Analyse av tillit i elektronisk samvirke

Atle Refsdal
SINTEF IKT

Oversikt

- Tillit
  - Hvorfor analysere tillit?
  - Tillit i elektronisk samvirke
  - Tillit og oppførsel
- Modellering og analyse
  - Nytten av modeller
  - Et språk for modellering av tillit og oppførsel
- En metode for å utvikle tillitspolicies
  - Metoden bruker modeller uttrykt i språket
  - Erfaring fra anvendelse av språk og metode i industrielt case
- Hva har vi oppnådd?

Hvorfor analysere tillit?

- "Uten et visst sikkerhetsnivå *og tillit til teknologien* kan ikke IKT-basert samhandling videreutvikles"
  - Fra "Beskrivelse av tema og fagsøyler i VERDIKT", Forskningsrådet, 2009 (min uthevelse)

- Sikkerhet alene er ikke nok!
- Potensielle brukere må være villige til å ta i bruk teknologien – også når penger eller sensitiv informasjon er involvert (risk)
- Tillit ≠ tillitsverdighet

Hvorfor analysere tillit?

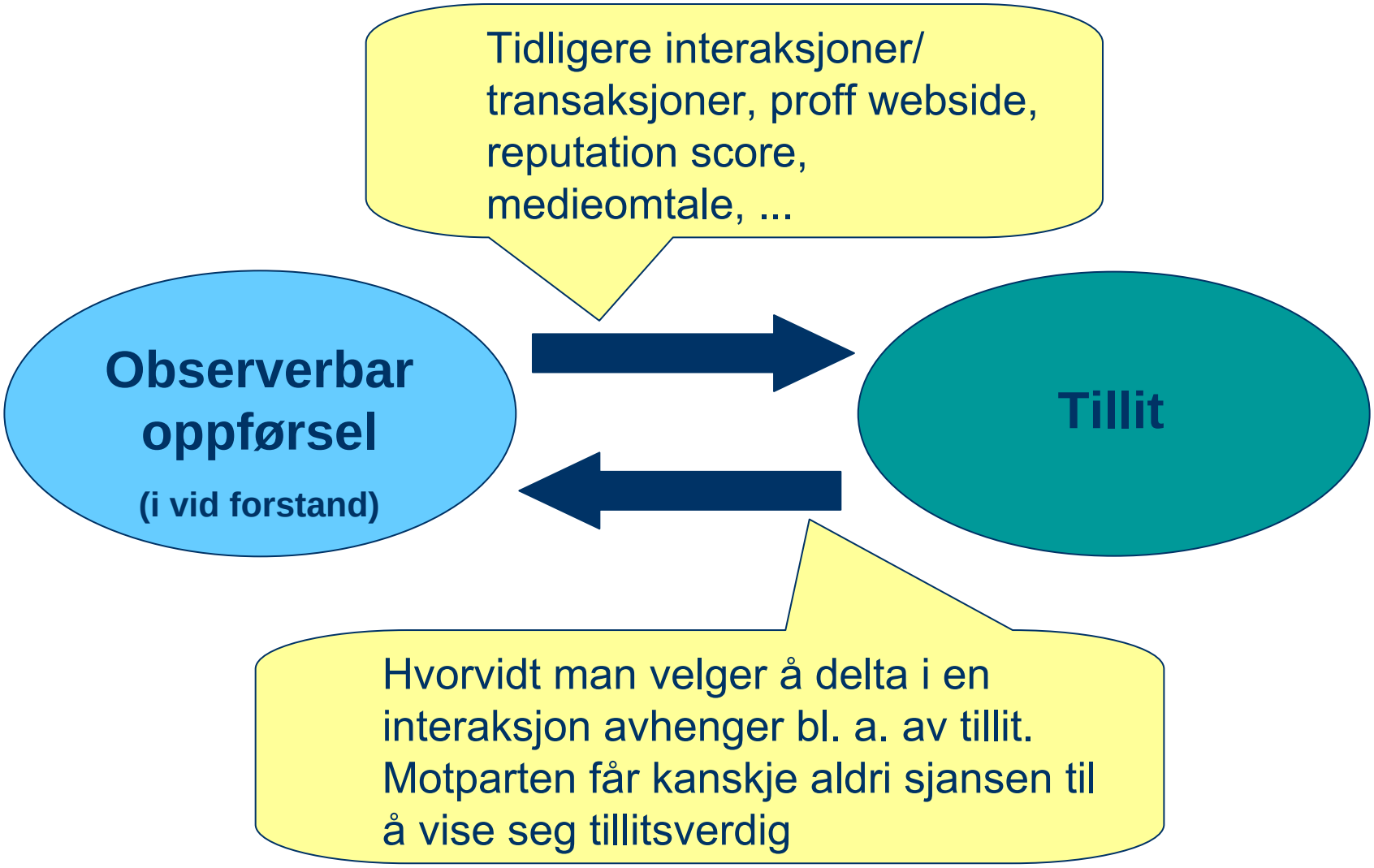
- Ønsker forståelse av systemer som inneholder aktører som tar beslutninger basert på tillit

