

Tilnærming til PKI

Dato: 10.08.04
Versjon: 1.0
Forfatter: Geir Bergersen
Bouvet AS

Innhold

1	Innledning	3
2	Hva er pki.....	4
3	Metodikk	5
3.1	Analyse	5
3.2	Valg.....	6
3.3	Handling.....	8
4	Anvendelser	8
4.1	Målgruppe	8
4.2	Beskrivelse og kategorisering av anvendelser	9
4.3	Funksjonalitet/Nytte.....	11
5	Sikkerhetsbehov	11
5.1	Juridiske krav	11
5.2	Sikkerhetsmessige krav.....	12
5.3	PKI Kravspesifikasjon	13
6	Markedsløsninger.....	13
6.1	Leverandører i det norske markedet	13
6.2	Målgruppe	13
6.3	PKI Løsningsspesifikasjon.....	14
6.4	Kostnader	15
7	Konseptuelle valg.....	16
7.1	Samtrafikkproblemstillingen.....	16
7.2	Eie eller Leie tjenester	17
8	Eksempler på vurderinger	18
8.1	Markedsløsning: BankID	18
8.2	Anvendelse: Byggesøknader.....	19

1 INNLEDNING

Fremover vil flere og flere offentlige tjenester kunne gjøres tilgjengelig over Internett. Dette vil kunne gi det offentlige store administrative besparelser.

”Offentlig elektronisk informasjon skal bli mer brukervennlig og lettere tilgjengelig.”
eNorge 2005

Det er mange typer offentlige tjenester som er aktuelt å tilrettelegge for elektronisk kommunikasjon via Internet. Det kan eksempelvis være løsninger for å gi brukerne tilgang til informasjon fra forvaltningens produksjonssystemer. Eksempel på dette kan være å gi borgere tilgang til status på egen saksbehandling, eller tilgang til informasjon fra GAB-registeret, Folkeregisteret etc. Andre løsninger kan være at brukeren skal avlevere informasjon til det offentlig. Dette kan være ulike typer søknader (byggesøknad, søknad om skjenkebevilling, barnehagesøknad) eller innrapportering. En tredje variant kan være inngåelse av avtaler og kontrakter mellom det offentlige og private aktører over nett.

Denne utviklingen forutsetter at man kan sikre disse funksjonene på en hensiktsmessig måte.

Eksempler på typiske sikkerhetsbehov:

- Sikker identifisering av en person eller system
- Holde konfidensielle dokumenter hemmelig og sikre
- Verifisere hvor dokumenter eller mail kommer fra
- Etablere tidspunkt for når et dokument eller mail ble laget eller sendt
- Muliggjøre sikker kommunikasjon og transaksjoner over intranett, ektranett og internett.
- Leverer sikker tilgang til VPN og/eller applikasjoner
- Sikker kommunikasjon mellom applikasjoner (eks: web browser) og/eller maskiner sikkert og konfidensielt

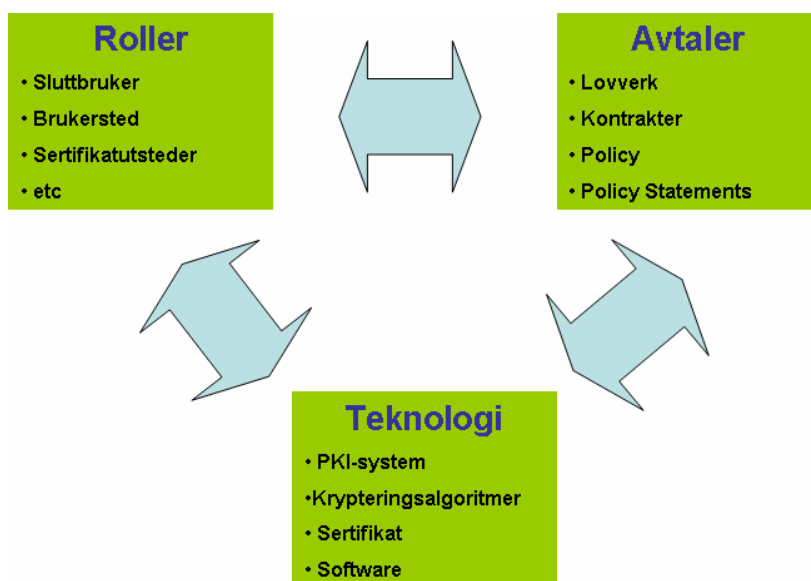
Utfordringen er å løse disse behov på en enkel og oversiktlig måte. Her kan PKI være en nyttig mekanisme.

Dette dokumentet er et forsøk på å gi en lettfattelig forklaring på hva PKI er og hva det kan brukes til, samt gi en metodisk tilnærming til PKI i fm implementering av PKI-støttede tjenester. Dokumentet søker å gi beslutningstakere i kommuner og andre en første oversikt over problematikken og mulighetene.

2 HVA ER PKI

PKI står for ”public key infrastructure” og er en infrastruktur for identifisering og sikring innen datakommunikasjon. Kjernen i en PKI er et såkalt sertifikat som knyttes til en person. Denne personen kan bruke sertifikatet til å identifisere seg elektronisk, samt signere dokumenter etc. PKI er infrastrukturen rundt som sikrer tilliten slik at det er mulig.

En PKI består av tre hoveddeler som må spille sammen på en naturlig måte for å skape nødvendig tillit:



- **Teknologi:**
 - PKI sikrer ved bruk av algoritmer for kryptering og digital signatur, ved hjelp av såkalt nøkler¹. Dette er rett og slett matematiske formler, som gjør det tilnærmet umulig å ”låse” opp informasjon uten bruk av riktig nøkkel.
 - For å sikre at en nøkkel tilhører riktig person, koples person og (offentlig) nøkkel til et sertifikat.
 - I tillegg må det være programmer (software) for utføring av pålogging, signering ved bruk av nøkler og sertifikater etc.
- **Roller:** For å sikre at innholdet i et sertifikat er korrekt og gyldig trenger man en såkalt tiltrodd tredjepart som garanterer for dette, en sertifikatutsteder. En **Sluttbruker** skaffer seg et sertifikat fra **Sertifikatutsteder**. Han benytter sertifikatet på et **Brukersted** for å identifisere seg. **Brukerstedet** må sjekke gyldigheten av det sertifikatet som benyttes. Dette gjøres ved å sende en henvendelse til **Sertifikatutsteder** eller en **Verifiseringsautoritet**. Hvis sluttbrukeren inngår en avtale, kan det være nyttig å bruke en **Tidsstempingstjeneste** som knytter gyldig tid til et dokument. For at dette skal fungere må alle parter stole på hverandre.
- **Avtaler:** Alt fra lover og regler til mellom partene, samt regler om hva PKIen støtter (sikkerhetsnivå etc)..

¹ Man bruker en såkalt privat (kun tilgjengelig for brukeren) nøkkel til å kryptere og en offentlig nøkkel for å dekode.

