

# Säker e-kommunikation 2009-04-22

---

Leif Forsman

## Agenda

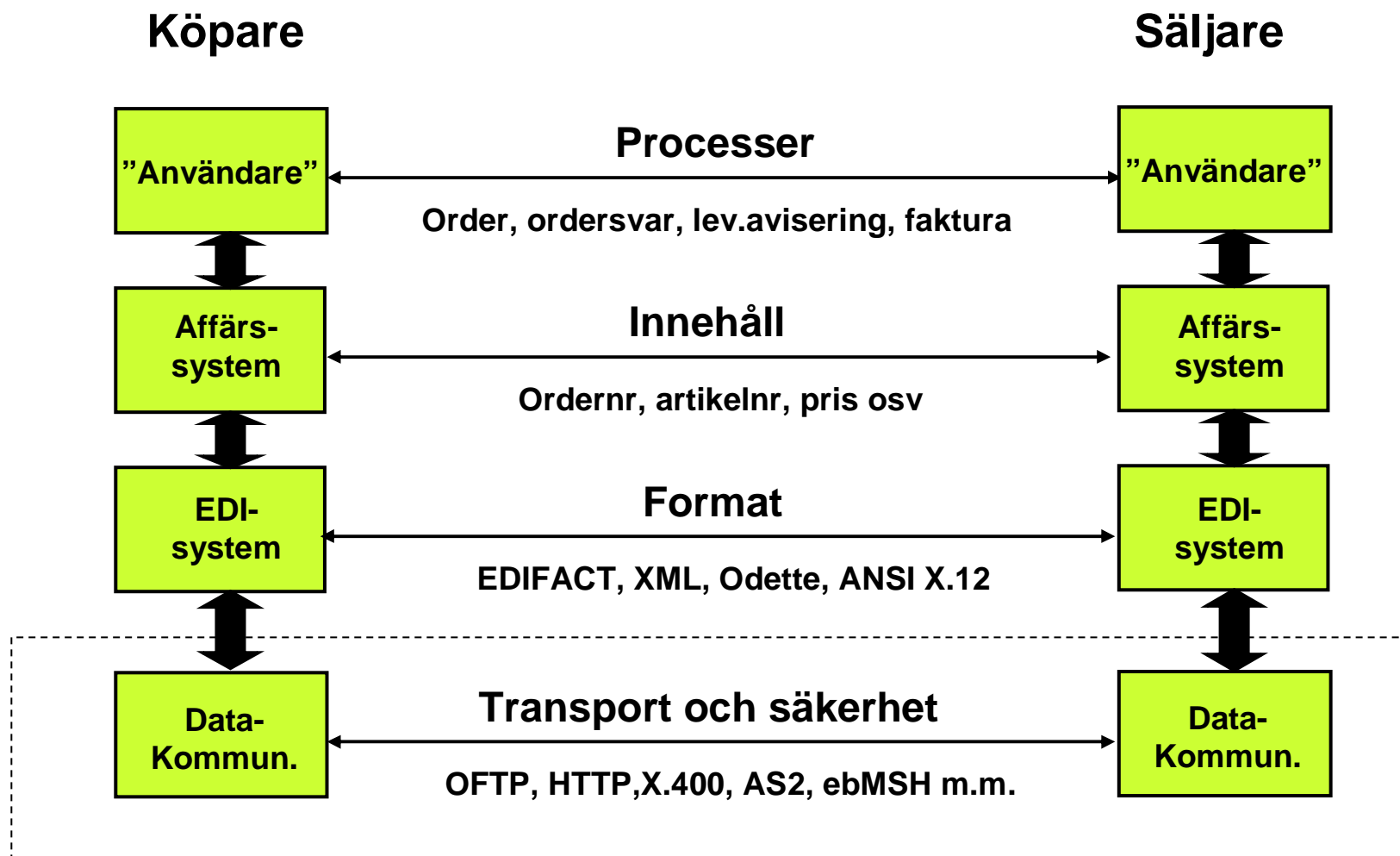
- Inledning
- Bakgrund och historik
- Vilka risker och hot finns ?
- Vilka säkerhetslösningar finns det för att skydda sig ?
- Genomgång av olika filöverföringsprotokoll och deras stöd för säkerhet
- Sammanfattning
- Frågor och diskussioner

## Vem är jag ?

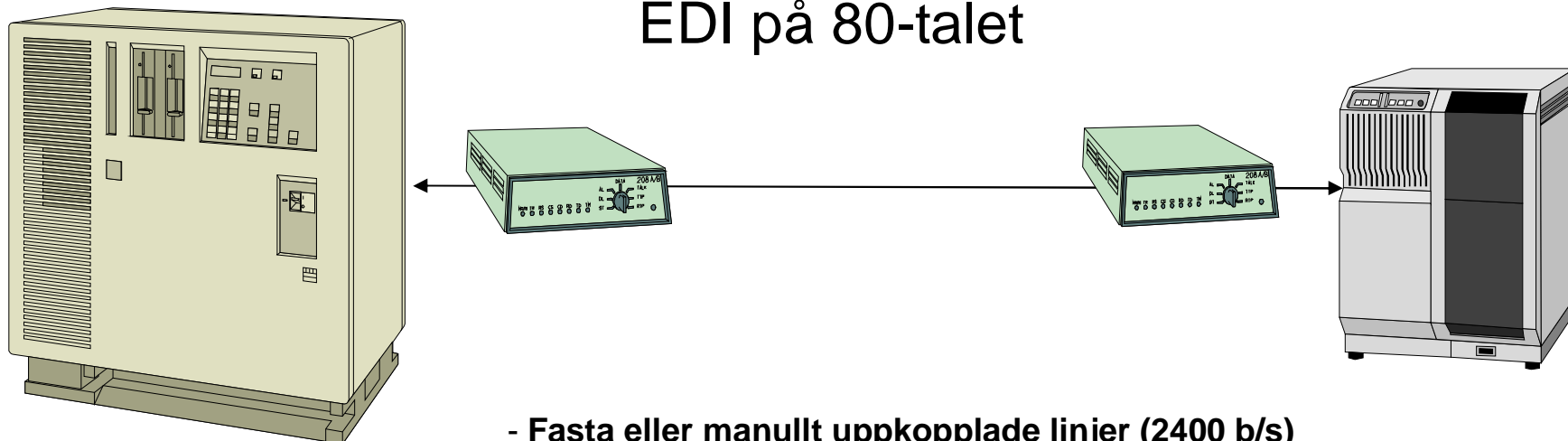
- **Arbetar på Logica (fd WM-data sen drygt 10 år)**
- **Har arbetat med EDI/e-handel i över 20 år**
  - Logica (WM-data)
  - PostNet
  - ASG (DHL)
  - EDIS/GEA/NEA
- **Jobbade med utveckling av datakommunikations-system på Ericsson under 10 år (bla Datex-nätet)**



