Betalingstransaksjoner på nettet sikkerhet og standarder

Knut Soelberg og Jon Ølnes
Norsk Regnesentral (NR)

Knut.Soelberg@nr.no

COMBO brukermøte, London, 22. november -96

Innhold

1. Åpne og lukkede nettverk - Internett og sikkerhet
2. Krav til sikre tjenester på Internett
3. Kryptografi
4. Kommunikasjonssikkerhet og meldingssikkerhet
5. Elektronisk legitimasjon - sertifikater
6. Handel i åpne nett - modeller for betaling
7. SET (Secure Electronic Transactions)
8. Konklusjoner

Internett og kommunikasjonssikkerhet

- Ikke-kommersielt forskningsnettverk siden 70-tallet
  Liten sikkerhet i de vanligste tjenestene (ubeskyttede passord, eller helt åpent)
  Ingen kommunikasjonssikkerhet - meldinger i klartekst
- Kommersiell bruk i noen få år
  Beskytte adgang til tjenester - sikre tjenester
  Beskytte kommunikasjon
  Bruk til handel og betaling
- "Sikkerhetsstandarder" er under utvikling
  "Standard" produkter eller spesifikasjoner
  Dagens "standarder" ikke tilstrekkelige (alene) for bank / betaling
  Bruk av kryptografi er nødvendig, men problematisk (politisk)

Sikkerhet - langt mer enn tekniske løsninger

Tekniske løsninger er viktig, men

- Administrative regler og rutiner som faktisk følges
- Kvalitetssikring - unngå feil og mangler i systemer, endringshåndtering
- Lekkasje og innsideangrep

blir enda viktigere en før fordi tjenestene bllir meget tilgjengelige på Internett

Krav til sikre tjenester på Internett (1)

1. Tilgjengelighet
   Tjenester tilgjengelig med tilfredsstillende ytelse for legale brukere
2. Integritet
   Dataintegritet: Sikre mot uautorisert endring av informasjon
   Systemintegritet: Sikre at systemer / programmer oppfører seg som de skal
3. Konfidensialitet
   Holde informasjon skjult for uvedkommende
4. Sporbarhet
   Bevis for en hendelse "vilkårlig" tid i etterkant - krever logging og integritet.

   Sikker kommunikasjon i åpne nett krever bruk av kryptografi

Krav til sikre tjenester på Internett (2)

- Tjenesten må se sikkert ut
  - Enkel bruk - små muligheter for feil bruk
  - Skal ikke se "suspekt" ut
  - God integrasjon - brukergrensesnitt etc.
  - Brukernes ansvar må være klart - uaktsomhet, misbruk osv.
- Beskyttelse mot utenforstående
  - Bruk av kryptografi for å sikre kommunikasjon
  - Meget sikre datasystemer og sikker Internett-tilkobling
  - Vanskelig å lure brukere (uten at disse opptrer uaktsomt)
- Beskytte aktørene mot hverandre
  - Kjøpere, selgere, betalingsformidlere

Opponionens formening om et systems sikkerhetsnivå har ofte ikke noe med systemets faktiske sikkerhetsnivå å gjøre - gir store utfordringer

Kryptografi

Hvor lang tid trengs for å knekke en kryptert melding?

- Prøve alle nøkler eller snarveier (om mulig)
- Må ta hensyn til utvikling av teknologi og hvilke ressurser en angriper har
  - Sikkert nok i dag er ikke sikkert nok om et par år
  - Banker må være forberedt på angrep fra ressurssterke angripere
- Store nok nøkler er nødvendig, helst > 80 bits (> 512 bits for signering)

Dagens bankløsning - 40 bits nøkler:

- En avansert angriper kan knekke dette på rimelig tid
  - ... men ikke raskt nok til å kunne endre informasjonen,
  - ... men det vil være mulig om noen få år (sikkert i to år?)
- Enkelt å endre til sterkere kryptering - avhengig av amerikansk lovgivning eller bruk av produkter fra andre land

Sikre kommunikasjon eller meldinger?

