



Stockholms  
universitet

# eLeg 2.0

Leif Johansson

Internetdagarna 2008

## Ny form för eLeg:

- Enklare för tjänsteleverantörer.
- Konkurrensutsätt alla led.
- Bättre skydd för den personliga integriteten.
- Ingen Single Point of Failure

# Enklare

# Öppen teknologi

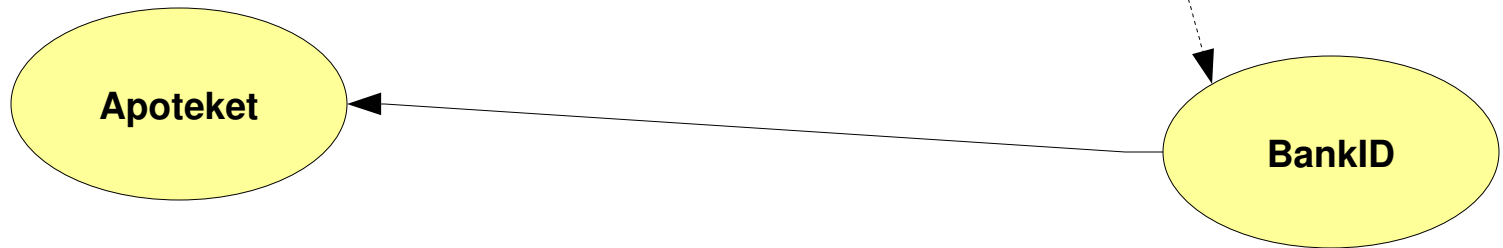
- Använd **bara** öppen teknologi (ju fler...)
  - SAML 2.0 WebSSO
  - OpenID 2.0 (?)
  - Information Card (!)
- **Resultat**
  - Avsevärt lägre kostnader för tjänsteleverantörer.
  - Multipla interoperabla implementationer existerar.

