UNIVERSITETET I OSLO

Institutt for informatikk

Hvor anvendelig er PKI?

Masteroppgave

30 studiepoeng

Jon Magne Nielsen

18. desember 2006

Innhold

1 Sammendrag

Denne oppgaven ser på bruken av elektronisk ID i statlige etater i Norge i dag. Det ses spesielt på om bruken av tekologien PKI er en god løsning på etatenes behov på dette området. Som utgangspunkt for analysen er det sett spesielt på to statlige etater. Disse etatenes behov og bruk av elektronisk ID generelt og PKI spesielt blir undersøkt.

Det er videre gjort rede for hvilke lover, forskrifter og andre førende dokumenter som danner de formelle rammebetingelsene for etaters bruk av PKI. Det offentliges behov for samordning av tjenester og i definering av felles krav blir beskrevet. Til slutt i oppgaven blir det vist at det er nødvendig å se på hensikten etatene har med å ta i bruk løsninger for elektronisk ID.

Teknologien som ligger til grunn for PKI blir beskrevet. Alternative teknologier til PKI som svar på behovet for elektronisk identifisering blir også beskrevet. Denne oppgaven ser på fordeler og ulemper ved tekologiene. Jeg fremsetter også en hypotese hvor jeg spør om PKI kan brukes til alt, og som jeg svarer på i konklusjonen.

2 Innledning

2.1 Om masteroppgaven

2.1.1 Gjennomføring

Dette er en masteroppgave ved som er gjennomført ved Institutt for informatikk ved Universitetet i Oslo. Oppgaven er gjennomført høstsemesteret 2006.

Oppgaven er gjennomført først og fremst gjennom litteraturundersøkelser, søk på Internett og intervju/dialog med nøkkelperson i hver av de to etatene. Det er som utgangspunkt for analysen lagt mest vekt på dagens situasjon og ikke så mye på fortid eller framtid. Oppgaven er en statusrapport som beskriver dagens situasjon innenfor det aktuelle fagfeltet. Forhold vedrørende historikk og videre fremtidig utvikling er bare summarisk berørt

Oppgaven er gjennomført av en masterstudent som til daglig er ansatt i Produktregisteret. Produktregisteret er en av to etater som vil bli nærmere analysert i denne oppgaven.

2.1.2 Disposisjon

Kapittel 1 er sammendraget av dokumentet.

I kapittel 2 gjengis oppgaveformuleringen, og det beskrives hvordan oppgaven er gjennomført . Videre er det tatt med definisjoner av en del sentrale begreper.

I kapittel 3 er det en gjennomgang av de grunnleggende begrepene som er viktig for forståelsen av oppgaven, en gjennomgang av det regelverk som skal danne basis for bruk av elektronisk ID i Norge og offentlig forvaltning spesielt, og dessuten en gjennomgang av teknologien som ligger til grunn.

I kapittel 4 er det en gjennomgang av to etater som er tatt som utgangspunkt for vurderingen av i hvilken grad de bruker elektronisk ID og PKI. Produktregisteret og Brønnøysundregistrene er to ulike etater som sammen gir et nyansert bilde på bruken av PKI og elektronisk ID. Det er også gjort en summarisk gjennomgang av bruken av PKI i andre etater til slutt.

I kapittel 5 analyseres bruken av PKI, behovene etatene faktisk har for PKI, om hvilken betydning disse forskjellene i behov har. Det er også gjort kategoriseringer av etater etter hvorfor de trenger elektronisk identifisering, da dette har betydning for hvilke teknologiske valg de bør gjøre.

I kapittel 6 fokuseres på de viktigste punktene i analysen.

2.2 Spørsmålsstillingen

2.2.1 Oppgaveformuleringen

Når kan og bør PKI brukes? Hvordan kan tillit opprettholdes i en åpen elektronisk kommunikasjon.

Med utgangspunkt i de problemstillinger en eller flere norske etater har med håndtering av elektronisk ID, undersøk om PKI er svaret på problemstillingene.

Det skal i undersøkelsen legges vekt på tekniske aspekter og på hvilken måte lover, regler og sentrale føringer har hatt betydning for etatenes beslutninger på området hvor PKI kan benyttes. Der behovet for internasjonalt samarbeid innen dette området har hatt betydning, skal dette drøftes.

2.2.2 Nærmere presisering/utdyping av oppgaveformuleringen

En spissformulert hypotese: PKI kan brukes til alt (der det er behov for elektronisk identifisering og signering).

Der begrepet digital signatur er benyttet, har det i denne teksten samme betydning som elektronisk signatur. Grunnen til at det hovedsakelig er brukt elektronisk, er at det er dette begrepet som stort sett brukes i lovverket.

Åpen elektronisk kommunikasjon betyr at kommunikasjonen er basert på internasjonale standarder. Det betyr når det gjelder PKI at kommunikasjonen er basert på sertifikater som er utstedt av godkjente sertifikatutstedere.

Det er et begrenset antall lover, regler og sentrale føringer som er relevante i denne oppgaven. I oppgaven er det her avgrenset til bare å gjelde førende dokumenter som har betydning for de aktuelle etatene som er lagt til grunn for besvarelse av oppgaven.

Kapittel 3.1 er det foretatt en detaljert gjennomgang av de viktigste begrepene for å forstå fagområdet elektronisk ID, signering og PKI.

2.2.3 Definisjoner

PKI (Public Key Infrastructure) – en tekologi som brukes til elektronisk signering og identifisering. PKI er en infrastruktur for digitale signaturer som er basert på teknologien om asymmetrisk kryptering

Autentisering – det å bringe på det rene at en person eller annet subjekt er den vedkommende utgir seg for å være.

Ikke-benekt – det å knytte en opplysning til en person slik at den ikke kan nekte å stå bak denne opplysningen.

Single-sign-on – det at man ikke trenger å autentisere seg mer enn en gang for å logge inn på en elektronisk tjeneste, selv om denne tjenesten består av en samling komponenter med hver sine sikkerhetsbehov og implementasjoner av sikkerhet.

Deklarant – deklarasjonsansvarlig firma.

2.2.4 Mål – hva har denne oppgaven til hensikt å påvise?

Hensikten med dokumentet er blant annet:

- Oppklaring av begreper, behov og roller.
- Påvisning av hvilke føringer som finnes
- Hvem som gir føringene
- Hvem som har interesser av at PKI-løsninger eksisterer.

Hensikten med en analyse av disse forholdene er at en slik analyse kan bidra til at det for beslutningstakere i virksomhetene som er aktører på dette markedet blir enklere å se hva som må legges vekt på ved innføring av elektronisk signering og elektronisk ID, spesielt rettet mot PKI. For disse er det mange teknologier og føringer å forholde seg til, som det kan være nyttig å forstå i en sammenheng.

3 Bakgrunnsmateriale

3.1 Sentrale begreper

En ID er data som unikt identifiserer en person. I denne oppgaven handler det om juridisk bindende identifikasjon. Det er spesielt personer det er viktig å identifisere. En ID brukes i en elektronisk sammenheng gjerne i relasjon til utveksling av data. Med en elektronisk signatur har man etablert en knytning mellom en person som har signert og de dataene denne personen har signert på. Bruk av elektronisk signatur i en kommunikasjon gjør at partene slipper å måtte ha egne kontrollrutiner. Det er tilstrekkelig at man har tillit til systemet og til en tiltrodd tredjepart som garanterer identiteten til de andre aktørene i systemet.

3.1.1 ID og eID

I en forpliktende kommunikasjon mellom to parter er det avgjørende at begge er sikre på hvem motparten er. Dersom en part ikke vet hvem motparten er, så må motparten legitimere seg. Man må legge fram et "bevis" for at man er den man gir seg ut for å være. Det er identitetene (ID) til de som kommuniserer som må avklares.

Innen lov og rett er en ID noe som er entydig knyttet til en person. Dette kan være en fysisk eller juridisk person. Det er imidlertid ikke definert entydig i lovverket hva en ID er.

Organisasjonsnummer brukes for å identifisere juridiske personer (enheter/foretak) i Norge, og tildeles ved registrering i Enhetsregisteret, som er et register under Brønnøysundregistrene. Organisasjonsnummeret består av ni siffer og starter på tallet 8 eller 9. [2]

Foretaksnummer, arbeidsgivernummer og momsnummer er eksempler på ulike numre som tidligere ble brukt av myndighetene for å identifisere en og samme enhet. Disse numrene er ikke lenger i bruk, men er i stedet erstattet av ett organisasjonsnummer som entydig identifiserer enhetene.

Fødselsnummer brukes for å identifisere fysiske personer som er eller har vært registrert som bosatt i Norge. Fødselsnummeret består av elleve sifre. De seks første sifrene viser fødselsdato. De tre neste sifrene er individnummer. De skiller mellom

personer som er født på samme dag, viser århundret vedkommende er født i og om personen er kvinne eller mann. De to siste sifrene er kontrollsifre. [4]

Når man skal identifisere en person er også hensikten med identifiseringen av betydning. I denne forbindelse er det relevant å spesifisere hvilke opplysninger om hverandre man trenger i en kommunikasjon ved siden av å vite at identifikasjonsbeviset er ekte. Ved en korrespondanse med en etat, kan det av og til være tilstrekkelig å bare identifisere at saksbehandleren representerer etaten, og ikke hvem den fysiske personen som er saksbehandler. Et annet eksempel kan være at det ved kjøp av alkohol i butikken vil være tilstrekkelig overfor den som sitter i kassen at identifikasjonen viser at man er over 18 år.

eID er en ID som benyttes i en elektronisk kommunikasjon. En eID kan defineres som den som undertegner, jfr esignaturlovens §3 punkt 4. [3], i en elektronisk kommunikasjon.

I NOU 2001:10 Uten penn og blekk [1] konstateres at "store deler av forvaltningen har tjenstlig behov for tilgang til korrekt navn og fødselsnummer i henhold til folkeregisteret". Et personsertifikatbegrep i offentlig sektor bør derfor muliggjøre en kobling til fødselsnummer.

3.1.2 Signatur og elektronisk signatur

En signatur er en måte å knytte et dokument til en identitet. Tradisjonelt gjøres dette ved å skrive med håndskrift navnet sitt på papirdokumentet. Ideen bygger på at det er vanskelig for andre å kopiere en slik håndskrevet signatur.

En signatur på et dokument betyr at mottakeren av dokumentet kan stole på at det er den personen som har signert som er opphavet til dokumentet (autentisering). Dersom avsenderen senere ikke vil vedkjenne seg dokumentet, kan mottakeren ved hjelp av den elektroniske signaturen bevise at det var avsenderen som signerte (ikke-benekt).

En elektronisk signatur er en elektronisk fremstilt knytning mellom en elektronisk identitet og elektronisk lagrede data.

I loven om elektronisk signatur (esignaturloven) defineres det tre forskjellige typer elektroniske signaturer avhengig av graden av følsomhet og graden av økonomisk konsekvens ved systemfeil/funksjonsfeil. Denne inndelingen bygger på at jo enklere den elektroniske signaturen er, jo mindre sikker kan man være på at signaturen er ekte. En sannsynlig grunn til at man deler inn i forskjellige sikkerhetsnivåer, er at det

er forskjell på hvor sikker man trenger å være (behovet), og at det er mer kostbart med de sikreste elektroniske signaturene.

Dessuten er esignaturloven en norsk implementasjon av EU-direktivet om en fellesskapsramme for elektronisk signatur [5]. I denne loven er det også på samme måte delt inn 3 sikkerhetsnivåer.

Disse nivåene er "elektronisk signatur", "avansert elektronisk signatur" og "kvalifisert elektronisk signatur". Kvalifisert elektronisk signatur er den mest sikre, og den det er detaljert spesifisert krav til i loven. Denne loven blir nærmere omtalt i kapittel 3.2.2

Hvem som kan bli utstedere av kvalifiserte elektroniske sertifikater er definert i Forskrift om krav til utsteder av kvalifiserte sertifikater [7].

En elektronisk signering skjer ved hjelp av en hemmelig unik kode (f.eks. et passord) som bare signaturholderen har sammen med en algoritme. Dette vil bli nærmere forklart i kapittel 3.3.1.

3.1.3 Tillit

Tillit er vesentlig i samfunnet. Stort sett alle handlinger der flere enn en person er involvert er basert på tillit i varierende grad og form.. Man har tillit til at ting fungerer og at noen har et ansvar for å "ordne opp" hvis ting eller tjenester/systemer ikke tilfredsstiller avtalt kvalitet eller kvantitet. Videre har den enkelte en forvenning om at samfunnet reagerer med påtale/straff ved grove, bevisste tillitsbrudd.

En forutsetning for at tillit er nødvendig er fraværet av å ha full oversikt. For eksempel har man tillit til at en TV skal skru seg på når en setter i strømmen uten å vite hvordan TV-en er satt sammen. "Tillit er en strategi for å håndtere usikkerhet og redusere kompleksitet", Engen [8].

I papirbaserte systemer er det altså mye tillit som ikke er regulert eller standardisert. Det er basert på normer og erfaringer. For eksempel hvis man skal legitimere seg med et vanlig ID-kort i dag, er det flere tillitsbetraktninger man legger til grunn. ID-kortet inneholder vanligvis bilde, navn, fødselsdato, utsteder og en del andre opplysninger. Disse opplysningene brukes i dag til å verifisere at ID-kortet som sådan er gyldig og at ID-kortet tilhører den personen som er i besittelse av kortet. I tillegg bekreftes opplysningen som er av aktuell interesse (f.eks. at fødselsdatoen tilsier at personen er over 18 år ved kjøp av alkohol).

