

”Rättslig Informationsförsörjning – säkerhet”

Stiftelsen för rättsinformation

Svenska Föreningen för ADB och Juridik

29 november 2007

Informationssäkerhet

En modell

Olle Olsson

Swedish Institute of Computer Science

SWEDISH
INSTITUTE OF
COMPUTER
SCIENCE

SICS

SICS – Swedish Institute of Computer Science

Nationellt
forskningsinstitut

– FoU inom IT

Mål:

– Bedriva avancerad och
fokuserad forskning
inom strategiskt viktiga
IT-områden



Sponsorer:

- TeliaSonera
- Ericsson
- Saab Systems
- FMV
- Green Cargo
- ABB
- Bombardier Transportation

Om informationssäkerhet

Säkerhet:

- Av vad?
- För vem?
- Uppnå vad?

Budskap:

- Säkerhet bidrar till tillförlitlighet
- Medel för balansering av intressentintressen

Historiska drivkrafter

”Datacentraltiden” – fokus på:

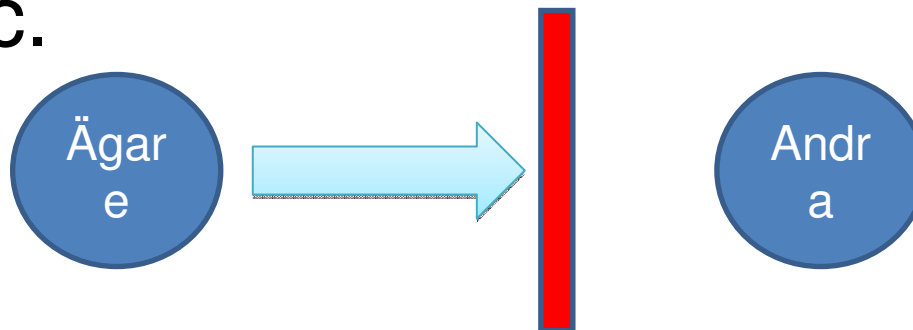
- Fysiskt skydd av data (media)
 - Ej förlora/ej förstöra (förlora egen åtkomst)
 - Oavsiktligt
 - Avsiktligt
 - Ej sprida (andra får åtkomst)
 - Stöld
- Säkerställa arkivering
 - Åtkomst inom viss framtid

Informationssäkerhet – förr

Betoning på:

- Mål: hemlighållande
- Objekt: ett hanterligt antal databaser

Begränsa tillgång, bygg murar, stäng in,
etc.



Dagens drivkrafter

Sammanhanget IKT (I nformations- och k ommunikationst eknol

Bred användning	verksamhet på IT-bas
Föränderligt landskap	teknik, verksamhet, ...
Sammanvävda	nätverkssamhället
Kritisk infrastruktur	för samhälle och aktörer
Logiskt skydd	digitala sfären – data och program
Fysiskt skydd	datorer, nätverk, minnen, ...

Övergripande mål

Information (i samhället) skall bidra till:

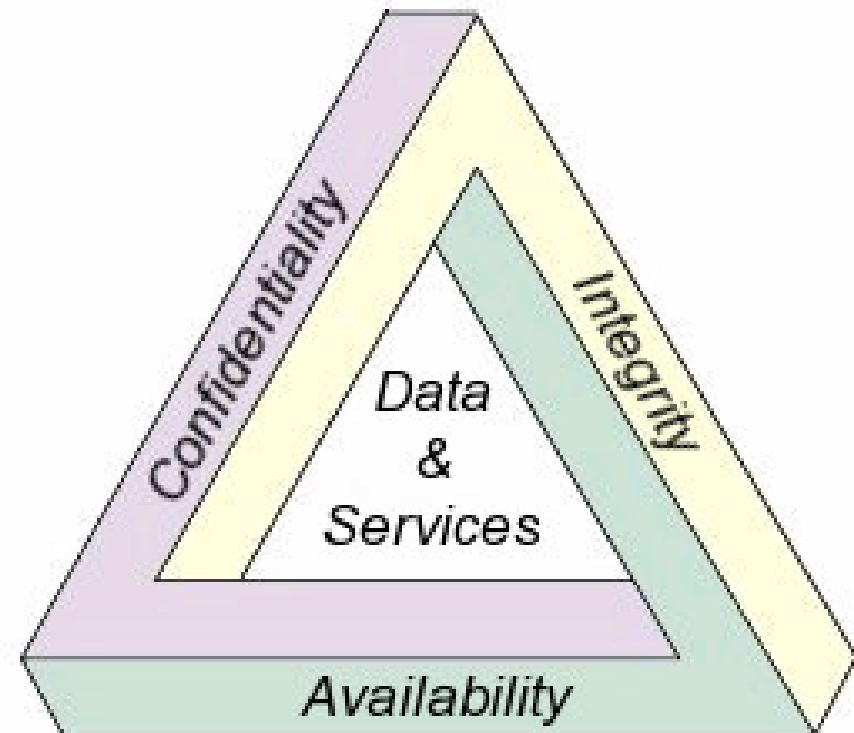
- Kostnadseffektivitet
- Kvalitet
- Transparens
- Uniformitet
- Delaktighet
- Innovativitet
- Etc. ...

