

PKI og digitale signaturer

Sikkerhet har tallrike aspekter, mange av dem ute av syne for de fleste av oss. Samtidig har vi ved tidligere anledninger konstatert at usynlig sikkerhet som regel er det samme som dårlig eller ingen sikkerhet. Som så ofte ellers, handler det om å trekke grenser og å gjøre valg – som er optimale for formålet og virksomheten.

Å treffe slike valg blir ikke lettere når problemstillingene blir til selv-motsigelser. For eksempel trenger vi en PKI – *Public Key Infrastructure* – for å etablere pålitelige mekanismer for autentisering av brukere og sikker utveksling av informasjon. Sikringen gjelder imidlertid kun for parter som har tilgang til den samme PKI. Med mindre alle personer vi skal kommunisere med har tilgang til den samme PKI, er den med andre ord kun nyttig for intern kommunikasjon. Og dersom det kun er den interne kommunikasjonen som skal sikres, finnes det langt enklere løsninger enn å etablere en PKI.

Så – hvor skal vi begynne? Med høna eller egget? Mens målsettingen er enkel – å etablere god sikkerhet og høy pålitelighet, er veien til målet både kronglete og lang: En PKI er på den ene siden en forutsetning, og på den andre siden av beskjeden nytte.

PKI – kort og godt

En PKI er – i all sin kompleksitet – først og fremst en metode og mekanisme for utveksling av spesifikk informasjon innenfor et domene: En virksomhet, en kommune, et område, en bransje, et land, en verden. Det sentrale element er krypteringsnøkler: Med utgangspunkt i en såkalt asymmetrisk krypteringsalgoritme, utstedes personlige nøkkelpar til alle brukere – og til en rekke tjenester. Den ene nøkkelen er privat og personlig, den andre er offentlig og fritt tilgjengelig. Nøkkelparet – og algoritmen som ligger til grunn – fungerer slik at det som er låst (kryptert) med den ene, kun kan låses opp (dekrypteres) med den andre.

Effekten av denne asymmetrien er høyst interessant. Skal vi sende en melding til Hansen, sørger vi for å kryptere den med hans offentlige nøkkel. Siden den deretter kun kan dekrypteres med Hansens personlige nøkkel, kan vi være sikre på at – når den blir lest, er det av den riktige Hansen. I meldingen kan vi også inkludere vår signatur, kryptert med vår personlige nøkkel, slik at Hansen selv kan verifisere – ved hjelp av vår offentlige nøkkel – at det virkelig er vi som har sendt meldingen.

I tillegg til mekanismene er en PKI også en infrastruktur for å gjøre nøkler og annen informasjon tilgjengelig for brukere og programmer. Eksemplet er ett av mange på hvordan en PKI kan benyttes. Et annet og like viktig område er selve autentiseringen: Hvordan brukerne identifiserer seg overfor systemene og motsatt: Hvordan brukerne og deres programmer kan forsikre seg om at de kommuniserer med riktig tje-

neste, og ikke en 'impersonator' som er ute etter å skaffe seg informasjon (passord etc.).

Her er vi inne på et av de mest følsomme områdene innen IT-sikkerhet: Vi kan bygge all verdens murer rundt oss og våre hemmeligheter, men uten å vite med sikkerhet hvem som er legitime brukere og hvem som ikke er det, har vi lite oppnådd.

Åpne spørsmål, tynne svar?

Motivasjonen for å skaffe en PKI er innlysende: Bedre sikkerhet, mer kontroll, en enklere hverdag. Samtidig er det også åpenbart at en løsning omfatter langt mer enn å definere og utlevere en samling krypteringsnøkler:

- ✓ Hvem kan utstede nøklene (CA – *Certificate Authority*) og på hvilke premisser skal de utstedes, sperres og inndras?
- ✓ Hvordan skal de lagres (katalogtjeneste), hvilken annen informasjon skal inkluderes, hvem skal ha tilgang til hvilken informasjon og hvilke aksessmekanismer skal støttes?
- ✓ Hvilke offentlige lover og forskrifter kommer vi i kontakt med og hvordan forholder vi oss til dem (konsesjoner, begrensninger, kontrollfunksjoner og så videre)? Hvilke forpliktelser påtar brukerne seg og hvordan skal de legitimere seg under registreringen?
- ✓ Hvilke autentiserings-mekanismer skal vi velge? Passord er velkjent og utilstrekkelig, Smartkort er kjent, men klønete, andre fysiske duppedingser kan være bedre, men alle er utsett for fysisk slitasje og feil med tilhørende administrasjon. Finger-skannere er på vei inn, men ikke tilstrekkelig utbredte og tilgjengelige. Andre alternativer finnes, men er langt fra ideelle.
- ✓ Hvilke primære og eventuelt sekundære tjenester ønsker vi å dekke? Autentisering er viktig, spesielt i forbindelse med et voksende antall brukere utenfor lokalnettet (på reise, hjemmekontor). Mange organisasjoner har valgt en PKI-løsning for primært å dekke nettopp dette behovet, men står kostnadene da i forhold til gevinsten?
- ✓ Hva med digitale signaturer? Hvilken rolle spiller de og hva er den praktiske verdien?
- ✓ Hvilken leverandør og tilhørende løsning skal velges? Skal vi være vår egen CA (utsteder), eller kan/bør vi overlate rollen til andre?
- ✓ Hvilke verktøy skal integreres i løsningen, og hvilke grensesnitt må etableres mot andre parter?
- ✓ Kan PKI hjelpe oss på veien mot *single sign-on* (SSO), eller får vi i stedet et ekstra påloggings-nivå som gjør hverdagen enda mer komplisert for brukerne?

Slik kan vi fortsette – spørsmålene er tallrike og vanskelige, og vi sitter uvegerlig tilbake med spørsmålet om PKI i det hele tatt er en god idé.

B2B – Business-to-Business
C2B – Consumer-to-Business

Må det virkelig være så vanskelig, og hva er alternativene? Samtidig har løsningene – om vi lytter til leverandørene i segmentet – et enormt potensiale på en rekke områder, ikke minst innen e-handel i alle sine fasetter (C2B, B2B og så videre).

Behov i kø

Mens utfordringene og spørsmålene hopper seg opp, hersker det liten uenighet om behovenes størrelse og omfang. Det teknologiske grunnlaget for en universell – eller i alle fall nasjonal – PKI finnes, og en lang rekke transaksjoner og operasjoner ville blitt langt enklere med en slik tjeneste på plass. Sikker epost/meldingsutveksling og effektivisert e-handel (se side 34) er glimrende eksempler som vi har vært inne på en rekke ganger tidligere her i Mellvik-Rapporten.

Lang historie, stort lerret

PKI-problematikken har stått på agendaen siden tidlig på 90-tallet. Det faktum at vi praktisk talt står på stedet hvil med hensyn til en rekke viktige spørsmål, forteller sitt om utfordringene. Den ideelle situasjonen er lett å visualisere: En global myndighet som har hele verdens tillit, og som tar på seg det overordnede ansvaret for mekanismer, standarder og delegering av praktiske oppgaver: Identitetskontroll, utstedelse, inndraging og administrasjon av digitale identitetskort, og katalogtjenester som gjør informasjonen effektivt tilgjengelig. FN er den eneste spiselige kandidaten til dette vervet, og spørsmålet har vært tatt opp en rekke ganger, uten resultat: Ikke blir problemstillingen forstått, og ikke har FN ressurser til å gripe fatt i den.

Dermed er denne muligheten borte – for den overskuelige fremtid. Idéen var nok urealistisk i utgangspunktet: Overnasjonale organer som FN, blir til på bakgrunn av klare behov og hendelser, med utgangspunkt i brede initiativer fra et betydelig antall land. Så langt har ingen land eller stater verken tatt initiativ eller ansvar for en PKI, og lite tyder på at situasjonen vil forandre seg de nærmeste årene. Vi befinner oss kort og godt på steinaldernivå med hensyn til forståelse av utfordringen, viktigheten av å gripe fatt i den og konsekvensene av å la være.