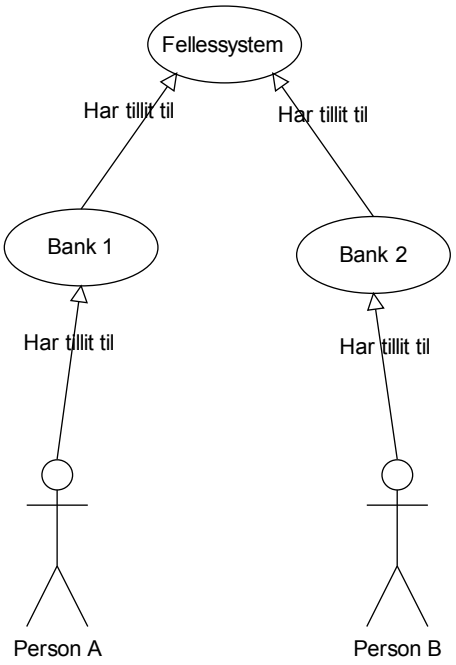
I dette eksempelet er det flere tillitsforhold:

- Først vil gjerne den som skal kontrollere ID-kortet validere kortet. Man ser om det ser ekte ut, at det kommer fra en utsteder man har tillit til. Man ser også på om kortet er ødelagt på noen måte som kan tyde på at det er kompromittert.
- Deretter vil man kontrollere om kortet tilhører den personen som holder det. Dette gjør man først og fremst ved å se på bildet, men også kjønn/alder er elementer i vurderingen.
- Til slutt vil man se etter den opplysningen man er interessert i, i dette tilfellet at eksempelvis reglementert aldersgrense er overholdt.

Et viktig aspekt ved tillit, som er illustrert ved dette eksempelet er at i stedet for å bruke tid på å bygge opp tillit til hverandre har man tillit til en utsteder av ID-kortet. Dette er en tredjepart som begge parter har tillit til.

Tillit i en elektronisk kommunikasjon kan etableres på tilsvarende måte. Først må det etableres en tiltrodd tredjepart som kan utstede et elektronisk sertifikat. Den elektroniske kommunikasjonen kan da utføres ved at avsenderen elektronisk signerer den opplysningen som er relevant med et sertifikat avsenderen har. Alle som da skal kontrollere denne opplysningen, vil først sjekke at sertifikatet er intakt og utstedt av en gyldig utsteder. Deretter kan man sjekke med tredjeparten om sertifikatet tilhører den personen som vi ønsker å motta den aktuelle informasjonen fra. Dersom disse kontrollene resulterer i en positiv bekreftelse, kan man til slutt hente ut de aktuelle dataene. De tekniske sidene ved dette vil jeg komme tilbake til i kapittel 3.3.

Tredjeparter kan tilsvarende ha tillit til andre. Slik tillit er ofte hierarkisk. Figur 1 viser et eksempel hvor en person A har tillit til Bank 1, mens en Person B har tillit til Bank 2. Begge bankene har tillit til et Fellessystem. Dette er en tillitskjede hvor Person A kan ha tillit til Person B gjennom tillitskjeden fordi elementene i denne kjeden har tillit til de andre delene av kjeden de er knyttet til.



Figur 1. Eksempel på en tillitskjede hvor A og B får tillit til hverandre.

I en elektronisk kommunikasjon er det ikke bare fysiske personer som kan inneha sertifikater, det kan også IT-løsninger.

I en del sammenhenger kan tillit kvantifiseres i kroner og øre. F.eks. Bank ID kan garantere 100.000 kr for at en signatur de har utstedt er ekte [6]. Her er det banken som er utsteder av Bank ID-sertifikatet som er garantisten.

Det er ikke alle sertifikater som er like generelle. F.eks. vil banken ikke garantere for identiteten for andre formål en bank-formål eller andre formål de eventuelt kan tjene penger på ved å ha denne garantistrollen.

IT-systemer som består av kommunikasjonsløsninger hvor man krever tillit mellom de som bruker systemet er ofte dedikerte. Det vil si at de er utviklet for et bestemt formål, og er ikke tenkt brukt til andre formål. Et annet bank-eksempel: i dag utsteder Skandiabanken sertifikater for bruk til pålogging på sin nettbank, men dette sertifikatet vil ikke Skandiabanken gå god for (det vil si ta økonomisk ansvar for) til annen bruk enn mot sin egen nettbank. Dersom Skandiabanken hadde blitt enige med BankID om at identitetene kunne brukes om hverandre i hvert nett og dermed ville tillitskjeden blitt utvidet.

Federering handler om å slå sammen slike tillitskjeder. Utfordringene ved federering går på det økonomiske (hvem skal være økonomisk ansvarlig for bruken), og på det tekniske samspillet (kompatibilitet). Når det gjelder kompatibiliteten er det også et økonomisk spørsmål hvem som er økonomisk ansvarlig hvis det oppstår kompatibilitetsproblemer. Siden federering handler om å slå sammen to registre med personopplysninger, er dette også noe som angår personvernet.

Et annet aspekt ved det med tillitsbegrepet er de enkelte brukernes tillit til at personopplysningene om dem selv ikke blir gjort tilgjenglige for uvedkommende og eventuelt misbrukt. Det er mange interessegrupper, blant annet Datatilsynet som er skeptisk til det å ha en felles elektronisk ID for alle formål. Datatilsynet mener dette gjør personer sårbare ved ID-tyveri og at det forenkler overvåkningen av personer.

3.2 Lover, forskrifter og sentrale begreper

Det som regulerer norske etaters bruk av elektronisk ID er de lover, regler og føringer som er gitt av norske myndigheter. Innen området elektronisk ID og elektronisk signering er det først og fremst esignaturloven som gjelder. Esignaturloven har sin basis i EU-direktivet Direktiv 1999/93/EC om en fellesskapsramme for elektronisk signatur.

I Norge er det grunnloven som er det overordnete, bestemmende regelverket. Der lovene ikke er i konflikt med grunnloven, gjelder den enekelte love. Der forskrifter ikke er i konflikt med lover eller grunnloven, gjelder den enkelte forskrift.

Generelt kan man si at bestemmelser som er gjort av Stortinget er overordnet bestemmelser gjort av Regjeringen, som i sin tur er overordnet bestemmelser gjort av departementene som igjen er overordnet for de underliggende etater. Forøvrig vedtar Stortinget også Statsbudsjettet som også gir instrukser for hvordan statlige etater skal forholde seg.

3.2.1 EU-direktivet

Om direktivet

Direktiv 1999/93/EC om en fellesskapsramme for elektronisk signatur har som hovedformål å legge til rette for fri flyt av tjenester og produkter basert på elektroniske signaturer, samt sikre elementær juridisk aksept av elektroniske signaturer på tvers av landegrensene.

Generelt er et direktiv et dokument som lages på EU-nivå. Et slikt dokument kan sees på som et kompromiss mellom medlemslandene i EU. Et direktiv skal inkorporeres i en nasjonal lov for hvert medlemsland (inkludert EØS). I Norge er EU-direktivet om elektronisk signatur inkorporert i lov om elektronisk signatur (esignaturloven) [3] med forskrifter. Det er Post- og teletilsynet som er den norske myndigheten som forvalter denne loven.

Bakgrunn og innføring

Forslaget til direktivet ble publisert i 1998, men forut for det var det en del medlemsland som hadde foreslått eller introdusert nasjonale lover om elektroniske signaturer fordi de så dette som en forutsetning for vekst innen e-handel og for å sikre tillit i elektronske transaksjoner.

For at slik nasjonal lovgiving ikke skulle være til hinder for fremtidig fri elektronisk handel i det indre markedet, og for å klargjøre den juridiske gyldigheten til elektroniske signaturer, kom direktivet på plass.

Alle de 25 medlemslandene i EU har nå tatt inn de generelle prinsippene i direktivet i sin nasjonale lovgivning.

Typene av elektronisk signatur i direktivet

Det er tre former for elektroniske signaturer som blir beskrevet i direktivet. Den første, elektronisk signatur ("electronic signature"), er den enkleste. Det kan være så enkelt som å signere en e-post med en persons navn, eller bruk av en pin-kode. Hensikten er å identifisere og autentisere data, og ikke entiteten (les: personen) som signerer.

Den andre formen for signatur i direktivet er avansert elektronisk signatur ("advanced electronic signature"). Kravene til denne signaturen er definert i artikkel 2.2 i direktivet. Direktivet er nøytralt med hensyn til valg av teknologi for fremstilling av de elektroniske signaturene, men denne formen for signatur refererer seg i praksis til PKI.

Den siste formen for signatur er omtalt i artikkel 5.1 i direktivet blir definert som kvalifisert elektronisk signatur ("qualified electronic signature"). Den er basert på et kvalifisert sertifikat og laget av en sikker signaturfremstiller som tilfresstiller kravene gitt i vedleggene I, II og III til direktivet.

I direktivet er den som signerer identifisert som "a person who holds the signature creation device and acts either on his own behalf or on behalf of the natural or legal

person or entity he represents". Det vil si at personen i prinsippet kan være enten en juridisk eller fysisk person.

Det indre markedet

Artikkel 3 i direktivet angir at en leverandør av sertifikattjenester som har blitt godkjent i ett medlemsland, skal kunne tilby sine tjenester i andre medlemsland basert på reglene gitt i sitt opprinnelsesland. Kravene til disse leverandørene er definert i vedleggene til direktivet (som igjen er innlemmet i nasjonal lovgivning), men det er opptil myndighetene i det enkelte medlemsland å bestemme hvordan de vil føre tilsyn med leverandørene av slike sertifikattjenester.

Følgene av direktivet

Det er laget en rapport [12] om hvordan direktivet har fungert i de første årene. Denne rapporten sier at direktivet har sørget for juridisk sikkerhet og forutsigbarhet mht gyldigheten av elektroniske signaturer i EU. Det er imidlertid eksempler på inkompatibilitet på interoperabiliteten. Videre sier rapporten at bruken av kvalifiserte elektroniske signaturer har vært mye mindre enn forventet. Videre er videreutviklingen av PKI-infrastruktur og markedet for omsetning av PKI relaterte tjenester i dag ikke i tråd med de forventningene og forhåpningene blant de som vedtok direktivet. Det er fortsatt bare to dominerende bruksområder som i dag har fått stort bruksvolum Det ene er utstedelse av elektroniske ID-kort. Dette utføres i regi av myndighetene i enkelte medlemsland. Det andre er bruken av engangspassord innen bank-sektoren.

Det er ingen enkle svar på hvorfor markedet for elektroniske signaturer ikke utvikler seg raskere. En årsak kan være at markedet enda ikke er modne for en så avansert teknologi som PKI representerer. En annen årsak kan være at de som tilbyr tjenester basert på denne teknologien ikke viser interesse for at deres løsning skal kunne samspille med andres løsninger. En tredje mulig årsak kan være at det mangler løsninger som bruker kvalifiserte elektroniske signaturer. Det pekes på at det kanskje ikke er tilstrekkelige incitamenter for å påta seg rollen som tiltrodd tredjepart, samt incitamenter for at disse tredjepartene skal garantere for bruken av hverandres løsninger. Det er også problemer med teknisk interoperabilitet over landegrensene. Smartkortet er den mest brukte enheten for bruk av PKI. Dette er en teknologi som har en relativt høy pris per signatur. Arkivering av elektronisk signerte dokumenter er også komplekst.

3.2.2 Esignaturloven

Esignaturloven er en norsk implementasjon av EU-direktiv 1999/93/EC om en fellesskapsramme for elektronisk signatur. Denne loven har derfor mye av de samme elementene i seg.

Hensikten med esignaturloven er å forankre bruken av elektroniske signaturer i norsk lov, definere forutsetninger og krav til signaturene og systemene signaturene skal fungere i, samt sikre interoperatibilitet på tvers av EU/EØS-området for elektroniske signaturer.

På samme måte som i direktivet er det i esignaturloven delt inn i 3 sikkerhets/kvalitetsnivåer for elektroniske signaturer:

1. "Elektronisk signatur" som er stiller krav om at det er data i elektronisk form som er knyttet til andre elektroniske data og der dette brukes som autentiseringsmetode for hvem som har signert.
2. "Avansert elektronisk signatur" er en sikrere elektronisk signatur hvor det stilles krav om at den er entydig knyttet til undertegneren, kan identifisere undertegneren, er laget ved hjelp av midler som bare undertegneren har kontroll over, og at det er knyttet til andre elektroniske data på en slik måte at det kan oppdages om disse har blitt endret etter signering. Det stilles ikke krav til hvordan dette skal gjøres.
3. "Kvalifisert elektronisk signatur" er en avansert elektronisk signatur som er basert på et kvalifisert sertifikat og fremstilt av et godkjent sikkert signaturfremstillingssystem. Dette er den sikreste elektroniske signaturen.

I loven blir det definert krav til kvalifiserte sertifikater og godkjente sikre signaturfremstillingssystemer. Blant annet skal et sertifikat inneholde opplysninger om sertifikatutstederen, undertegnerens navn (eller pseudonym med opplysning om at det er et pseudonym) og eventuelt ytterligere opplysninger om undertegneren, dersom de er relevante for bruken av sertifikatet, sertifikatets ikrafttredelses- og utløpsdato med mere.

Det er også definert roller og hvilke ansvarsområder disse rollene har. For eksempel stilles det krav til at sertifikatutsteder sørger for en hurtig og sikker katalog- og tilbaketrekkingstjeneste, og sikrer at det er mulig å fastslå dato og tidspunkt for ikrafttredelse eller tilbaketrekking av et sertifikat.

Det er Post- og teletilsynet som er myndigheten i Norge som forvalter og fører tilsyn med bruken av esignaturloven med forskrifter.

