Federerad OpenID Connect

Tankar om en Proof-of-Concept

Vilka möjligheter finns? Vilka utmaningar?

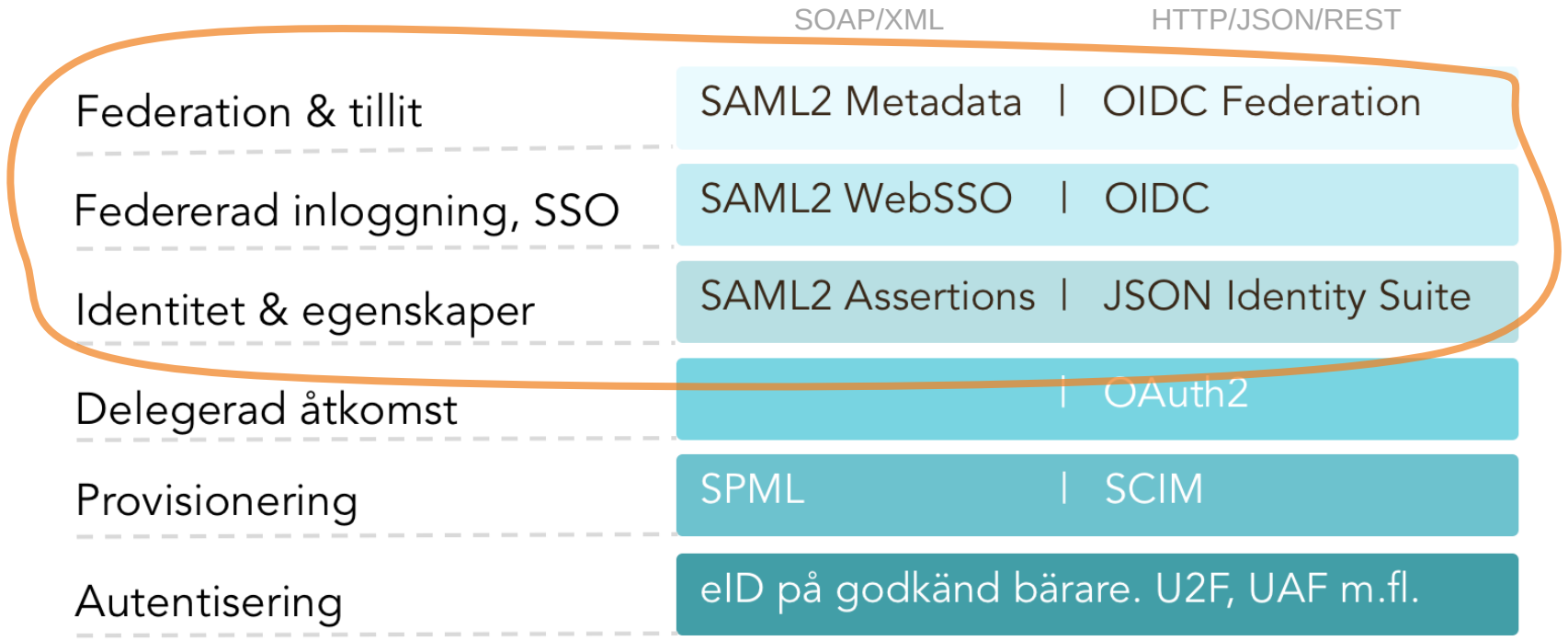
Sambi

inera

15 mars 2018

Per Mützell
Per.Mutzell@inera.se

Referensarkitektur IAM - standarder & protokoll



Brett stöd för applikationsteknik, webb, appar, rika klienter osv.

SAML2 ***och*** *OpenID Connect - parallellt stöd över lång tid!*

inera

Federerad OpenID Connect - drivkrafter och möjligheter

Vad behöver vi ha i federationen?