# OSI-modell för EDI



## EDI på 80-talet



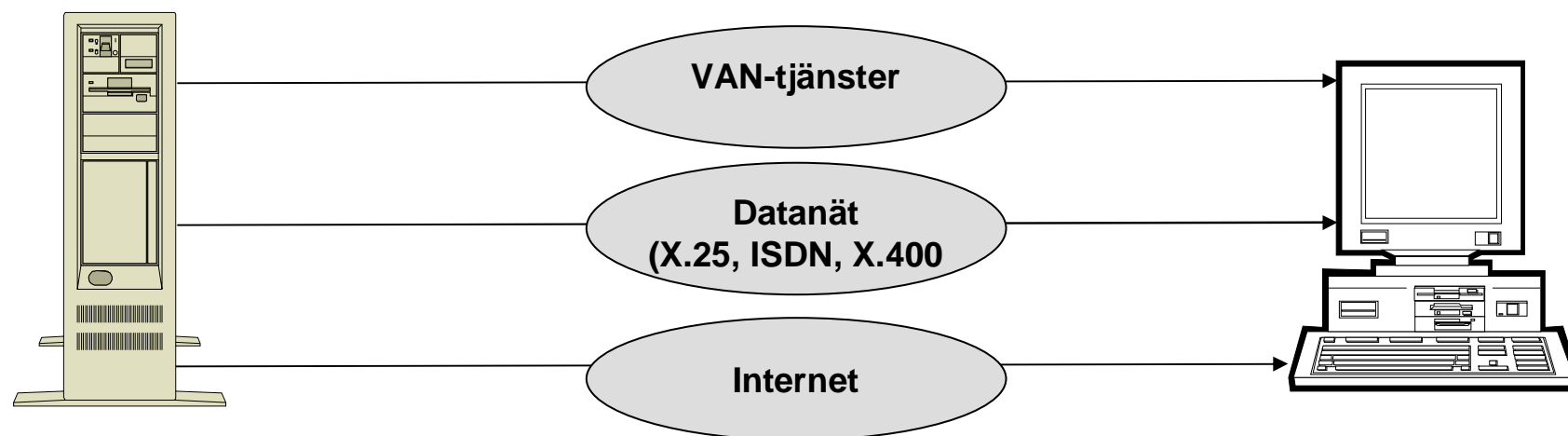
- Fasta eller manuellt uppkopplade linjer (2400 b/s)
- Binärsynkrona protokoll (IBM BSC 2780)
- Batchöverföringar (1-3 gånger/dag)
- Dyrt
- Få parter
- Låg säkerhetsrisk

## Men det började hända saker:

Bilindustrin skapade Odette-konceptet  
(Meddelandeformat och, filöverföringsprotokollet  
OFTP)

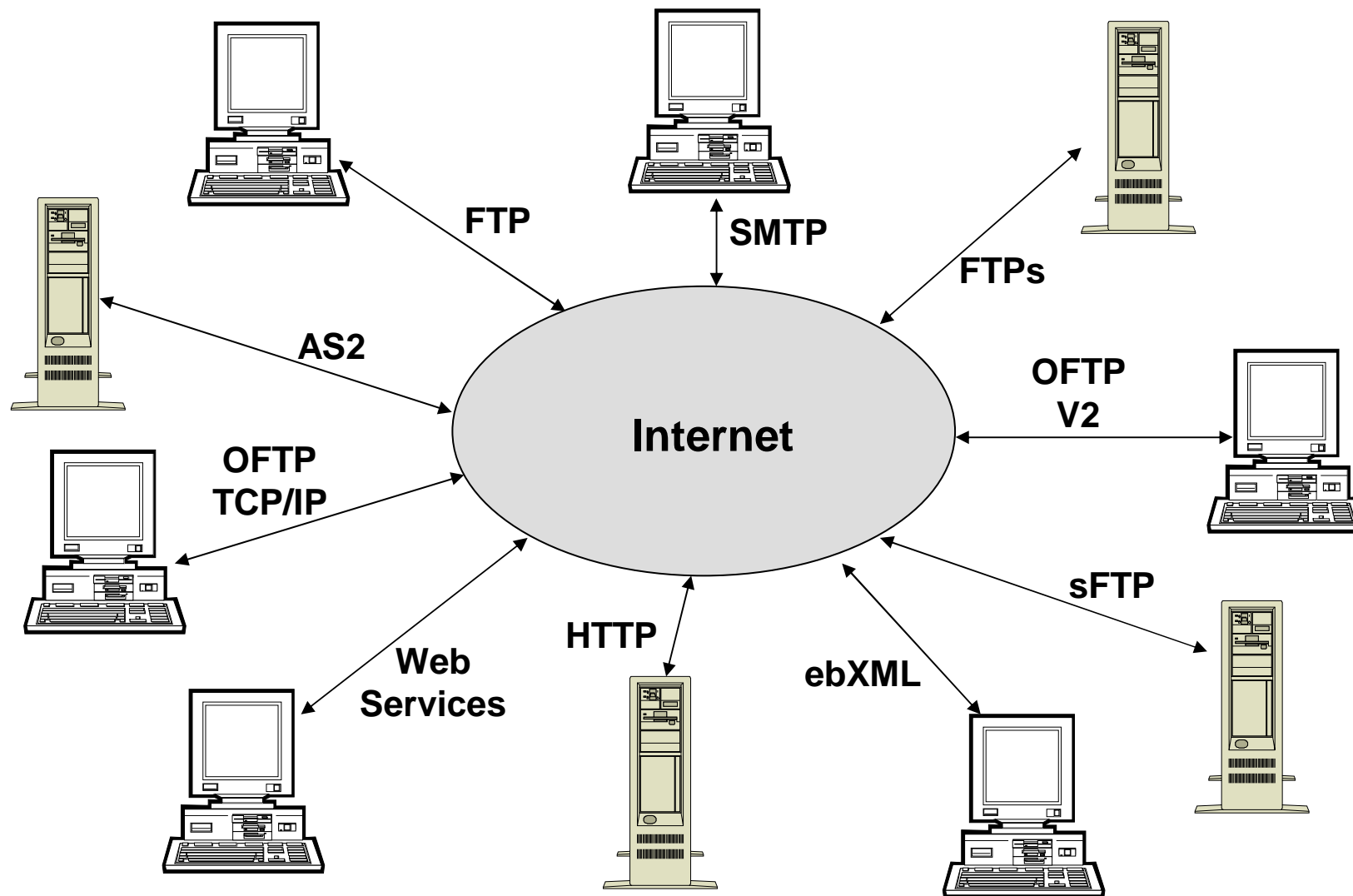
- EDIFACT föddes (standard för EDI-meddelanden)
- Dedikerade nätverk för datakommunikation (Datex X.21, Datapak X.25, ISDN).

