

# COIP

SUNET Collaboration Infrastructure Platform

SONC

2010-12-07

Johan Berggren/Leif Johansson

[jbn@sunset.se](mailto:jbn@sunset.se)

# Agenda

- Utmaningar
- Kort teknisk genomgång
- Exempel på integration

# Problemet, eller utmaningen..

- Kurs med deltagare från  $> 1$  högskola
- Forskargrupp med medlemmar utspridda över hela Sverige
- Ingen IdP sitter på hela svaret!
- Behov av en Collaborativ organisation

# Collaborativ Organisation (CO)

- Representerar en grupp av identiteter i en identitetsfederation
- Spänner över organisationsgränser
- Medlemmar i en CO behöver inte tillhöra samma IdP
- IdPn har inte alla attribut om medlemmarna i en CO

# Lösningen

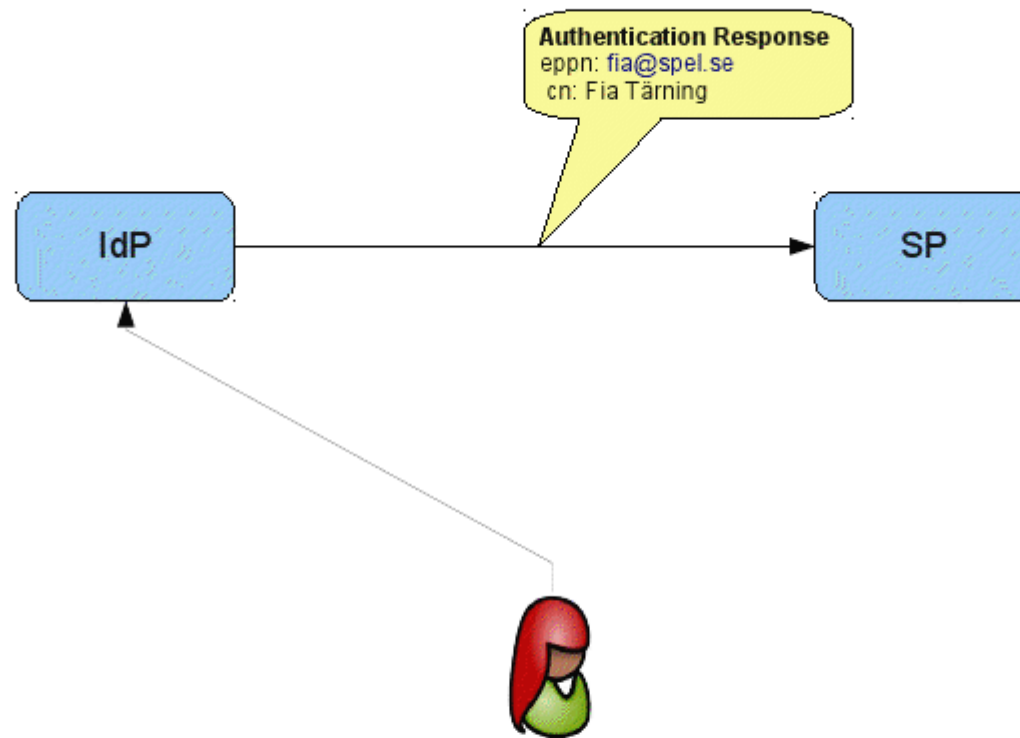
- Entitlements (tillhörighet)
- Representera gruppstillhörighet med entitlements