- **Minska teknikinlåsning, stöd för mobilitet**
  - Anslut tjänster till federationen med tillgänglig standardteknik, valfritt OpenID Connect eller SAML2

Tekniska krav

- implementationsprofiler

- attributprofiler

för OpenID Connect

- **Decentraliserad** och **skalbar administration** av federationen
  - Registrera nya tjänster inom federationen smartare, delegera ansvar till rätt nivå

OpenID Connect Federation

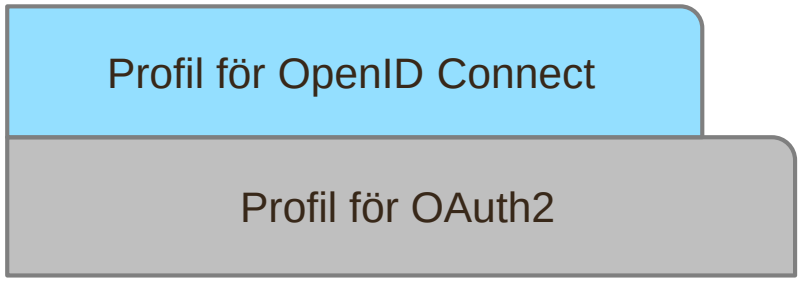
inera

Tekniska krav
- Implementationsprofiler för OpenID Connect

- Standarder är ”rymliga” – profiler är centrala. Certifiering är välkommet!
- **iGov** - International Government Assurance Profile
- **HEART** - Health Relationship Trust

Med sikte på att motsvara höga säkerhetskrav (som åtkomst till patientinformation)

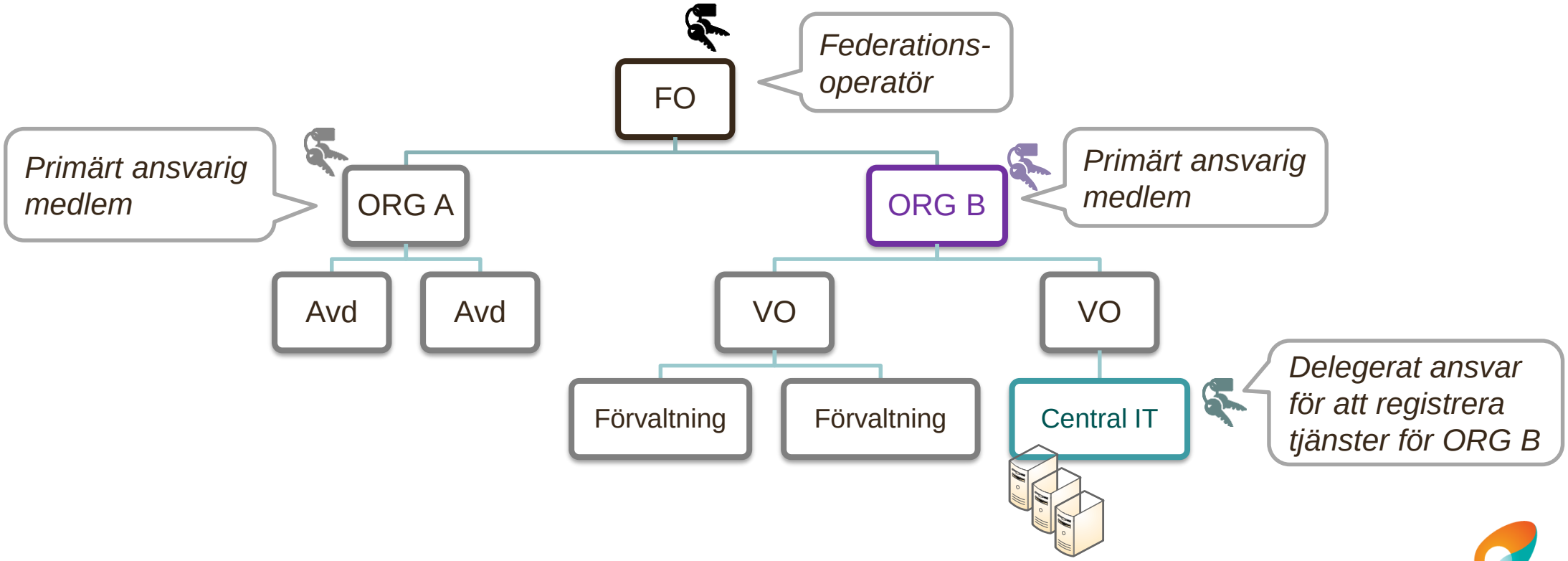
Lagkrav har varit drivkraft



inera

OpenID Connect Federation

Möjlighet: Decentraliserad och **skalbar administration** inom federationen – *men hur?*

