Identitetsfederationer

Internetdagarna 2007

Leif Johansson

Stockholms universitet

Enheten för IT och media

¿Que?

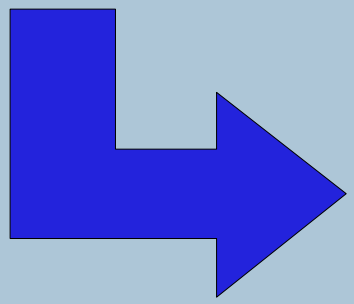
En [identitets]federation är en klubb av klubbar där medlemmarna kommit överens om *hur* man ska lita på varandras medlemmar.

IRL: Schengen

- Schengen (”light”)
  - Genom att begränsa rörlighet på flygplatser räcker det att göra passkontroll vid inpassering till Schengen-regionen.
  - Länderna i Schengen delar på ansvaret (och kostnaderna) för identitetskontroll.

Ekonomiska drivkrafter

- Riktig ID-kontroll kostar.
- Tillit mellan organisationer är billigt.



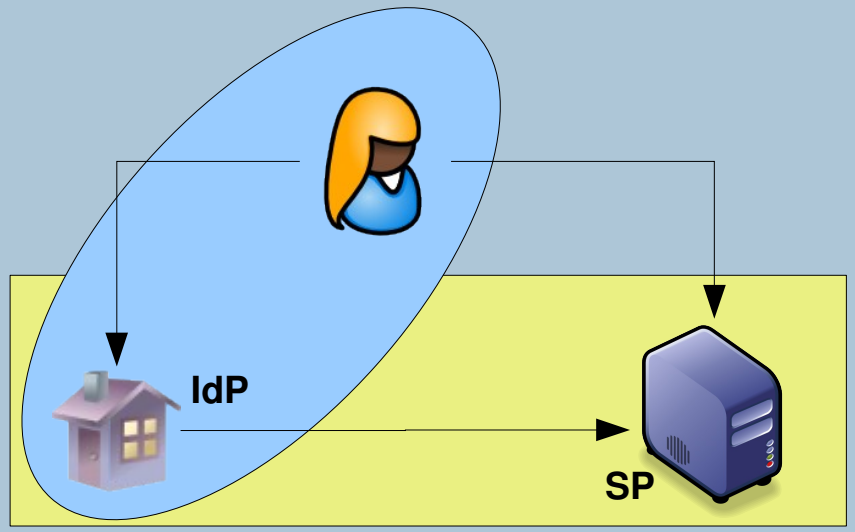
Låt oss använda de identiteter som våra kunder redan har!

Tekniska drivkrafter

- Separation av egenskaper
  - Authenticering
  - Identifiering
- Abstraherade gränssnitt mot applikationer
  - Utvecklare **vill inte** koda mot OpenID, SAML, Kerberos etc etc
- N-Tierproblemet & delegerade rättigheter
  - Varför vill Facebook ha mitt Gmail-lösenord egentligen?

Federationer GK

- IdP
  - Identitetsutfärdare (”Identity Provider”)
- SP
  - Tjänsteutgivare (”Service Provider” aka ”Relying Party”)

