

## **Kominn - Et sikkert eNorge**

### *Elektroniske sertifikater for sikker tilgang til nettbaserte offentlige tjenester*

*Versjon 1.1 - oktober 2003*

*av Plogen*

Offentlig sektor skal løse sine sikkerhetsbehov for elektroniske tjenester ved hjelp av elektronisk signatur og PKI (*Public Key Infrastructure*<sup>1</sup>). Løsninger basert på sertifikater har et stort fortrinn ved å realisere flere sikkerhetstjenester som offentlige elektroniske tjenester har behov for (autentisering, integritetssikring, konfidensialitet, ikke-benektning).

Regjeringens plan for *eNorge*<sup>2</sup> har som målsetning at forholdene skal være lagt tilrette for allmenn bruk av standardbaserte elektroniske signaturer innen utgangen av 2005. *Strategi for IKT i offentlig sektor 2003-2005*<sup>3</sup> og *Nasjonal strategi for informasjonssikkerhet*<sup>4</sup> slår fast at målsettingen skal nås ved å samordne innføring og bruk av elektronisk signatur og PKI i offentlig sektor. Plogen har mange års erfaring med PKI løsninger, og peker på vesentlige misforhold mellom myndighetenes strategi og det offentliges målsetting. Avslutningsvis summerer vi opp våre nøkkelpunkter for utbredelse av PKI.

### **Nåsituasjonen**

*Tilstandsrapport for eNorge*<sup>5</sup>, juni 2003, konkluderte med at *innføringen av elektroniske signaturer går saktere enn forventet*. Årsakene til at det går sakte er flere, men utbredelsen i forvaltningen har stor betydning.

Offentlig sektor, med mer enn 750.000<sup>6</sup> ansatte, er den dominerende aktøren i markedet. Utviklingen i markedet avhenger derfor i stor grad av hvordan offentlig sektor løser sine behov for elektroniske signaturer. Totalmarkedet preges i dag av forvaltningens avventende holdning. I tillegg finnes det praktiske og ikke minst regulatoriske forhold som hemmer innføring av PKI i større skala.

### **Markedets reaksjon på lovverket**

Lov om digitale signaturer pålegger den som utsteder sertifikater et betydelig ansvar. Aktørene i markedet søker å redusere risikoen knyttet til dette ansvaret. Utsteder (CA) av sertifikater kan blant annet:

1. Sette prisen på sertifikater så høyt at den reflekterer utsteders ansvar og risiko.
2. Inngå avtaler som fordeler ansvar og risiko mellom utsteder og brukersted, og sperre for bruk av utsteders sertifikater overfor andre enn avtalepartnere.
3. Velge å tilby ikke-kvalifiserte sertifikater som ikke medfører samme ansvar som kvalifiserte.

Markedets etterspørsel etter sertifikater er så lav at alternativ 1 i praksis er utelukket. Alternativ 2 brukes av alle kjente utstedere av kvalifiserte sertifikater. Et godt eksempel er ZebSigns brukeravtale, som slår fast at sertifikatnehaveren er ansvarlig for ikke å bruke sitt sertifikat overfor brukersteder som mangler avtale med ZebSign. Det fremgår ikke av avtalen

<sup>1</sup> For informasjon om PKI: <http://www.pki-forum.no>

<sup>2</sup> eNorge 2005, NHD, mai 2002

<sup>3</sup> Strategi for IKT i offentlig sektor, AAD, februar 2003

<sup>4</sup> eNorge, Nasjonal strategi for informasjonssikkerhet, NHD, juni 2003

<sup>5</sup> eNorge Tilstandsrapport, NHD, juni 2003

<sup>6</sup> Arbeidskraftundersøkelsen 2002, SSB, mars 2003

hvordan innehaveren kan beskytte seg mot å bruke sertifikatet i strid med avtalen. Utstedere som ønsker å utstede åpne sertifikater, velger alternativ 3. Posten Norge tilbyr gratis individualsertifikater, uten begrensninger på bruk, men sertifikatene er ikke-kvalifiserte.