Begreppet "säkerhet"

- Samlingsbegrepp
 - Ett antal icke-funktionella aspekter
- Säkerhet mångfacetterat
 - Mångdimensionellt
- Konkreta målsättningar
 - I varje sammanhang
 - För varje aspekt

Aspekter: CIA-triaden

- Konfidentialitet ("confidentiality")
 - Skyddas information mot otilbörlig åtkomst?
- Integritet ("integrity")
 - Har data ändrats otilbörligt/oönskat?
- Tillgänglighet ("availability")
 - Fås information inom rimlig tid?



Aspekter: Parkers hexad

- Konfidentialitet (“confidentiality”)
 - Vem ska inte få tillgång till information?
- Innehav (“possession”, “control”)
 - Har någon annan tillgång till information?
- Integritet (“integrity”)
 - Är informationen oförändrad?
- Autentisering (“authenticity”)
 - Är informationen tillskriven rätt källa?
- Åtkomlighet (“availability”)
 - Kan information åkommas inom rimlig tid?
- Användbarhet (“utility”)
 - Kan informationen användas på avsett sätt?

Aspekter: ytterligare några

- Autentisering av aktör (“authentication”)
 - Vem är du?
- Auktorisering av aktör (“authorization”)
 - Vad får du göra?
- Tillförlitlighet (“admissibility”)
 - Kan jag lita på dina mekanismer?
- Säkerhetsgranskning (“auditing”)
 - Är säkerheten väldefinierad och underbyggd?
- Spårbarhet (“accountability”)
 - Vem har gjort vad med data?
- Icke-förnekelse (“non-repudiation”)
 - Hur visa vem som gett vad till vem?

Medel för informationssäkerhet

Typer av medel:

- Tekniska
 - Fysiska – apparater , sladdar, kort, minnen, ...
 - Logiska – digitala mekanismer
- Administrativa
 - arbetsgång, hantering, processer
- Policies
- Lagar, förordningar, ...
- Standarder
- Etc. ...

Tekniska medel - exempel

- Konfidentialitet
 - Kryptografi
- Integritet
 - Checksummer & digitala signaturer
- Åtkomlighet
 - Indexering och sökning
- Autentisering
 - Signering

Säkerhet m.a.p. vad?

- Objekt-perspektiv:
 - Information/data
 - Tillämpning/program
 - Dator
 - Nätverk
- Process-perspektiv
 - Användande
 - Vidareförädling
 - Etc.

Riskhantering

- Komplementärt synsätt
 - Fokusskifte
- Innefattar
 - Riskanalys
 - Hot
 - Sårbarhet
 - Konsekvensanalys
 - Kostnader
- Konkret
 - Riskhanteringsplan
 - Riskhanteringsprocess

Säkerhet/risk – ekosystemet

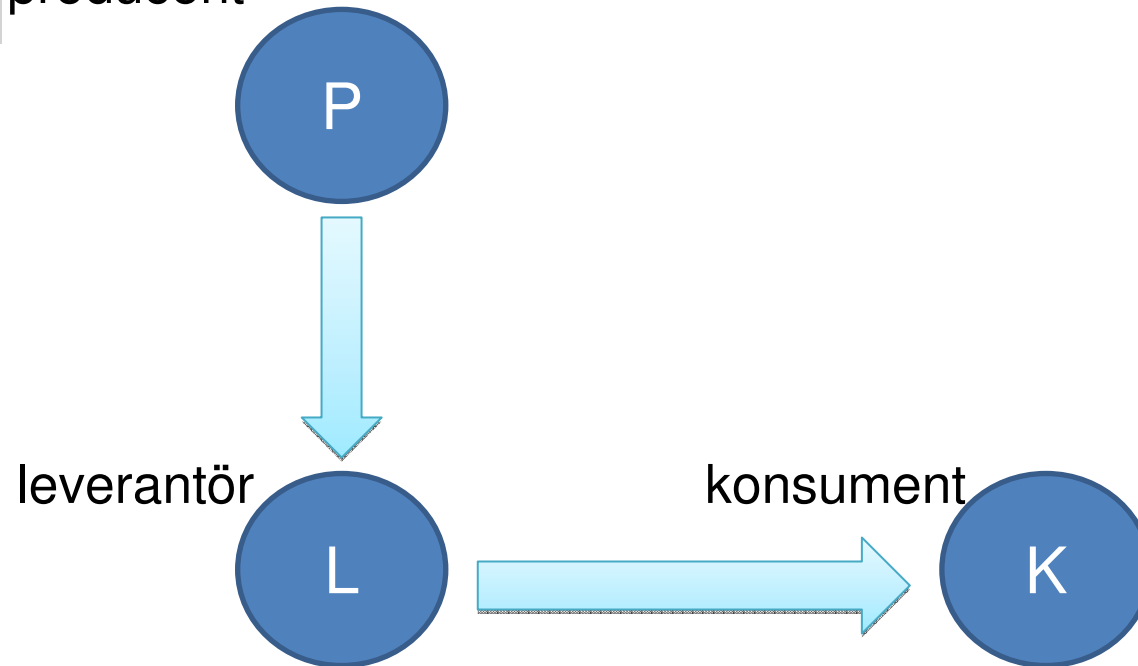
- Nätverkad värld
 - Intressenter (*stakeholders*)
 - Beroenderelationer
 - Egennyttan och ömsesidig nytta
 - Säkerhet är gemensam utmaning
- Uppnå goda effekter
 - Tillit/förtroende
 - Kostnadseffektivitet