## 90-talet



- Toppledarforum väljer X.400 som kommunikationsstandard
- Tulldata väljer OFTP/X.25 som kommunikationsstandard
- Internet börjar användas för EDI

# 2000-talet



## Historik sammanfattning

- Internet är bärare för all ny EDI-kommunikation
- Det innebär att det är ”billigt”, men även ökade risker
- Det finns många olika kommunikationsprotokoll att välja på
- Dessa erbjuder mer eller mindre säkerhet
- Man kan komplettera säkerheten i kommunikationsprotokollen med signering och kryptering på meddelandenivå
- Och vad ska man då välja ?
- Behoven och kraven ska styra detta !

## Vilka risker behöver man beakta ?

- Meddelanden kan försvinna
- Meddelanden kan förändras innan de når mottagaren
- Någon kan läsa/avlyssna innehållet i meddelanden
- Meddelanden kan skickas av falsk avsändare
- Någon part kan förneka att man skickat eller tagit emot ett meddelande
  
- Sannolikheten och konsekvensen av detta ska ställas i relation till säkerheten i den befintliga lösningen
- Säkerhet kostar och är komplicerat och ska därmed ha rätt nivå
- Legala krav kan kräva att dokument garanterat ska kunna knytas till ett företag eller en person

## Olika typer av säkerhet

- **Säker transport av elektroniska dokument (att dom verkligen kommer fram)**
- **Skydd mot förändring av innehållet i dokumenten**
- **Skydd mot insyn i dokumentens innehåll**
- **Säker verifiering av avsändare**
- **Säker verifiering av mottagare**
- **”Icke förnekbarhet av avsändande”**
- **”Icke förnekbarhet av mottagande”**

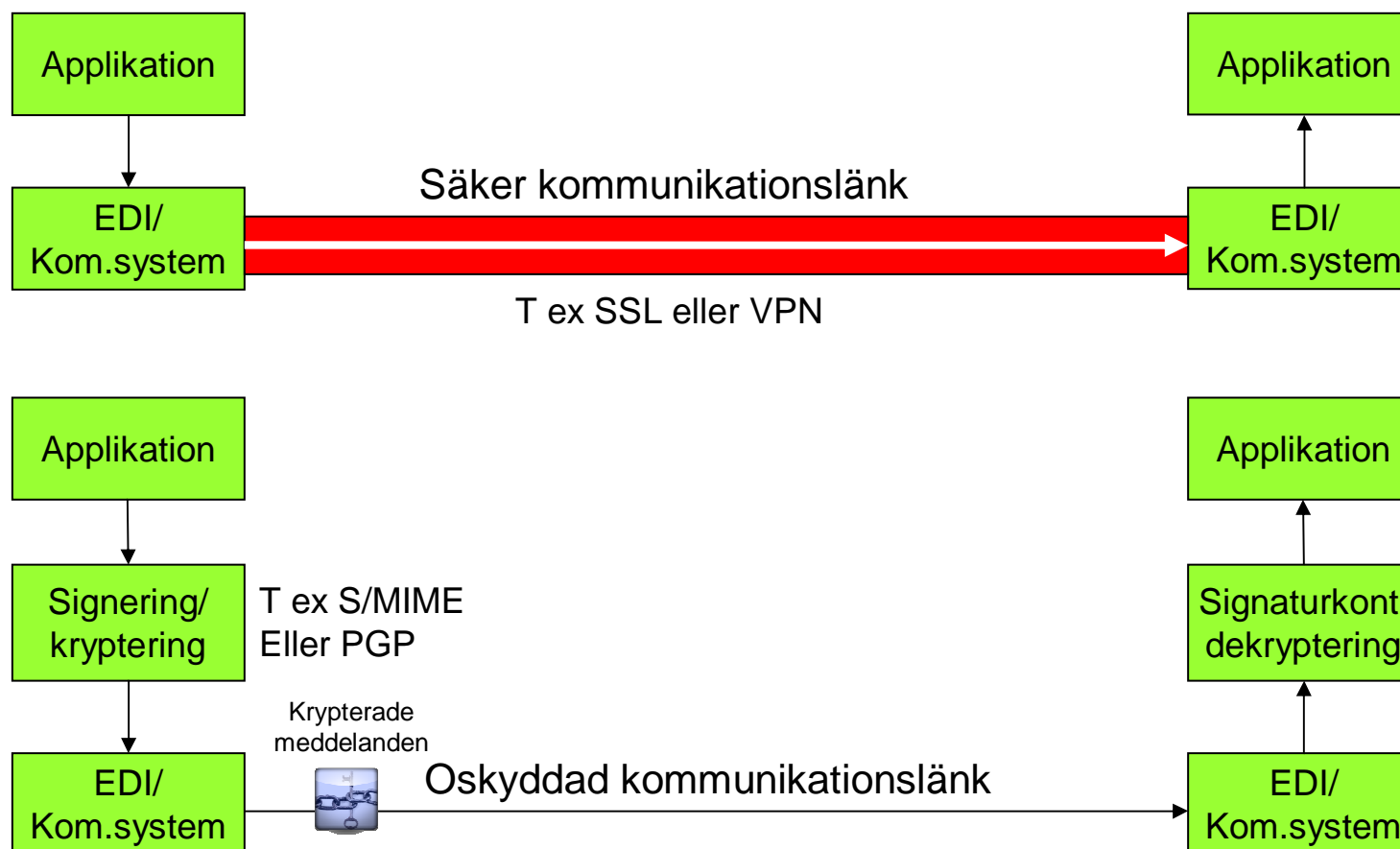
## Säker transport av elektroniska dokument

- **Välj endast professionella kommunikationsprodukter!**
- **Välj ett kommunikationsprotokoll som matchar de krav som finns**
- **Säkerställ att lösningen loggar både lyckade och misslyckade överföringar**
- **Lösningen bör ha automatisk omsändning**
- **Larm ska kunna skapas när en överföringen misslyckats (efter omsändning)**
- **Det ska vara möjligt att söka i loggar för undersöka hur en överföring gått**
- **Loggar bör sparas minst 3 månader**
- **Räkna med att Din motparts system inte fungerar lika bra som Ditt !**
- **Kommunikationsprotokoll med bra kvittensfunktioner är att föredra**