# COIP

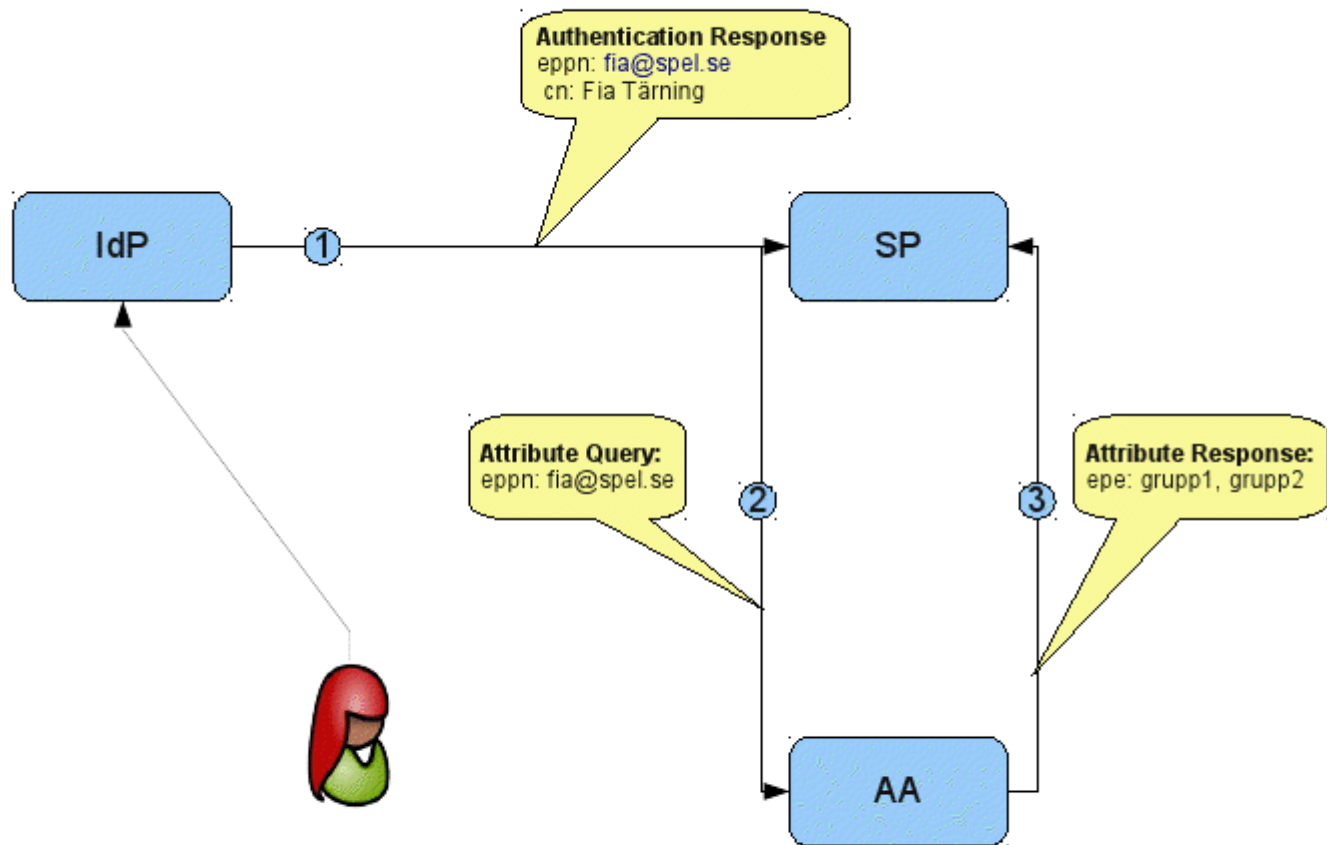
- Ett verktyg för att administrera eduPersonEntitlement
- Utvecklas av NORDUnet under kontrakt av SUNET
- COIP är öppen källkod under en NORDUnet BSD licens (2-clause BSD license)
- Källkod tillgänglig från [git://git.nordu.net:coip.git](https://git.nordu.net:coip.git) och från github
- Använder befintlig teknologi

# Befintlig teknologi

- SAML2
- Shibboleth
- Datamodellen är GMAI
  - General Model for Authorization Information
- Attribut leverantör (Attribute authority)
  - Shibboleth IdP utan inloggning
  - Returnerar endast attribut givet identifierare
  - eppn => gruppmedlemsskap
  - Oberoende av IdP
  - Listar alla grupper som en individ är medlem i







# Webapplikation för underhåll av grupper

- Federerad tjänst
- Administrera sina grupper
  - Skapa grupper
  - Bjuda in personer
- Delegering av namnrum
- ACL-system med inspiration från AFS ACL:er

# Integration med din SP

```
<MetadataProvider type="XML" uri="http://md.swamid.se/md/swamid-coip.xml"
    backingFilePath="swamid-aa.xml" reloadInterval="300">
    <SignatureMetadataFilter certificate="md-signer.crt"/>
</MetadataProvider>
```

```
<AttributeResolver type="Chaining">
    <AttributeResolver type="Query"/>
    <AttributeResolver type="SimpleAggregation"
        attributeId="eppn" format="urn:oid:1.3.6.1.4.1.5923.1.1.1.6-NameID">
        <Entity>https://coip-test.swamid.se/idp/shibboleth</Entity>
    </AttributeResolver>
</AttributeResolver>
```

# Exempel på integration

- Provisionering av konton för användare i olika organisationer – tex GRID
- Behörighetshantering
- Collaborativa hjälpmedel
- LMS
- Lobber
  - [www.lobber.se](http://www.lobber.se)

# Mer information

Demo (våldigt) snart på [coip-test.sunet.se](http://coip-test.sunet.se)

Håll ögonen på:

- <https://brainstorm.swami.se/storm/25/>
- <https://portal.nordu.net/display/COIP>
- [www.swami.se](http://www.swami.se)