# Mer konkurrens



ID-kontroll med körkort  
LoA 3\*

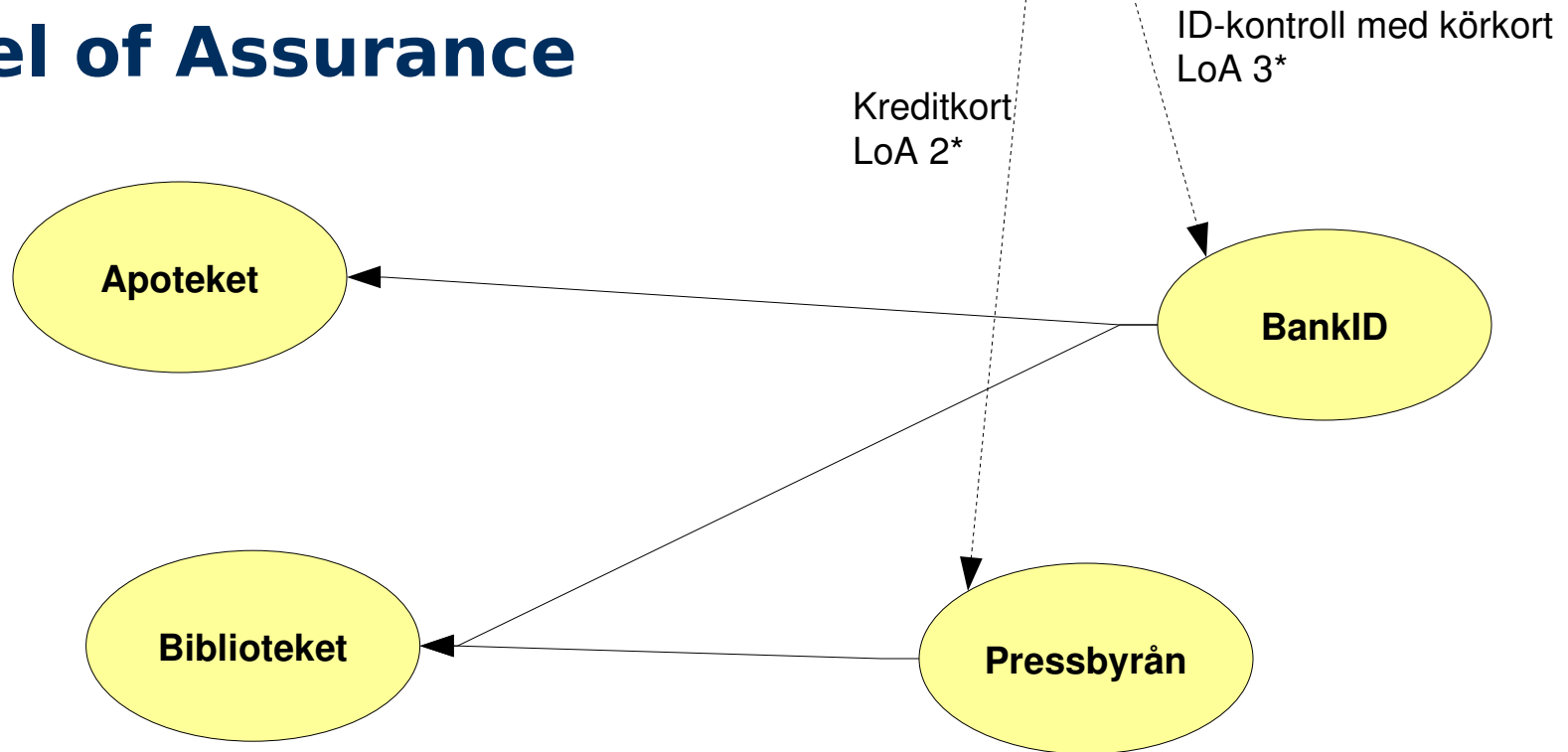
## Level of Assurance



\* NIST SP 800-63



# Level of Assurance



\* NIST SP 800-63

# Fler identitetsutfärdare

- Identitetsutfärdare på flera säkerhetsnivåer
  - Bygg inte mer säkerhet än som behövs
- **Resultat**
  - Pressbyrån/ICA/Konsum konkurrensutsätter BankID
  - Fler användare av teknologin betyder lägre kostnader

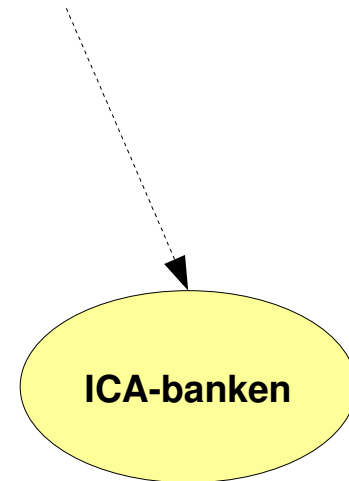
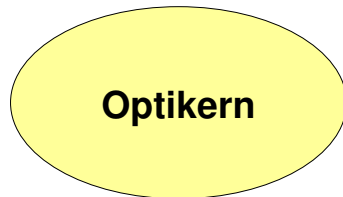


# Skydd av personlig integritet



ssn: 19700101-0000  
namn: Sven Svensson  
adress: Bokstavsgränd 1

# Pseudonymitet





ssn: 19700101-0000  
namn: Sven Svensson  
adress: Bokstavsgränd 1

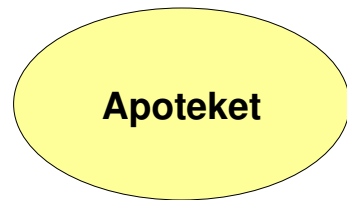
## Pseudonymitet



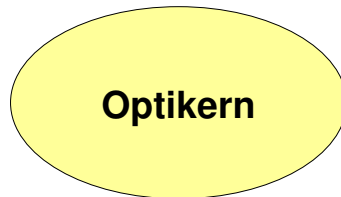
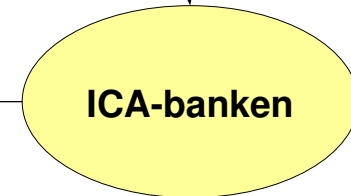


ssn: 19700101-0000  
namn: Sven Svensson  
adress: Bokstavsgränd 1

## Pseudonymitet



id: 02134ab6-79c7-4b13-a6f8-9e5839863b8c  
ssn: 19700101-0000  
adress: Bokstavsgränd 1



id: 50de6f0e-360e-49e8-853b-98e801c313a1  
adress: Bokstavsgränd 1



ssn: 19700101-0000  
namn: Sven Svensson  
adress: Bokstavsgränd 1

## Pseudonymitet

id: 02134ab6-79c7-4b13-a6f8-9e5839863b8c  
ssn: 19700101-0000  
adress: Bokstavsgränd 1