Tilnærming til PKI

Dato: 22.09.2004

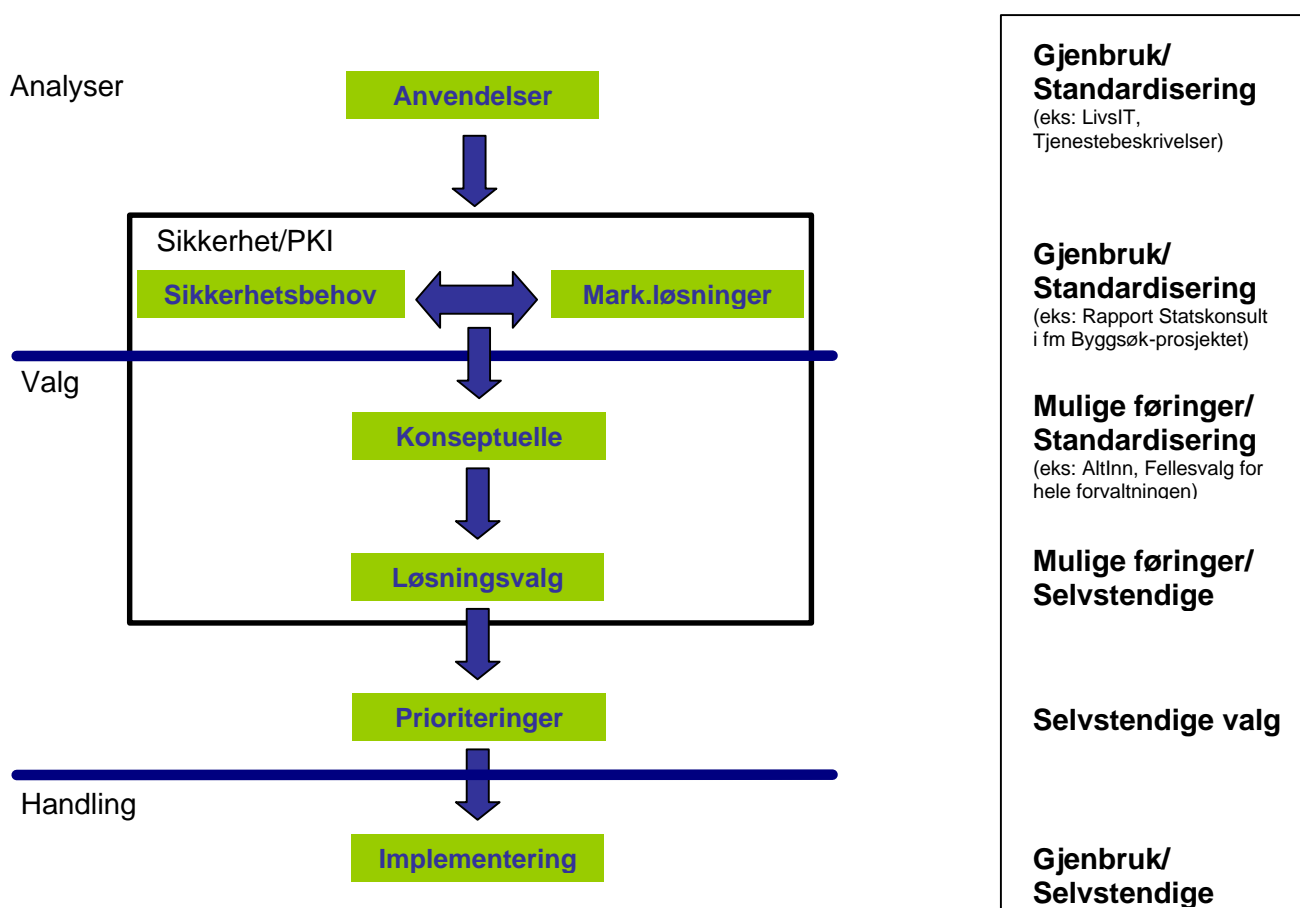
3 METODIKK

Her følger en enkel metodikk for hvordan en organisasjon skal tilnærme seg PKI for å dekke sine sikkerhetsbehov: Hovedbidraget i denne metodikken er forslag til kriterier for hvordan man skal analysere anvendelsene i forhold til PKI, og også hvordan man skal analysere ulike markedsløsninger.

Målet er at beslutningstakere og andre kan gjøre en bevisst vurdering av nye offentlige tjenester som skal presenteres på internett, og hvilke sikkerhetstjenester disse krever.

Vi ønsker å vise hvor det kan og bør komme samordning og fellesinnsats, og hvor det er annonsert at det kommer standarder/føringer som gjør valg enklere og som gir muligheter for gjenbruk av løsninger.

En skjematisk fremstilling av metodikken:



3.1 Analyse

Fase	Hovedaktivitet	Aktiviteter	Mulighet for gjenbruk og standardisering?
------	----------------	-------------	---

Tilnærming til PKI

Dato: 22.09.2004

Analyse	Anvendelser	<ul style="list-style-type: none"> • Definere Målgrupper • Beskrivelser og kategorisering (inkl. beskrive hvem som skal gjøres elektronisk tilgjengelig og vice versa) • Informasjonsmodellering² • Funksjonalitet/Nytte 	Ja. Beskrivelser og kategorisering bør standardiseres (eks. LivsIt, KS Tjenestebeskrivelser).. Bør delvis kunne gjøre felles og gjenbrukes for alle kommuner.
	Sikkerhetsbehov	<ul style="list-style-type: none"> • Juridiske • Sikkerhetsmessige 	Ja. Vurderinger bør ha allmenn gyldighet, og kunne standardiseres og gjenbrukes hos andre kommuner (eks. Statskonsultrapporter i fm Byggsøk-prosjektet)
	Markedsløsninger	<ul style="list-style-type: none"> • Beskrive Målgrupper • PKI • Løsningsspesifikasjon • Kostnader 	Ja. Bør kunne standardiseres og gjøres felles for alle.

Forutsetningen for å gjøre riktig valg mht konsepter og løsninger er gode analyser.

3.2 Valg

Fase	Hovedaktivitet	Aktivitet	Mulighet for gjenbruk og standardisering?
Valg	Konseptuelle	<ul style="list-style-type: none"> • Lukket vs åpen Brukergruppe³ • Tjenestesikring vs Skallsikring • Eie eller Leie tjenester 	Her kan det komme standardisering og føringer/overordnede valg fra departementer og andre sentrale instanser. Mulige eksempler på dette er AltInn som nasjonal påloggingsportal)

² Informasjonsmodellering er en teknikk for beskrivelse av prosesser og hvilke data som inngår i disse, beskrivelser av disse og hvem som er eier av dataelementene. Dette vil igjen gjøre det enklere for andre aktører å benytte data og prosesser om igjen.

³ Lukket brukergruppe er en definert gruppe brukere som alle får sertifikat fra samme leverandør. Åpen brukergruppe har ingen definerte grenser, og kan få sertifikater fra ulike leverandører.

Tilnærming til PKI

Dato: 22.09.2004

	Sikkerhetsmessig Løsningsvalg	<ul style="list-style-type: none"> • Sertifikatleverandør(er) • Tekniske løsninger. 	<p>Kan komme noen føringer/valg fra sentralt hold, men vil antakeligvis åpne for noen selvstendige valg av konkrete løsninger. Valg kan også påvirkes av fremtidige utvikling (resultater fra SEID⁴ og andre former for standardisering). Muligheter for samordning av anskaffelser, men kan også være avhengig av lokale forhold (tilgang på kompetanse for eksempel).</p>
	Prioriteringer	<ul style="list-style-type: none"> • Kost/Nyttevurdering Anvendelse • Kost/Nyttevurdering Sikkerhetstjeneste 	<p>Konsekvensanalyse inklusiv kost-/ nyttevurdering kan avvike fra ulike kommuner pga ulik størrelse, ulik sammensetning av bedrifter og demografi blant borgere, og ulike kommuners behov.</p>

Når man har en helhetlig forståelse av behov og muligheter, bør man gjøre en del konseptuelle valg. Dette er de store beslutninger som kan gi føringer for alle anvendelsene. Hvis man ikke er bevisst disse, kan man risikere å investere mye ressurser, for å måtte gjøre mye på nytt senere. Det er en del initiativ på gang for samordning og viktige valg på konseptuelt nivå (i regi av departementene).