# Skydd mot insyn och förändring

Det finns två modeller för att säkerställa detta:

- Via en säker "tunnel"
- Genom signering/kryptering av själva meddelandet



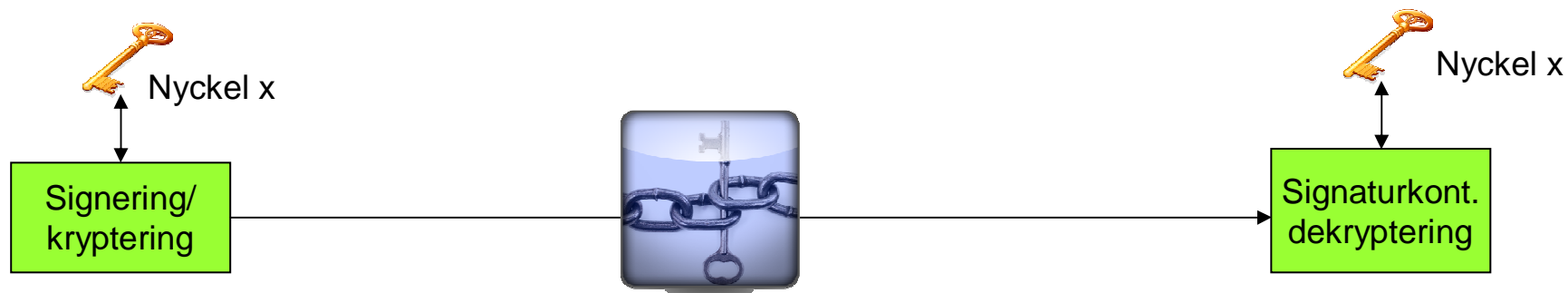
## Nyckeln till säkerhet är sigillnycklar och certifikat

Två olika typer av sigillnycklar kan användas:

- Symmetriska
- Asymmetriska.

### Symmetriska

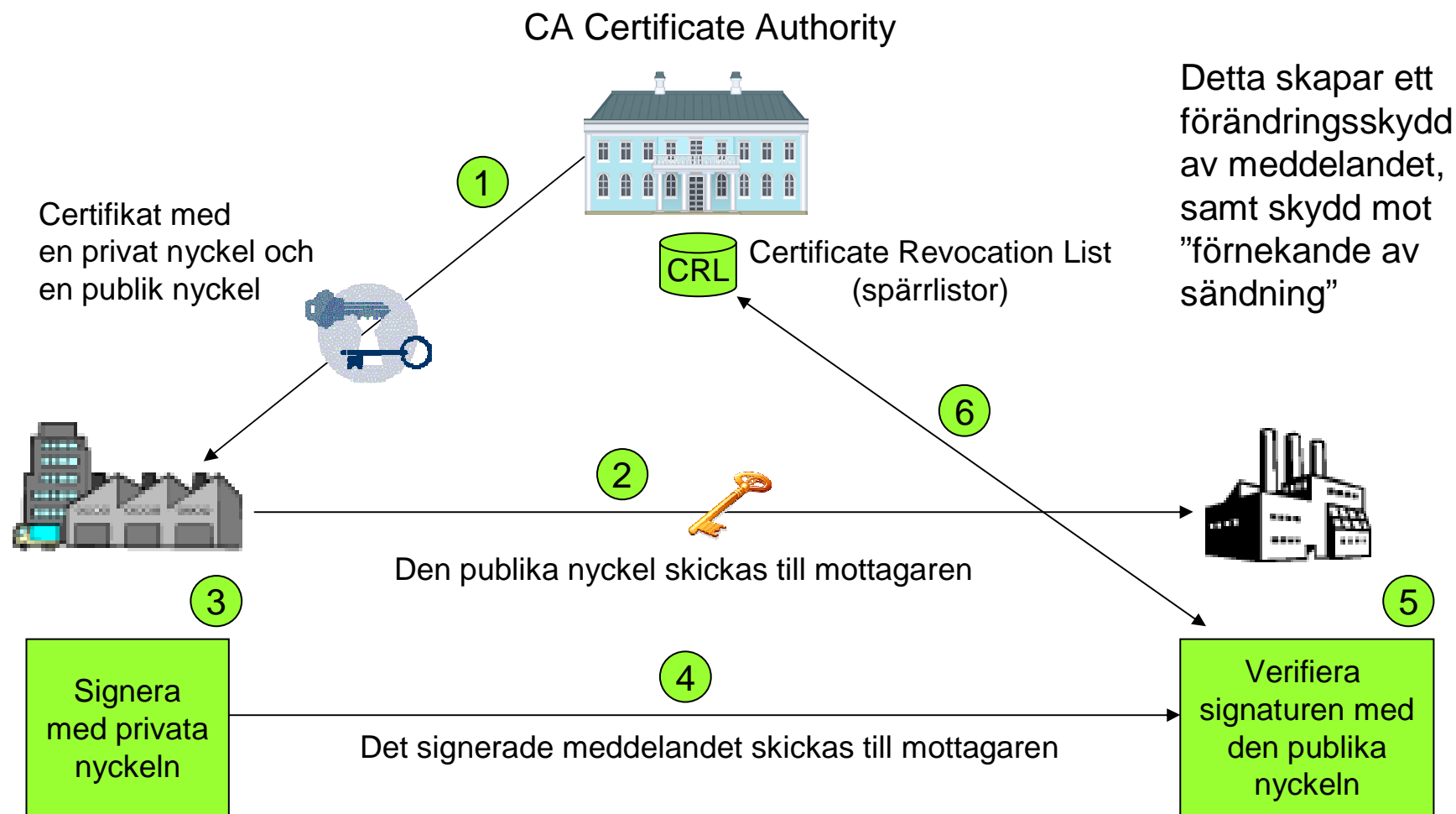
Samma sigillnyckel används hos avsändaren och mottagaren.