Tilhørende forskrifter er:

- Forskrift om krav til utsteder av kvalifiserte sertifikater mv. [7]. Denne forskriften definerer utstederne av kvalifiserte sertifikaters forhold til myndighetene (Post- og teletilsynet) og regulerer grunnlaget for Post- og teletilsynets tilsynsaktivitet innenfor dette fagområdet.
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) [13]. Denne forskriften er først og fremst en samling krav til offentlig forvaltning når de tar i bruk elektronisk kommunikasjon med andre.
- Forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere [14]. Denne forskriften etablerer selvdeklarasjonsordninger hvor sertifikatutstedere ved en selvdeklarasjon kan melde fra til et oppnevnt tilsynsorgan om at forskriftens krav er oppfylt. Formålet med forskriften er å høyne sikkerhetsnivået for sertifikattjenester og dermed øke tilliten til og bruken av slike tjenester. I forkriften vises til den til enhver tid gjeldende "Kravspesifikasjon for PKI i offentlig sektor". Videre defineres det 3 sertifikatklasser som er forskjellig fra typene av elektroniske signaturer i esignaturloven. Disse sertifikatklassene er "Person-Høyt", "Person-Standard" og "Virksomhet". Disse beskrives nærmere i kapittel 3.2.3.

De to største godkjente norske tilbyderne av kvalifiserte signaturer er Bank ID og Buypass. Bank ID eies av BBS (Bankenes Betalingssentral) og Byupass eies av Norsk Tipping og Posten Norge. Zebsign, som ble godkjent først, er nå kjøpt opp av BBS. Bank ID og Buypass har garantibeløp på sine sertifikater på henholdsvis 100 000 kr og 5 000 kr.

Hele tabellen med tilbydere av kvalifiserte elektroniske sertifikater (hentet fra Post- og teletilsynet [29]:

Navn	**Reg.dato**	**Sertifikatpolicy**	**Merknad**
ZebSign AS	25.04.2002	ZebSign Person ID Policy	Angivelse av at sertifikatet er kvalifisert
ZebSign AS	03.02.2003	ZebSign Community ID Policy	Angivelse av at sertifikatet er kvalifisert
Buypass AS	11.05.2005	Certificate Policy Buypass Class 3 Certificates	
Commfides Norge AS	29.11.2005	Certificate practice statement. Commfides Class 3 Certificates	

Navn	**Reg.dato**	**Sertifikatpolicy**	**Merknad**
Fokus Bank ASA	16.02.2006	Norsk BankID sertifikatpolicy for banklagrede kvalifiserte sertifikater til personkunder	Sentrallagret løsning
Bankenes ID-tjeneste AS	22.05.2006	Norsk BankID sertifikatpolicy for banklagrede kvalifiserte sertifikater til personkunder	Sentrallagret løsning RA som er tilknyttet utsteder Om RA (registerings- autoritet) for Norsk Bank ID
DnB NOR Bank ASA	28.06.2006	Norsk BankID sertifikatpolicy for banklagrede kvalifiserte sertifikater til personkunder	Sentrallagret løsning
Nordea Bank Norge ASA	29.06.2006	Norsk BankID sertifikatpolicy for banklagrede kvalifiserte sertifikater til personkunder	Sentrallagret løsning
Terra-Gruppen AS	30.06.2006	Norsk BankID sertifikatpolicy for banklagrede kvalifiserte sertifikater til personkunder	Sentrallagret løsning RA som er tilknyttet utsteder Om RA (registerings- autoritet) for Norsk Bank ID
Sparebank 1 Utvikling DA	03.07.2006	Norsk BankID sertifikatpolicy for banklagrede kvalifiserte sertifikater til personkunder	Sentrallagret løsning RA som er tilknyttet utsteder Om RA (registerings- autoritet) for Norsk Bank ID

3.2.3 Kravspesifikasjonen for PKI i offentlig sektor

Formål og bakgrunn

Kravspesifikasjonen for PKI i offentlig sektor er en overordnet, funksjonell kravspesifikasjon for anskaffelse av PKI (Public Key Infrastructure) til bruk i forbindelse med elektronisk kommunikasjon med og i offentlig sektor. Denne kravspesifikasjonen skal legges til grunn for felles rammeavtaler for bruk i offentlig sektor. Elektronisk kommunikasjon med offentlig sektor har vært et politisk mål, bl.a. for å forenkle og effektivisere tilgangen og kommunikasjonen mot og innenfor den offentlige forvaltningen. Grunnlagsdokumenter for kravspesifikasjonen er blant annet esignaturloven og rapportene fra SEID-prosjektet. For mer om SEID, se kapittel 3.3.3.

Et av målene er at kravspesifikasjonen skal kunne forenkle vurderinger rundt valg av sikkerhetsmekanismer for ulike anvendelser i forvaltningen. Det er et mål at

kravspesifikasjonen skal dekke de antatt mest vanlige behovene for elektronisk ID, signatur og kryptering. Forfatterne av kravspesifikasjonen har gjort antakelsen om at kravene som ligger til grunn for Altinn og de beslektede systemene i den norske helsesektoren er dekkende for disse behovene.

Bruk av kravspesifikasjonen

Hensikten med kravspesifikasjonen er at den skal legges til grunn for alle offentlige forespørsler om tilbud av aktuelle produkter og tjenester innen PKI-området.

På grunnlag av kravspesifikasjonen vil det bli utarbeidet spesifikke produkt- eller tjenestebeskrivelser som det kan foretas enkeltanskaffelser i henhold til eller det kan med bakgrunn i disse inngås en eller flere rammeavtaler med en eller flere tilbydere. En enkelt rammeavtale eller enkeltanbud trenger ikke omfatte alle tjenestene/kravene i kravspesifikasjonen, men bare de som er relevante.

Omfang

PKI dekker kravene til løsninger for autentisering/identifisering, signering og kryptering (ikke krypteringen i seg selv, men krypteringsnøkkelutvekslingen) for kommunikasjon i og med offentlig virksomhet.

En vanlig inndeling i hovedfunksjoner når det gjelder PKI kan være:

- sertifikatutsteder (SA) som utsteder og verifiserer digitale sertifikater
- registreringsautoritet (RA) som verifiserer opplysninger som skal inngå i et sertifikat
- katalog- og oppslagstjenester

Kravspesifikasjonen stiller krav innen disse områdene. I tillegg stilles det krav når det gjelder bl.a. løsninger/integrasjon og samtrafikk/samspill.

Kravtabeller

Kravspesifikasjonen er bygd opp av en rekke krav som er nummererte. Disse kravene er gruppert inn i tabeller med ett krav per rad. I tabellene har kolonnene kravnummer, selve kravet – tekstlig beskrevet, en kolonne som sier hvor viktig det er at kravet tilfredsstilles, samt en kolonne som indikerer om leverandøren som leverer en løsning mener kravet er tilfredsstilt i tilbudet.

Sikkerhetsnivåer

Dette er sertifikatklasser som samsvarer med Forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere, og ikke sikkerhetsnivåene i esignaturloven:

Person-Høyt	Her stilles det kav om kvalifisert signatur slik det er definert i E-signaturloven [5]. Sertifikatet skal være utstedt av sertifikatutsteder som er godkjent. Sertifikatutsteder skal ha rutiner som bl.a. medfører personlig frammøte for å få sertifikatet. Det stilles krav om to-faktor autentisering (f.eks vha smart-kort).
Person-Standard	Her stilles det ikke kav om kvalifisert signatur slik det er definert i E-signaturloven. Sertifikatet skal være utstedt av en sertifikatutsteder som er godkjent. Sertifikatutsteder trenger ikke ha rutiner som krever personlig frammøte, men at de har sikkerhet tilsvarende at sertifikatet sendes til folkeregistrert adresse. Det stilles ikke krav om to-faktor autentisering.
Virksomhet	Sikkerheten er her noenlunde tilsvarende som for Person-Standard.

Krav gitt i kravtabeller

I kravtabellen "Overordnede krav til leveransen" stilles det krav til sertifikatautoritet og registreringsautoritet, katalog og oppslagstjenester, integrasjonspakker, brukervennlighet, leveransekapasitet, informasjonssikkerhet og utbredelse. Dette er overordnede krav som definerer/avgrenser tilbudet.

Det er fire kravtabeller med krav til nøkler og sertifikater. Først stilles en del generelle krav. Dette omfatter bl.a. krav til nøkkelgenerering, tilbakekallingstjensete, fornyelse, algoritmer og nøkkellengde. Deretter stilles det krav som gjelder for personsertifikater i sertifikatklasse Person-Høy. Her stilles det bl.a. krav til at sertifikatet skal være kvalifisert iht. E-signaturloven og hvordan den private nøkkelen sikres, samt levetiden til sertifikatet. Videre stilles det krav som gjelder for personsertifikater i sertifikatklasse Standard. Her stilles det bl.a. krav til identifikasjon av sertifikatsøker, hvordan den private nøkkelen sikres, samt levetiden til sertifikatet. I den siste kravtabellen for nøkler og sertifikater stilles det krav til virksomhetssertifikater. Her spesifiseres det bl.a. krav til identifikasjon av virksomheten, hvordan den private nøkkelen sikres, samt levetiden til sertifikatet

Det er to kravtabeller med krav til katalog og oppslagstjenester. Den ene kravtabellen omhandler sertifikatkataloger og tilbakekallingslister. Her defineres det krav til driftsmessige aspekter som ytelse, oppetid. Den andre tabellen er krav til kobling til fødselsnummer.

I kravtabellen med krav til RA tjeneste, stilles det krav til at leverandøren skal tilby både sentral og lokal registreringsautoritets-tjeneste/-utstedelsesprosess. Det stilles forskjellige krav til RA-tjenesten avhengig av om sertifikatene som utstedes er personsertifikater i sertifikatklasse Høy, personsertifikater i sertifikatklasse Standard eller virksomhetssertifikater.

I kravtabellen med krav til signaturfremstillingssystem, er det stort sett referanser og gjengivelse av andre standarder, bl.a. EU-standarder.
Det er egne kravtabeller for brukskvalitet, for krav til integrasjon i applikasjon, for krav til hvilken maskinvare eller programvare som skal brukes i løsningen og kvaliteten på brukerstøtten. Leverandøren skal spesifisere og framskaffe all nødvendig dokumentasjon for tjenesten slik at det er tilgjengelig for gjennomsyn av kunden. Det er definert krav i en egen kravtabell for hvilken dokumentasjon som kan tilbys. Responstider og tilgjengelighet skal spesifiseres i en egen kravtabell.

I kravtabellen med krav til samspill og samtrafikk er det et overordnet ønske at flest mulige løsninger for elektronisk signatur skal være kompatible med hverandre. Dette vil i sin tur bl.a. føre til at brukerne slipper å ha mange forskjellige elektroniske signaturer i ulike sammenhenger.

Det er også en kravtabell over opsjoner som omfatter krav som ofte ikke er aktuelle, det vil si de er for spesielle typer bruk. Dette inkluderer krav til tidsstempling, notartjeneste, langtidslagring, tilgjengelighet, sikkerhetsportal, løsning for intern bruk i offentlige virksomheter og hardware-basert løsning for virksomhetssertifikater.

Vedlegg til kravspesifikasjonen

Det er 5 vedlegg til kravspesifikasjonen. Det første vedlegget gir en utdyping og forklaring av sikkerhetsnivåene som er brukt i kravspesifikasjonen. Det andre vedlegget er en vurdering av krav til sikkerhetsnivåer ved elektronisk kommunikasjon med forvaltningen. De øvrige vedleggene beskriver arbeidsgruppens og referansegruppens sammensetning, samt omfatter en ekstern oppsummering av SEID-workshop om samtrafikk mai 2004 og SEID-prosjektets Leveranse oppgave 1 "Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater".

3.3 Teknologi

Hvis man skal ha en elektronisk kommunikasjon mellom to parter i dag, hvor partene skal være sikre på at motparten er den de utgir seg for å være kan dette løses ved hjelp av forskjellige tekologier i dag. En elektronisk signatur på et dokument er data som er et resultat av en kryptering av en verdi som igjen et resultat av å kjøre dokumentet gjennom en Hash-algoritme. Biometriske løsninger er også mulig å benytte i løsninger med elektronisk ID, men er fortsatt ikke vanlige i Norge.

3.3.1 Symmetriske nøkler

Den eldste formen for en av to kommuniserende parter å verifisere at en elektronisk kommunikasjon var skrevet av den andre parten, var at de krypterte meldingen med et passord bare de to visste. En slik kryptering kan skje ved at de opprinnelige dataene blir behandlet av en krypteringsalgoritme. De krypterte dataene blir da sendt til mottakeren som bruker sin dekrypteringsalgoritme for å hente tilbake de opprinnelige dataene. Et eksempel på en enkel form for slik kryptering er at man i en tekst bytter ut bokstaven A med B, B med C og så videre til slutt Å med A. Mer avanserte algoritmer tar en kode/passord som parameter, og der er gjerne selve algoritmen åpen. Det er også mulig å legge til tidsstempel, sekvensnummer og kontrollkoder for å sikre at meldingen ikke er endret eller forsinket. Dette kalles symmetrisk kryptering, siden samme nøkkel brukes til kryptering og dekryptering.

Den største fordelen med symmetriske nøkler er at algoritmene er raske i forhold til hvor sterk krypteringen er. Ulempen er at den er sårbar å bruke når det er mange involvert, fordi mange da har tilgang til den hemmelige nøkkelen, og hvis den kommer på avveie, må alle bytte den ut.

En måte å bruke symmetriske nøkler til autentisering av en melding uten å kryptere hele teksten, er at man har en algoritme som beregner en autentiseringskode basert på alle tegnene i teksten, og at denne algoritmen mottar et passord som parameter. En slik algoritme kalles gjerne en MAC-algoritme [9, s. 55]. MAC-en til meldingen sendes med meldingen, og mottakeren kan påvise at det er en autentisk melding ved å kjøre samme algoritme. Det er flere algoritmer som kan brukes til å generere en MAC, blant annet den mest vanlige symmetriske krypteringsalgoritmen DES.