- Hva er risikoen?
- Hvilke muligheter gir det?
- Hva er den beste policyen for slike beslutninger?

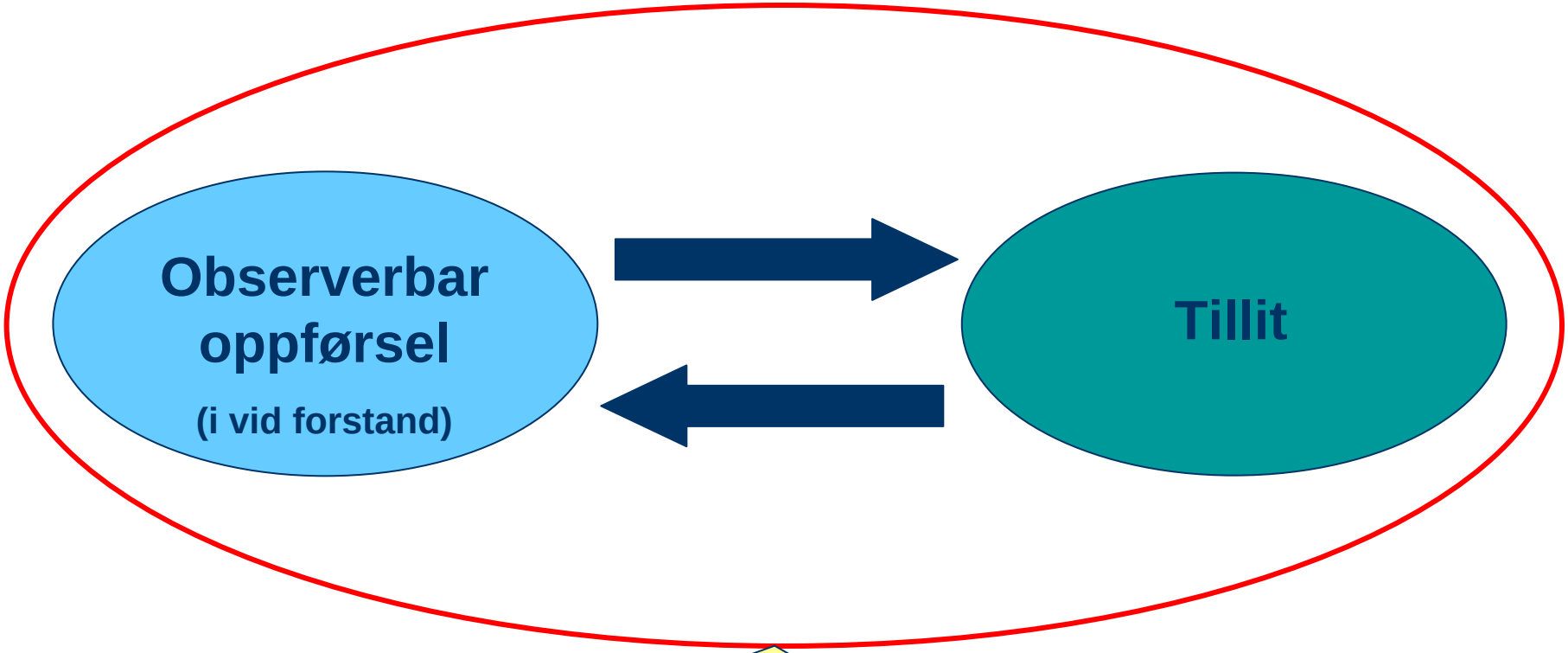
Tillit i elektronisk samvirke

- I “vanlig” omgang med andre personer, brukes en rekke intuitive faktorer for å bygge tillit
  - klesdrakt, velstelthet, håndtrykk, blikk, ...
  - bevisst eller ubevisst
- Ved elektronisk kommunikasjon må tillit bygges på andre måter
  - reputation systems, kvalitet på websider, elektroniske signaturer (krever tillit til infrastruktur)...
- Dessuten er det ekstra vanskelig å vite hva man skal gjøre hvis man blir lurt
