Er identitetsfederering en forutsetning for en vellykket SOA?

HelsIT

Trondheim 23.09.2009

Seniorrådgiver Kjell Atle Lund, Acando

Medforfatter: Seniorrådgiver Jon Gupta, Acando

© Acando AB

Hva er identitetsfederering?

Den kinesiske muren

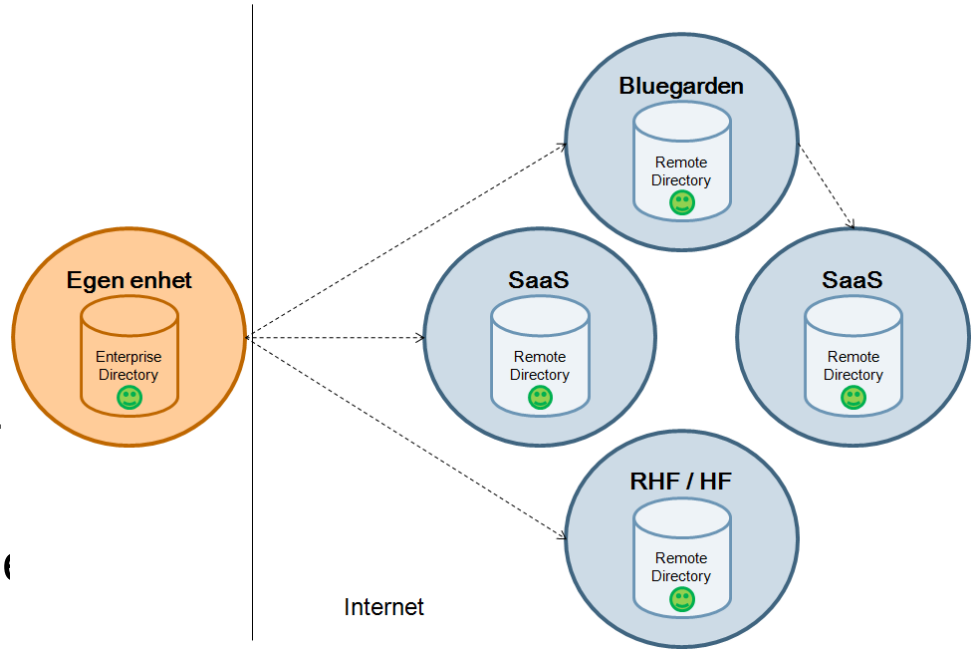
- Man stoler på identitetsbeviset som er utstedt fordi man stoler på utsteder
- Identitetsbeviset er skapt iht. en standard som er anerkjent hos tjenesteleverandør
- Identitetsbeviset utveksles mellom tjenestekonsument og leverandør iht. en standard protokoll

© Acando AB

Utfordring nr 1

En felles identitetskatalog er en utopi

- Hvert fagsystem - hver sin brukerdatabase
- Konsolidering av identitetslagre har pågått i mange år
- 3.parts programvare tjenester innfører nye identitetslagre som virksomheten må forholde seg til