3.3.2 Hash-algoritmer

En annen type algoritmer for å lage en autentiseringskode er enveis hash-funksjoner. Dette er avanserte funksjoner som tar en variabel lengde tekst som inndata og produserer utdata med en bestemt lengde. Algoritmene som i dag brukes til elektronisk signering er basert på hash-funksjoner.

Krav til en hash-funksjon H [9, s. 59]:

1. H fungerer på data uavhengig av størrelsen på datamengden.
2. H produserer en fast lengde utdata (blokk).
3. H(x) er relativt enkel å beregne for alle verdier av x, slik at både maskinvare- og programvareimplementasjoner av algoritmen er brukbare.

4. For alle blokkverdier av h, er det nær umulig ("computationally infeasible") å kunne beregne den opprinnelige teksten x slik at H(x) = h. Dette er ofte omtalt som enveis-egenskapen ved slike algoritmer.
5. For alle verdier av teksten x, skal det være nær umulig ("computationally infeasible") å finne andre tekster som gir samme hash. Det vil si det skal være nær umulig å finne en $y \neq x$ med H(y) = H(x). Dette er ofte omtalt som svak kollisjonsmotstand ("weak collision resistance").
6. Det er generelt nær umulig å finne to sett data (x, y) slik at H(x) = H(y). Altså det å finne to ulike opprinnelige tekster som gir samme hash-verdi. Dette omtales ofte som sterk kollisjonsmotstand ("strong collision resistance").

Eksempler på sikre hash-funksjoner er MD5, SHA-1 og SHA-256.

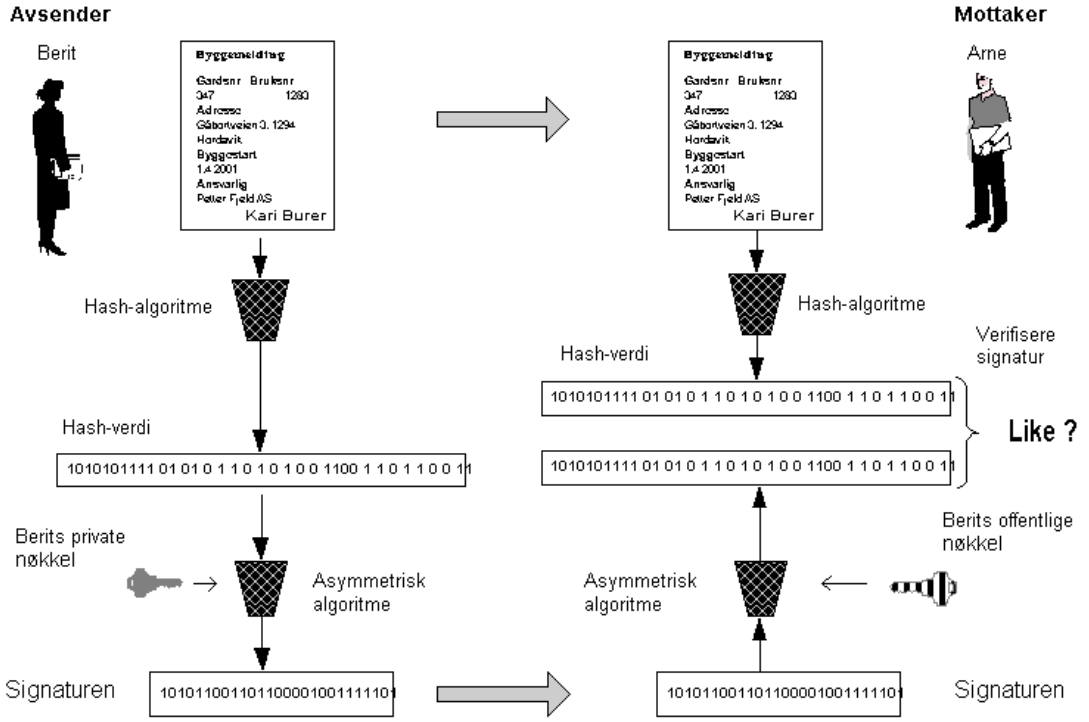
3.3.3 Asymmetriske nøkler

Asymmetriske nøkler går ut på at hver av de to partene har to nøkler hver. Hver part har altså et nøkkelpar som består av en offentlig og en privat nøkkel. Den offentlige nøkkelen er åpent tilgjengelig, mens den private nøkkelen må hver enkelt part holde for seg selv. Til asymmetrisk kryptering brukes spesielle matematiske metoder slik at ved genereringen av nøkkelparet vil det være følgende sammenheng mellom de to nøklene: dersom man krypterer en informasjon med den offentlige nøkkelen, er det bare mulig å dekryptere den ved hjelp av den private nøkkelen.

Asymmetrisk kryptering gjør at man kan bestemme hvem som kan lese et dokument ved å kryptere dokumentene med mottakernes offentlige nøkkel. Ingen andre vil da kunne lese dokumentet. Ulempen er at disse algoritmene er forholdsvis trege. En vanlig løsning på dette er at dokumenter krypteres med symmetrisk kryptering ved hjelp av en engangsnøkkel. Deretter krypteres bare engangsnøkkelen med asymmetrisk kryptering.

Lengden på en asymmetrisk nøkkel sier noe om hvor sikker den er. Etter hvert som datamaskinene får større og større regnekraft, er det nødvendig med lengre nøkkel for å sikre seg at nøkkelen ikke blir kompromittert.

Tilsvarende kan hash-verdier fra et dokument krypteres med asymmetrisk kryptering. Den krypterte hash-verdien er en elektronisk signatur.



Figur 2. Hentet fra figur 3.2 [22]. Dette illustrerer signering og verifisering av et dokument.

3.3.4 PKI

I NOU 2001:10 Uten penn og blekk [22] er en rapport avgitt av et utvalg som var bredt representert fra offentlig forvaltning og ledet av FAD. Utvalget utredet en policy for offentlig forvaltning på området bruk av digital signatur, dokumentkryptering for konfidensialitetsformål og tilhørende infrastruktur (PKI). I kapittel 3 [22] står det at "den mest lovende, og stadig mer brukte løsningen for elektroniske signaturer i dag, er digitale signaturer med tilhørende infrastruktur, såkalt PKI (Public Key Infrastructure).". Dette er en holdning som fortsatt er sterkt gjeldende i FAD. Siden FAD er det departementet som har ansvaret for IT-politikken i Norge, er det interessant å se nærmere på denne teknologien som en løsning på behovene for hvordan tillit kan opprettholdes i en åpen elektronisk kommunikasjon.

Rapporten [22] gir i kapittel 3 en god beskrivelse av hva PKI er, og er utgangspunkt for beskrivelsen av PKI nedenfor.

PKI er en infrastruktur for digitale signaturer som er basert på teknologien om asymmetrisk kryptering.

PKI har fire egenskaper som er vesentlige å ivareta når man skal innføre elektronisk samhandling over nett i stor skala (hentet fra [22]):

Autentisering – muligheter for å vite hvem avsenderen av en elektronisk meddelelse er.
Integritetsbeskyttelse – muligheter for å sikre meddelelsen slik at alle forsøk på endringer blir oppdaget.
Konfidensialitetsbeskyttelse – muligheter for å forvrenge innholdet (kryptere) slik at det blir uleselig for andre enn mottakeren.
Sikring av ikke-benekting – muligheter for å knytte innholdet til avsenderen slik at vedkommende ikke kan nekte for å stå bak det.

Et digitalt sertifikat er en samling data i tilknytning til den unike offentlige nøkkelen til en person som bekrefter på en tillitvekkende måte at det er riktig identitet.
Et kvalifisert elektronisk sertifikat er et sertifikat som har en tillitvekkende knytning mellom en identitet og en kvalifisert elektronisk signatur.

Dersom to parter som ikke kjenner hverandre fra før skal kommunisere ved hjelp av asymmetrisk kryptering, trenger de å etablere tillit. Dette kan være gjennom en tillitskjede, hvor en tredjepart som begge har tillit til, kan ta på seg å bekrefte sammenhengen mellom den offentlige nøkkelen og eieren av nøkkelparet. En slik virksomhet kalles ofte for tiltrodd tredjepart (TTP). En viktig oppgave for en TTP er å være sertifikatutsteder. Dette er en rolle som er definert i Esignaturloven. En vanlig måte å etablere tillit til et sertifikat er å signere sertifikatet med en elektronisk signatur. Dette gjøres av sertifikatutstederen.

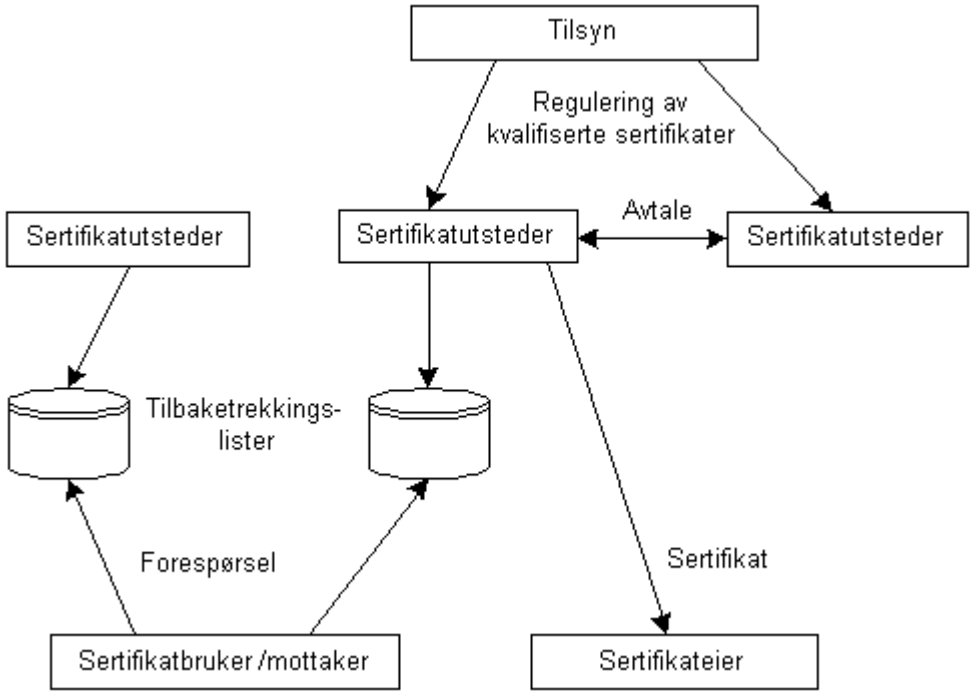
Dersom infrastrukturen skal være åpen, forutsetter dette at kommunikasjonen foregår etter standardiserte protokoller mellom parter som har tillit til hverandre. Denne tilliten kan inngås mellom to sertifikatutstedere.

En viktig forutsetning for at en infrastruktur skal være åpen er gjensidige garantier. Det er sertifikatutstederen som er ansvarlig for hvor sikkert sertifikatet er, og som derfor må garantere for i hvilken grad det er ekte. I hvor stor grad en sertifikatutsteder har tillit til en annen måles i penger. En annen viktig forutsetning for en åpen infrastruktur som brukes til dokumenter som må være signert, er at denne infrastrukturen er etablert i henhold til lover og forskrifter som gjelder for området. Esignaturloven danner grunnlaget for denne forankringen.

En viktig oppgave for sertifikatutsteder er å holde oversikt over de til enhver tid gyldige sertifikatene. Utstederen må ha et sikkert system for utlevering av sertifikater,

ha et raskt system for å trekke tilbake sertifikater som har blitt kompromittert, og ha denne katalogen tilgjengelig for alle som skal ha verifisert et sertifikat. Sertifikater utstedes for begrensete tidsperioder, ofte 2 år om gangen. Sertifikatutsteder lagrer kopier av dem i en katalog slik at de er tilgjengelige for sertifikateierens samhandlingspartnere. De sertifikatene som tidligere har vært gyldige, men som ikke lenger er gyldige kunngjøres i en egen liste, såkalt tilbaketrekkingsliste. Denne listen tidsstemples og signeres av den sertifikatutstederen som har trukket sertifikatet tilbake.

Det er som regel sertifikatutsteder som genererer nøkkelparet som sertifikateieren skal benytte. I noen tilfeller kan sertifikateieren selv generere sitt nøkkelpar for så å sende sin offentlige nøkkel til sertifikatutstederen og få et sertifikat i retur. De private nøklene må oppbevares trygt, for eksempel i et smartkort, på en diskett eller kryptert på harddisken.



Figur 3. Hentet fra figur 3.7 [22]. Figuren illustrerer tillitsforholdene i en PKI.

3.3.5 X.509 og SEID

Hvis et sertifikat skal brukes i stor skala i en i PKI, må det være standardisert. Sertifikatutstederne må utstede sertifikatet i henhold til en sertifikatpolicy.

X.509 er en svært utbredt teknisk standard for sertifikater. Standarden beskriver feltene sertifikatet skal være bygget opp av. For at sertifikatene skal fungere i en åpen infrastruktur er det viktig at alle feltene tolkes likt av alle systemene som bruker dem.

Uten penn og blekk [22] og senere, de tre leveransene fra SEID-prosjektet [10, 26, 27] definerer norske tilpasninger/tolkninger/utvidelser/presiseringer til feltene i X.509. Dette er hovedsakelig for å tilpasse den tekniske standarden for sertifikater til det norske regelverket, det vil si esignaturloven med tilhørende forskrifter, samt Kravspesifikasjonen for PKI i offentlig sektor.