  - Til hvem klager jeg hvis varen jeg kjøpte fra et nettsted i Brasil aldri kommer?

Tillit og observerbar oppførsel



Tillit og observerbar oppførsel

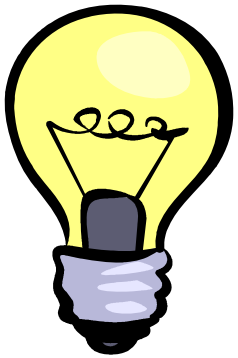


Nytten av modeller ved analyse

- Her: grafiske modeller – bokser og piler
- Læringsprosessen ved å lage modellene
  - systematisk innsamling og strukturering av informasjon
- Hjelpemiddel til formidling og kommunikasjon
  - kan for eksempel peke på bestemte deler av en modell
- Dokumentasjon

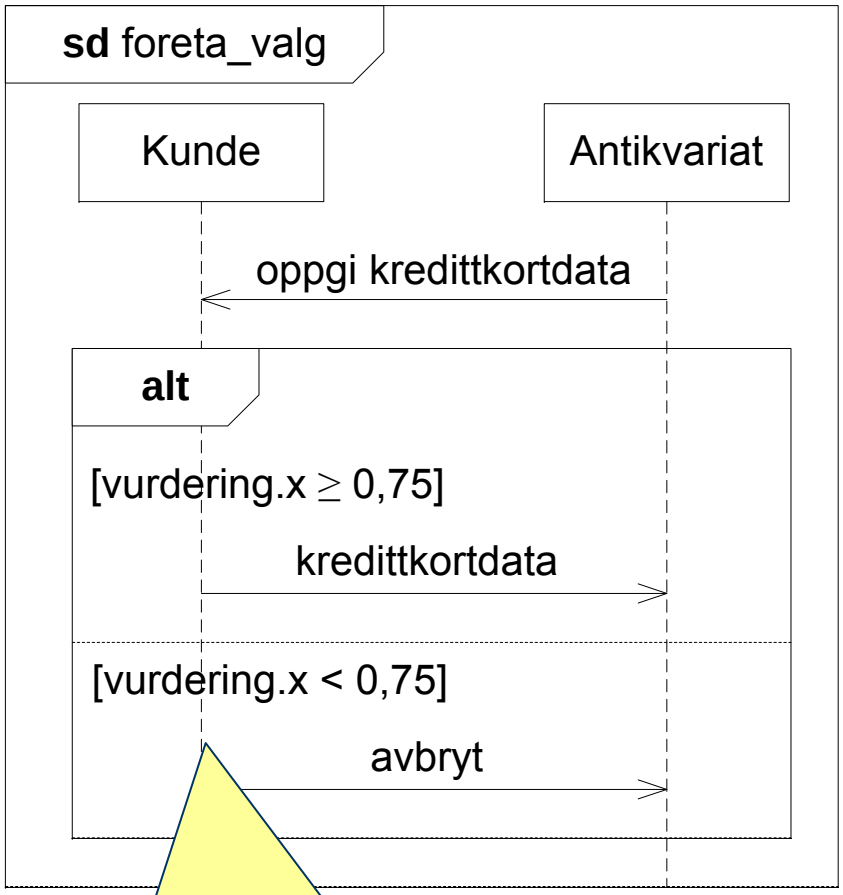
- Vi ønsker modeller som kan fange inn både observerbar oppførsel og tillitsvurderinger/beslutninger