Ekosystemet – roller

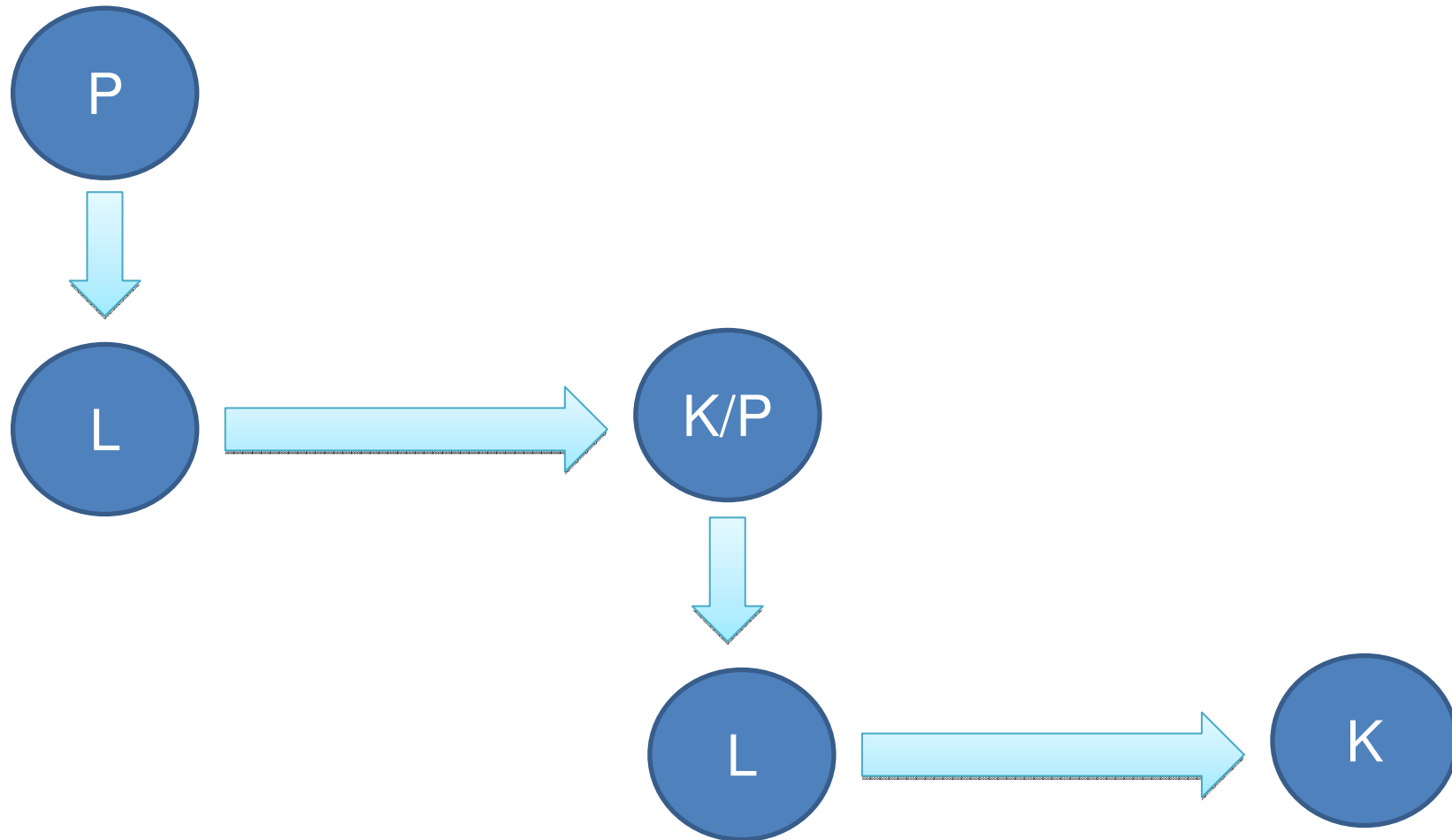
- Informationsproducenter
 - Säkerställa information ("data")
- Informationsleverantörer
 - Säkerställa informationstjänster
- Informationskonsumenter
 - Säkerställa informationsanvändning