Første leveranse i SEID-prosjektet (samarbeidsprosjekt for eID og eSignatur) [10] hadde følgende mandat: "Med utgangspunkt i relevante internasjonale standarder, utarbeide en norsk profil for personsertifikater som skal dekke bruken av både kvalifiserte sertifikater og sertifikater med tilsvarende tillit- og kvalitetsnivå. I tillegg skal en norsk profil for virksomhetssertifikater utarbeides". SEID-prosjektets arbeidsgruppe bestod av representanter for næringslivet.

Hovedutfordringene med å få tilpasset X.509 til norske forhold er knytningen til norske regelverk og tegnsettproblemer.

Når det gjelder tilpasningene av felter, er det i esignaturloven definert tre typer signaturer. Det er ingen felter i den nåværende X.509 standarden (X.509v3) som kan brukes til å beskrive hvilken av disse tre typer elektronisk signatur sertifikatet representerer. Også i Kravspesifikasjonen for PKI i offentlig sektor skilles det mellom sertifikater (Person-høy, Person-lav og Virksomhet), som det er nødvendig å gjøre en tilpasning til for å få representert.

Det er viktig at disse norske tilpasningene i så stor grad som mulig er i overensstemmelse med den internasjonale standarden, og da videre også i tråd med tilsvarende tilpasninger i andre land. Den norske profilen har tilpasninger på tre basisfelter, samt sju sertifikatutvidelser.

Den andre utfordringen med tilpasning av X.509 til norske forhold gjelder tegnsett. For eksempel er det krav om at det i sertifikatet skal stå navnet på sertifikateieren. Dersom dette navnet har norske bokstaver som ÆØÅ, er dette typiske problemer hvis man skal kommunisere med andre land.

Problemet med tegnsett gjelder imidlertid også i andre sammenhenger i Norge. Dette kan for eksempel være mellom to datamaskiner som er ulikt konfigurert. Forskjeller i konfigurasjon kan oppstå når man bruker forskjellig tegnsett, forskjellig versjon av programvare og så videre.

I Buypass har man opplevd at det med å skrive navnet korrekt kan by på problemer. I begynnelsen i feltet for utsteder av sertifikatene skrev de "Buypass". Men kravet var at det skulle stå helt korrekt navn på utsteder. Etter hvert endret de dette derfor til "Buypass AS". For oss mennesker ser vi at dette dreier seg om samme firma, men med maskinell sammenlikning er to ulike tekst-strenger.

Den andre leveransen av SEID-prosjektet [26] definerte et grensesnitt mot oppslagstjenester. Oppslagstjenesten er en tjeneste som tilbyr brukersteder tilgang til å forespørre informasjon om sertifikatinnehaver som ikke fremgår av sertifikatinnehaverens sertifikat, for eksempel sertifikatinnehaverens fødselsnummer.

Den tredje leveransen av SEID-prosjektet [27] omhandlet signering av dataobjekter for langtidslagring. Denne leveransen tar for seg hovedutfordringene ved langtidslagring av elektronisk signert materiale. En av disse utfordringene er å ta vare på og, ved behov, utveksle all tilleggsinformasjon som er nødvendig for at signaturen skal kunne valideres i ettertid. For PKI-baserte elektroniske signaturer vil tilleggsinformasjon typisk omfatte Sertifikater og annen tilknyttet Valideringsdata som er nødvendig for å kunne bekrefte gyldigheten av sertifikatene på det tidspunkt signaturen ble laget. En annen utfordring ved langtidslagring er at enhver elektronisk signatur av natur har en tidsbegrenset kryptografisk levetid samt potensielle svakheter ved de hash-algoritmer som er blitt benyttet.

3.3.6 Biometriske løsninger

Alle mennesker har statiske og dynamiske psykologiske/oppførselsmessige biologiske særtrekk som er med på å identifisere hvem vi er i forhold til omverden. Disse trekkene kan brukes av IT-systemer til å identifisere personene. Typiske biologiske karakteristiske egenskaper [24] er:

- ansiktsproposjoner og form
- iris og retina mønstre
- fingeravtrykk
- DNA
- stemmen

Fingeravtrykk og DNA er biologiske karakteristikker som også blir brukt til sikker identifisering i rettssaker. Til denne bruken er sikkerheten for at det er korrekt identifisering høy.

Det finnes også løsninger montert på for eksempel flyplasser for å grovsortere store menneskemengder som går forbi for å gjenkjenne spesielle personer (for eksempel terrorister) basert på egenskaper som bevegelsesmønstre (om man hinker, armbevegelser og lignende), høyde og så videre. Disse løsningene har en svært høy feilrate.

Til forskjell fra elektronisk ID som baserer seg på PKI, opereres det når det gjelder biometriske løsninger med sannsynligheter for å identifisere riktig. For å kvantifisere disse sannsynlighetene opereres det med toleransegrenser:

- FAR (false acceptance rate) – hvor mange ganger systemet feilaktig vil gi en positiv identifisering (falske positive).
- FRR (false rejection rate) – hvor mange ganger systemet ikke vil gi en postiv identifisering der det skulle vært gitt (falske negative).

I dag er fortsatt biometriske ID-løsninger for usikre til alene å kunne bli brukt til elektronisk signering. Det finnes eksempler på hvordan sikkerheten kan kompromitteres på de forskjellige biometriske ID-løsningene [22 s. 12]

En annen ulempe med biometriske ID-løsninger er at det brukerne av løsningen skal sikre sannsynligvis har lavere verdi enn det som er nøkkelen. For eksempel rapporterte BBC [25] om at en Mercedes med fingeravtrykkidentifisering som middel mot at bilen skulle bli stjålet hadde resultert i at fingeren til bileieren var blitt kuttet av. Sannsynligvis har tross alt fingeren høyere verdi for bileieren enn bilen.

For IT-systemer som inngår i en løsning basert på biometrisk identifisering, vil det ikke være mulig for en maskin å signere. All identifisering knyttes til en bestemt person. Identifisering tilsvarende virksomhetssertifikatet som defineres i Kravspesifikasjonen for PKI i offentlig sektor vil derfor ikke være mulig.

I USA vil det i 2008 bli nye krav til førerkortene. Siden 11. september 2001 har myndighetene vært svært opptatt av sikkerhet, og det er forventinger [11] til at man vil definere en enhetlig standard som vil omfatte biometriske data. I Malaysia utstedes i følge en artikkel i New Scientist [26] legitimasjonskort med biometrisk identifikasjon til alle landets innbyggere. Legitimasjonskortet er standard kredittkortstørrelse og inneholder en chip (et såkalt smartkort) hvor det blant annet er lagret biometrisk informasjon om kortinnehaveren.

Innen biometrisk identifisering foregår det mye forskning. Forskningen går først og fremst på å øke treffsikkerheten på de eksisterende teknologiene, men også på å finne nye typer biologiske karakteristika som kan gi en enda mer treffsikker identifisering. Det forskes også på å gjøre løsningene mer effektive og enkle å bruke.

3.3.7 Identifisering og internasjonale forhold

I utlandet er det ofte sterk skepsis til at sentrale myndigheter skal ha en sentral database over alle personer med en unik ID per person. Det er også stor forskjell på hvilke typer ID-sertifikater/-bevis som finnes i ulike land. Hva som finnes av personregistre er i stor grad avhengig av historiske forhold, det vil si i hvilke sammenhenger det har vært behov for slike registre. Det er i de forskjellige land også forskjell på kvaliteten i personregistrene.

I Norge er det ikke noe sentralt folkeregisterinstitutt. Det er Skatteetaten som tildeler fødselsnummer, men i hvor stor grad de vedlikeholder kvaliteten på registeret er avhengig av hvilke incitamenter de har for å holde det ajour. Trygdeetaten er en etat som bruker disse fødselsnumrene i stor grad. Siden Trygdeetaten betaler ut trygd til personer basert på fødselsnummer, har de ofte større økonomisk interesse av at kvaliteten på fødselsnumrene er høy enn det Skatteetaten har.

4 Undersøkelser om bruk

De to etatene det i denne oppgaven er valgt å se på er Produktregisteret og Brønnøysundregistrene, og da spesielt Altinn-løsningen til Brønnøysundregistrene. Dette er to statlige etater som er underlagt hvert sitt departement, og har ulike behov knyttet til elektronisk ID.

Et moment som skiller etater sine behov i forhold til elektronisk ID fra andre virksomheter, er at dette er virksomheter som har monopol på tjenestene sine og ikke har til hensikt å gå med overskudd. Motivet er derfor ikke å tjene penger på det, men å spare penger på det gjennom forenklinger og automatiseringer.

En drivkraft for etatene for innføring av tjenester basert på elektronisk ID er også politiske føringer. Alle etater får fra sine respektive overordnede anmodninger om å tilrettelegge for elektroniske tjenester for å forenkle kontakten med brukerne, for å kunne tilby tjenestene større deler av døgnet, og for at tjenestene skal være tilgjengelig der brukerne er (for eksempel hjemme), samt ønske om forenkling hvor man ser de ulike tjenestene i sammenheng.

Ved undersøkelse av etatene sees det spesielt på aspekter som:

- sammenhenger
- fellesnevnere
- utfordringer

mellom disse to etatene.

4.1 Produktregisteret

4.1.1 Om Produktregisteret

Produktregisteret er et statlig register over farlige kjemikalier som omsettes i Norge Produktregisteret ble opprettet ved et stortingsvedtak i 1981. Produktregisteret er i dag underlagt Miljøverndepartementet. I §21 i Forskrift om klassifisering, merking mv. av farlige kjemikalier [17], er det definert hvilke kjemikalieopplysninger som er pliktige å melde inn til Produktregisteret. Mikrobiologiske produkter skal dessuten meldes inn i henhold til Forskrift om deklarering og merking av mikrobiologiske produkter som ved bruk vil kunne tilføres det ytre miljøet. Ut over dette er det ingen lov eller forskrift som direkte definerer Produktregisterets oppgaver.

Det dokumentet som derfor definerer mål og oppgaver for Produktregisteret er Stortingsproposisjon nr 1 (statsbudsjettet). I statsbudsjettet for 2007 [15] er Produktregisterets mål definert til å "samle inn, systematisere og arkivere opplysningar om kjemikaliar, leggje til rette opplysningar ut frå registrerte data slik at definerte brukarar får tilgang til riktig informasjon, og omarbeide graderte data til ugradert informasjon for å gjere opplysningane meir allment tilgjengelege.". Disse definerte brukerne er andre statlige etater: Arbeidstilsynet, Oljedirektoratet, Giftinformasjonen, Statens forureiningstilsyn, Statens institutt for folkehelse, Statens arbeidsmiljøinstitutt og Direktoratet for brann- og eksplosjonsvern.

Sikkerhetsutvalget for Produktregisteret er direkte underlagt Miljøverndepartementet og ble opprettet i 1984. Utvalget fører tilsyn med at Produktregisterets til enhver tid gjeldende sikkerhetsreglement følges. Grunnlaget for sikkerhetsreglementet som gjelder i produktregisteret er "Rutiner for sikkerhet for Produktregisteret og virksomheter som bruker beskyttelsesgradert informasjon fra Produktregisteret" [21] som er bestemt av departementet.

Sikkerhetsreglementet er fundert i Beskyttelsesinstruksen [19], men kravene i sikkerhetsreglementet er høyere enn det som går frem av §12 i denne instruksen. Dette medfører at Produktregisterets graderte datanett har en sikkerhetsgradering som gjør at NSM (Nasjonal sikkerhetsmyndighet) er tilsyns-/godkjenningsmyndighet for at nettverket er i henhold til de sikkerhetskrav som NSM bestemmer. Disse kravene er gitt av Sikkerhetsloven [16] med tilhørende forskrifter, blant annet Forskrift om informasjonssikkerhet [20]. For hver gang det gjøres vesentlige endringer på systemet dokumenteres disse utførlig etter mal gitt av NSM, og oversendes NSM for godkjenning.

Grunnen til de strenge sikkerhetsreglene er at de opplysningene produsentene og importørene av kjemikaliene skal melde inn til Produktregisteret er svært sensitive forretningshemmeligheter. De typisk mest sensitive opplysningene er sammensetningsopplysningene, det vil si det eksakte innholdet av kjemiske stoffer i et produkt. For et firma i Norge eller utlandet som har brukt store beløp på å forske ut et unikt virkestoff, vil det være svært ødeleggende om konkurrentene fikk tak i disse opplysningene. Det er gjort en verdivurdering og teoretisk beregnet den økonomiske verdien av summen av alle disse hemmeligstemplede opplysningene i Produktregisteret. Departementet har blant annet tatt hensyn til denne verdivurderingen ved fastsettelsen av sikkerhetsreglene.

4.1.2 Behovene og kravene

I Produktregisteret registreres forskjellige roller som ulike firmaer har til produktene. Den viktigste rollen er deklarasjonsansvarlig. Det firmaet som er deklarasjonsansvarlig for et produkt, er det som er ansvarlig for at opplysningene om produktet er korrekte. Det er den som produserer eller importerer produktet, det vil si den som tar initiativet til at det kommer på det norske markedet, som er deklarasjonsansvarlig. I henhold til EØS-avtalen har firmaer i hele EØS-området anledning til å importere produkter til Norge.

Produktregisteret har laget en egen løsning for innmelding av produkter over Internett. Denne løsningen består i dag av et Windows-program, eDeklarasjon, som de deklarasjonsansvarlige firmaene kan laste ned fra en hjemmeside hos Produktregisteret. eDeklarasjon inneholder en liten database. De deklarasjonsansvarlige firmaene kan så legge inn alle opplysningene om alle produktene sine i databasen ved hjelp av eDeklarasjon, og når opplyningene er ferdig oppdatert, lager eDeklarasjon en fil som sendes over til en web-service på en server hos Produktregisteret. Deretter blir filen hentet videre inn til det graderte systemet hos Produktregisteret.

Det viktigste kravet for Produktregisteret er at opplysningene ikke kommer på avveie. Derfor er den filen som lages av eDeklarasjon kryptert, slik at den kun kan leses med Produktregisterets private nøkkel.

