Svenskt federationsforum

möte 5

Internetdagarna 21 nov 2016

Möte nr 5

- Vad som händer
- Utbyta idéer
- Identifiera gemensamma arbeten

Från mötet 24 nov 2015 - Fortsatt gemensamt arbete?

- En POC för federativ hantering av appinloggning och IoT – identifiering av enheter
- Gemensamma federerade infrastrukturtjänster
- Säkerhetskrav och tillitsarbeten mellan federationerna
- Samordnad kravställning på de stora molntjänsternas federativa anpassning
- Entitetskategorier
- Livscykelhantering av användare
- Standardisering
- Anvisningstjänst
- Nyckelhantering och krypto
- Onbording för användarutrustning
- Test och testverktyg
- Hur komma igång. Låt inte det bästa bli det godas fiende
- Hur får vi gång en dialog och samla informationen?

Program

10:30 Status för

- SWAMID, eduroam, GÉANT Association
- Skolfederation
- Sambi
- E-legitimationsnämnden

12:00 Teknikutveckling

- OIDC användningsområden, testverktyg och federation
- Self-Sovereign Identity (SSI)

12:30 Lunch

13:30 För Internetdagarna gemensam session

14.00 Inblick i två sektorers arbete med federationer

Vård och omsorg

- vad gör regioner och landsting inom federativ inloggning, behörighetsstyrning, SSO samt mobil åtkomst

Polismyndigheten

- federativt arbete inom myndigheter

- Diskussion
  - Vilka är likheterna, skillnaderna och vad är av generellt intresse för alla federationer

15.00 Fika

15.30 Tillit i federationer

- Pågående arbeten
  - Tillitsmodellen för betrodda tjänster enligt eIDAS,
    Björn Hesthamar, Post- och telestyrelsen
  - Granskning av medlemmar anslutna via ombud?
    Staffan Hagnell, IIS
  - Status för SWAMID granskning av AL1 och AL2,
    Pål Axelsson, Swamid
- Diskussion - Hur skapa tillit bland federationens medlemmar?
  - Ändras verkligen en federation behovet av tillit mellan de medverkande parterna?
  - Hur bör tillsyn ske av medlemmarna i en federation?
  - Vad kan göras för att vidareutveckla säkerheten i federation?

16.30 Samarbetsfrågor och plan för fortsatt arbete

- Hantering av appar
- …flera

Sammanfattning och plan

17.00

Status för våra federationer

Leif Johansson, SUNET

Eduroam, SWAMID och GÉANT Association

Länk till presentation: **HTTP://BIT.LY/2FHBTOZ**

Skolfederation

Statusuppdatering

Agneta Wistrand

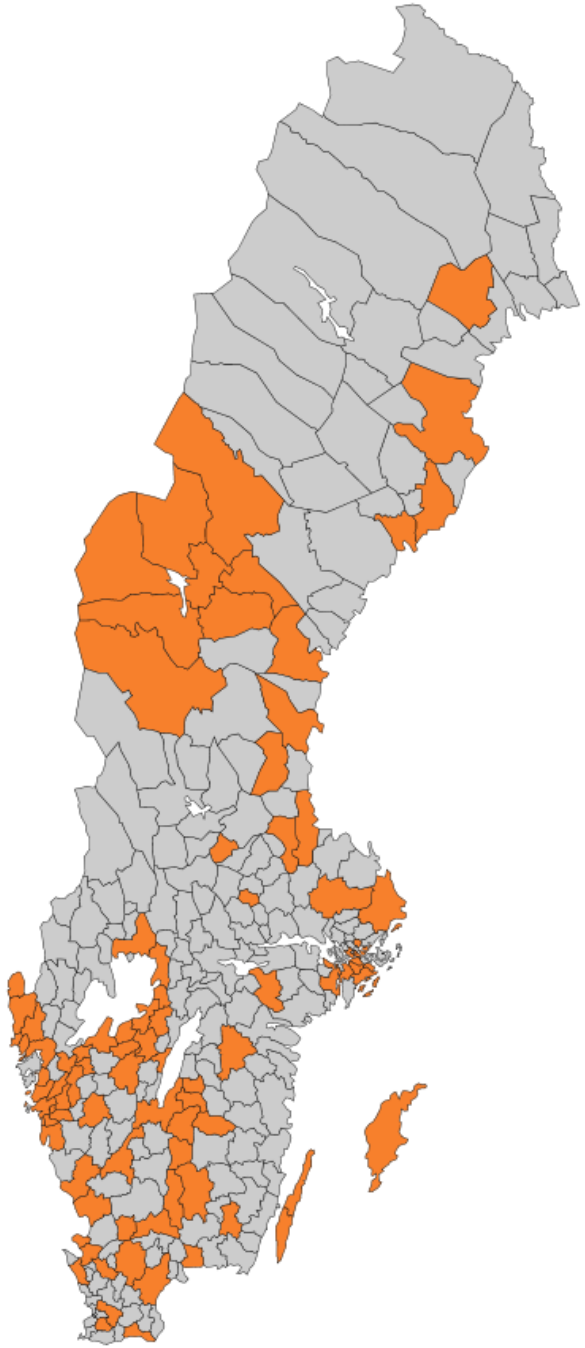
IIS, Internetstiftelsen i Sverige

För ett år sedan

- 139 medlemmar
  - 98 användarorganisationer
  - 41 tjänsteleverantörer

+ 25%

Skolfederation



174 MEDLEMMAR

123 ANVÄNDARORGANISATIONER

- 93 kommunala skolhuvudmän – karta
- 24 friskolor
- 5 förbund
- 1 myndighet

51 TJÄNSTELEVERANTÖRER

Skolfederation

51 tjänsteleverantörer

AXIELL EDUCATION & MEDIA

BONNIER EDUCATION AB

COMFACT AB

CONDIDACT AB

CREAZA AS

DIGILÄR AB

EDIMIA EDUCATION AB

EDQU AB

EKONOMIKÖRKORT PG HB

FILMOTEKET STOCKHOLM AB

FRIDTJUV AB

GLEERUPS UTBILDNING AB

GLOSBOKEN AB

INFOMENTOR P.O.D.B AB

INLÄSNINGSTJÄNST UTBILDNI...

INVIGOS AB

IST SVERIGE AB

ITSAC AB

ITSLEARNING AB

KIKORA AB

LANTMÄTERIET

LEARNIFY AB

LIBER AB

LINFRE EDUCATION

MEDIACENTER VÄSTERBOTTEN

MEDIAPOOLEN VÄSTRA GÖTAL...

MV-NORDIC AB

MYSTUDYWEB SWEDEN AB

NATUR & KULTUR

NE NATIONALENCYKLOPEDIN AB

NOVA SOFTWARE AB

PING PONG AB

SANOMA UTBILDNING

SCHOOLIDO AB

SCHOOLSOFT AB

SKOLON AB

SLI AB

SMART CLASSROOM MANAGER

SOFTRONIC AB

SPSM TJÄNSTELEVERANTÖR

STOCKHOLMS UNIVERSITET

STUDENTLITTERATUR AB

SVENSKA INSTITUTET FMS AB

SWEDISH FILM AB

TEMPUS INFORMATION SYSTE...

TERSUS SKOLSYSTEM AB

TIETO SWEDEN HEALTHCARE &...

