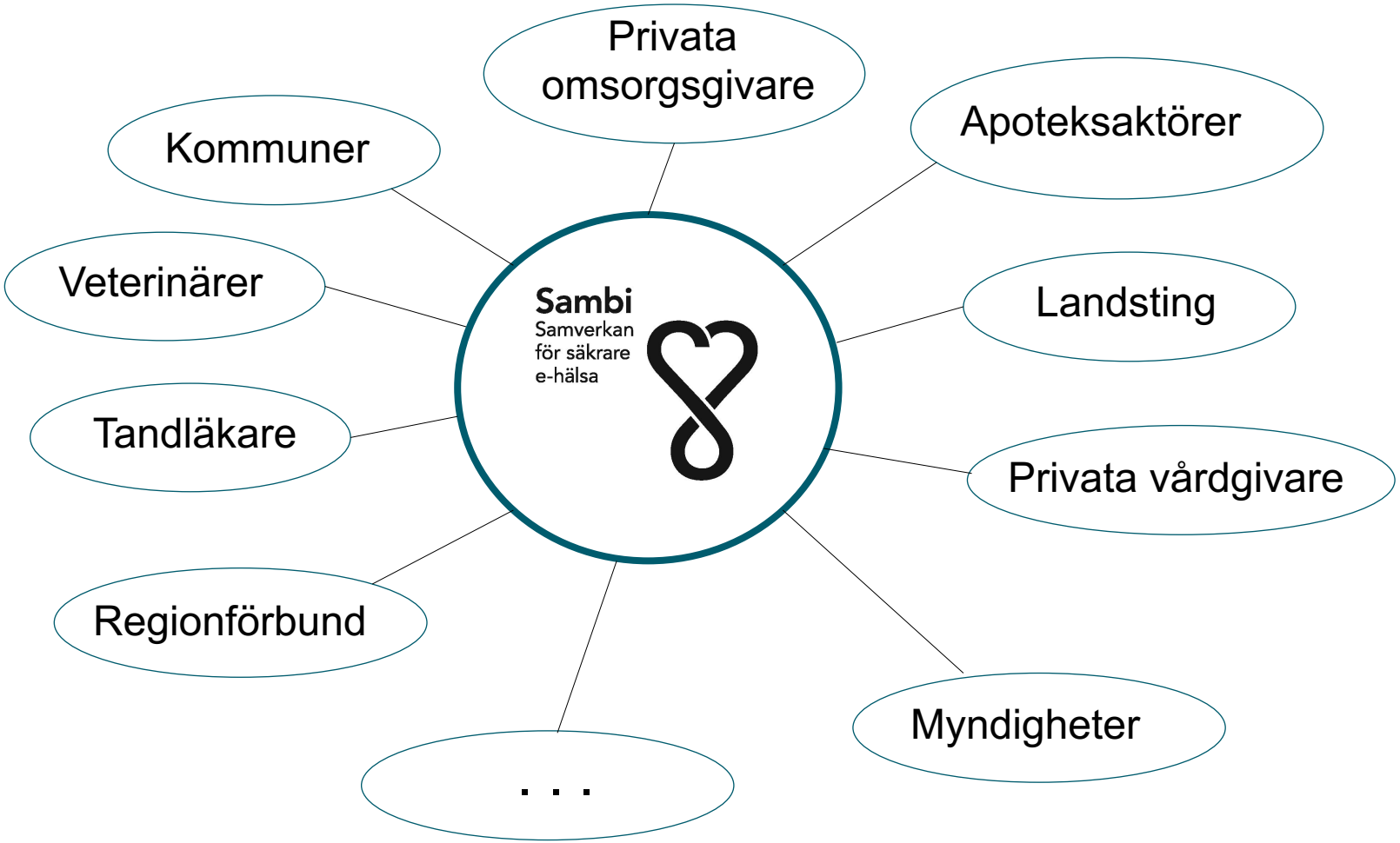
Sambi

Samverkan
för säkrare
e-hälsa

Sambiombud

18-03-15

Målgrupper för Sambi



Varför återförsäljare?