Grunnleggende idé

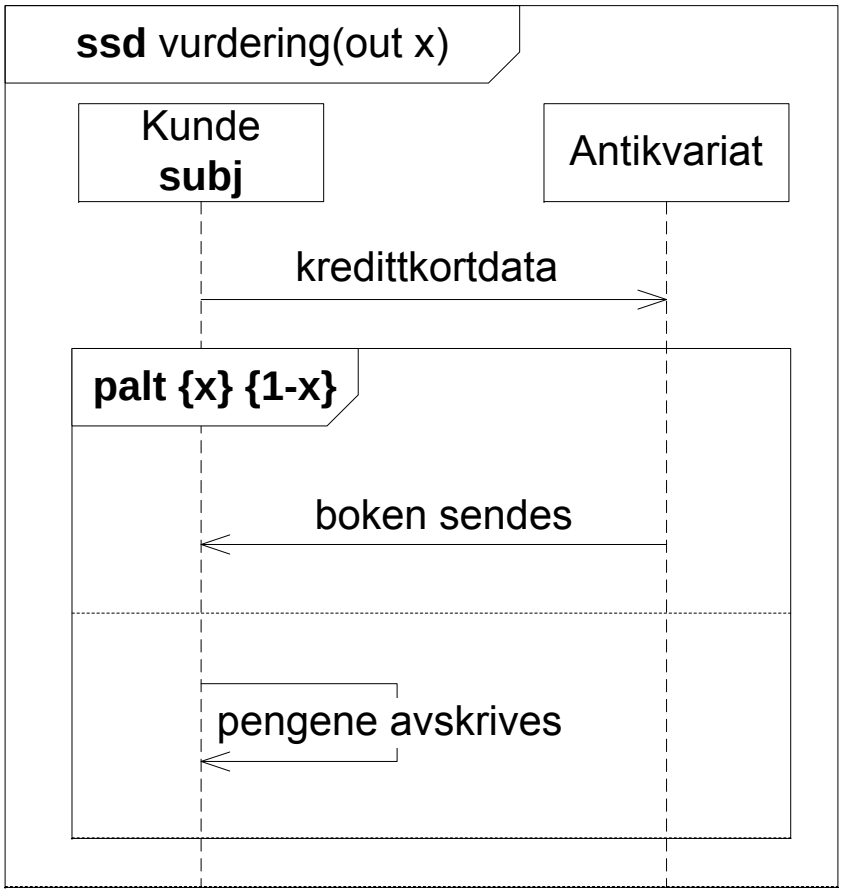


- Utgangspunkt: sekvensdiagrammer
  - egner seg godt til å modellere interaksjon
- Uttrykker tillit ved *subjektive* probabilistiske sekvensdiagrammer
  - uttrykker hva en aktør (subjektet) *tror* om andres oppførsel
  - sannsynligheter representerer estimater gjort av subjektet
- To typer diagrammer:
  - Objektive diagrammer viser faktisk (og observerbar) oppførsel
  - Subjektive diagrammer viser sannsynlighetsestimater gjort av en aktør
- Det objektive diagrammet refererer til det subjektive
  - viser *hvilke* sannsynlighetsestimater som gjøres, og
  - *hvordan* disse estimatene påvirker valg av handling