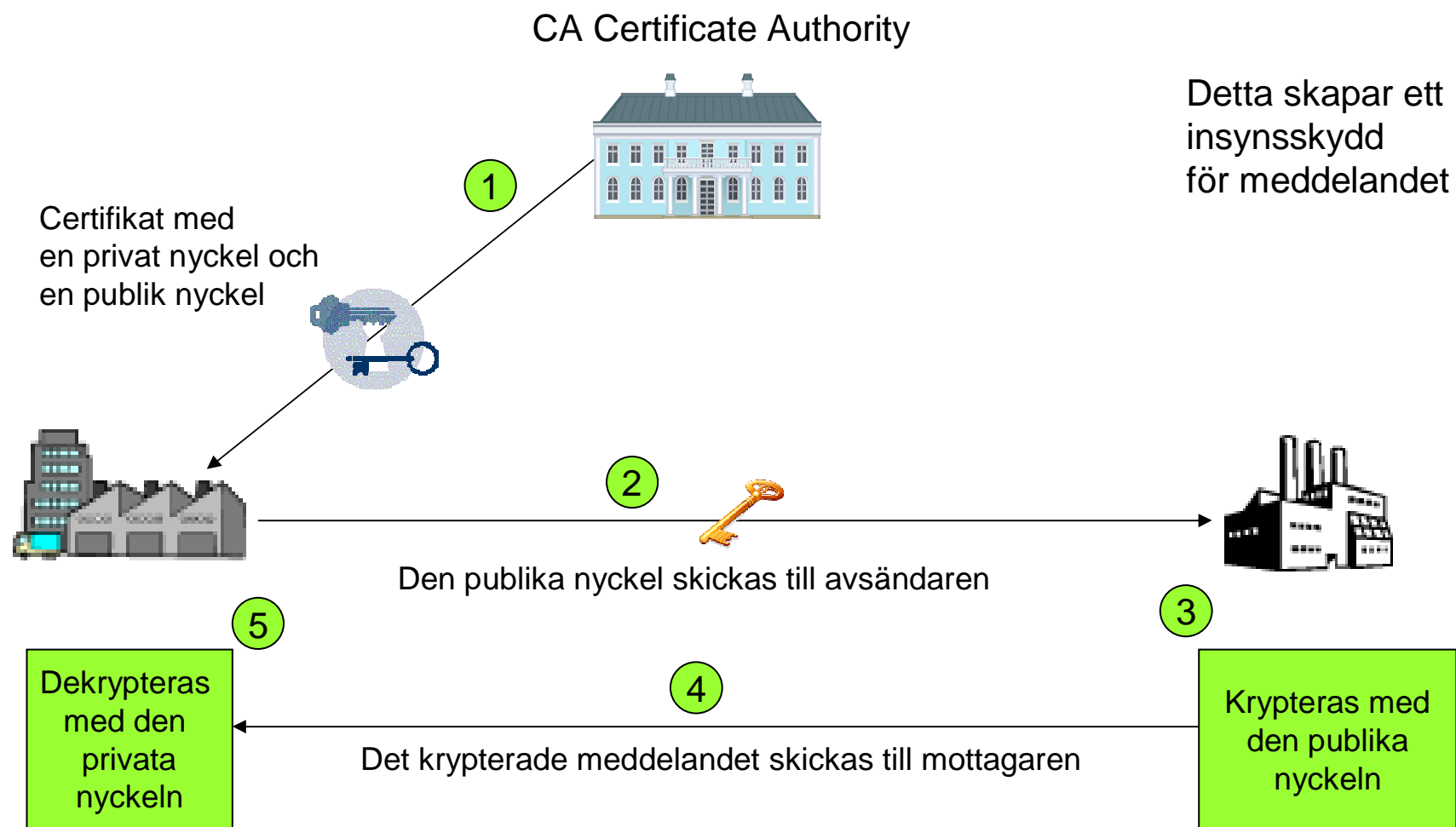
**Nackdelar:**

- De hemliga sigillnycklarna måste skickas mellan parterna

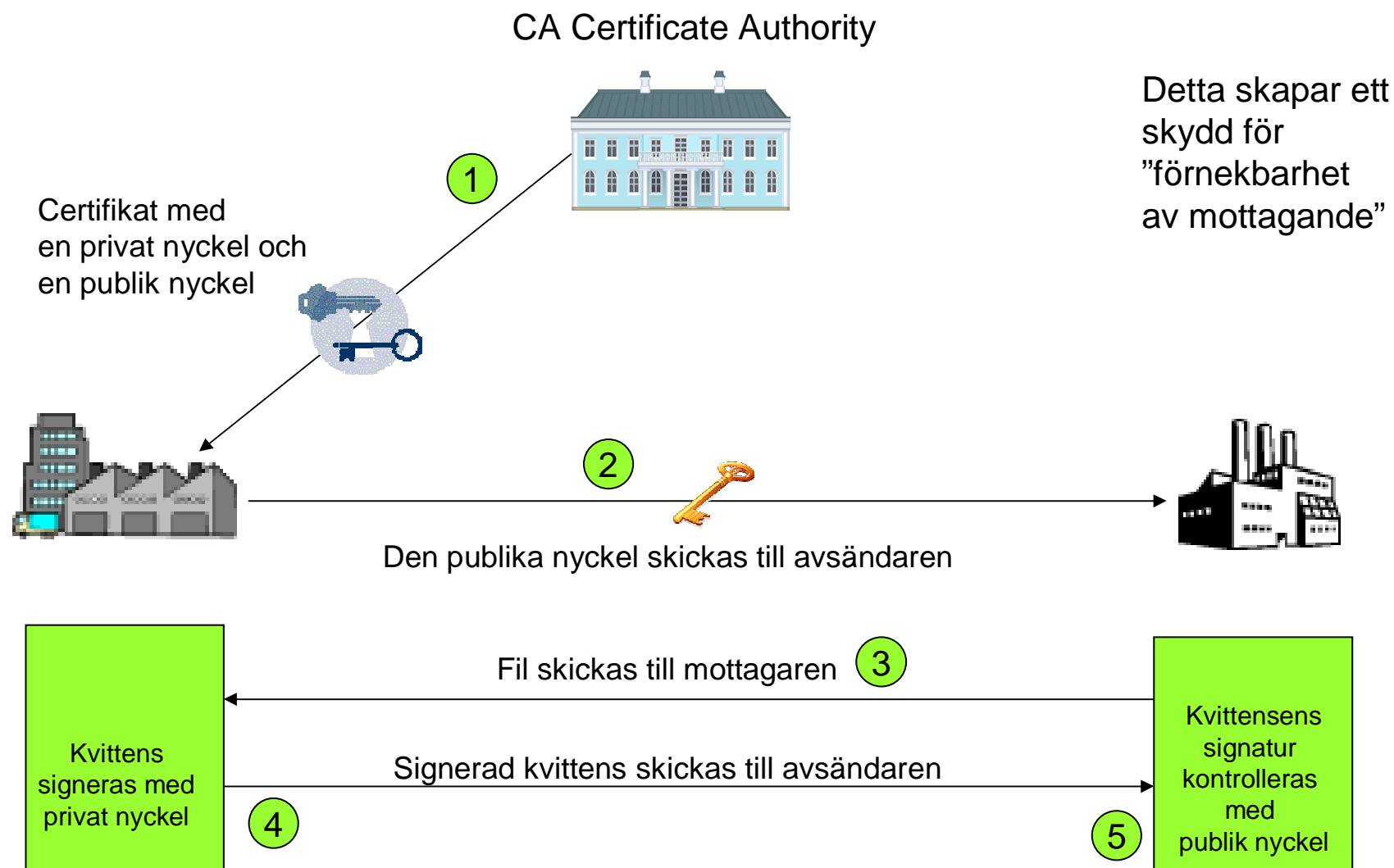
# PKI (Public Key Infrastructure), asymmetriska nycklar, signering