Ekosystemet – relationer / 1

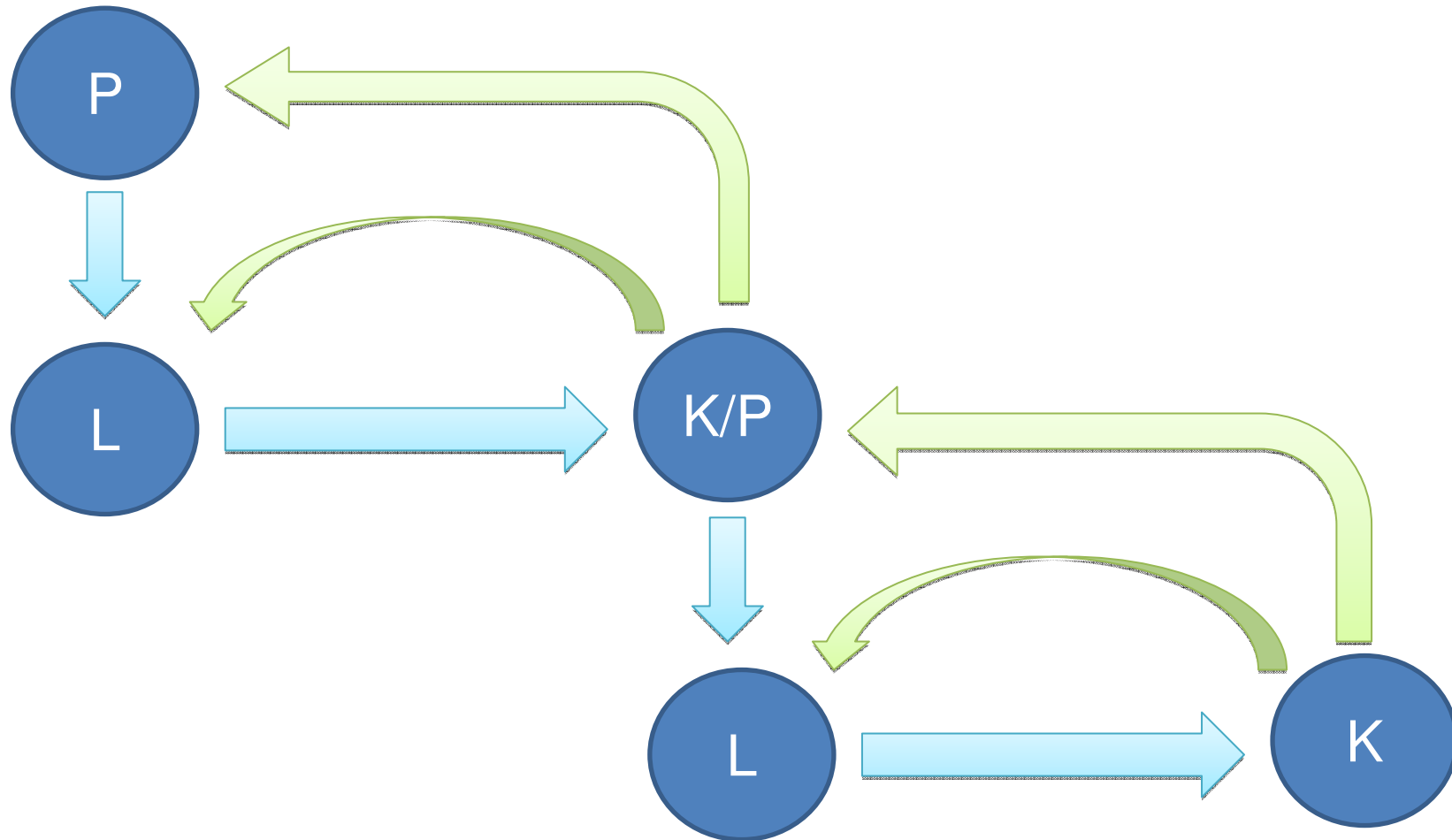
producent



Ekosystemet – relationer / 2



Återkoppling i ekosystemet



Informationssäkerhet – nu

Balansering mellan:

- Ramverk för säkerhet
- Verksamhetens kvalitets- och produktionskrav

Generellt: innefattar all verksamhetsdata

- Databaser, dokument, epost, wikis, IRC, etc.