TIMEEDIT AB

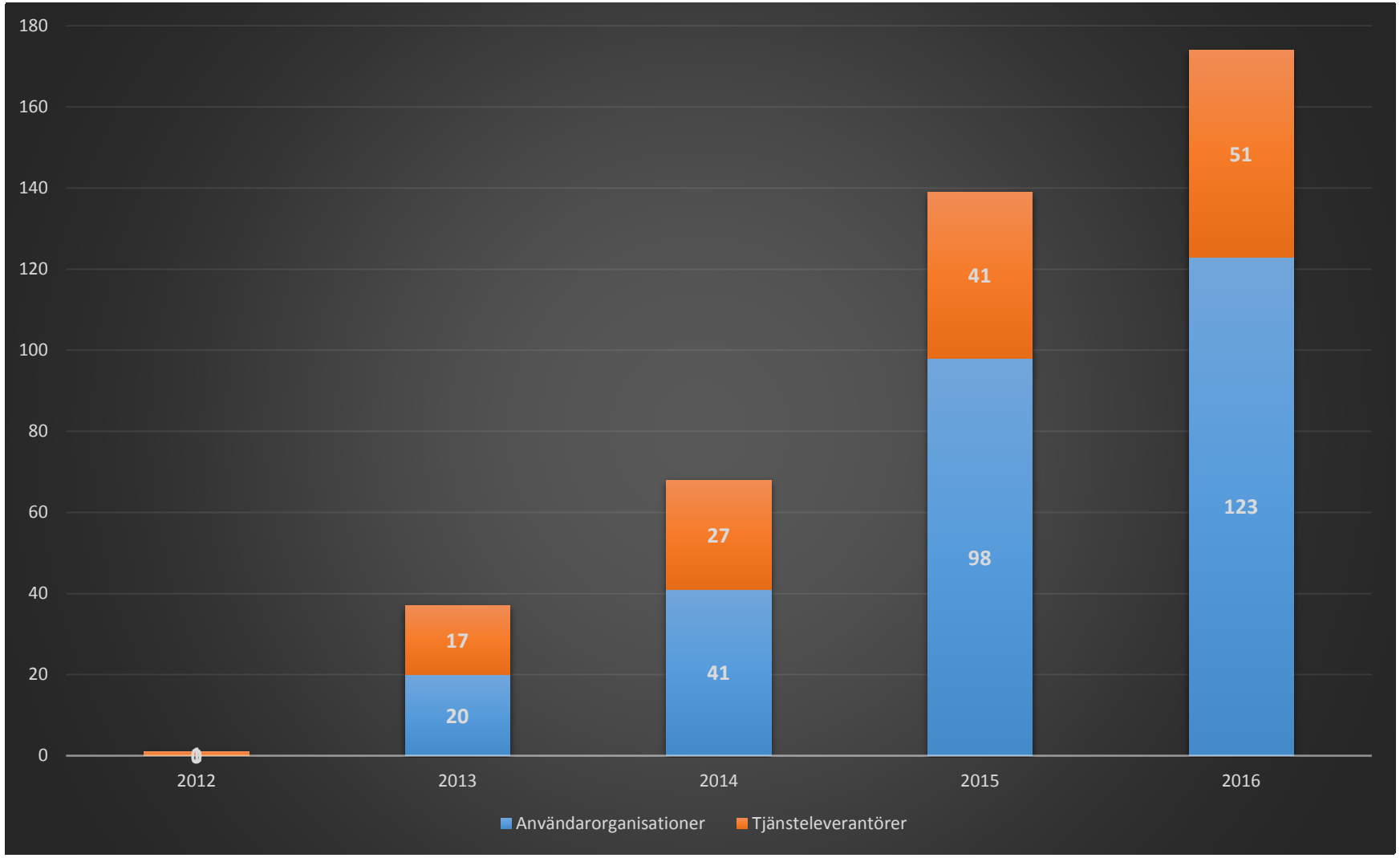
UNIKUM – UNIKT LÄRANDE AB

URKUND

WORDFINDER SOFTWARE AB

Skolfederation

Medlemsutveckling



Skolfederation

Under året

- Utökat medlemsbegrepp

  utbildningsanordnare som bedriver utbildningar vid vilka studiestöd kan lämnas enligt studiestödsförordningen (2000:655) och dess tillhörande bilaga

- Ny version av attributprofilen, via SIS

- Skolverkets nya strategier för grund- och gymnasieskola

- Erfarenhetsutbyte i Alingsås

Skolfederation

På gång

- Imorgon: Digitaliserings möjligheter i skolans värld
- Skolverket och digitala nationella prov
- Halvdagars infomöten med kommun-värdar
  - Nästa i Staffanstorp 5/12
- Introduktionskurser i vår

Skolfederation

Vidareutveckling

- App-proxy: förenklad inloggning för tjänster som enbart levereras som native-app
- Livscykelhantering av användarkonton, pågående arbete i SIS/TK 450
- Microsoft ADFS: problematik med ADFS och eGov 2.0, behov av samordning för åtgärd

Skolfederation

Tack

- Besök oss i IIS federationsmonter!
- info@skolfederation.se
- www.skolfederation.se

#skolfed

Skolfederation

Sambi
Samverkan
för säkrare
e-hälsa

Svenskt federationsforum

Internetdagarna 2016-11-21

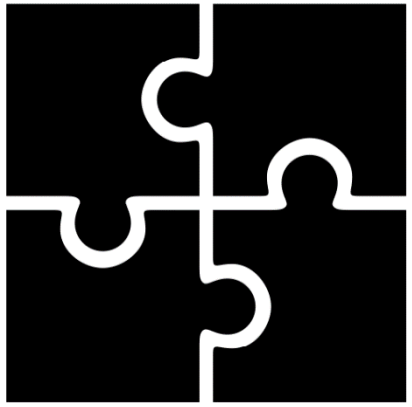
Manne Andersson, eHälsomyndigheten
Robert Sundin, IIS

SEKTORN

- Ökad säkerhet
- Stimulera utveckling

ANVÄNDARORGANISATION

- Valfrihet att välja sin egen lösning
- Enklare tjänsteintegration
- Enhetlig administration av användare



TJÄNSTELEVERANTÖR

- Slippa administration av användare
- Enklare integration av användarorganisationer

ANVÄNDARE

- SSO, en inloggning till alla tjänster

Sambi

Medlemmar

Användarorganisationer

- Stockholms stad
- Stockholms Läns Landsting
- Danderyds kommun

E-tjänster

- SLL Beställningsportalen

18 månader i produktion

Betrodd part	Betrodd som	Återkommande granskning senast / Notering
Tieto Sweden AB, Brokertjänst	Leverantör till tjänsteleverantör	2018-06-09
Stockholms läns landsting, Beställningsportalen (HSF, Avdelningen för Närsjukvård, Rehabilitering, habilitering och hjälpmedel)	Tjänsteleverantör	2018-09-21
Stockholms stad	Användarorganisation	2018-10-07
Inera AB, katalogtjänst HSA	Leverantör till Användarorganisation	2018-10-16
Inera AB, IdP i Inera Nationella Säkerhetstjänster	Leverantör till Användarorganisation	2019-10-05
SLL Stockholms läns sjukvårdsområde, IdP	Användarorganisation	Godkänd med krav på komplettering
Danderyds kommun	Användarorganisation	Godkänd med förbehåll
Lidingö stad	Användarorganisation	Godkänd med förbehåll

Sambi

- Tre under granskning

- Huddinge kommun

Svensk e-legitimation

Planerade anslutningar

eHälsomyndigheten

- Avveckling av dagens säkerhetslösning planerad till maj/juni 2019. Därefter sker anslutning ”via” Sambi
- Arrangerar anpassade Sambiutbildningar under två år

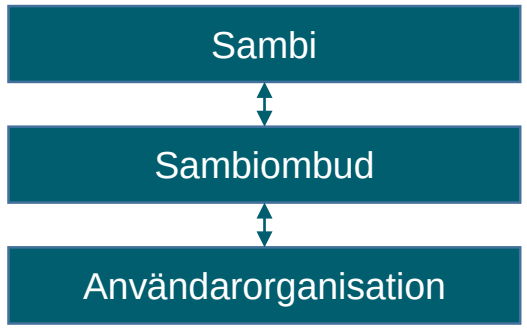
Inera

- Flera pågående aktiviteter - Per Mützell berättar mer i eftermiddag

Tillit

Sambiombud

- Möjligheten till hantering via ombud är avgörande för små vårdgivare utan egna IT-förmågor

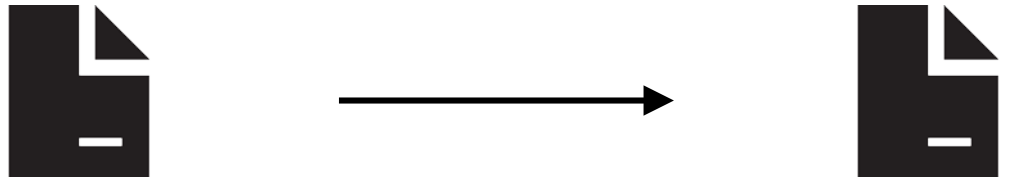


Granskning av molntjänster

- Molntjänster kan inte betraktas som särfall, utan är en självklar del i modern IT-infrastruktur som måste hanteras