Apoteket



Optikern

id: 50de6f0e-360e-49e8-853b-98e801c313a1  
adress: Bokstavsgränd 1

ICA-banken

# Bättre skydd av personlig integritet

- Pseudonymitet är normen!
  - Identiteten blir spårbar men inte länkbar mellan olika tjänsteleverantörer.
- **Resultat**
  - Du vågar låna böcker och förnya recept med samma identitet!

# Ingen single-point-of-failure

# Statens roll

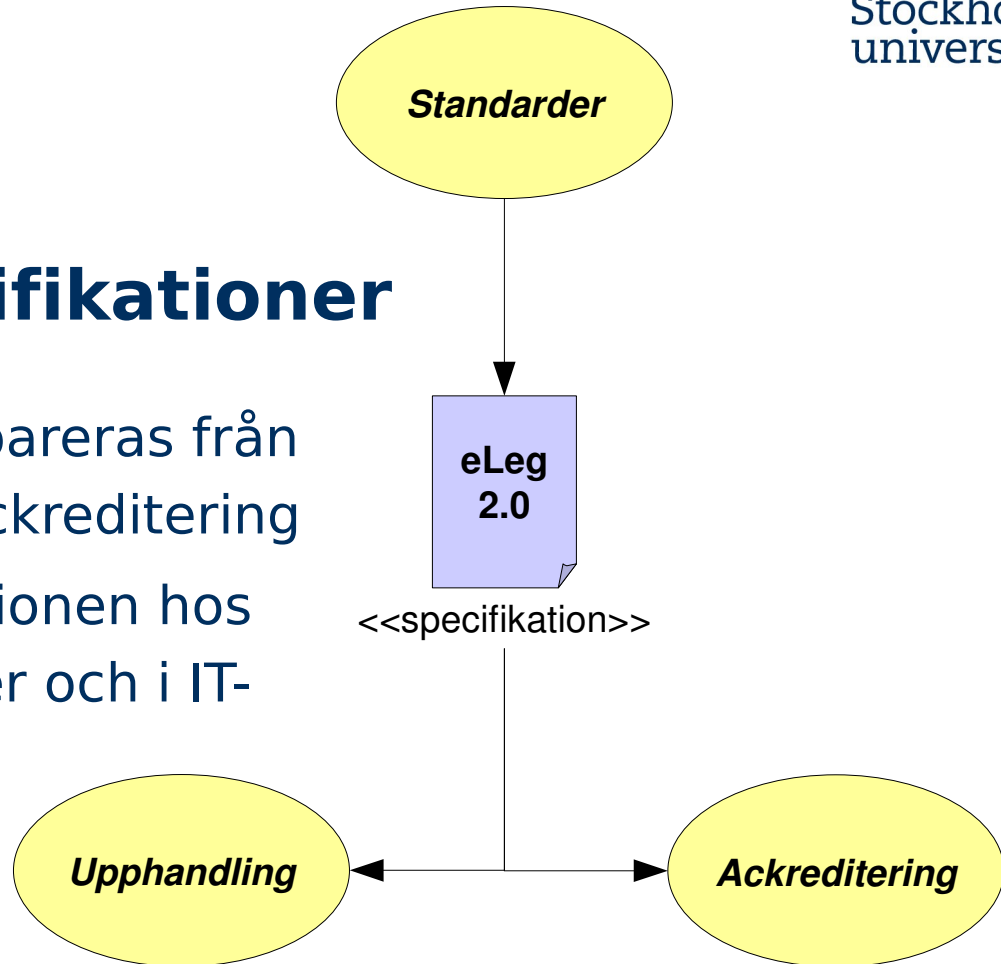
- Statens roll:
  - Äga och underhålla specifikationer
  - Ackreditera nya aktörer – gör inte *bara* upphandling
- **Resultat**
  - Ingen ”statlig CA” som kan gå sönder



