beslutninger om akseptabel risiko.

Akseptkriterier kan uttrykkes med ord eller være tallfestet [13] ?

En uønsket hendelse: det man vil beskytte seg mot. Tilfeldige hendelser og villede handlinger.

Fordelingsvirkninger: beskrive virkningene for hver enkelt gruppe på en slik måte som gir beslutningstakeren et best mulig grunnlag for å ta hensyn til dette i vurderingen av tiltaket [5].

Ikke-benekting: en mekanisme som kan knyttes til elektronisk samhandling, og som er slik at de deltakende partene ikke kan benekte å ha deltatt i deler eller hele samhandlingen [1].

Interessent: alle som har et forhold til et datasystem eller prosessen systemet er en del av. I denne sammenhengen er søkere, tiltakshaver, prosjekterende aktører, naboer og lovgiver interessenter.

Konsekvens: Mulig følge av en uønsket hendelse. Konsekvenser kan uttrykkes med ord eller som en tallverdi for omfanget av skader på mennesker, miljø eller materielle verdier [13].?

Konsekvensanalyse: en systematisk kartlegging av fordeler og ulemper knyttet til et konkret prosjekt [1] ?

Kostnadseffektivitetsanalyse: finne tiltak som minimerer kostnadene for å oppnå et gitt mål [1] ?

Nytte-kostnadsanalyse: forsøker i tillegg til en kostnadseffektivitetsanalyse å verdsette nytten av det aktuelle prosjektet [1] ?

Risiko: Uttrykk for den fare som uønskede hendelser representerer for mennesker, miljø eller materielle verdier. Risikoen uttrykkes ved sannsynligheten for og konsekvensene av de uønskede hendelsene [13] ?

Risikoen i et bestemt prosjekt: vil være knyttet til sannsynligheten for avvik fra et forventet resultat [1] ?

Risikoanalyser: fokuserer på skader som systemet blir utsatt for, mens sårbarhetsanalyser har fokus på systemets overlevelsesevne [16]. En systematisk analyse av trusler mot et objekt og den risiko disse innebærer for objektet [7].

Samfunnsøkonomisk lønnsomt: at befolkningen til sammen er villig til å betale minst så mye som tiltaket faktisk koster [1] ?

Signatar: Den som signerer.

Sårbarhet: Uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet [10].

Sårbarhetsanalyse: En systematisk gjennomgang av et system i den hensikt å beregne systemets evne til å motstå trusler og overleve uønskede hendelser, ved å identifisere trusler, klargjøre risiko og evaluere evne til stabilisering av systemet [10]. Det er mer omfattende enn en risikoanalyse med hensyn til det som skjer etter at ulykken har inntruffet. Systemet havner i en annen tilstand som skal normaliseres igjen. Men denne tankegangen inneholder egentlig å se angrep sekvensielt. Det kan komme angrep i ett sett slik at hva som er normaltilstand kan diskuteres og at systemet må jobbe mot mange typer angrep på en gang for å få tilbake en normal tilstand.

Trussel: Ethvert forhold eller enhver enhet med potensiale til å forårsake en uønsket hendelse [10].

Villede (bevisste) handlinger: Handlinger som er planlagte og utførte med overlegg [10].

8 Litteratur

1] Arbeids- og administrasjonsdepartementet: *Veiledning til forskrift om elektronisk kommunikasjon med og i forvaltningen*, 1. juli 2002, http://www.statskonsult.no/prosjekt/Veiledningtileforskrift/index.htm

2] Adams, John: *Cars, cholera, and Cows. The Management of Risk and Uncertainty.* Policy Analysis nr. 335, March 4, 1999.

3] *Bokmålsordboka*. Universitetsforlaget 1990, ISBN 82-00-07667-9

4] Finansdepartementet: *Nytte-kostnadsanalyser. Prinsipper for lønnsomhetsvurderinger i offentlig sektor*, NOU 1997:27

5] Finsansdepartementet: *Nytte-kostnadsanalyser. Veiledning i bruk av lønnsomhetsvurderinger i offentlig sektor*, NOU 1998:16

6] Finansdepartementet: *Veileding i samfunnsøkonomiske analyser*. R-0579 B, Oslo 2000

7] Forbruker- og administrasjonsdepartementet: *Datateknikk og samfunnets sårbarhet*, NOU 1986: 12

8] Galtung, Andreas og Riisnæs, Rolf: *Rettslige aspekter ved digitale signaturer*, Universitetet i Oslo, Mars 1994

9] ISTEV: *Legal Issues of Evidence and Liability in the Provision of Trusted Services (CA and TTP services)* Final Report, October 1998, Istituto per lo Studio della Vulnerabilità delle Società Tecnologicamente Evolute. ftp://ftp.cordis.lu/pub/infosec/docs/legal-final-report.doc [sett 2.11.99]

10] Justis- og politidepartementet: *Et sårbart samfunn*. NOU 2000: 24, 3. juli 2000, ISBN 82-583-0537-9

11] Kommunal- og regionaldepartementet: *Veiledning til forskrift om saksbehandling og kontroll i byggesaker 1977*, SAK, Utgave januar 2002

12] Kommunal- og regionaldepartementet: *Forskrift til plan- og bygningsloven om godkjenning av foretak for ansvarsrett 1977*, GOF, Ajourført med endringer senest ved forskrift 29.august 2001 nr. 1071

13] Miljøverndepartementet: *Lov 1985-06-14 nr 77: Plan- og bygningslov*

14] Norsk Standard 5814: *Krav til risikoanalyser*, Norges standardiseringsforbund (NSF) august 1991.

15] Samtaler med Øivind Rooth, BE

16] Skavland, Einar og Jakobsen, Øyvind Mejdell: *Objekt- og informasjonssikkerhet, metode for risiko- og sårbarhetsanalyse*. Institutt for produksjons- og kvalitetsteknikk, NTNU:

17] Statskonsult: *Elektronisk plan- og byggesaksbehandling og krav om signatur mv. i lover og forskrifter*. 19.09.02

18] Unico as: *Kravspesifikasjon ByggSøk*, Juni 2002

9 Vedlegg

Risikoanalyse – utdrag.

REFERANSER

Tittel:	Signaturkrav, risiko og elektroniske byggesøknader.
Forfatter(e):	Annikken Bonnevie Seip og Amund Eriksen
Statskonsults rapportnummer:	2003:14
Prosjektnummer:	816
Prosjektnavn:	ByggSøk - risikovurdering
Prosjektleder:	Amund Eriksen
Oppdragsgiver(e):	Statens bygningstekniske etat(BE)
Resymé:	Ulike typer elektroniske signaturer dekker ulike sider ved kravet til underskrift i en søknad. Risikoene varierer for ulike brukere (interessenter).
Arbeidsområde:	☐ Styring og resultatorientering ☐ Omstilling og organisasjonsformer ☒ Informasjonsteknologi ☐ Kommunikasjonsutvikling ☐ Internasjonalisering ☐ Lederskapsutvikling
Emneord:	Elektronisk signatur, risiko, byggesøknad
Dato:	November 2003
Sider:	44
Utgiver:	Statskonsult Postboks 8115 Dep 0032 OSLO