Elektronisk betaling

einar.snekkenes@nr.no

Forskningssjef
Elektroniske markeder og sikkerhet

Norsk Regnesentral

Temaer

- NR
- Kan vi ha tillit?
- Betaling - alternativer
- Betalingsprodukter
- Aktør kategorier
- Aktørers Interesser
- Byggeklosser
- Systemer
- Sikkerhet
- Konklusjoner og mer kunnskap

NR

- Stiftelse, 40+ år
- ca 100 forskere innen matematikkk og IKT
- Nært samarbeid med UiO
- Elektroniske markeder og sikkerhet
  - Prototyping
  - Spesifikasjon og analyse av sikkerhet
  - Hva er mulig teoretisk? – Hva er gjennomførbart i praksis?

Kan vi ha tillit?

- CERT/CC- rap. sårbarheter
  www.cert.org

95	'96	'97	'98	'99	'00	Q1'01
171	345	311	262	417	1090	633

- Tyveri av kredittkortnummer
- Nettbank, editering av HTML kildekode
- Britisk bank, ansatt samlet inn PIN etc vha PDA inne i minibank
- Gjør finansbransjen tilstrekkelig for å sikre seg?

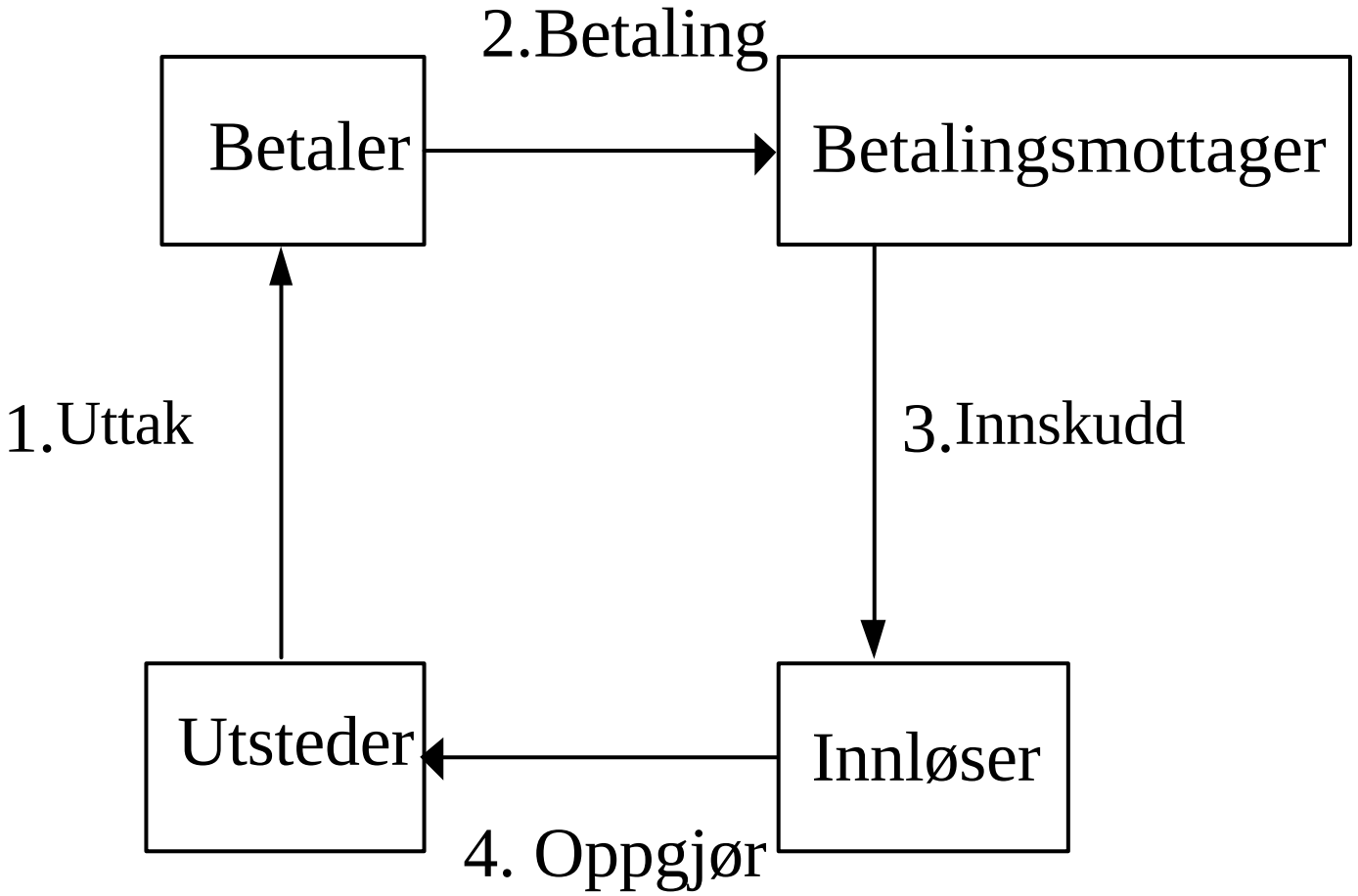
Betaling – alternativer og valg

- Hvem holder oversikten? Token/konto
- Beløpets størrelse – mikro/ småbeløp/ 'store' beløp
- Robusthet: On-line/ off-line
- Anonymitet: Ingen/ uansett/ brytes ved forsøk på 'dobbelbetaling'.

Betalingsprodukter

- Sjekker
- Bankremisser
- Kontanter
- Overførsler
- ...

Aktørene – Token eksempel



Parters interesser

- Betaler
  - Samtykke, riktig mottager og beløp, få gjenytelse, mottager må ikke kunne nekte for betaling, følsom informasjon må ikke forlate kontroll
- Mottager
  - Være sikret mottak av betaling hvis ytelse leveres, påstand om betaling må kunne valideres
