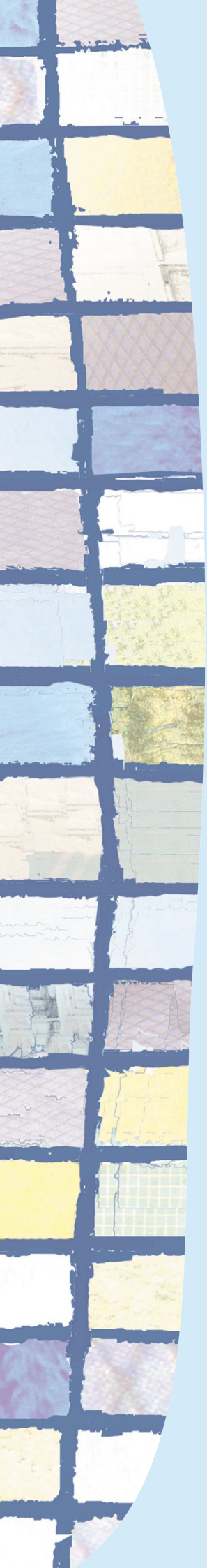

Oppdragsrapport nr. 8 - 2004

Dag Slettemeås

Grunnlagsdokument

- forbrukervinkling på Public Key Infrastructure (PKI)

SIFO

SIFO | Statens institutt for forbruksforskning
Postboks 4682, Nydalen,
0405 Oslo

Oppdragsrapport nr. 8 - 2004

Tittel	**Antall sider**	**Dato**
Grunnlagsdokument – forbrukervinkling på *Public Key Infrastructure* (PKI).	78	30.10.2004
Title Background Document – Consumer Perspective on Public Key Infrastructure (PKI).		
Forfatter(e)	**Prosjektnummer**	**Faglig ansvarlig sign.**
Dag Slettemeås	11-2004-8	
Oppdragsgiver Nærings- og handelsdepartementet		

Sammendrag

I denne rapporten anlegges et forbrukerperspektiv på utviklingen av PKI i Norge. Det vil si at vi bygger opp argumentasjonen rundt forbrukernes posisjon, deres holdninger og atferd, og benytter dette som bakgrunn for å utvikle konkrete forbrukerrettede spørsmål. Disse spørsmålene, som ligger i vedlegget til denne rapporten, vil kunne benyttes videre i kvantitative surveyer eller som grunnlag for fokusgrupper i en PKI-undersøkelse.

I første omgang argumenteres det for viktigheten av å inkludere forbrukere både i innovasjons- og informasjonsprosessen ved større satsinger som denne. En PKI-infrastruktur vil være kompleks både rent teknologisk og med hensyn til rollestrukturer. Det er dermed viktig at forbrukere, som til slutt skal benytte og bygge tillit til denne infrastrukturen, blir inkludert gjennom en forbrukervinklet analyse. Dette betyr ikke at alt forbrukerne sier skal følges – det er *perspektivet* som anlegges som er avgjørende.

Videre ser vi på mulige problemer som kan oppstå ved en eventuell tjeneste- og rolleblanding. Ettersom PKI Forum har som formål å samordne PKI-satsingen – en satsing som inkluderer både offentlige og private aktører – tar vi opp problemstillinger rundt reell eller oppfattet sammenblanding av forbruker- og borgerrollen. Dette er spesielt relevant i forbindelse med tidligere offentlige tjenester som nå er konkurranseutsatt.

Andre forhold som diskuteres i et forbrukerperspektiv er sikkerhet, personvern og tillit. Over tid har ”cyberspace” utviklet seg fra å være preget av anarki i en tidlig fase til å bli likere vår ”analoge” verden, ved at lovverk og reguleringer har hentet igjen teknologien på flere områder. Samtidig har antallet aktører som ønsker personlig informasjon fra brukere eksplodert. Dermed har personvern og konfidensialitet blitt høyt prioriterte områder for borgere/ forbrukere i den elektroniske samhandlingen. Digital teknologi åpner i større grad for kopling av til dels uskyldige *data*, og en slik sammenstilling kan konvertere dataene til slagkraftig og til dels kompromitterende *informasjon*.

Tillit er i tillegg et avgjørende punkt for at elektronisk samhandling virkelig skal skyte fart. Her er forbrukernes *oppfatning* av trygghet viktig. Denne oppfatningen er basert på en subjektiv vurdering av de forhold forbrukerne har mulighet og kapasitet til å ta inn over seg. ”Systemet” som sådant er for komplekst til at enkeltindividet kan tilegne seg full informasjon, for så å gjøre fornuftige og kalkulerte valg. Dermed må de ty til *tillit som verktøy* når valget om å gjennomføre en e-handelstransaksjon skal tas. Tillit er vanskelig å vurdere fordi forbrukere benytter både *kalkulerende* og *følelsesmessige* avveininger. De kan handle rasjonelt i ett øyeblikk og stole på maveføIelsen i et annet. Det er likevel viktig å skaffe innblikk i hvilke forhold som er *viktigst* for forbrukerne når det gjelder tillit og bruk av PKI-relaterte tjenester.

Utover disse forbrukervurderingene tar rapporten for seg flere piloter og undersøkelser som er gjort på PKI-feltet den siste tiden. Her ser vi spesielt på Norsk Tipping, BankID, Lånekassen, samt litt på det som er gjort mot offentlig sektor og i kommuner. Undersøkelsene tolkes i lys av forbrukerperspektivet og det vurderes hvorvidt, eller på hvilken måte, funnene kan benyttes videre i en eventuell forbrukerundersøkelse.

Som et komparativt utgangspunkt tar vi for oss Eivind Jacobsens arbeid rundt utviklingen av elektronisk betalingsformidling i Norge på 1980- og 90-tallet. For den enkelte forbruker innebærer elektronisk formidling av penger ofte store beløp, og sikkerhet er dermed et meget viktig aspekt i forbrukersammenheng. Kan man stole på at disse systemene håndterer transaksjoner på en sikker og stabil måte? Og hvilken nytte kan disse systemene gi som tidligere systemer manglet? Ettersom dette også er relevante problemstillinger for en fremtidig PKI-utrulling, er det naturlig å se nærmere på PKI-utviklingen i parallell til utviklingen av elektronisk betalingsformidling i Norge. Jacobsen fokuserer spesielt på de forhandlinger, konflikter og den strategiske posisjonering bankene stod for på 1980- og -90-tallet.

Dette forhindret en rask og samordnet utrulling av bankkort og terminaler. Det kan spores visse likhetstrekk i debatten rundt PKI-utviklingen, selv om premissene og aktørgruppene er noe forskjellige. Poenget er å få frem de uønskete effekter som kan oppstå når et ikke-kooperativt miljø får befeste seg. Ved at aktører velger ren egennytte som dominerende strategi kan den totale situasjonen forverre seg for alle aktørgrupper, samt for samfunnet som helhet, og herunder forbrukerne. Jacobsen oppsummerer videre forbruksforskningslitteraturen når det gjelder forbrukerinteresser og –krav, og ser disse i lys av betalingskort-problematikken. De relevante interesser/ krav som nevnes er; tilgjengelighet og valgmuligheter; pris og effektivitet; og forbrukerbeskyttelse. I denne rapporten brukes disse punktene som utgangspunkt for vurdering av forbrukerinteresser og –krav i forbindelse med PKI.

I tolkningskapitlet har vi sammenstilt vurderinger rundt forbrukerperspektivet, de foreliggende PKI-undersøkelsene, og erfaringene fra utviklingen av elektronisk betalingsformidling i Norge. Tolkningene er tematisk oppdelt og underkapitlene avrundes med konkretiseringer av spørsmål eller spørsmålstema som utgangspunkt for en workshop.

Videre diskuteres metodisk tilnærming til en forbrukerundersøkelse. Her forelås det en metodetriangulering mellom kvantitativ og kvalitativ metode. Kvantitativ metode gir breddeforståelse mens kvalitativ metode gir dybdeforståelse. Som kvalitativ metode foreslås mer spesifikt fokusgrupper. Det presiseres i kapitlet at metodetriangulering er ønskelig men at dette betinges av de finansielle ressurser som foreligger.

Avslutningsvis presenteres et sammendrag av workshopen som ble gjennomført med bakgrunn i en foreløpig versjon av dette grunnlagsdokumentet. Her ble relevante aktører invitert til å diskutere spørsmålstemaer og problemstillinger. Grunnlagsdokumentet og workshopen har til slutt dannet utgangspunkt for en konkretisering av forbrukerspørsmål. Disse er presentert i rapportens vedlegg.

Summary

In this report we apply a consumer perspective to the development of PKI in Norway. We make our arguments from the position of the consumer, with emphasis on attitudes and conduct, and hence develop questions for a consumer-related PKI-survey. It is vital to include consumers in the innovation and information processes, in particular in large and complex developments like that of PKI.

This report also considers potential problems that may arise in mixing roles and services. The purpose of PKI Forum is to coordinate the actions of public and private actors, and there might be confusion among individuals as to whether they should act as *consumers* or *citizens* in various instances. This is particularly relevant regarding former public services that are now privatized.

Furthermore, we discuss security, trust and privacy issues in a consumer perspective. Cyberspace has become more similar to our “analogue” world as regulations have caught up with technology in many instances. At the same time the amount of online actors that want personal information from citizens has surged dramatically, and privacy is therefore a key consumer issue. Digitisation makes possible transfer and compilation of data in new ways that might prove compromising to consumers. Hence trust is vital for the success of electronic interaction on a large scale. Trust is a subjective comprehension and based on the capacity for information gathering and evaluation by the individual consumer. Trust is thus a tool that can be used to reduce complexity. At the same time it is difficult to evaluate trust as it may vary from being a rational, calculative matter to becoming a “gut feeling” based on less rational factors.

Moreover, we consider several recent PKI-pilots and studies. These studies are discussed from consumer angle and evaluated as to how they can contribute to a potential consumer survey. In addition we use the works of Eivind Jacobsen on the development of electronic payment systems in Norway as a comparative case to PKI development. In electronic payment security is a key aspect, and questions arise as to whether these systems can be trusted. Further, what added value can they provide that earlier systems lacked? Such questions are as relevant to the development of PKI as to electronic payments. The main point is to focus on the negative, and potentially damaging effects, that surface in a non-cooperative environment.

In the final chapters we consider findings from all the previous chapters and interpret and discuss these in context. The interpretations are presented in sub-chapters and followed up by more specific questions or themes that where debated in a later workshop. This workshop is described in the final chapter.

Before the workshop is presented we describe a methodology for the consumer survey. A methodological triangulation between quantitative and qualitative methods is suggested, but such a triangulation is of course a more costly approach.

Finally, a preliminary list of questions, based on this report and on the workshop, is presented in the appendix.

Stikkord

PKI, elektronisk signatur, elektronisk ID, borger, forbruker, tillit, sikkerhet, personvern

Keywords

PKI, digital signature, electronic ID, citizen, consumer, trust, security, privacy

Grunnlagsdokument - forbrukervinkling på Public Key Infrastructure (PKI)

av

Dag Slettemeås

2004

STATENS INSTITUTT FOR FORBRUKSFORSKNING
postboks 4682, 0405 Oslo

Forord

PKI Forum er et samarbeidsforum for PKI (Public Key Infrastructure) med deltagelse fra næringsliv, forvaltning og bransjer (leverandører). Nærings- og handelsdepartementet er ansvarlig departement for PKI Forum. Som en del av PKI Forums satsing på en helhetlig strategi for PKI-utrulling i Norge har PKI Forums gruppe for forbrukerspørsmål fått i oppgave å ivareta forbrukerperspektivet. PKI Forums gruppe for forbrukerspørsmål har følgende mandat:

> *Gruppen skal kartlegge forbrukerinteresser samt både nåværende og fremtidig forbrukerbehov. Resultatene skal formidles til forbrukere, PKI-Forum, leverandører og tjenesteytere.*
>
> *Med forbruker menes privatpersoner / sluttbruker. Mandatet omfatter ikke personer som er rolleutøvere i virksomheter (attributtsertifikater) og virksomheter selv (virksomhetssertifikater).*

Resultatmålene er som følger:

> *Kartlegge og sammenfatte eksisterende undersøkelser samt foreta nødvendige undersøkelser om forbrukerinteresser og behov.*
>
> *Kartlegge hva forbrukere opplever som brukervennlig. Brukervennlighet omfatter bl.a. brukergrensesnitt, motivasjon, anskaffelsesprosess av nøkler / sertifikat, prismodeller og samtrafikk nasjonalt og internasjonalt.*
>
> *Kartlegge og ta stilling til personvernspørsmål.*

Med bakgrunn i gruppens mandat ble det fremmet en forespørsel til det daværende Nærings- og handelsdepartementet om midler til å utarbeide et grunnlagsdokument som tar for seg sluttbrukeres atferd og holdninger i forhold til PKI-utviklingen. Det ble innvilget midler til å utarbeide et konkret grunnlagsdokument for videreutvikling av spørsmål beregnet på forbrukere / borgere. I tillegg skulle det tilrettelegges for en workshop i regi av forbrukergruppen, der relevante parter kunne delta og bidra med temaer og spørsmål.

Dette grunnlagsdokumentet skal dermed danne utgangspunktet for en eventuell videre undersøkelse av forbrukeres / borgeres holdninger knyttet til en infrastruktur for elektronisk signatur og identifikasjon. I dokumentets vedlegg ligger et spørreskjema, som enten kan benyttes i en kvantitativ landsdekkende survey, eller som et utgangspunkt for fokusgrupper. Spørsmålene er utarbeidet på grunnlag av delanalyser fra dette dokumentet og innspill fra workshopen.

Per Myrseth (IBM) har vært forbrukergruppens leder og har bidratt sterkt i å få forbrukerspørsmål på banen, mens gruppen som helhet har diskutert seg frem til fruktbare vinklinger som er videreført i dette dokumentet. Dag Slettemeås (SIFO) har skrevet dokumentet med innspill og kvalitetssikring fra Per Myrseth. Videre har Kata-

rina de Brisis og Kristian Bergem fra Moderninseringsdepartementet vært sentrale aktører. Andre sterke bidragsytere har vært Agnes Beathe Steen-Fosse (eforum) og Kåre Presttun (Mnemonic).

Innhold

Sammendrag

I denne rapporten anlegges et forbrukerperspektiv på utviklingen av PKI i Norge. Det vil si at vi bygger opp argumentasjonen rundt forbrukernes posisjon, deres holdninger og atferd, og benytter dette som bakgrunn for å utvikle konkrete forbrukerrettede spørsmål. Disse spørsmålene, som ligger i vedlegget til denne rapporten, vil kunne benyttes videre i kvantitative surveyer eller som grunnlag for fokusgrupper i en PKI-undersøkelse.

I første omgang argumenteres det for viktigheten av å inkludere forbrukere både i innovasjons- og informasjonsprosessen ved større satsinger som denne. En PKI-infrastruktur vil være kompleks både rent teknologisk og med hensyn til rollestrukturer. Det er dermed viktig at forbrukere, som til slutt skal benytte og bygge tillit til denne infrastrukturen, blir inkludert gjennom en forbrukervinklet analyse. Dette betyr ikke at alt forbrukerne sier skal følges – det er *perspektivet* som anlegges som er avgjørende.

Videre ser vi på mulige problemer som kan oppstå ved en eventuell tjeneste- og rolleblanding. Ettersom PKI Forum har som formål å samordne PKI-satsingen – en satsing som inkluderer både offentlige og private aktører – tar vi opp problemstillinger rundt reell eller oppfattet sammenblanding av forbruker- og borgerrollen. Dette er spesielt relevant i forbindelse med tidligere offentlige tjenester som nå er konkurranseutsatt.

Andre forhold som diskuteres i et forbrukerperspektiv er sikkerhet, personvern og tillit. Over tid har ”cyberspace” utviklet seg fra å være preget av anarki i en tidlig fase til å bli likere vår ”analoge” verden, ved at lovverk og reguleringer har hentet igjen teknologien på flere områder. Samtidig har antallet aktører som ønsker personlig informasjon fra brukere eksplodert. Dermed har personvern og konfidensialitet blitt høyt prioriterte områder for borgere/ forbrukere i den elektroniske samhandlingen.

Digital teknologi åpner i større grad for kopling av til dels uskyldige *data*, og en slik sammenstilling kan konvertere dataene til slagkraftig og til dels kompromitterende *informasjon*. Lovverket åpner for at kommersielle aktører kan samle inn data fra brukere dersom de får et aktivt og informert samtykke fra brukeren til dette. Byrden på forbrukeren blir over tid stadig større ettersom et økende antall aktører ønsker et slikt samtykke. Dermed øker risikoen for at såkalt ”svake forbrukergrupper” (barn, eldre, etc) vil kunne bli utnyttet.

Tillit er i tillegg et avgjørende punkt for at elektronisk samhandling virkelig skal skyte fart. Her er forbrukernes *oppfatning* av trygghet viktig. Denne oppfatningen er basert på en subjektiv vurdering av de forhold forbrukerne har mulighet og kapasitet til å ta inn over seg. ”Systemet” som sådant er for komplekst til at enkeltindividet kan tilegne seg full informasjon, for så å gjøre fornuftige og kalkulerte valg. Dermed må de ty til *tillit som verktøy* når valget om å gjennomføre en e-handelstransaksjon skal tas.

Dersom man foretar gjentatte transaksjoner, og alt går slik det forventes, kan faktisk erfaring styrke tilliten til "systemet". I denne sammenheng kan systemet innebære Internett, e-handelsbransjen, e-handelsbedriften, lovverk og myndigheter, eller en kombinasjon av disse. Tillit er vanskelig å vurdere fordi forbrukere benytter både *kalkulerende* og *følelsesmessige* avveininger. De kan handle rasjonelt i ett øyeblikk og stole på maveføIelsen i et annet. Det er likevel viktig å skaffe innblikk i hvilke forhold som er *viktigst* for forbrukerne når det gjelder tillit og bruk av PKI-relaterte tjenester.

Utover disse forbrukervurderingene tar rapporten for seg flere piloter og undersøkelser som er gjort på PKI-feltet den siste tiden. Her ser vi spesielt på Norsk Tipping, BankID, Lånekassen, samt litt på det som er gjort mot offentlig sektor og i kommuner. Undersøkelsene tolkes i lys av forbrukerperspektivet og det vurderes hvorvidt, eller på hvilken måte, funnene kan benyttes videre i en eventuell forbrukerundersøkelse.

Som et komparativt utgangspunkt tar vi for oss Eivind Jacobsens arbeid rundt utviklingen av elektronisk betalingsformidling i Norge på 1980- og 90-tallet. For den enkelte forbruker innebærer elektronisk formidling av penger ofte store beløp, og sikkerhet er dermed et meget viktig aspekt i forbrukersammenheng. Kan man stole på at disse systemene håndterer transaksjoner på en sikker og stabil måte? Og hvilken nytte kan disse systemene gi som tidligere systemer manglet? Ettersom dette også er relevante problemstillinger for en fremtidig PKI-utrulling, er det naturlig å se nærmere på PKI-utviklingen i parallell til utviklingen av elektronisk betalingsformidling i Norge.

Jacobsen fokuserer spesielt på de forhandlinger, konflikter og den strategiske posisjonering bankene stod for på 1980- og -90-tallet. Dette forhindret en rask og samordnet utrulling av bankkort og terminaler. Det kan spores visse likhetstrekk i debatten rundt PKI-utviklingen, selv om premissene og aktørgruppene er noe forskjellige. Poenget er å få frem de uønskete effekter som kan oppstå når et ikkekooperativt miljø får befeste seg. Ved at aktører velger ren egennytte som dominerende strategi kan den totale situasjonen forverre seg for alle aktørgrupper, samt for samfunnet som helhet, og herunder forbrukerne.

Jacobsen oppsummerer videre forbruksforskningslitteraturen når det gjelder forbrukerinteresser og –krav, og ser disse i lys av betalingskort-problematikken. De relevante interesser/ krav som nevnes er; tilgjengelighet og valgmuligheter; pris og effektivitet; og forbrukerbeskyttelse. I denne rapporten brukes disse punktene som utgangspunkt for vurdering av forbrukerinteresser og –krav i forbindelse med PKI.

I tolkningskapitlet har vi sammenstilt vurderinger rundt forbrukerperspektivet, de foreliggende PKI-undersøkelsene, og erfaringene fra utviklingen av elektronisk betalingsformidling i Norge. Tolkningene er tematisk oppdelt og underkapitlene avrundes med konkretiseringer av spørsmål eller spørsmålstema som utgangspunkt for en workshop.

Videre diskuteres metodisk tilnærming til en forbrukerundersøkelse. Her forelås det en metodetriangulering mellom kvantitativ og kvalitativ metode. Kvantitativ metode gir breddeforståelse mens kvalitativ metode gir dybdeforståelse. Som kvalitativ metode foreslås mer spesifikt fokusgrupper. Det presiseres i kapitlet at metodetriangulering er ønskelig men at dette betinges av de finansielle ressurser som foreligger.

Til slutt presenteres et sammendrag av workshopen som ble gjennomført med bakgrunn i en foreløpig versjon av dette grunnlagsdokumentet. Her ble relevante aktører invitert til å diskutere spørsmålstemaer og problemstillinger. Grunnlagsdokumentet

og workshopen har til slutt dannet utgangspunkt for en konkretisering av forbruker-spørsmål. Disse er presentert i rapportens vedlegg.

Innledning

Denne rapporten har som hovedformål å finne frem til måter PKI Forums gruppe for forbrukerspørsmål kan kople sitt mandat mot Forumets kommunikasjonsstrategi, og videre konkretisere forhold som er avgjørende for en utrulling[1] av PKI (Public Key Infrastructure) i nær fremtid.

Et av virkemidlene for å nå forbrukergruppens målsetning er å kartlegge holdninger og faktisk atferd hos norske forbrukere/ borgere, og samtidig se på utviklingsmønstre i norsk og internasjonalt samfunnsliv, næringsliv og forvaltning som er relevant for utvikling og utrulling av PKI i Norge. Med dette som bakgrunn vil rapporten ta utgangspunkt i en *forbrukervinkling* og ikke en teknisk, politisk eller bransjeorientert tilnærming til PKI, selv om dette er relevante faktorer. Det er *perspektivet* vi her velger som legger premissene for argumentasjonen og gangen i rapporten. Denne rapporten vil søke å identifisere de områder hvor vi ønsker ytterligere informasjon om forbrukere og deres atferd. Det er et mål at det som en oppfølging av denne rapporten gjennomføres en undersøkelse rettet mot norske forbrukere for å innhente den ønskede informasjon.

Det er PKI Forum's *fokusgruppe for forbrukerspørsmål* som står for grunnlagsdokumentet. Gruppens mandat er som følger:

> *Gruppen skal kartlegge forbrukerinteresser samt både nåværende og fremtidig forbrukerbehov. Resultatene skal formidles til forbrukere, PKI-Forum, leverandører og tjenesteytere.*
>
> *Med forbruker menes privatpersoner/ sluttbruker. Mandatet omfatter ikke personer som er rolleutøvere i virksomheter (attributtsertifikater) og virksomheter selv (virksomhetssertifikater).*

Resultatmålene for forbrukergruppen er som følger:

> *Kartlegge og sammenfatte eksisterende undersøkelser samt foreta nødvendige undersøkelser om forbrukerinteresser og behov.*
>
> *Kartlegge hva forbrukere opplever som brukervennlig. Brukervennlighet omfatter bl.a. brukergrensesnitt, motivasjon, anskaffelsesprosess av nøkler / sertifikat, prismodeller og samtrafikk nasjonalt og internasjonalt.*
>
> *Kartlegge og ta stilling til personvernspørsmål.*

Forbrukergruppens mandat og resultatmål danner utgangspunktet for målsetningen om å gjennomføre en forbrukerundersøkelse rundt PKI-relevante forhold.

[1] I bransjeterminologien er det vanlig å omtale PKI med "utrulling" – altså en helhetlig utvikling og implementering av teknologi og rollestrukturer.

1.1 Kommunikasjon mot sluttbrukere?

Hovedmålsetningen for forbrukergruppen er å identifisere norske forbrukeres motivasjon og modenhet for å ta i bruk e-signatur og e-legitimasjon, slik at en PKI-utrulling kan finne sted på fornuftige premisser. Før en utrulling finner sted virker det formålstjenlig at forbrukerne indirekte har bidratt ved at deres modenhet og behov er belyst og analysert.

Samtidig fremheves det i PKI Forumets reviderte kommunikasjonsstrategi[2] at forbrukere ikke primært er en målgruppe PKI Forumet bør henvende seg til. Det hevdes at primærgruppene det skal kommuniseres mot vil være myndigheter, brukersteder og tjenesteutviklere. Det nye momentet i revidert strategi er at kommunikasjonen mot sluttbrukere hovedsakelig skal skje gjennom brukersteder. Dermed er sluttbrukere fortsatt ikke en prioritert gruppe, selv om det hevdes at "Forumet likevel kan bidra med grunnlagsmaterialet for brukerstedene som kan benyttes i en slik kommunikasjon". Det er ikke nødvendigvis noen motsetning i en *forbrukervinklet tilnærming* til PKI og en *ikke-forbrukerrettet kommunikasjonsstrategi*, og det virker fornuftig å henvende seg til de tre ovennevnte primærgrupperinger.

Likevel, med blant annet bakgrunn i erfaringer fra utrullingen av elektronisk betalingsformidling på 90-tallet (kapittel 4), kan det virke hensiktsmessig å ha en presis, enkel og samkjørt kommunikasjonsstrategi mot forbrukerne, selv i forkant av en utrulling. Da vil forbrukerne kunne etablere tillit til et enhetlig system, og redusere/ fjerne usikkerhet rundt hvorvidt PKI blir gangbart eller ikke. Det verste som kan skje i forbindelse med en slik utrulling er at forbrukerne sitter på gjerdet og venter, fordi de er usikre på hva dette er, hvem som er med, og hva en skal bruke de ulike tjenestene til (signatur, legitimasjon, etc). Dersom det satses tungt på kommunikasjon mot brukerstedene bør en viktig del av strategien være hvordan brukerstedene videre skal forholde seg til en "felles skissert plan" for å dra med seg sluttbrukerne.