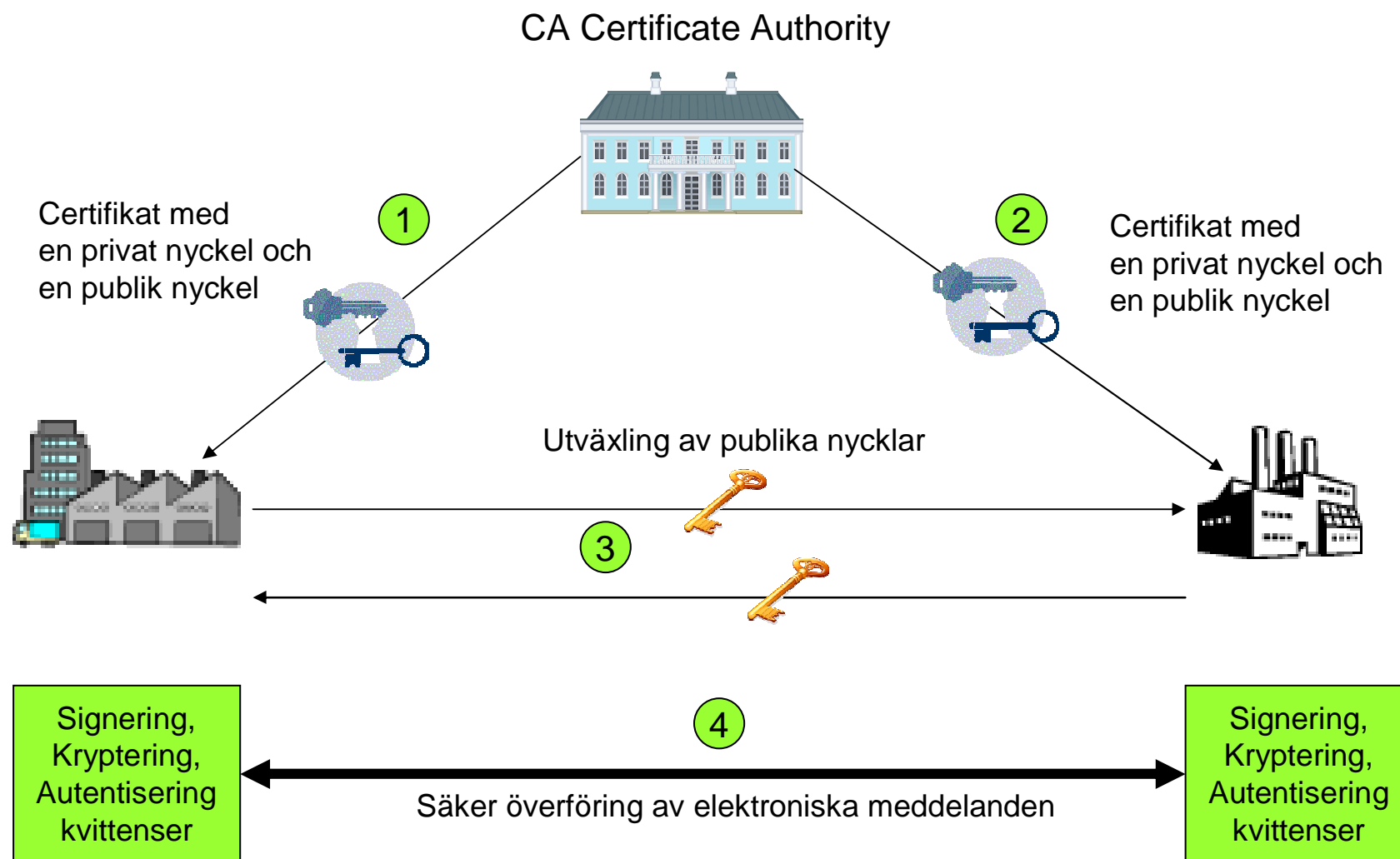
# PKI (Public Key Infrastructure), asymmetriska nycklar, kryptering



# PKI (Public Key Infrastructure), asymmetriska nycklar, signerad kvittens

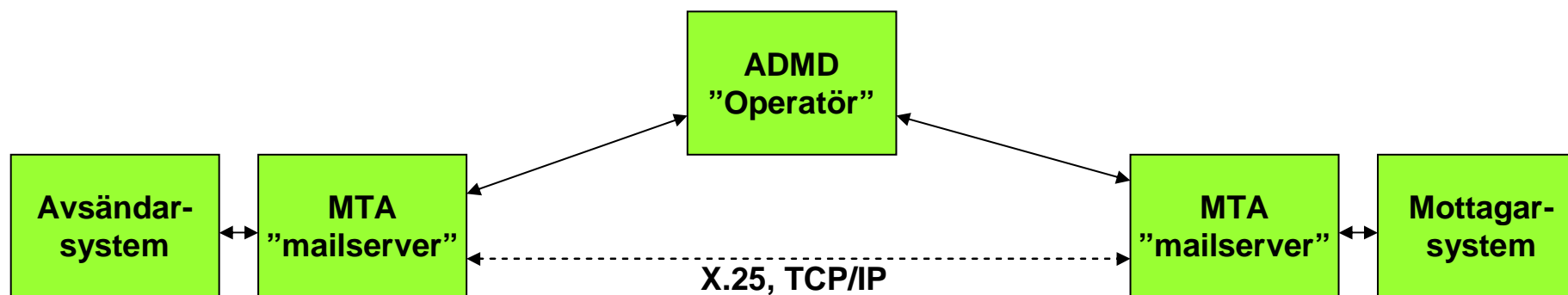


# PKI (Public Key Infrastructure), asymmetriska nycklar



## X.400

- Ursprungligen framtaget för elektronisk post
- Avancerat protokoll med många funktioner (komplext)
- Mycket bra kvittenser i två nivåer
- Dyrt att skicka via ADMD
- Ej över Internet (säkert)
- Dyra produkter
- Utdöende protokoll