Objektivt diagram



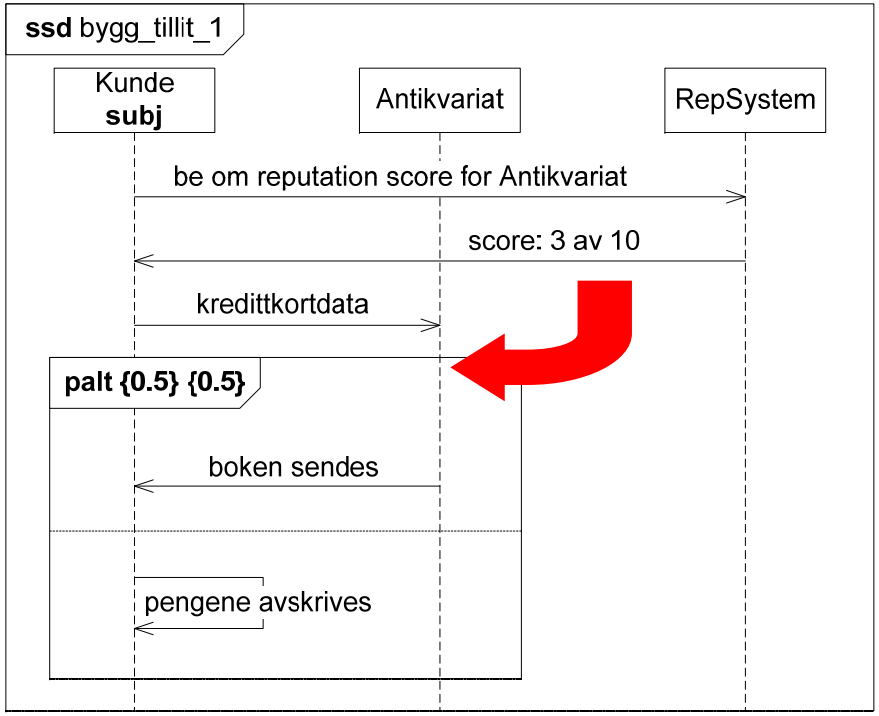
Subjektivt diagram

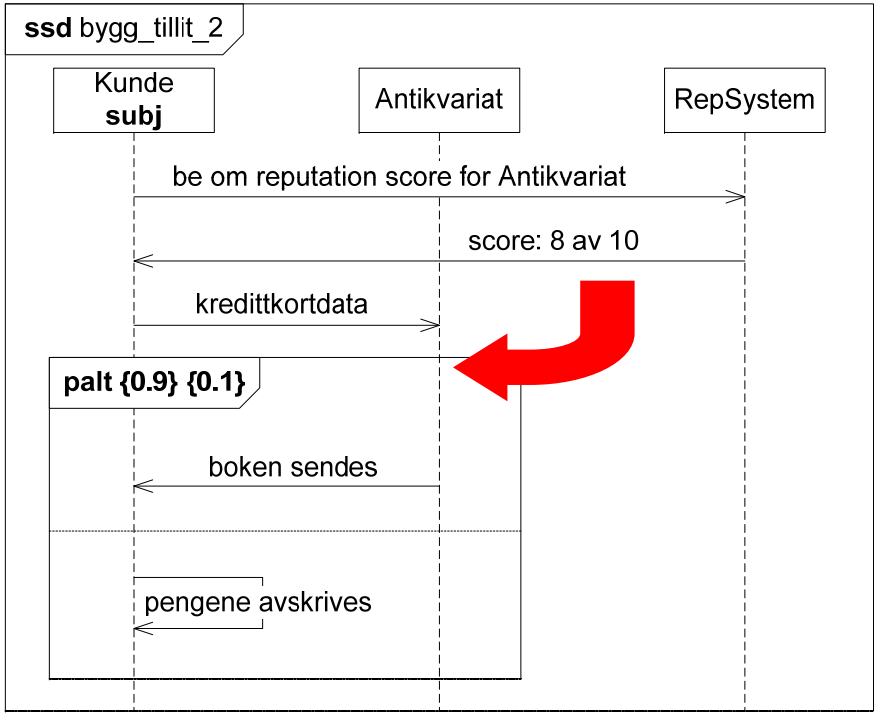


Guardene viser hva som er kriteriet for å velge det ene eller andre alternativet