Behörighetsmodell för vård- och omsorg

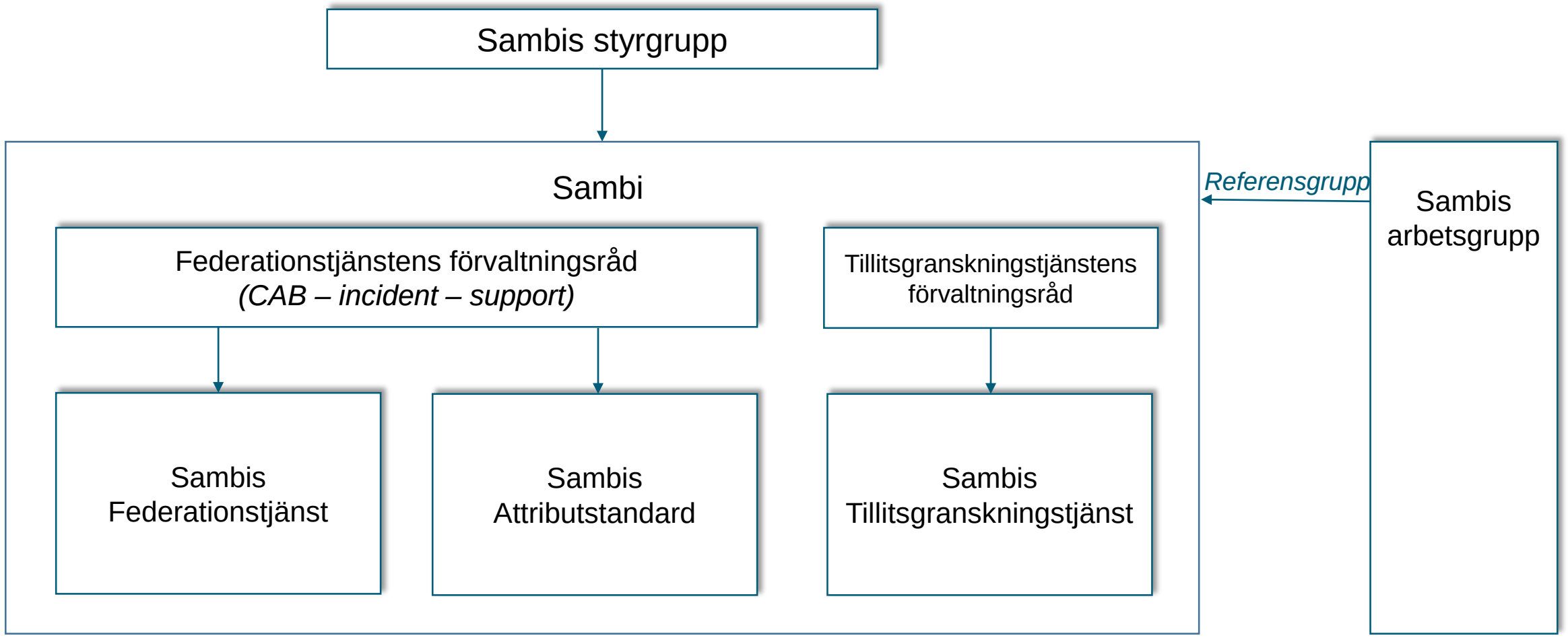
”/…/ ett gemensamt ramverk (principer) för egenskapsbaserad behörighetsstyrning /…/”



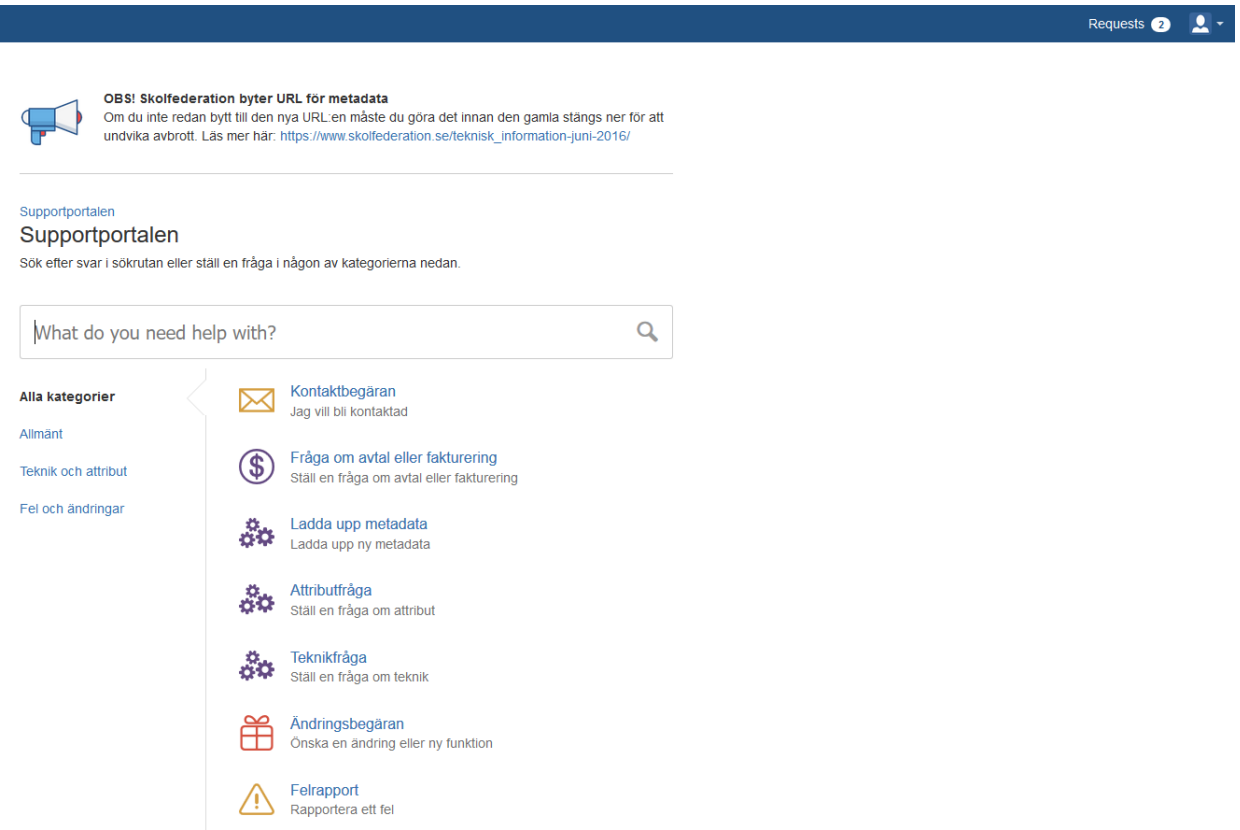
Attributprofil
- vad -

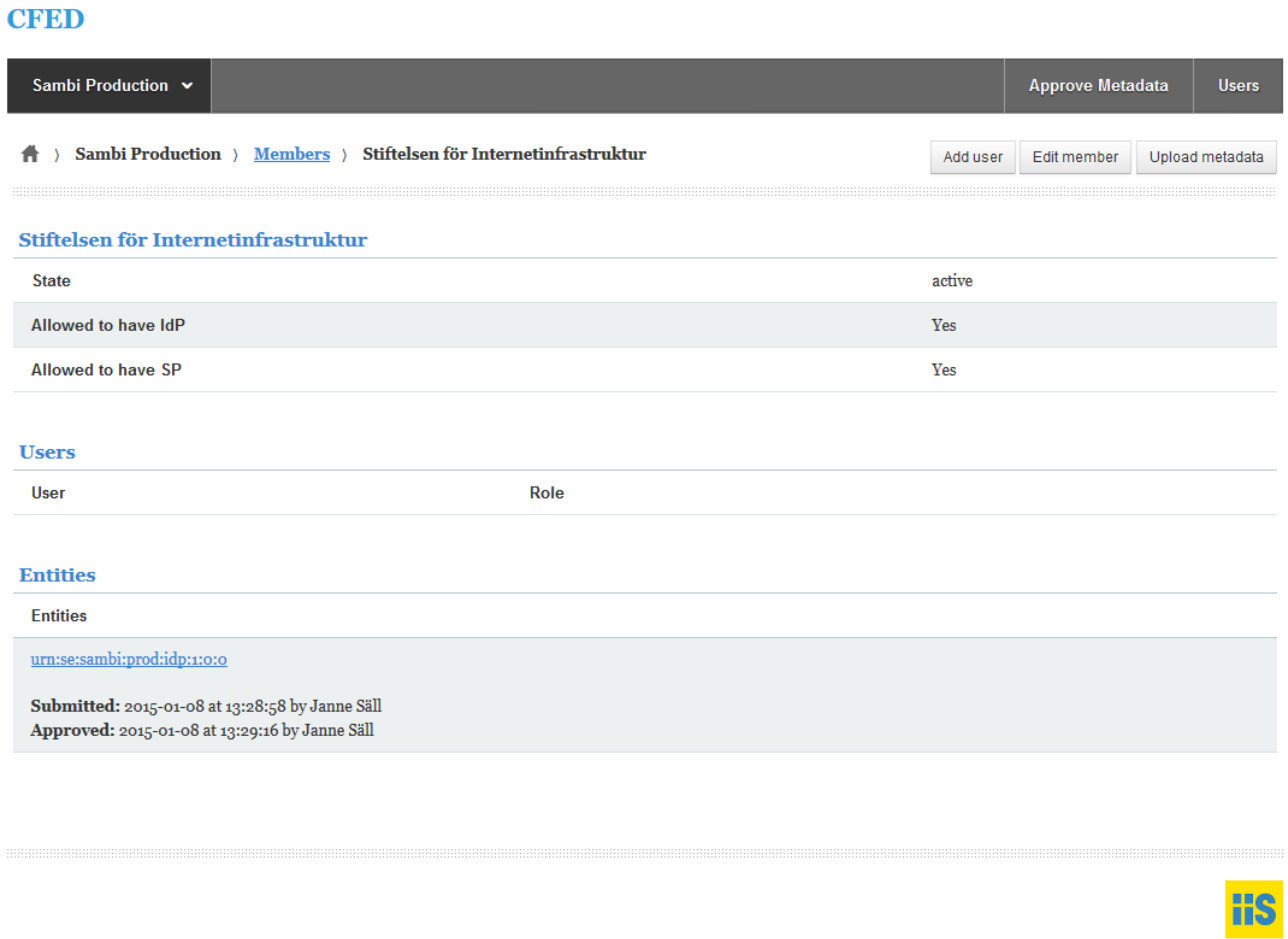
Behörighetsmodell
- hur -

Organisation



Självbetjäning under utveckling





Övrigt

- Feta klienter, maskiner och native-appar
  - Diskussion om OIDC/OAhut 2.0

- ADFS
  - Konstaterar fler frågor avseende problematiken kring ADFS och eGov 2.0
  - Det har funnits flera spridda initiativ gällande kravställning på utveckling – **dags för samordning?**

E-LEGITIMATIONS NÄMNDEN

Läget i Sverige och med eIDAS

2016-11-21

eva.sartorius@elegnamnden.se

Hänt sedan sist

Det senaste året

- Vad hände med det som var tänkt?
  - Övergångslösning
- Samlat in behov genom enkät och dialog, informerat
- Genomfört regeringsuppdrag om det kommande
- Sjösatt pilottestmiljö för e-tjänsters koppling till utländska e-legitimationer (den svenska eIDAS-noden)
  - Har testat med Danmark och Österrike
  - Norge, Island, Estland och Storbritannien är på gång in
  - Svenska parter som vill påverka är välkomna!