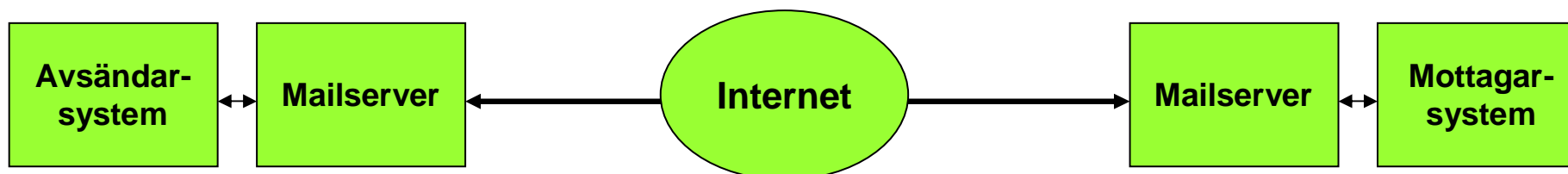
## OFTP Version 1

- Framtaget av bilindustrin på 80-talet
- Punkt-till-punkt protokoll
- Har utvecklats under åren
- Mycket bra kvittenser i två nivåer
- Enkelt att administrera och ansluta nya parter
- Ej över Internet (säkert)
- Nätkostnader
- Produkter finns för alla plattformar
- Relativt dyra produkter



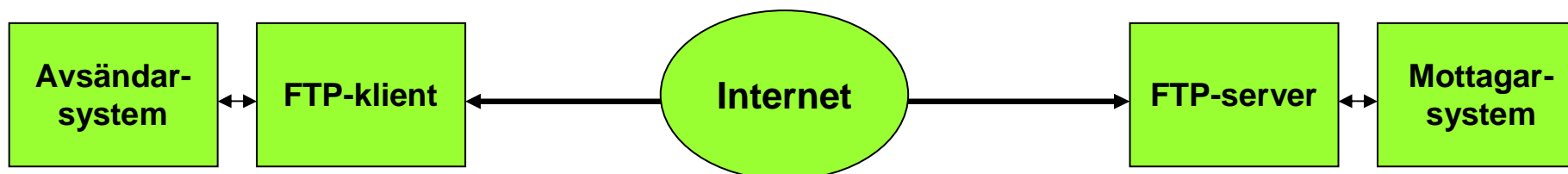
# SMTP

- Ej punkt-till-punkt (kan ta lång tid)
- Över Internet (osäkert)
- Dåliga kvittenser
- Enkelt
- Ej för tidskritiska meddelanden



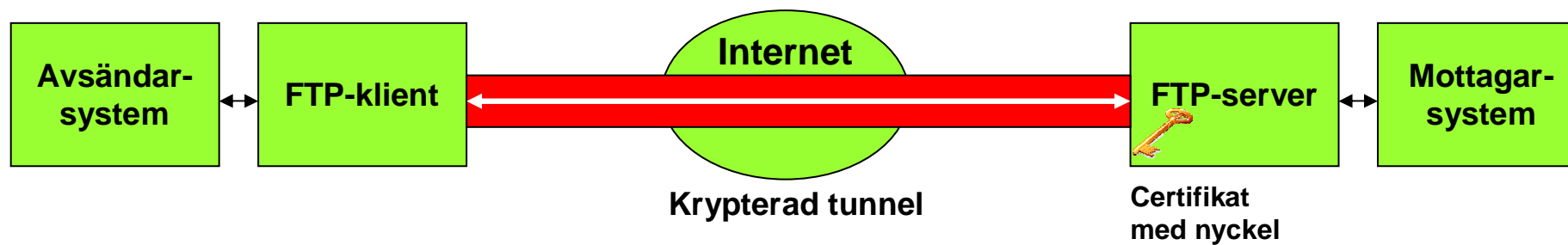
# FTP

- Punkt-till-punkt
- Enkelt protokoll
- Över Internet (osäkert)
- Enkla kvittenser
- Finns många billiga produkter
- Saknar ofta bra loggnings/övervakningsfunktioner



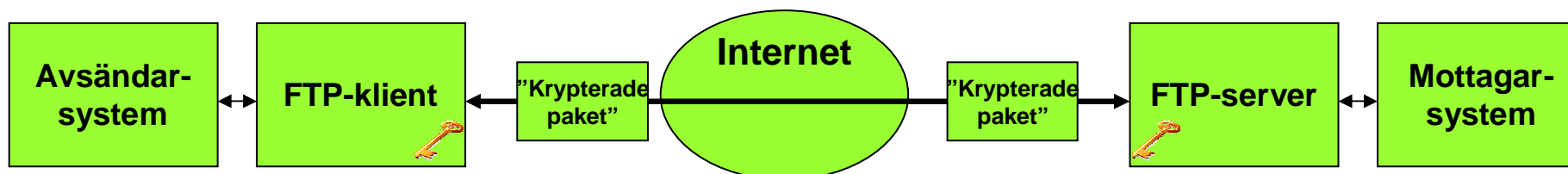
## FTPs

- Punkt-till-punkt
- Enkelt protokoll
- SSL över Internet (säkert)
- Enkla kvittenser
- Saknar ofta bra loggnings/övervakningsfunktioner



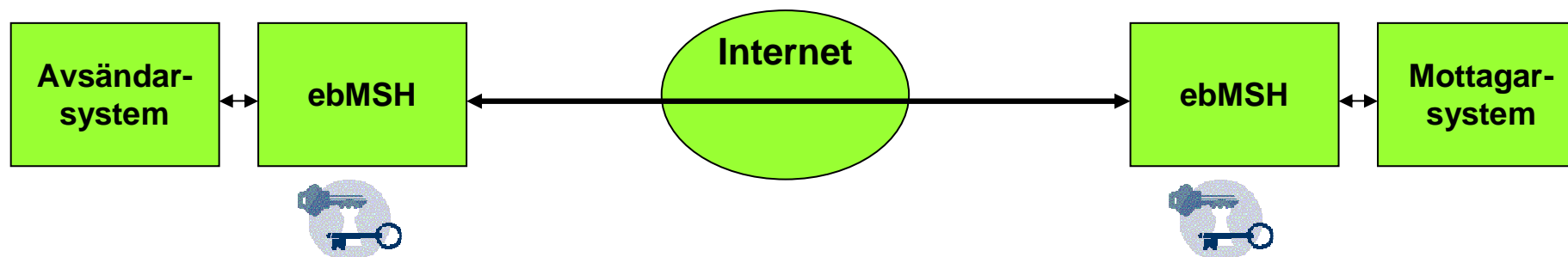
## sFTP

- Punkt-till-punkt
- Finns i många plattformar och produkter
- Krypterat (SSH) över Internet (säkert)
- Enkla kvittenser
- Saknar ofta bra loggnings/övervakningsfunktioner
- Kan kräva administration av nyckelpar