I forbindelse med utrullingen av elektroniske betalingskort var blant annet kundebehandlerne i de enkelte bankfilialene instrumentelle i å markedsføre kortenes fortreffelighet mot kundene. Dette har også vært tilfellet der bankene måtte overtale kundene til å bruke nettbank. Viseadministrerende direktør Bo Harald i Nordea hevder at det viktigste i den sammenheng ikke var fokus på videre forenkling og forbedring av teknologien, men overtaling, rådgivning og markedsføring, for å endre atferd fra det forbrukerne var vant til[3]. Det har tatt tid å endre atferden, men nå har Nordea flere millioner nettbankkunder i Norden. For nye banktjenester handler det nå om å bygge videre på den nye "vanens makt".

Uansett virker det fornuftig å ha en kommunikasjonsstrategi som direkte eller indirekte er rettet mot forbrukerne, selv i god tid før utrullingen. Da kan forbrukerne forberede seg og ikke få følelsen at de får en slik infrastruktur og tilhørende tjenester rett i fanget uten forvarsel. Folk må bli vant til tanken om å skulle håndtere elektronisk legitimasjon og signatur, men da må "markedsføringen" være enkel og samkjørt. I PKI Forums strategidokument[4] fremheves det også under felles ansvar, punkt 4, at det skal gjennomføres informasjons- og bevisstgjøringskampanjer mot forbrukere. Dette er også helt i tråd med PKI-Forums opprinnelige mandat om å få frem brukervennli-

[2] PKI Forum Sekretariatet – revidert kommunikasjonsstrategi av 01.06.2004.
[3] Annonsebilag for IBM og IBM Business Partnere.
[4] PKI Forum – *Strategi for en samfunnsinfrastruktur for elektronisk signatur og elektronisk ID i Norge,* av 20. juni 2002, s.30

ge PKI-løsninger, og kommunisere dem ut til publikum[5]. Kommunikasjon mot forbrukere må uansett finne sted, og bør opprettholdes som et viktig delmål i den endelige kommunikasjonsstrategien.

1.2 Forbrukervinkling og forbrukerundersøkelse

PKI Forum som koordineringsorgan for PKI er klar over kompleksiteten i denne infrastrukturen og at dette nødvendigvis vil gi seg utslag i forbruker-/ borgersentrerte hindringer. Dermed bør det avdekkes hvilke hindringer man står overfor før en større utrulling av PKI finner sted. Man bør samtidig se på hvilke faktorer som er kritiske for at forbrukeren/ borgeren ønsker å ta i bruk en slik løsning. Vi bruker her "forbruker" om sluttbruker i et markedsperspektiv og "borger" om sluttbruker i et statlig/ offentlig perspektiv. Vi foretar dette skillet fordi både offentlig forvaltning/ myndigheter og private aktører er satt til å samarbeide om en infrastruktur som krysser kommersielle og ikke-kommersielle tjenestebånd.

I kapittel 2 vil vi se nærmere på denne todelingen av innbyggernes roller, fordi disse rollene tradisjonelt sett har medført ulike og delvis separate sett av rettigheter og plikter. En satsing på et fullverdig PKI-tilbud kan innebære en blanding (eller oppfattet blanding) av roller hos norske innbyggere som kan virke forvirrende. Dermed er det relevant å se nærmere på denne problemstillingen.

I forkant av en eventuell undersøkelse, som vil være landsrepresentativ og gjennomført i regi av et egnet meningsmålingsinstitutt, vil det være viktig å hente inn og analysere funn fra andre liknende undersøkelser. Dermed vil vi på et mer kvalifisert grunnlag kunne utarbeide relevante spørsmål til undersøkelsen. Dette vil vi gjøre i kapittel 3. I tillegg vil vi ta for oss utbredelsen av bankkort i Norge, for å ha et komparativt case å sammenlikne med, og som allerede er historisk dokumentert. Dette gjøres i kapittel 4. Til slutt vil vi i korte trekk oppsummere funnene fra de tidligere kapitlene og ta for oss faktorer som vurderes som viktige for en undersøkelse, og som samtidig kan synliggjøre de begrensninger en slik undersøkelse faktisk har. Det vil også konkretiseres spørsmål til en undersøkelse i kapittel 5, mens det i kapittel 6 redegjøres for mulige metodevalg.

I kapittel 7 presenteres utfallet av en workshop som ble holdt for relevante aktører. Før workshopen ble en foreløpig versjon av dette grunnlagsdokumentet distribuert slik at man kunne forberede seg til sesjonen. I ettertid ble funn fra grunnlagsdokumentet og fra workshopen samkjørt og forbrukerrelaterte PKI-spørsmål formulert. Disse presenteres i rapportens vedlegg.

[5] Fra referat plenumsmøte 14. november 2002 i Nydalen.

2 Forbrukerperspektivet

Det å benytte forbrukerperspektivet i elektronisk samhandling innebærer hovedsakelig å sette seg inn i sluttbrukers situasjon – altså et bottom-up perspektiv som ikke tar utgangspunkt i teknologi, politikk eller bransjeinteresser.

Generelle forbrukerinteresser tilsier at de tjenester som tilbys bør være tilpasset brukernes behov og ønsker på en rimelig og relevant måte (Slettemeås 2002: 23). Det er ofte lett at brukerbehov blir oversett på områder der teknologien har en så rask utvikling og utbredelse som innen elektronisk forretningsdrift og forvaltning. Da er det viktig å foreta en ”reality-check” for å se hvor man ligger i landet mht. forbrukere. Utviklingstakt og krav til lønnsomhet medfører at det ofte lanseres premature løsninger, eller en tjeneste som ikke mottas av sluttbrukerne slik forventningene skulle tilsi. Dette kan gi enda større kostnader og mindre inntjening enn om man hadde foretatt en grundig brukerevaluering først.

Dette er spesielt viktig når det gjelder større og mer komplekse teknologiske visjoner – slik som satsingen på en nasjonal *Public Key Infrastructure.* Her er det snakk om en infrastruktur som skal tåle tidens tann og som er bygget opp av et komplekst nett av relasjoner og teknologi. Alle som deltar i en slik infrastruktur har ulike krav, ansvar og oppgaver – og alle er like viktige for at infrastrukturen skal fungere optimalt. Infrastrukturen må være robust og stabil, men likevel være fleksibel nok til å ta inn over seg den raske utviklingstakten som finner sted på teknologisiden.

Dersom man skal få en mest mulig komplett evaluering før en storstilet utrulling, bør derfor flere aspekter vurderes og analyseres i sammenheng. Det er vanskelig å få et godt bilde av fremtidig brukeradopsjon av et slikt system dersom man for eksempel kun baserer seg på én brukerundersøkelse (holdninger), eller én brukertest (erfaringer / usability-test). Dette gjelder særskilt teknologi som brukere på forhånd ikke har hatt særlig befatning med. Det er alltid vanskelig å forholde seg til ”fremtiden” ved å spørre folk om holdninger de har til det relevante fenomenet, eller til liknende og relaterte fenomen. Dermed må det foretas en bred gjennomgang av flere forhold som til sammen gir et bilde av hvor forbrukeren står.

I disse tider er det gjerne fokus på de muligheter ny digital teknologi gir for individuelle og skreddersydde tilbud og løsninger. Samtidig er fokus rettet mot å standardisere visse løsninger, slik at tillit kan bygges til én løsning og brukerne kan ”lære” å ta i bruk denne løsningen. Vi vet at økt konkurranse gjerne driver løsninger i retning av å bli mer brukervennlige – og rimeligere – samtidig som man ønsker at noen kontrollerer og ivaretar alle aktørers interesser i et teknologisk samkvem.

Vi ser blant annet paradokset i Microsoft’s operativsystem Windows; dette er ikke en åpen kilde-løsning og den låser brukere inn i ett system som sjeldent slipper andre til. Ettersom Microsoft har tilnærmet monopolmakt reduseres mulighetene for at andre aktører med bedre, mer brukervennlige og rimeligere løsninger slipper til. Samti-

dig kan det med sikkerhet hevdes at mange brukere er fornøyd med å lære seg ett system, for dermed å slippe å forholde seg til et mangfold av systemer, for eksempel ved skifte av jobb.

Hva veier så tyngst i dette henseendet? Nye – og muligens bedre og rimeligere løsninger – eller enkelhet, bekvemmelighet og mulighet for å bygge kompetanse over tid? Vi vil ikke ta stilling til dette nå – dette er kun en illustrasjon på viktigheten av å ta flere faktorer i betraktning når man skal vurdere brukernes ofte ambivalente forhold til ny teknologi.

2.1 Forbruker og borger

I et forbrukerperspektiv er det viktig å vurdere de roller et individ har i kraft av å være innebygger i en nasjonalstat. En sluttbruker av ulike elektroniske tjenester vil være tilknyttet forbrukerrollen i de henseender der kommersielle aktører opererer sammen med individet i et konkurranseutsatt marked. I slike tilfeller vil forbrukeren være beskyttet av blant annet kjøpsloven, e-handelsdirektivet og markedsføringsloven.

Over tid har flere og flere tjenester som tidligere var statlige og kommunale anliggender blitt satt ut til kommersielle aktører. Dermed har tjenester som det offentlige tidligere var ansvarlige for, og som var knyttet til borgerrollen, blitt overført til et konkurranseutsatt marked. Slik aktiveres også forbrukerrollen. Denne overføringen av tjenester til kommersielle aktører kan føre til en faktisk sammenblanding av roller og regelverk – men like viktig – det kan føre til en *oppfattet endring blant landets innbyggere, som enten er reell eller ikke reell.* Dersom et individ for eksempel tror at staten fremdeles er tilbyder av en spesiell tjeneste, og den ikke er det, innebærer dette flere problemstillinger:

- Individet tror staten tar seg av forhold tilknyttet tjenestetilbudet og opptrer dermed passivt i forhold til informasjonsinnhenting og kritisk evaluering av tilbudet.
- Individet kan bli misbrukt i flere henseender fordi han/ hun ikke er oppmerksom på forholdet. For eksempel ved å gi fra seg unødvendig eller sensitiv informasjon til kommersielle aktører.
- Endringen kan ha ført til en sammenblanding av kontrollinstanser og juridiske regler knyttet til tjenestetilbudet.
- Grunnen til at individet forholder seg passiv kan bunne i informasjonssvikt om endringer rundt tjenestetilbudet.

Ergo så kan borger- og forbrukerrollene *faktisk* være endret, de kan *oppfattes* å være endret, eller de kan være *sammenblandet* i en ny og mer ugjennomsiktig (og kompleks) rollestruktur.

I forbindelse med en PKI-utrulling og nye tjenester der sikkerhet, legitimasjon og signaturer gjøres relevant, er det viktig å se på individets rolle. Ettersom kommersielle og offentlige aktører samarbeider om en satsing betyr det at begge grupperinger ønsker en PKI for sine sluttbrukere. Men for sluttbrukeren er det ikke innlysende hva dette innebærer, og om en bør forholde seg til PKI i et konkurranseutsatt marked, i forhold til offentlige tjenester, eller som en kombinasjon av begge. Vil ulike regler, policyer og lovverk gjelde for kommersielle og offentlige tjenester? Bør man være en bevisst og skeptisk forbruker i forhold til kommersielle PKI-tjenester og en godtakende, passiv borger i forhold til offentlige tjenester? Dette er en problemstilling man bør ha i mente når kommunikasjon/ markedsføring står på dagsordenen.

I Slettemeås og Helle-Valle (2003) tas denne problematikken opp i forhold til bredbåndssatsingen i Norge. Et av hovedspørsmålene som stilles her er hvorvidt det er som ”aktive forbrukere vi ønsker å forholde oss til bredbånd?”. Det samme spørsmålet kan stilles om PKI som infrastruktur. Det pekes på i nevnte rapport at innbyggerne blir ”tvunget” til å innta en forbrukerrolle, ved å forholde seg til tilbud i et marked. Dette fordi myndighetene ikke har vurdert denne infrastrukturen som en borgerrett, eller et allemannseie. I konklusjonen hevdes det at (Slettemeås og Helle-Valle 2003: 66):

> *Bredbåndsteknologien, i et konvergerende teknologisk bilde, representerer i tillegg et så komplekst felt at de fleste forbrukere ikke har kapasitet til å skaffe seg oversikt over kortsiktig versus langsiktig nytte (…). Dermed kan det argumenteres for en relativt sterk grad av koordinering og samordning av utbygging og regulering på bredbåndsfeltet, mens innholdssiden fremdeles kan operere på kommersielle vilkår. På den måten sikrer man seg mot ”digitale skiller” i befolkningen gjennom utjevnende politikk, koordinering av ressurser, (…), samt et helhetlig strategisk perspektiv på teknologifronten. Da kan det bygges et fundament for langsiktig, reflektert samfunnsnytte – ikke kun kortsiktig, ureflektert eller underinformert forbrukernytte.*

Selv om dette er en annen type infrastruktur enn PKI er det likevel relevant å betrakte problemstillingen om hvorvidt man skal forholde seg til dette som forbruker i et konkurranseutsatt marked, som borger, eller som en kombinasjon av begge.

2.2 Sikkerhet og brukertjenester

Innen elektronisk tjenestehandel og saksgang har forbrukere blitt mer og mer vant til kommersielle og offentlige tjenestetilbud. Samtidig har lov- og regelverk kommet etter og tatt grep om ”cyberspace” til forskjell fra de mer ”anarkiske” tilstander som preget første fase av Internettets levetid. Tidligere måtte forbrukere være svært varsomme med hvilke tjenester de forholdt seg til, hva slags informasjon de avga, og hvordan transaksjonene foregikk. Dette medførte at forbrukerne i stor grad måtte ha *tillit* til den kommersielle e-handelsaktørens intensjoner, samt de sikkerhetsmekanismer nettet kunne tilby (spesielt på transaksjonssiden).

Vi har den siste tiden sett endringer, både av teknologisk og juridisk art, som har påvirket bruken av nettjenester i positiv retning. Stadig flere forbrukere benytter nettet til flere typer tjenester, og tidligere ”analoge” tjenester tilbys elektronisk eller ”digitalt”.

Samtidig som Internett og webtjenester gjøres sikrere, både juridisk og teknologisk, tilbys nye typer tjenester som krever en høyere grad av sikkerhet og vern av personopplysninger. I tillegg kommer nye deltjenester som er tilknyttet eksisterende elektroniske tjenestetilbud. Her er det relevant å nevne digitale signaturer. Dette er en type tjeneste som kun har vært tilgjengelig i den analoge verden, der man blant annet signerer dokumenter personlig. Dette krever at man fysisk overleverer dokumentet, eller signerer det og sender det i posten. I og med at mer og mer av saksbehandling og informasjonsoverføring skjer digitalt, er signaturaspektet en flaskehals i saksbehandlingsprosessen.

Det er ikke bare signeringsfunksjonen som er relevant. Nye tjenester vil også øke kravene til konfidensialitet og autentisering av personer. Det er her PKI kommer inn som en infrastruktur som tilbyr alle de nevnte ”sikkerhetstjenester”. Samtidig stilles det spørsmål ved håndtering og oppbevaring av persondata – noe som er svært viktig i vurderingen av borger- / forbrukerrollen i de neste tiår.

PKI-teknologien er tiltenkt å være så ”åpen” som mulig, slik at flest mulig aktører kan nyttiggjøre seg infrastrukturen. Det innebærer at mange aktører vil bidra i den raske utviklingen, en utvikling som fremstår som kompleks og uforstående. Dermed er det naturlig å forvente at mange sluttbrukere (og små bedrifter) ikke vil ha kunnskap nok om den underliggende PKI-teknologien. Det kan heller ikke forventes at en gjennomsnittlig sertifikateier/ sertifikatbruker vil lese og forstå lange og komplekse juridiske dokument som regulerer kontraktsforholdene mellom de ulike aktørene i en PKI, og samtidig forstå de ulike rollene i infrastrukturen.

Tar man dette på alvor betyr det at før en kritisk masse av sertifikater utstedes og tas i bruk, bør det vurderes hvordan man kan informere og lære opp brukere (borgere og forbrukere, avhengig av tjenestekategori) i deres respektive roller, ansvarsområder, og rettigheter som ”funksjonelle brukere” av sertifikater i en PKI[6]. Det er også viktig å erkjenne at forbrukere og bedrifter behandles som forskjellig enheter og dermed knyttes til ulike juridiske rammeverk.

2.3 Sikkerhet og personvern

Når begrepet personvern benyttes innenfor området informasjonssikkerhet og elektronisk samhandling, snakkes det gjerne om at personlig identifiserbar informasjon og sensitiv informasjon vil bli innsamlet og brukt *kun* for de bruksområder de opprinnelig var tiltenkt[7].

- ***personlig identifiserbar informasjon:*** informasjon som kan spores tilbake til et individ, som navn, personnummer, postadresse og e-postadresse
- ***sensitiv informasjon:*** informasjon som under visse omstendigheter krever spesiell beskyttelse, som finansiell og medisinsk informasjon, samt informasjon knyttet til barn. Personnummer er ikke lenger vurdert som sensitiv informasjon i Norge.

Det hevdes samtidig at *personvern* ikke er det samme som *konfidensialitet* og *sikkerhet.* Konfidensialitet refererer til en forventning om at informasjon ikke vil gjøres tilgjengelig for, eller vil bli sett av, uautoriserte aktører. Sikkerhet refererer til de teknologiske virkemidler som tas i bruk for å forhindre tyveri og / eller uautorisert tilgang til informasjon. Teknologiske virkemidler, slik som SSL[8] og kryptering av beskjeder, kan benyttes for å skape en rimelig forventning om personvern.

I elektronisk samhandling er bekymringer knyttet til personvern en av de mest betydningsfulle utfordringer forbrukere og myndigheter står overfor. Digital teknologi åpner for innsamling, lagring og kopling av data på en måte som kun muliggjøres av denne teknologien, og Internett legger spesielt til rette for overføring, spredning og samkjøring av ulike datakilder. Dermed kan data som ”uskyldig” samles fra separate kilder virke mer slagkraftige og kompromitterende når de settes sammen og danner ”ny informasjon.” I tillegg til disse koplingsmulighetene har også *omfanget* av personopplysninger økt; slik som URL’er man besøker, søkeord man benytter seg av og cookies (tekstfiler) fra nettsteder man har besøkt (Teknologirådet 2004: 10). Samtidig

[6] Information Security Committee; *PKI Assessment Guidelines* – C.5 Consumer Issues and Privacy: s.55
[7] Ibid.: ss.63-64
[8] SSL betyr secure sockets layer og er en type PKI-aktivert sikker kommunikasjonsform som vanligvis benyttes for at en browser skal kunne autentisere (identifisere) en webside og lage en sikker link til browseren for å forhindre uønsket infiltrering mens kommunikasjonen foregår. SSL innebærer som oftest at man slipper nøkkeldistribusjon ved at det benyttes selv-signerende sertifikater som plasseres i browser-softwaren, som tiltrodde sertifikater før softwaren distribueres, eller den legges til av bruker i ettertid.

må man være klar over at det ikke er teknologien i seg selv som har negativ eller positiv innvirkning på personvernet – det er anvendelsen av og premissene for utviklingen av ny teknologi som er avgjørende (NOU 1997:19).

I følge OECDs *Privacy Guidelines*[9] legges det frem visse retningslinjer for beskyttelse av persondata:

- *Innsamlingsbegrensninger* – data bør samles inn på lovlig og rettferdig vis.
- *Datakvalitet* – personlige data bør kun benyttes for relevante hensikter, og dataene bør være oppdaterte og korrekte.
- *Spesifisering av hensikt* – det må informeres om hensikten med bruk av personlige data.
- *Bruksbegrensning* – data bør ikke avsløres til andre aktører / formål uten samtykke fra bruker eller som spesifisert i regelverk.
- *Sikkerhetsgaranti* – personlige data bør beskyttes av rimelige sikkerhetstiltak for å forhindre tap, ødeleggelse og misbruk av data.
- *Åpenhet* – generell policy om åpenhet med hensyn til utvikling / endringer rundt bruk av personlige data.
- *Individuell deltakelse* – individer har rettigheter med hensyn til egne personlige data som besittes av andre.
- *Ansvarlighet* – den som kontrollerer de personlige dataene er ansvarlig for å rette seg etter de gitte prinsipper.

Dette kan fremstå som generelle retningslinjer, og de ble fremsatt av OECD i 1980, men er like gyldige i dagens elektroniske samfunn. Ved innføring av en PKI, som i utgangspunktet skaper nye aktørrelasjoner og koplinger av teknologi og ansvar, er det avgjørende at det eksisterer åpenhet om hva personlige data benyttes til. Dette gjelder håndtering av data, hvem som er ansvarlig for beskyttelse og datakvalitet, etc. Dette er en stor utfordring for alle aktører og selv om det er en erkjennelse at kompleksiteten er formidabel for den gjennomsnittlige bruker, skal alle brukere ha like muligheter for å spore tilbake og identifisere bruken av avgitt personlig informasjon. Dette kan virke som en utopi og fordrer stor grad av tillit til de mekanismer og aktører som opererer i en PKI.

Det at strukturer blir mer sammenvevd og uoversiktlige gjør det også vanskelig for den enkelte forbruker / borger *å identifisere hvor / hvordan bruddet har foregått* (f.eks hvem som har levert ut personlig informasjon urettmessig til en tredjepart). PKI har som mål å bygge opp tillitsstrukturer av aktører som kontrollerer hverandre. Dermed blir det avgjørende å identifisere hvilke aktører forbrukerne setter sin tillit til i et slikt system. Dette går vi nærmere inn på i neste kapittel om tillit.

Datatilsynet skriver i *Personvernrapporten*[10] at personvern handler om retten til å være i fred dersom en selv ønsker det. Det sier seg selv at dette i stor grad blir en subjektiv opplevelse av hvor grensen for eget privatliv skal gå. Likevel må Datatilsynet og andre myndigheter følge opp med juridiske retningslinjer som beskytter den enkelte borgers krav på vern av personlig integritet. Det hevdes at kunnskap er makt og at denne kunnskapen lett kan bli misbrukt. Derfor bør utenforstående aktører besitte minst mulig opplysninger om enkeltborgere. Med andre ord skal det kun samles inn data som er helt nødvendig for et gitt formål, og dette skal være saklig begrunnet. Dessuten skal den enkelte ha rett til innsyn i egne data, og ha mulighet for å be om at data slettes. Gjennomgangstonen i Personvernrapporten, og også rapportens

[9] Ref. i PKI Assessment Guidelines; s.64
[10] Datatilsynets årsmelding til AAD "med ny vri", Oslo, april 2004. Tilgjengelig på www.datatilsynet.no

tittel, fremsetter påstanden om at det stadig blir "vanskeligere å verne om det private". Et annet viktig dokument i denne sammenheng er Datatilsynets notat om "Risikovurdering av informasjonssystem"[11], som tar for seg risiko og personvern med utgangspunkt i Personopplysningsloven.

PKI-Forums Juss- og Regelverksgruppe[12] har blant annet sett på problemstillingen med personopplysninger i forhold til PKI. I hovedsak forholder man seg her til den nye Personopplysningsloven av 01.01.2001, som bygger på et EU-direktiv av 1995[13]. I Jussgruppens rapport hevdes det at misbruk av personopplysninger kan få alvorlige følger, så vel personlig som sosialt, for den skadelidte. Samtidig er det vanskelig å påvise økonomisk tap ved personvernkrenkelser. Derfor vil det være særlig viktig å være oppmerksom på denne type brudd, og sikre at det juridiske rammeverket støtter den enkelte borger i slike tilfeller.

Jussgruppen ser dessuten Lov om elektronisk signatur (LES) og Personopplysningsloven i sammenheng. Det fremgår av LES at sertifikatutsteder kun kan hente inn personopplysninger direkte fra den det gjelder, eller med dennes *uttrykkelige samtykke.* Dessuten skal det kun samles inn informasjon som er relevant for *utstedelse* eller *opprettholdelse* av et sertifikat. Jussgruppen hevder at dette er i samsvar med Personopplysningsloven.

Når det gjelder bruk av personnummer som identifikasjon sier Personopplysningsloven (§ 12) at fødselsnummer og andre entydige identifikasjonsmidler kun kan benyttes når det er saklig behov for sikker identifisering og dersom metoden er nødvendig for å oppnå slik identifisering (personnummer er som nevnt ikke lenger vurdert som sensitiv opplysning). Personnummer åpner for sporing, noe som både er en fordel og en ulempe. Fordelen er at dette gir en entydig identifikasjon av en person. Samtidig så åpner det for uheldige koplinger, kartlegging og kontroll.

Jussgruppa viser til NOU 2001:10 "Uten penn og blekk" der det anbefales fire typer sertifikater[14]. Blant disse er det kun anbefalt å innta fødselsnummeret i såkalte *offentlige personsertifikat*, hvor den offentlige virksomhet har et begrunnet behov for dette. Utover dette anbefales det unike identifikatorer som er ulike fødselsnummeret, men som kan oversettes av sertifikatutsteder ved behov. Jussgruppen tolker utvalgets intensjon dit hen at det ikke er ønskelig med utstrakt bruk av personnummer. Men jussgruppa påpeker også at utvalgets utsagn ikke er gjeldende rett, og at mange usikkerhetsmomenter dermed fremdeles gjenstår.

I jussgruppas foreløpige rapport nevnes det fire mulige løsninger for bruk av fødselsnummer i et sertifikat:

a) fødselsnummer i sertifikatet, men eksponering kun mot mottakere som har behov for dette
b) ikke fødselsnummer i sertifikatet, men oversette til fødselsnummer mulig for autoriserte mottakere. Oversettelse skjer hos mottaker
c) utlevering av fødselsnummer til autoriserte mottakere ved kopling av sertifikatopplysninger mot registre hos utsteder
d) sertifikatholder har to forskjellige sertifikater, et med og et uten fødselsnummer

[11] Datatilsynet: "Risikovurdering av informasjonssystem", utgitt 15.02.02
[12] Revidert problemnotat etter møte 29.01.03: "Rettslige rammevilkår om digitale signaturer og PKI"
[13] Europaparlamentet og –rådets direktiv 95/46/EC av 24.oktober 1995.
[14] Disse 4 er: Ansattesertifikater, Virksomhetssertifikater, Offentlige personsertifikater og Profesjonssertifikater.