Utfordringen for offentlig forvaltning er at ingen av de tre alternativene markedet foretrekker peker i retning av myndighetenes mål; en allmenn utbredelse av allment anvendbare, kvalifiserte sertifikater innen utgangen av 2005.

### **Offentlig forvaltning og det kommersielle markedet har ulike behov.**

PKI løser behov for autentisering, integritet, konfidensialitet og ikke-benektning i en og samme teknologi. Dette er utvilsomt viktig for offentlig sektor. Behovet er likevel ikke større enn at tunge offentlige aktører velger andre teknikker enn PKI. For eksempel Skattedirektoratet i sine publikumstjenester.

Privat sektor har ikke samme behov for å løse flere sikkerhetsbehov med en enkelt teknologi, og ønsket om samordnede løsninger er til tider diametralt motsatt. En nettbutikk ønsker enkel autentisering av kunder, men det er ikke selvfølgelig at en løsning som gjør det like enkelt å handle hos konkurrenten blir ønsket velkommen.

Kommersielle aktører legger liten vekt på at PKI faglig sett kan presenteres om et enkelt og brukervennlig verktøy. Publikum, kundene, viser ingen spesiell preferanse for PKI når de har anledning til å velge. Etter to års erfaring med Postens elektroniske ID åpnet Posten sine nettjenester for autentisering med PIN kode. Det er også tankevekkende at et voksende marked av nettbutikker nesten uten unntak velger andre løsninger på sine sikkerhetsbehov enn PKI.

Anvendelser for og utbredelse av PKI fremstår som et klassisk 'høna og egget' problem i offentlig sektor. Denne problemstillingen kan ikke generaliseres. Andre funksjonelle krav og redusert behov for samordnede løsninger er årsaken til at store deler av privat sektor velger andre løsninger enn PKI.

### **PKI alene er ikke nøkkelen til effektivisering av offentlig sektor.**

Hva skjer dersom en borger utrustet med et kvalifisert sertifikat sender en elektronisk henvendelse til forvaltningen? For Rikstrykdeverket og Skattedirektoratet, begge etater med omfattende publikumskontakt, er svaret enkelt. Etatene nekter deg å kommunisere elektronisk med din saksbehandler. Deler av statsforvaltningen hevder at barrièren med å skrive et brev på papir, putte det i konvolutt og postlegge det, er nødvendig for å hindre at etaten "drukner i henvendelser". Validiteten av et slikt syn er uvesentlig. Det er nok å slå fast at holdningen hemmer utbredelsen av PKI løsninger og en generell modernisering av forvaltningen.

### **Det offentliges sak- og arkivsystemer er i all hovedsak glemt.**

Lokalforvaltningen aksepterer og oppmuntrer til elektronisk kommunikasjon med borgerne. Her trer en annen utfordring frem, en utfordring som vil øke i omfang i takt med utbredelsen av PKI løsninger. Heller enn å effektivisere, kan bruk av kvalifiserte signaturer i dag medføre merarbeid for det offentlige. Sak og arkivsystemene i forvaltningen er lite forberedt på å ta imot henvendelser med kvalifisert elektronisk signatur, og det er i fag-, sak- og arkivsystemene nøkkelen til økt effektivitet og bedre service ligger.

Manglende fokus på arkiv- og saksbehandlingsmessige konsekvenser av PKI, kan i stor grad føres tilbake til kommersielle aktørers rolle og deres innsikt i forvaltningens behov. Plogen

har i tidligere analyser fremhevet kompetansen som finnes hos Riksarkivaren. Regjeringens ambisiøse mål frem mot 2005 krever at denne kompetansen mobiliseres nå.

### **Oppsummering**

Vi har sett at den relative stillstand som preger markedet for PKI løsninger i stor grad er en konsekvens av myndighetenes egne beslutninger.