Derfor er dagens referanse kunder for PKI-løsninger typisk å finne blant store internasjonale selskaper, og unntaksvis i store offentlige etater, i hovedsak i USA. Motivasjonen for de fleste har vært å bringe bruker-autentiseringen under kontroll i forbindelse med eksploderende bruk av ekstern aksess via VPN, eller å effektivisere papirløse handelstransaksjoner. Løsningene er uten unntak kostbare og kompliserte – og underutnyttet: Potensialet til å utvide bruksområdene, til epost, meldingsformidling, *Single Sign-on* og generell informasjonssikring, er sjelden utnyttet – av en rekke årsaker: Standardene er mangelfulle – i sin eksistens, utbredelse eller begge deler, og løsningene kommer i veien for brukerne og bruken i stedet for å støtte den.

Mislykket business

I enkelte land har nåværende eller forhenværende statlige selskaper/instanser forsøkt å etablere nasjonale registre – med epost-adresser og annen kontaktinformasjon – gratis for alle borgere, uten at resultatene har kommet. På våre kanter har Posten i samarbeid med PKI-leverandøren ZebSign, gjort et slikt fremstøt – så langt med magre resultater. Fellesnevneren for de fleste initiativer av dette slaget er at de begynner i feil ende: De etablerer en kostnadsfri tjeneste som få forstår nytten av, og vegrer seg for å investere i markedsføring av tjenesten. Ei heller lages det tilleggstjenester som kan gjøre registreringen umiddelbart nyttig. Dermed forblir de lite kjent og lite benyttet, og den praktiske verdien blir deretter.

Samtidig er det rimelig å påpeke at det er langt fra trivielt å etablere PKI-tjenester på en måte som gir den nødvendige tillit. Nettopp tillit er hva det hele dreier seg om: For at en PKI skal ha noen som helst verdi, må alle brukere ha tillit til at informasjonen er pålitelig. Dersom et søk etter Peder Aas' offentlige nøkkel lykkes, skal vi vite med sikkerhet at personen er unik, i live og ikke har rapportert sin nøkkel (ID-kort) kompromittert. Å sikre en slik grad av pålitelighet og samtidig ta vare på kritiske grenseganger mot personvern og offentlige registre, forutsetter grundig juridisk forarbeid som munner ut i rutiner, regelverk og prosedyrer. Disse må i sin tur godkjennes av offentlige myndigheter. I flere europeiske land har slike øvelser stoppet av seg selv, fordi lovverket ikke har den nødvendige fleksibilitet.

Her ligger forklaringen på at PKI-løsninger fortsatt er forbeholdt store organisasjoner – som på den ene siden har juridisk ekspertise til å ivareta grensesnittet mot myndigheter, lover og forskrifter, og på den andre siden kontroll over den informasjonen som skal til for å gjøre tjenesten nyttig.

Ut med FN og regjering, inn med Microsoft?

Dermed skulle vi tro at diskusjonen var over – inntil de riktige myndigheter forstår sin rolle og tar de nødvendige initiativer. Imidlertid er behovene akutte, mulighetene store og fristende, og markedet lett tilgjengelig via et eksploderende Internett: Med utgangspunkt i en brukerbasis på over 110 millioner på HotMail, ser Microsoft et enormt potensiale ved å tre inn i den rollen FN skulle og burde ha hatt. Utgangspunktet er glimrende – den antatt største aktive⁹ Internett-baserte brukerdata-basen i verden, som fortsetter å vokse daglig. Også andre aktører kunne ha tatt tilsvarende initiativer, for eksempel AOL og AT&T. Sistnevnte er imidlertid hemmet av offentlige reguleringer av historisk opprinnelse, mens AOL har hatt mer enn nok med å holde Microsoft unna i konkurransemessig forstand. Dessuten har begge det aller meste av sin tyngde innenlands i USA, mens HotMail er genuint internasjonal.

⁹ Tallene fra Microsoft sier ingen ting om hvor stor del av den registrerte brukermengden i HotMail som er aktive.

Hvem finnes i Microsofts Passport – og hvorfor?

Hundretusenvise av IT-brukere – inklusive oss – mottok overraskende et brev fra Microsoft i løpet av fjoråret, med bekreftelse på vår registrering i Passport. Spørsmålet som dukket opp var naturligvis hvor selskapet får navnene fra? Ikke har vi vært HotMail-bruker, aldri har vi registrert oss i MSN eller andre Microsoft-tjenester, og ikke får vi noen forklaring fra Microsoft.