# Modellen

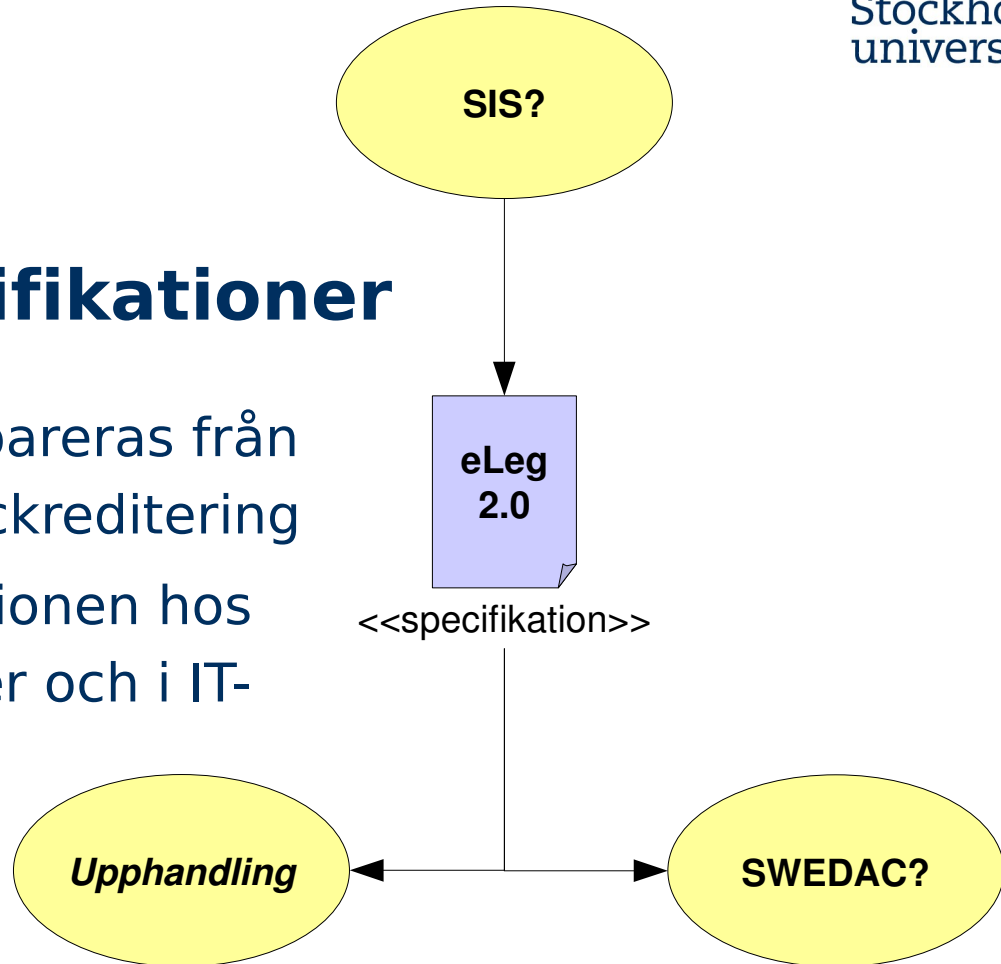
## eLeg 2.0: Specifikationer

- Specifikationen separeras från upphandling och ackreditering
- Förankra specifikationen hos marknadens aktörer och i IT-branschen