Uansett vil det kunne oppstå konflikt rundt ideen om ”gjenbruk” av sertifikater og forbrukernes oppfatninger med hensyn til innsamling og oppbevaring av data. Det må gjøres uttrykkelig klart for forbrukerne at selv om sertifikater gjenbrukes til andre tjenesteformål, så vil ikke de data (personalia) som oppgis ved utstedelse av sertifikatet (til CA[15]) deles med andre tredjeparter.

Dersom en slik eksponering likevel skulle forekomme, i en eller annen sammenheng, så vil *samtykke fra forbruker* bli avgjørende. Såfremt man får en borger/ forbrukers samtykke kan man i stor grad samle inn og utnytte data til mange formål. I Personopplysningsloven legges det opp til langt større frihet for den enkelte borger til å vurdere hva en vil takke ja til. Dette gir selvsagt større fleksibilitet men samtidig kan det oppstå en situasjon der den enkelte borger må forholde seg til et stort antall forespørsler fra private og offentlige tjenestetilbydere. I slike tilfeller fryktes det at ”svakere” forbrukergrupper vil være mindre kritiske til hva de takker ja til. Dermed er potensialet for misbruk større ved at innsamlete data koples mot andre datakilder, mens det enkelte individ mister oversikt over hvor ulike data havner.

Slik sett er det avgjørende å identifisere hvor tilliten skal bygges i forhold til PKI-infrastrukturen og samtidig vurdere om brukerne oppfatter at de har eller bygger tillit på ”samme sted” som aktørene i infrastrukturen ønsker at dette skal forekomme.

2.4 Sikkerhet og tillit

I e-Norge planen har viktigheten av en sikker infrastruktur for elektroniske tjenester vært fremhevet. Dette ses som helt nødvendig for å skape tillit hos brukere slik at ”elektronisk samhandling over Internett virkelig skyter fart.”

PKI Forum har også i sitt strategidokument[16] presisert at mangel på tillit er en av de viktigste barrierene for gjennombrudd av handel og overføring av sensitiv informasjon på Internett. Det hevdes her at elektroniske grenseflater (f.eks nettsteder) ikke gir mulighet for en ”rik toveis kommunikasjon” mellom bruker og tjenestetilbyder. Det hevdes videre at dersom brukeren ikke har kjennskap til, eller en relasjon med tjenestetilbyderen fra før, så må tilliten baseres på den informasjon som er tilgjengelig på nettstedet.

Her legges det opp til en *kalkulerende form* for tillit der brukeren samler inn informasjon om tjenestetilbyderen via nettsteder. Det fokuseres også på tekniske garantier fra sertifiseringer, og på betryggende avtaler som regulerer ansvar, samt gode tilsynsordninger. I forslaget til hva som kan bidra til økt tillit til elektroniske tjenester, som er støttet av PKI, fokuserer strateginotatet på:

a) Sertifiseringsordninger:
   At en uavhengig tredjepart kan bidra til et tilstrekkelig tillitsnivå gjennom en sertifisering av enten aktør/ rolle eller en elektronisk tjeneste som helhet.

b) Garanti- og forsikringsordninger:
   Garanti- og forsikringsprodukter i markedet som er tilpasset virksomheter på Internett hvor nettstedet autentiseres og kvalitetsvurderes.

[15] CA = Certificate Authority
[16] PKI Forum – *Strategi for en samfunnsinfrastruktur for elektronisk signatur og elektronisk ID i Norge,* av 20.juni 2002; s.24

c) PKI-tjenester og tillit:
PKI-tjenester markedsføres ofte som ”tillitstjenester”, og har derav behov for en meget høy grad av tillit. Erkjennelsen er at man ikke bare må ha tillit til aktøren det kommuniseres med, mens også til sikkerheten i de tekniske løsningene.

En indikasjon på forbrukeres tillit til Internett og sikkerhetssystemer har vært å se på antall betalingstransaksjoner som foregår over nettet. Her har vi sett en formidabel økning de siste årene. Volumet av betalingstransaksjoner steg blant annet med 30 % fra 2002 til 2003[17]. Dette er likevel ikke en indikasjon på den *faktiske* sikkerheten i systemet. Omfanget av webhacking og misbruk av kredittkort har også økt betydelig. Ser man på misbruk relativt til antall transaksjoner er nok likevel tallene mer moderate.

Antall transaksjoner er ikke det beste parameteret på folks tillit til Internett, men gir en konkret indikasjon på retningen i utviklingen. Flere handler på nett, og dette gjøres stadig oftere gjennom online-transaksjoner – noe som tyder på at vi blir mer ”modne” for e-handel og de muligheter Internett legger til rette for.

Vi nevnte at selv om tilliten er høy, sier denne svært lite om den faktiske sikkerheten og risikoen som ligger i elektronisk handel og transaksjon. Det som fremkommer er forbrukernes *oppfatning* av trygghet, basert på en subjektiv vurdering av de forhold forbrukerne har mulighet og kapasitet til å ta inn over seg. ”Systemet” som sådant er for komplekst til at enkeltindividet kan tilegne seg full informasjon, for så å gjøre fornuftige og kalkulerte valg. Dermed må de ty til *tillit som verktøy* når valget om å gjennomføre en e-handelstransaksjon skal tas.

Dersom man foretar gjentatte transaksjoner, og alt går slik det forventes, kan faktisk erfaring styrke tilliten til ”systemet”. I denne sammenheng kan systemet innebære Internett, e-handelsbransjen, e-handelsbedriften, lovverk og myndigheter, eller en kombinasjon av disse. Tillit er vanskelig å vurdere fordi forbrukere benytter både *kalkulerende* og *følelsesmessige* avveininger. De kan handle rasjonelt i ett øyeblikk og stole på maveføIelsen i et annet. Det er likevel viktig å skaffe innblikk i hvilke forhold som er *viktigst* for forbrukerne når det gjelder tillit og e-handel.

Tidligere forskning har vist at mange forbrukere i stor grad stoler på bedrifter de kjenner til fra tradisjonell handel når disse tilbyr varer/tjenester over Internett (bl.a. Slettemeås et al 2002). I slike tilfeller er tilliten knyttet til bedriften, og ikke til Internett som handels-, distribusjons- og transaksjonskanal (Teknologirådet 2004). Forbrukerne leser verken personvern-policy’er, leter etter tillitsmerker som Nsafe, eller ser etter om SSL-kryptering er iverksatt. Man stoler på at bedriften ”ordner opp”. Altså ser det ut som om *rykte* og *renommé,* samt det å *ha vært lenge i markedet*, er viktige faktorer for å lykkes på Internett. Dette er i så fall avgjørende når en skal vurdere angrepsvinkel for PKI. Bør PKI introduseres gjennom store, velrenommerte bedrifter (som Norsk Tipping, bankene, etc) for å sikre adopsjon av teknologien og tilhørende tjenester?

Vi nevner i senere kapittel at en annen måte å bygge tillit til PKI på vil være å fokusere på ”systemet” (slik som det elektroniske systemet for betalingskort), uavhengig av de aktører som er involvert i et slikt system. Dermed slipper forbrukerne å bygge bilaterale tillitsrelasjoner til de enkelte bedrifter/ institusjoner.

[17] Handel.no: ”Hindrer misbruk av kredittkort”, 09.05.2003

Et annet moment som er viktig for tilliten til Internett og sikkerhet er venner og bekjentes erfaringer med tjenester. Dette viser en delrapport for den svenske Post- och telestyrelsen[18], og det støttes av funn fra Slettemeås et al (2002). Dermed er tilliten indirekte knyttet til bedriftene, tjenestene og Internett via venner og bekjente. Forbrukerne nevner det også som ekstra trygt dersom slike tjenester står under statlig tilsyn.

Et annet interessant moment er at forbrukere ser ut til å godta en høyere grad av usikkerhet og risiko når *tilbudet er godt nok*. Det uttrykkes gjerne stor skepsis til sikkerheten på Internett generelt sett, mens man likevel foretar transaksjoner over nett så lenge pristilbudet er bra. Her er det et misforhold mellom holdninger og faktisk atferd på makronivå.

Dette er derimot i tråd med deler av tillitslitteraturen (bl.a. Luhmann 1988). Luhmann hevder at tillit krever et tidlig engasjement fra personen selv, og situasjoner der tillit er involvert forutsetter risiko. En kan unngå å ta risikoen, men da unnlater en også de tilhørende fordelene som er implisitte i valget. Risiko fremkommer likevel bare som en del av enkelte avgjørelser eller handlinger. Med andre ord, risiko eksisterer ikke alene. Hvis en avstår fra en handling løper en ingen risiko. Det er en ren *intern* kalkulering av *eksterne* forhold som skaper risiko. Tillit er dermed basert på et sirkulært forhold mellom risiko og handling, der begge er komplementære krav. Risiko er dessuten bare mulig i en situasjon der potensiell skadevirkning er større enn den forventede fordelen.

Dette betyr at risikoen i mange tilfeller oppveies av den potensielle fordelen som situasjonen impliserer. Et godt eksempel kan her være det irske flyselskapet Ryanair. Dette er et selskap som har hatt en eksplosjonsartet vekst de siste årene. Dette på tross av at selskapet stort sett kun opererer på nett, har dårlige tidspunkt for flyavganger, benytter flyplasser utenom de store byene, og har et ubrukelig Internettgrensesnitt. Man må blant annet booke hver enkelt reise for seg dersom turen innebærer mellomlandinger, og bagasjen må sjekkes inn på nytt. Dessuten benyttes flyene mer intenst enn hva som er vanlig i europeisk flytrafikk. Her er det helt klart den lave prisen som får forbrukerne til å nedvurdere/ overse de risikoelement og bekvemmelighetsfaktorer som de ellers vurderer som svært viktige.

Et annet interessant tilfelle, som det ikke er mye litteratur og empiri rundt, er nordmenns bruk av utenlandske spill- og gambling-tjenester på Internett. Det er mulig at nettgamblere er mindre risikoaverse enn ”nordmenn flest”, men disse spillerne foretar transaksjoner over landegrensene, og oppgir personlig informasjon for å kunne spille på slike nettsteder. Ser man på nordmenns holdninger til Internett er denne kategorien tjenester nettopp slike man burde ha ”minst tillit til”: Gambling-selskapene opererer kun på Internett, er basert i utlandet, og krever personlig og transaksjonsnødvendig informasjon. Likevel spilte nordmenn anslagsvis for 1,4 milliarder kroner på utenlandske nettsteder i 2003[19]. Det hevdes også at hele 45% av nettspillerne kun spiller på utenlandske nettsteder.

Skal vi oppsummere tillit og nettbruk er dette et vanskelig fenomen å avsløre med forbrukerundersøkelser. Man kan likevel få et innblikk i hva forbrukere ser på som viktig, hvordan de opptrer i forhold til enkeltselskaper, og hvor de vurderer at ansvar for sikkerhet ligger dersom noe skulle gå galt; hos nettselskapene, hos bransjeorganisasjoner, hos myndigheter og tilsyn, eller hos brukerne selv.

[18] Ref. i Handel.no: ”Tilfreds med dagens betalingsløsninger”, 20.10.2003
[19] Ref. Dagens Næringsliv: ”Klare for norske spillopper”, 14. april 2004, s. 45

3 Funn fra relevante undersøkelser / piloter

I dette kapitlet går vi gjennom ulike pilotstudier og undersøkelser som allerede har vært gjennomført her til lands. Tilgang og tid har medført at bare enkelte studier er referert. Undersøkelsene og analysene varierer i karakter og respondentene baseres på ulike univers av aktører. I enkelte tilfeller er det forbrukere som er respondenter, i andre tilfeller er det offentlig ansatte som svarer i kraft av sin arbeidstakerrolle. Etter en kort gjennomgang av de mest relevante funnene fra disse studiene foretar vi en kort evaluering og vurderer hvordan det kan utledes relevante spørsmål til den senere undersøkelsen.

3.1 Norsk Tipping

Denne studien er basert på en brukerundersøkelse blant Norsk Tippings nettspillere[20] gjennomført våren 2003. Undersøkelsen hadde følgende karakteristika:

- 5000 nettspillere registrert i perioden mai - september 2002
- spørreundersøkelse 11-24 februar 2003
- svarprosent: 10 (N=453)
- utvalg: 90 % menn
- utdannelse: 50% med høyere utdannelse
- hovedtyngde alder: 30-50 år
- PKI-løsning: Smartkort

Det viste seg i denne undersøkelsen at det store flertallet av nettspillerne på forhånd svarte at de hadde ganske eller svært stor tillit til *nettsikkerheten* hos Norsk Tipping. De med videregående og høyere utdanning lå rundt 40% både på "ganske" og "svært" høy tillit, mens nesten 64% av de med grunnskole viste seg å ha svært høy tillit til Norsk Tippings sikkerhetsrutiner før de hadde prøvd ut nettspill-løsningen.

Det bør nevnes her at denne undersøkelsen antakeligvis overestimerer brukernes positive holdninger til sikkerhet og brukervennlighet. Utvalget er ikke representativt for den generelle befolkningen (overvekt av menn og unge spillere med stor interesse for tjenesten). Likevel vil vi referere de viktigste funnene og diskutere disse kort mot slutten av kapitlet.

Jevnt over (uavhengig av utdanning) økte tilliten til Norsk Tippings nettsikkerhet etter at nettspill var blitt tatt i bruk. Andelen med svært høy tillit lå nå rundt 60% for de med videregående og høyere utdanning, mens andelen hadde steget til nesten 75% for spillere med grunnskole. Det må her sies at den "totale tilliten" (både ganske og svært høy tillit) for alle tre utdanningskategorier var nær 95%, noe som er svært høyt.

[20] Norsk Tipping (slidepresentasjon – intern): "Brukerundersøkelse blant Norsk Tippings nettspillere", 2003.

Også når det gjaldt *brukervennlighet* kom Norsk Tippings nettløsning godt ut, der mellom 75 og 80% av de spurte oppfattet løsningen som ganske bra eller svært bra. Det var en noe lavere andel av de med høy utdanning som syntes løsningen var svært brukervennlig jamført med de med lavere utdanning.

På spørsmål om sikkerhet i overføring av informasjon mellom spillere og tippeselskapet ved benyttelse av smartkort, følte igjen en stor andel av brukerne at overføringen var trygg; rundt 78% for de med høyere utdanning, og igjen en noe større andel (ca 88%) for de med grunnskole.

De aller fleste mente Norsk Tippings smartkort kunne benyttes på andre tjenester i tillegg til spilltjenesten. Igjen viste tendensen seg å være at de med lavere utdanning hadde noe mer tiltro til smartkortbruk på andre tjenester (ca. 62% svært enige) enn de med høyere utdanning (ca. 45% svært enige).

Når brukerne ble spurt om hvordan de oppfattet elektronisk legitimasjon og digital signatur i forhold til dagens sikkerhetsregime for nettjenester, viste det seg igjen at de fleste mente det ville være tryggere med et nytt digitalt ID-system for nettjenester (77% for den yngste alderskategorien og 100% for den eldste). For de som var svært enige i påstanden viste denne holdningen seg å stige med alderen for så å synke igjen for de aller eldste. Det er vanskelig å forklare denne tendensen. Ser man derimot på den totale trygghetsholdningen (enig og svært enig i påstanden) kan det tenkes at de yngre er mer fornøyde med, eller har høyere tillit til dagens system, enn det de eldre har, samtidig som eldre generelt sett har vist seg å være mer skeptiske til nettsikkerhet. Dermed kan PKI være en løsning som vil bidra til økt bruk av nettjenester blant middelaldrene og eldre, dersom man vet om og har nytte av tjenesten.

Nærmere 85% av både menn og kvinner mente at elektronisk legitimasjon måtte kunne *benyttes på flere maskiner*. Dermed viser fleksibilitet med hensyn til arbeidsstasjon seg å være et viktig element. Dette kan ha sammenheng med at mange av dagens nettbrukere har PC og Internettilgang både hjemme og på jobb. En fersk undersøkelse fra Nsafe[21] viser at nordmenn liker å handle i arbeidstiden. Her var det bøker som stod i sentrum, men det er ingen grunn til å tro at tendensen er annerledes for andre varer / tjenester. Derfor er det viktig å ha en sikkerhetsløsning som fungerer på jobb så vel som hjemme.

Når deltakerne ble spurt om hvor enige/ uenige de var i påstanden om hvorvidt den elektroniske legitimasjonen *fysisk burde kunne koples fra datamaskinen* etter endt bruk for å hindre misbruk fra andre, var 69% av kvinnene svært enige i dette mens 66% av mennene hadde samme oppfatning. Igjen viser den totale enigheten (enig og svært enig) seg å være rundt 80 - 90% for begge kjønn – altså svært høyt. Det var ubetydelige variasjoner i alder.

I kontrollspørsmålet om hvorvidt man synes dagens sikkerhetssituasjon på internett, mht kredittkortnummer og personopplysninger, er sikker nok, var litt over 30% av kvinnene enige i dette, mens ca. 40% av mennene mente det samme. Andelen som stilte seg nøytrale til spørsmålet var relativ høy – 35% for kvinnene og 25% for mennene. Det er interessant å se at selv om folk mener PKI vil være tryggere enn dagens sikkerhetsmekanismer (mellom 77 og 100%) er det likevel relativt mange som synes dagens situasjon er grei nok. Graden av enighet synker noe med alder – det

[21] Ref. i handel.no 14.05.2004: "Handler i arbeidstiden!"
www.handel.no/modules/module_111/news_item_view.asp?iNewsId=2555&iCategoryId=87&iResponse=3

vil si jo eldre man er jo lavere er tendensen til at man finner dagens netthandel sikker nok (her er det ikke skilt på de som faktisk har handlet og ikke – det kan være en svakhet og dermed gi lav validitet). Dermed blir det relevant å gå i mer detalj på hvilke *tjenester* som eventuelt bør benytte nye PKI-løsninger.

Et interessant funn er at selv om de fleste var interesserte i at Norsk Tippings løsning skulle kunne benyttes på andre tjenester, var det mange som ønsket at *personalia ikke skulle gjenbrukes* gjennom en infrastruktur for elektronisk legitimasjon. Gjenbruk vil lette oppgaven med å fylle inn data / informasjon om den enkelte (demografiske data, psykografiske data og kjøpshistorikk). Hele 75% av de med grunnskole sa nei til gjenbruk, mens ca. 60% av universitetsutdannede sa det samme. Kvinner var noe mer skeptiske til slik gjenbruk (75%) enn det menn var (63%). Dette kan være et hinder for effektiv bruk av PKI over flere bransjer og tjenestegrupper. I en undersøkelse vil det være relevant å identifisere hvordan *gjenbruk* kan tilpasses brukerne, gitt deres behov og bekymringer.

Generelt sett viser Norsk Tipping seg å ha høy tillit i befolkningen. I MMIs profilundersøkelse[22] av store norske bedrifter for 2003, skårer Norsk Tipping nest høyest på folks totalinntrykk. Hele 75% av et landsrepresentativt utvalg av befolkningen sier de har et godt inntrykk av Norsk Tipping. Dette kan påvirke den gjennomgåtte undersøkelsen på flere måter. En effekt kan være at folk har så høy tillit til Norsk Tipping at de lar være å vurdere sikkerhetsaspektet på en kritisk måte. Dermed plasseres hele tillitsbyrden på selskapet og ikke på infrastruktur, regelverk eller annet. Hvis man tolker generelt fra tallene i denne undersøkelsen kan man ende opp med å overestimere folks tillit og behov for PKI, fordi man er positivt innstilt til bedriften og bedriftens tjenester i utgangspunktet. Dessuten er spillerne menn, og relativt ”avanserte” nettbrukere, som muligens er mindre skeptiske til nye teknologiske muligheter.

Et annet interessant ”funn” i undersøkelsen er at dersom forbrukere har høy initiell tillit til en bedrift eller institusjon kan det tyde på at dette er et svært gunstig utgangspunkt for lansering av PKI-tjenester og tilhørende infrastruktur. Ettersom folk benytter tillit som verktøy til å redusere kompleksitet og usikkerhet (Luhmann 1999), kan det fremstå som om folk ikke er så opptatte av andre faktorer, slik som tiltrodde tredjeparter (TTP’er), sikkerhetsinfrastruktur, personvern-policy’er etc. Dermed bør fokus ligge på å markedsføre *nytten* av signatur- og identifikasjonstjenestene fremfor teknologien og aktørrelasjonene som ligger bak.

En annen observasjon er at det er vanskelig å si seg uenig i mange av påstandene i denne undersøkelsen. Det er naturlig å være enig i det meste, dersom dette ikke settes opp mot f.eks betalingsvillighet. Dessuten vil faktisk bruk avhenge av mange faktorer (innhold, kostnad, interesse, viktigheten av sikkerhet i det enkelte tilfelle, etc.)

Et annet viktig forhold er at Norsk Tippings smartkort i en tidlig fase (pilotfasen) ble tildelt gratis til testbrukerne. Dermed er det noe vanskelig å foreta en vurdering av undersøkelsen på generelt grunnlag. Brukerne av løsningen betaler i dag 79,- i årsavgift. I Oppdal Kommune er det Norsk Tipping som leverer smartkortløsningen, som i tillegg kan benyttes til andre tjenester, og sluttbrukerpakken har her samme årspris (se kapittel 3.5). Det er foreløpig ikke foretatt brukerevalueringer rundt disse tjenestene fra kommunens side. Dersom en reell landsomfattende utrulling av PKI innebærer ulike betalingsmodeller, vil disse med stor sannsynlighet gi utslag på folks adopsjon og bruk av tilhørende tjenester.

[22] MMI undersøkelse referert i Aftenposten, 2. september 2003: s.11. De spurte utgjør et representativt utvalg på 856 personer og de har vurdert 115 av landets største bedrifter i perioden 19. – 27. mai

I en tidligere intern undersøkelse fra 2002[23] gjorde Norsk Tipping seg visse erfaringer med brukernes syn på nettløsningen og bruken av Smartkort. Her viste det seg at enkelte syntes at dette var "tungvint". Brukervennligheten var ikke helt god, installasjonen var noe vanskelig og en måtte bruke koder flere ganger i prosessen. Det viste seg også at brukerne ikke var så opptatt av sikkerhet, dersom de ikke konkret hadde opplevd negative hendelser. Mangel på sikkerhetsvurdering her støtter opp om tesen om at brukerne stoler fullt og fast på at Norsk Tipping "ordner opp" dersom noe skulle gå galt. Et annet forhold var at mange mente at Norsk Tipping var "eier" av løsningen og at den derfor ikke kunne benyttes til andre ting/tjenester. I denne situasjonen er det også Buypass (som står for sertifikatet) som har kundekontakt med brukeren. Her kan det oppstå vanskeligheter ettersom forbrukere ikke "ønsker å se" tredjepartsleverandører, men forholder seg til tjenestetilbyderen. Det er gjerne her tilliten bygges.

3.1.1 Bachelor-oppgave om digitale signaturer

I Bachelor-oppgaven "Digitale Signaturer – og standardiserte løsninger" åpner Aune og Rosvold med at forbrukerne i dag må forholde seg til flere løsninger (sikkerhetsløsninger) på forskjellige tjenester, mens den ideelle løsningen vil være å ha *ett passord som gjelder for alle tjenester.* Her har forfatterne allerede tatt standpunkt til brukernes interesser uten først å redegjøre for en konkret problemstilling hvor dette spørsmålet er innbakt.

Deretter går forfatterne gjennom et sett av brukerorienterte problemstillinger som danner utgangspunktet for oppgaven. Disse er (Aune og Rosvold 2003: 11):

- Vil teknisk standardisering av digitale signaturer gi økt brukevennlighet?
- Vil én løsning gi mange muligheter?
- Vil én løsning redusere skepsisen til bruk av digitale signaturer? (eller til tjenestebruk mer konkret?)

I den kvantitative delen av undersøkelsen settes avhengig variabel "holdning" (positiv eller negativ til e-ID) opp mot en rekke bakgrunnsvariabler. Dette gjøres i forsøk på avdekke hva slags type forbrukere som er mest / minst positive til e-ID. Utover dette gir funnene lite innsikt i faktisk eller potensiell bruk av PKI, relevante tjenestealternativer, kritiske faktorer for å ta i bruk PKI, etc.

I den kvalitative delen av oppgaven (Aune og Risvold 2003: 90-96) er funnene basert på intervjuer med relevante fagpersoner. Dette gir innsikt i viktige aspekter sett fra aktørenes side, men belyser dermed ikke konkrete brukererfaringer eller brukerholdninger. Dette erkjennes også i oppgaven.

I et av sitatene fokuseres det på behovet for å se digitale signaturer fra brukernes ståsted og at en ikke kun må tenke teknisk utvikling og salg. En annen forutsetning for suksess som vektlegges er at det må tilbys tjenester som folk har bruk for. Her er utfordringen å få bedrifter på banen slik at disse ser hvilke muligheter som ligger i en slik samordnet infrastruktur. Det må her tilføyes at bedrifter og bransjer ikke må overtales (les: overkjøres) for en hver pris – infrastrukturen må stå i forhold til hvilke tjenester som tilbys og de sikkerhetskrav som påfølger, samt bruksfrekvens. Altså, volumet av potensielle tjenester må økes ettersom (antakeligvis) ingen vil kjøpe elektronisk signatur *per se* – e-signaturen må kunne brukes til noe konkret. Her er det na-

[23] Referert på PKI Forbrukergruppas møte 28.11.2002

turlig å stille seg spørsmålet om forbrukere opplever at én kritisk tjeneste blir inngangsporten til bruk av PKI også i andre sammenhenger – og til andre tjenester?