Den eneste sannsynlige forklaringen vi har funnet, er at alle som har kommet i skade for å registrere sine produkter – Windows, applikasjoner, utstyr eller annet – er blitt tildelt det privilegium å bli Passport-registrert.

Vi kan styre oss for en slik praksis, som er klart i strid med betingelsene for vår registrering – på registreringstidspunktet. Microsoft benekter naturlig nok at en slik blanding av registre forekommer, men har samtidig ingen forklaring på fenomenet.

Samtidig observerer vi at betingelsene nå er oppdatert: I de fleste sammenhenger hvor vi tilbys en registrering hos Microsoft, er Passport-tjenesten nevnt eksplisitt. Mens dette er redelig nok, er historien også en demonstrasjon på hvordan betingelser og regler forandres underveis. Det finnes en lang rekke eksempler på slike forhold – ikke minst i forbindelse med programvarelisenser, hvilket gir Microsoft liten troverdighet i slike sammenhenger. Privatbrukere har imidlertid sjelden noe forhold til slike erfaringer, og er neppe troende til å lese kompliserte betingelsesdokumenter før de registrerer seg.

Ikke minst derfor har Passport foranlediget en strøm av advarsler og skepsis fra mange hold – og trigget oppretelsen av alternative tjenester med tilsvarende funksjonalitet. Dette forholdet kommer vi tilbake til i neste utgave av Mellvik-Rapporten.

Med utgangspunkt i HotMail lanserte Microsoft i fjor sin Passport-tjeneste – et register som er gratis tilgjengelig for hele verden, der vi kan legge inn all verdens informasjon om oss selv, som dermed blir lett tilgjengelig – for oss – uansett hvor vi måtte befinne oss. At den samme informasjonen dermed blir tilgjengelig også for Microsoft er innlysende, selv om det ikke sies eksplisitt. Alle HotMail-brukere er automatisk blitt Passport-medlemmer – sammen med titusener av andre, mer eller mindre frivillig (se rammen). Microsoft legger ikke skjul på at ambisjonen er å utvikle en generalisert internasjonal PKI.

I utgangspunktet er den registrerte informasjonen upålitelig i den forstand at hvem som helst kan registrere hva som helst. Over tid tror imidlertid Microsoft at påliteligheten vil vokse, blant annet ved at brukerne registrerer kredittkort, personnummere, førerkortnummere, programvarelisenser (!) og annen personlig informasjon. Videre ligger det i kortene at det kan etableres flere nivåer eller graderinger av registrert informasjon: Brukere som har legitimert seg i en eller annen sammenheng, får en 'bedre' gradering enn de som kun har oppgitt navn og andre data *on line*.¹⁰

Som vi har vært inne på tidligere her i Mellvik-Rapporten, har Microsofts initiativ vakt sterke reaksjoner. Vi kan ta av oss hatten for selskapets evne til å se muligheter og å utnytte dem, men det er også innlysende at mer informasjon og flere tjenester gir mer makt og større muligheter til misbruk. Historien kommer ikke nettopp Microsoft til støtte i så henseende, like lite som andre monopoler og monopolister har demonstrert mer tanke for kundene enn for seg selv. Derfor har det dukket opp konkurrerende alternativer fra flere hold, og bare fremtiden vil vise om noen av dem får praktisk verdi i PKI-sammenheng.

Andre alternativer

At Microsoft og andre store aktører i markedet tar mål av seg til å etablere nasjonale eller globale 'identifikasjons-tjenester', betyr ikke at dette er den eneste farbare veien. De store har riktignok både ressurser og tilstedeværelse som legger forholdene til rette for å tilta seg en slik rolle, men det er ingen ting – teknologisk eller praktisk – i veien for at også mindre aktører kan ta på seg slike oppgaver.