”Gjør de store valg før de små!”

Når de konseptuelle valgene er gjort, kan man gjøre konkret sikkerhetsmessige løsningsvalg. Ved å sette Anvendelsenes PKI Kravspesifikasjon opp mot Leverandørens PKI Løsningsspesifikasjon, vil man lettere kunne gjøre korrekt teknologi/leverandørvalg.

Når de sikkerhetsmessige valgene er gjort kan man slutføre en kost/nyttevurdering av anvendelsen. Et sentralt spørsmål er om anvendelsen kan helt eller delvis realiseres uten bruk av sikkerhetstjenester som PKI eller ikke:

- Hvis PKI ikke er nødvendig for realisering av anvendelsen vil vurderingen om man skal etablere den gjøres uavhengig av PKI-orienterte krav.
- Hvis PKI er en forutsetning for helt eller delvis å realisere en anvendelse eller på annen måte er nyttig for anvendelsen, vil man måtte gjøre en kost/nyttevurdering for dette også.

Anvendelser bør prioriteres etter hvilken som gir størst gevinst..

⁴ SEID-prosjektet er et samarbeidsprosjekt om elektronisk ID (eID) og elektronisk signatur (eSignatur) med deltakelse fra 16 forskjellige aktører fra offentlig og privat sektor.

Tilnærming til PKI

Dato: 22.09.2004

3.3 Handling

Fase	Hovedaktivitet	Aktivitet	Mulighet for gjenbruk og standardisering?
Handling	Implementering	<ul style="list-style-type: none"> • Design av løsninger • Sikkerhetsinfrastruktur • Anvendelse/Tjeneste • Sikkerhetstjeneste 	Mulig samarbeid på tvers av etater internt i en kommune og mellom ulike (f)kommuner. Bør være fokus på mulig gjenbruk og standardisering.
	Erfaringsdeling	<ul style="list-style-type: none"> • Løsningsvalg • Påvist nytte • Andre erfaring 	Resultater fra alle kommunale prosjekter bør samles inn for på den måten bygge strukturkapital.

Ved implementering av løsninger, er det også viktig med fokus på mulig gjenbruk og standardisering av løsninger. Med gjenbruk menes her

- Gjenbruk av løsninger for nye anvendelser i samme kommune. Eksempel: Tilrettelegger man for en type skjema bør det ikke være tilsvarende kostnader å tilrettelegge for andre.
- Gjenbruk av løsninger mellom kommuner. Eksempel: Tilrettelegger man en anvendelse med PKI for én kommune, bør det ikke være tilsvarende kostnad for en annen kommune. For å oppnå dette er det muligens behov for en samordning av anskaffelser.

For å oppnå dette bør man være bevisst på konkurransehensyn og eiendomsrett.

4 ANVENDELSER

4.1 Målgruppe

For å kunne gjøre en kvalifisert vurdering av nytten må man vite noe om målgruppen:

- Antall
- Hyppighet av kommunikasjon: Er anvendelsen repeterende, eller en engangsanvendelse, sett fra brukeren?
- Livssituasjon (ref LivsIt⁵)
- Interne bruker (ansatte) eller Eksterne brukere (Borgere og andre private aktører)
- Profesjonelle aktører eller privatpersoner)
- Rolle

Poenget er om vi når målgruppen vi ønsker via den kanalen vi etablerer for anvendelsen (typisk web og Internet), og er målgruppen stor nok til at det forsvaret investeringen.

⁵ LivsIT- konseptet skal klassifisere offentlig elektronisk informasjon på Internettet med utgangspunkt i livssituasjoner.

Tilnærming til PKI

Dato: 22.09.2004

4.2 Beskrivelse og kategorisering av anvendelser

Det fins en rekke tjenester som kan vurderes å tilrettelegges for elektronisk kommunikasjon, og mulig bruk av PKI for sikring. Eksempelvis kan nevnes⁶:

Avtaler

Anbudsprosesser

Kjøps-/salgskontrakter

Rammeavtaler

Bevillinger

Søknad om bevilling til salg av øl

Søknad om serveringsbevilling

Søknad om skjenkebevilling

Byggesak

Tilgang til Geodata

Tilgang til GAB-opplysninger

Byggesøknad

Nabovarsel

Melding om tiltak

Søknad om tillatelse til tiltak

Tinglysingsdokumenter

Begjæring om oppdeling i eierseksjoner

Diverse

Søknad om nedsettelse m.m. av skatt

Søknad om næringsfond

Fast eiendom

Søknad om konsesjon på erverv av fast eiendom

Kultur og fritid

Søknad om leie kommunale idretts- og svømmehaller, skolerom

Søknad om arrangementstilskudd

Søknad om ledsagerbevis

Søknad til tilskudd til allment kulturarbeid

Søknad om tilskudd til lekeplass/nærmiljøtiltak

Landbruk

Søknad om bygging av landbruksvei

Søknad om godkjenning av plan for landbruksvei

Søknad om statstilskudd til skogsveier

Oppmåling

Rekvisisjon av kartforretning

Skole og barnehage

Flyttemelding

eLæring-applikasjoner og -portaler

Elektronisk eksamen

Søknad om SFO-plass, barnehageplass

Søknad om redusert foreldrebetaling

Søknader husbanken

Søknad om boligtilskudd

Søknad om kommunalt etableringslån

⁶ Liste hovedsakelig hentet fra Sluttrapport i Fosen-prosjektet og interne dokumenter fra DDT-prosjektet.

Tilnærming til PKI

Dato: 22.09.2004

Søknad om kommunalt tilskudd til utbedring

Søknad om lån til kjøp av bolig

Søknad om lån til utbedring av bolig

Søknad om lån/kvalitetstilskudd til oppføring

Tilgangskontroll

Portaler

Hjemmekontor/VPN⁷

Distribusjon av Programvare

Generelt

Tilgang til saksdokumenter

Sikker meldingsutveksling mellom systemer og applikasjoner

Sikker arkivering av saksdokumenter

Mulige anvendelser bør beskrives og katalogiseres, for å etablere felles referanser i det offentlige (Eksempler: Tjenestebeskrivelser fra KS⁸, LivsIT⁹ etc.). Listingene over er ikke katalogisert ut fra dette, men heller etter fagområder. Vi foreslår at det gjøres et sentralt arbeid for å lage en mer komplett liste over mulige anvendelser og gjøre en felles kategorisering.

En fordel for å samordne analysearbeidet på tvers av (f)kommuner er å ha en felles referanseramme for hvilke offentlige tjenester det er aktuelt å presentere på Internett. For å oppnå dette bør man enes om beskrivelser og kategorisering av disse. På den måten vil man relativt raskt få oversikt over mangler i analysearbeidet for alle kommuner samlet.