En annen utfordring for digital signatur er hypotesen om at folk må ha *tillit* til de tjenestene som tilbys for å ta i bruk tjenester med digital signering (ref. kapittel 2.4). Det hevdes at høna og egget-problematikken ikke eksisterer på dette problemfeltet fordi e-ID ikke kan selges til brukere uten relevante tjenester. Derfor virker det igjen naturlig for en eventuell forbrukerundersøkelse å se hva som kan være relevante tjenester, og rasjonalet bak valget av tjenester som har PKI tilknyttet (hverdagsliv og kontekst).

Intervjuobjektene i oppgaven mener at *kjente navn, varemerker* og *aktører* er viktige tillitsfaktorer. Tjenestene må samtidig *fungere* og *være nyttige* for brukeren. Det nevnes også som en fordel at myndighetene setter *stempel* på slike tjenester. Tenker vi forbrukerundersøkelse igjen, virker det her naturlig å spørre videre om behovet og grad av involvering fra myndighetenes side (garanti, samordning, hands-off, overordnet ansvar, etc).

En respondent fra en bedrift som benytter smartkortløsning (ibid: 93) hevdet at ideen om å *gjenbruke* digitale ID'er er god, men at man dermed blir mer avhengig av at denne fungerer til enhver tid (og har høyeste sikkerhetsgrad). Respondenten nevner at det nok er lurt å spre risikoen litt slik at man ikke låses til én måte å identifisere seg på, dersom det skulle oppstå feil ved løsningen.

Andre intervjuobjekter som ble konfrontert med denne uttalelsen var likevel enige om at det burde foreligge mulighet for kun én ID, men med muligheter for å velge flere ID'er dersom brukeren skulle ønske dette – nettopp for å spre risikoen ved potensielle feil. Andre faktorer som virker relevante i forbrukersammenheng er at med én ID og én pinkode er man "åpen helt inn" dersom noen skulle få tak i koden. Som det beskrives i kapittel 4.3.3 om forbrukerbeskyttelse så er ikke sikkerhetskjeden sterkere enn det svakeste leddet – og dette er ofte forbrukeren. Samtidig vil en ID som til en hver tid har den strengeste sikkerhetsgraden ofte ha lavere brukervennlighet.

En mulighet som ble fremmet er en slags "hoved-ID" der de fleste tjenestene kan samles. Samtidig kan vi spørre oss: hva med utenlandske tjenester? I dag er det mange forbrukere som handler varer/ tjenester eller spiller på utenlandske nettsteder. Dermed forsvinner noe av effekten ved kun å ha en "hjemlig" e-ID. På den annen side virker det uansett fornuftig å "lære seg" funksjoner inntil en felles internasjonal standard dukker opp.

Et intervjuobjekt hevder at *duplikatløsninger* er viktig – det å f.eks ha samme løsning i et smartkort og på en mobiltelefon. I en brukerundersøkelse kan vi bygge videre på dette og spørre hva slags type løsning som fenger mest, eventuelt hva som passer i ulike situasjoner (f.eks soft-sertifikat vs. smartkort vs. mobil-PKI).

Det var relativt enighet om at *en felles standard* vil være nødvendig for at tilbudet av tjenester skal yngle, for så å appellere til brukere. Dermed vil etterspørselen etter tjenester øke, og slik sett etterspørselen etter e-ID. Dette avhenger selvsagt av *bevisstheten hos forbrukerne* om at en slik standard finnes og at man nå kan hoppe ned fra gjerdet. I kapittel 4 trekker vi veksler på erfaringer fra utrullingen av elektronisk betalingsformidling på 90-tallet som en viktig parallell til en forestående PKI-utrulling. Erfaringen her peker på viktigheten av å få forbrukerne involvert i et relativt gjennomsiktig, forenklet regime.

3.2 BankID

Bank-ID er et samarbeid mellom norske banker som ønsker å utstede e-legitimasjon for identifisering og signering på internett[24]. I selve BankID-sertifikatet benyttes en kombinasjon av fødselsnummer og passord, mens det for identifisering i tillegg kreves en sikkerhetskode. Målet med BankID-samarbeidet er i henhold til Grethe Sørensen[25] at kundene skal kunne benytte BankID-sertifikatet ved mange brukersteder som f.eks nettbanker, nettbutikker og offentlige tjenester. Dermed trenger man kun ett brukernavn og ett passord for tilgang til tjenester fra flere tilbydere. BankID-samarbeidet har også hatt en målsetning om å lære opp kunden i bruk av elektronisk legitimasjon og signatur via nettbankene.

BankIDs tall viser at det i 2002 var hele 1.65 millioner nettbank-kunder her i landet. Av disse benyttet 67% seg av nettbanken hver uke. Fordelen med at bankene drar noe av lasset her er at banktjenester brukes ofte – og kundene har allerede tillit til bankene. Dette er påstander fra banknæringen, men det er kjent i ulike forskningsresultater at forbrukere generelt sett har høy tillit til banken sin, selv om mange er misfornøyde (og passive) med hensyn til tjenester, gebyrer og renter (Berg og Borgeraas 2004). Bankene er kjent for sikkerhet, selv med visse barnesykdommer i begynnelsen av nettbank-perioden, og bankene er fokusert på transaksjonstjenester og er dermed helt avhengige av en høy grad av sikkerhet. Dette er forbrukerne klar over.

Her er det interessant å se på utviklingen i Danmark. Der ønsket man å lansere digital signatur ved at borgerne kunne bestille en personlig signatur til selvangivelsen fra Told og Skattestyrelsen[26]. Denne skulle også kunne brukes til offentlige søknader og kommersielle kontrakter. Like etter at dette kom ut i mediene fremkom det at signaturen ikke tilfredsstilte EUs krav til sikkerhet for digitale signaturer. De danske bankene ønsket dermed ikke å samarbeide med TDC, som hadde ansvaret for utrullingen. En av grunnene til bankenes misnøye var at det ikke krevdes *personlig kontakt* ved utdelingen av e-underskriften[27]. Det må nevnes at de danske bankene allerede benyttet seg av en tidlig versjon av e-signatur for landets 1,6 millioner bankkunder. Dette kan ha styrket bankenes motvilje mot en slik fellesløsning, sett i et kostnadsstrategisk perspektiv (se bl.a. Jacobsen 1992).

Bankenes mål er å legge til rette for allmenn bruk av sertifikater allerede før eNorges 2005-målsetning. Man ønsker også ”gjenbruk” av BankID-løsningen i elektroniske tjenester fra offentlig og privat sektor. Vi så av undersøkelsen med Norsk Tippings kunder at selv om de fleste var interessert i at en slik løsning skulle kunne benyttes på andre tjenester, var det mange som ikke ønsket gjenbruk av personalia gjennom en infrastruktur for elektronisk legitimasjon. Dette er et viktig moment å ta hensyn til før en større utrulling finner sted. Det kan tenkes at brukere tror at all demografisk og sikkerhetsinformasjon vil deles med kommersielle 3.parter, mens de selv ikke ønsker at dette skal forekomme. En måte å takle dette på er å klargjøre for forbrukerne hva slags informasjon som ligger i sertifikatene og hva slags informasjon som deles mellom partene.

Målsetningen for BankID-samarbeidet for 2004 er 500 000 brukere og minst 100 BankID-brukersteder, samt minst 20 nettbanker og finansportaler. Status i mars

[24] BankID Samarbeidets felles strategi for utbredelse av BankID 2004 v/ Grethe Sørensen, koordinator BankID Samarbeidet – PKI-forums plenumsmøte 04.03.04
[25] Ibid.
[26] Ref. i Digi.no 07.02.2003: ”Dansk, digital signatur via selvangivelsen”. www.digi.no/php/art.php?id=69937
[27] Ref. i Digi.no 12.07.2003: ”Digital dansk signatur kan bli en fiasko”. www.digi.no/php/art.php?id=85321

2004 er 30 brukersteder og 6 nettbanker. BankID-samarbeidet har også koplet seg mot kommuner som Fosen, Numedal og DDT[28].

Av konkrete erfaringer fra pilotene som er gjennomført hevdes det at BankID-løsningen er enkel å bruke for kundene, selv om infrastrukturen er teknisk kompleks og flere leverandører må samspille. Et annet moment er at kundene ser ut til å foretrekke banklagret fremfor lokallagret BankID[29]. BankID-satsingen vil foreløpig vente med smartkort. I sammenheng med vår forbrukervinkling på PKI-utrulling vil det være interessant å se på forbrukernes forhold til *type* e-ID (softsertifikat, nettsentrisk, smartkort, SIM-kort i mobiltelefon, etc). Ønsker forbrukerne å ha en "fysisk" eID som de kan ta å føle på, eller er type eID og nøkkelbærer irrelevant? Vi vil se nærmere på dette momentet mot slutten av rapporten.

BankID-samarbeidet beskriver egne sikkerhetstjenester slik:

- *Identifisering* – bruker BankID som elektronisk legitimasjon for betaling fra nettkonto eller for å logge seg på et nettsted.
- *Signering* – bruker BankID til å lage personlig elektronisk underskrift, f.eks ved avtaleinngåelse med et Bank-ID brukersted (netthandel).
- Brukere får også *oversikt* over alle signerte dokumenter og systemet lar brukeren verifisere signaturer etter lagring og arkivering.

Det er tenkt at et BankID-brukersted inngår avtale med sin bank. Man skal slippe å forholde seg til hvorvidt brukerne har banklagret eller lokallagret BankID, eller hvilken bank som har utstedt brukerens BankID. Dermed gir brukerstedsløsningen tilgang til alle utstedte BankID'er og gir rom for nye tjenester. Her er det tenkt på følgende tjenester, som også kan være et utgangspunkt for et spørsmålsbatteri om tjenester folk kan tenke seg i den senere forbrukerundersøkelsen:

- nye betalingsformer
- rettidig pengeinnkreving
- fortolling og omregistrering
- innrapportering til offentlig sektor
- låneprosesser
- søknadsbehandling
- avtaleinngåelse
- elektroniske valg
- multisignatur-løsninger
- digital kvittering
- forsikring
- annet

3.3 Lånekassen

Lånekassen gjennomførte en forstudie høsten 2001[30] og gjennomførte et forprosjekt i 2002. Dette ble etterfulgt av et pilotprosjekt høsten 2002 (samarbeid med AltINN fra desember 2002). Denne piloten ble evaluert våren 2004. Lånekassen var dermed den første statlige etat som tok i bruk en fullelektronisk løsning med bruk av PKI[31].

[28] DDT = Det Digitale Trøndelag
[29] Ref. BankID Samarbeidets felles strategi for utbredelse av BankID 2004 v/ Grethe Sørensen, koordinator BankID Samarbeidet – PKI-forums plenumsmøte 04.03.04
[30] Presentasjon fra Lånekassen – PKI-forums plenumsmøte 04.03.04
[31] Lankassen.no: "Lånekassen tar i bruk digital signatur", 7. januar 2004

Målsetningen med piloten var å utvikle en sikker måte å håndtere *konto-til-konto overføring* av lån/stipend. Underskriften for kundens/ studentens gjeldsforpliktelse skulle dessuten være *juridisk holdbar***.** Det avgjørende momentet var dermed å legge til rette for *sikker identifisering* av mottaker og kontroll av at studentene faktisk var tatt opp ved de respektive studier det var søkt om, og at de hadde påbegynt utdanningen.

Løsningen skulle dessuten gi *bedre kundeservice* og være vesentlig *rimeligere* enn det dagens situasjon tillater, og heller ikke medføre merarbeid for lærestedene. Målsetningen for Lånekassen er videre at flest mulig skal signere gjeldsbrevet elektronisk i fremtiden. Dermed slipper studentene å stå i kø på lærestedet ved semesterstart, og man slipper også køen ved bank eller postkontor.

Lånekassens krav til elektronisk løsning:

- Vite hvem avsender er (identifisering, autentisering)
- Oppdage endringer
- Hindre innsyn (kryptering)
- Knytte innhold til avsender (ikke-benekting)
- Elektronisk underskrift
- Lagring

PKI dekker disse kravene og sikkerhetsnivået må være høyt. Lånekassen ser for seg en løsning der *smartkort* skal ta seg av den elektronisk signaturen.

Fremgangsmåten for brukerne er slik at studenten søker lån og stipend → vedtak fattes i Lånekassen → semesteravgiften betales → e-post sendes til studenten, som går inn på AltINN-portalen og identifiserer seg med smartkortet. Her åpnes skjema med vedtak, låneavtale og gjeldsbrev. Skjemaet signeres og etter kort tid utbetales pengene direkte til studentens konto.

I dag kan studenten gjøre alt elektronisk bortsett fra siste fase – å få pengene overført til konto. Her må man fysisk møte på Lånekassens studentkontor og signere for mottak, og deretter gå i nærmeste bank for å sette inn pengene.

I dagens samfunn, der mange (spesielt unge og studenter) benytter nettbank, er dette en tungvint og tidkrevende måte å løse oppgaven på, fordi man ofte ikke har filialer i nærheten. Alternativet er Postbanken (som eies av DNB). Her må man betale et høyt gebyr for å overføre penger til egen konto, dersom man ikke er DNB eller Postbanken-kunde. I tillegg kan det være ekstra irriterende å ikke få gjennomført siste fase i prosessen ettersom resten av søknadsfasen er tilgjengelig elektronisk.

Dette fremstår dessuten som en fin inngangsport til bruk av PKI ettersom så å si alle studenter søker lån ved norske høyskoler og universiteter. Dermed kan unge borgere i en tidlig fase se hvilken nytte PKI og smartkort kan gi, dersom dette blir det endelige valget. Frekvensen for bruk er derimot lav; 1-2 ganger i året.

I et prøveprosjekt ved Høgskolen i Lillehammer (gjennomført sammen med Statskonsult) ble elektronisk signering av gjeldsbrev for studielån gjennomført og evaluert for Lånekassen[32] (2003/2004). Her ble det gjennomført to kvantitative undersøkelser, én før og én etter signering av gjeldsbrevet, samt to fokusgruppeintervjuer av henholdsvis deltakere og ikke-deltakere i prosjektet. 271 personer fikk kort for signering og 250 personer signerte elektronisk i prøveprosjektet.

[32] Statskonsult og Lånekassen; ”Evaluering av PKI-pilot ved Høgskolen i Lillehammer”. (Offentlig)

Studentene som deltok i prøveprosjektet var erfarne studenter, det vil si studenter som tidligere hadde mottatt lån og stipend. I evalueringen kom det frem at de aller fleste mente elektronisk signering av gjeldsbrev var en enkel måte å få utbetalt lån på. En del av studentene mente dessuten at selve prosjektet var spennende og at de var lei av å stå i kø for å signere gjeldsbrev og hente lån. Det var derimot få som var opptatt av sikkerhet i evalueringen av prosjektet.

I tillegg til konkrete erfaringer med PKI'en ble det lagt vekt på *informasjonsfaktoren* i Lånekasseprosjektet. Det fremkom at e-post var desidert den viktigste informasjonskanalen for informasjon relatert til prosjektet. Deretter kom Internett og *Classfronter,* mens plakater og SMS var lite brukt i denne forbindelse. Erfaringer fra prøveprosjektet har resultert i en anbefaling om at Lånekassen skiller på ulike typer av informasjon til studentene:

- **hvorfor PKI**-informasjon
- **hva er PKI**-informasjon
- **hvordan gå fram**-informasjon

Avrundingsvis viste det seg at det var sterk motstand mot å betale for smartkort i forbindelse med signering av gjeldsbrev. Hele 3 av 4 studenter var i mot å øke semesteravgiften på grunn av smartkortet. Motstanden kan eksemplifiseres gjennom følgende sitat fra ett av fokusgruppeintervjuene:

> "Denne løsningen er det Lånekassa som tjener mest på. Da må de ta kostnadene."

3.4 Offentlig sektor

I denne undersøkelsen[33] har målgruppen vært "alle" offentlige virksomheter (ca. 900 totalt), og rekruttering til undersøkelsen foregikk ved utsendelse av e-post til postmottak i ulike virksomheter, rettet til ansvarlig for IKT-strategi. Spørsmålene kunne besvares over Internett. Rundt 310 foretak svarte på undersøkelsen og halvparten av disse var kommuner. Nedenfor deles svarene inn tematisk og beskrives deretter:

Kjennskap til PKI:
Hovedspørsmålene er knyttet til kjennskap til begrepene elektronisk ID og signatur, og begrepet PKI. Her skiller helseforetakene seg ut ved å ha svært god kjennskap til disse begrepene. Likevel er det få foretak totalt sett (ca. 9 av 310) i denne kategorien. Også når det gjelder kompetansen på bruk av denne teknologien i de respektive virksomheter er det helseforetakene som skiller seg ut med høyere grad av (egenvurdert) kompetanse.

Tilbud av elektroniske tjenester:
Når det ble spurt om på hvilke områder virksomheten hadde tatt i bruk elektroniske tjenester på tvers av virksomheter (elektronisk saksgang mot andre offentlige virksomheter, tjenester mot publikum som involverer systemer i flere etater, eller sikker e-post mellom virksomheter), skilte helseforetakene seg ut igjen. Her hadde 70% (av totalt 10 foretak) tatt i bruk "utadrettede" tjenester, mens 31% i statlig forvaltning hadde gjort det samme (totalt 78 foretak). Blant øvrig statlig forretningsdrift/ stiftelser var prosentandelen 20 (totalt 44 foretak), mens prosentandelen kun var 10 for kommuner og fylkeskommuner (av totalt 172).

[33] eNorge 2005 – Undersøkelse om bruk av elektronisk ID og signatur i offentlig sektor (TNS Gallup februar 2004)

Identifikasjon:
Når det gjaldt sikkerhetsmekanismer for å identifisere brukere var det ca. 30% av de deltakende offentlige foretakene som ikke hadde noen form for sikker løsning, mens hele 50% av helseforetakene manglet det samme. Samtidig svarte 40% av helseforetakene at de benyttet seg av enkel pålogging med passord. For de andre foretakene var snittet her ca 10%. Når det senere ble spurt hvorvidt foretakene benyttet avansert pålogging var ja-svarprosenten svært høy – rundt 80% for de fleste foretak bortsett fra kommuner som lå nærmere 50%. Når det til slutt ble spurt om bruk av PKI var også ja-svarprosenten relativt høy – 70% for helseforetak, 50% for øvrig statlig forretningsdrift, 42% for statlig forvaltning og 26% for kommuner / fylkeskommuner. Dette betyr nok at virksomhetene benytter seg av flere sikkerhetsmekanismer avhengig av tjeneste og krav til sikkerhetsnivå.

Nye tjenester:
Når det ble stilt spørsmål rundt konkrete planer for innføring av nye elektroniske tjenester i virksomhetene de neste ett til to år, var det få som hadde planer om enkle tjenester. Vi kan her anta at slike tjenester i stor grad eksisterer hos virksomhetene. For tjenester som er integrert med interne systemer derimot, hadde 64% av virksomhetene konkrete planer (relativt jevnt fordelt over typer offentlige foretak), mens for tjenester på tvers av virksomheter hadde 37% av virksomhetene konkrete planer.

Når det gjaldt tjenester på tvers av virksomheter og mot publikum hadde alle helseforetakene (100%) konkrete planer, mens snittet for resten lå rundt 35%. Når det ble spurt om type sikkerhetsordninger tilknyttet de nye tjenestene hadde 60% av foretakene planlagt å benytte avansert pålogging, 23% ingen løsning overhodet, 17% PKI og 15% enkel pålogging. Det må her presiseres at dette gjelder for tjenestene samlet sett, ikke kun de avanserte. Det er helseforetakene som i størst grad ønsker å benytte PKI til sine nye tjenestetilbud. Vi har tidligere sett at det også er disse foretakene som i utstrakt grad ønsker å ta i bruk avanserte tjenester på tvers av virksomheter og mot publikum. I tillegg opererer man ofte med sensitive data i disse foretakene. Dermed virker det naturlig at disse vil ha noe større behov for PKI eller liknende sikkerhetsmekanismer relativt til andre offentlige instanser.

Relevante problemstillinger i nye tjenester:
Respondentene i undersøkelsen ble bedt om å rangere de ulike problemstillingene som de nye elektronske tjenestene aktualiserer. Alle de grupperte foretakene satte ”beskyttelse av sensitive data/ personopplysninger ved overføring mellom virksomheter eller personer” som den desidert viktigste problemstillingen å ta hensyn til. Denne prioriteringen var soleklar hos alle grupperingene. Den nest viktigste problemstillingen viste seg å være ”kontroll med tilgang til interne systemer”. Deretter kom ”sikker identifikasjon av avsender av meldinger”, mens ”juridisk gyldige signaturer på elektroniske dokumenter” lå lavest på prioriteringslisten.

Vi kan tolke det dit hen at beskyttelse av sensitive data ligger i bunn for den elektroniske tjenestes virke og funksjon. Uten en slik beskyttelse nytter det ikke med sikker identifikasjon og juridisk bindende signaturer. Samtidig kan det tenkes at det kun er få tjenester, eller kun siste fase i et tjenesteforløp, som krever identifikasjon og signatur. Dermed er behovet mht frekvens lavere for disse ”sikkerhetstjenestene”, selv om kravet til sikkerhet når ID og signatur benyttes er høy.

PKI aktuell sikkerhetsmekanisme?
På spørsmål om elektronisk ID (PKI) har vært aktuell som sikkerhetsmekanisme for noen av virksomhetens IKT-systemer, sa hele 38% at dette ikke hadde vært vurdert brukt, mens 43% hevdet at dette var under vurdering. 7% av de spurte sa at e-ID var

besluttet brukt på en eller flere planlagte tjenester eller var i bruk i dag, mens like mange hevdet at elektronisk signatur var besluttet brukt som alternativ til vanlig signatur i en eller flere tjenester.

Egen kompetanse:
Når det gjaldt vurdering av egen (virksomhetens) kompetanse mht e-ID og e-signatur, følte rundt 40% av de IT-ansvarlige i foretakene at denne kompetansen var god nok. I kommuner og fylkeskommuner var den oppfattede modenheten noe lavere; kun 15% mente kompetansen på området var tilstrekkelig. Helseforetakene var de som i størst grad mente de var modne nok til å ta i bruk e-ID og e-signatur (70%), mens 30-40% av de andre foretakene mente det samme.

Tilstrekkelig uten PKI?
Når respondentene ble spurt om *alle* nyttige tjenester innen de respektive virksomheter kunne la seg realisere uten elektronisk ID, var rundt 24% enige i påstanden, mens nærmere 60% var uenige (16% usikre). Dermed mener en fjerdedel av de spurte at PKI (per i dag) ikke er nødvendig.

PKI forums oppgaver:
Det ble informert om at koordineringsorganet for PKI skal legge til rette for bruken av elektronisk ID i offentlig forvaltning. Foretakene ble spurt om å rangere tre av de antatt viktigste oppgavene til et slikt organ. Her var hele 95% enige om at samarbeid om løsninger og standarder var organets viktigste oppgave. Deretter kom samarbeid om felles elektronisk ID på tvers av tjenester med 62%. Identifisering av eventuelle hindringer for å ta i bruk e-ID var den tredje viktigste oppgaven, med 29% enige i påstanden.

Hvis vi skal vurdere nytten av denne undersøkelsen i et forbrukerperspektiv, er den noe mindre relevant enn de andre undersøkelsene. Dette fordi respondentene er såkalte ”eksperter” på feltet, selv om kompetansen rundt PKI er svært sprikende. Det kan antas at den jevne forbruker har langt lavere kompetanse på feltet enn det respondentene her har.

Likevel kan det være interessant i en forbrukerundersøkelse å tilnærme seg noen av de samme problemstillingene. Spesielt gjelder dette kjennskapen til begrepene e-signatur, e-legitimasjon og PKI. Det kan antas at få vet hva det sistnevnte begrepet innebærer, mens en større andel vil resonnere seg frem til en definisjon av de to første, med utgangspunkt i et ”analogt begrepsapparat”. Poenget er å få frem et entydig begrep, som i det videre kan kommuniseres / markedsføres til forbrukerne over lenger tid, slik at disse får et forhold til hva dette er og de mulighetene som ligger i en slik løsning. Dette poenget ble også understreket i kapittel 1.1.

3.5 Kommuner

Det er i dag flere kommuner som er i gang med, eller har vært igjennom piloteringer, av ulike PKI-løsninger. Norges fremste ”digitaliserte” kommune, Oppdal, er intet unntak her[34]. Kommunen har vært gjennom flere forsøk og har prøvd ut løsninger på ulike bruksområder. Målet har vært å få til løsning(er) som flest mulig innbyggere er komfortable med og som senker brukerterskelen til et akseptabelt nivå.

[34] Se www.oppdal.kommune.no

Den løsningen man nå står med er Norsk Tippings smartkort-løsning. Det betyr at Norsk Tipping står for utstedelse og produksjon av smartkort, og bedriften tilbyr også en sluttbrukerpakke (smartkort, smartkortleser og installasjons-CD) til 79,- per år. Målet er å tilrettelegge for bruk av så mange kommunale tjenester som mulig. Buypass leverer selve tjenestene for sikker identifisering og signering, mens ZebSign utsteder den elektroniske ID'en som lagres i smartkortet.

På kommunens nettsider, som er rettet mot kommunens innbyggere, bedrifter og hytteeiere, lanseres ulike tjenester som smartkortet kan brukes til. Disse er som følger (per mai 2004):

- Elektronisk innsending og signering av utvalgte søknader til kommunen
- Kjøp og betaling av billetter hos Billettservice.no
- Bruk av Norsk Tippings spilltjenester på nett
- Sende sikker og sporbar e-post (e-kurér)
- Betaling i kantinen og PC-pålogging for kommuneansatte
- Smartkort som lånekort på biblioteket i Oppdal
- Bestilling og betaling over nett for Postens adresseendringstjenester

Kommunen har foreløpig ikke foretatt noen brukeranalyse i etterkant, men det er også et tidlig stadium for denne type løsning. Det man likevel hadde håpet på i en tidlig fase var å få smartkortet lansert som "pass" innenfor Schengen-området. Etter terrorsanslagene 11. september 2001 ble sikkerhetsvilkårene revurdert globalt – også i EU. Dermed er det fremdeles knyttet usikkerhet til hvilket sikkerhetsnivå som skal gjelde for denne type kort.