Uttrykket 'ta på seg' er overlagt valgt i denne sammenheng, med bakgrunn i en interessant markedstrend: Sikkerhet er krevende, kritisk og

¹⁰ Antallet HotMail-registrerte varianter av navnene George Bush, Bill Gates og Larry Ellison skal på et tidspunkt ha vært formidabelt.

kostbart. Behovet for ekspertise er stort og voksende, mens tilgangen i beste fall er beskjeden. Hva er mer naturlig enn å angripe problemet på samme måte som vi de siste årene har gjort på andre områder: Vi setter tjenesteleveransene bort til spesialister – etter *outsourcing*- eller ASP-modellen.

Om vi kan sette bort noe så kritisk som sikkerhet? Spørsmålet er like naturlig som svaret er enkelt: Vi har allerede satt bort en rekke andre tjenester vi er fullstendig avhengige av. Har vi valgt å overlate ansvaret for IT-systemer, applikasjoner og/eller nettverk til andre, har vi samtidig kjøpt deres pålitelighet og evne til å ivareta våre interesser. Vi kjøper tjenester fra vaktelskaper og transportører, flyselskaper og bilverksteder – alle med mulighet til å sette våre liv og verdier i fare dersom de ikke gjør en skikkelig jobb. Mindre naturlig er det ikke å legge tilsvarende tankegang til grunn for IT-sikkerhet generelt – og PKI spesielt.

Nettopp derfor dukker det i disse dager opp leverandører av IT-sikkerhetstjenester (MSSP – *Managed Security Service Provider*). Uten å gå i detalj med hensyn til hvilke tjenester de kan tilby, er det innlysende at slike leverandører, gjennom levering av PKI-tjenester til flere kunder, har mulighet til å levere pålitelig autentisering og tilhørende nøkler på tvers av kundenes organisasjoner. Ønsker vi dette? Javisst – så lenge vi har tillit til leverandøren, hvilket i sin tur er en forutsetning for hele tjenesten. Dessuten er dette en mulighet som kan velges inn eller ut, ikke en nødvendighet.

Konseptet befinner seg fortsatt på et tidlig stadium, men det er lett å se et betydelig potensiale her – gitt at standardene kommer på plass, og leverandørene spiller sine kort riktig.

En annen variant, som i motsetning til den hierarkiske PKI-modellen baserer seg på gjensidig tillit, kan etableres gjennom rene programvareløsninger: Bedriftsinterne PKI-systemer kobles sammen via smart programvare som styres av policy-baserte regelverk og kommuniserer via standardprotokoller eller proprietære mekanismer. Tankegangen har mye til felles med det idémessige grunnlaget for PGP (*Pretty Good Privacy*, se Mellvik-Rapporten nr. 17), og trekker på mer enn 10 års erfaring i den forbindelse. Så langt er faktisk PGP den eneste PKI-teknologien som kan sies å ha lykket i stor skala i markedet, et forhold vi kommer tilbake til avslutningsvis.

Også slike løsninger er ferske og mangler den modenhet og erfaringsbase vi finner det naturlig å kreve av kritiske sikkerhets-systemer. Samtidig representerer de en spennende progresjon fra den relative stillstand vi har hatt på området de siste årene. En av aktørene i segmentet er amerikanske Sigaba Inc., hvis løsning for sikker epost diskuteres på side 34.

PKI-tjenester

Blant de mest kjente internasjonale leverandørene av PKI-tjenester og tilhørende programvare finner vi

- Entrust Inc. (eies av CA)
- Baltimore Technologies Inc.
- Digital Signature Trust Co. (eies av Identrus)

Se for eksempel Sigabas *White Paper* om **Global Authentication** på www.sigaba.com/products/white-papers.html.

Digitale signaturer

Uttrykket digitale signaturer dukker opp i hverdagen vel så ofte som PKI. Samtidig er begrepet lite forstått og uklart definert, der det stadig blandes sammen med såkalte e-signaturer og andre uttrykk. Mens en 'e-signatur' er en digital representasjon av en tradisjonell underskrift, i form av et bilde som importeres til dokumenter og telefakser, er en digital signatur noe helt annet: Et digitalt identitetskort hvis ekthet når som helst kan kontrolleres via krypteringsnøkler, slik vi forklarte innledningsvis.