”det bør ikke være nødvendig at alle kommuner skal gjøre de samme analyser hver for seg”

Et forslag til dimensjoner for klassifisering kan være:

- Målgruppe
 - Interne (Ansatte)/Eksterne (borgere)
 - Profesjonelle brukere/Privatpersoner
 - LivsIt
- Løsningstype
 - Innlevering (eks: søknader)
 - Utlevering (eks: kartdata, GAB-opplysninger)
 - Tilgangskontroll (eks: til applikasjoner etc)

Et annet viktig poeng er at det ikke bør være nødvendig for alle brukersteder/(f)kommuner å gjøre sine egne analyser. Det er store besparelser i samordning og deling av informasjon. Eksempelvis bør det være problemfritt å gjøre gjenbruk av alle vurderinger i det juridiske behovet knyttet til sikkerhet (signatur). Det bør etableres en rapportdatabase, som samler alle analyser og erfaringer, slik at de

⁷ Virtual Private Network (Sikker forbindelse over internett)

⁸ Nasjonal tjenstekatalog (NTK) er en sentral database som inneholder beskrivelser av de tjenestene som kommunen yter overfor sine innbyggere innen kommunale tjenesteområder som blant annet skole, helse og tekniske tjenester. NTK Beskrivelsene følger en fast struktur og gir en unik oversikt over tjenestetilbudet – til nytte for både innbygger, servicekontor og saksbehandler.

Nasjonal tjenstekatalog bygger på Statskonsults mal «Til tjeneste!» og er en fullstendig implementering av den feltinndelingen som fremkommer der.

⁹ LivsIT- konseptet skal klassifisere offentlig elektronisk informasjon på Internettet med utgangspunkt i livssituasjoner. Livssituasjoner er reelle situasjoner som folk kjenner seg igjen i. Eksempler på livssituasjoner (Samboer, Foreldre, Arbeidssøker, Boligbygger, Nabo)

kommer alle kommuner til gode. Hvis man i tillegg har felles referanseramme for hva de ulike tjenester inneholder, vil dette kunne gi store besparelser fremover.

4.3 Funksjonalitet/Nytte

Hvilken funksjonalitet en skal ha i en anvendelse faller utenfor rammen av dette dokumentet og vil ikke vurderes.

For å kunne vurdere nytten av PKI, må man i tillegg til de sikkerhetmessige forhold, også vurdere nytten av de anvendelser som kan realiseres pga PKI. Det har ingen hensikt å gå over til mer elektronisk kommunikasjon hvis dette ikke har noen nytte.

Nytten bør kunne måles i

- Besparelser (i tid og ressurser) for brukersted (kommune el).
- Økt kvalitet for brukerne

Da er det følgende stikkord man bør være opptatt av

- Automatisering
- Forenkling (hoppe over manuelle kontroller eks)
- Selvbetjening
- Økt tilgjengelighet
- Standardisering
- Nye verdiøkende tjenester for brukeren

5 SIKKERHETSBEHOV

5.1 Juridiske krav¹⁰

Det er et uttalt politisk mål i Norge at elektronisk korrespondanse skal være like pålitelig og juridisk bindende som korrespondanse ved bruk av papir. Siden det er en lang rekke krav om signatur i lover, forskrifter og regelverk, peker dette direkte på behovet for digitale signaturer.

Lovverket er generelt sett tilpasset bruk av digital signatur som fullgodt alternativ for håndskrevet. Dette har vært gjort gjennom det såkalt eRegelprosjektet:

- Fra 01. januar 2002 er 39 lover endret, og mange flere lover har vært unødvendig å endre.
- Evt. lovkrav om ”skriftlig” er i utgangspunktet teknologinøytralt, hvis ikke annet er uttrykkelig nevnt. Dette betyr at der loven krever skriftlig kommunikasjon kan PKI normalt kunne benyttes¹¹.
- Mottaker må normalt ha godtatt elektronisk kommunikasjon – av og til uttrykkelig akseptert¹².
- Visse meldinger må sikres dokumentasjon for at de er sendt/mottatt (”rekommandert”)¹³. Her kan PKI være nyttig.
- For visse avtaler/meldinger stilles visse ”kvalitetskrav” til sikringsmåten¹⁴. Her vil PKI, og ulike nivåer på denne være godkjente metoder¹⁵.

¹⁰ Poenger og momenter er hentet fra Presentasjon ”Elektroniske disposisjoner, Lover og regler man bør kjenne til. Adv Gunnar Harstad, Sparebankforeningen.

¹¹ Eksempel på dette er betalingsoppfordring i fm inkasso, se Inkassoloven § 10.

¹² Eksempel her er Bustadsoppføringslova § 6a.

¹³ Eksempel på dette kan være forelegg som legges frem for barnefar, se Barnelova § 12.

¹⁴ Eksempel her kan være avtaler om kredittkjøp, se kredittkjøpsloven § 3a (krav om at avtalens innhold skal være tilgjengelig for kjøperen, og det er benyttet betryggende metode for autentisering).

¹⁵ I enkelte sammenhenger, spesielt overfor offentlig sektor, kan det tenkes at elektroniske dokumenter bare vil bli akseptert dersom de har en såkalt kvalifisert signatur. Utstedere av kvalifiserte sertifikater skal registreres hos Post- og teletilsynet, og blir underlagt en kvalitetsmessig sertifisering. Generelt kan man si at kvalifiserte signaturer alltid skal anses

I vurdering av en anvendelse, bør det derfor vurderes om loven stiller noen krav til hvordan kommunikasjonen skal foregå i fm akkurat denne anvendelsen. Er det krav om skriftlighet, vil en elektronisk kommunikasjon kunne nødvendiggjøre bruk av PKI.

Det fins en egen forskrift om elektronisk kommunikasjon med og i forvaltningen, som også kan gi støtte i vurdering av behovet for PKI: § 4. Krav til sikker identifisering, bruk av sikkerhetstjenester mv.

1. Henvendelser til forvaltningsorgan, som kan fremsettes i elektronisk form, og som ikke er underlagt særskilte formkrav eller krav til konfidensialitet mv., kan fremsettes uten bruk av sikkerhetstjenester med mindre annet er bestemt i medhold av nr 2-4 nedenfor.
2. Forvaltningsorganet kan i det enkelte tilfelle be om opplysninger som bekrefter avsenders identitet eller fullmakter dersom dette er av betydning for håndtering av henvendelsen.
3. Forvaltningsorganet kan også stille krav om at bestemte fremgangsmåter, sikkerhetstjenester og -produkter skal tas i bruk for å sikre autentisering, ikke-benekting, integritet og konfidensialitet.
4. Forvaltningsorganet kan fastsette at krav som nevnt i nr. 2 og 3 ovenfor skal gjelde generelt for nærmere angitte typer av henvendelser.
5. På områder der det er åpnet for elektronisk kommunikasjon, men der henvendelser er underlagt særskilte formkrav eller krav til konfidensialitet mv., skal forvaltningsorganet fastsette hvilke fremgangsmåter, sikkerhetstjenester og sikkerhetsprodukter som oppfyller kravene til form eller konfidensialitet mv.

5.2 Sikkerhetsmessige krav¹⁶

Som det fremgår over så kan digitale signaturer være et juridisk krav i fm elektronisk kommunikasjon.

Utover dette kan digital signatur også ha en sikkerhetsmessig begrunnelse. Sikkerhetsmessig er digitale signaturer først og fremst viktig der det er et element av mistro mellom partene, enten ved at avsender mistenker mottaker for å ville tukle med informasjonen, avsender ikke er sikker på at mottaker er riktig person, eller ved at mottaker trenger et meget sterkt bevis for hva avsenderen ga fra seg.

Eksempler på risikoer som skal reduseres:

- Forfalskninger
- Sensitiv data på avveie
- Nekte for inngåelse av avtaler
- Gi uvedkommende tilgang til informasjon
- Uenighet om når avtale er inngått eller når melding er sendt.