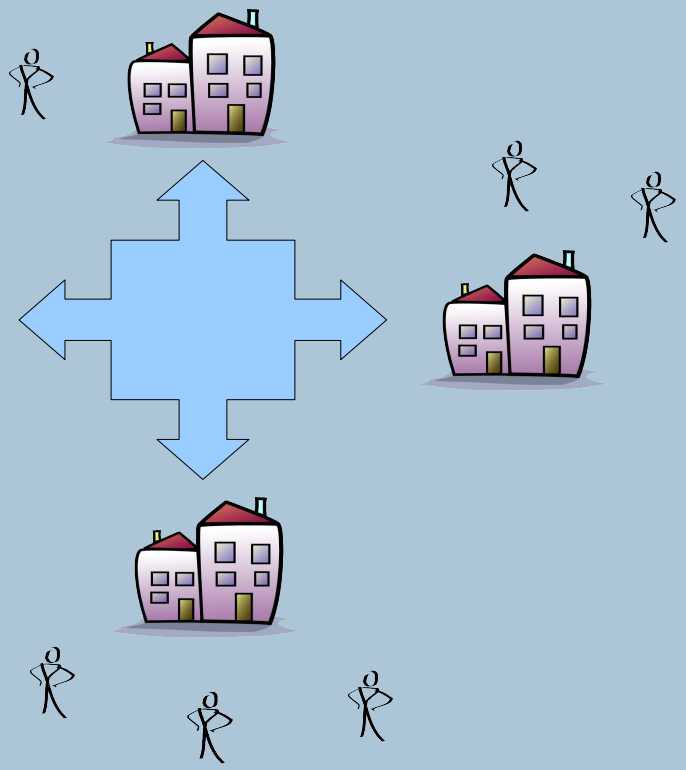


Federationer GK

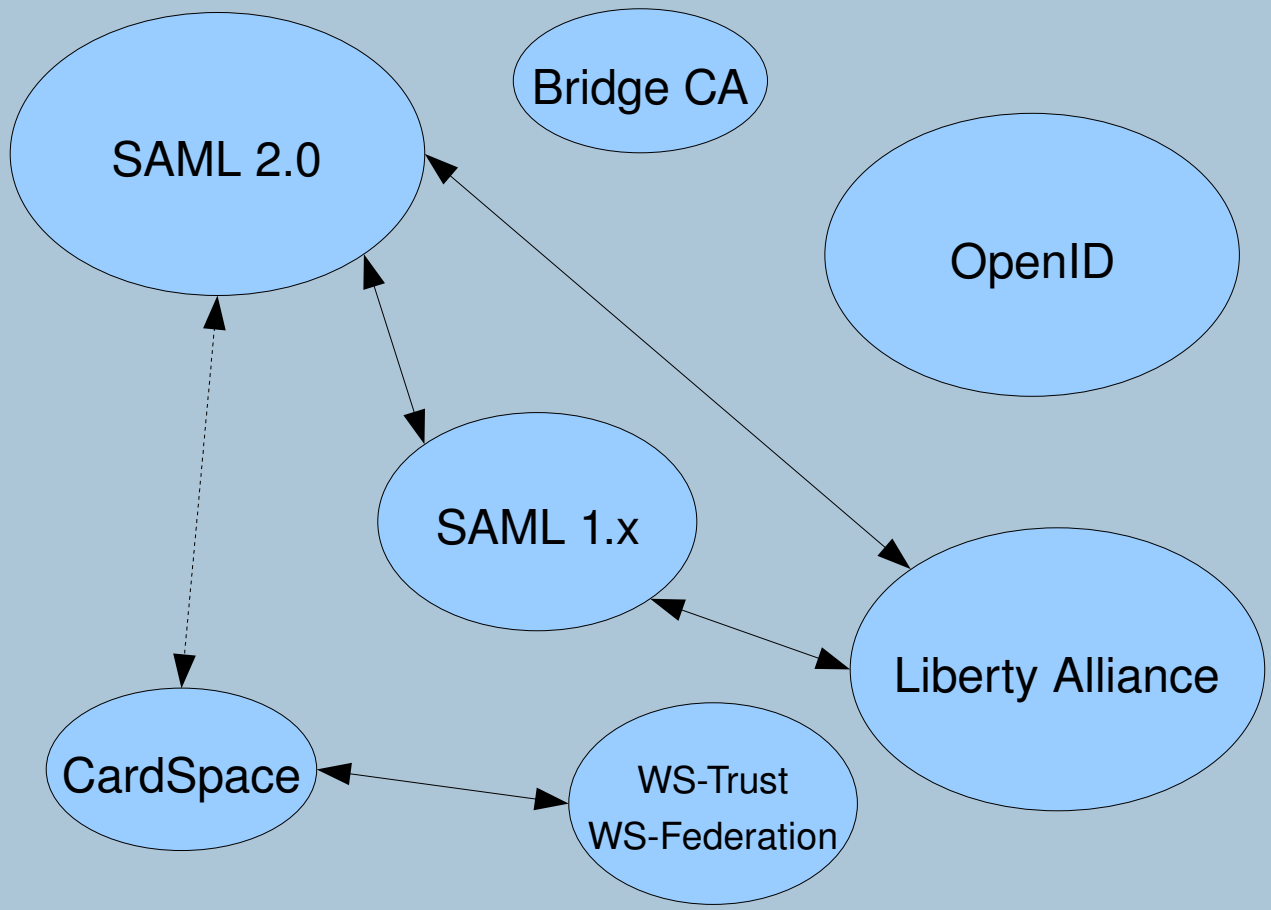
- IdP:n producerar (påståenden om) identiteter
- SP:n konsumerar (påståenden om) identiteter
- IdP:n och SP:n litar på varandra

Federation: Circle-of-Trust

- Ett antal IdP och SP litar på varandra (inte sällan via en PKI)
- Identiteter behandlas lika av alla medlemmar i federationen



Identifieringens IT-ekosystem



Identifieringens heliga Graal

Göra säker och enkel identifiering utan att rulla ut ny programvara till klienterna.

Enkelt, Billigt, Säkert – Pick any two!

Religionsdags!

SAML vs OpenID

(ADFS har redan förlorat)

OpenID

- Enkelt och bra! Tex:
  - Ingen mekanism för revokering av identiteter.
  - Man litar på SPn (!)
  - Användning av HTTP redirects gör det svårt att skilja en attack från ett legitimt byte av identitetsutgivare.
  - Säkerhet är ”out of scope” - inget tekniskt stöd för tilliten mellan SP och IdP eller mellan SP och användare.
  - Teori och praktik står långt ifrån varandra – ”allt blir bra i 2.0”
- OK för tillämpningar där mail-nonce är ok

SAML

- XML-baserat protokoll för identitetsutbyte
- Säkerhet med WS-Security och/eller TLS
- Profileras mot flera olika användningsfall:
  - Web SSO
  - SIP
  - Radius/Diameter
- OASIS SSTC, Liberty Alliance, (IETF)

Vad branchen brottas med idag:

- Hur hittar jag min IdP? (”discovery”)
  - Identiteten är adressen till min IdP (OpenID)
  - Separat tjänst – IdP Discovery Service
  - Gå till IdP:n först (dvs en Portal)
  - Ingen IdP alls? (CardSpace)
- Hur hittar jag *din* IdP? (”invitation”)
  - Hur ger jag dig rättigheter i min Wiki/LMS innan jag vet hur din identitet stavas?
- Hur kan jag lita på dig? (”trust”)
  - Små PKI:er vs Stora PKI:er
- Hur kan vi anställa färre advokater?

Vad ska jag göra?

- Applikationsutvecklare:
  - Skriv mekanismneutral kod – glöm både SAML *och* OpenID fort!
  - Låt applikationsservern göra jobbet (och kräv att den gör det)!
- Tjänsteleverantör:
  - Använd alla mekanismer som passar ihop med dina krav på minsta säkerhetsnivå.
- Identitetsutgivare:
  - Tänk på vilka löften som följer med varje identitet du utfärdar.
  - Stöd flera mekanismer (dvs agera gateway).

Vad bör vi göra i Sverige?
(löpsedelsversionen)

- **Bryta** beroendet på dagens **e-legitimation**.
- Bygg **federationer** istället för PKI:er.
- **Sluta leka** med hemsnickrad teknologi **Verva**!

Demo

F & S