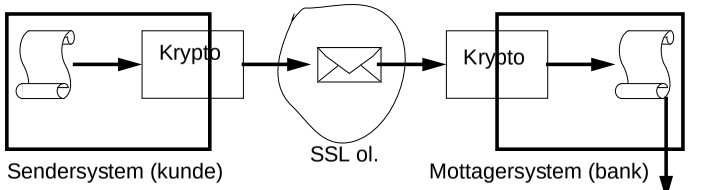
Dagens betalingsløsninger - kommunikasjonssikkerhet (f.eks SSL):

- Avsender*maskin* krypterer nettverkstrafikk
- Ingen signaturer
  - Forholdsvis dårlig sporbarhet (bevis for en hendelse)
  - Forholdsvis dårlig mot innsideangrep
- Mellomlagring er usikkert (punkt til punkt sikkerhet)
- Akseptabelt (midlertidig) for bank- og betalingstjenester

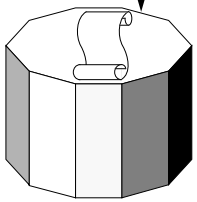
Framtidige løsninger - meldingssikkerhet (f.eks SET):

- Avsender*person* signerer og krypterer en melding
- Meldingen sendes - ingen krav til nettverket, mellomlagring OK (ende til ende)
- Mottager kan dekryptere, sjekke signatur, og lagre med signatur
  - Sporbarhet / innsideangrep: Signaturen beskytter

Kommunikasjonssikkerhet

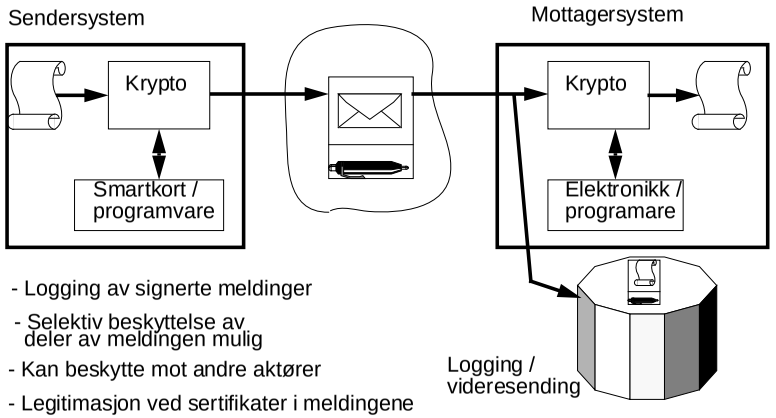


- Beskytter mot andre aktører, dårlig mot innsideangrep
- OK for punkt-til-punkt ved høy ensidig tillit (f.eks. kunde mot bank)
- Kan bruke ekstra autentisering (DigiPass)
- Sporbarhet bare ved klartekst logging



NR

Meldingssikkerhet

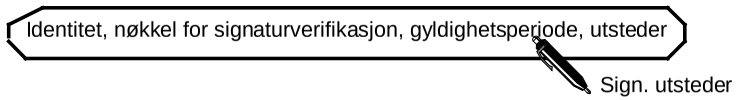


- Logging av signerte meldinger
- Selektiv beskyttelse av deler av meldingen mulig
- Kan beskytte mot andre aktører
- Legitimasjon ved sertifikater i meldingene

NR

Elektronisk legitimasjon - sertifikater

- Sertifikat:



- Utsteder - “Tiltrodd TredjePart (TTP)
  - Må stole på utsteders signatur - godta legitimasjonen
  - Regler for utstedelse, sikkerhet, av og til objektivitet
- Trenger forskjellig legitimasjon for forskjellige formål
  - ID-kort fra jobben
  - “Borgerkort” for kommunikasjon med det offentlige?
  - Elektronisk bankkort
  - Regler for hva som godtas i gitte sammenhenger

NR

For betaling og banktjenester

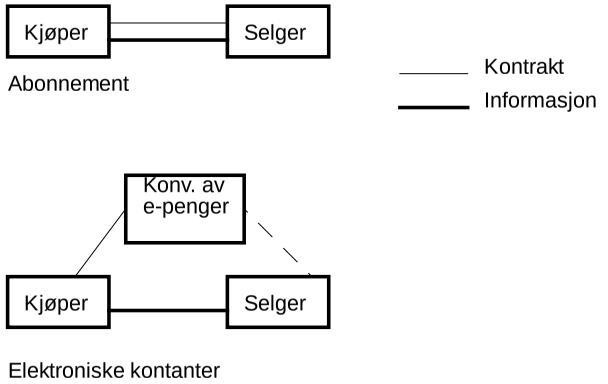
- Elektronisk bankkort:
  - Banker (og kortselskap) vil sertifisere sine kontoinnehavere
  - Har allerede autorisert disse når konto ble opprettet
  - Sertifikat (og smartkort) kan utstedes “på samme måte som bankkort”
  - Selgere, og bank/kortselskap, trenger også sertifikater
- Framtidas bankkort kan ha:
  - Kryptografi for digitale signaturer - betaling i nettverk fra datamaskin
  - Vanlig smartkort for butikkterminaler
  - Elektronisk lommebok / kontantkort
- Smartkort kommer - kortlesere er standard på PCer om ganske kort tid
- Hva bremser utbredelsen av elektronisk legitimasjon og bankkort i dag?
  - Mangel på utbygd infrastruktur for TTP-tjenester
  - Flere initiativ på gang - bla. i forbindelse med SET