Det betyr at digitale signaturer er uløselig knyttet til en PKI, og ikke kan eksistere på egen hånd. Videre betyr det at å inkludere digitale signaturer i korrespondanse (dokumenter, meldinger etc.) ikke har noen verdi med mindre mottakeren har mulighet for å kontakte den tjeneren som har utstedt signaturen. Og sist, men ikke minst: Dersom denne muligheten finnes, er dens verdi avhengig av at mottakeren har tillit til utstederen.

Igjen observerer vi tallrike utfordringer som savner generelle løsninger – først og fremst på grunn av PKI-problemene vi allerede har diskutert. Samtidig er behovet for pålitelige digitale signaturer akutt, ikke minst i forbindelse med elektronisk handel. Derfor har det i løpet av de siste årene dukket opp leverandører og løsninger rettet spesifikt mot nettopp dette segmentet, og gjerne med fokus på amerikansk offentlig sektor, som i løpet av et år gjør innkjøp i en størrelsesorden som får et norsk statsbudsjett til å se ut som veksllepenger. De potensielle effektivitetsgevinstene i reduksjon av papirmengden er formidable, og kreativiteten fra kunde- og leverandørsiden tilsvarende.

En toneangivende leverandør på området er amerikanske Silanis Inc. [www.silanis.com] med *Decisions Moving at the Speed of eBusiness* som markedsførings-slogan. Selskapet leverer tjenester og programvare rettet mot elektronisk handel – mekanismer for verifikasjon av at elektroniske dokumenter er hva de gir seg ut for å være. Spesialiserte løsninger for et marked som er smalt og stort på samme tid, og med en erfaringsbase som gir føringer for den videre utviklingen innen digitale signaturer generelt.

At løsningene er omfattende og tunge, forteller sitt om umodne mekanismer, manglende standarder – og ikke minst kompleks juss: Lovverket har store problemer med å følge med i utviklingen. Variasjonene er betydelige fra land til land, og uklarhetene med hensyn til hva som skal til for å gjøre elektroniske dokumenter og transaksjoner juridisk bindende, er tilsvarende store.

Konklusjon

Til tross for mange års utvikling og tunge investeringer, er PKI-løsninger – og dermed digitale signaturer – i 2002 fortsatt befengt med flere spørsmål enn svar. Noen viktige observasjoner når behov og løsninger skal evalueres er:

- ✓ En PKI er kostbar og komplisert, og må ha betydelig umiddelbar nytteverdi for å kunne rettferdiggjøres: Minst to for-

retningskritiske applikasjoner. Videre fordrer en PKI-løsning betydelig innsats for klargjøring av rettigheter og ansvar i organisasjonen. Mange uskrevne regler må dokumenteres og implementeres i en PKI før den kan virke etter hensikten.

- ✓ Digitale sertifikater og nøkler utstedes til enkeltpersoner og knyttes til unike brukernavn. I de fleste organisasjoner har én bruker mange forskjellige navn (brukernavn) på ulike systemer, kanskje sågar flere navn på samme system, avhengig av oppgaven som skal utføres. En homogenisering er nødvendig før en PKI kan utnyttes fullt ut, hvilket i mange tilfeller er en smertefull og lang prosess, blant annet fordi arbeidsmetodikk (gamle vaner) må legges om.
- ✓ En PKI knyttes tett mot organisasjonens brukerdatabase, som må forefinnes i en katalogtjeneste med tilgang via LDAP (Novell Directory Services, Microsoft Active Directory og lignende). Etableringen av en slik tjeneste er en betydelig oppgave som bør være gjennomført og testet før PKI-arbeidet starter. Likeledes må katalogtjenesten være PKI-klarert – ha innarbeidet begreper og mekanismer for oppretting, endring og sletting av sertifikater, nøkler og annen relevant informasjon.
- ✓ PKI-løsningen må være kompatibel med applikasjonene: De to forretningskritiske applikasjonene vi forutsatte i første punkt, er bare begynnelsen. Målsettingen er å få integrert flest mulig av virksomhetens applikasjoner i PKI-systemet, slik at autentisering (effektivt *Single SignOn*) og kryptering av data ved behov, blir sømløse, usynlige tjenester. Med mange produkter på markedet og få standarder, ser vi ofte at virksomhetskritiske løsninger er tilpasset én PKI-variant, mens en annen vanskelig lar seg bruke.
- ✓ Autentiserings-mekanismene er selve grunnmuren i et PKI-system. Dagens løsninger med Smartkort og andre 'duppedingser' er en overgang. Fingerskannere er på vei inn og blir i disse dager standardutstyr på stadig flere bærbare systemer. Forsøk på å inkludere mobiltelefonen i autentiseringsprosessen har så langt ikke lyktes, og blir for komplisert inntil Bluetooth eller en annen PAN-teknologi etableres som standardutstyr på både mobiltelefoner og PC-utstyr.