Konsekvensen dersom krypteringen ikke skulle virke, er at opplysningene kan leses av eventuelle hackere som avlytter kommunikasjonen inn mot Produktregisteret eller bryter seg inn i den serveren som mottar filene som sendes inn. Dette ville være et kritisk problem som i ytterste konsekvens kan få følger for eksistensen til Produktregisteret.

For Produktregisteret er det også viktig at vi kan være sikre på at opplyningen kommer fra det firmaet som faktisk er deklarasjonsansvarlig for det produktet den hevder å eie. Derfor må også filen signeres før den sendes over til Produktregisteret.

Konsekvensen ved en uoppdaget feil i signaturen, er for eksempel at en konkurrent A kunne sendt inn en melding om adresseendring på et firma B. Konkurrenten A kunne deretter utgi seg for å være firma B og be om å få se på de opplyningene som firma B tidligere har meldt inn. Det vil si at konkurrenten til firmaet får tilsendt forretningshemmelighetene til en falsk adresse. I praksis vil dette være vanskelig fordi opplysningene som legges inn i systemet vil bli manuelt kontrollert før det legges inn, og begjæringer om å få opplyst gradert informasjon de tidligere har sendt inn er så

sjelden forekommende, at saksbehandler i Produktregisteret har tid og anledning til å kontrollere forespørselen nøye. Svarbrev til firmaer blir i størst mulig grad formulert slik at man unngår å nevne selve de sensitive opplysningene siden disse er kjent hos begge parter fra før.

En annen konsekvens ved en uoppdaget feil i signaturen, kan være at konkurrenten A kan utgi seg for å være firma B og melder at alle opplyninger hos firmaet B ikke lenger er sensitive. Deretter kan konkurrent A som "mannen i gata" be om innsyn i følsomme opplysninger innmeldt av firma B. Dette er også så sjelden tilfelle at saksbehandler vil fange opp forsøket på "innbrudd".

En tredje konsekvens ved en uoppdaget feil i signaturen, er at de deklarasjonsansvarlige firmaene skulle kunne hevde at de likevel ikke sendte inn en opplysning (ikke-benekt). Dette kunne vært brukt hvis det deklarasjonsansvarlige firmaet fikk en erstatningssak mot seg fordi noen skadelidte hevder de har blitt utsatt for farlige kjemikalier fordi firmaet ikke har opplyst om hvilke farlige ingredienser det har, eller ikke opplyst hvor farlig disse ingrediensene er.

Oppsummert kan man altså si at det viktigste for Produktregisteret er at opplysninger ikke kommer på avveie, og derfor stiller vesentlig strengere krav til krypteringen enn til signeringen.

4.1.3 Brukes PKI?

Produktregisteret bruker i dag ikke PKI i betydningen at de i sin elektroniske kommunikasjon baserer seg på sertifikater som er utstedt av godkjente sertifikatutstedere.

Når Produktregisteret tok i bruk eDeklarasjon, var det integrert med løsningen E-kurer som ble levert av Posten Norge. Enkelt sagt var E-kurer en webbasert e-post-løsning hvor man kunne signere e-post-meldingene. Signeringen var basert på X.509-sertifikater som var utstedt av Posten. Slik sett kan man si at løsningen var basert på PKI-teknologi, men selve epost-løsningen var lukket ved at man måtte ha en avtale med Posten for å kunne bruke signeringen. E-kurer ble nedlagt av Posten etter kort tid på grunn av manglende marked for å gjøre løsningen lønnsom.

Fram til nå har Produktregisteret basert seg på en egenutviklet lukket løsning. Produktregisteret har et gyldig elektronisk virksomhetssertifikat utstedt til seg av en av de norske godkjente utstedere av elektroniske sertifikater. Videre utsteder Produktregisteret sertifikater til de deklarasjonsansvarlige firmaene. eDeklarasjon krypterer så filen som inneholder opplysningene slik at de bare kan leses med nøkkel

Produktregisteret har, samt at den signeres med sertifikat utstedt av Produktregisteret. Dagens løsning er gratis for firmaene siden Produktregisteret ikke tar seg betalt for sertifikatene eller tjenesten forøvrig. Dette er firmaene godt fornøyde med.

Internasjonalt fungerer også dagens løsning. Siden løsningen er utviklet av og for Produktregisteret, er det Produktregisteret som må utføre oppgavene som en sertifikatutsteder ville hatt i en PKI-løsning. Dette innbefatter blant annet å sikre at sertifikatet utstedes til riktig deklarasjonsansvarlig firma.

På det tidspunktet Produktregisteret tok i bruk E-kurer, var ennå ikke Kravspesifikasjonen for PKI i offentlig sektor klar. Selv om E-kurer hadde en lukket arkitektur som var ulik den som er skissert i esignaturloven, mente jurister hos leverandøren av E-kurer at støtten for autentisering og ikke-benekt i E-kurer var tilstrekkelig for Produktregisterets behov. Når Produktregisteret i tillegg fikk en akseptabel kryptering og integrasjon mot Produktregisterets mottaksløsning, ble E-kurer valgt.

Når E-kurer ble lagt ned, vurderte Produktregisteret om den nye løsningen skulle forutsette sertifikater fra godkjente sertifikattilbydere eller om Produktregisteret selv skulle produsere sertifikatene. Fordelen med egenproduserte sertifikater var at deklarantene ville slippe å kjøpe et sertifikat (spare penger), mens ulempen er at det er liten grad av ikke-benekt hvis deklarantene skulle klare å påvise svakheter i Produktregisterets interne rutiner som sertifikattilbyder. Et annet moment var at dette skulle være en midlertidig løsning fram til Produktregisteret skulle ta i bruk Altinn. Valget ble egenproduserte sertifikater. Derfor har Produktregisteret heller ikke gjort vesentlig bruk av Kravspesifikasjonen for PKI i offentlig sektor.

Produktregisteret ble med i Altinn-samarbeidet i 2005. Produktregisteret har derfor på noe sikt en intensjon om å basere seg på Altinn til mottak fra eDeklarasjon. Etter at Sikkerhetsportalen sommeren 2006 ble lagt ned, har Produktregisteret inntil videre lagt det videre arbeidet med tilpasning til Altinn på is fordi det var Sikkerhetsportalen fra Altinn som Produktregisteret først og fremst ville gjøre nytte av.

4.2 Brønnøysundregistrene og Altinn

4.2.1 Om Brønnøysundregistrene

Brønnøysundregistrene er en forvaltningsetat med ansvar for kontroll- og registreringsordninger for næringslivet i Norge. Etatens overordnede mål [21] er å

bidra til økt økonomisk trygghet og effektivitet både for næringslivet og i samfunnet generelt.

Brønnøysundregistrene består av følgende registre: Løsøreregisteret, Ektepaktregisteret, Akvakulturregisteret, Registeret for utøvere av alternativ behandling, Gjeldsordningsregisteret, Konkursregisteret, Jegerregisteret, Regnskapsregisteret, Foretaksregisteret, Enhetsregisteret, Oppgaveregisteret, EMAS, Reservasjonsregisteret og Partiregisteret. I tillegg kommer Gebyrsentralen som registrerer bilag og krever inn gebyrer på vegne av namsmennene i forbindelse med tvangssalg og utleggsforretninger til staten.

De meldepliktige opplysningene til disse registrene meldes inn til Brønnøysundregistrene av de/den som er meldepliktig.

For Brønnøysundregistrene er det viktig at informasjonen som finnes i registrene skal gjøres tilgjengelige på en brukervennlig måte til en rimelig kostnad. Derfor er mesteparten av informasjonen som ligger lagret i Brønnøysundregistrenes databaser tilgjengelig for publikum.

Brønnøysundregistrene henter sine inntekter fra gebyrer på oppslag mot databasene. Hvert år sendes det ut 250 000 fakturaer etter oppslag i databasene.

4.2.2 Om Altinn

Altinn er en tjeneste på Internett som driftes og forvaltes av en sentral forvaltningsorganisasjon som er felles for alle deltagende etater i samarbeidet. Altinn sentralforvaltning er opprettet som en avdeling ved Brønnøysundregistrene.

De etatene som er med i Altinn-samarbeidet i dag er:

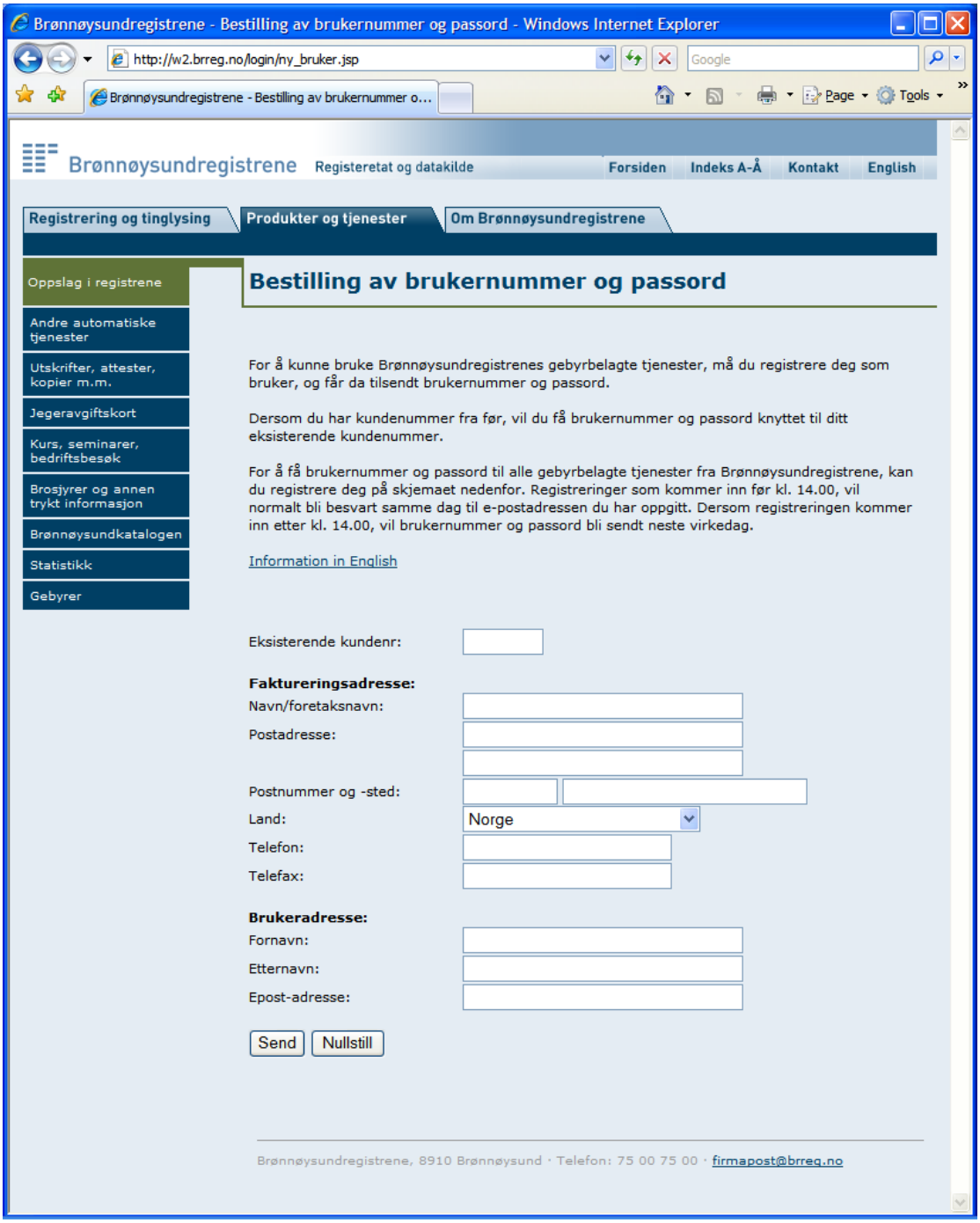
- Skatteetaten
- Statistisk sentralbyrå
- Brønnøysundregistrene
- Lånekassen
- Konkurransetilsynet
- Kredittilsynet
- Fiskeri- og kystdepartementet
- Norges bank
- Økokrim
- Produktregistret
- Statens innkrevingssentral

- Statens landbruksforvaltning
- Husbanken
- Statens forurensningstilsyn
- Patentstyret
- Lotteri- og stiftelsestilsynet
- Luftfartstilsynet
- Mattilsynet

Altinn ble opprettet for å være en felles portal for innrapportering av meldepliktige opplysninger til staten. Altinn er fortsatt inne i en ekpanderende utvikling hvor flere og flere etater melder seg på samarbeidet, og hvor disse etatene tilbyr og tilrettelegger for innrapportering av stadig større deler av opplysningene gjennom Altinn. For de etatene som knytter seg til Altinn tilbys en ferdig utviklet infrastruktur for elektronisk innrapportering som relativt raskt kan tilpasses nye etater.

4.2.3 Behovene og kravene

Brønnøysundregistrene har behov for autentisering i elektroniske tjenester for å sikre betaling ved salg av informasjon (oppslag i registrene). Det viktige å få avklart er derfor den som skal betale for oppslaget. I figur 4 vises registreringsbildet som er det første brukerne av de gebyrbelagte oppslagstjenestene møter når de skal bruke tjenestene. Figuren viser hvor viktig denne autentiseringen er for Brønnøysundregistrene.



Figur 4. Registrering som bruker av oppslagstjenester ved Brønnøysundregistrene.

Brønnøysundregistrene har også behov for ikke-benekt. Når oppgavepliktige firmaer og personer melder inn sine opplysninger har Brønnøysundregistrene i en del sammenhenger behov for å kunne bevise at en avgiver (eller mottaker) ikke skal kunne benekte at han har avgitt (eller mottatt) opplysningene.