En positiv erfaring som ble gjort i Oppdal kommune var gjennomføringen av lokalvalg i 2003. Nær 30% av innbyggerne stemte elektronisk og det var kø i sentrum for å prøve ordningen. Man har tro på enda større oppslutning i fremtiden dersom valgloven endres, og innbyggerne kan stemme hjemme i stuen heller enn i valglokalene. En annen erfaring er at informasjonsspredning er en kritisk faktor for å få folk engasjert og oppmerksomme på de muligheter som ligger i en PKI. I Oppdal har det vært annonsert i lokalpressen, gjennom brosjyrer og via stands på det lokale kjøpesenteret.

For at kommunen skal fungere til det beste for kommunens innbyggere må de som ikke har tilgang på PC kunne benytte publikumsterminaler som er lette å bruke for de med lav eller ingen grunnkompetanse innen PC-bruk.

En hypotese som er relevant for forbrukerundersøkelsen er hvorvidt lokale initiativ har større slagkraft og kan gjennomføres over kortere tid enn det nasjonale initiativ kan. Det kan tenkes at en lokal satsing fra kommunens side, sammen med utvalgte og tiltrodde bedrifter, kan gi en rask kritisk masse av brukere, dersom tjenestene er interessante nok for innbyggerne. For mer erfaringsmateriale fra kommuner, se blant annet Høykom-rapport 406 om erfaringer med PKI[35].

[35] Høykom-rapport 406: "Digital signatur/PKI – erfaringer og løsninger fra Høykomprosjekter", september 2004
http://www.hoykom.net/hoykom/web_hoykom_prosjekter.nsf/a1b9d00d779649e9c1256d7b0033f036/0ae47f04843ffc0cc1256e92002f6ed6/$FILE/Rapport%20406%20Erfaringer%20med%20PKI.pdf

4 Utbredelsen av bankkort i Norge

4.1 Bakgrunn og kopling til PKI-utviklingen

I løpet av 1980-årene ble et høyt antall betalingskort introdusert i det norske og det europeiske markedet. Den faktiske bruken lå noe etter selve utbredelsen av systemene på dette tidspunktet, men den var likevel formidabel. I første del av 90-tallet var norske forbrukere i besittelse av 2-3 millioner kort som kunne benyttes i minibanker og betalingsterminaler i butikker. I og med denne veksten i bruk av elektroniske betalingskort er det interessant å se forbrukernes posisjon og påvirkning på denne betalingsformen og på forhold knyttet til systemene (Jacobsen 1990).

For den enkelte forbruker[36] innebar elektronisk formidling av penger ofte store beløp, og dermed var sikkerhet et meget viktig aspekt i forbrukersammenheng. Kunne man stole på at disse systemene håndterte transaksjoner på en sikker og stabil måte? Og hvilken nytte kunne disse systemene gi som tidligere systemer manglet? Dette er problemstillinger som i høyeste grad er relevante for en fremtidig PKI-utrulling. Vi ønsker derfor å se nærmere på forhold knyttet til elektronisk betalingsformidling som en parallell til PKI-utviklingen.

Når det gjelder forbrukernytte ved introduksjon av plastkort for transaksjon mener Mitchell (1988) at det fra forbrukernes synsvinkel vil være flere fordeler sammenliknet med kontantoppgjør eller bruk av sjekk. Fordelen med det elektroniske systemet er at denne måten er rask (effektivitet), man slipper å bære med seg store kontantbeløp (sikkerhet), man kan sjekke saldo (oversikt, kontroll), og man kan ta ut penger i butikker (tilgjengelighet). Dermed har Mitchell identifisert en rekke merverdier som synliggjøres for forbrukeren ved introduksjon av elektronisk betaling.

Av negative aspekter hevder Mitchell at spesielt debetbetaling innebærer tap av renteinntekter som påløper i perioden fra betaling initieres til konto er ferdig avregnet (tap av *float*). Dette fordi kontoen belastes for kjøpssummen umiddelbart etter handelen. Et annet punkt er at systemfeil og manglende dekning kan medføre at betalingskortet ikke aksepteres. Dette kan oppleves som pinlig og stressende for forbrukeren, spesielt dersom det er andre kunder tilstede. Et tredje moment er at systemet legger igjen elektroniske spor, noe som kan øke trusselen mot personvernet. Fra 1988 og frem til i dag har trusselbildet endret seg på mange måter. Kopling av data

[36] Når man skal vurdere forbrukeratferd er det viktig å foreta avgrensinger for å kunne forholde seg til aktørgruppen på en enklere måte. Det er vanlig både i økonomisk og i sosiologisk teori å se forbrukeren som en rasjonell aktør, som er opplyst og informert, og som følger en viss egeninteresse. Jacobsen (1990:2) velger å se forbrukeren som moderat rasjonell – en aktør som søker alternativer som er ”bra nok” og ikke alltid ”de beste”, slik man ofte forutsetter i klassisk økonomisk teori. Dette fordi det også knyttes kostnader til beslutningstaking og det å gjennomføre transaksjoner. Alternative modeller kan være bildet av forbrukeren som normativ aktør – en som er impulsiv, følelses- eller vanemessig styrt.

fra ulike kilder kan potensielt utgjøre en alvorlig personverntrussel mot den enkelte forbruker, slik vi diskuterer i kapittel 2.

Det elektroniske betalingssystemet EFTPOS[37], som vurderes i dette kapitlet, innebar en *kapitalisering*, en *rasjonalisering* og en *integrering* av transaksjonskjeden (Jacobsen 1990:6).

- Kapitalisering: betydelige investeringer i kortmasse, terminalutstyr, nettverk og datakraft. Samtidig måtte organisasjoner bygges opp (institutional capital) og kompetanse (human capital) for utvikling, drift, vedlikehold og markedsføring av systemene.

- Rasjonalisering: de variable kostnadene ved transaksjoner ville synke over tid, og elektronisk betaling ble dermed langt billigere enn sjekk og girobetaling.

- Integrasjon: vertikal og horisontal. Ved vertikal integrasjon forsvinner ett eller flere ledd i transaksjonskjeden (enkeltbanker kuttes ut og kortbetaler koples direkte til nettverkssystemet og sentrale datasentraler). Dermed kan ofte detaljistleddet kuttes ut. Man får også en fullstendig samordning av betalingsrutiner mellom de ulike ledd i distribusjonssystemet. Den horisontale integrasjonen viser seg på to måter; banker og kortselskaper går inn i felles eierselskaper for nettverks- og driftstjenester, samtidig som bransjestandarder utvikles for kort, terminaler og kommunikasjonsrutiner.

På slutten av 80-tallet var det bankutstedte debetkort som dominerte i varehandelen. Samtidig var det forskjeller i teknologisk satsing blant sparebankene og forretningsbankene. Mens sparebankene satset på magnetstripekort, ønsket forretningsbankene å gå dirkekte til de mer avanserte smartkortene, med chip for lagring av data.

Jacobsen tar også opp variasjoner i den internasjonale oppbyggingen av EFTPOS-systemer. Mens Danmark hadde ett nett som var koplet opp mot én sentral, ønsket man i USA en langt sterkere grad av konkurranse mellom ulike alternative nettverk. Vi kommer tilbake til hvilke utslag dette kan ha gitt på utbredelse og bruk av betalingskort.

4.2 Magnetstripekort versus smartkort

I utviklingen av elektroniske betalingssystemer involveres forbrukere i en prosess som er så kompleks at den enkelte forbruker ikke har informasjon, kompetanse eller interesse nok til å skaffe seg oversikt over situasjonen. Dermed er det også vanskelig for den enkelte forbruker å uttrykke sine behov og ønsker i forbindelse med det nye systemet. I slike tilfeller er det gjerne myndighetene som involveres og som handler på vegne av forbrukerne. Her handler man ut fra et sett ideer om hva som er til forbrukernes beste. I forbindelse med utviklingen av betalingskort i Norge var bankene (og tilknyttede enheter) de primære aktørene, mens myndighetene igjen reagerte i forhold til bankenes planer, strategier og faktiske valg. Andre relevante "aktører" var de eksisterende teknologiske standarder, som delvis representerte aktørenes teknologiske kunnskap og økonomiske ressurser, og delvis internasjonale standarder for kort, utstyr og kommunikasjon – samt juridiske reguleringer (Jacobsen 1993).

[37] EFTPOS = Electronic Funds Transfer at the Point Of Sale

Vi vil se på de forhandlinger og konflikter som oppstod i kjølvannet av betalingskort-utviklingen i Norge på 80- og 90-tallet. Disse gir innsikt i hvor vanskelig, og eventuelt ødeleggende, en slik situasjon kan fremstå i et ikke-kooperativt miljø. Det kan spores visse likhetstrekk i debatten rundt PKI-utviklingen, selv om premissene og aktørgruppene er noe forskjellige. Poenget er å få frem uønskete effekter som oppstår når et ikke-kooperativt miljø eksisterer mellom de involverte aktører, i dette tilfellet primært sparebankene og forretningsbankene. Ved å velge ren egennytte som dominerende strategi kan den totale situasjonen forverre seg for begge aktørgrupper, samt for samfunnet som helhet, og herunder forbrukerne. For dypere innsikt i spillteoretisk tilnærming til betalingskort-problematikken, se Jacobsen (1992).

Det kan antas at bankene på denne tiden var for involverte i å fronte sine strategier til å tenke helhet og forbrukernytte. Det var store irreversible kostnader inne i bildet og markedssignalene var for svake. I 1987, da EFTPOS-systemet ble introdusert, valgte sparebankene å fortsette med magnetstripe-teknologien som allerede ble benyttet på bankkort til bruk i minibanker. Forretningsbankene derimot tok i bruk det nye franske chip-baserte Smartkortet (Jacobsen 1993). I fire år (1987-1991) var disse teknologiene dårlig integrert, selv om bankene utad ønsket integrering og standardisering. Dette ville selvsagt gi storskalafordeler, lavere priser og hurtigere utrulling av kort og terminaler.

Selv om integrasjon rent rasjonelt sett var den beste strategien, gikk begge bankgrupperinger hardt ut mot hverandres teknologier. Det ble kranglet om funksjonelle, økonomiske og sikkerhetsmessige faktorer ved de to systemene, og mens krangelen pågikk bremset utrullingen opp. Bankene kom i økonomiske vanskeligheter fordi storskalaeffekten uteble. For forbrukerne resulterte dette i lav utrullingstakt av terminaler, relativt dyre transaksjoner og forvirring rundt prosedyrer, korttyper, etc (Jacobsen 1993, Rogers 1983).

Først i 1991 ble de to bankgrupperingene enige om å standardisere terminaler og markedsføring mot publikum. Dermed ble det felleseide Axess etablert, med sparebankene og forretningsbankene på eiersiden. Axess skulle utvikle og administrere systemet, og alle terminaler ble utstyrt slik at både magnetstripe- og smartkort kunne benyttes.

Vi ser her at det er mange elementer som interagerer i utviklingen av en bestemt teknologi. Magnetstripekort var det naturlige valg for sparebankene ettersom dette var en teknologi de allerede var kjent med og hadde investert betydelige summer i – både på kortsiden, på terminalsiden og i rutiner. Selv om smartkort ble markedsført som sikrere – og som ”fremtidens kort” fordi chipen åpnet muligheter for en bredere utnyttelse – ble ikke dette noen suksess i Norge på 90-tallet. Det er først nå man snakker om en utrulling av denne korttypen i stor skala, blant annet i forbindelse med PKI. Det kan tenkes at magnetstripekort var en ”god nok” løsning på den tiden og at en omfattende smartkort-utrulling ville vært prematur fordi man ikke kunne ta i bruk fordelene som denne teknologien la til rette for. I dag er sikkerhetssituasjonen og sikkerhetsbehovet, samt mulighetsrommet et helt annet enn på 80- og 90-tallet.

Etter 1991 har bruken av magnetstripekort tatt helt av og blitt dominerende på transaksjonsfronten. Norske forbrukere har adoptert teknologien og trykket den til sitt hjerte. Selv om forbrukerne mangler oversikt i et såpass komplekst system, viser gjentatte erfaringer med bruk av slike kort at dette er et system man kan stole på. Dermed bygges tillit til selve *transaksjonssystemet* over tid (ref. kapittel 2.4 om sikkerhet og tillit). Det er ikke lenger banken eller butikkene forbrukerne har tillit til i denne sammenheng, men selve systemet som formidler betaling.

Dette er også interessant i PKI-strategisk sammenheng. Bør det i markedsføringen av PKI vektlegges en tung satsing på et system som folk kan bygge sin tillit til, eller skal man satse på den tillit som ligger i de bilaterale kundeforhold – mellom for eksempel kunde-bank, kunde-butikk, kunde-spillselskap, etc?

Etter 1991 fremstår markedsføringen av bankkort som en stor suksess. Diffusjon av kort og økningen i transaksjoner blant forbrukere viste seg å bli formidabel. Mye av dette kan i tillegg tilskrives bankgrupperingenes bruk av negative og positive incitamenter. Bankansatte ble brukt i direktemarkedsføring av betalingskort og dets fordeler. Samtidig la man opp til spesialtilbud og skreddersydde løsninger for større kundegrupper (positive incitamenter). Den andre måten å ”skyve” forbrukere i retning av å benytte betalingskort var å legge hindringer i veien for alternativene. Prisene ble hevet for andre transaksjonsformer (som sjekker og giroer) og tilgjengeligheten til andre betalingsmetoder ble over tid redusert (negative incitamenter).

Tenker man på forbrukernes ønsker/ behov kan det vurderes dit hen at det å begrense andre muligheter for å gjennomføre en transaksjon har negativ forbrukernytte. Dette fordi ulike forbrukergrupper har ulike behov. Det er kjent at eldre borgere bruker lenger tid på å tilegne seg ny teknologi, og slik har det også vært med betalingskort. Ved å heve gebyrene eller fjerne tilgangen til andre betalingsformer vil denne gruppen falle dårligere ut. Samtidig ser vi av erfaringene fra betalingskortkonflikten at en enhetlig, samordnet satsing må til for å sikre rask spredning av en ny teknologi, og dermed oppnå en kritisk masse brukere. Det å ta i bruk både positive og negative incitamenter er en nødvendighet i så måte, selv om enkelte brukergrupper kan falle uheldig ut. Disse bør eventuelt kompenseres på andre måter (bl.a brukeropplæring) dersom negative incitamenter benyttes i utstrakt grad.

Det ble tidligere nevnt at mens man i Norge, etter hvert, samordnet sin satsing på betalingskort, var det et langt sterkere innslag av konkurranse mellom alternative nettverk i USA. Dette kan ha ført til en tregere utrulling av betalingskort og bidratt til at f.eks betaling ved bruk av sjekkhefter har vært dominerende gjennom hele 90-tallet i et av verdens mest gjennom-teknologiserte land. Dette fordi bankene konkurrerer mot hverandre på alle plan og ikke ser felles nytte av samordning og koordinering av enkelte funksjoner.

4.3 Forbrukerbehov

Vi har sett av eksemplet med utrullingen av elektroniske betalingskort at forbrukerne ikke kom på banen slik man kunne ønske seg sett fra et forbrukerpolitisk ståsted. Aktørinteressene og deres økonomiske og strategiske posisjoneringer førte til at forbrukerne måtte vike i en viktig nasjonal og internasjonal systemsatsing. Jacobsen (1990) oppsummerer forbruksforskningslitteraturen når det gjelder forbrukerinteresser og –krav, og ser disse i lys av betalingskort-problematikken. De relevante kravene som nevnes er:

- Tilgjengelighet og valgmuligheter
- Pris og effektivitet
- Forbrukerbeskyttelse

4.3.1 Tilgjengelighet og valgmuligheter

Jacobsen hevder at forbrukerne har interesse av at EFTPOS-systemene skal være tilgjengelige på flest mulige steder, til flest mulige tidspunkter og til flest mulige typer betalingstransaksjoner. Det hevdes også at tilgjengelighetskravet bunner i et mer generelt krav om tilgjengelighet til alternative betalingsmåter i ulike betalingssituasjoner (Jacobsen 1990:11). Dette er ikke helt i tråd med praksisen der negative incitamenter introduseres for å fremme en ny betalingsform. Vi ser derfor et lite paradoks i kort-utrullingen og antatte forbrukerinteresser. Det påpekes at eksklusiviteten i det minste må begrenses til et minimum og at grensesnittet må være tilpasset de fleste forbrukere (kort, terminalutstyr, omgivelser og regler for bruk). Gjeldene lov tilsier at penger (sedler og mynter) alltid skal være tilgjengelige betalingsmidler, og disse er i plastikk-verdenen fremdeles flittig brukt blant forbrukerne. Det samme vil nok gjelde for signaturer i fremtiden; muligheten for å signere for hånd vil nok eksistere i lang tid fremover, selv om elektroniske signaturer kan vise seg å bli en viktig supplerende tjeneste.

Vi har sett at samordningsproblemer og markedssvikt har figurert i utbredelsen av elektroniske betalingskort i Norge, noe som i en periode påvirket spredningstakten av denne betalingsformen. Jo flere selskaper som engasjerer seg i et slikt system, desto nærmere kommer systemet et *offentlig gode* (Jacobsen 1990:12, Moore 1987). Dermed blir det vanskeligere å fordele kostnader og fremheve de fordeler som knyttes til teknologiske og institusjonelle valg. Da kan det også bli vanskelig å etablere systemer med en viss type teknologi og et høyt volum, som samtidig er regningsvarende for de deltakende parter.

Jacobsen fremhever her muligheten for å ”privatisere” de antatte offentlige godene. Ved monopolisering av *teknologi* og *nettverk* kan slike systemer etableres. Han fremhever bankforeningene og bankenes datasentraler som eksempler på dette, der disse regulerer og kontrollerer tilgangen til nettverkene, tilgang til å benytte samme kort- og terminalstandard, og gebyrlegging av selskapenes tjenester. Dermed omgår man ”gratispassasjerproblemet”. En får samtidig realisert de ”felles” interesser som eksisterer blant konkurrentene, og slik sett økt tjenestevolumet.

Det blir også fremhevet av Jacobsen at liknende mekanismer råder for *teknologiske standarder og utstyr*, der grupperingene må vurdere stordriftsgevinster (felles standard) opp mot vern av egne markedsandeler (særløsninger). I sistnevnte tilfelle hindrer man andre fra å konkurrere om samme kundegruppe, men man har heller ikke adgang til konkurrentenes markeder. Dermed blir det ingen reell konkurranse, og ingen stordriftsfordeler. Problemet her er å vite hva de andre aktørenes strategier og agendaer er i en situasjon der en står overfor en større teknologisk satsing. Utfallet avhenger av hva de andre aktørene tenker og gjør i samme situasjon, samtidig som ingen har kontroll over de andres valg. Man spiller sine kort samtidig, eller prøver å få førstetrekksfordelen. En slik situasjon kan føre til handlingslammelse. Til en viss grad står dagens PKI-aktører overfor samme problemstilling[38].

Manglende standardisering kan også gi et markedsføringsproblem overfor forbrukerne, slik vi har vært inne på tidligere. En standardisering av grensesnitt mellom systemer, samt juridiske og økonomiske forhold, kan lette tillitsbyggingen til systemet og dermed øke utbredelsen og volumet, og forhindre usikkerhet både hos de respektive

[38] Vi kan igjen henvise til Jacobsen (1992) som tar for seg en spillteoretisk vinkling til aktørers vurderinger og beslutninger i en slik situasjon.

kommersielle aktører og hos forbrukerne. Men dette må også kommuniseres ut til forbrukerne på en enhetlig og forståelig måte.
Det har vært bred enighet om at bankgrupperingenes valg av ulike kortløsninger forsinket utbredelsen av EFTPOS i Norge. Selv om man fikk en viss samordning over tid har dette ført til betydelige transaksjonskostnader i form av forhandlinger, forhalinger og støy (Jacobsen 1990:13). Det offentliges svar på, og involvering i denne situasjonen preget av markedssvikt, var opprettelsen av ”Samordningsutvalget for betalingsformidling”.

Jacobsen oppsummerer forbrukernes interesser ved å påpeke viktigheten av en samordning mellom kortselskaper når det gjelder standarder, nettverksressurser og markedsføringsstrategi. Tilbudet må være så enhetlig som mulig og det må kunne oppnås stordriftsfordeler. Dessuten må tilbudet gjøres tilgjengelig for alle, og ikke utelukke marginalgrupper til fordel for gjennomsnittskundene. Dette er en fare dersom man kun lar aktørenes egeninteresser råde i et marked preget av sterk konkurranse og liten samordning. Samordning kan derfor sies å være en forbrukerinteresse.

4.3.2 Pris og effektivitet

Pris er i alle henseender en svært viktig forbrukerinteresse, fordi forbrukeren tenker på seg selv og sin egennytte. Forskning viser at miljøbevissthet og andre hensyn kan virke inn på pristoleransen, men stort sett er forbrukeren ute etter ”gode nok” løsninger gitt de ressurser denne besitter (økonomi, kunnskap, tid). Effektivitet er et annet ”behov”, spesielt i dagens situasjon der man hele tiden snakker om tidsklemme og det å frigjøre tid gjennom å ta i bruk ny teknologi. Som med elektroniske betalingsformidling kan også e-signatur og e-legitimasjon tenkes å være ”tjenester” som effektiviserer hverdagen, spesielt for de forbrukere som er sterkt involvert i andre elektroniske rutiner. Da kan ”analoge” signaturer, postgang og oppmøte virke som flaskehalser og bidra til lite effektiv handel og saksgang.

EFTPOS-systemet var dyrt å implementere, slik et omfattende PKI-system vil være. Dermed dukker spørsmålet om gebyrlegging opp. Skal forbrukerne finansiere satsingen og de faktiske kostnader, slik at dette ikke subsidieres fra andre typer tjenester eller de alternative tilgjengelige tjenestene? Da kan man ende opp med en situasjon der kunder som ikke benytter systemet straffes for nyvinningen gjennom høyere avgifter på bruk av alternative metoder (ref. kapittel 4.2). Jacobsen (1990) hevder at forbrukerne uansett har interesse av at kostnadene, og dermed prisene på tjenestene, blir så lave som mulig.

Det er som sagt en utfordring å finne en nøkkel for samfunnsoptimal samordning av strategier for teknologisk fornyelse (hvilken teknologi skal det satses på) og for standardisering av systemer og rutiner. Konkurrenter skal *samarbeide og konkurrere*, og samtidig finne en optimal fordeling av *kostnader og gevinster*. I selve håndteringen av denne problemstillingen kan forbrukernes behov og stemmer forsvinne, slik det delvis gjorde i EFTPOS-utviklingen.

Jacobsen konkluderer med at forbrukerinteressene må finne et balansepunkt mellom nødvendig samordning av systemer for å oppnå storskalafordeler (ved å overkomme en spredningsterskel), og nok konkurranse til å sikre at effektiviseringsgevinster presses nedover i transaksjonskjeden til forbrukerne.

4.3.3 Forbrukerbeskyttelse

Av forbrukerpolitisk involvering i utviklingen av EFTPOS-systemet hevder Jacobsen (1990) at det er *forbrukerbeskyttelse* man har konsentrert seg om. Det har vært fremhevet at personlig sikkerhet er viktig for mange forbrukere, og spesielt for de eldre. Dette understøttes av nyere rapporter og undersøkelser, spesielt i forbindelse med Internett som ny transaksjons- og distribusjonskanal.

Innen betalingsformidling nevnte vi tidligere de psykologiske problemene (om enn relativt små) som kunne oppstå ved systemsvikt, samtidig som økonomiske tap kan forekomme. Hovedpunkter i sikkerhetstankegangen er at forbrukerne må sikres mot tyveri og misbruk av sine virkemidler. Dessuten må de beskyttes mot seg selv, for å forhindre misbruk eller feil bruk av virkemidler der forbrukeren ikke er klar over forholdet. Her er det avgjørende å styrke forbrukerens kompetanse rundt f.eks betalingssystemet, eller i vårt tilfelle; forhold knyttet til bruk av e-signatur/ e-legitimasjon. Sikkerhetskjeden er ikke sterkere enn det svakeste leddet i kjeden, og dette er ofte forbrukeren.

Forbrukerne må også opplyses om hva som er uaktsom bruk av et system og konsekvensene av slike handlinger. Dette er myndighetenes overordnete ansvar. I dagens samfunn legges det opp til at stadig mer ansvar flyttes over til forbrukerne, og at disse må være bevisste på hva de samtykker til[39]. Dermed må forbrukerne forholde seg *aktivt* til stadig flere forhold, noe som *ansvarliggjør* den enkelte forbruker i langt større grad enn tidligere (ref. kapittel 2.1 om forbruker- og borgerrollen).

Allerede ved introduksjonen av elektroniske betalingsmidler så man viktigheten av å beskytte den enkeltes personlige integritet. I et slikt system samles det opp store mengder data. Når disse dataene koples sammen, fra ulike kilder, kan man danne seg en profil av den enkelte forbruker. Dermed er risikoen for misbruk også høyere hvis slik informasjon skulle havne i feil hender. I dagens informasjonssamfunn er denne risikoen langt høyere enn tidlig på 90-tallet. Dermed er det av stor viktighet å vurdere hva slags informasjon som er nødvendig å gi til ulike aktører i markedet.

Det er nevnt tidligere at et marked sjeldent fungerer helt tilfredsstillende, og dermed er kravet til forbrukerbeskyttelse særs relevant. Instanser som blant annet Forbrukerrådet, Forbrukerombudet og Datatilsynet skal være forbrukernes organ i sammenhenger der markedet ikke fungerer, og der forbrukerne står svakt alene. Samtidig er det ikke alltid sammenfallende interesser mellom det markedsaktører og forbrukere forventer og hva instansene fremsetter som krav.