NR

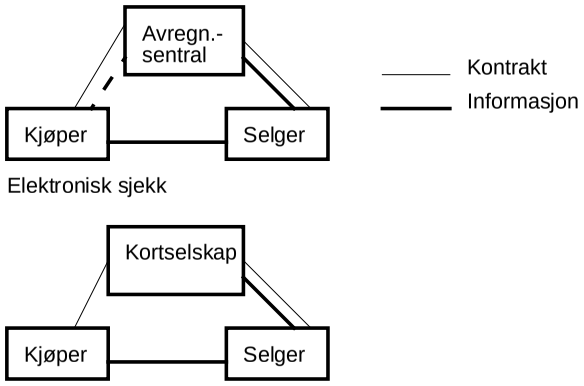
Handel i åpne nett

- År 2003: 30 Mrd. (McKinsey) eller 3000 Mrd. (Credit Card Management)
  Dvs.: Ingen vet, men i hvert fall et betydelig volum
- Handel omfatter:
  - "Postordre" (med eller uten betaling) av fysiske varer
  - Informasjon - nyheter, programvare, ...
  - Spill og underholdning
  - Reservasjoner - turisme, billetter, ...
  - Selgere samles på "markedsplasser"
- Suksess avhengig av at betaling også kan gjøres over nett
  - I dag er kortbruk eneste mulighet - oppgi kortnummeret, belastning
  - "Mikrotransaksjoner" må også støttes - betaling av småbeløp
  - Kortselskapene ønsker mest mulig av markedet!

Modeller for betaling (1)



Modeller for betaling (2)



Secure Electronic Transaction (SET)

- Teknisk spesifikasjon for sikre betalingstransaksjoner med betalingskort over åpne nett
- Utviklet av VISA og Mastercard i tillegg til støtte fra en rekke samarbeidspartnere fra IT-industrien
- Lagt vekt på at SET skal være en åpen standard
  - Basert på meldingssikkerhet
  - Benytter standarder for kryptografi ol., slik som RSA, DES, SHA-1, PKCS#7 og X.509
- Spesifiserer betalingssystem og sertifisering
- Betalingsformidlere kommuniserer på eksisterende int. (bank-)nettverk
- Kundeforhold (f.eks. med kortselskap) må eksistere på forhånd
- Selgere autoriseres/sertifiseres ("autorisert MasterCard forretning")
- SET applikasjonener vil typisk benytte web og/eller e-post som bærer av SET meldinger

SET

- Spesifikasjonen er ikke ferdig før 1. kvartal 1997
- Referanseimplementasjon underveis
- TTP infrastruktur i forbindelse med SET under utvikling
- Kommersielle leverandører har varslet at SET vil implementeres i deres produkter for elektronisk handel
- Vil støtte bruk av smartkort i senere utgaver
- SET er et godt skritt i riktig retning for utbredelse av elektroniske betalingstransaksjoner mellom tilfeldige aktører tilkoblet Internett
  - Men veldig amerikansk
  - Spesifiserer ikke bestilling, kun betaling
  - Lite egnet for “mikrotransaksjoner”(?)

Konklusjoner

- Dagens bank- og betalingstjenester på Internett:
  - Sikre nok i dagens situasjon
  - Neppe den langsiktige løsningen
- Elektronisk handel blir et viktig område
  - Viktig med nasjonale løsninger for betaling
- Betaling i åpne nett krever meldingssikkerhet
  - Skal beskytte aktører også mot hverandre
  - Fordel også for banktjenester i åpne nett
- Skikkelig kryptografi er nødvendig
- Elektronisk legitimasjon trengs
  - Sertifikater og bruk av smartkort