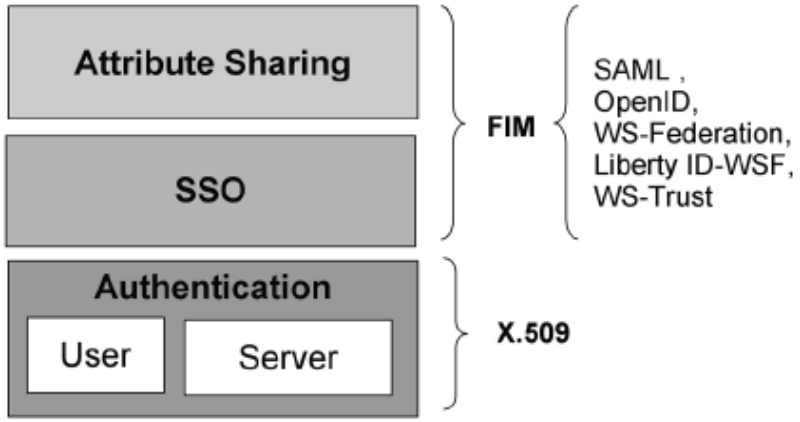


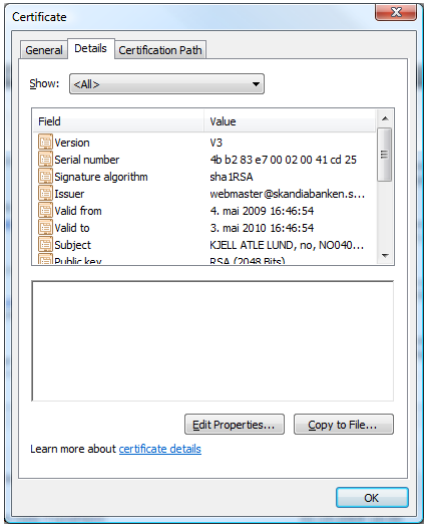
© Acando AB

Utfordring nr 2

Er PKI løsningen alene?

- Rettet mot bruk av sertifikater for autentiseringsformål (klient / server)
- Sertifikat attributter er faste i X509 sertifikatet i gyldighetsperioden
- Attributter utover sertifikater er vanskelig å få til på en standardisert måte
- Sertifikatforvaltning ift tjenester blir omfattende og komplisert



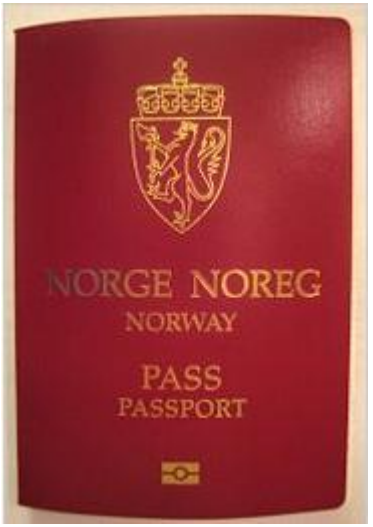


© Acando AB

Utfordring nr 3

Mangel på et fleksibelt og standardisert identitetsbevis

- Identitetsbevis er ikke nødvendigvis **interoperable** på tvers av sikkerhetsgrenser
- Identitetsbevis følger ikke nødvendigvis en **standard**
- Identitetsbevis kan forutsette proprietære **utvekslingsprotokoller**
- Identitetsbevis kan være lite **tilpasningsdyktige**
- Identitetsbevis har forskjellige **sikkerhetsstyrker** og svakheter