Domännamns registrarer	Sambiombud
Webbhotell	eID
E-mejl	Directory service
Domännamn	IdP (SAML)
Hosting, immaterialrätt…	Implementation av ett strukturerat säkerhetsarbete (motsvarande ISO 27001)

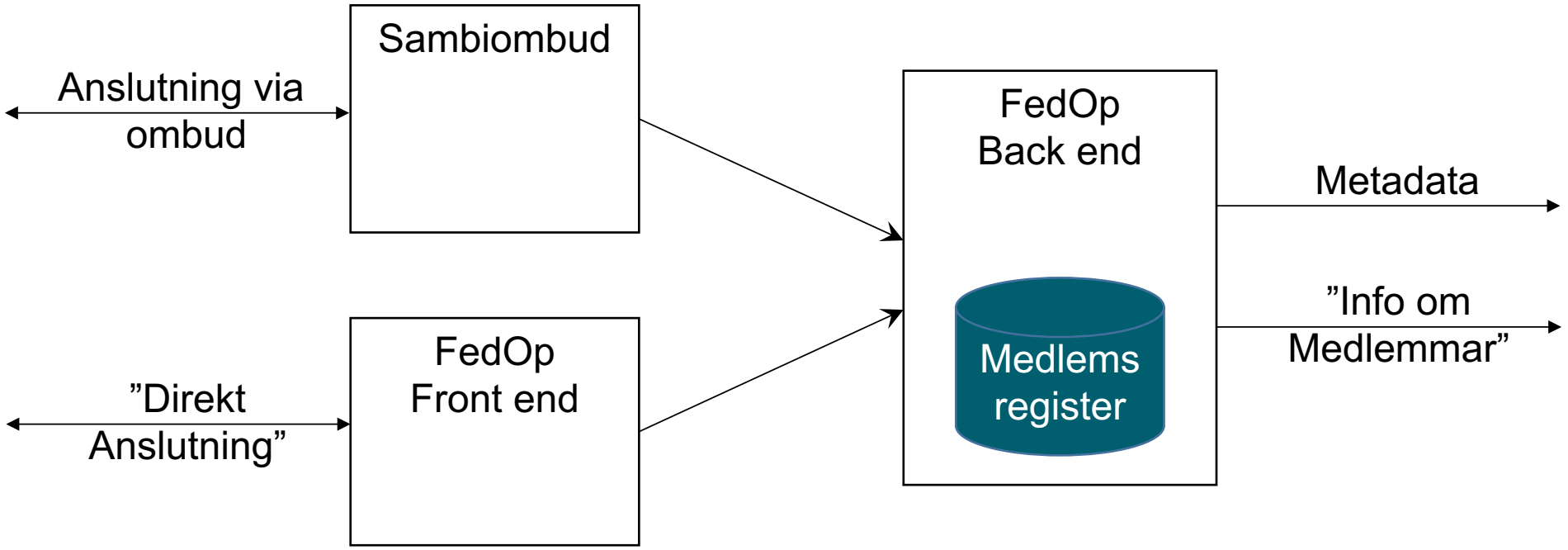
Centrala krav för Sambi,
gäller även för anslutning via Sambiombud

- En användarorganisation ska fortsatt ha ett tydligt ansvar för sina användare och deras identiteter och behörighetsstyrande attribut.
- Det ska alltid framgå vilken organisation som en individ representerar även när ombud används.
- En användarorganisation ska alltid ha ett eget juridiskt bindande avtal med federationen.
- Problem till följd av att ombud inte sköter sina åtaganden ska kunna hanteras.