Videre må man vurdere hvilke konsekvenser brudd på disse vil medføre:

- Hvor ofte kan man regne med at dette vil skje

å tilfredsstillte evt. krav i lover og annet regelverk om underskrift, men også ikke-kvalifiserte signaturer kan oppfylle krav om rettslig gyldighet.

16 Digitale signaturer, sertifikater, tillit og TTP-tjenester (PKI CS Notat 1/2001: Jon Ølnes)

- Hvor mye tid og penger kan man tape på det skjer.

Hvis et brudd på sikkerheten ikke er sannsynlig og ikke medfører særlige konsekvenser for noen av partene, vil det være mindre behov for å etablere en sikkerhetsløsning rundt anvendelsen.

Tradisjonelt har vi i Norge høy grad av tillit til at offentlig sektor behandler informasjonen vår skikkelig, og i de fleste tilfeller vil antagelig en offentlig etat ha tilstrekkelig bevis gjennom et gjennomarbeidet loggesystem eller enklere mekanismer enn digitale signaturer.

Det kan tenkes at behovet for signaturer faller helt bort i en del tilfeller ved overgang til elektronisk kommunikasjon. Det er rimelig klart at sesjonslogging og transaksjonslogging for elektronisk korrespondanse kan gi en helt annen nøyaktighet i sporbarheten enn det en vanligvis har ved papirkorrespondanse. En utredning av det reelle behovet for digitale signaturer ville antagelig ha konkludert med at behovet er mindre enn det forvaltningen tror.

5.3 PKI Kravspesifikasjon

Krav til sikkerhetstjenester rundt løsningen kan gi en PKI kravspesifikasjon¹⁷.

Generelt sett kan man dekke sikkerhetsbehov gjennom følgende fire sikkerhetstjenester:

- Autentisering: **Identifisering** av personer eller systemer.
- Konfidensialitet: **Hemmeligholdelse** av informasjon gjennom kryptering.
- Integritet: **Endringssikring**: Ikke mulig å endre informasjon uten at det merkes.
- Ikke-benektning: Skape en sterk knytning mellom informasjonsinnhold og den som signerer, slik at det i etterkant regnes som **bevist** at personen har signert.

I tillegg til å avklare hvilke sikkerhetstjenester man har behov for, må man også spesifisere hvordan dette teknisk kan implementeres i selve anvendelsen. Det kan være forhold som

- Teknisk miljø
- Utviklingsverktøy
- Formater for utveksling og brukerdialog
- Etc.

6 MARKEDSLØSNINGER

6.1 Leverandører i det norske markedet

Eksempler på sertifikatleverandører: Bankene, Buypass (Zesign), Zesign, Posten (Zesign), Telenor (Zesign), Skandiabanken og Verisign. I tillegg fins det en rekke teknologiselskaper og konsulenthussom kan levere løsninger og tjenester rundt bruken av sertifikater.

6.2 Målgruppe

Ved valg av en eller flere sertifikatleverandører, må man være bevisst på hvilken utbredelse disse har eller vil få. Her er **Antall** og **Demografi** viktige stikkord. Hvordan leverandøren kan håndtere en

¹⁷ Det er ikke bare PKI som kan gi elektronisk signatur i juridisk forstand eller dekke andre sikkerhetsmessig behov. Bruk av PIN, Brukernavn og passord kan også være tilstrekkelig. Dette dokumentet fokuserer kun på PKI som løsning. Et poeng i så måte er at standardisering av teknikker kan være besparende i seg selv, så bruk av PKI kan være nyttig selv om behovene stiller svakere krav.

Tilnærming til PKI

Dato: 22.09.2004

utrulling til nye brukere er også sentralt. Det er viktig å velge en sertifikatleverandør som naturlig når den brukergruppen man ønsker å tilby tjenester til.

6.3 PKI Løsningsspesifikasjon

På samme måte som man må vurdere hvilke PKI-behov en anvendelse har, må man ved vurdering av leverandører, gjøre de samme vurderinger i forhold til hva de leverer.

6.3.1 Nøkkelbærer

Nøkkelbærer er et begrep som brukes om den mekanismen som inneholder en brukers sertifikat og private nøkkel. En bruker må ha dette tilgjengelig for å benytte PKI-en.. Ulike leverandører har ulike løsninger:

- Software (eks. BankID)
 - Lokallagret (installeres på brukerens PC).
 - Nettsentrisk (lagres på et felles sted som brukeren kan nå over internett)
- Smartkort: (eks. Buypass)
- USB-token: en liten minnebrikke som koples til USB-porten på PC'en.
- Mobiltelefon (eks. Telenor)

Ved valg av leverandør må man være bevisst på hvilke nøkkelbærer som brukes, og om dette er hensiktsmessig i forhold til anvendelsene.

Eksempelvis er lokallagret SW ofte raskere og enklere i bruk, mens nettsentrisk SW-løsning er mer mobil (kan lettere benyttes på flere ulike PC-er) (se 4.3.5 for detaljer).

6.3.2 PKI sikkerhetsfunksjoner

I fm en PKI er det ulike funksjoner som benyttes for å yte de ulike sikkerhetstjenester. Noen av disse må integreres i selve anvendelsen og andre tilbys av tredjepart.

- Kryptering: Kjernefunksjonalitet i PKI, og gjør et innhold uleselig, uten at man låser opp med riktig nøkkel.
- Signering: Dette er funksjonalitet som ved hjelp av krypteringsteknologi, knytter et innhold uløselig til en person. Brukes både til autentisering og signering.
- Revokeringskontroll: Dette er funksjonalitet hos sertifikatutsteder (alt Valideringsautoritet), som sjekker gyldighet til sertifikat og dermed til en signering.
- Tidsstempling: En tjeneste som beregner og gir gyldig tid.
- Notartjeneste: Dette er strengt tatt ikke en PKI-mekanisme, men er likevel en viktig mekanisme i denne sammenheng. Det vil være behov for lagring og journalføring av digitalt signerte dokumenter hos en tredjepart som alle stoler på, for å styrke bevisføring ved tvister.

Ved vurdering av ulike løsninger/leverandører må man også vurdere hvilke funksjoner de kan tilby, og evt. begrensninger i disse. Eksempelvis kan en leverandør levere signering på noen dokumentformater (pdf), men brukerstedet har andre preferanser (word).

Tilnærming til PKI

Dato: 22.09.2004

6.3.3 PKI Tjenester

PKI funksjonene leverer teknologier og tjenester som gjør det mulig å tilby PKI tjenester. Sammen med avtaleverket vil de bestemme hvilke PKI tjenester som tilbys i en PKI. Generelt sett kan man dekke sikkerhetsbehov gjennom følgende 4 PKI sikkerhetstjenester:

- Autentisering: **Identifisering** av personer eller systemer.
- Konfidensialitet: **Hemmeligholdelse** av informasjon gjennom kryptering.
- Integritet: **Endringsikring**: Ikke mulig å endre informasjon uten at det merkes.
- Ikke-benektning: Skape en sterk knytning mellom informasjonsinnhold og den som signerer, slik at det i etterkant regnes som **bevist** at personen har signert.

En mulig analogi for å forstå dette bedre er gamle dagers signeringsring, som ble brukt til å sende fortrolige brev mellom parter:

- Ringen hadde et symbol som knyttet ringen til eieren. Ringen kunne brukes til å merke en forsegling, for å vise hvem som var avsender (autentisering).
- Forseglingen av et brev kunne ikke brytes uten at det ble oppdaget (integritet).
- Knytningen mellom ringen (merket), forseglingen og brevet, skapte også en form for ikke benekting.
- Hvis forseglingen hadde vært umulig å bryte hadde vi også hatt konfidensialitet.