BankID MinID Microsoft ORACLE OpenID ca

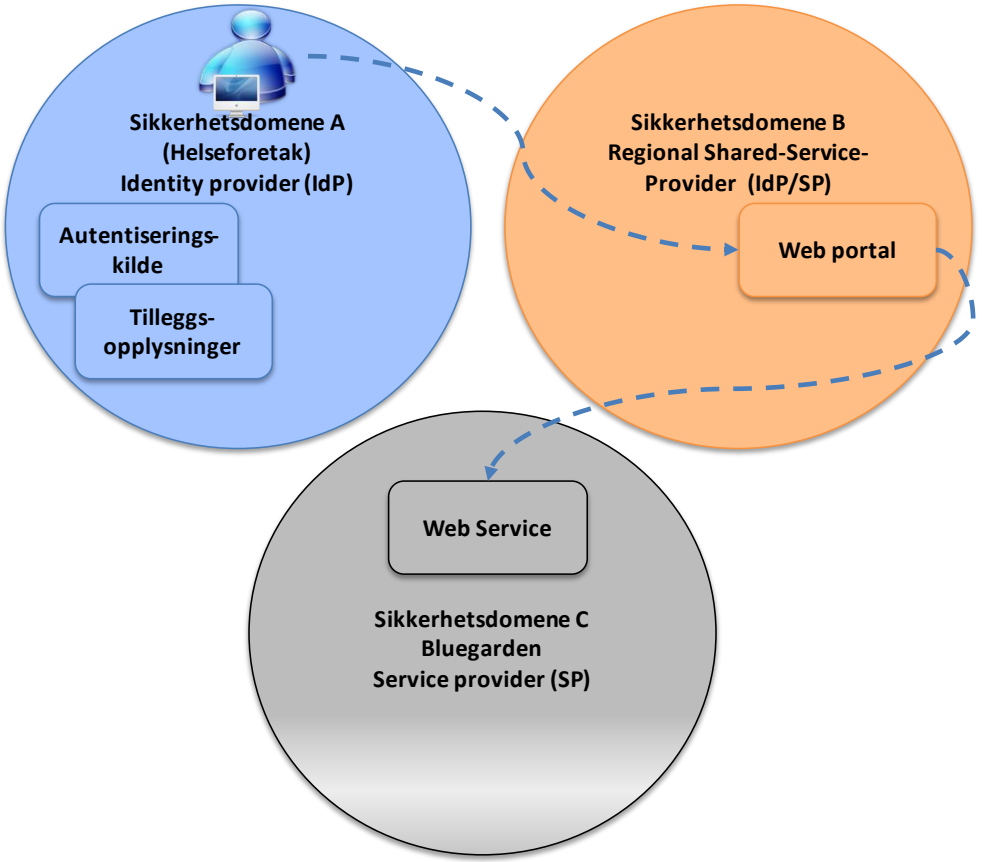
© Acando AB

acando

Utfordring nr 4

Punkt til punkt sikkerhet er ikke lenger nok

- Sikkerhet stopper tradisjonelt ved første webserver
- Leverandørkjeden i en tjenesteorientert arkitektur er ukjent
- Bransjenormen stiller krav til sikkerhet som nå må håndteres langs hele leverandørkjeden

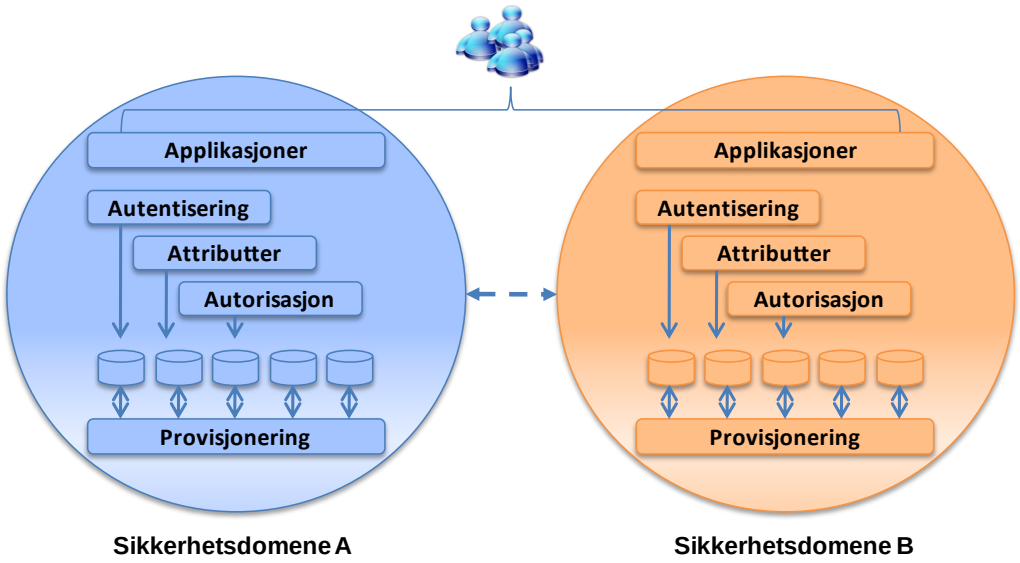


© Acando AB

Utfordring nr 5

Vi må ha en brukerkonto per tjenesteleverandør

- Tjenesteleverandører krever ofte en brukerkonto pga av betalingsforhold
- For å få tilgang til tjenesten må det først opprettes en brukerkonto som Web Service konsumenten kan benytte seg av
- Man bør kunne opprette identiteten til tjenestekonsumenten midlertidig eller permanent