- Regjeringens ønske om å ta en minimalistisk rolle overfor markedskreftene støter sammen med det faktum at det offentlige ikke kan løpe fra sin plass som markedets største aktør.
- Leverandørene på sin side opplever en uakseptabel kommersiell risiko knyttet til massespredning av sertifikater i privat sektor.

## **Nøkkelpunkter for utbredelse av PKI**

### **All fokus må være på utbredelse av teknologien**

PKI er ingen ny teknologi, umoden kanskje, men det skyldes manglende bruk, ikke fartstid i markedet. Flere store PKI prosjekter, også internasjonale, ble igangsatt i andre halvdel av 1990-tallet. Mangelen på suksess er påfallende. En generell erfaring er at “den perfekte PKI løsning” ikke sikrer utbredelse. Derimot er det lett å vise at manglende utbredelse gjør en hvilket som helst PKI løsning irrelevant.

### **Etabler folkesertifikatet**

Kun sentrale myndigheter kan gjennomføre PKI som felles sikkerhetsløsning på alle forvaltningsnivå, samt sikre et allment, ikke-diskriminerende sertifikattilbud for bruk i offentlige tjenester.

Folkesertifikatet er sertifikatet som gir alle borgere som ønsker det tilgang til flertallet av offentlige tjenester. Erfaringene med OCES i Danmark demonstrerer at folkesertifikatet er en billig og lett tilgjengelig løsning i forhold til de alternativer som diskuteres i Norge. Egenskapene til folkesertifikatet vil også fortelle et avventende marked hva det offentlige ønsker.

- **Krav til sertifikatenes innhold** – bla. innehaverens navn og adresse, samt den offentlige signaturnøkkelen.
- **Krav til utstedelse av sertifikater** – bla. hvordan mottakerens identitet skal sikres.
- **Krav til sertifiseringscenterets sikkerhet** – bla. krav til fremstilling, beskyttelse og oppbevaring av nøkler.

Et slikt folkesertifikat vil umiddelbart kunne benyttes for å autentisere kunder overfor et flertall av nettbutikker. De fleste nettbutikker har en brukerregistrering som lett kan erstattes av folkesertifikatet, mens betaling uansett skjer i en separat tjeneste.

### **Tilrettelegg offentlige tjenester for folkesertifikatet**

Alternative løsninger til PKI, som vi ser hos de store statsetatene, blokkerer myndighetenes mål for PKI i 2005. Det finnes ingen realisme i å hevde at PKI kan konkurrere ut alternative mekanismer i planperioden. Tvert imot, må det offentlige være forberedt på å bruke mild tvang for å nå sine egne målsettinger. Det kraftigste grep det offentlige kan ta er å kreve at elektronisk levering av selvangivelsen fra PC skal autentiseres med folkesertifikatet.

Sammenlignet med nær sagt alle andre offentlige anvendelser er dette enkelt å gjennomføre: det er en ren autentisering, - det kreves ingen inngrep i etatens saksbehandlingssystemer.

### **Oppsummering**

Det er vanskelig å se at myndighetene kan nå sine nasjonale ambisjoner gjennom enkeltstående, lokale prosjekter. Fyrtårnsprosjekter, som lyser opp når prosjektmidlene er bevilget og slukker når midlene tar slutt, skalerer ikke til nasjonale løsninger. Markedet trenger en satsing med et omfang som kan:

- etablere nasjonale standarder for offentlige tjenester og datautveksling.
- eksponere kostnadene for realisering av PKI-tjenester for hele offentlig sektor.

I Sverige betaler det offentlige helt opp mot 5 kroner for kontrolloppslag hver gang et sertifikat brukes. Blir prisleiet sammenlignbart i Norge? Det er to år til eNorge skal være lagt til rette for allmenn bruk av PKI. Vi kommer ikke dit før forvaltningen vet hva innføring og bruk av PKI vil koste.

### **Om Plogen**

Plogen er en norsk rådgivingsorganisasjon som tilbyr et bredt spekter av profesjonelle tjenester innen IKT.

<http://www.plogen.no>