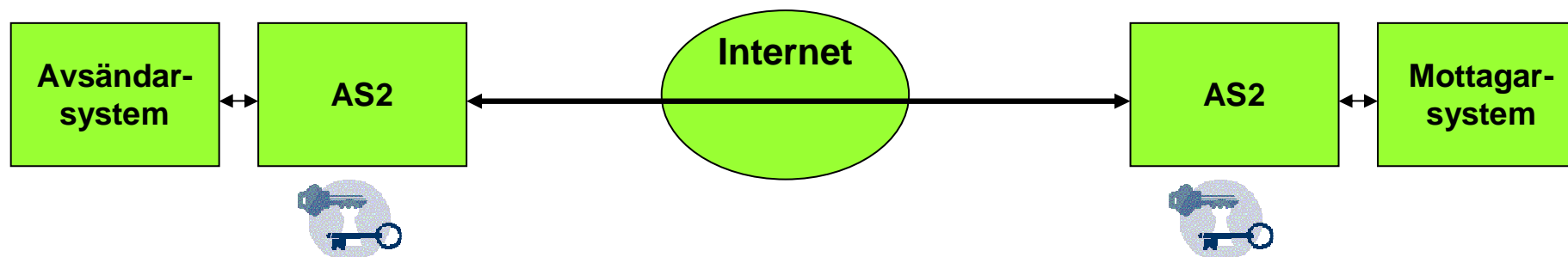
## ebXML

- En del av ebXML-standarden (ISO-standard)
- Avancerat protokoll med många funktion (komplext)
- Mycket bra kvittenser
- Har bra stöd för omsändning, loggning m.m.
- Har stöd för en mängd olika säkerhetsfunktioner (signering, kryptering)
- Ännu ej så spritt
- Svefakturans Transportprofil Bas bygger på denna standard
- Open-source produkter finns



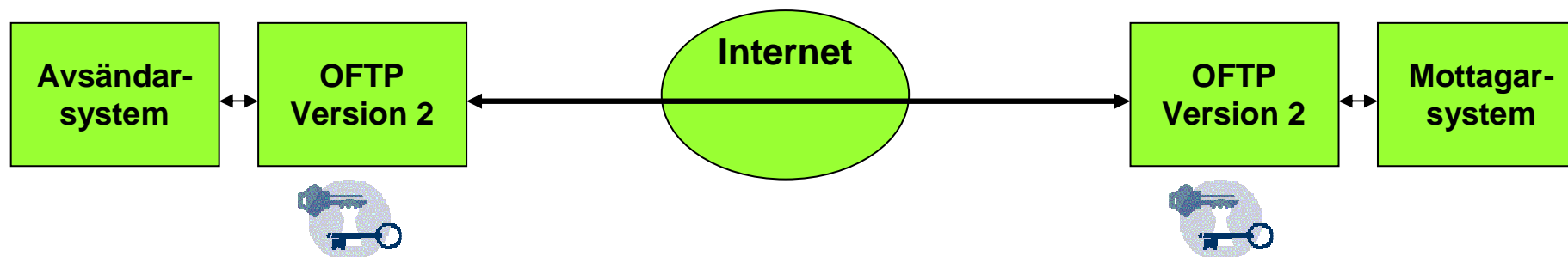
## AS2

- Protokoll som kommer från USA
- Avancerat protokoll med många funktion (komplext)
- Mycket bra kvittenser
- Har stöd för omsändning loggning m.m.
- Har stöd för en mängd olika säkerhetsfunktioner (signering, kryptering)
- Ej så spritt i Europa, men kommer mer och mer
- Dyra produkter



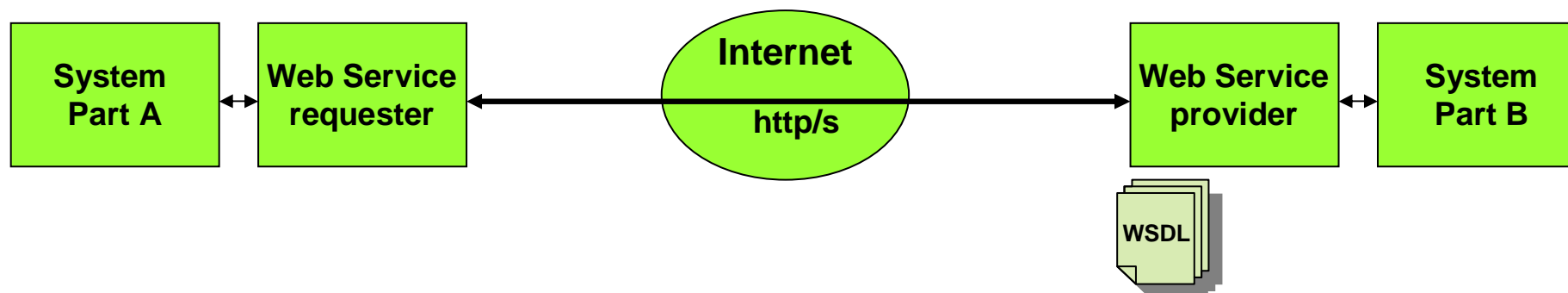
## OFTP Version 2

- Vidareutveckling av OFTP version 1 för Internet-kommunikation
- Bakåtkompatibelt mot tidigare OFTP-versioner
- Mycket bra kvittenser
- Har stöd för en mängd olika säkerhetsfunktioner (signering, kryptering)
- Ännu ej så spritt
- Få (dyra) produkter



## Web Service

- Ramverk/koncept inom SOA-arkitekturen
- Passar framförallt för fråga/svar i realtid (API)
- Ingen standard för "filöverföring"
- Det går att skapa en Web Service för att lämna eller ta emot EDI-meddelanden
- Har stöd för krypterad trafik (SSL)
- Ännu ej så spritt för EDI



## Sammanfattning

- **Behovet av säkerhetsfunktioner har ökat**
- **Minimikravet är att ha en säker funktion för transport med bra loggning**
- **Det finns ett stort utbud av lösningar för att skapa högre säkerhet**
- **Säkerhet är komplext och kostar pengar**
- **Behoven ska styra vilka säkerhetsfunktioner man ska använda**

## Frågor och diskussioner