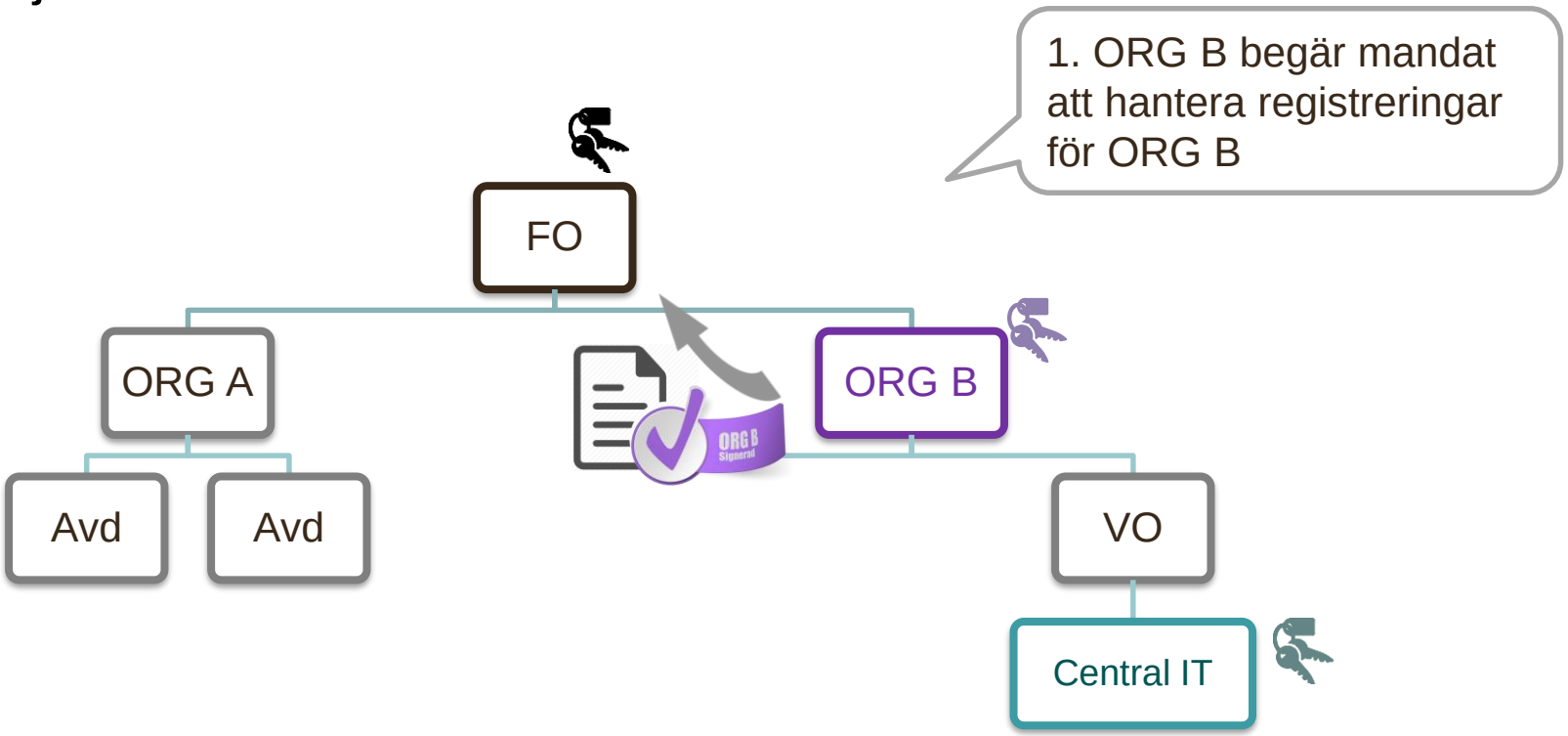


inera

OpenID Connect Federation

Användningsfall:

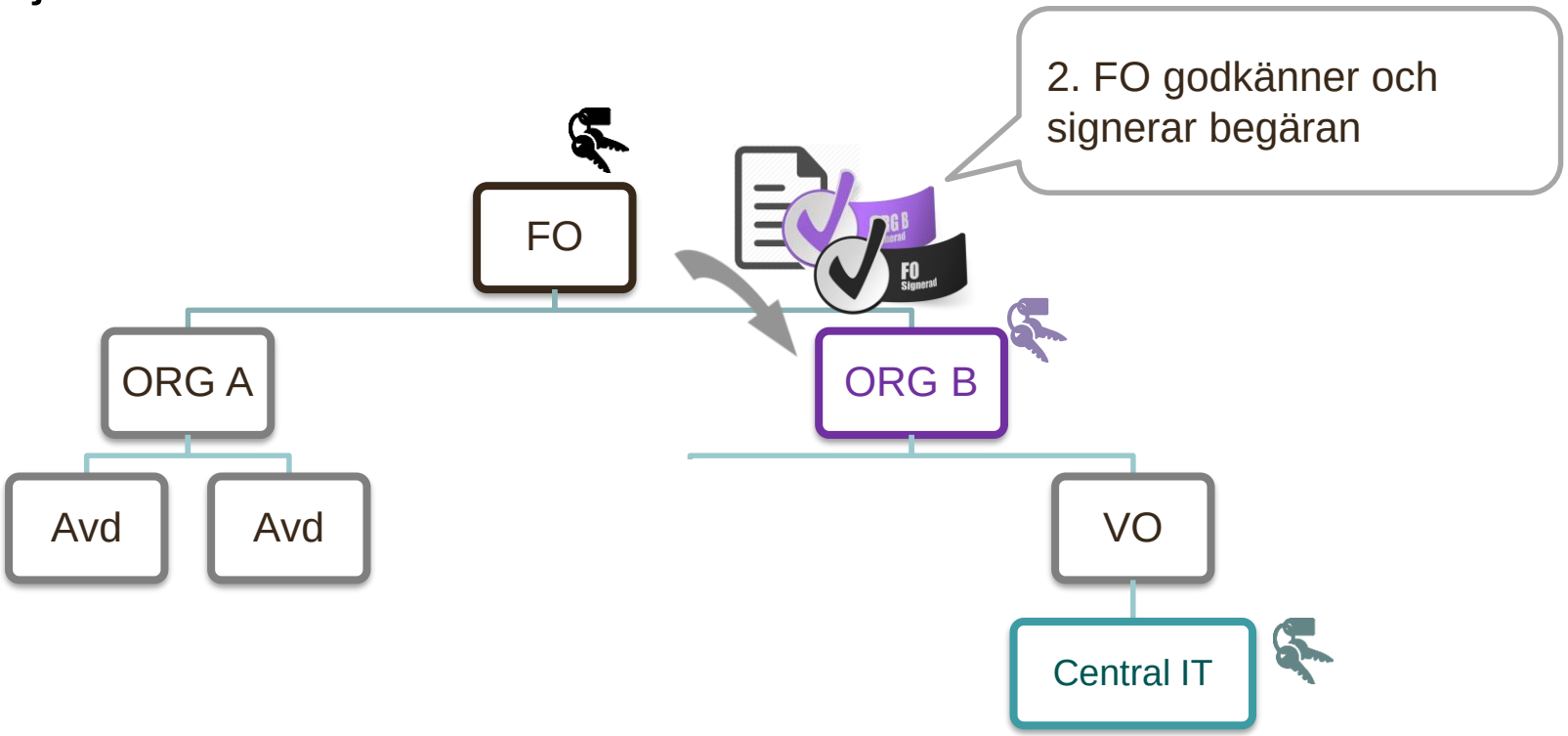
Registrera tjänster i federationen



OpenID Connect Federation

Användningsfall:

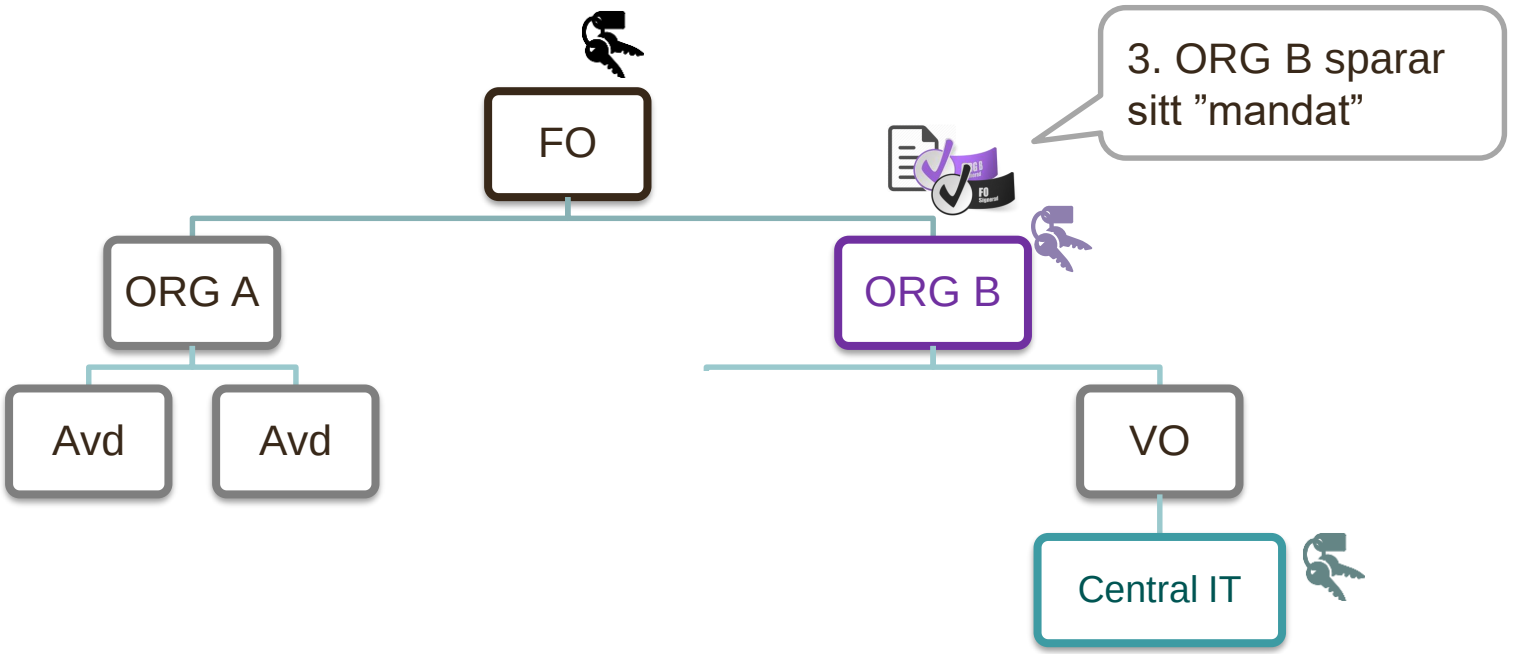
Registrera tjänster i federationen



OpenID Connect Federation

Användningsfall:

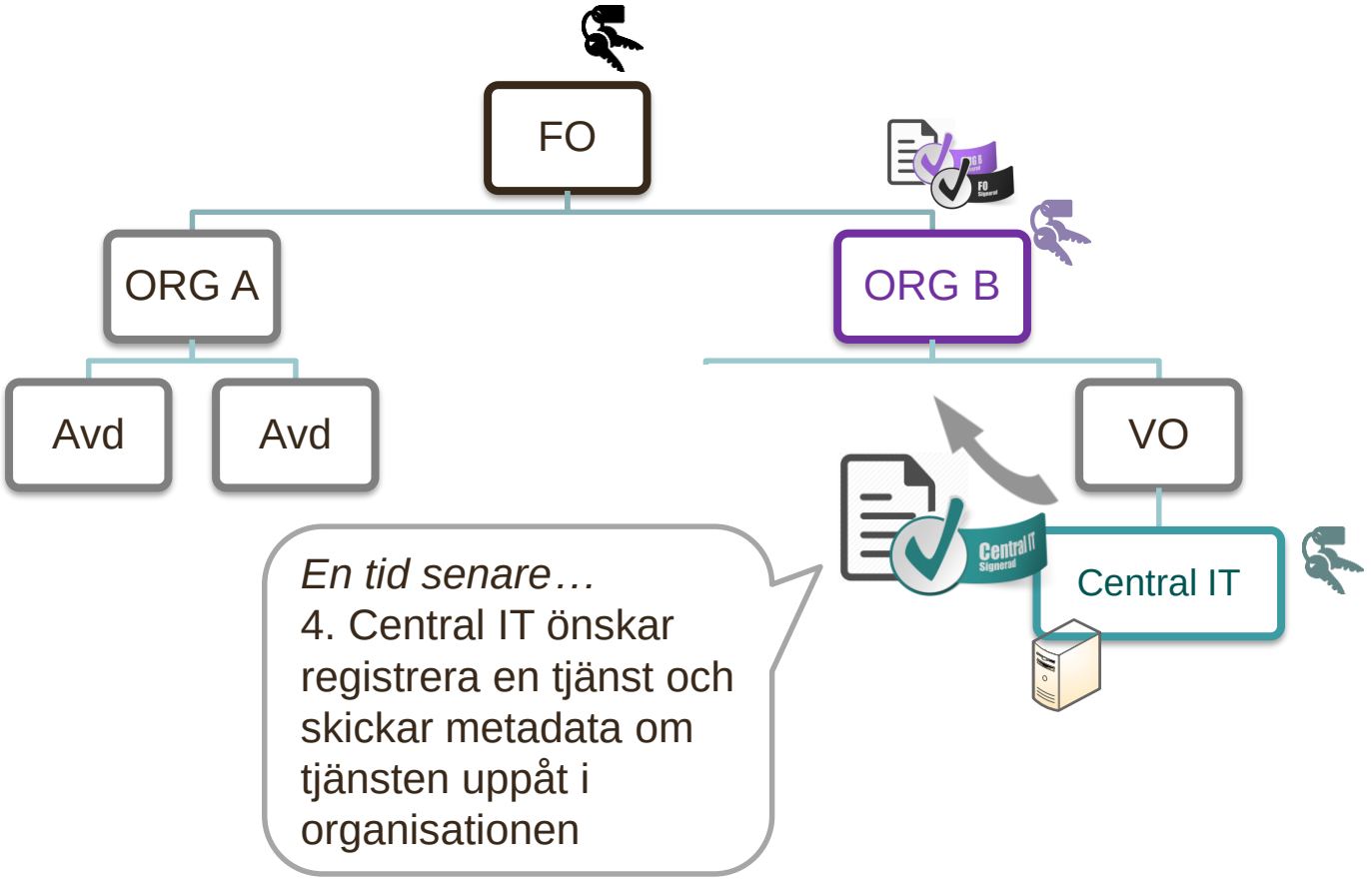
Registrera tjänster i federationen



OpenID Connect Federation

Användningsfall:

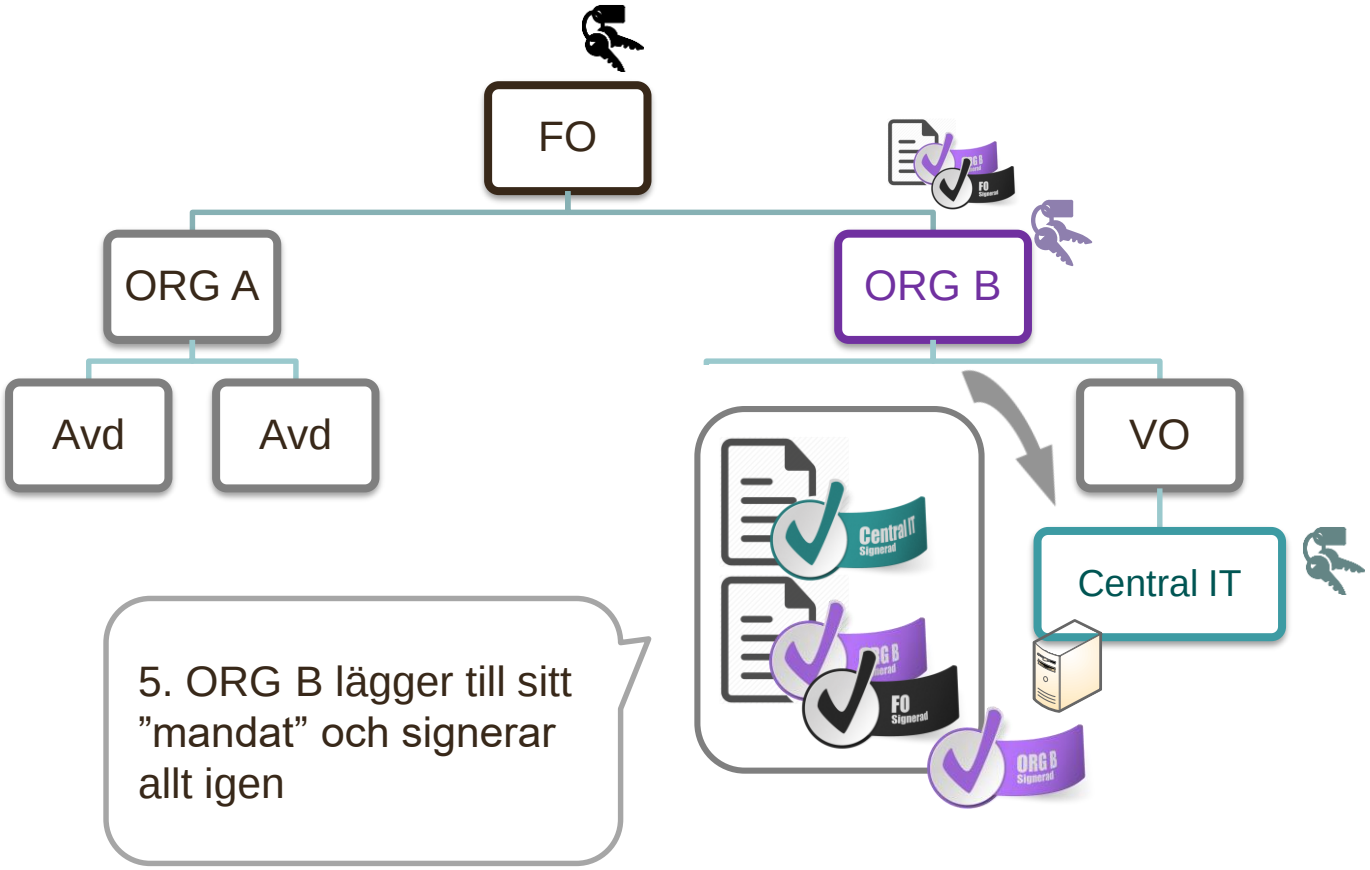
Registrera tjänster i federationen



OpenID Connect Federation

Användningsfall:

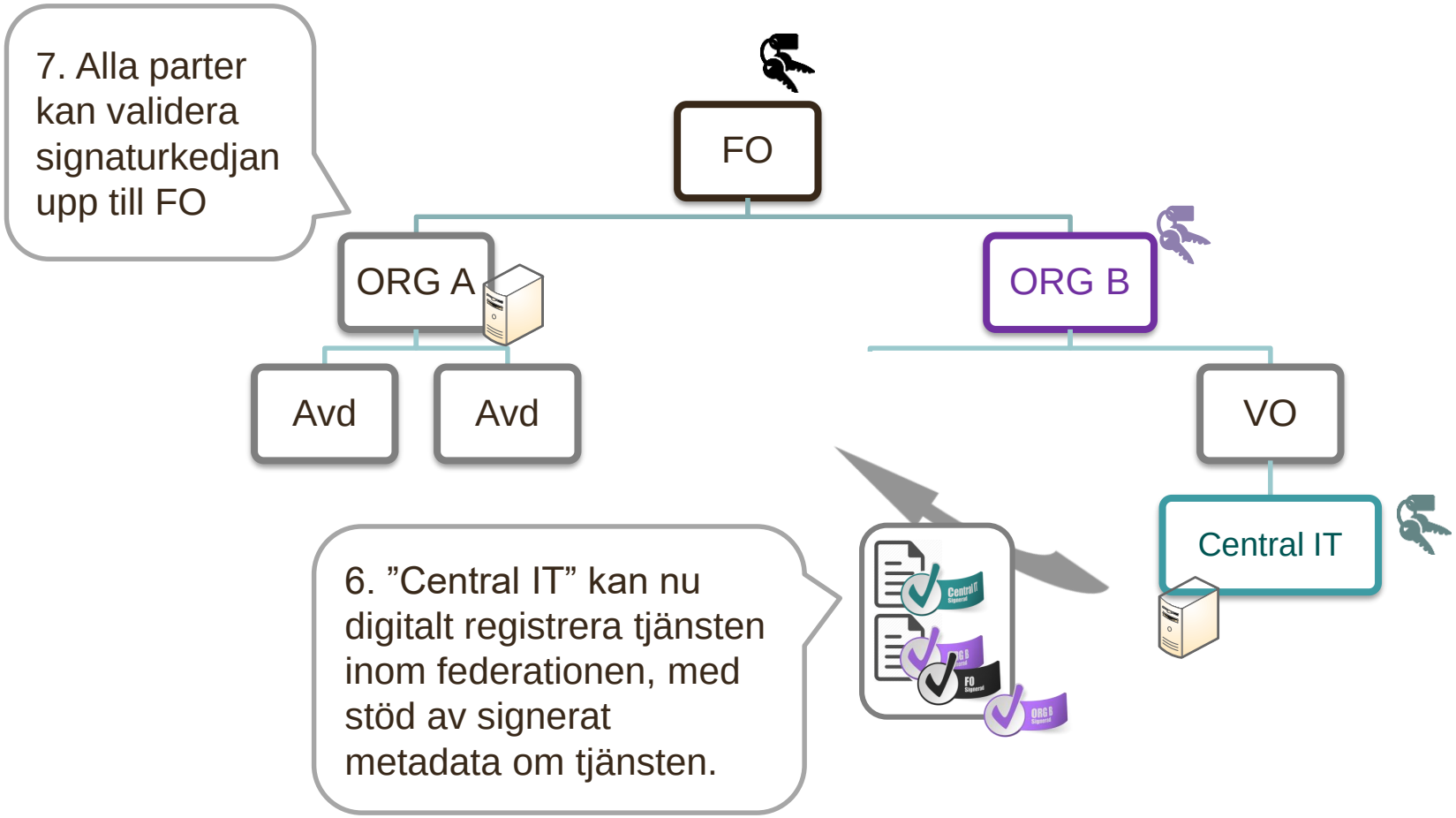
Registrera tjänster i federationen



OpenID Connect Federation

Användningsfall:

Registrera tjänster i federationen



OpenID Connect Federation
- utmaningar

- Specifikationen är ännu i *draft*
- Hur kan vi verifiera tekniken (Proof-of-Concept)?
- Hur fungerar återkallande av signeringsnycklar?
- Hur länge ska nycklar och signerad metadata gälla?
- Hur hanterar vi *SAML2 Metadata* parallellt?

inera

OpenID Connect Federation
- möjligheter!

- Stor potential - **decentralisera ansvar och administration** inom federationen
- Standardiserat stöd för **ombudsroll** inom federationen
  (ORG B är ombud att ansvara för registreringar ”bakom B”)
- Registrering av nya tjänster med **dynamik och inbyggd säkerhet** !

Tack för uppmärksamheten!

OpenId Connect Federation

sambi.se

Identitet och åtkomsthantering - inera.se