E-LEGITIMATIONS NÄMNDEN

Aktiviteter framåt

E-legitimationsnämndens mål

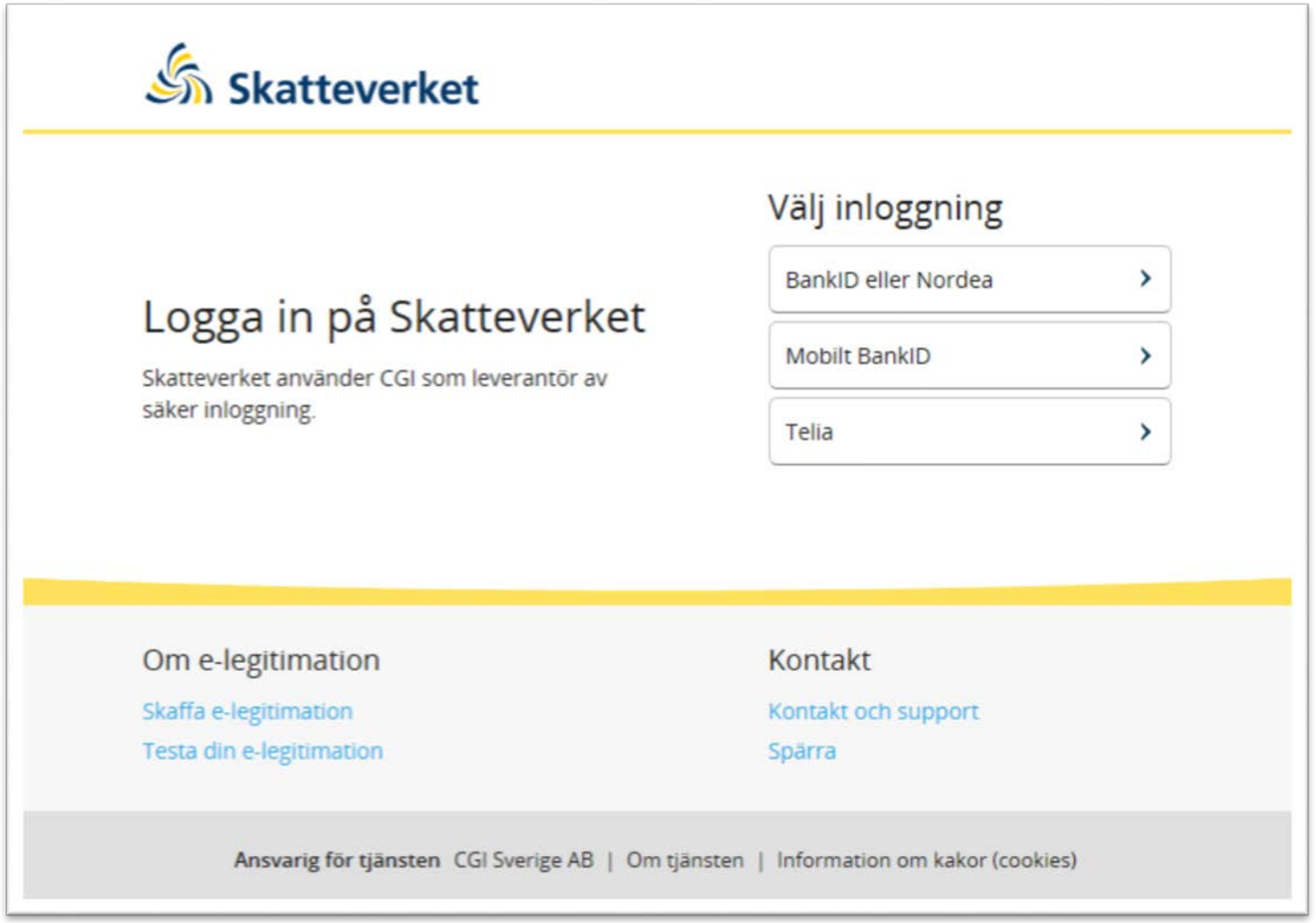
- Alla ska kunna få tillgång till säkra e-legitimationer som är enkla att använda

- Det ska vara enkelt och säkert för digitala tjänster att inkludera e-legitimering och e-underskrift

- Det ska vara kostnadseffektivt för offentlig sektor med e-legitimering och e-underskrift