Roll implicerar

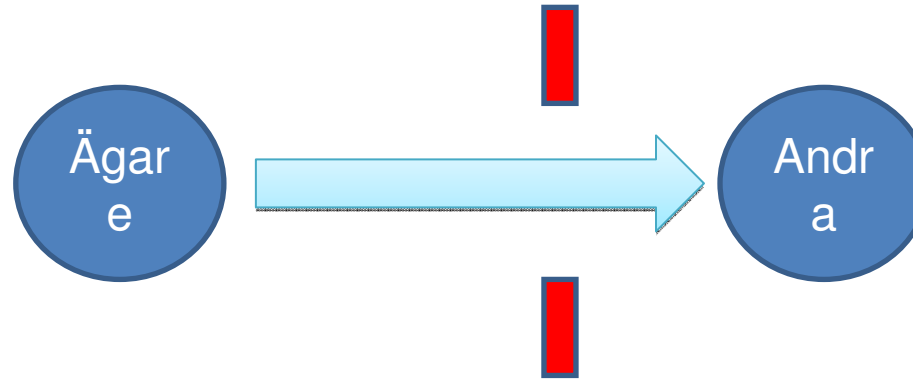
- Ansvarsområde
- Behov/önskningskrav

Relationer implicerar

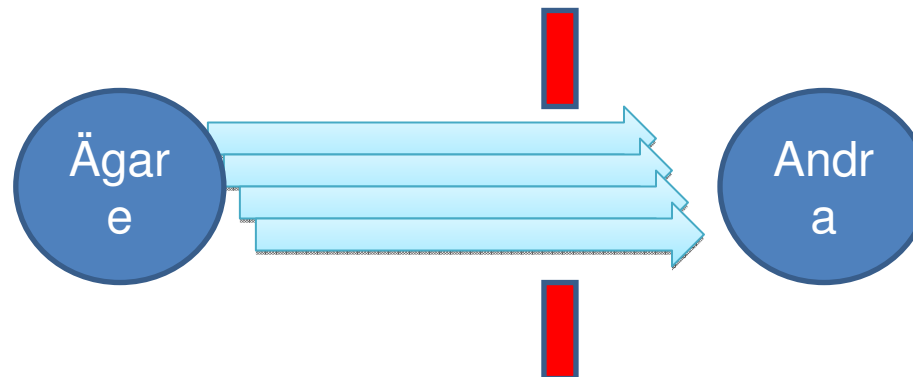
- Förväntningar

Leverantörsperspektiv / 1

- Ge tillgång till information

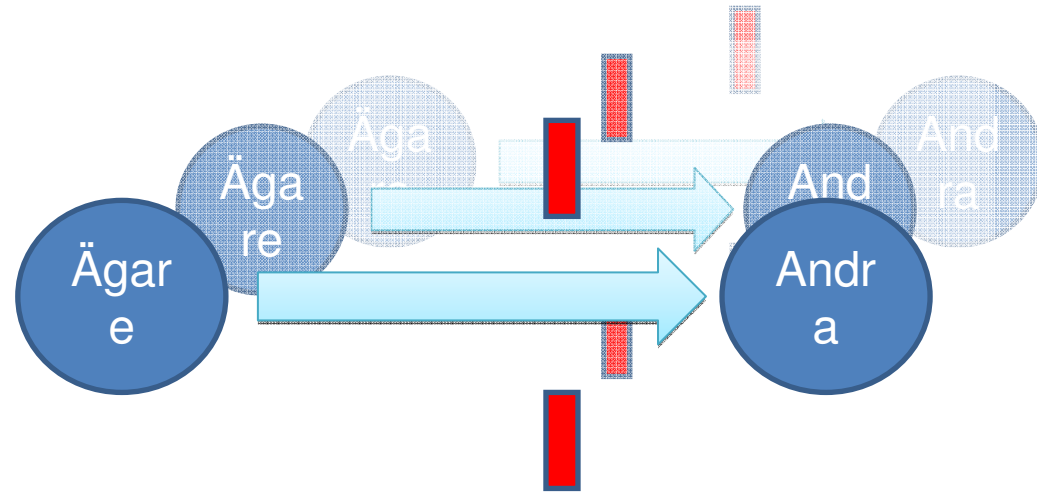