Mens dagens PKI-løsninger ivaretar viktige oppgaver i mange organisasjoner, er det med andre ord fortsatt ikke innlysende at den hierarkiske PKI-modellen som preger dagens produkter, er riktig vei til målet. Utfordringene er for mange og resultatene står kun unntaksvis i forhold til investeringene. Fremskrittene er små og sjeldne, mens behovene er akutte. Derfor er det naturlig å anbefale forsiktighet med hensyn til nyinvesteringer: Med mindre det kan sannsynliggjøres at kosteffektiviteten blir god i løpet av kort tid, er å avvente utviklingen bedre enn å satse på dårlige odds.

Hvorvidt generaliserte, globale tjenester fra Microsoft eller andre vil få en signifikant rolle i dette bildet, gjenstår å se. Vi tror sjansene er små

PAN – Personal Area Network, diskuteres i en egen artikkel i neste utgave av Mellvik-Rapporten, se baksiden for detaljer.

fordi dimensjonene blir for store og tilliten for liten. Det hele handler som vi har nevnt, om tillit, og der den mangler har tjenesten liten verdi. Dessuten – dersom én eller flere slike tjenester mot formodning skulle lykkes, er det fortsatt ikke innlysende at myndighetene kan tillate en slik maktfaktor å utvikle seg. Vel er effektive reguleringer langt vanskeligere å iverksette i en global Internett-verden enn tidligere, men sunn fornuft lar seg fortsatt selge til folk flest.

En ny tillitsmodell

Sannsynligheten er stor for at vi i løpet av de neste to årene vil se en helt ny generasjon løsninger basert på en annen tillitsmodell. Dagens hierarkiske modell er forankret i tradisjonell tenkning om organisasjon og maktstrukturer som ikke lar seg realisere i en grenseløs verden med større frihetsgrader på de fleste områder enn noe tidligere samfunn. Internettet er en praktisk demonstrasjon på hvordan det vi tidligere betegnet som kaos og anarki, ikke bare kan fungere, men sågar fungerer bedre enn noen kjent modell.

Vi nevnte PGP ovenfor, og teknologien – som eies av Network Associates (NAI) – opplever en oppblomstring i disse dager. Dette skjer til tross for at NAI nylig la ned all produktutvikling rundt PGP, og annonserte stopp i salget av eksisterende produkter. Dermed blir det den åpne (*Open Source*-produktet OpenPGP) utgaven av teknologien som nyter godt av fremgangen.

Drivkraften bak oppblomstringen er et eksploderende behov for sikring og autentisering av epost. Andre tilgjengelige alternativer tar utgangspunkt i en eller annen tradisjonell PKI, og har vist seg vanskelige å realisere i praksis – av de samme årsakene som vi har diskutert ovenfor.

PGP er på sin side fundamentert på en distribuert tillitsmodell, der hver og én bestemmer hvem som er til å stole på, og forholder seg til dette (*web of trust* på fagspråket). Ansvarsfordelingen blir dermed en helt annen: Alle må ta et større ansvar for seg selv enn tilfellet er i den hierarkiske modellen, der en overordnet myndighet sitter med styring og ansvar. Av samme årsak blir skalerbarheten dramatisk bedre: Ingen enkelt flaskehals kan blokkere hele systemet.

Neste generasjons PKI-løsninger vil ta utgangspunkt i disse erfaringene, og legge grunnlaget for en skalerbar, fleksibel, effektiv og pålitelig infrastruktur for utveksling av digitale identitetskort – i en verden der det er naturlig for de fleste av oss å selv velge hvem vi kan og bør stole på. Ideen om at andre vet best og bør ta ansvaret, gikk ut på dato lenge før Berlin-muren falt. ■