- Utsteder og Innløser
  - 'Pengemengde' må ikke øke. Påstand om betaling må kunne valideres. Ønsker (mest mulig) informasjon om transaksjon.

Hvordan? Kryptografiske byggeklosser!

- Digitale signaturer – offentlig nøkkel kryptografi
- Hash funksjoner
- Blinde signaturer
- Deling av hemmeligheter
- ’Bit commitment’
- ...

Systemer – 100+!

- MONDEX
- Proton
- CyberCash
- SET
- CyberCoin
- eCash (ex Digicash)
- CAFE
- ...

Sikkerhet

- Kerckhoffs eller 'security through obscurity'
- Ofte vanskelig å få tilgang til detaljer om betalingsløsninger
- Teoretisk sikkerhet – sikkerhet i implementasjon - bruksomgivelse
- Tillit: ha få hemmeligheter?
- Hva må brukere gjøre/ikke gjøre/ for at betalingstjenester skal være sikre?

Konklusjon

- Mye å velge mellom!
- e-betaling i fremtiden: Hva gjør de store aktørene?
- Svindel og bedrag : Vi har mer i vente.
- Beskyttelse, sikkerhet og tillit – En kan gjøre mer enn det som gjøres nå!
- Ikke alt er salgbart – kanskje noen har en annen forretningsmodell enn deg, og kan gi bort noe som er svært likt det du ønsker å ta betalt for?

Mer kunnskap?

- **Digital Cash - commerce on the net, 2nd edition, Peter Wayner, AP Professional, 1997.**
- The Economics of Electronic Commerce, S.Y. Choi et al, Macmillan Technical Publishing, 1997.
- eBusiness Essentials, M. Norris et al, John Wiley, 2000.
- ”Hva med betalingen?”, Business Standard, s 52, nr 4, 2000.
- Eksempler på sikkerhetsbrudd
  http://www.addsecure.net/breach.htm
- Spørsmål?
  - Kontakt: einar.snekkenes@nr.no