© Acando AB

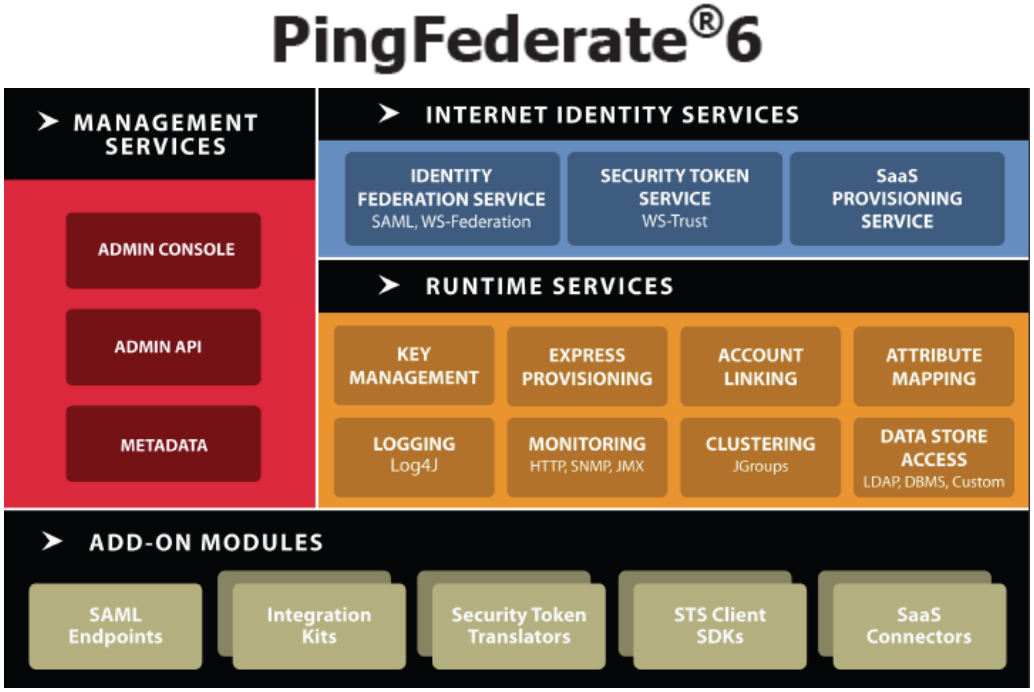
Hovedutfordringer ved samhandling i en tjenesteorientert arkitektur

- Sikkerhetsarkitekturen må
  - forholde seg til forskjellige identitetskilder / utstedere
  - sikre løse koblinger mellom identitetskilder, identitetsbevis, autentiseringsprotokoller og autorisasjonskrav
  - transformere identitetsbevis på tvers av sikkerhets- og organisatoriske grenser
  - forholde seg til ende-til-ende sikkerhet
- Bransjenormen legger føringer for sikkerhet