Dette var ikke spesielt sikkert, men ble akseptert som sikkert nok. Ny teknologi gjøre nå dette med atskillig større tillitt.

Ikke alle sertifikatleverandører leverer verken teknologisk eller avtalemessig alle PKI tjenester. Eksempelvis kan en sertifikatleverandør tilby både autentisering og integritet (signering), men ikke kryptering. Det kan også være ulike styrker på for eksempel ikke-benektning. En uavhengig tidsstempingstjeneste vil kunne være mer overbevisende enn en enkel logg fra sertifikatleverandøren.

6.3.4 Øvrige krav

Andre krav som er nødvendig å analysere både mht anvendelsene og de ulike løsninger som er tilgjengelig fra de ulike leverandørene:

- Brukervennlighet: Selvforklarende, Rask i bruk, supportapparat etc.
- Utrullingskvalitet: Sikker og effektiv utrulling av sertifikater og evt. integrasjon mot tjenester
- SLA: Service Level Agreement (opptider, tilgjengelighet, Responstider etc.)
- Åpenhet: Noen løsninger er helt åpne i betydning av at man kan bruke åpne standarder og standardfunksjonalitet for å gjøre nødvendig validering om et sertifikat er gyldig. Andre løsninger stiller krav til bruk av proprietær programvare fra leverandøren, og dette krever en integrasjon mot tjenesteapplikasjonen. Dette kan være kostnadsdrivende og skaper bindinger til leverandøren.

6.4 Kostnader

For å kunne gjøre en kost/nytttevurdering av en tjeneste, må man få frem en klart bilde av kostnader. Her er det ulike varianter hos de ulike leverandørene. Under følger en oppstilling av kostnadselementer man må være obs på:

- Anskaffelse av Sertifikater (for brukersted og/eller bruker)
- Implementering av kode for signering, autentisering inkludert validering mot sertifikatutsteder.

Tilnærming til PKI

Dato: 22.09.2004

- Driftskostnader
- Abonnement for bruk av en løsning
- Transaksjon for bruk av sertifikater. Her er det vanlig å ta betalt for validering av et sertifikat.

Dette gjelder både selve PKI'en, PKI tilleggstjenester og selve tjenesten som det PKI-tilrettelegges for.

7 KONSEPTUELLE VALG

Før man starter et PKI-prosjekt bør man gjøre en del strategiske vurdering og valg mht PKI. Disse vil igjen påvirke valg av teknologi.

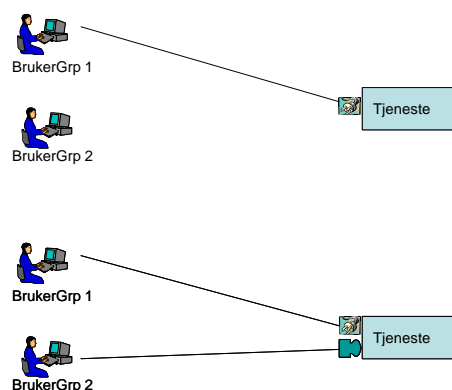
7.1 Samtrafikkproblemstillingen

En utfordring er at ulike PKI-domener, ikke kommuniserer på tvers (har samtrafikk). Dette betyr at selv om en har tilrettelagt for PKI-tjenester på en anvendelse, kan anvendelsen ikke nødvendigvis benyttes av en sluttbruker som har sertifikat fra en annen leverandør.

Dette fører til to strategiske valg

7.1.1 En eller flere sertifikatleverandører (Lukkes vs. Åpen brukergruppe)

- Tilrettelegger i anvendelsene for bruk av sertifikater fra kun én sertifikatleverandør og dermed én brukergruppe. Dette kalles også Lukket brukergruppe¹⁸.
- Åpne anvendelsene for flere ulike sertifikat- og teknologileverandører og dermed brukergrupper. Dette kalles også Åpen brukergruppe¹⁹.



Hvis brukergruppen er begrenset og kjent på forhånd kan en lukket brukergruppe være hensiktsmessig. Eksempel på dette er hvis anvendelsene kun er knyttet til interne brukere i en organisasjon. På den annen side vil en lukket løsning kunne være svært hemmende på sikt, da man kan utelukke brukergrupper, og man skaper sterke bindinger til én leverandør. Hvis man velger én sertifikatleverandør, må man være svært bevisst på målgruppen for anvendelsene og sertifikatutstederen.

¹⁸ De fleste initiativ i det offentlige hittil har satsset på én sertifikatleverandør. Hovedargumentet har nok vært å få testet ut PKI i mest mulig kontrollerte former, og ikke et reelt valg av en lukket brukergruppe.

¹⁹ Smartkom i Stavanger har åpnet for bruk av både Buypass og BankID. Oslo Kommune har kjørt en pilot der de i prinsippet åpner for mange ulike PKIer.

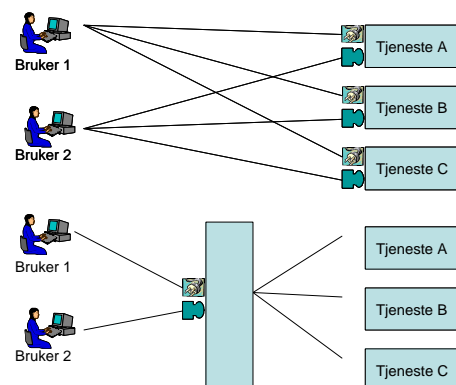
Tilnærming til PKI

Dato: 22.09.2004

7.1.2 Tjenstesikring vs. Skallsikring

Det er i hovedsak to former for pki-enabling av løsninger:

- Tjenstesikring: Implementering av en PKI-baserte tjenester direkte mot og i sluttbrukerapplikasjonene. Dette kalles også Ende-til-ende-sikkerhet²⁰.
- Skallsikring: Implementering av PKI-basert autentisering og signering som en frittstående tjeneste, som igjen kommuniserer med flere sluttbrukerapplikasjoner²¹.



Hvis man ønsker en åpen brukergruppe (med sertifikater fra ulike sertifikatutstedere), vil tjenstesikring av alle anvendelser med alle løsninger kunne bli svært kostnadskrevenende. I en skallsikringsløsning vil man lettere kunne åpne for flere pki-domener mot samme anvendelser. En slik skallsikringsløsning vil kunne gjøre det lettere å etablere eksempelvis Single Sign On (SSO). Man vil også kunne styre hvilket sikkerhetsnivå man ønsker til de ulike anvendelsene. Eksempelvis kan man kreve PKI for tilgang til sakspapirer, men kun passord for tilgang til

En videreutvikling av en slik løsning kan være å kople seg opp mot en samtrafikkløsning, som fungerer som en felles valideringstjeneste og klassifisering av ulike PKI-domener (policies)²².

7.2 Eie eller Leie tjenester

Mange kommuner etc. vil kanskje synes det er en forlokkende tanke å være sertifikatutsteder selv til sine ansatte og borgere. Etablering og drift av et PKI-domene er svært kostnadskrevenende, og egner seg bare for helt enkle eller helt spesielle behov (som forsvaret). Til internt bruk hvor kravet til sikkerhet og tillitt ikke er det stor er det relativt greit å etablere egen PKI.

Utfordringen vil være hvis man trenger en sterk tillit for kommunikasjon med andre, og det er det som er fremtidens anvendelser (elektronisk kommunikasjon mellom forvaltningsnivåer, og mellom forvaltning og globalt næringsliv, og mellom forvaltning og ukjente borgere).