- Ge tillgång till all publicerad information

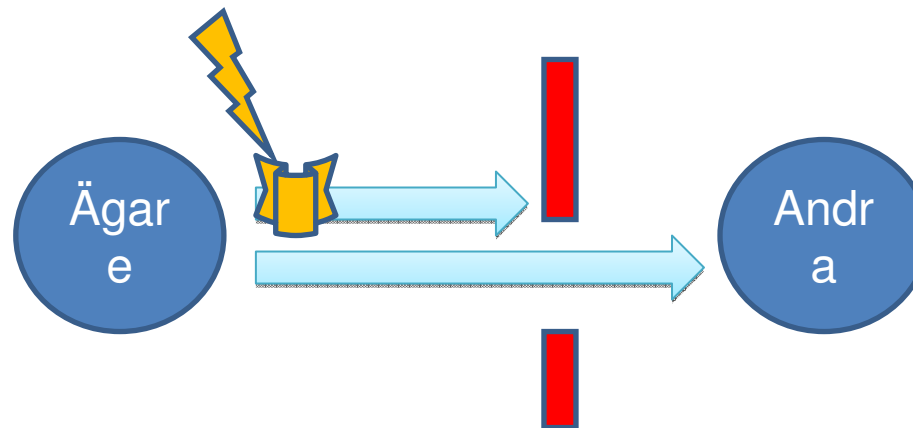


Leverantörsperspektiv / 2

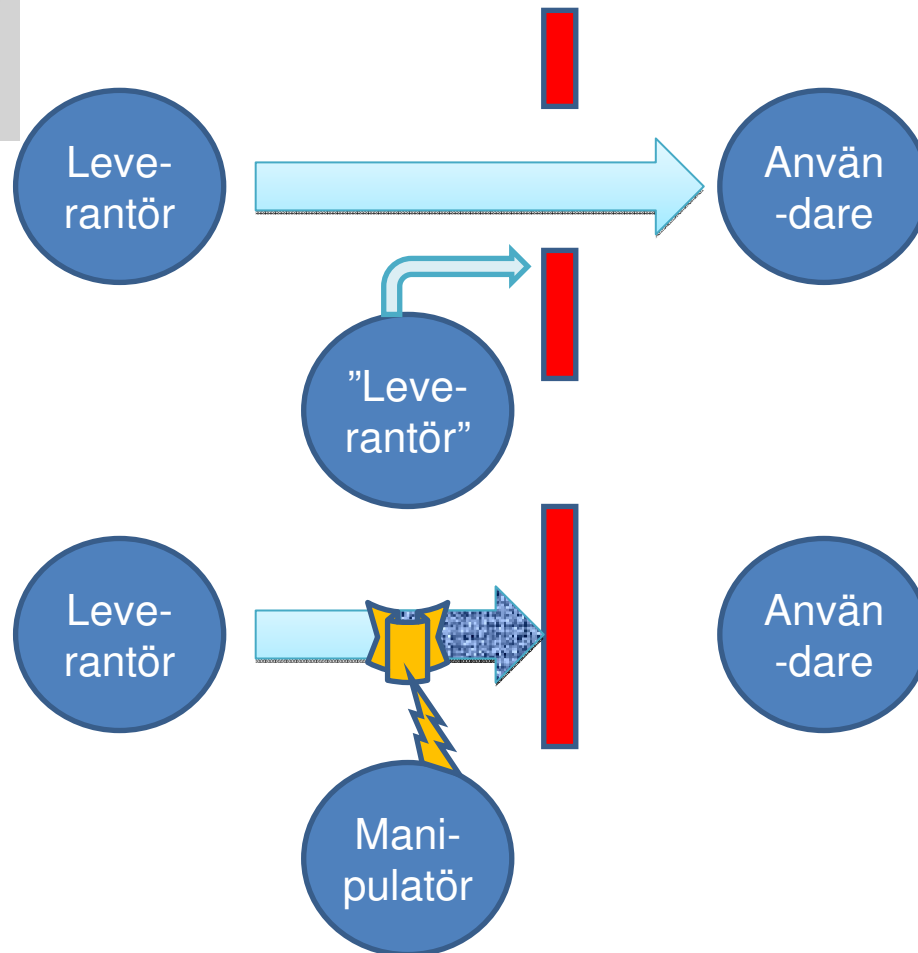
- Ge tillgång över tiden



- Ej ge tillgång till "osann" information



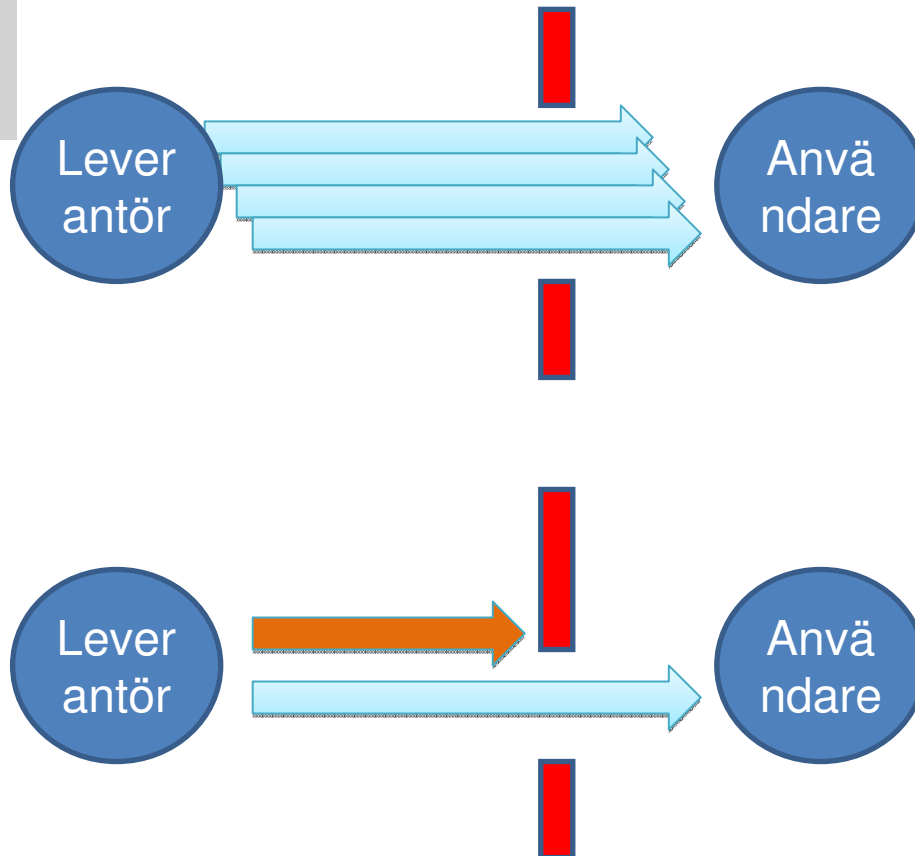
Konsumentperspektiv / 1