© Acando AB

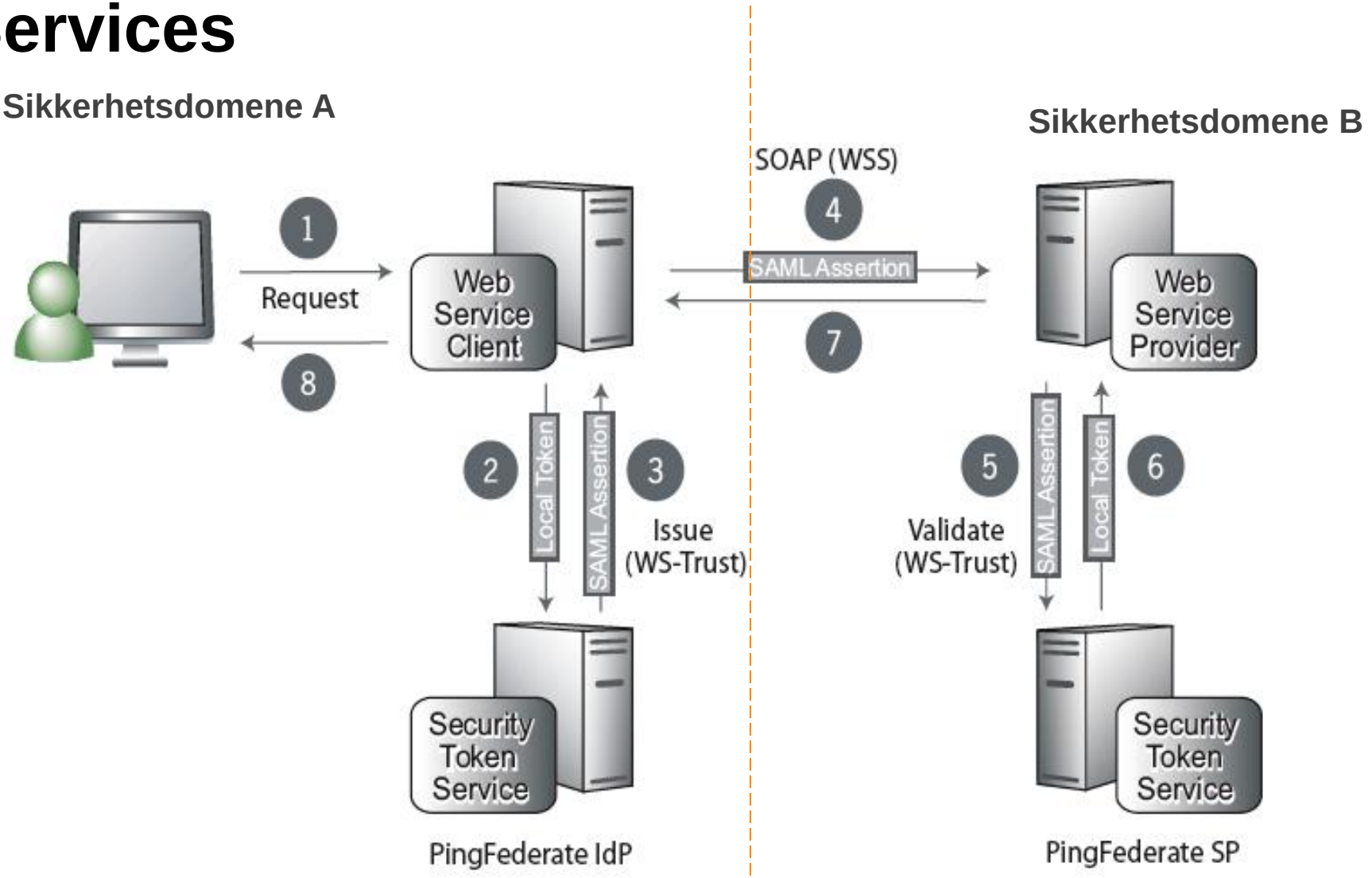
Eksempel på en identitetsfedereringsløsning

- Støtter sikkerhetsstandardene
  - WS-Trust, WS-Security og SAML
- Sikrer løse koblinger til
  - IDM / IAM løsninger
  - Sikkerhetsdomener
  - Attributtlagre
  - Identitetsbeviser
- Enkel administrasjon
- Ferdige integrasjonsmoduler
- Brukerprovisjonering
- Skalerbarhet