På den annen side fins det allerede og vil komme langt flere leverandører som kan tilby tilleggsfunksjonalitet. Et typisk område for outsourcing vil kunne være ulike løsninger for skallsikring og kryssvalidering, samt tidsstempling og notartjeneste. Det bør derfor vurderes om det er hensiktsmessig å leie fremfor å eie disse tjenestene. PKI-tilbudet i markedet er under en rivende utvikling, og det kan være fordeler med å overlate utviklingen til tredjeparter.

²⁰ I DDT prosjektet ble det etablert tjenstesikringsløsninger opp mot to anvendelser; markedsplassen ehandel.no og en kartdataapplikasjon.

²¹ Oslo Kommune har hatt en pilot på dette. Hvis Altinn kommer til å fungere som en felles inngangsport til ulike offentlige etater, vil det også være en skallsikringsløsning. I Altinn foregår det nå en pilot med Lånekassen og Buypass.

²² Eksempel på dette er Det Norske Veritas

8 EKSEMPLER PÅ VURDERINGER

8.1 Markedsløsning: BankID

Bankene har etablert en PKI for det norske markedet. I løpet av 2004 og 2005 vil dette bli implementert som sikkerhetsløsning for de fleste nettbankene, og bankene vil også levere dette til private og offentlige virksomheter.

Under følger en subjektiv vurdering av BankID som PKI-løsning, med utgangspunkt i de kriterier som er fremsatt. Dette er et **eksempel** på en vurdering og ikke noe fasitsvar. Poenget er å eksemplifisere kriteriene. BankID er under utvikling, og enhver bør gjøre sin egen vurdering.

8.1.1 Målgruppe

BankID vil i første rekke rulles ut til de som har nettbank. Det er i dag i underkant av 2 mill. nordmenn. Forutsetning for å få BankID er et kundeforhold til en bank som utsteder dette. Eksempelvis kan personer som kun har kundeforhold til Skandiabanken ikke få BankID per i dag.

Bankene kan nekte utstedelse av BankID til personer. Dette kan utelukke enkeltpersoner fra en offentlig anvendelse som krever BankID.

Når det gjelder demografi, så er det en overvekt av yngre personer som har nettbank. Det er også disse som vil være de mest aktive brukerne av offentlige nettbaserte tjenester.

BankID leverer per i dag kun personlige sertifikater. Andre type sertifikater er under vurdering.

8.1.2 Nøkkelbærer

BankID bruker såkalt soft-sertifikat. Det betyr at nøkkel og sertifikat lagres i et stykke software. Det fins to varianter:

- Banklagret løsning: I denne løsningen lagres sertifikatet og tilhørende nøkler hos banken (fysisk hos BBS). Brukeren får tilgang til dette over nett gjennom en engangspassordløsning. Dette betyr at ved bruk må brukeren registrere personnummer, engangspassord og statisk passord. Per i dag ser det ut som om dette er den prefererte løsningen fra de fleste bankene, med unntak av Fokus Bank.
- Lokallagret løsning: I denne løsningen installeres sertifikatet med nøkkel på egen PC. Brukeren får tilgang til dette ved å registrere et statisk passord, men kun fra PC som har installert dette. Per i dag er det Fokus som vil levere denne løsningen.

Banklagret løsning er mest mobil (kan brukes fra hvilken som helst PC uten noen form for forarbeid). Lokallagret løsning fungerer best for de som hovedsakelig jobber fra samme PC (eks. jobb-pc)

Lokallagret løsning er enklere og raskere i bruk (mindre tasting for brukeren).

For interne løsninger med interne brukere (ansatte) som hyppig vil benytte BankID kan det bli noe tungvint med banklagret BankID. Noen brukere vil synes det er en for omstendelig prosess å for eksempel logge seg på når dette skal skje flere ganger om dagen. Her vil muligens lokallagret løsning være å foretrekke.

For ekstern løsning med eksterne brukere (borgere) vil trolig behovet for mobilitet være viktigere.

Tilnærming til PKI

Dato: 22.09.2004

8.1.3 Sikkerhetsfunksjoner

- Signering: BankID leverer signeringsfunksjonalitet på to dokumentformater per idag:
 - PDF
 - Fritekst
- Tidsstempling: BankID leverer ikke tidsstemplingstjeneste per i dag.
- Notartjeneste: BankID leverer ikke notartjeneste per i dag.

8.1.4 Sikkerhetstjenester

BankID leverer

- Autentisering: **Identifisering** av personer eller systemer.
- Integritet: **Endringssikring**: Ikke mulig å endre informasjon uten at det merkes.

Verken funksjonalitet eller policy støtter konfidensialitet (**Hemmeligholdelse** av informasjon gjennom kryptering).

Det kan diskuteres i hvilken grad BankID støtter Ikke-benektning (Skape en sterk knytning mellom informasjonsinnhold og den som signerer, slik at det i etterkant regnes som **bevist** at personen har signert), men en viss grad av ikke-benektning er tilstede. Problemet er at det er ingen uavhengig part som verken garanterer for tidspunkt eller lagring av signatur.

8.1.5 Øvrige krav

- Brukervennlighet: BankID er selvforklarende, og i og med at bankene tar BankID i bruk i egne nettbanker vil de aller fleste bli fortrolige med løsningene. Alle anvendelser vil se like ut. På den andre siden er Banklagret løsning ganske omstendelig og noe tungvint ved hyppig bruk.
- Utrullingskvalitet: Bankene har tradisjon for store utrullinger, og organisasjon til å levere et tilstrekkelig supportapparat. De har store distribusjonsnett, som kan håndtere kunderegistrering (inkludert legitimasjonskontroll). De har i underkant av to millioner egne kunder som skal håndteres. Utrullingskvaliteten må derfor sies å være solid.
- SLA: Service Level Agreement (oppetider, tilgjengelighet, Responstider etc): Selv i pilotdrift har dette vært bra, og må regnes å bli meget bra i full drift.
- Åpenhet: Løsningen må sies å være ganske lukket. BankID er en proprietær løsning som krever egen software for etablering av autentiserings- og signeringsfunksjonalitet. Denne må integreres i selve anvendelsen.

8.1.6 Kostnader

Bankene har ikke helt klarlagt kostnadsbildet rundt BankID, men slik det ser ut i dag er det to kostnadselementer som er sentrale:

- Implementering: Med BankID får man en CD med dokumentasjon, bibliotek av funksjoner og eksempelkode for implementering. Erfaringsmessig så langt vil en implementering av BankID ligge på mellom 50' – 200', avhengig av selve anvendelsen (autorisasjonsløsning etc.).
- Transaksjonskostnader: Bankene ser for seg en kostnad per validering av sertifikat, samt valideringsoppslag (tilleggsinformasjon som personnummer etc.). Transaksjonskostnaden vil kunne ligge mellom 0,20 – 2 kroner, men dette vil bli avklart i løpet av høsten 2004.

8.2 Anvendelse: Byggesøknader

Mange av de offentlige initiativene hittil har vært nært knyttet til byggesøknader.

Etter oppdrag fra Kommunal- og regionaldepartementet og Miljøverndepartementet har Statens bygningstekniske etat og Statens kartverk etablert et verktøy som bidrar til å effektivisere den kommunale plan- og byggesaksbehandlingen. Byggsøkprosjektet har utviklet et system for å fylle ut byggesøknader på Internett. Den ferdige utfylte søknaden skal kunne overføres elektronisk til kommunens egne saksbehandlingssystemer.