Et eksempel kan være følgende: Forbrukerrådet laget i 2001 en liste over råd forbrukere burde forholde seg til ved handel over nett. Ett av disse gikk ut på at forbrukeren ikke burde oppgi kredittkortnummer til bedriften man handler med. Samtidig forsøkte nettbransjen å bygge tillit til denne betalingsformen. På den tiden var det langt færre svindelforsøk på nett enn i den tradisjonelle handelen, men skepsisen blant forbrukerne var likevel langt høyere for netthandelen.

Det kan også antas at det er i forbrukernes interesse å kunne betale med kort på nett, fordi dette er mer effektivt og bekvemmelig (Slettemeås et. al. 2002). Dermed ser man at aktørene *de facto* motarbeidet hverandre, selv om alle parter hadde interesse av å legge til rette for handel på nett, samt gjøre dette så sikkert, effektivt og

[39] Ref. endringen som fant sted med den nye personopplysningsloven av 1. januar 2001

bekvemt som mulig for forbrukeren. Det er altså en vanskelig balansegang å veie behovet for beskyttelse mot behovet for effektivitet og tilgjengelighet. Samtidig er det vanskelig å vurdere hvor sikkerhetsrisikoen ligger; om systemet fremkaller usikkerhet eller om e-aktørenes intensjoner er uærlige.

Problemet med EFTPOS-systemet, og også en fremtidig PK-infrastruktur, er at investeringene som knyttes til systemene er svært høye og de tar lang tid å utvikle. Dersom løsningene er sub-optimale er det fare for at systemet likevel vil kunne få et langt liv, noe som ikke er i brukernes interesse. Det er også en kjensgjerning at innføring og spredning av innovasjoner gjøres under betydelig usikkerhet. Det hevdes i Jacobsen (1990) at normativ beslutningsteori i slike tilfeller tilsier at en bør velge systemløsninger som er korrigerbare, reversible og fleksible (Collingridge 1980).

Dette faller ofte sammen med at forbrukerinteresser kommer sent med i utformingen av slike systemer, og at innflytelsen i markedet heller materialiseres som en *etterskuddskontroll.*

Vi har sett at de ulike kravene kan komme i konflikt med hverandre. Pris og tilgjengelighet må avveies mot forbrukerbeskyttelse og sikkerhet i systemene (Jacobsen 1990:20). Samtidig som sikkerhetstiltak kan virke hemmende på effektivitet og tilgjengelighet, kan det også heve prisnivået på tjenester, fordi kontroll og sikringstiltak virker fordyrende på systemene. Dette kan likevel kompenseres ved samfunnsmessig og bedriftsmessig effektivisering over tid. Reguleringer kan også begrense konkurransen på ulike nivåer i systemene, samt at disse kan virke fordyrende på systemene. Samtidig kan slike reguleringer bidra til økt tillit og dermed økt bruk over tid.

5 Tolkninger og viktige tilleggsfaktorer

Under PKI Forums formål står det: ”PKI er ikke et mål i seg selv. Det er alle de tjenester som PKI skal muliggjøre som er viktig å fokusere på, ikke PKI-teknologien i seg selv.” Dette fordrer fokus på nytteverdien av PKI som en muliggjørende faktor for avanserte tjenester på nett og som en sikker teknologi som gir tillit til elektronisk samhandling.

Forumets formål om å fokusere på tjenester fremfor teknologi vil være et godt utgangspunkt når det skal vurderes spørsmål til en forbrukerundersøkelse.

Nedenfor vil vi gå igjennom, kategorisere og videreføre de tolkninger som har blitt gjort så langt i dokumentet. Dette gjelder forbrukerperspektivet (kap. 2), relevante funn fra tidligere undersøkelser (kap. 3) og bankkort-analogien (kap. 4). I tillegg vil vi i kategoriseringene legge inn faktorer som ikke er kommet frem i de foregående kapitler. Samtidig vil vi operasjonalisere og foreslå spørsmål som kan inngå i en spørreundersøkelse rettet mot norske forbrukere. Disse presenteres i varierende form og er tenkt som veiledning til videre konkretisering av spørsmål etter den skisserte workshopen.

5.1 Borger / forbruker

Stadig flere tjenester blir konkurranseutsatt og vi får flere tilbydere i ulike markeder. Dette krever mer av forbrukerne i form av at de aktivt må forholde seg til ulike tilbud og tilbydere. Mer ansvar overføres til forbrukerne selv om de også får flere rettigheter. Tendensen til å redusere mellomledd reverseres ved at nye mellomledd kommer til for å forenkle prosessen for forbrukerne i et stadig mer komplekst marked. Samtidig kan det være enkelte arenaer der forbrukerne ikke ønsker å være forbrukere – for eksempel på infrastruktur-siden?

Relevant spørsmål her kan være:

- *Ønsker du som forbruker å forholde deg til elektronisk ID og elektronisk signatur i et marked, eller bør dette være myndighetenes oppgave?*

- *Ønsker du å være <u>forbruker</u> når det gjelder tjenester og <u>borger</u> når det gjelder infrastruktur?*

Kresne, egennyttige forbrukere, har ikke samfunnsinteresser som sin prioritering. Dersom en prematur løsning fungerer dårlig kan de ty til en indre sanksjon – altså tilbaketrekking fra relasjonen (Luhmann 1999). Et eksempel her kan være bruk av notartjenesten AltInn, dersom denne utvikles til en forbrukertjeneste. AltInn er egentlig en løsning for innrapportering fra næringslivet men kan videreutvikles til en mal, eller et ”PKI-nav”, som skal skjule kompleksiteten også for *forbrukere.* Dermed skal

tjenesten forenkle noe som i utgangspunktet er tungvint. Vi har sett at Bedriftsforbundet har pekt på kritikkverdige forhold ved AltInn, og at systemet i stor grad har gjort prosesser som skulle forenkles mer tungrodde[40]. Blant annet har brukerne måttet sende inn skjema både til Brønnøysundregisteret og en blåkopi til likningsmyndighetene. Brukere har fått strafferenter selv om de har levert til tidsfristen, og systemet krever at Adobe Acrobat er installert. Tilpasninger må også gjøres både ved benyttelse av Opera og Internet Explorer nettlesere. Dette er forhold som skaper stor misnøye hos brukere, og brukervennligheten må være høy for å sikre et minimumsgrunnlag for rask utrulling av PKI i forbrukermarkedet.

Relevant spørsmål her kan være:

- *Er det greit å gå over til en sikrere løsning (PKI) med flere muligheter som signatur og identifikasjon dersom du må oppgradere PC-utstyr eller programvare?*

Kristin Vestmo i Steria[41] hevder at myndighetene har en feilaktig oppfatning av PKI-situasjonen i Norge, der de tror at markedskreftene skal ordne det meste. Dette vil både næringsliv og folk flest tape på. Som strategisk rådgiver har hun fulgt prosessen der den norske selvangivelsen kom på Internett. Hun hevder at tunge aktører i markedet kjemper om makten i dette markedet. Dette er naturlig ettersom den som først får gjennomslag for egen teknologi vil få store fordeler relativt til konkurrentene. Dermed bremser utviklingen opp. Dette argumentet er i tråd med situasjonen som ble skissert i kapittel 4.

Relevante spørsmål her kan være:

- *Bør markedet jobbe med utvikling av sikrere handel (signatur og legitimasjon) på Internett, eller er myndigheter og det offentlige best skikket til dette?*

- *Bør markedet utvikle og myndighetene stå for tilsyn, merkeordninger, etc?*

- *Er det greit at forbrukerne avgjør hva slags informasjon de vil gi fra seg til ulike aktører på Internett, eller bør dette reguleres av myndigheter?*

Brukerkompetanse – eller opplæring av forbrukere i viktige forhold knyttet til bruk og sikring av egen nøkkel/ nøkkelbærer – er fra forbrukersiden et viktig punkt, spesielt når det gjelder ny og kompleks teknologi. Brukeren kan ofte ses som det ”svakeste ledd” i sikkerhetskjeden. Spørsmålet er om forbrukeren ser seg selv som det svakeste leddet, eller om det teknologien (eller annet) som er problemet?

Relevante spørsmål her kan være:

- *Synes du at du vet for lite om hvordan man skal opptre sikkert på Internett?*

- *Savner du brukeropplæring, eller er dette noe en bør klare selv?*

- *Er det teknologien som er vanskelig eller ligger problemet hos brukerne som ikke setter seg godt nok inn i hvordan de skal gå frem?*

En bekymring som ofte kommer fra forbrukersiden er at den raske teknologiske utviklingen vil skape et *digitalt skille* mellom ”de som kan” og ”de som ikke kan”. Her er det gjerne fattige og eldre som betraktes som utsatte grupper (Frønes 2003). Ved en

[40] Handel.no: “– Altinn fungerer dårlig”, 12.05.2004
[41] Ref i Aftenposten.no: “Nettbrukerne taper på fri konkurranse”, 19.01.2003

bred utrulling av ny og kompleks teknologi, der det stilles enda høyere krav til PC-utstyr og programvare, kan det tenkes at dette skillet kan øke.

5.2 Tillit og brukervennlighet

Det hevdes av man gjennom PKI ønsker å bygge tillit til elektronisk handel. Men først må man bygge tillit til PKI, og spørsmålet er hvordan dette kan gjøres? Eller spørsmålet stilt på en annen måte; må man bygge tillit til PKI for å få i gang de tjenester man ønsker? Dessuten; kan det bygges tillit hos forbrukerne på et generelt plan? Vi har sett at enkelte forskningsresultater tyder på at tillit er et subjektivt parameter og "settes sammen" av ulike kalkulative vurderinger, forsøk på å redusere kompleksitet (tillit som forenklende verktøy) og en viss grad av "mavefølelse". Erfaringer viser også at mange følger tips fra venner og kjente etter at disse har gjort egne erfaringer.

Relevante spørsmål her kan være:

- *Hvem eller hva stoler du på når du gjennomfører en transaksjon på nettet? Bedriften, Internett, dine rettigheter som forbruker, flere av disse?*

- *Hvor viktig er din familie og venner som kilder til å "tipse" om nett-tjenester? Betyr deres anbefaling mye for tilliten til nettstedet?*

- *Hvis du skulle signere et dokument eller identifisere deg for en bedrift/ instans over Internett – ville du stolt på denne bedriften/ instansen eller på selve "systemet" for signering?*

- *Er sikkerhet et teknisk, juridisk, eller et tillitsspørsmål – eller en kombinasjon av disse? Hva er viktigst?*

Spørsmål rundt personvern:

- *Føler du en avmakt i forhold til egne persondata, eller har du tiltro til at de selskaper du avgir informasjon til ikke sprer denne informasjonen videre?*

- *Betyr det mye for deg at persondata oppbevares på en forsvarlig måte?*

Når det gjelder brukervennlighet så er dette et utrolig viktig moment når brukerne først har vist en bestemt aktør tillit nok til å ta i bruk tjenesten. Tidligere IT-Minister Ansgar Gabrielsen har blant annet påstått at det skal være like enkelt for norske borgere å identifisere seg eller signere et dokument elektronisk på Internett som det er å gå i minibanken og ta ut kontanter[42]. Brukervennlighet, enkelhet og tilgjengelighet har i tillegg blitt vektlagt som sentrale forbrukerkrav/ -behov.

I PKI-Forums eget strateginotat fremstår nettopp dette som en hindring for adopsjon av PKI-løsninger[43]:

> *"For å oppnå vesentlige sikkerhetsgevinster er det påkrevd med bruk av nøkkellagre (for eksempel smartkort eller USB-baserte løsninger) for å beskytte private nøkler. De organisasjoner som har forsøkt å benytte slike, har opplevd at dette går på kraftig bekostning av systemets brukervennlighet, hvilket av brukeren ofte oppleves som en*

[42] Ref. i Handel.no: "Baner vei for nye nett-tjenester", 06.10.2003
[43] PKI Forums strateginotat av 20. juni 2002, s. 51

større ulempe enn den fordelen den økede sikkerheten gir. Brukere er for øvrig oftest ikke klar over styrken i de forskjellige sikkerhetsløsningene.

Uten å spørre brukerne direkte kan vi konstatere at det vil være et svært sentralt poeng å forenkle sikkerhetsløsningene nok slik at forbrukerne faktisk ”gidder” å ta disse i bruk.

Derfor må hovedmålet være å redusere kompleksitet for forbrukere. Vi ser av andre trender i dag at forbrukerne ønsker å forenkle sin egen hverdag og sitt forhold til ”digitale” tilbud:

- Netcom gjør det bra – ”én pris” på tellerskritt uavhengig av hvem du ringer til.

- *Triple play* i bredbåndsmarkedet – *bundling* av tjenester som TV, Internett og telefoni fra én leverandør. Det viser seg at stadig flere ønsker dette fremfor friheten til å ”shoppe” tjenester fra ulike leverandører.

- Forbrukerne tar i bruk ”nye elektroniske mellomledd” som vurderer pris/ kvalitet i forhold til relevante tjenestetilbud.

Forenkling kan også gi mobil-PKI et fortrinn i forhold til andre løsninger. Mobil-PKI-leverandører som Telenor hevder å kunne redusere kompleksiteten for brukerne ved at de kun benytter én pin-dialog, mot to som er vanlig på Internett. Dessuten kan mobilen benyttes i utlandet (mobilitet som poeng) mot f.eks nettbank.

- *Det kan spørres konkret om hvilke typer løsninger / nøkkelbærere forbrukerne ønsker seg mest, eller har mest tro på:*

  a) Sertifikat på PC’en (soft-sertifikat)
  b) Nettsentrisk
  c) Smartkort
  d) Fingeravtrykk (biometri)
  e) Mobiltelefon (SIM-kort)

5.3 Eksogene faktorer

Det er flere forhold utenfor ”det norske markedet” som kan bidra til å bestemme den videre veien for PKI i Norge. Dette er eksogene faktorer som legger begrensinger på relevansen av forbrukernes input til hvordan en slik utrulling kan foregå på en mest mulig fornuftig måte. Nedenfor går vi kort gjennom noen av disse:

Samarbeid på EU-nivå om felles standarder, utrullingstidspunkt etc. er et eksempel. Blant annet er PKI Challenge et prosjekt med målsetning om å skape et miljø for fullt integrert PKI-utvikling i Europa, men på en slik måte at e-handel og tjenester likevel kan utføres ved bruk av heterogene PKI-produkter og tjenester.

Generelle EU-direktiv må følges av Norge, og Norge er ”best i klassen” når det gjelder å innlemme EU-direktiv i norsk lovgivning. Samtidig er BankID policy på nåværende tidspunkt en sertifikatpolicy som er ikke-kvalifisert i henhold til EUs standarder. Bankenes standardiseringskontor har godkjent BankID policy og alle banker som ønsker å utstede sertifikater under dagens BankID policy vil utstede ikke-kvalifiserte sertifikater. For at én eller flere banker skal kunne utstede kvalifiserte sertifikater må

det gjøres endringer i BankID sertifikatpolicy for å oppfylle ETSI spesifikasjoner for kvalifiserte sertifikat policy[44]. I tillegg må innholdet i sertifikatene endres til å inneholde objektidentifikatorer / informasjon som viser at de er utstedt under en kvalifisert policy. Siden BankID policy pt. ikke er kvalifisert kan den heller ikke registreres hos Post- og teletilsynet som kvalifisert. Trolig vil BankID sertifikat policy med enkle grep kunne bli en kvalifisert policy.

På EU-nivå har man dessuten ønsket en felles standard for å håndtere identitetsdata for alle borgere i Unionen. Blant annet har EUs smartkortprosjekt hatt som mål å gi alle innbyggere et e-ID-kort, men det er store variasjoner i hvor langt de ulike medlemslandene har kommet[45]. I mange europeiske land utstedes ID-nøklene av myndighetene, mens norske banker (gjennom BankID samarbeidet) og Zebsign gjør det samme her i Norge.

På personvern-siden vil globale tendenser påvirke Norge i høyeste grad. Dette gjelder blant annet de anti-terrortiltak som har blitt iverksatt etter 11. september 2001. Myndigheter i alle land, spesielt i USA og Europa, har lagt om sine tiltak for å sikre borgere og nasjonal infrastruktur mot terror. Dette påvirker krav og betingelser for sikkerhet her til lands. I USA må man blant annet skanne ansikt og fingeravtrykk for å besøke landet f.o.m. 30. september 2004[46]. Denne informasjonen lagres sammen med andre data i verdens største biometriske database. Amerikanske borgere, og muligens EU-borgere, må etter hvert avfinne seg med at pass i fremtiden vil inneholde en databrikke med biometriske data om borgeren[47]. Dette kan også bli tilfellet for norske pass om ikke lenge. En slik utviklingstendens kan også påvirke norsk forskning rundt biometriske data[48], og gjøre denne teknologien mer relevant på flere felt. Det kan dessuten påvirke forbrukerne i retning av å bli mer "vant til" denne formen for identifisering.

Med hjemmel i USAs *The Patriot Act* er EU og USA kommet i strid om blant annet adgang til PNR-data (Passenger Name Record)[49]. USA ønsker tilgang til disse dataene fra europeiske flyselskaper, og da også opplysninger som EUs personverndirektiv oppfatter som sensitive. Dersom USA vinner igjennom svekkes personvernet ytterligere i EU (og følgelig Norge), men det kan medføre at borgerne venner seg til en lavere terskel for personvern. Med andre ord, toleransen for overvåkning og registrering av individer kan ha økt som en konsekvens av 11. september.

En undersøkelse utført for TV2[50] viste at 70 % av respondentene mente det var viktigere å bekjempe organisert kriminalitet enn å verne om privatlivets fred. Datatilsynets egne undersøkelser viser derimot at nordmenn har en videre oppfatning av hvilke opplysninger som anses som følsomme enn det som lovverket definerer[51].

I en større sammenheng kan disse tendensene påvirke forbrukernes forhold til både sikkerhet og til personvern og overvåking. Her kan utviklingen trekke i to retninger – enten godtar man utstrakt bruk av personlige data, eller så blir man mer og mer opptatt av å sikre sin egen person og sfære mot offentligheten.

---

[44] Ref. ETSI TS 101 456 v.1.2.1
[45] Ref. Aftenposten: "Europeisk e-identitet på vei", 24. mai 2003
[46] Ref. VG: "Bush vil ha ditt fingeravtrykk", 3. april 2004
[47] Ref. i Dagbladet.no: "Gjør deg klar til å scannes" 16.12.2003 www.dagbladet.no/dinside/2003/12/16/386309.html
[48] Sintefs-forskningspris for 2003 gikk blant annet til fire forskere (SINFTEF og Idex) for å ha utviklet et sensorsystem som analyserer og gjenkjenner fingeravtrykk. Ref. i Teknisk Ukeblad nr. 14-2004, s.26
[49] Ref. i Aftenposten.no: "En velkommen Storebror?", 14.04.2004
[50] Ref. Aftenposten Aften: "Krimbekjempelse viktigere enn personvern", 24.06.2003
[51] Aftenposten – kronikk: "Sårbart samfunn – usårbare mennesker?", 27.06.2003

Relevante spørsmål her kan være:

- *I tråd med den økende terror-beredskapen i verden, føler du at det er behov for sikrere rutiner for bruk av Internett, for eksempel sikring av persondata, bedre rutiner for legitimering, etc.*

- *Eventuelt: Er sikkerhetstiltakene på vei til å gå ut over personvernet? Føler du at man heller bør fokusere på å redusere innsamling av personlig informasjon?*

En annen viktig og relevant utvikling er den som store tunge aktører som Visa står for. Innen transaksjoner på Internett har blant annet Visa hatt en viktig innvirkning. Nylig ble selskapet tildelt en industriell pris for sitt nye system for sikker netthandel[52]. Dette systemet (3-D-Secure) eller "Verified by Visa" som Visa kaller det, og "MasterCard SecureCode" som MasterCard markedsfører, er et system der brukeren autentiserer seg når han bruker kortet på nettet. Det er kortutsteders bank som bestemmer autentiseringsmetoden. I Norge vil for eksempel de fleste bankene bruke BankID som autentiseringsmetode.

Når forbrukeren handler på Internett skal dette systemet garantere kortinnehavers identitet. Her må et personlig passord oppgis ved betaling for varer/ tjenester på Internett, slik det gjøres i tradisjonell handel. Denne utviklingen kan blant annet tolkes dit hen at flere blir vant til sikker handel på nett og benytter betalingskort i ustrakt grad. I tillegg kan kortenes kvalitetsmessige utvikling gjøre sitt til at forbrukerne kopler høy sikkerhet med stadig flere bruksmuligheter for denne type kort.

Visa er også i ferd med å bytte ut magnetstripekort med smartkort, og hele 10% av totalt 1,2 milliarder kort har allerede denne løsningen[53]. Dette viser en trend i retning av at forbrukerne mer eller mindre blir "påtvunget" å ta i bruk smartkort. Visa har gått sammen med EuroCard og MasterCard (EMV) om dette systemet. En slik utvikling som disse tre selskapene her står for vil med høy sannsynlighet påvirke bruken av PKI og nøkkelbærere i Norge. Grunnen til denne utviklingen er i stor grad basert på det forhold at bankene i Europa fra 1. januar 2005 er ansvarlige for all svindel som gjennomføres med kort som mangler chip[54]. Utviklingen av slike chip-baserte (EMV) kort går derfor veldig raskt i Europa, og det er en målsetning om at standarden også skal være innført i alle minibankautomater innen 2005.

Relevant spørsmål kan her være:

- *Kredittkortene kommer etter hvert til å bytte fra magnetstriper til såkalte smartkort, med en data-chip foran. Synes du denne type kort også burde kunne brukes som ID-kort for elektroniske identifisering og signering av dokumenter?*

Tall fra Teller viser dessuten at handel med norske Visa-kort på nettet økte med 146 % i 2003, og det er forventet en dobling også i 2004[55]. Den totale handelen med Visa-kort på nettet i 2003 var 3,2 milliarder kroner, og dette utgjorde hele 13% av Visas totale omsetning.

Dette kan gi en indikasjon på modenheten for handel på nett, og at forbrukerne generelt sett har større tillit til sikkerhetssystemene og aktørene som er etablert i denne kanalen. Faren for en ny og vanskelig forståelig løsing som PKI er da at forbrukerne er *tilfredse nok* med dagens løsninger. Undersøkelser fra Sverige viser at forbruker-

[52] Ref. i Handel.no: "Trygg ehandel gir ehandelsvekst", 30.04.2004
[53] Ref. i Computerworld.no: "Visakort med skjerm", 19.05.2004
[54] Ref. i Handel.no "Elektroniske kontantkort – Bidrar til økt ehandel", 29.03.2004
[55] Ref. i Handel.no: "Kraftig vekst i netthandelen", 12.02.2004

ne har liten kunnskap om nye betalingstjenester som e-lommebok og digital signatur/ PKI[56]. Kunnskapen er her et problem. I tillegg hevdes det at forbrukerne ser få fordeler ved å ta i bruk nye betalingstjenester, slik at nytteaspektet må fremheves enkelt og tydelig for forbrukerne.

En annen trend som er "utenfor kontroll" her hjemme er inkorporeringen av smartkort-lesere i nye PC'er. Dersom nye PC'er i den norske markedet får dette som standard, kan det lette utrullingen og bruk av smartkort som e-ID og e-signatur.

Kort oppsummert kan vi si at folk er vant til å bruke kreditt- og debetkort, og man har gjerne flere kort liggende. Dessuten øker stadig antall transaksjoner der betalingskort er innblandet, både i tradisjonell handel og kontantuttak, og over Internett. I 2003 ble det registrert 702 millioner transaksjoner med kort til varekjøp og kontantuttak[57], og vi kan vel dermed stadfeste at dette markedet er modent eller *alminneliggjort* for slik kortbruk.

Relevant spørsmål kan her være:

- *Det er en økende tendens til at betalingskort som Visa blir sikrere ved at man får såkalte "smartkort". Dessuten kan disse, eller liknende kort, brukes til identifikasjon og signatur over Internett. Virker det naturlig for deg å ha et "fysisk kort" som en ID for mange tjenester over Internett, eller er det vel så greit å ha sertifikater liggende på PC'en?*

5.4 Informasjonstilgang

Vi har diskutert behovet for å kommunisere med forbrukerne angående det å ta i bruk ny teknologi. Samtidig er det ikke lett å vite hva, hvor mye eller hvordan informasjonen bør spres til forbrukerne. Dette kan være et relevant felt å spørre forbrukerne direkte om. Nedenfor listes ikke konkrete spørsmål, men spørsmål som er av interesse å vite mer om – gitt at de stilles på riktig måte:

- *Hva trenger forbrukeren å vite for å ta elektronisk signatur i bruk?*

- *Er det viktig for forbrukeren å vite noe særlig om e-signatur for å ta dette i bruk?*

- *Vil de vite noe om tjenestene, om den tekniske løsningen, om aktørene som bidrar i infrastrukturen, eller en blanding av dette?*

I samme vending har vi sett at markedsføring av nye tjenester er viktig for å få en raskere utrulling, og denne markedsføringen bør ideelt sett være samkjørt selv om markedsaktørene konkurrerer. Nedenfor er det enkelte ting vi ønsker å vite i så måte:

- *Hvordan skal en kommunisere eller markedsføre de ulike begrepene – eID , eSignatur, PKI, etc…*

- *Bør man kun markedsføre én sikkerhetstjeneste (e-signatur), så vil de andre tjenestene følge etter?*

[56] Ref. i Handel.no: "Tilfreds med dagens betalingsløsninger", 20.10.2003
[57] Handel.no: "Stor tillit til nettbetaling", 06.05.2004

- *Bør man gå bort fra fokus på PKI i det hele tatt og kun vektlegge de faktiske tjenestene man kan tilby med denne teknologien integrert?*

- *Bør det fokuseres på de analoge ekvivalentene når man skal kommunisere? (Signering, ansiktsgjenkjenning, pass, bankkort, kredittkort…)*

- *Forbrukere har vist seg å ikke være spesielt opptatte av personvern-policy'er, SSL, merkeordninger, etc, men de stoler mer direkte på tjenestetilbydere. Vil det dermed være en feilprioritering å markedsføre TTP'er overfor forbrukere, selv om disse er viktige for rollestrukturen i PKI?*

- *Dersom man går gjennom en sikkerhetsprosess online - er det da ønskelig med mye informasjon om sikkerhet underveis (bekreftelser ved hvert steg), eller en kort og brukervennlig prosedyre (men at man da må stole på at sikkerheten er ivaretatt).*

- *Er behovet forskjellig ved ulike typer transaksjoner?*

5.5 Merverdier med PKI?

I PKI Forums strategidokument av 2002, s. 31, hevdes det at selv om mesteparten av PKI-bruk i fremtiden vil være knyttet til autentisering, er det nettopp signaturer (avanserte elektroniske signaturer) som skiller PKI fra andre teknologier med tanke på nytteverdi. Hvor viktig er for eksempel autentiserings-biten?