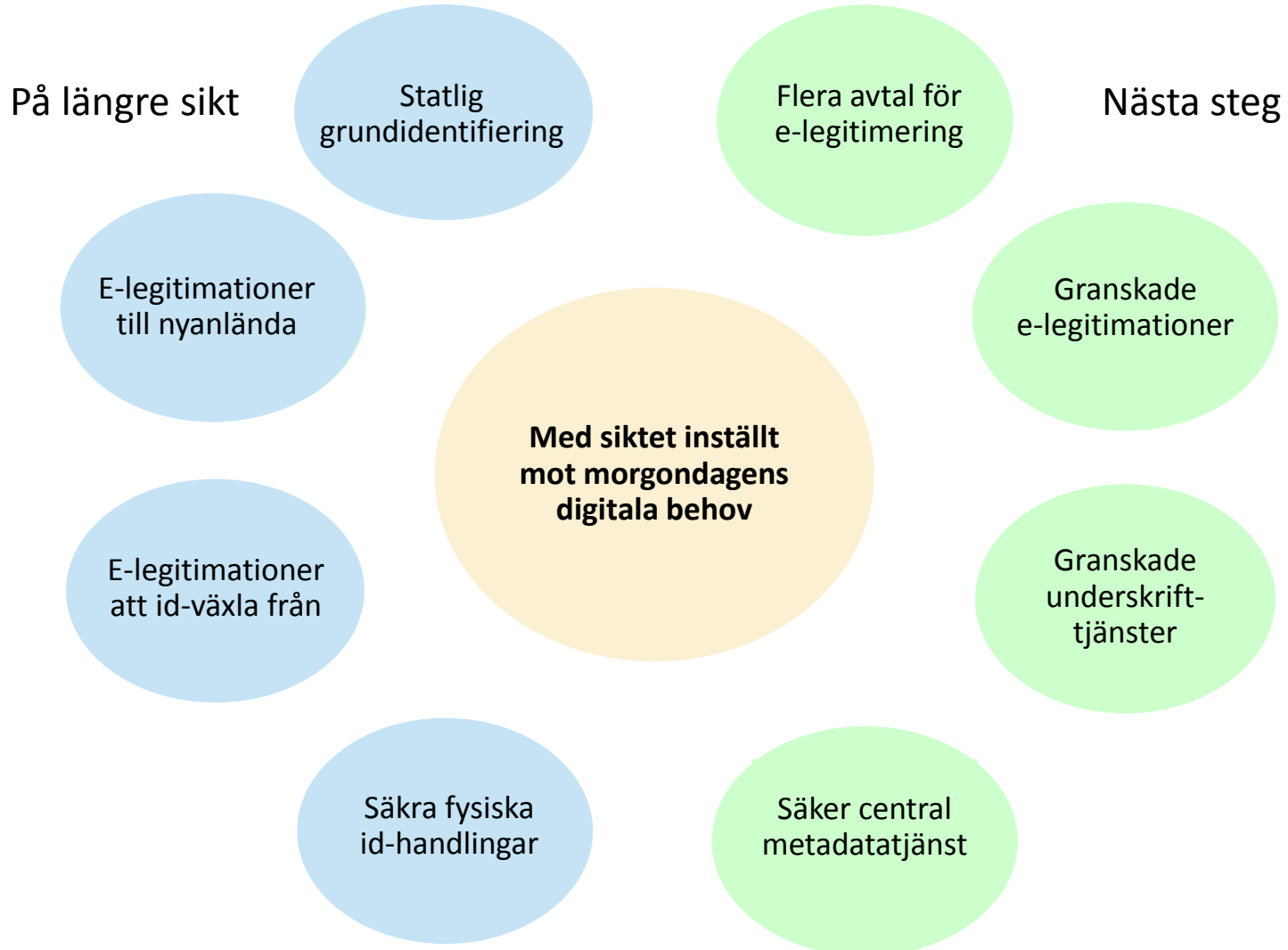
E-LEGITIMATIONS NÄMNDEN

Idag finns bara tre sätt att logga in .. som inte är tillgängliga för alla



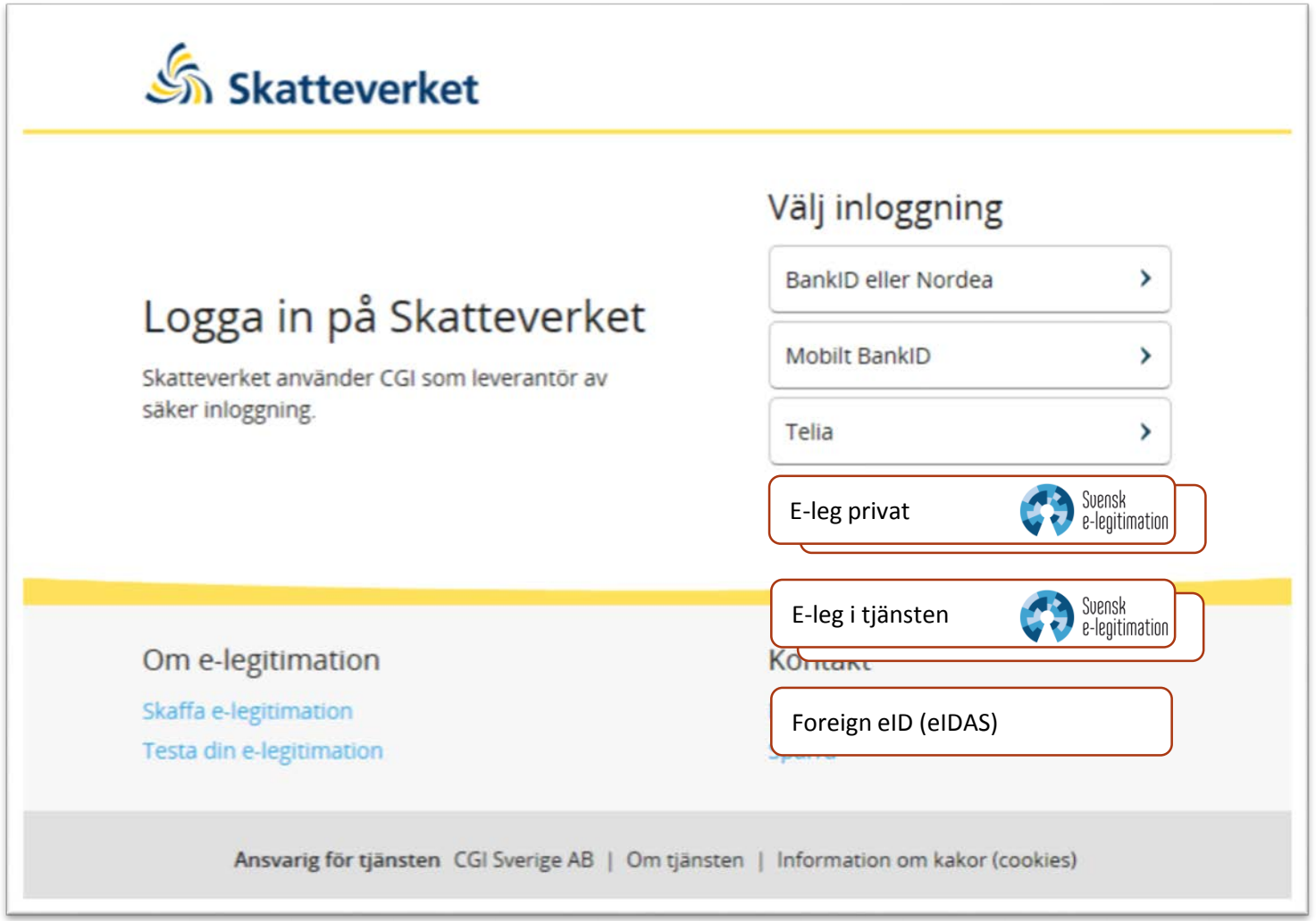
E-LEGITIMATIONS NÄMNDEN

Nämndens regeringsrapport



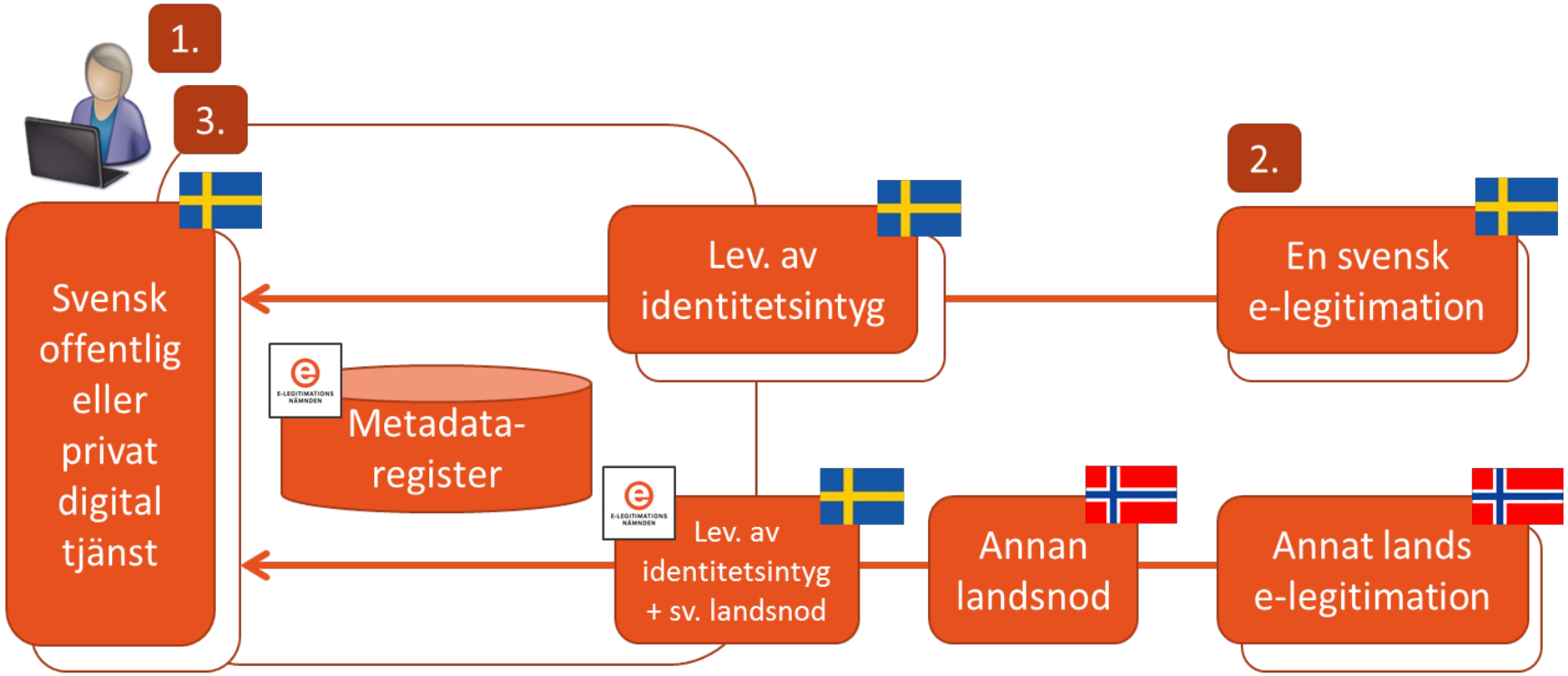
E-LEGITIMATIONS NÄMNDEN

I morgon finns fler – tillgängliga för alla



E-LEGITIMATIONS NÄMNDEN

Förenklad översikt över e-legitimeringsflödet



1. Användaren vill logga in i en tjänst
2. Användaren e-legitimerar sig
3. Användaren loggas in i tjänsten.

E-LEGITIMATIONS NÄMNDEN

Vad behöver nämnden göra nu?

1. Främja offentlig upphandling av identitetsintyg även från nya e-legitimationsutfärdare
2. Koppla in ”Foreign eID” (eIDAS-noden)
3. Metadataregister – nationell identitetsfederation
4. Förvalta tekniskt ramverk för intygstrafiken (SAML 2.0)
5. Kvalitetsmärka svenska e-legitimationer och granska underskrifttjänster (samt ev. attributtjänster)

E-LEGITIMATIONS NÄMNDEN

Välkommen till E-legitimationsdagen

1 februari 2017

Inbjudan finns på

elegnamnden.se

Där finns även vår rapport till regeringen

25 oktober 2016

Roland Hedberg, Sunet

TEKNIKUTVECKLING

OIDC ANVÄNDNINGSOMRÅDEN, TESTVERKTYG OCH FEDERATION
SELF-SOVEREIGN IDENTITY (SSI)

Se separat presentation!