Det subjektive diagrammet viser hvilken tillitsvurdering som gjøres

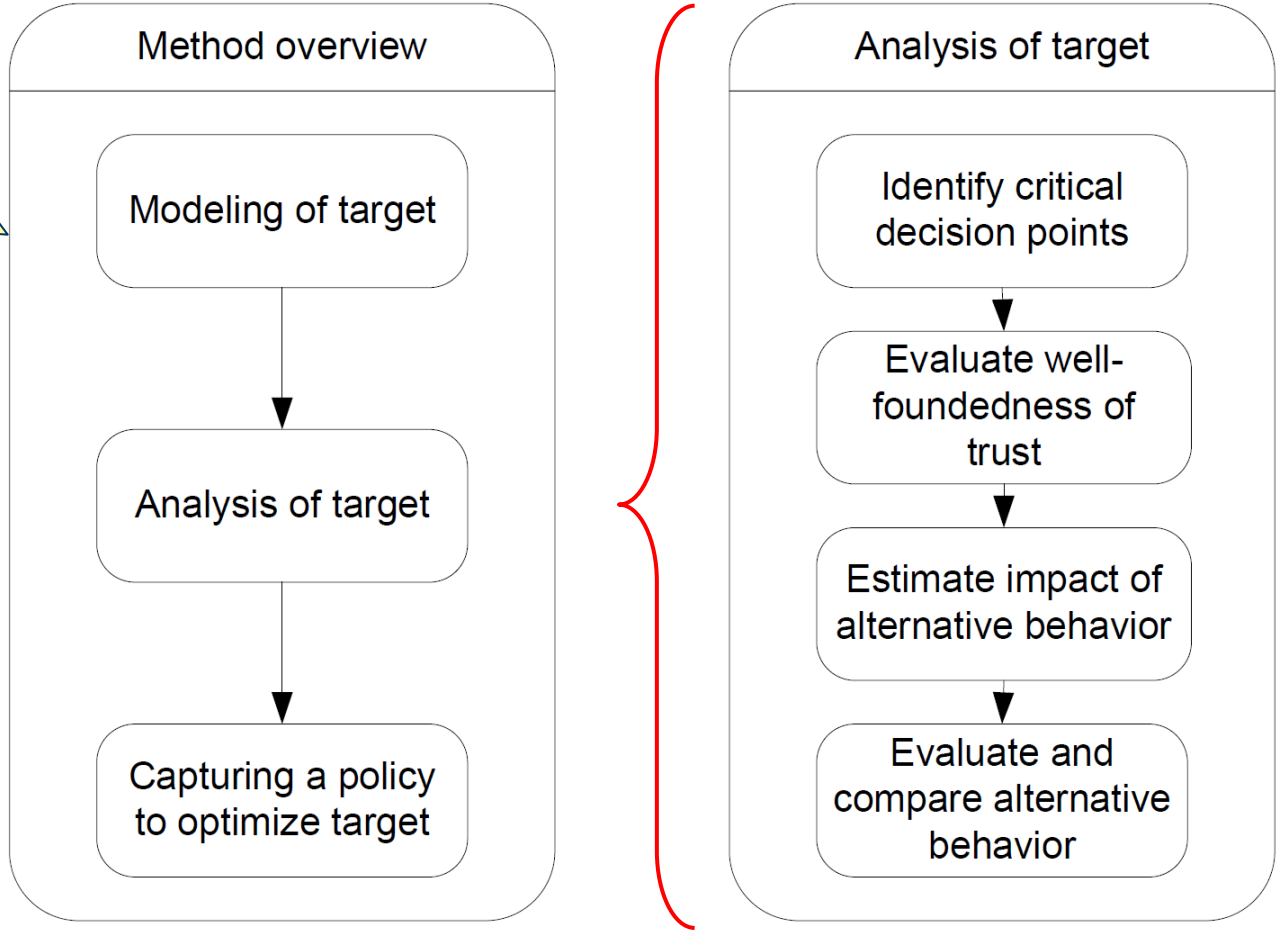
Eksempel: hvordan reputation kan påvirke tillit