Hos enkelte organisasjoner har opptil 60% av tid benyttet til *help desk* mandag morgen vært knyttet til å gjenopprette glemte passord[58]. Tid og penger spart i form av enklere/ færre passord og pin-koder vil være av betydelig omfang, samt at forbrukerne vil bli mindre frustrerte pga glemte passord. Hvordan stiller forbrukere seg til dette? Nedenfor er det listet problemstillinger som det eventuelt kan utledes konkrete spørsmål til:

- *Er det relevant å samkjøre en strategi som fokuserer primært på e-signatur, slik vi nevnte mht. markedsføring ovenfor?*

- *Vil e-signatur gi en klar merverdi for forbrukerne, i og med at signering har vært en flaskehals i elektronisk saksgang?*

- *En annen mulig merverdi i forbindelse med PKI kan være forenkling og eliminering av pin-koder (i Norge). Oppfatter forbrukerne dette som en viktig merverdi? Ulike spørsmålsformuleringer kan benyttes her.*

- *Andre merverdier kan være kvalitetsforbedring, gjennom elektroniske kvitteringsmekanismer. PKI-basert autentisering vil gi enklere mulighet for innsyn i egen saksbehandling og egne sensitive personopplysninger.*

[58] EEMA – The European Forum for Electronic Business: "Identity Solutions for Better Businesses – an EEMA Workshop – 26-27.02.2003. www.eema.org/event_R.asp?FirstParam=133

5.6 Konkret på løsninger

Nedenfor vil gå konkret inn på potensielle spørsmål som er mer rettet mot løsninger og enkeltproblemstillinger. Spørsmålene er ikke nødvendigvis utledet fra de tidligere kapitlene.

En problemstilling som opptar mange er hvorvidt ulike sertifikater bør ha ulike sikkerhetskrav og funksjonalitet. Spørsmål som da er relevante er:

- *Hvilke applikasjoner kan/ bør knyttes til samme type signatur?*

- *Bør en skille tjenestegruppene bevisst for å sikre enkelhet, samt bygge kompetanse og tillit?*

- *Forbrukerne kan for eksempel forespeiles en tredeling av elektroniske ID'er og kommentere dette:*
  1) Offentlige: høye sikkerhetskrav, lav frekvens (Borgerkort)
  2) Bank: høye sikkerhetskrav, høy frekvens (Bankkort)
  3) *Kommersielle: middels sikkerhetskrav, middels frekvens (Handelskort)*

- *Eller ønsker forbrukerne ett sertifikat / kort med kun det høyeste sikkerhetsnivået – en ID som kan brukes til "alt"? (referér til uttalelsen om at "alle som blir født bør få en e-ID")*

- *Bør det også være mulighet for å være anonym ved bruk av nett-tjenester? (problemer: hvitvasking, ulovlig handel, ulovlig porno)*.

- *Er bruken av personnummer problematisk for forbrukerne? Oppfattes dette fremdeles som "sensitiv informasjon" selv om det ikke lenger er definert som det?*

- *Hva tror forbrukerne om sikkerheten mht en digital signatur versus en signatur på papir? Er sikkerheten like god, lavere, eller høyere?*

Vi berører så vidt *gjenbruk* av e-ID'er ovenfor. Men dette er et viktig tema som bør oppta forbrukerne så vel som aktørene i en PKI. For eksempel kan det da spørres om faktisk bruk av PKI-relaterte tjenester:

- *Har du benyttet tjenester der du har kunnet signere elektronisk eller identifisere deg elektronisk?*

- *Dersom én tjeneste; er denne tjenesten "inngangsporten" til videre PKI-bruk (evt. annet ord) for deg?*

- *Kjenner du til hvorvidt du kan benytte denne løsningen også til andre tjenester?*

- *Virker det naturlig å benytte den til andre tjenester?*

Pris og prisstrategier er et viktig tema i PKI-sammenheng. Vi har sett at norske forbrukere i stadig større grad handler og utfører andre tjenester over nett[59], og at betaling med kredittkort blir mer vanlig. Det betyr at modenheten øker, noe som igjen kan bety at forbrukerne er "klare" for neste steg i utviklingen. Samtidig er norske forbrukere blitt vant til at ting er "gratis" på nett. Dersom forbrukerne finner nytten i en tjeneste kan man likevel finne unntak. Filmwebs bestill-betal løsning for kino er et eksempel der man faktisk betaler *mer* "online" enn ved oppmøte. Men dette er relativt uvanlig i nettsammenheng, fordi det forventes at utstrakt grad av "selvbetjening" skal fjerne unødige kostnader (ansatte, mellomledd).

Uansett kan det antas at betalingsvilligheten er lav for PKI, fordi brukerne etterspør tjenester, ikke kun en legitimasjons- eller signeringsfunksjon. Derfor må prisen bakes inn i tjenester dersom forbrukerne skal betale. Spørsmålet er da hvordan betaling skal foregå – og dersom mange aktører går sammen om PKI – hvordan fordeles gevinster og kostnader?

Foreslåtte strategier for prising er:

- Transaksjonsprising (betaling per transaksjon)
- Flat prisstruktur (engangsbetaling, f.eks abonnementsordning)

Det er vanskelig å spørre forbrukere om pris og betalingsvillighet. Det er ofte slik at, selv med konkrete eksempler, så har forbrukere lett for å overestimere egen betalingsvillighet (Nysveen & Pedersen 2004). Det er dessuten vanskeligere å få gode data på dette i en kvantitativ undersøkelse der man har liten mulighet til å presentere utstrakt grad av informasjon og stimuli i forkant av undersøkelsen. Her vil konkrete usability-tester og piloteringer gi bedre resultater.

5.7 Behov for PKI?

I sin vurdering av OASIS-rapportene hevder Jon Ølnes[60] at det er en *samfunnsinfrastruktur* som er målet for PKI Forum, og at en slik infrastruktur må sikre kommunikasjon mellom vilkårlige og uavhengige parter. Det betyr at det ikke skal være en forutsetning at det for eksempel eksisterer et kundeforhold mellom forbruker og en kommersiell part. I en slik infrastruktur kreves også en *åpen teknologi* og *åpne forretningsmodeller.* Her er det fremdeles en vei å gå for norske aktører, hevder Ølnes.

Et annet poeng som nevnes av Ølnes er antakelsen om at nær 95% av elektroniske tjenester kan gjennomføres uten PKI, bortsett fra de tilfeller der det er krav om avansert elektronisk signatur. Ølnes vektlegger også at priskalkyler og overslag for en slik infrastruktur helt klart gir PKI et problem i forhold til eksisterende løsninger. Vi var tidligere inne på at "moderat rasjonelle forbrukere" ofte nøyer seg med løsninger som er "bra nok", og pris er samtidig et viktig element. Selv om PKI i det store og hele er en "bedre" løsning må den måles mot nytte og kostnader.

Andre momenter som peker på at folk er "fornøyde nok" eller "ikke bryr seg om" sikkerhetsløsninger, og at dagens løsninger dermed stort sett er tilstrekkelige, kan være følgende:

- Få sjekker SSL-ikonet nederst i browseren.
- Få kan verifisere N-safe merket, dersom de i det hele tatt kjenner til det.

[59] Tall fra MMI (i regi av eforum) viser at netthandelen har tredoblet seg det siste året (per mai 2004) og at handelen dermed har økt fra 1,8 til 3,85 milliarder kroner.
[60] I PKI-Forums plenumsmøte 4. mars 2003. Presentasjon: "OASIS rapportene og norsk PKI – er vi på rett spor?

- Hvem sjekker soft-sertifikatet i Skandiabanken?
- Få leser personvern-policy'er på nettsteder.

Dette kan vi for så vidt spørre forbrukerne mer inngående om for å få et bilde av hvor opptatt man faktisk er av sikkerhet. Det kan være slik at forbrukere nå er fornøyde med sikkerheten, men savner "noe mer", altså f.eks en signeringsfunksjon for å slippe postale utsendelser og faks.

Utover dette kan det mer konkret spørres om behovene for å utnytte det PKI kan tilby per i dag:

- *Synes du det er behov for å kunne signere dokumenter over Internett i dag? (Eventuelt eksempler.)*

- *Synes du det er behov for å identifisere deg på en sikrere måte over Internett enn den muligheten du har i dag?*

- *Bør det være én type sikkerhetsinfrastruktur som er lik over hele landet, for alle tjenester?*

- *Bør alle identifisere seg med samme type løsning – for eksempel med et smartkort eller et sertifikat på PC'en, eller er det greit å ha flere muligheter?*

- *Bør en slik løsning kunne benyttes i utlandet?*

Vi kan avslutningsvis liste opp de aktuelle tjenester der PKI kan utnyttes og spørre om behovene for å signere (gradering) eller identifisere seg ved å benytte PKI, eller om dagens løsninger er gode nok. Her kan vi ta utgangspunkt i BankIDs liste i kapittel 3.2 og supplere med flere.

I tillegg kan det være interessant å se på *elektronisk stemmegivning* som "tjeneste". Vi så i kapittel 3.5 at det har vært gjennomført elektroniske lokalvalg i 2003, men elektronisk stemmegivning for hele befolkningen (Stortingsvalg) er foreløpig noe usikkert. Kommunalminister Erna Solberg har nedsatt en arbeidsgruppe som skal utrede om det er praktisk mulig å innføre slik stemmegivning. Det vurderes foreløpig dit hen at det er for mange ubesvarte spørsmål før dette kan gjennomføres på landsbasis[61]. En slik valgmulighet vil i så fall kunne ha en viktig innvirkning på folks forhold til en e-ID – fordi det involverer hele den norske befolkningen.

En annen interessant tjeneste kan koples til *jobbsøknader*. Antall jobbsøknader som sendes hvert år er formidabelt høyt. Her kreves både signatur vedlagt søknaden og flere attesterte kopier av vitnemål, anbefalelsesbrev og lignende. Da er det behov både for en signeringsfunksjon og en notar som besitter og kontrollerer en databank med dokumenter. Ektheten av dokumentene må verifiseres når dette etterspørres. Her er dessuten flere betalingsmodeller mulige (abonnement, transaksjonsspesifikk betaling, etc). Ettersom forbrukeren må kunne oppdatere dokumenter hele tiden virker en abonnementsordning som et naturlig valg.

Så langt er potensielle spørsmål kategorisert i temabolker. Dette gjør at flere av spørsmålene overlapper noe. Samtidig kan det være nyttig å se bakgrunnen for hvorfor man stiller de aktuelle spørsmål. I en eventuell undersøkelse må man uan-

[61] Les også Solbergs kronikk i Aftenposten, 14. juni 2004: "Bør vi innføre elektronisk stemmegivning?"

sett begrense seg og plukke et utvalg spørsmål som gir et godt grunnlag for å vurdere brukernes holdninger og modenhet for en fremtidig PKI-utrulling.

6 Metodevalg og utfordringer

6.1 Metode og spørsmål

Før en går i gang med en forbrukerundersøkelse er det viktig å få klarhet i hvilken metode man ønsker å benytte og hvorfor. Det er i hovedsak to måter å gå frem på i en samfunnsvitenskapelig metodevurdering; kvalitativ og kvantitativ metode. Den første metoden innebærer som oftest dybdeintervjuer med respondenter som er trukket ut fordi de virker spesielt interessante for formålet. I kvalitativ metode kan en også observere eller benytte fokusgruppeintervjuer. I kvantitativ metode er det gjerne vanlig å gjennomføre en survey (enquête) med et større utvalg respondenter. Ettersom man ønsker svar fra mange personer er det fornuftig å ha en strukturert intervjuguide og gjennomføre undersøkelsen over telefon eller via Internett.

Spørsmålene en stiller i en undersøkelse kan deles inn i ulike kategorier avhengig hva slags svar man ønsker eller forventer i en gitt situasjon. En kan benytte flere typer spørsmålsgrupper i samme undersøkelse dersom en ser seg tjent med det. Her er det et par momenter å huske på:

- Kognitive spørsmål: Dette er spørsmål som stilles dersom man ønsker kjennskap til individenes faktiske atferd og "harde fakta". I en slik sammenheng ønsker man gjerne å teste individenes kunnskap og viten om et spesielt fenomen.

- Evaluative spørsmål: Dette er spørsmål der man er ute etter holdninger, meninger, tro, verdier og ulike motiver for atferd og holdinger.

- Tidshorisont: Ønsker man spørsmål om forhold knyttet til fortid, nåtid eller fremtid.

Hvordan man formulerer spørsmål i en undersøkelse har også stor innvirkning på de svar man får. I utgangspunktet bør man trakte etter svar dannet på et mest mulig objektivt grunnlag, og dermed er det viktig å unngå "ledende" spørsmålsformuleringer. Problemer som kan dukke opp når det gjelder formulering av spørsmål kan være:

- Ledende eller annen type spørsmålsformulering kan gi uriktige svar.

- For lange spørsmål blir ofte upresise og kan gi rom for flere tolkningsmuligheter.

- Svaralternativene passer ikke til de spørsmål som er stilt.

De krav en bør stille til spørsmålsformuleringer er dermed at:

- Spørsmålene må være lette å forstå.
- En må unngå flertydigheter i formuleringen.
- Det bør ikke stilles ledende spørsmål, og en bør balansere disse.
- Det er også en erkjennelse at holdningsspørsmål, og spørsmål om "fremtiden", er mer problematiske enn rene fakta- og atferdsspørsmål.

6.2 Reliabilitet og validitet

Et annet viktig moment er å sikre reliabilitet og validitet i undersøkelsen. Reliabilitet går på å sikre at de data som samles inn er *pålitelige og nøyaktige*. Kan vi stole på at datainnsamlingen er gjennomført på en mest mulig korrekt måte? Validitet på sin side går ut på å sikre at de data som samles inn er *relevante* for problemstillingen som danner grunnlaget for selve undersøkelsen.

Hellevik (1991) beskriver to plan i forskningsprosessen. Når man skal formulere en problemstilling eller tolke resultatene av en undersøkelse er forskeren på teoriplanet. Selve datainnsamlingen og behandlingen av data derimot foregår på empiriplanet.

Det er viktig at begrepsbruken på de to plan samsvarer – og den *definisjonsmessige validiteten* avgjør hvor godt samsvaret er mellom den teoretisk definerte variabelen og den operasjonelt definerte variabelen. *Reliabiliteten* sier noe om samsvaret mellom den operasjonelle variabelen og de data som samles inn. Til slutt sier samsvaret mellom den definisjonsmessige validiteten og reliabiliteten noe om *datas validitet*.

Det har i de siste årene vært debatt rundt hvorvidt reliabiliteten og validiteten er god nok når man trekker utvalg i sammenheng med Internett[62]. Dersom utvalget som trekkes er foretatt ved sannsynlighetsutvelging (ikke selvseleksjon), der utvalget baseres på en kjent populasjon (eller univers) hvor respondentene har lik sannsynlighet for å bli trukket ut, skulle ikke dette by på problemer. Poenget her er at respondentene, som gjerne deltar i et panel over lenger tid, ofte rekrutteres over telefon, for så å få tilsendt linker til undersøkelser online. Her kan en bare generalisere tilbake til Internett-befolkningen og ikke befolkningen som helhet.

6.3 Utvalg og univers

I en undersøkelse av norske forbrukere er det viktig å vite hva slags utvalg man ønsker til undersøkelsen. Dersom man er opptatt av å "fange" hele befolkningen og sikre representativitet i undersøkelsen, er det *teoretiske universet* alle norske innbyggere. Ut fra dette universet trekkes et utvalg, og de data som hentes inn fra utvalget kan dermed analyseres og generaliseres tilbake til det teoretiske universet – altså den norske befolkning.

Når det trekkes et utvalg kan det forekomme avvik fra universet som enten skyldes tilfeldigheter, eller som er av systematisk karakter. Respondenter som rekrutteres

[62] Blant annet debatt i Analysen – Organ for norsk markedsanalyse forening, nr. 2 – juni 2001

ved *selvseleksjonen* eller tilfeller der forskeren bruker *skjønn*, kan være eksempler på systematiske avvik i utvalgsprosessen.

Det som er avgjørende er at man benytter en form for *sannsynlighetsutvelging*. Det vil si at det benyttes utvalgsteknikker med den egenskap at alle enheter i universet har en *kjent* sannsynlighet for å komme med i utvalget. Forutsetningen er at en da kan stille opp en fullstendig universliste (gjelder ikke for klyngeutvelging). Hovedteknikkene for dette er (Hellevik 1991):

- Enkel tilfeldig utvelging: dette er en loddtrekningsmekanisme der enhetene er nummerert. Alle enhetene har en lik sannsynlighet for å blir trukket ut og komme med i utvalget. I tillegg har alle kombinasjoner av enheter (med en gitt størrelse) lik sannsynlighet for å bli trukket ut.

- Systematisk utvelging: her plukkes enhetene ut med et visst intervall, gitt at en benytter et tilfeldig startpunkt. For eksempel kan hver 5. enhet trekkes ut. Her har alle enheter lik sannsynlighet for å trekkes ut, men ikke alle kombinasjoner av enheter har lik sannsynlighet.

- Stratifisert utvelging: enhetene i universlista grupperes sammen i ulike kategorier (strata). Kjønn kan for eksempel være en stratifiseringsvariabel. I en proporsjonal stratifisert utvelging er forholdet mellom gruppene representativt for fordelingen i universet. Dette er ikke tilfellet i en disproporsjonal stratifisert utvelging.

- Klyngeutvelging: her benyttes ei liste over klynger som enhetene skal grupperes i. Det er ikke enhetene som skal undersøkes direkte, men heller grupper, gjerne representert ved geografiske områder. Er det snakk om kommuner, lages ei liste over alle kommuner. På basis av denne lista kan en velge en utvalgsmetode og så trekke utvalget. En kan gjerne foreta uttrekkene i flere trinn.

Alternativet til sannsynlighetsutvelging er *ikke-sannsynlighetsutvelging*, slik som skjønnsmessig utvelging, selvseleksjon, slumpmessig utvelging og kvoteutvelging. Ingen av disse metodene er å anbefale i vårt tilfelle. Her er sjansene for å få systematiske avvik store. Ved å la tilfeldighetene råde i utvalgsprosessen sikrer en seg mot systematiske avvik.

Andre momenter en må ta hensyn til når en stiller spørsmål er å identifisere hvem analyseenhetene er; er det individer eller husholdninger, og deretter bør en vurdere hvem i husholdet som vil være ”gode informanter” på vegne av husholdet.

Et av de viktigste elementene å tenke på i en undersøkelse er hvilke data en faktisk trenger for å gjennomføre de analysene en ønsker. Og hva får vi egentlig svar på når vi spør?

6.4 Hvilken metode bør velges?

Målsetningen med undersøkelsen er å identifisere hvor norske forbrukere står i forhold til en fremtidig *Public Key Infrastructure* som tilrettelegger for elektronisk signatur og legitimasjon. Og hva må til for at forbrukerne skal endre holdning og adoptere denne teknologien? Dessuten er det viktig å vite hva slags PKI-tjenester forbrukerne vil ha.

I dette tilfellet virker det fornuftig å foreta en metodetriangulering, men kostnader er selvsagt avgjørende i så måte. I en metodetriangulering benytter vi oss både av kvantitativ og kvalitativ metode. Kvantitativ metode sikrer bredde i svarene, og dersom vi benytter oss av et representativt utvalg av den norske befolkning (eller av *Internett-befolkningen)*, kan vi generalisere svarene tilbake til dette universet.

Fordelen med å inkludere kvalitativ metode er at en kan få bedre innsikt i enkeltforhold knyttet til PKI. Dersom det er noe man ønsker å vite mer om gir kvalitativ metode en mulighet for å gå i dybden og dermed sikre innsikt i de enkelte respondentenes motivasjon for holdninger og atferd. Her kan det benyttes enten individuelle intervjuer, intervjuer med husstander eller fokusgrupper.

I fokusgrupper samles gjerne 6 til 10 personer for å samtale om et spesielt emne. Disse har ikke kjennskap til hverandre på forhånd, men en viss homogenitet i gruppen kan være ønskelig. Diskusjonsformen er ikke spesielt strukturert og med denne åpenheten forsøker man å fange inn gruppens reaksjoner og holdninger i forhold til visse tema eller problemstillinger. En moderator står for selve ”intervjuingen” og kommer med nye emner, samt at han/hun passer på å holde samtalen i gang og på rett spor. Fokusgruppen gir en fin gruppedynamikk selv om gruppen er kunstig sammensatt for et temabasert formål.

I et kvantitativt undersøkelsesopplegg (survey) burde det i utgangspunktet fokuseres på befolkingen som helhet, fordi dette kan gi det rikeste materialet. En kan få innblikk i hvordan ”de som står utenfor” ser på Internett-utviklingen og på *hvorfor* disse brukerne står utenfor. Er det kompetanse, tid, kostnader, eller følelse av utrygghet med mediet som gjør at Internett ikke er blitt tatt i bruk? Samtidig er det viktig i PKI-sammenheng å favne de som ikke benytter PC og Internett, fordi disse likevel kan tenkes å benytte infrastrukturen gjennom smartkort i terminaler i sentrum av kommuner og liknende. I et slikt tilfelle vil telefonbasert survey være fornuftig, eventuelt en postal survey.

På den annen side er det nå så mange som benytter Internett, og tendensen viser en utjevning med tanke på alder og kjønn. Dessuten er PKI aller viktigst i sammenheng med en hel-elektronisk saksgang, og i et slikt tilfelle må man nødvendigvis være bruker av PC/ Internett. Utviklingen går i retning av at *Internettbefolkningen* på mange områder stadig blir likere den faktiske befolkningen i landet, selv om det fremdeles kan være markante forskjeller på enkelte områder.

Ved å henvende seg til Internettbrukere vil man i tillegg tilgjengeliggjøre en kvantitativ datainnsamlingsmetode der respondentene kan gjennomføre undersøkelsen over Internett. For å få et representativt utvalg av *Internett-befolkningen* bør man ha et utvalg på mellom 500 og 1000 personer. I et online panel blir deltakerne kompensert for deltakelsen, men de er vanligvis ikke selvrekruttert. Deltakerne blir gjerne rekruttert tilfeldig over telefon og det lagres en del bakgrunnsinformasjon om deltakerne (som oppdateres jevnlig), slik at man slipper å spørre om dette i selve undersøkelsen. Typisk bakgrunnsinformasjon vil være demografi, livsstil og medie- og Internettvaner. Man kan også følge individene videre over tid (noe frafall) og man kan fokusere på enkeltgrupper (som f.eks kvinnelige brukere). Slike undersøkelser kan i tillegg gjennomføres på kort tid relativt til telefon- eller postale undersøkelser.

7 Workshop

Som en avsluttende øvelse i forbindelse med grunnlagsdokumentet ble det gjennomført en workshop i regi av PKI Forums forbrukergruppe. Denne workshopen ville gi aktører i PKI Forum anledning til å komme med innspill til metode, gjennomføring av en eventuell spørreundersøkelse og konkretisering av relevante temaer og spørsmål. I forkant av workshopen ble en foreløpig versjon av dette grunnlagsdokumentet sendt ut til relevante parter slik at man bedre kunne forberede seg til møtet.

Workshopen ble innledet med en gjennomgang av Forbrukergruppens formål og mandat ved gruppeleder Per Myrseth. Gjennomgangen ble lagt frem med følgende prioriteringer:

- Klargjøre mål og fremgangsmåte for dagen
- Kort gjennomgang av forbrukergruppas grunnlagsnotat
- Orientering om aktuelle undersøkelsesmetoder
- Identifisere tema om forbrukere
- Identifisere sammenhenger mellom tema som kommende datagrunnlag skal kunne gi svar på
- Prioritere tema
- Oppsummering og diskusjon om veien videre

Videre ble grunnlagsdokumentet presentert i kortfattet versjon ved Dag Slettemeås. Denne gjennomgangen hadde følgende mal:

- Forbrukerperspektivet
- Tidligere undersøkelser
- Bankkort-utrullingen på 90-tallet – en analogi
  - » pluss sentrale forbrukerforhold
- Spørsmålskategorier
- Metodevalg

Workshopen bar preg av relativt fri diskusjon og ”brainstorming” for å komme frem til velformulerte og valide spørsmålstema. Likevel ble det holdt en viss struktur på diskusjonen ved at man hadde visse hovedkategorier å forholde seg til. Her var to tilnærminger presentert. Disse to tilnærmingene fungerte som rettesnorer underveis i workshopen:

1) Inndeling etter ulike hovedvariabler:

- Demografi:
  - Alder, kjønn, bosted, yrke, utdanning
- Psykografi:
  - Sportsinteressert, friluftsengasjert, idealist, aktiv innen humanitært arbeid, teknolog

- Adferd:
  - Hyppighet på Internettbruk, erfaring med bruk av Internett, erfaring ved elektronisk handel, bruk av kort på nett
- Holdninger:
  - Forbrukers syn på dagens status (tillit, tjenestetilbud, vanskelighetsgrad, etc)
- Forventninger:
  - Holdninger til egen fremtidig adferd eller til de tilbud en antar eller ønsker vil komme
- Tjenester:
  - Hvilke tjenester ønsker forbrukere, når ønsker de tjenestene (tidshorisont), hvor sterkt ønsker de tjenestene.