Svenskt federationsforum

Paus

Åter kl 14.00

Inblick i två sektorers arbete med federationer

Vård- och omsorgssektorn
Polismyndigheten

Per Mützell, Inera

VÅRD- OCH OMSORGSSEKTORN

VAD GÖR REGIONER OCH LANDSTING INOM FEDERATIV INLOGGNING, BEHÖRIGHETSSTYRNING, SSO SAMT MOBIL ÅTKOMST

Svenskt federationsforum – Internetdagarna

Federativa initiativ och lösningar inom eHälsa

Samverkan inom regioner & landsting för bl.a.
*- samordnad **singelinloggning***
*- skalbar **behörighetstyrning***
*- **mobil åtkomst***
inom och mellan organisationer

2016-11-21

Per Mützell, Senior Lösningsarkitekt, Alcesys

Per.Mutzell@inera.se

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

Bakgrund

- Vård- och omsorg i Sverige – en starkt decentraliserad organisation
  - **Stort samverkansbehov!**
- Federativ samverkan har funnits i många olika former över tid
  - Gemensam struktur, policies och riktlinjer för **utgivning av eID** / eTjänstelegitimation (SITHS)
  - Gemensamma policies och riktlinjer för **katalog/attributhantering** för medarbetare och organisation (HSA)
  - **Förlitande** (trust) som huvudprincip vid säkra integrationer (RIVTA)

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

Ur *Handlingsplan 2013–2018*, övergripande målbild

Landstings, regioners och kommuners samarbete inom eHälsoområdet

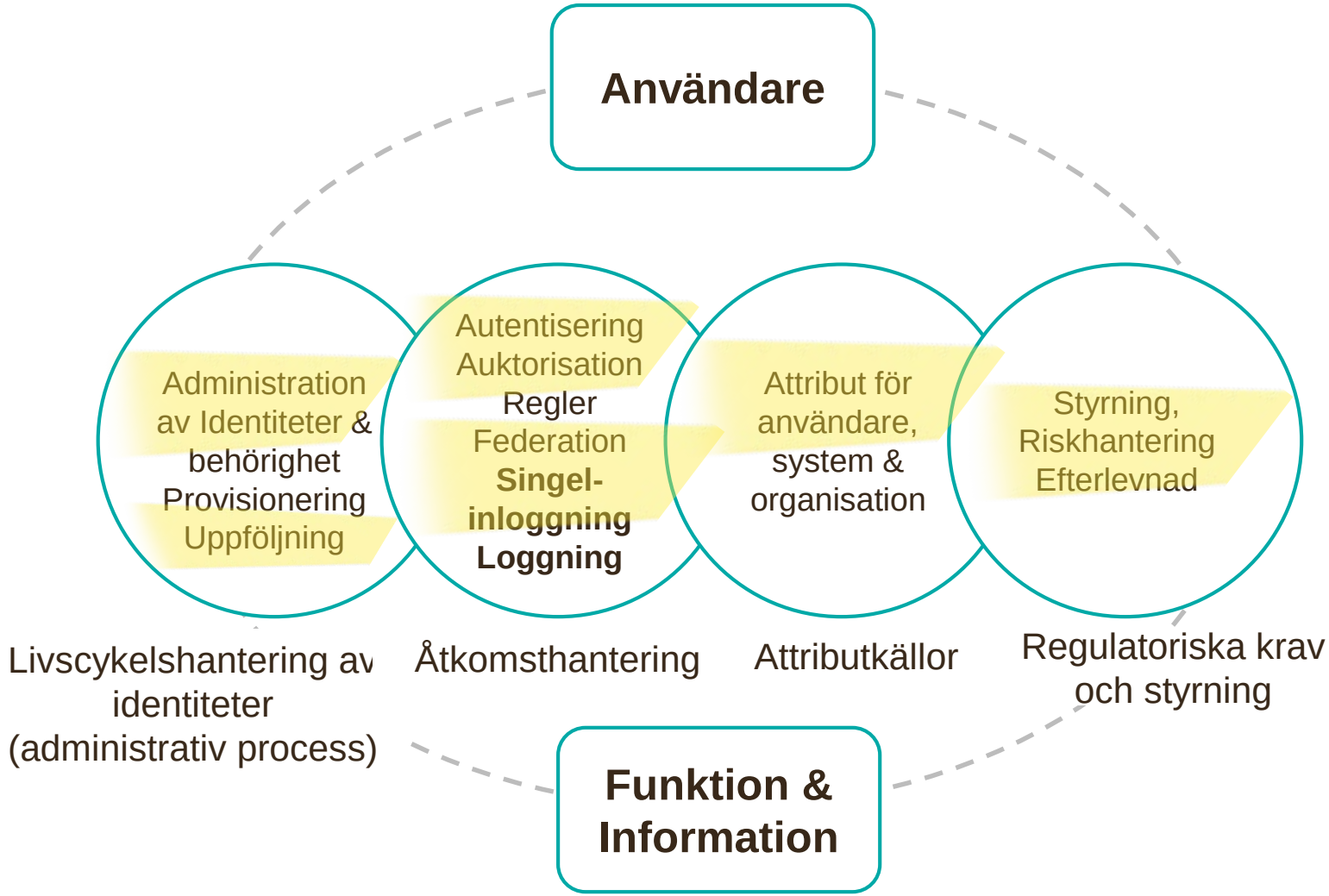
av medarbetarna kan år 2016 nå sina professionella verksamhetssystem med **en** samordnad, enkel och säker inloggning (single-sign-on)

Eller med andra ord:

Användaren har snabb, enkel och säker tillgång till den information hen behöver när den behövs!

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

Som grund behövs en infrastruktur för
Identitet och åtkomst



inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

Drivkrafter & verksamhetsmål

Drivkrafter & verksamhetsmål

Källa: *Förstudie SSO i regioner och landsting* (2015/16)

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

Taktisk nivå – hur genomförs då detta?

- **Gemensamt arbete**
  - Förstudie – *SSO i landsting och regioner* (2015/16)
  - Projekt IDA Access - ***Referensarkitektur för Identitet och Åtkomst*** (ht 2016)
    → ***Gemensamt kravunderlag*** *inom identitet och åtkomst för upphandling och vidareutveckling av framtida IT-stöd!*

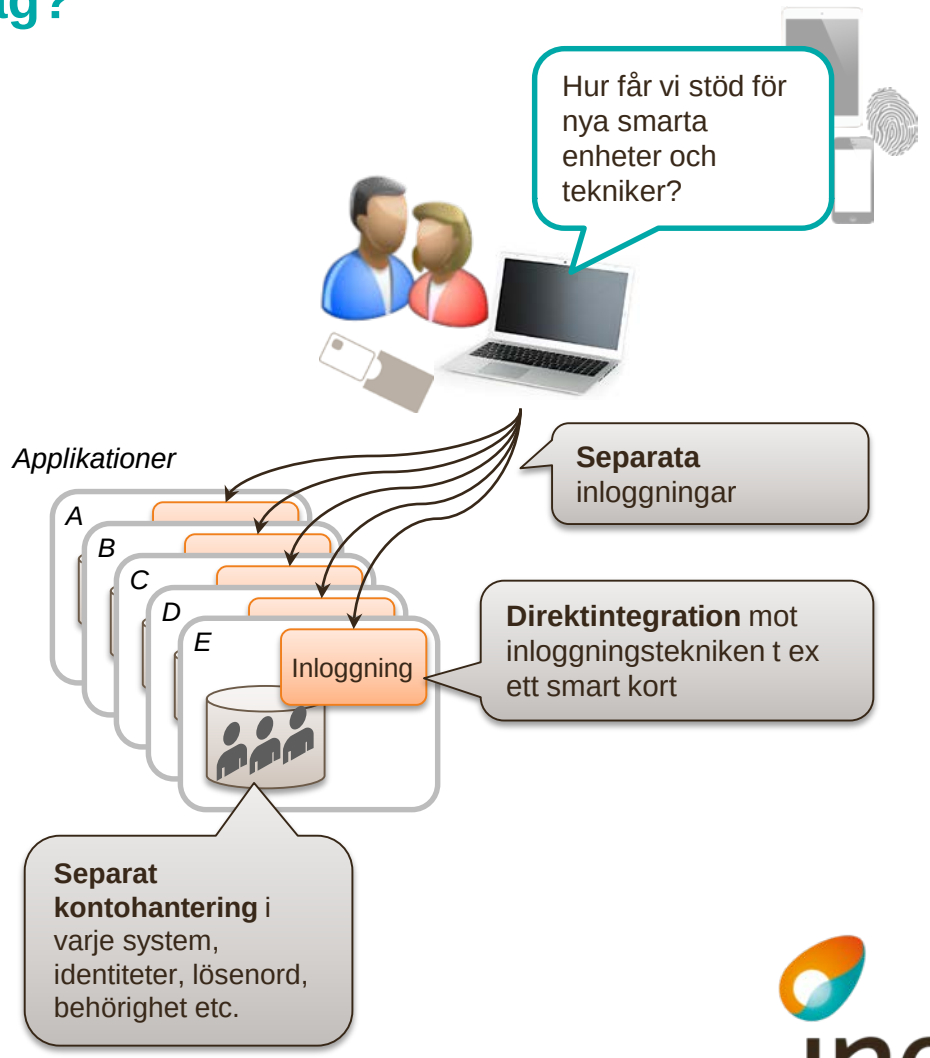
- **Respektive organisation**, regionalt och lokalt
  - Etablera den IT-infrastruktur (förmågor) som behövs, t.ex. *Identifieringstjänst (IdP)*.
  - Verifiera verksamhetsnytta och användarrespons i piloter
  - Kravställa på IT-stödet för anslutning mot IT-infrastrukturen, t.ex. för *federerad inloggning*.