Sambiombud

- Svensk e-identitet
- Federationsoperatörens eget

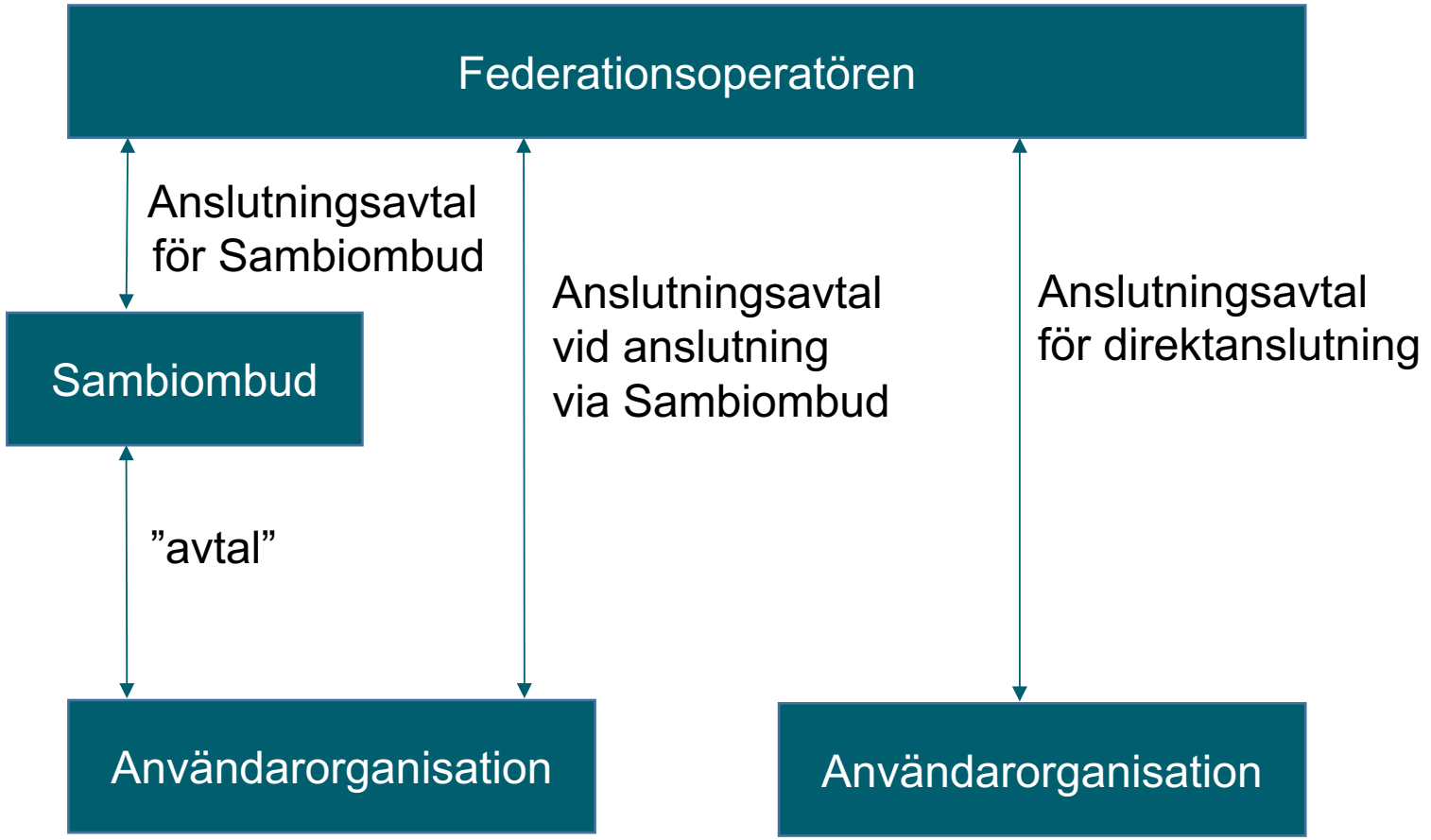
Erfarenheter från IIS domännamnsregistry