2) Inndeling etter hovedtema presentert i grunnlagsdokumentet:

- Borger / forbrukerrelaterte spørsmål:
  - offentlige og private tjenester i samspill…
  - Infrastruktur versus tjenester…
- Påvirkning fra ytre / eksogene faktorer:
  - spesielt med tanke på personvern…
- Markedsføring av PKI – hvordan kommunisere PKI og tjenester:
  - hva trenger man å vite – hva vil man vite…
  - fokusering av begreper…
- Hva er viktigst å få frem ved PKI-bruk (merverdi):
  - signering, sikkerhet, identifikasjon, etc – eller satse på alt…
- Konkret på løsninger:
  - se på *faktisk bruk, ønsket bruk ut fra konkrete problemstillinger, etc.*
- Hvordan belyse betalingsvillighet?
  - forskjell på offentlige og private tjenester
  - oppfatninger om hvem som tjener på PKI og dermed bør ta kostnad, etc.
  - Prismodeller: årsavgift, pris per transaksjon, etc
  - Effekt av at man er vant til at ting er ”gratis” på nett…

Det ble til at gruppen i stor grad fulgte inndelingen i punkt 1) og etter grundig diskusjon ble korte anbefalinger til spørsmålstema lagt direkte inn i presentasjonsmaterialet. Utfallet av dette presenteres i tabellen nedenfor.

Atferd	Atferd relatert spesielt til Internettbruk - Erfaring med bruk av Internett - Erfaring ved elektronisk handel - Bruk av kort på nett - Hva er terskelen for at ikke-nettbrukere skal bli nettbrukere? - Hvorfor slutter noen å benytte teknologien? - Hva brukes nettet til (knyttes mot PKI)? - Holdninger til det å legge igjen personalia, kredittkort og lignende - Mobilerfaring, mobilhandel
Holdninger	Forbrukers syn på dagens status (tillit, tjenestetilbud, vanskelighetsgrad…) - Vil man gjøre x på nettet hvis det var mulig? - Kriterier for valg, forutsetninger for å endre adferd, gevinster?

	- Hva hindrer en i å gjøre det? - Viktighet av mobilitet, kunne gjøre tjenesten på ulikt utstyr - Er det viktig at den elektroniske ID'en kan brukes på ulike tjenester eller gjenbrukes? - Følelse av trygghet / utrygghet ved å bruke Internett, email, MSN - Tillit til teknologi og tjenester basert på faktisk erfaringer eller informasjon - Behov for tillit, versus adferd ved å sjekke tillit - Kan gevinster / premier gi endret risikoadferd? - Kan gevinster gi endret holdning til personvern, reklame, det å avgi informasjon om seg selv eller andre? - Kalkulert risiko eller uvitenhet? - Er nytteverdi vesentlig for å være nettbruker? - Brukervennlighet versus sikkerhet - Ved problemer, hvor lang tid tar det før en benytter tjenesten på nytt?
Foreventninger	Fremtidige holdninger til egen adferd eller til de tilbud en antar/ønsker vil komme - Gjenbruk av eID - Signatur på nett gir bindende avtaler - Ved skjemautfylling på nett, forventer man at en innsending er juridisk bindende - Elektronisk ID skal gi mulighet for gjenbruk / preutfylling av kjente data i ulike tjenester - "Min side" arkiv over digitale signerte dokumenter - Tilsyn som bistår forbrukere med deres interesser overfor tjenestetilbydere - Brukere har og vil ha liten kompetanse på teknologi og sikkerhet - Forventer om at "ting går greit" - Bedre brukervennlighet - Kan man bruke privat ID i jobbsammenheng?
Tjenester	Hvilke tjenester ønsker forbrukere, når ønsker de tjenestene (tidshorisont), hvor sterkt ønsker de tjenestene - Se undersøkelse fra Gallup, August 2004 (Meyer)
Diverse	Diverse tema hvor vi bør vite noe om forbruker og borgeres holdninger - Personvern - Aggregerte tjenester og produkter - Utstrakt bruk av underleverandører gjør at forbrukere ofte må forholde seg til en mengde aktører i relasjon til hver enkelt transaksjon - Hvis problemer eller feil, hva forventes av hjelp og assistanse? (teknisk, misbruk, vare ikke levert, søknad ikke kommet frem…) - Hva er minimum av hva en forbruker versus en borger bør vite om tillit, sikkerhet, PKI? - Hva forventes av brukere i forbindelse med å oppdage evt. misbruk eller feil? - Betalingsvilje, hva gjør at forbrukere har betalingsvilje for kostnadene ved PKI? - Hva slags utstyrskrav er forbrukere tjent med? - Brukervennlighet, hva gjør brukere hvis PKI blir for lite brukervennlig? - Hvordan skal forbrukere validere mottatte signerte dokumenter? - Hvordan bør en håndtere arkivering av signerte dokumenter for forbrukere og borgere, hva vil være i forbrukernes interesser?

Litteratur

Aune, Ann Inger og Ingrid Annita Rosvold (2003): *Digitale signaturer – og standardiserte løsninger.* IF 298 Bacheloroppgave, Høgskolen i Nord-Trøndelag.

Berg, Lisbet og Elling Borgeraas (2004): *Hindringer for mobilitet i bankmarkedet.* SIFO fagrapport nr. 2 – 2004.

Collingridge, D. (1980): *The Social Control of Technology.* London: Francis Pinter Ltd.

Datatilsynet (2002): *Risikovurdering av informasjonssystem – med utgangspunkt i forskrift til personopplysningsloven.* 15.02.2002

Datatilsynet (2004): *Personvernrapporten* - Datatilsynets årsmelding til AAD "med ny vri", Oslo, april 2004. Tilgjengelig på www.datatilsynet.no

Frønes, Ivar (2002). *Digitale skiller: utfordringer og strategier.* Bergen: Fagbokforlaget.

Hellevik, Ottar (1991): *Forskningsmetode i sosiologi og statsvitenskap.* Oslo: Universitetsforlaget.

Høykom-rapport 406 (2004): *Digital signatur/PKI – erfaringer og løsninger fra Høykomprosjekter.*

Information Security Committee: *PKI Assessment Guidelines.* Ref.: American Bar Association - http://www.abanet.org/scitech/ec/isc/pag/pag.html

Jacobsen, Eivind (1990): *Kommer forbrukeren til kort? – om forbrukerinteresser og elektroniske betalingskort.* Paper til Nasjonal sosiologisk fagkonferanse Geiranger, Norge. 9-13 mai, 1990.

Jacobsen, Eivind (1992): *Veksling mellom spill – når bankene spiller kort.* SIFO paper, januar 1992.

Jacobsen, Eivind (1993): *Technological Money. A theoretical account of consumers' dealings with electronic debet cards.* Paper for the Fourth National Sociology Conference. Department of Sociology and Political Science. Røros Hotell, Norway. June 17-20, 1993.

Luhmann, Niklas (1999): *Tillid – en mekanisme til reduktion af social kompleksitet.* København: Hans Reitzels forlag. (Basert på orginalutgave av 1973: *Vertrauen. Ein Mechanismus der Reduktion Sozialer Komplexität.* Stuttgart: Ferdinand Enke Verlag.

Luhmann, Niklas (1988): “Familiarity, Confidence, Trust: Problems and Alternatives”. I D. Gambetta, red., *Trust. Making and Breaking Cooperative Relations.* New York: Basil Blackwell Inc.

Mitchell, J. (1988): ”Electronic funds transfer at point of sale: a consumer viewpoint”. I *Journal of Consumer Studies and Home Economics,* 12.

NHD: (2003): *e-Norge - Nasjonal strategi for informasjonssikkerhet. Utfordringer, prioriteringer og tiltak.* Juni, 2003.

NOU 2001:10: *Uten penn og blekk. Bruk av digitale signaturer i elektronisk samhandling med og i forvaltningen (Nærings- og handelsdepartementet).* Oslo: Statens forvaltningstjeneste.

NOU 1997:19: *Et bedre personvern – forslag til lov om behandling av personopplysninger (Justis- og politidepartementet).* Oslo: Statens forvaltningstjeneste.

Nysveen, Herbjørn & Per E. Pedersen (2004): *Consumers’ willingness to pay for services in digital networks – A literature review.* SNF Working Paper No. 04/2004.

PKI-Forum: *Strategi for en samfunnsinfrastruktur for elektronisk signatur og elektronisk ID i Norge.* 20.juni 2002

Rogers, E. (1983): *Diffusion of Innovations, Third Edition.* New York: The Free Press.

Slettemeås, Dag (2002): *Høyforbruk – Forbrukerbehov som utgangspunkt for offentlig etterspørsel og markedstilbud.* SIFO oppdragsrapport nr. 3 – 2002.

Slettemeås, Dag et. al. (2002): *Det interaktive reiseliv. Samtykkebasert markedsføring av reiselivstjenester med fokus på forbrukernes tillit.* SIFO oppdragsrapport nr. 8 – 2002.

Slettemeås, Dag og Jo Helle-Valle (2003): *Forbrukerne og utvikling av bredbånd i Norge – fra borger til kunde?* SIFO oppdragsrapport nr. 6 – 2003.

Teknologirådet (2004): *Holdninger til personvern. Rapport fra fokusgrupper om elektroniske spor og personvern.* Teknologirådet rapport 1, februar 2004

Annen relevant litteratur

Beck, Ulrich (1992): *Risk Society. Towards a New Modernity.* London: SAGE Publications Ltd.

Camp, L. Jean (2000): *Trust and risk in Internet commerce.* Cambridge, MA: MIT Press.

Chadwick, Scott A. (2001): "*Communicating Trust in e-commerce Interactions*". Management Communication Quarterly, Vol. 14, No.4, May 2001 (653-658). Sage Publications, Inc.
URL: http://www.hartman-communicatie.nl/Nieuws/Nieuws_2001_08_SC.htm 10.06.03.

Dasgupta, P. (1988): "*Trust as a commodity*". Gambetta, D. (red.): "*Trust. Making and breaking cooperative relations*". New York: Basil Blackwell Inc.

Dulsrud, Arne 2002 "*Tillit og transaksjoner – en kvalitativ analyse av kontraktsrelasjoner i norsk hvitfiskeksport*". SIFO fagrapport nr. 2-2002

Einwiller, Sabine; Will, Markus (2001) "*The Role of Reputation to Engender Trust in Electronic Markets"*. Proceedings of the 5th Int. Conference on Corporate Reputation, Identity and Competitiveness, May 17.19, 2001, Paris, France.
URL:http://www.informationobjects.ch:8080/NetAcademy/naservice/publications.nsf/all_pk/1869 01.06.03

Fukuyama, Francis (1998): "*The Virtual Handshake: E-commerce and the Challenge of Trust".* The Merill Lynch Forum, 1998 Merill Lynch & Co., Inc.
URL: http://www.ml.com/woml/forum/pdfs/ecommerce.pdf 03.03.03

Giddens, Anthony (1994): "Replies and Critiques. Risk, Trust, Reflexivity". I U. Beck, A. Giddens & S. Lash (reds.): *Reflexive Modernization: Politics, Tradition and Aesthetics in Modern Social Order. Cambridge:* Polity Press.

Grabner-Kraeuter, Sonja (2002): "*The Role of Consumers' Trust in Online-Shopping"*, Journal of Business Ethics 39: s.43-50, 2002.
URL: www.ifi.uni-klu.ac.at/IWAS/HM/eBusiness/doc/Grabner_Kraeuter_2002.pdf 27.05.03

Grabner-Kraeuter, Sonja & Kaluscha, E. A. (2003): "*Empirical research in on-line trust: a review and critical assessment*". International Journal of Human-Computer Studies 58 (2003). URL: www.sciencedirect.com

Lagerspetz, O. (1996): "*The tacit demand: a study in trust".* Åbo: Filosofiska institutionen.

Mordal, Tove (2003): *Faktorer bak en vellykket e-handel.* I TemaNord-serien (in print).

Tepfers, C. og C. M. Davidsen (2001): ”*Konsumentkrigen”.* Oslo: J. W. Cappelens Forlag AS.

Tokvam, Ole. E. red. (1996): *”Elektronisk marked”.*
URL: http://www.jus.uio.no/iri/lib/rapporter/elektronisk_marked/index.html 01.06.03

Torsvik, G. (2000): ”*Tillit og økonomi*”. Sosiologi i dag – Årgang 30 nr.3-2000 s.13-30. Oslo: Novus Forlag.

Vedlegg

Forslag til spørsmål – PKI forbrukerundersøkelse:

Demografiske spørsmål:

a. Alder
b. Kjønn
c. Sivilstand
d. Bosted (kommunenummer)
e. Utdanning
f. Yrke (kategorier)
g. Inntekt

Internett:

1. Har du tilgang til Internett? Hvis ja, hvor?
- hjemme
- jobb
- andre steder (eks. skole, kafé)

2. Hva slags Internettilknytning har du hjemme?
- analogt modem
- ISDN-linje
- ADSL eller annet bredbånd

3. Hva slags Internettilknytning har du på jobb?
- analogt modem
- ISDN-linje
- ADSL eller annet bredbånd

4. Når begynte du å bruke Internett (regelmessig)?
- hvilket år (cirka)?

5. Hvor mange timer bruker du på Internett hjemme hver uke?
- 0-2 timer
- 3-6 timer
- Over 6 timer

6. Hvor mange timer bruker du på Internett på jobb hver uke?
- 0-2 timer
- 3-6 timer
- Over 6 timer

7. Hva bruker du Internett til, og hvor mye benytter du disse tjenestene? (sjeldent, av og til, ofte)
- e-post
- surfe
- informasjon (aviser etc)
- underholdning
- nettbank
- netthandel
- offentlige tjenester

8. Dersom du handler på nett, benytter du som regel kort (Visa, andre) eller postoppkrav?

9. Har du noen gang blitt svindlet på nett?

10. Hvis ja, på hvilke måte? Velg en eller flere av alternativene nedenfor.
- Min bankkonto ble tappet etter at kredittkortnummeret mitt ble lagt ut på et nettsted
- Jeg mistenker at personlig informasjon har lekket fra et nettfirma ettersom jeg får tilsendt e-post (evt. annen markedsføring) som er tilpasset meg.
- Min identitet har blitt misbrukt. Jeg tror / er sikker på at dette har skjedd etter at jeg har lagt ut mine data på nettet.
- (eventuelt andre kategorier)

11. Hvis nei, har du opplevd andre forhold som har gjort deg skeptisk til nettbruk eller netthandel? – beskriv kort (åpent felt evt. alternativer)

Registrering og autentisering:

12. Benytter du autentisering ved bruk av passord eller pinkoder på Internett?
- Ja – én til hver tjeneste
- Ja – men samme passord går ofte igjen
- Ja – og jeg har forskjellige passord til nesten alle tjenester
- Nei – benytter få tjenester med passord
- Nei – benytter aldri tjenester med passord

13. Hvor mange passord / pinkoder benytter du totalt i din hverdag, både på nett og ellers? (Eks.: bankkort, nettreisebyrå, arbeidsplass, etc)
- 0-5
- 5-15
- 25-50
- over 50

14. Hva er din holdning til passord på nett?
- Ikke noe problem – har ingen passord på nett
- ikke noe problem – har få passord på nett
- Ikke noe problem – har funnet et system som fungerer for meg
- synes det er for mange passord å holde styr på

15. Ville det vært fornuftig å ha ett autentiseringssystem å forholde seg til?

16. Er du på det nåværende tidspunkt registrert som bruker/medlem av et nettsted?

- Ja
- Nei
- Ikke relevant

17. Ta stilling til om du syns det er for mye personlig informasjon som må legges inn på nettsteder i forhold til det du skal utføre, generelt sett?
    1 Helt enig
    2 Enig
    3 Usikker
    4 Uenig
    5 Helt uenig
    6 Har ikke noe forhold til det

18. Har krav til for mye informasjonsavgivelse ført til at du har avbrutt en registrerning?

19. Har krav til for mye informasjonsavgivelse ført til at du har lagt inn ukorrekte data om deg selv?

20. Føler du deg generelt sett kompetent som nettbruker? (gradering)

21. Dersom ikke, hva er grunnen til dette?
- Har ikke behov for mye internettkunnskap, bruker nettet lite
- Har ikke tid til å sette meg inn i det
- Nettsidene er for vanskelige å bruke

22. Synes du det er vanskelig å være nettbruker? (ja/nei)

23. Dersom ja, vurder følgende to påstander:
- Jeg savner brukeropplæring i Internettbruk
- Dette noe jeg bør klare selv

24. Dersom du ønsker slik opplæring, hvordan bør den foregå?
- Annonse med enkel informasjon
- Et nettsted for enkel læring (eLæring)
- Informasjonsskriv i posten

Elektronisk identifikasjon og signering:

En elektronisk ID gjør at du kan legitimere deg, logge deg på ulike tjenester og signere dokumenter på Internett uavhengig av om dette gjelder offentlige eller private tjenester.

25. Er det viktig for deg at du får tilgang til en slik løsning for ditt bruk?
- Nei, det fungerer bra med de løsninger som eksisterer i dag
- Ja, det har jeg behov for nå
- Ja, men ikke akkurat nå. Over tid er det interessant.

26. Bruk av én og samme elektronisk ID kan gi deg pålogging mot mange ulike tjenester. Ta stilling til påstandene nedenfor og gi svar fra helt uenig til helt enig (5 graderinger)
- Dette virker effektivt og passer meg bra
- Jeg synes det er bedre å ha flere ID'er slik at man kan spre risikoen dersom noe skulle skje med den ene.

- Det bør være flere ID'er med ulike sikkerhetsnivåer tilpasset ulike tjenestekategorier.

27. Virker det fornuftig med en felles løsning for både offentlige og private tjenester, eller bør man skille disse nivåene?
- Bra med én løsning som kan brukes til alt (borgerkort)
- Bedre med én for offentlig sektor og én for privat sektor
- Bedre med f.eks én "handels-ID" (netthandel), én "bank-ID" (transaksjoner) og én "offentlig ID" (offentlige tjenester, pass, etc)

28. Virker det positivt eller negativt at f.eks et privat selskap kan gi deg en elektronisk ID som du også kan bruke til offentlige tjenester?
- Positivt
- Negativt

29. Har du benyttet offentlige tjenester der du må legitimere deg, eventuelt signere digitalt?

30. Hvis ja, hvilke tjenester?
- Byggsøknader
- Barnehageplass
- Selvangivelsen
- Lånekassa
- Andre

31. Er en signatur på nett like bindende som en håndskrevet signatur?
- ja det er den
- vet ikke, men det burde den være
- nei det er den ikke
- vet ikke, men den burde ikke være det

32. Dersom du måtte oppgradere PC og programvare for å kunne ta i bruk en slik elektronisk ID, ville du da ha oppgradert?
- ja
- nei, ville ikke brukt penger på det
- nei, ville ikke benyttet en slik ID i det hele tatt

33. Dersom du skulle ta i bruk elektronisk ID, ville du da hatt et eget arkiv for dine elektronisk signerte dokumenter og kontrakter?
- nei
- ja, ville hatt det på min PC
- ja, ville hatt mulighet til å kontakte en offentlig instans for å få denne oversikten
- ja, vil ha dette hos den som er ansvarlig for min ID
- ja, jeg ville hatt denne hos en nøytral tredjepart, en notarius av noe slag.

34. Dersom noe skulle gå galt i forbindelse med din elektroniske ID eller signerte avtaler, hvordan bør dette håndteres?
- bør ordnes opp med den aktør / bedrift / instans der problemet har oppstått
- bør være en bransjeorganisasjon som kan kontaktes
- bør være et offentlig tilsyn som har oversikt med denne type ting

35. Forventer du at en elektronisk ID som kan benyttes hos private aktører og offentlige instanser også bør kunne benyttes på jobben?

36. Hvordan bør en slik elektronisk ID helst være? (velg)
- et fysisk kort à la bankkort
- et sertifikat som ligger på pc'ene
- et SIM-kort så jeg kan bruke mobilen min

37. Ville det vært best å ha én elektronisk ID her eller muligheten til å ha alle ID'er tilgjengelig (kort, sertifikat på PC, SIM-kort)?
- Én elektronisk ID
- Flere ID'er avhengig av hva slags teknologi jeg benytter

38. Hvis elektronisk ID ble tilgjengelig for alle borgere, til alle typer tjenester, hva slags informasjon ville du ønske deg? (fra lite viktig til svært viktig for alle alternativer)
Fra hvem:
- kort og ryddig informasjon fra myndighetene
- informasjon fra de tjenestetilbydere jeg skal forholde meg til
Hva slags informasjon:
- informasjon om hva dette er for noe
- informasjon om hvordan jeg kan ta dette i bruk og komme i gang
- informasjon om de tjenester dette kan brukes til

39. Et slikt system for elektronisk identifikasjon og signering vil koste mye å etablere. Dersom brukerne må ta noe av kostnadene – hvordan burde disse innhentes?
- Gjennom at brukere betaler en avgift per år (som ved Visakort; kort = ca 250,- per år)
- Ved å betale en liten avgift for hver transaksjon (eks. 2 kroner for å signere et dokument)
- Gjennom å betale en engangsavgift (som ved passutstedelse; pass = 990,-)
- Vet ikke

40. Hvis du måtte betale slik det legges opp til ovenfor, ville du da vurdert å ta i bruk denne muligheten eller ikke? (Velg det alternativ som passer best):
- Ja, dersom satsene virker fornuftige og jeg har behov for tjenesten
- Nei, dette burde de som leverer tjenestene ta seg av.
- Nei, vil ikke betale noen ting. Alt på nett bør være gratis.
- Nei, i alle fall ikke nå. Men om noen år kan det være aktuelt
- Vet ikke

Mobiltelefon:

41. Har du mobiltelefon? (filter)

42. Har du hatt mobiltelefon lenge?

43. Hvor mye benytter du mobiltelefonen?
- tidsbruk per uke (cirka)

44. Benytter du den av og til til andre tjenester enn å ringe og sms'e med venner og kjente?

45. Dersom ja, til hva?
- nettbank
- parkering

- kinobilletter
- annet

46. Skulle du ønske du kunne benytte mobilen til flere typer tjenester?

47. Dersom ja, hvilke? (åpent felt eller alternativer)

Sikkerhet og personvern: (noe usystematisk)

48. Er du skeptisk til å legge igjen kortnummer på Internett?

49. Dersom skeptisk, medfører dette at du ikke handler på nett eller at du benytter andre muligheter som f.eks postoppkrav?
- gjør at jeg ikke handler på nett
- benytter andre betalingsmuligheter

50. Dersom skeptisk, er det avhengig av hvilken tjeneste / hvilket selskap du forholder deg til, eller gjelder for Internett generelt?

51. Er du skeptisk til å legge igjen persondata på Internett?
- ja, legger aldri igjen data om meg selv
- ja, men legger kun igjen der det er strengt nødvendig
- ja, stort sett, men ikke der det er selskaper jeg stoler på
- nei, gir ofte fra meg data om meg selv – stoler generelt sett på nettselskapene
- nei, gir ofte fra meg data om meg selv – stoler på min egen vurdering i hvert tilfelle
- ikke relevant

52. Føler du en avmakt i forhold til egne persondata, eller har du tiltro til at de selskaper du avgir informasjon til ikke sprer denne informasjonen videre?

53. Når du handler på Internett, sjekker du da følgende:
- hengelåsen nederst på nettsiden (SSL-kryptering)?
    - ja alltid
    - av og til
    - nei aldri – gidder ikke
    - nei aldri – vet ikke hva dette er
- om butikken er Nsafe-merket?
    - ja alltid
    - av og til
    - nei aldri – gidder ikke
    - nei aldri – vet ikke hva dette er
- leser personvern policy'en som skal være på nettsiden?
    - ja alltid
    - av og til
    - nei aldri – gidder ikke
    - nei aldri – vet ikke hva dette er

54. Har bedriftene lov til å gi informasjon videre til andre parter?
- ja
- ja, med mitt samtykke
- nei

55. Dersom du måtte gi fra deg informasjon til et **privat selskap**, hva slags informasjon ville være greit å gi fra seg?
- navn
- kjønn
- alder
- adresse
- inntekt
- betalingskortinformasjon
- type jobb
- telefonnummer
- interesser
- personnummer
- e-postadresse

56. Dersom du måtte gi fra deg informasjon til en **offentlig institusjon**, hva slags informasjon ville være greit å gi fra seg?
- navn
- kjønn
- alder
- adresse
- inntekt
- betalingskortinformasjon
- type jobb
- telefonnummer
- interesser
- personnummer
- e-postadresse

57. Dersom skeptisk, er du mer eller mindre skeptisk til å gi fra deg persondata på Internett enn i forhold til over telefon eller direkte til en kundebehandler?

58. Dersom skeptisk: Personopplysningsloven gir deg rett til å be en bedrift om å slette dine data fra deres register. Gjør dette forholdet deg mindre skeptisk til å levere ut informasjon om deg selv?

59. Dersom nei; hvorfor ikke?
- Vet ikke om de faktisk sletter informasjonen
- Vet ikke hva slags data de har om meg
- Tror ikke bedriftene selv har full kontroll over alle data (for dårlig sikkerhet, håndtering av data)

60. Dersom du har mistanke om misbruk av persondata – hvem ville du kontakte da? (Åpent, men muligheter: nettstedet, politiet, Datatilsynet, Forbrukerrådet, andre)

61. Leser du hvilke rettigheter du har som bruker/medlem av et nettsted, generelt sett?
    1 Ja, ofte
    2 Av og til
    3 Nei, aldri

62. Hvor viktig er det for deg at et nettsted kan vise til en liste med medlemsrettigheter?
    1 Svært viktig
    2 Ganske viktig

3 Litt viktig
4 Ikke viktig
5 Har ikke noe forhold til det

63. Dersom for eksempel en nettbedrift har et *svært bra tilbud* eller noe som gjør at det er store muligheter for *gevinst* – ville du da vurdert å ta en noe større risiko enn normalt sett?

64. Ville du avgitt mer data om deg selv i et slikt tilfelle?

65. Bør myndigheter avgjøre hva slags data du kan gi fra deg til private / offentlige aktører eller bør du kunne vurdere dette selv?