En metode for å utvikle tillitspolicies

Modellene brukes gjennom hele prosessen



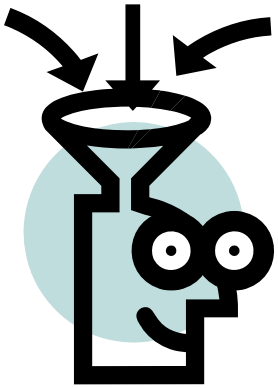
Anvendelse i industrielt case

- Analyse gjennomført på vegne av DNV høsten 2008
- DNV tilbyr en “one-stop” tjeneste for validering av elektroniske sertifikater og signaturer
  - fra ulike sertifikatautoriteter (CA’er) i ulike land
  - og med ulik kvalitet (m.h.p. krypto- og hashalgoritmer, nøkkellengde, sertifikatpolicy ...)
- Analyseobjekt: offentlig innkjøpssystem basert på elektroniske signaturer
  - med bruk av valideringstjenesten

Anvendelse i industrielt case

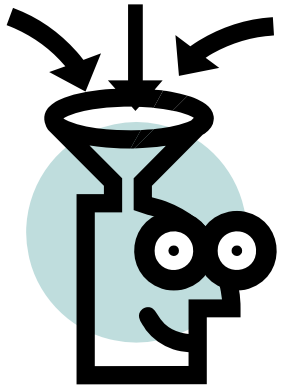
- Hvilken signaturkvalitet bør man kreve?
  - Lage policies for dette basert på analyse
- Må balansere følgende hensyn:
  - minimere risken for at ikke-autentiske tilbud aksepteres for videre evaluering (med hensyn på pris, kvalitet av produkt etc.)
  - unngå at autentiske tilbud forkastes uten videre evaluering
- Resultat: policyer som foreskriver ett av tre utvalgte kvalitetsnivåer, avhengig av pris på det som skal kjøpes

Erfaringer fra caset



- Gjennomførbarhet
  - Vi gjennomførte alle stegene (unntatt et delsteg), og lyktes i å definere anbefalte policies for valg av signaturkvalitet
- Kostnadseffektivitet
  - Analytikerne brukte i alt 127 timer (uten rapportskriving)
    - Vi antar at dette tallet kan reduseres (færre analytikere, mer erfaring)
  - De øvrige deltakerne brukte i alt 20 timer
  - Tallene må vurderes mot verdiene som står på spill i det enkelte tilfelle

Erfaringer fra caset



- Forståelighet
  - Modellene fungerte godt som hjelpemiddel til kommunikasjon
  - Mange tilfeller hvor deltakerne påpekte feil, ga tilleggsinformasjon, eller stilte spørsmål relatert til bestemte deler av modellene
  - Ved ett tilfelle (nøstede probabilistiske alternativer) var modellen vanskelig å forstå for deltakerne.
    ⇒ bruk interaction overview diagrams i stedet for vanlige sekvensdiagrammer
- Uttrykkskraft
  - Det var ingen tilfeller hvor relevant info fra deltakerne ikke lot seg uttrykke i modellene

Hva har vi oppnådd?

- Har utviklet et modelleringsspråk som kan fange inn både observerbar oppførsel og tillitsvurderinger
  - Vi kjenner ikke til andre språk for dette
- Språket egner seg for analyse av tillit og oppførsel i elektronisk samvirke (interaksjoner)
  - Hvordan bidrar tillit til å bestemme aktørers oppførsel?
  - Hvordan påvirkes aktørers tillit av observerbare faktorer?
  - I hvilken grad reflekterer en aktørs tillitsvurderinger virkeligheten – har aktøren for stor eller liten tillit til en gitt tjeneste eller annen aktør?

Hva har vi oppnådd?

- Språket kan kombineres med policy-språket for å uttrykke tillitspolicies
- Har utviklet en metode for å definere tillitspolicies
- Lovende resultater fra case-studie hos DNV

Referanser

- Atle Refsdal, Bjørnar Solhaug, and Ketil Stølen. *A UML-based method for the development of policies to support trust management*. In 2nd Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM'2008), pages 33–49. Springer, 2008.

- Atle Refsdal and Ketil Stølen. *Extending UML sequence diagrams to model trust-dependent behavior with the aim to support risk analysis*. Science of Computer Programming, 74(1-2):34–42, 2008.

- Bjørnar Solhaug and Ketil Stølen. *Compositional refinement of policies in UML – Exemplified for access control*. Technical Report A11359, SINTEF ICT, 2009