Avtalspaket

Part	Anslutningsavtal	Tillitsgransknings avtal
Direktansluten Medlem	Ja	Ja
Medlem ansluten via Sambiombud	Ja	Ja (Allmänna villkor)
Sambiombud	Ja	Ja

Trepartsavtal för Anslutning via Sambiombud



Direktansluten Medlem

Anslutningsavtal Sambi

- Sambi Bilaga 1 – Definitioner för Sambi
- Sambi Bilaga 2 – Tekniska krav
- Sambi Bilaga 3 – Tillitsramverk
- Sambi Bilaga 4 – Föreskrifter för Sambis Federationsoperatör
- Sambi Bilaga 5 – Avgifter

Tillitsgranskningsavtal

- Bilaga 1 – Tillitsgranskningens omfattning

  Finns för: Användarorganisation, Tjänsteleverantör, Leverantör till Användarorganisation, Leverantör till Tjänsteleverantör

Sambiombud

Sambiombudsavtal

- Sambi Bilaga 1 – Definitioner för Sambi
- Sambi Bilaga 2 – Tekniska krav
- Sambi Bilaga 3 – Tillitsramverk
- Sambi Bilaga 4 – Föreskrifter för Sambis Federationsoperatör
- Sambiombud Bilaga 5 – Föreskrifter för Sambiombud
- Sambiombud Bilaga 6 – Avgifter

Tillitsgranskningsavtal

Samma som för direktanslutna medlemmar

Granskning av Sambiombud

BILAGA 5 - Föreskrifter för Sambiombud

Version: 1.0

Innehåll

Uppgift	Användar-organisation	Sambiombud	Federations-operatör	Tillitsgransk-ningstjänst	Sambis styrgrupp
Upprätta tillitsdeklaration	Ansvarig	Behjälplig			
Vid initial tillitsgranskning, kontrollera och leverera en Fullständig tillitsdeklaration för Användarorganisationen till Sambis Tillitsgranskningstjänst.	Behjälplig	Ansvarig			
Vid återkommande tillitsgranskning, kontrollera och leverera en fullständig Tillitsdeklaration för Användarorganisationen till Sambis Tillitsgranskningstjänst.	Behjälplig	Ansvarig			

Granskning av Medlem ansluten via Sambiombud

Sambiombudet ska leverera en Fullständig tillitsdeklaration för Användarorganisationen till Sambis Tillitsgranskningstjänst, omfattande:

A. Generella krav
B. E-legitimationsutfärdare
C. Attribututgivare
D. Identitetsintygsutgivare

A. Generella krav - Säkerhetsarbete

Krav A.3: Betrodd Part ska för den tjänst som medlemskapet avser ha infört ett strukturerat säkerhetsarbete anpassat efter risker och säkerhetsbehov, bestående av:

- En **riskanalys** avseende tjänsten och dess funktioner. Denna ska ta hänsyn till skyddsvärde, befintliga skyddsåtgärder och legala krav. Riskanalysen ska omfatta analys av hot och sårbarheter, samt sannolikhet och konsekvens (skada) på Användare, den egna organisationen, andra Medlemmar och Federationsoperatören.
- Ett **ledningssystem för informationssäkerhet** för tjänsten baserat på ISO/IEC 27001 eller motsvarande. Säkerhetsåtgärderna ska hantera riskerna enligt riskanalysen för tjänsten och dess funktioner.
- Genomförd **internrevision** av införandet och efterlevnaden av säkerhetsregelverket för tjänsten.

Riskanalys och internrevision ska genomföras årligen och leda till en förbättringsplan innehållande rekommenderade säkerhetsåtgärder.

Några aktuella frågor

- Kan en koncern ansluta alla sina anslutna företag
- Granskning av Sambiombud
- Hur långt kan ett strukturerat säkerhetsarbete förenklas för Medlemmar anslutna via Sambiombud
- Hantering av Medlemmar och Sambiombud som inte lever upp till federationens krav
- Gränssnitt mellan federationsoperatören och Sambiombudet