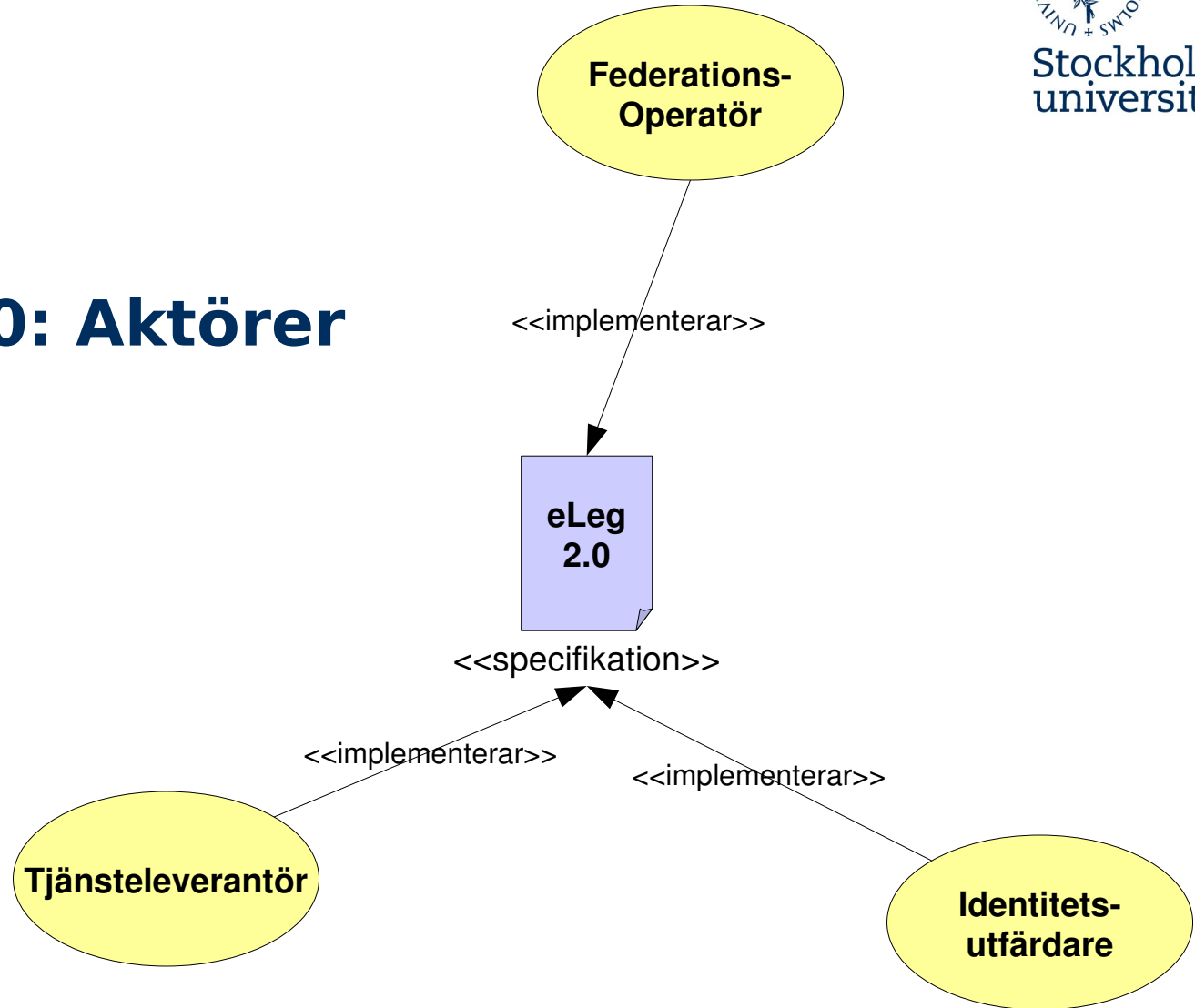


## eLeg 2.0: Specifikationer

- Specifikationen separeras från upphandling och ackreditering
- Förankra specifikationen hos marknadens aktörer och i IT-branschen



# eLeg 2.0: Aktörer



## eLeg 2.0: Transition från eID 1.0

- Köp en gateway mellan eID (BankID etc) och SAML
- Bygg en signeringsfunktion baserad på eLeg 2.0

## Vad gör resten av världen?

- E-Authentication Federation Architecture 2.0
  - <http://www.cio.gov/eauthentication/documents/EAuthFederationArchitectureInterfaceSpec.pdf>
- Liberty Alliance Project
  - Interfederation SIG (formeras)
- IDABD/Stork
  - <http://www.eid-stork.eu/>
- Interoperable SAML 2.0 Web Browser SSO Profile
  - <http://rnd.feide.no/documents/saml2simple.html>

## Gjort sedan sist:

- Gateway-funktion för dagens eID till SAML
  - AMS.se och SU.se
  - Licensregler för BankID sätter stop för produktion
- SAML IdP för identifieringen på Studera.NU
  - VHS.se och SWAMI.se

**leifj@it.su.se**