De kommunale initiativ har vært og bør være en implementering av denne løsningen, kombinert med tilgang til kommunale data (eks. kart og GAB-opplysninger) og innsyn i saksbehandlingen.

Under følger en vurdering av behovet og nytten med digital signatur i fm Byggsøknader, med fokus på de kriterier som er fremsatt.. Dette er et **eksempel** på en vurdering og ikke noe fasitsvar. Poenget er å eksemplifisere kriteriene. Mye av momentene er hentet utfra en rapport gjort av Statskonsult²³.

8.2.1 Målgruppe

Hvem (Roller i fm elektronisk løsning for byggsøknader):

- Tiltakshaver: Byggherre
- Ansvarlig søker: Skal ha nødvendig godkjenning.
- Naboer i fm nabovarsel.
- Faglige ansvarlige på ulike områder må ha godkjenning senest ved igangsetting

Demografi:

- Borgere og profesjonelle aktører
- Stor spredning i alder og livssituasjon.
- Ikke entydig gruppe.

Antall:

- Antall byggesøknader i kommunen (ca. 100.000 i hele Norge per år)
- Gjennomsnittlig antall berørte parter (se roller over)
- Hyppighet av kommunikasjon:
 - For borgere vil byggesøknad være en relativt sjelden foreteelse.
 - For profesjonelle aktører vil det være oftere

Konsekvenser:

- Det stiller større krav til enkelthet i bruk overfor borgere enn profesjonelle aktører
- Sjeldent utnyttelse gjør det uhensiktsmessig å anskaffe seg digitalt sertifikat kun for denne anvendelsen, og det bør derfor forutsettes at brukerne har digitalt sertifikat fra før.
- Krav til mobilitet

²³ Utredninger fra Statskonsult: Elektronisk plan- og byggesaksbehandling og krav om signatur m.v. i lover og forskrifter (19.09.02), og Signaturkrav, risiko og elektroniske byggesøknader (06.mars 2003).

Tilnærming til PKI

Dato: 22.09.2004

8.2.2 Nytte

Skriftlig søknadsutfylling og – behandling oppleves som frustrerende. Det går mye penger og tid med til mye ”rot”.

Funksjonelt sett er det derfor mye å hente på å gjøre byggesaksprosessen mer elektronisk:

- Fordeler for søker:
 - Online tilgang til og utfylling av opplysninger med begrenset innsynsrett
 - Tilgang til kartdata (skal begrenses til relevant bruk)
 - Automatisk overføring av GAB-data
 - Hjelp til søker om utfylling av søknad (sikre korrekt og komplett søknad)
 - Veiledning
 - Kontroll
 - Automatisk utfylling
 - Opplysninger registreres bare en gang
 - Redusere saksbehandlingstid (unngår forsinkende postgang)
 - Online tilgang til saksbehandling for å følge status på søknaden
- Fordeler for kommunen:
 - Mer korrekt og komplette søknader
 - Automatisk registrering i kommunal saksbehandlingssystemer
 - Bedre ressursutnyttelse i kommunene og i næringen.
 - Større grad av selvbetjening av søker

Som det fremgår av det over er det betydelig gevinster å hent med en elektronisk søknadsbehandling. I en fullverdig vurdering, bør man forsøke å kvantifisere besparelser/nyttene.

Spørsmålet så er om sikkerhetstjenester og PKI er en forutsetning for disse, eller om man kan oppnå dette uavhengig av disse.

8.2.3 Krav til sikkerhetstjenester

8.2.3.1 Juridiske krav

Plan- og bygningsloven krever at søknad skal undertegnes av tiltakshaver og ansvarlig søker.

- Bakgrunn for krav om underskrift:
 - Identifikasjon av underskriver/avsender.
 - Godtgjøring av at opplysningen er gitt av underskriver
 - Egenskapen om å vanskeliggjøre manipulering er viktig for både sender og mottaker.
 - Varslingsfunksjon om at underskriveren binder seg til de avgitte opplysningene i søknadsdokumentet.(straffeansvar for forseelser)
- Dette er ikke noe formkrav, slik at PKI kan benyttes til dette (men det kan også andre teknologier).

Videre er det et krav i bygningsloven at naboer og gjenboere skal varsles.

- Søknaden skal inneholde gjenparter av varselbrevene samt kvitteringer for at brevene er sendt.
- Alternativt til varsel er naboens skriftlige godkjennelse av tiltaket. Dette kan gjøres i en nettbasert løsning.

8.2.3.2 Sikkerhetsmessige problemstillinger å vurdere

- Behovet for å forhindre

-
- At noen sender inn falsk søknad
 - At det er usant at håndverker har alle papirene i orden
 - At noen signerer på vegne av andre
 - At noen usant ”dokumenterer” at nabovarsel er sendt, eller at naboen har samtykket
 - At noen starter å bygge uten å ha lov
 - Hvor uheldig er det at disse problemene kan inntreffe?
 - Skjer det ofte at det sendes falske søknader eller falsk dokumentasjon i forbindelse med nabovarsel/samtykke?
 - Hvor ofte opptrer profesjonelle på falske premisser?
 - Hvor mye arbeidstid og penger taper man på det?
 - Hvor mange rettsaker kan man få ved falske signaturer?
 - Involverer saksbehandlingen opplysninger som må holdes skjult for uvedkommende? Hvilke og hvor ofte?
 - Hvilke mekanismer gir systemeier akseptabel sikkerhet for at søknaden er i henhold til regelverket?

Generelt sett er det lav risiko forbundet med å bruke papirsøknader. Informasjonen er åpen og vil ikke være underlagt noen form for taushetserklæring.. Sikkerhetsmessig er det derfor kanskje ikke så mye å hente ved å gå over fra skriftlig til elektronisk signering.

8.2.4 PKI Kravspesifikasjon

Som det fremgår av det over er det en del juridiske krav til signering av byggesøknader. Hvis man ønsker å gjøre nabovarsel elektronisk, må det også fremskaffes bevis for at naboer har forhåndsgodkjent søknaden. De sikkerhetsmessige utover dette regnes ikke som svært sterke.

Hvis vi vurderer PKI sikkerhetstjenester ser vi at vi nok har behov for

- Autentisering: Sikker identifisering av de som signerer.. En autentiseringsmekanisme kan være nyttig ved automatisk utfylling av søknaden. Det er også nødvendig ved tilgang til begrenset informasjon (kartdata).
- Integritet. Ikke mulig å endre søknaden etter at signatur er påført. Dette vil være sikrere funksjonalitet enn ved skriftlige signaturer.
- En viss støtte for ikke-benektning. Man har behov for at søkeren ikke skal kunne nekte for å ha underskrevet søknaden, men det trengs neppe så sterk bevisføring at man trenger en uavhengig tidsstempling og notartjeneste.

Det er neppe noe behov for konfidensialitetsstøtte (kryptering), da opplysninger i byggesøknader ikke er underlagt taushetsplikt..

Det er ikke sikkert at man teknologisk må oppnå dette ved hjelp av PKI, men med PKI vil i all fall kravene være dekket.

Hvis vi ser på den praktiske utformingen av sikkerhetstjenestene er det også andre krav som må dekkes:

For de profesjonelle aktørene vil det være behov for at løsningen er effektiv, og relativt hurtig i bruk. For allmennheten er det mer behov for at løsningene er enkle og selvforklarende.

Da man ikke har identifiserte brukere på forhånd, må sertifikater være distribuert bredt på forhånd. Av samme grunn bør det være støtte for ulike sertifikatleverandører/samtrafikk.