- Få oförfalskad information

- Ej få manipulerad information

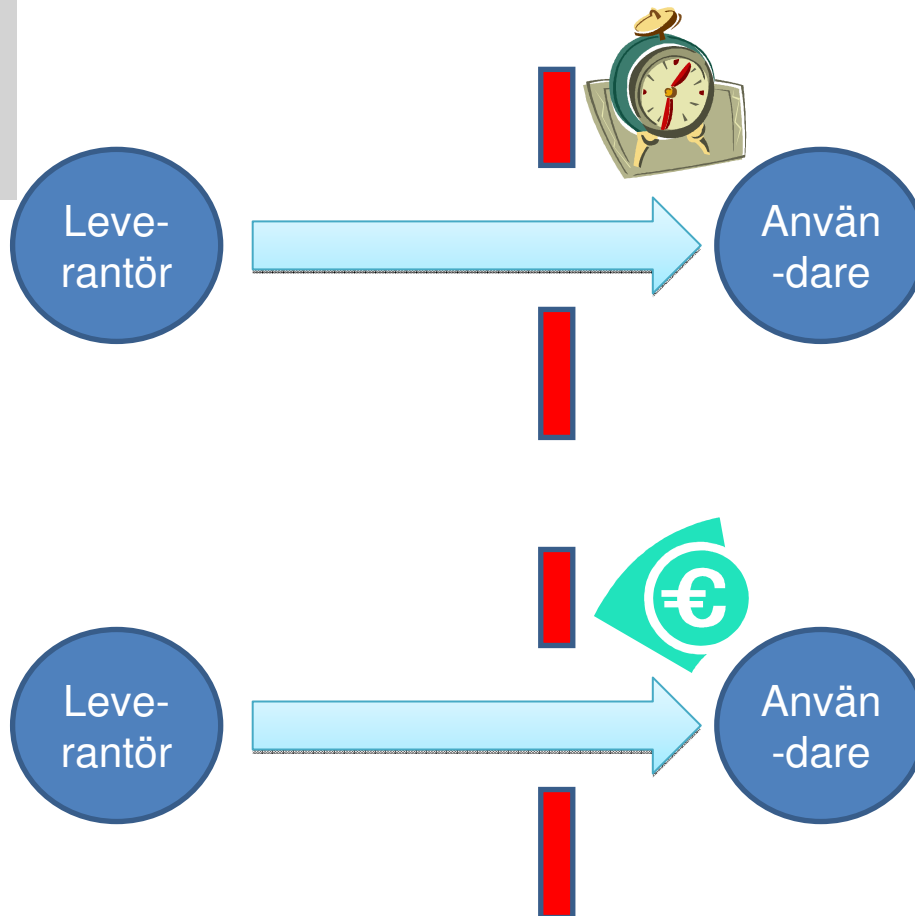
Konsumentperspektiv / 2



- Få all relevant information

- Ej få inaktuell information

Konsumentperspektiv / 3



- Få information när den behövs

- Få användbar information

Säkerhet: mål eller medel?