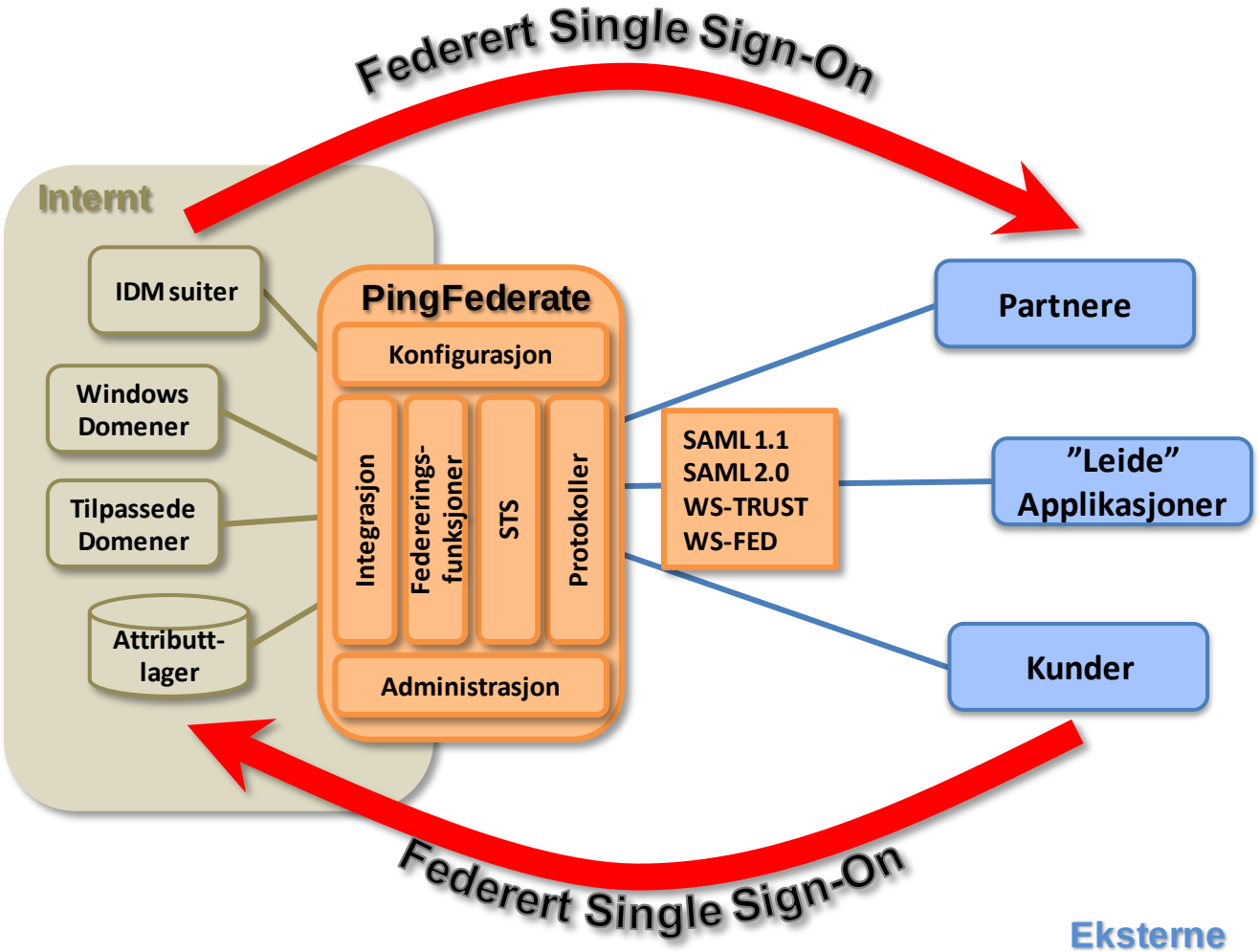


© Acando AB

Eksempel på identitetsfederering med Web Services



© Acando AB



Konklusjon

Identitetsfedereringsløsningen er en viktig forutsetning for å lykkes med en tjenesteorientert arkitektur

© Acando AB