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

Utgångsläget (från förstudien):
- finns stöd för SSO i applikationerna i vården idag?

Funktionalitet

- Applikationer som saknar stöd (egen löseninloggning)
- Enkelriktade uthoppslösningar (system→system)
- **AD-integrerad** inloggning (IWA/Kerberos)
  – endast lokal SSO, svårt med delade arbetsplatser
- **Proprietära lösningar**, ofta direktintegrerade med viss autentiseringteknik (hög kostnad, inlåsning)
- **Biljettbaserad standardiserad** inloggning med SSO
  - regionala & nationella webb-tjänster, administrativa system, molntjänster, Office365 etc.
  Förberedda för federativ samverkan.



inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

Referensarkitektur för Identitet & åtkomst

Ett samverkansprojekt drivet av Inera
med representanter från regioner och landsting

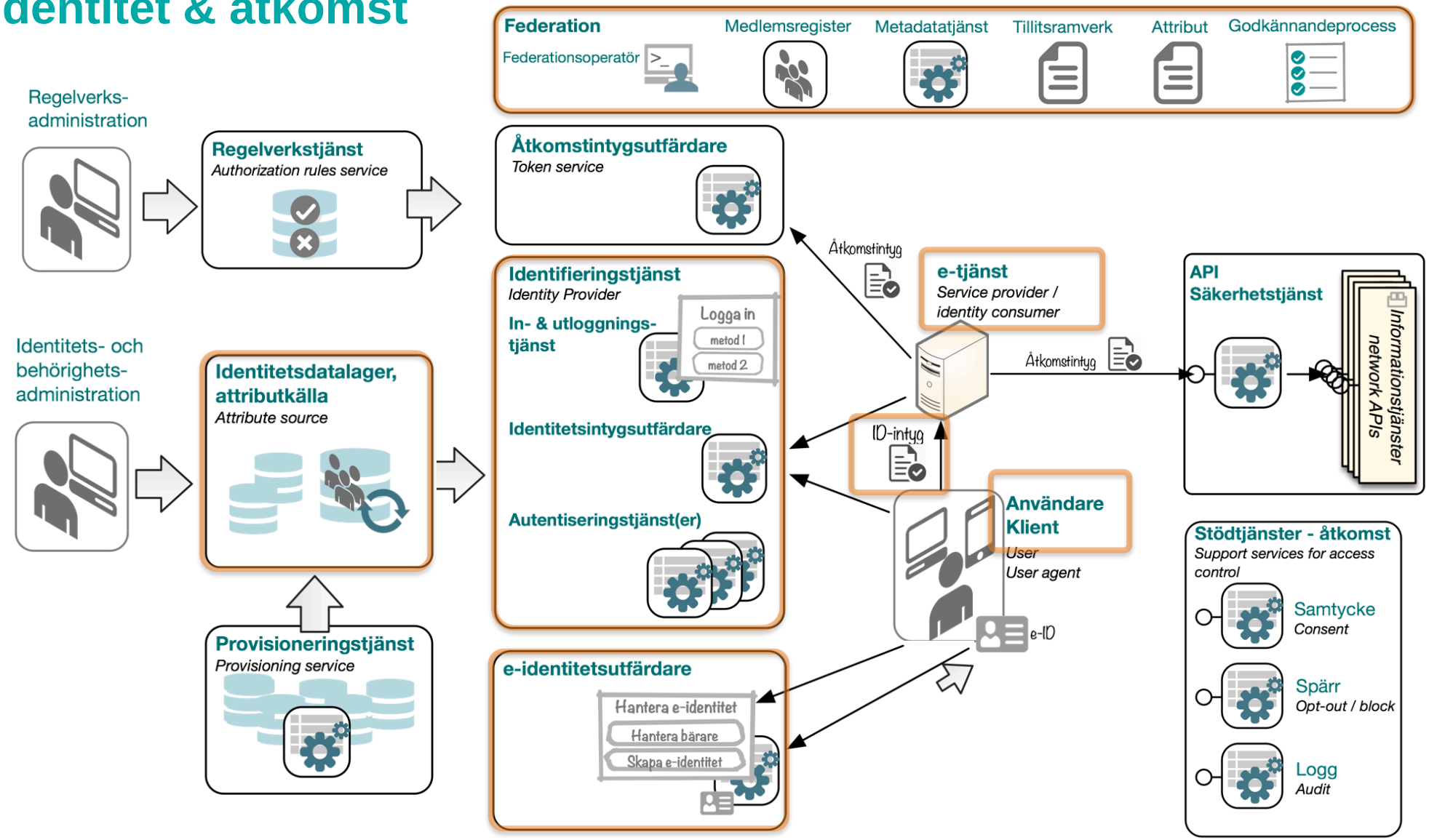
Styrande principer

- **Samverkan i federation**
  - Tillit via gemensamma ramverk
- **Separation av förmågor och lös koppling**
  - Skilja på att hantera säker inloggning respektive hantera verksamhetsinformation (federerad inloggning).
  - Undvik att integrera applikationer direkt mot e-identitetsbäraren!
- **Öppna standarder** för integration, ge flera val
  - **Standardiserad biljettbaserad** teknik för anslutning av e-tjänster, primärt *SAML2*, *OpenID Connect*.
  - Internationella/nationella **integrationsprofiler** för identitet & behörighet
- **Plattformsneutral infrastruktur**
  - **Flexibilitet i teknikval**, olika klientplattformar, mobilt IT-stöd osv.

Bredda stödet med flera protokoll → förenklar anslutning då olika applikationer har olika förutsättningar