I noen sammenhenger har Brønnøysundregistrene behov for autentisering for å vite om en person har rett til å gjøre den avgivingen av opplysninger som personen ønsker å gjøre. Dette kan for eksempel være å oppdatere hvem som sitter i en bedrifts styre. Konsekvensen av om noen legger inn feil opplysninger her kan være store for bedriften.

Altinn omfatter mange offentlige virksomheter og har derfor et variert behov for autentisering og PKI. Den av de statlige etatene som mottar den største mengden opplysninger via Altinn, er Skatteetaten. Skatteetaten har bruk for autentisering, men har ikke høye krav til sikkerhet. Dersom en kjeltring skulle sende inn skattetall for et firma, vil det verste som skjer være at firmaet får en del ekstraarbeid, og muligens utgifter til advokater, revisorer eller regnskapsfolk. Kjeltringen vil ikke tjene på det.

Lånekassen er en etat som er tilknyttet Altinn for å tilby sine kunder lån. De har derfor et behov for å være svært sikker i autentiseringen av studentene som ønsker å ta opp lån, siden konsekvensen ville være at lånet utbetales til feil person.

Altinn har hittil ikke tilpasset seg internasjonale forhold. Imidlertid er det flere av etatene som vil kunne motta opplysninger fra utenlandske firmaer og personer, så tilpasninger for slik bruk er nødvendig for Altinn.

4.2.4 Brukes PKI?

Brønnøysundregisteret bruker lite PKI i betydningen at de i sin elektroniske kommunikasjon baserer seg på sertifikater som er utstedt av godkjente sertifikatutstedere. PKI brukes i dag i Brønnøysundregistrene kun i prototypen om kontroll av heftelser. Her er det banken som vil ha sikkerhet for at Brønnøysundregistrene har signert. Denne tjenesten brukes av bankene for å sjekke heftelser ved for eksempel bilkjøp. Til dette brukes sertifikater fra Bank ID.

Skatteetaten bruker gjennom Altinn ikke PKI i betydningen at de i sin elektroniske kommunikasjon baserer seg på sertifikater som er utstedt av godkjente sertifikatutstedere. 90% av all momsrapportering kommer nå inn via Altinn.

Studentene kan gjennom Lånekassen sin løsning på Altinn elektronisk signere lånebevisene sine hvis de har godkjente sertifikater som er utstedt av Byupass.

Hittil i 2006 (per medio desember) er det foretatt drøyt 6 000 000 pålogginger på Altinn. Nesten halvparten av disse påloggingene var ved hjelp av pinkoden som finnes på selvangivelsen. Når man logger seg på via disse pin-kodene, har man mulighet til å legge inn sitt mobiltelefonnummer, slik at man kan få tilsendt engangs-PIN for pålogging til Altinn via SMS. Drøyt to millioner logget på ved hjelp av SMS. Drøyt 60 000 har logget på ved hjelp av smartkort (sertifikatet utstedt av Buypass). Smartkortet er påkrevet ved signering i Lånekassen, men kan også brukes til pålogging på andre tjenester i Altinn.

4.2.5 I hvilken grad er det sett på lover og andre førende dokumenter

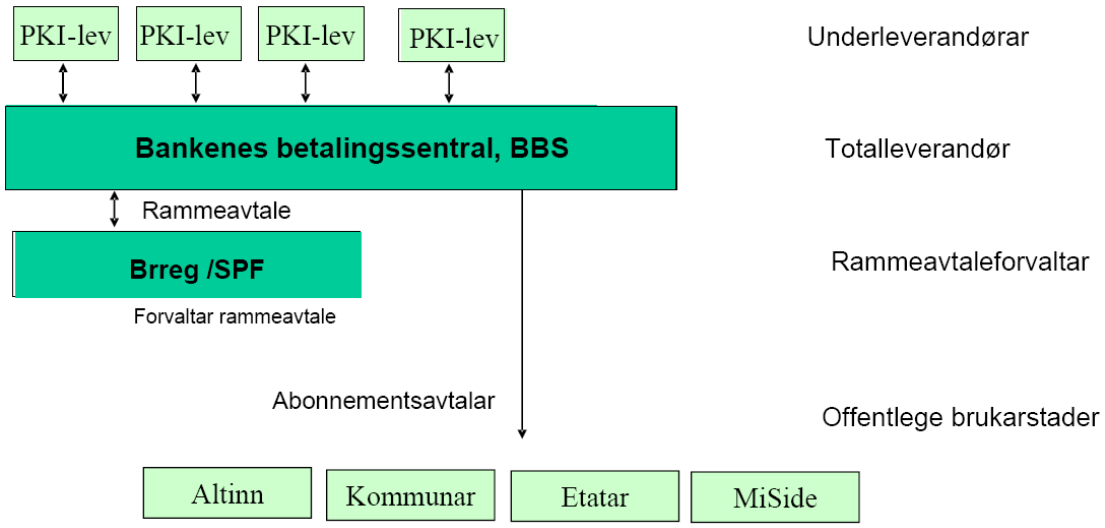
Det er vanskelig med sikkerhet å påvise på hvilken måte lover regler og sentrale føringer har hatt betydning for Brønnøysundregistrenes beslutninger når det gjelder elektronisk ID og PKI. I denne sammenhengen er det viktig å legge merke til at i Brønnøysundregistrene brukes PKI kun i en prototype. Denne prototypen har imidlertid vært operativ lenger enn de førende dokumentene som har vært gjennomgått i denne oppgaven. I Altinn brukes PKI av Lånekassen, men det er ikke undersøkt hvilke undersøkelser Lånekassen gjorde forut for etableringen av denne løsningen.

4.2.6 Sikkerhetsportalen

Sikkerhetsportalen var en storsatsing for å finne en felles løsning på sikkerhetsutfordringene i Altinn og MinSide. Til grunn for Sikkerhetsportalen lå en rammeavtale mellom Brønnøysundregistrene (på vegne av staten og Kommunenes Sentralforbund) og Bankenes Betalingssentral (BBS). Det var BBS som hadde utviklet og levert portalen og Brønnøysundregistrene som hadde ansvar for å forvalte den.

Sikkerhetsportalen skulle sørge for sikker dialog mellom brukeren og det offentlige på Internett, slik at ingen andre fikk tilgang til brukerens opplysninger. Portalen åpnet dessuten for felles innlogging til flere offentlige tjenester, noe som for alvor skulle komme innbyggerne til gode når flere etater og kommuner skulle ta løsningen i bruk.

Teknisk sett var hensikten å ha en felles overbygning til de offentlige tjenestene som benyttet portalen, slik at man trengte å autentisere seg i kun en felles innlogging. For å bruke portalen måtte brukerne ha en elektronisk ID. Ved Single-sign-on skulle systemet holde rede på identiteten uavhengig av hvordan brukeren navigerte seg gjennom de offentlige tjenestene som ble tilbudt gjennom portalen.



Figur 5. Roller til aktørene i Sikkerhetsportal-prosjektet. Figuren er hentet fra presentasjon av FAD i forbindelse med nedleggelsen av Sikkerhetsportalen 30. juni 2006 [24].

For det offentlige var det en intensjon at alle typer sertifikater som tilfredsstilte esignaturloven og kravspesifikasjonen for PKI i offentlig sektor, skulle fungere i Sikkerhetsportalen. I praksis var dette vanskelig. Spesielt er det grunn til å tro at forskjellen i garantibeløp (100 000 kr for Bank ID mot 5 000 kr for Buypass) var vanskelig å bli enige om. Etter hvert viste det seg at enkelte etater og andre potensielle brukere av portalen fortsatte å benytte tjenestene til sertifikattilbyderne direkte, og Sikkerhetsportalen ble til slutt besluttet avviklet 30. juni 2006, et halvt år etter at den ble lansert.

4.3 Kort om andre etater

De fleste statlige virksomheter som mottar innrapporteringer er i dag tilknyttet Altinn. I følge tall fra Brønnøysundregistrene står innrapportering av data til Skatteetaten for i underkant av 2/3 av all innrapportering til staten. Nest størst er NAV som står for i 1/5. NAV er imidlertid ikke en del av Altinn-samarbeidet. Tollvesenet, som mottar i underkant av 1/10 av innrapporteringene, er heller ikke med i Altinn-samarbeidet. Statistisk Sentralbyrå mottar også en del innrapportering, og de er med i Altinn-

samarbeidet. . Volumet av innrapporteringer til de andre statlige etatene er i denne sammenheng forholdsmessig mindre.

I hvilken grad det er nødvendig med PKI til disse innrapporteringene varierer, men alle etatene har et behov for autentisering. Å bruke PKI basert på sertifikater som er utstedt av godkjente sertifikatutstedere, innebærer ofte en investeringskostnad som for en del tilfeller ikke svarer seg.

PKI brukes også til andre formål enn innrapportering av meldepliktige opplysninger til staten.

I helsesektoren er det i dag stor bruk av PKI. Den eksisterende infrastrukturen for PKI i helsesektoren er tilpasset bransjen og har et stort antall brukere. Det betyr at det får konsekvenser for mange brukere når helsesektoren må tilpasse seg generelle krav som gjelder for alle øvrige bransjer, slik som Kravspesifikasjonen for PKI i offentlig sektor. Dette betyr at i den grad helsesektoren jobber mot felles krav til PKI-løsninger på tvers av bransjer, er det for å få gjennomslag for sine tilpasninger og teknologivalg. I helsesektoren brukes stort sett Buypass sine sertifikater.

En viktig hensikt for offentlig virksomhet for å ta i bruk løsninger basert på elektronisk ID, er at dette indirekte vil spare etatene for store beløp. Det er mange offentlige virksomheter som vil spare store beløp på blant annet å innføre automatisering av deler av sine oppgaver. Elektronisk saksbehandling av korrespondansen og elektronisk fakturabehandling er eksempler på oppgaver som har et stort potensial for rasjonaliseringsgevinster ved automatiseringer og forenklinger. Autentisering og elektronisk ID er viktige forutsetninger for å få fullgode løsninger for disse behovene på plass. Hittil har mangel på gode løsninger for elektronisk ID og PKI vært en av faktorene som har komplisert implementeringen av elektronisk behandling av etatenes oppgaver.

5 Vurdering og resultat

5.1 Tillit og elektronisk ID

5.1.1 Tillit mellom sertifikatutstedere

I dag er det i praksis to godkjente utstedere av elektroniske sertifikater i Norge. Disse tilbyr en type sertifikat hver. De har ikke noe avtale med hverandre. Grunnen til dette er først og fremst forskjellen i garantibeløpet de stiller for sertifikatene de har utstedt. Tillit handler om hvem som må betale hvis noe går galt, og en forutsetning for en avtale mellom disse som skal gjelde begge veier, må derfor være at garantibeløpet blir det samme.

Internasjonalt er federering en utfordring. Det vil si at når det gjelder tilliten mellom sertifikatutstedere i forskjellig land, er mangel på en god identifikator (for eksempel fødselsnummer) på tvers av landegrensene en utfordring. Det er nødvendig å vite når en person er den samme i to systemer som skal ha tillit til hverandre. For å oppnå tillit må det derfor bli en bedre samordning mellom landenes personregistre og bedriftsregistre.

5.1.2 Tillit til elektroniske sertifikater og elektronisk ID

Brukerne av PKI-løsninger kan være personer, firmaer og etater, For at disse skal ha tillit til PKI-løsningene, må blant annet følgende ønsker/krav være oppfylt:

- Løsningen må være sikker nok i forhold til behovet.
- Løsningen må være brukervennlig slik at de som signerer vet når de har signert, hvor det blir av den signerte informasjonen og så videre.
- Dersom det signerte dokumentet skal oppbevares over tid, må systemet kunne verifisere signaturen når det skulle bli nødvendig.

Dersom samme elektroniske sertifikat brukes til mange ulike formål, er den personen som har dette sertifikatet sårbar hvis det blir ødelagt eller kommer i feil hender. For at denne personen skal ha tillit til systemet, må personen være tilstrekkelig sikker på at det er vanskelig å stjele sertifikatet, og forholdsvis enkelt å få et nytt.

5.2 De tekniske aspektene

5.2.1 De tekniske utfordringene ved PKI

PKI er fortsatt en relativt ny teknologi i forhold til levetiden man ønsker på dokumenter som er signert med PKI-teknologi. Det er alltid en usikkerhet om at signaturen holder vann i hele dens tiltenkte levetid.

Tegnsett er en utfordring. I hvert fall så lenge man i sertifikatene har felter hvor det kan forekomme tegn som er spesielle for hvert land, vil dette være en konstant utfordring.

Etter hvert som dagens versjoner av systemer og programvare som brukes i en PKI-løsning oppgraderes eller byttes ut, kan man risikere at systemet fungerer litt anderledes. Dette kan få konsekvenser for PKI-løsningen.

En fare ved etableringen av PKI i offentlig sektor er at en kunne komme til å binde seg fast til en standard som passer for dagens behov, men som relativt sett representerer et lite tidsvindu, slik at den valgte løsningen etter hvert kan bli en stor ulempe.

Andre teknologier enn PKI kan være interessant på sikt. Til identifisering er biometriske teknologier det mest interessante alternativet. Biometriske teknologier er imidlertid fortsatt ikke mye utbredt, og teknologien er fortsatt for usikker til å være et godt alternativ. Det er ingen alternative teknologier som ligger an til å ta merkbare markedsandeler av markedet for elektronisk ID fra PKI. Den største trusselen for utbredelsen av PKI er derfor om potensielle brukere av teknologien velger enklere løsninger, slik som pin-kode-baserte, istedenfor en full PKI-løsning.