- Rättsinformation – ju mer användning desto bättre.
- Användbarhet är primär egenskap
 - ”Funktionell” egenskap
- Säkerhet är sekundär egenskap
 - ”Icke-funktionell” egenskap

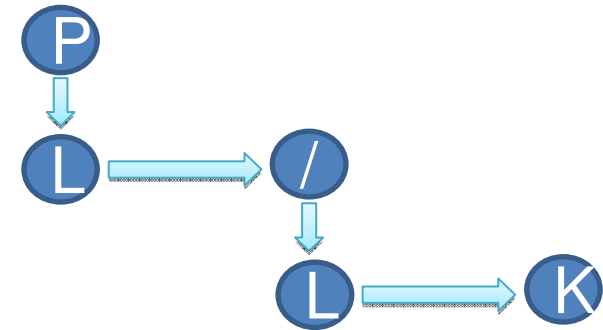
Säkerhetsaspekter - konsument

Integritet	Har data ändrats oönskat?
Tillgänglighet	Fås information inom rimlig tid?
Autentisering	Är informationen tillskriven rätt källa?
Åtkomlighet	Kan information åkommas inom rimlig tid?
Användbarhet	Kan informationen användas på avsett sätt?
Tillförlitlighet	Kan jag lita på dina mekanismer?
Säkerhetsgranskning	Är säkerheten väldefinierad och underbyggd?
Spårbarhet	Vem har gjort vad med data?
Icke-förnekelse	Hur visa vem som gett vad till vem?

Balans i försörjningskedjan

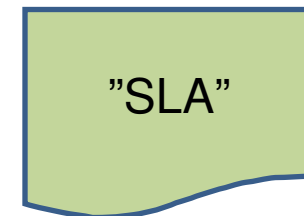
- Rättslig informationsförsörjning

- Producenter och konsumenter
- Kedjor av produktion och vidareförädling



- Balans i kedjan

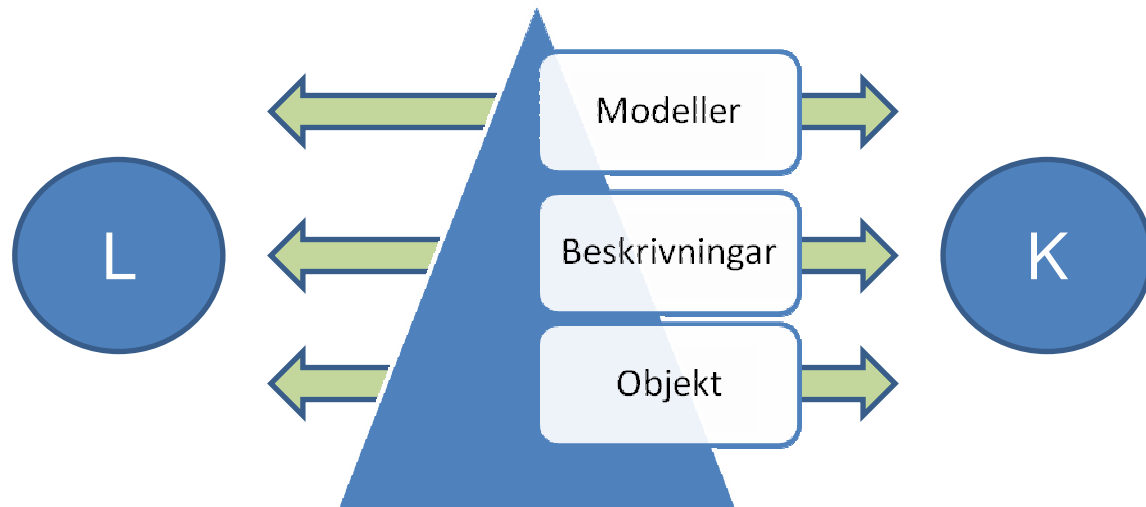
- Tydliga ömsesidiga förväntningar
- Underbyggda påståenden om att leva upp till förväntningar



Informationsförsörjningspusslet

	Dokument	Funktioner
Objekt	Innehåll	Beteende
Beskrivningar	.. av dokument ..av dokumentsamlingar	..av funktioner
Modeller	.. över beskrivningar	..över beskrivningar

Lägger grunden för
förväntningar och
åtaganden



Kvalitet i pusslet

- Objekt, beskrivningar, modeller ...
 - ...måste alla kvalitetssäkras
 - Del i gränssnittet mellan aktörer i kedjan
- En föränderlig värld
 - Ökad samordning: harmoniserad hantering av bredare informationsbaser
 - Verksamhets- och rollutveckling: hantering av ständig förändringsprocess
- Kvalitet
 - inom definierade ramar
 - över förändring i tiden

Sammanfattning

- Säkerhet rör
 - Inte bara information *i form av data*
 - Även *informationstjänster*
 - Inte bara *producentens* krav
 - Egentligen mer om *konsumentens* krav
- Informationssäkerhet
 - Underbygger tillförlitlig informationsanvändning
 - Kräver definierade mål och processer

Tack för uppmärksamheten!