5.2.2 Få gjennomslag for teknologien

En måte å få størst mulig gjennomslag for bruken av PKI på, er å først starte hos de etatene som har størst nytte av det og de som har forutsetninger for å forstå de grunnleggende prinsippene i teknologien, og deretter de andre etatene etter at "kritisk masse" [28] er oppnådd. Med kritisk masse menes at det er så mange brukere av en teknologi at den vil overleve av seg selv uten at den lenger må støttes aktivt av noen av aktørene I teorien om kritisk masse er det også slik at ved en infrastruktur av denne typen så øker verdien for en potensiell bruker i takt med antallet andre brukere som benytter den samme infrastrukturen.

Innen helsesektoren i Norge kan man si at man har oppnådd kritisk masse. For andre sektorer er det fortsatt nødvendig med en bevisst satsing for å få bedre gjennomslag for teknologien. Offentlige etater er selv blant de som vil tjene mye på å ta i bruk PKI.

5.3 Dele inn etatene etter hensikten med autentisering

I en analyse av bruken av elektronisk ID og signatur, er det vesentlig å se på hensikten etatene har med å ta i bruk denne teknologien. Tre kategorier behov for autentisering er betaling, beskyttelse av informasjon og sikring av ikke-benekt. Det er nødvendig at både etatene og etatenes forbindelser er klar over hvilken av disse kategoriene etatenes oppgaver hører inn under.

De fleste etatene har behov for ikke-benekt. Imidlertid er det ikke vanlig at de oppgavene etatene ønsker å bruke autentisering på både brukes til å sikre inntekter og samtidig har sterk fokus på beskyttelse av informasjon.

5.3.1 Betaling

Dette er en type etater som ønsker å være sikker på hvem som er betaleren for en tjeneste. Etaten har et direkte økonomisk behov for å autentisere brukeren og behovet kan lett kvantifiseres i penger fordi det er snakk om et konkret tap for hver gang autentiseringen mislykkes. Et annet kjennetegn ved etater som tilhører denne kategorien, er at det er etaten selv som blir den direkte skadelidende dersom tjenesten ikke fungerer.

Disse forholdene gjør at disse etatene lett kan gjøre en kost-nyttevurdering i forhold til sitt behov for PKI. De vil ikke bruke mer ressurser på anskaffelse og bruk av PKI-tjenester enn at de får tilstrekkelig inntjening per brukte krone på PKI-tjenestene.

Etatene med kun dette behovet vil i liten utstrekning være pådrivere for innføring av PKI i offentlig sektor. Men når PKI blir mer utbredt vil disse etatene også ta i bruk PKI i større og større utstrekning.

Etater med oppgaver i denne kategorien er blant andre Skatteetaten og Brønnøysundregistrene.

5.3.2 Beskyttelse av informasjon

Dette er en type etater som håndterer sensitiv informasjon. Denne sensitive informasjonen kan være vanskelig å kvantifisere i pengebeløp, og vil ofte variere

mye. Informasjonen det her er snakk om kan være forretningshemmeligheter, statshemmeligheter og personopplysninger. For eksempel betyr det mye for noen av dataavgiverne til Produktregisteret at en hemmelig ingrediens i et kjemisk produkt holdes hemmelig, mens det for andre dataavgivere ikke er viktig å hemmligholde ingrediensene i et kjemikalie. Tilsvarende er noen personer mer opptatt av å verne om opplysninger om sin helse enn andre.

Et kjennetegn for etater med oppgaver i denne kategorien er at etatene ikke direkte vil være den skadelidende hvis kvaliteten i tjenesten er dårlig. Etatene må imidlertid ta høyde for at de indirekte kan få et økonomisk tap som følge av feil i tjenesten. Etater som har slike oppgaver er ofte avhengig av tillit, og hvis problemer med en slik tjeneste skulle føre til tillitsbrudd, kan det ha svært alvorlige konsekvenser for de aktuelle etatene.

Etatene med dette behovet vil derfor kunne være pådrivere for innføring av PKI i offentlig sektor. De vil også være pådrivere for at PKI-tjenestene er så sikre som mulig (kan hende på bekostning av pris og brukervennlighet).

Etater med oppgaver i denne kategorien er blant andre Produktregisteret og i helsesektoren.

5.3.3 Sikring av ikke-benekt

Dette er en type etater som håndterer informasjon hvor avgiver eller mottaker av informasjonen ikke skal kunne benekte at han har sendt eller mottatt den aktuelle informasjonen. De fleste offentlige etater har behov for dette, fordi de fleste offentlige etater mottar data som må være signert. En av hensiktene med ikke-benekt, er at etaten kan være trygg på at det er en god kvalitet på informasjon som er signert, blant annet fordi det er lett å peke på den som er ansvarlig for kvaliteten på informasjonen.

Etatene med dette behovet vil til en viss grad være pådrivere for innføring av PKI i offentlig sektor. De vil også være pådrivere for at PKI-tjenestene er så sikre som mulig (kan hende på bekostning av pris og brukervennlighet).

5.4 Vurdering av PKI som løsning på etatenes behov

5.4.1 Når kan og bør PKI brukes

I hvilken grad det er nødvendig med PKI til etatenes behov varierer, men svært mange etater har et stort behov for en eller annen form for autentisering. Å bruke PKI basert

på sertifikater som er utstedt av godkjente sertifikatutstedere innebærer ofte en investeringskostnad som for en del enkeltoppgaver ikke svarer seg. Dersom etatene hadde sett summen behovene for elektronisk ID for alle sine oppgaver, ville likevel de fleste tjent inn denne investeringskostnaden i løpet av kort tid.

Men på samme måte som forskjellige etater har ulik behov for autentisering (hensikten er forskjellig), vil det også være variasjon i behovene hvis en ser på de enkelte oppgavene innefor hver etat hvor elektronisk ID vil være nyttig.

Det vil ofte være det oppgaveområdet hvor det først vil svare seg å benytte elektronisk ID, kombinert med at det skal gjennomføres en endring i den delen av organisasjonen, som vil være initierende og bestemmende for når og hvordan elektronisk ID innføres i en etat.

5.4.2 De førende dokumentene sett fra etatene

Relevansen til lovene, reglene og de førende dokumentene henger sammen med i hvilken grad etaten tar i bruk PKI fullt ut. Verken Produktregisteret eller Brønnøysundregisteret bruker i dag i særlig grad PKI i betydningen at de i sin elektroniske kommunikasjon baserer seg på sertifikater som er utstedt av godkjente sertifikatutstedere. Derfor har ikke disse reglene hatt vesentlig betydning.

I helsesektoren brukes PKI, og de baserer seg på de førende dokumentene.

5.5 Videre arbeid

5.5.1 Drøfte nærmere om portaler er riktig strategi

I Norge har det vært en satsing på portalløsninger (blant annet Altinn og MinSide). Det kunne være interessant å se på om det er riktig strategi for å få størst mulig gjennomslag for PKI-løsninger å koble innføringen av denne teknologien så tett med innføringen av disse protalløsningene.

Dersom det offentlige hadde utstedt elektroniske borgerkort, og tatt rollen som sertifikatutsteder, kunne det ha fått konsekvenser for de offentlige portalløsningene. Det kunne vært interessant å se nærmere på denne problemstillingen.

5.5.2 Se på andre synsvinkler enn fra etatene

Dersom en skal se på problemstillingen fra andre synsvinkler, for eksempel innbyggerne i Norge, ville sannsynligvis en del andre momenter hatt større betydning. Dette gjelder først og fremst sikkerhets, og personvernvurderinger rundt det å ha en eller flere elektroniske ID-kort, i hvilken grad det er nødvendig for brukerne å forstå teknologien, forenkling av offentlig sektor og det å gjøre de elektroniske tjenestene mer brukervennlig og tilgjengelig.

Det kunne også vært interessant å studere på dette i et mer internasjonalt perspektiv. Her kunne man sett på hva som skal til for å få på plass løsninger som er uavhengig av land. Man kunne sett på hvilke roller det offentlige bør spille (og ikke spille) for å få en best mulig integrasjon på tvers av landegrensene.

6 Konklusjon

PKI kan og bør brukes av offentlige etater. Jo større utbredelse teknologien får, jo større verdi har teknologien for alle brukerne av teknologien.

Teknologien og prinsippene for PKI er velkjente og gode. De teknologiske utfordringene ligger i å sikre kompatibilitet mellom forskjellige konfigurasjoner av tegnsett, og datamaskinkonfigurasjoner.

Det er viktig at de etatene som har et behov for autentisering som gjør at de er mest tjent med å ta i bruk PKI-teknologi er de som “drar lasset” for å oppnå “kritisk masse”. Myndighetene som definerer rammebetingelsene og legger til rette for innføring av PKI bør også ta hensyn til de etatene som har mest å tjene på innføringen.

Når det gjelder hypotesen “PKI kan brukes til alt”, er svaret at ja det kan det i en ideell verden. Det er imidlertid tvilsomt at det er hensiktsmessig i overskuelig framtid. De etater som i en elektronisk kommunikasjon i dag og på noenlunde kort sikt har behov for autentisering, integritetsbeskyttelse, konfidensialitetsbeskyttelse og/eller sikring av ikke-benekting, er PKI et godt valg.

Referanser

[1] NOU 2001:10 Uten penn og blekk, kapittel 12.1.3.
[2] http://www.brreg.no/samordning/organisasjonsnummeret.html
[3] LOV 2001-06-15 nr 81: Lov om elektronisk signatur (esignaturloven). http://www.lovdata.no/all/hl-20010615-081.html
[4] http://www.skatteetaten.no/Templates/Emne.aspx?id=9862&epslanguage=NO
[5] Direktiv 1999/93/EC om en fellesskapsramme for elektronisk signatur
[6] Norsk BankID sertifikatpolicy for banklagrede kvalifiserte sertifikater til personkunder, v 1.1 desember, 2005
[7] Forskrift om krav til utsteder av kvalifiserte sertifikater mv., http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20010615-0611.html
[8] Engen, Bård Ketil, Tillit og kommunikasjon i digitale læringsomgivelser, En undersøkelse av IKT-mediert medisinerutdanning ved Universitetet i Oslo, , avhandling for Dr. Polit-graden, InterMedia, Universitetet i Oslo 2004
[9] Stallings, William, Network Security Essentials, Applications and Standards, , 2. edition, Prentice Hall, 2003
[10] SEID-Prosjektet, Leveranse oppgave 1, Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater, versjon 1.01, 07.09.2004, http://www.dep.no/filarkiv/228037/SEID_-_Leveranse_1_-_v1.01.pdf
[11] Witte, Griff, Unlocking fingerprints, http://www.washingtonpost.com/wp-dyn/content/article/2006/08/27/AR2006082700511.html, The Washington Post artikkel, 28. august 2006, side D01
[12] Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures
[13] Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften), http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20040625-0988.html
[14] Forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere, http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20051121-1296.html
[15] St.prp. nr 1 (2006-2007), Del III Miljøverndepartementets budsjettforslag for 2007, Kapittel 1444 Produktregisteret, http://odin.dep.no/md/norsk/dok/regpubl/stprp/022001-030019/hov021-bn.html
[16] LOV 1998-03-20 nr 10: Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), http://lovdata.no/all/hl-19980320-010.html

[17] FOR 2002-07-16 nr 1139: Forskrift om klassifisering, merking mv. av farlige kjemikalier., http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20020716-1139.html

[18] Forskrift om deklarering og merking av mikrobiologiske produkter med et bruksområde som medfører tilføring til det ytre miljø, http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-19980122-0093.html

[19] Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen). http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-19720317-3352.html

[20] Forskrift om informasjonssikkerhet, http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20010701-0744.html

[21] "Rutiner for sikkerhet for Produktregisteret og virksomheter som bruker beskyttelsesgradert informasjon fra Produktregisteret". Vedlegg i brev med tittel "Rutiner for sikkerhet for Produktregisteret og dets brukervirksomheter" fra Miljøverndepartementet til Produktregisteret datert 14.04.2005 med dokumentnummer 200507039/1 i Produktregisterets journal.

[22] Norges offentlige utredninger NOU 2001:10 Uten penn og blekk, Bruk av digitale signaturer i elektronisk samhandling med og i forvaltningen, Utredning fra et utvalg oppnevnt ved kongelig resolusjon av 4. februar 2000, Avgitt til Arbeids- og administrasjonsdepartementet 2. mars 2001, http://odin.dep.no/fad/norsk/dok/andre_dok/nou/002001-020005/inn-bn.html

[23] FAD, Mi Side og Tryggingsportalen, Presentasjon på pressekonferanse 30. juni 2006, http://www.odin.no/filarkiv/285607/Pressekonf_MiSide_30.06.pdf

[24] Brömme, Arslan, A Classification of Biometric Applications wanted by Politics: Passport, Person Tracking, and Fight Against Terror, IFIP WCC 2002, Montreal, 25.-30. august 2002. http://www.aviomatik.de/publications/papers/ifip_wcc2002_broemme.pdf

[25] Kent, Jonathan, Malaysia car thieves steal finger, BBC News, http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

[26] SEID-Prosjektet, Leveranse oppgave 2, Grensesnitt for tilgang til Oppslagstjenester, versjon 1.02, 17.12.2004, http://odin.dep.no/filarkiv/265359/SEID_Leveranse_2_-_v1.02.pdf

[27] SEID-Prosjektet, Leveranse oppgave 3, SEID-SDO – Dataobjekt for langtidslagring og utveksling av elektroniske signaturer, versjon 1.0, 01.06.2005, http://odin.dep.no/filarkiv/265357/SEID_Leveranse_3_-_v1.0.pdf

[28] Hanseth & Monteiro, Understanding Information Infrastructures. Manuscript, 1997

[29] Post- og teletilsynet, Registrerte tilbydere av kvalifiserte signaturer, http://www.npt.no/portal/page?_pageid=121,47065&_dad=web&_schema=PORTAL&p_d_i=-121&p_d_c=&p_d_v=48615