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

Referensarkitektur
Identitet & åtkomst

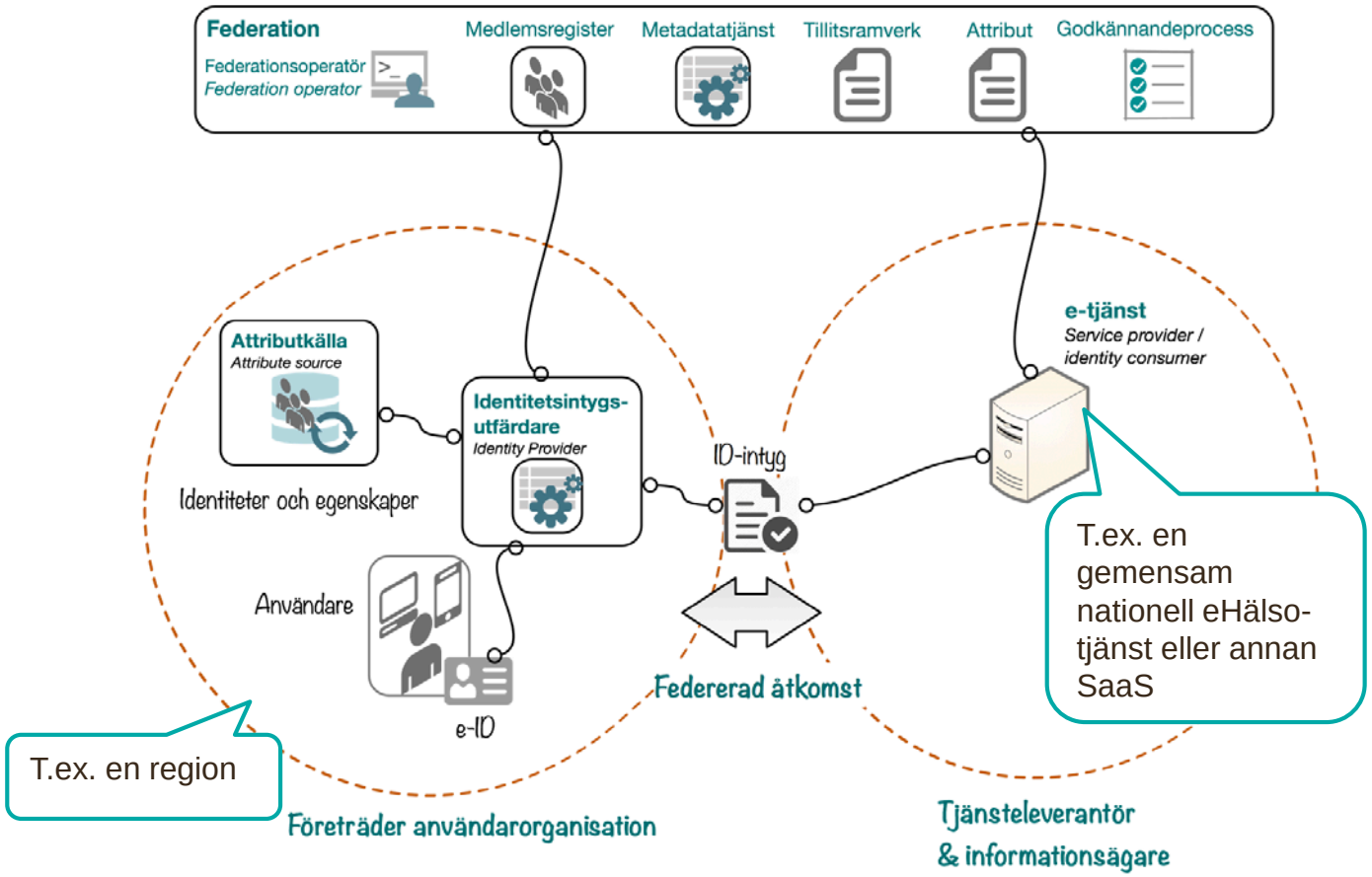


inera
LANDSTING OCH REGIONER
I SAMVERKAN FÖR E-HÄLSA

Några exempel på effekter

- Skalbarhet och minskad administration genom federativ åtkomst
- Mobil åtkomst med mobila bärare
- Flexibilitet och minskat teknikberoende
- Skalbarhet genom självservice med ärvd legitimering

Identitets- och behörighetsfederation

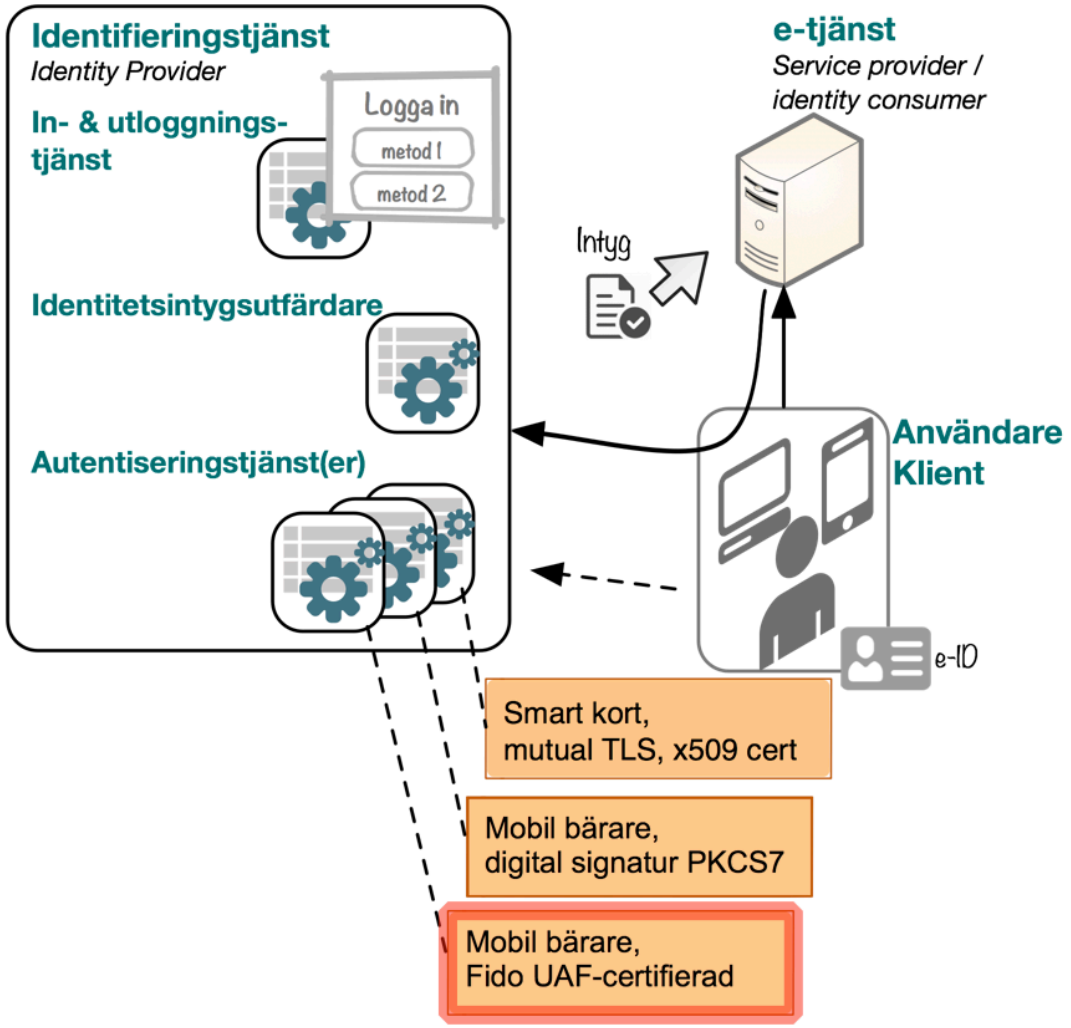


Framgångsfaktorer/pågående arbete

- **Behörighetsstyrande attribut**
  - Sambi Attributspecifikation 1.0, vidare arbete med modeller för behörighetsstyrning
- **Tillitsnivån** för e-identiteterna
  - Utgivningsprocesserna!
- **Ombudshantering/avtal**
  - Viktigt för mindre organisationer, samt samverkansparter/ombud
- Väl avvägda **säkerhetskrav** och effektiva anslutningsprocesser
- **Tekniskt ramverk** i linje med referensarkitekturen
- Anslutning av **gemensam nationell infrastruktur och e-tjänster** (”katalysatorer” / ”killerapps”)

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

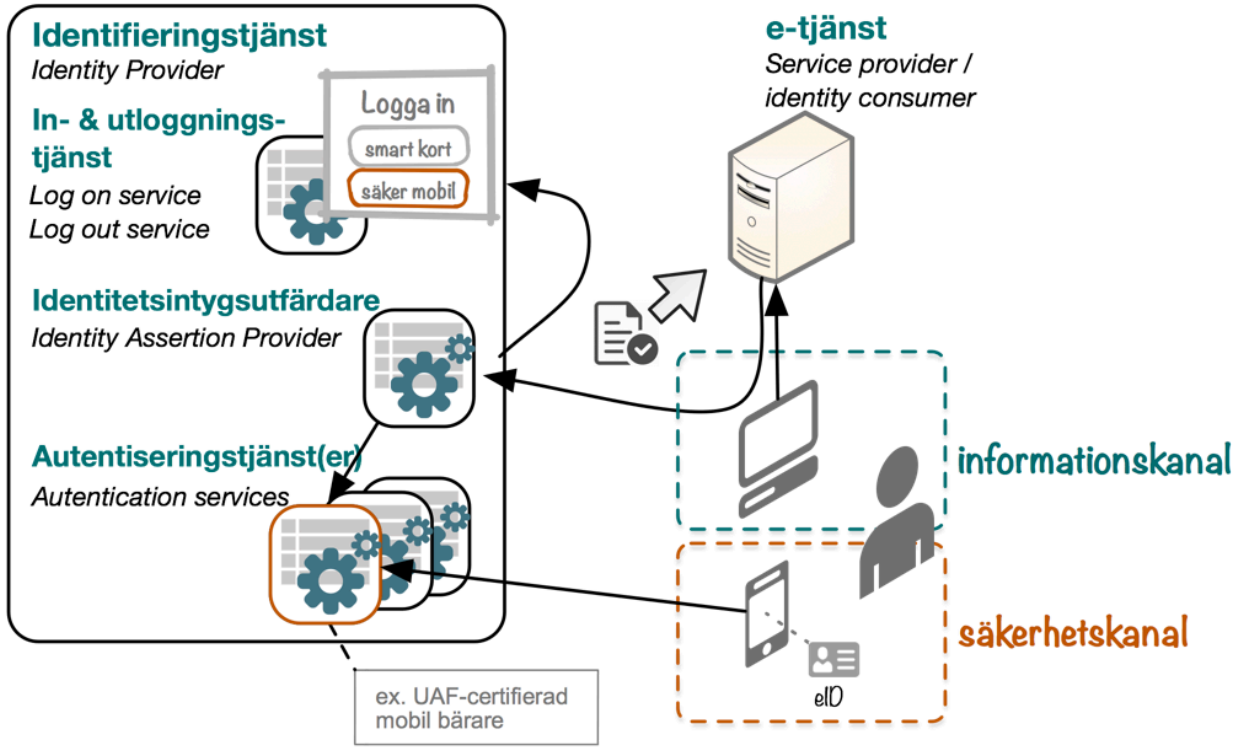
Anslut nya anpassade autentiseringmetoder, t.ex. mobil bärare för eID



- ✓ Möjliggör **mobil åtkomst**
- ✓ **Anpassa säkerhetslösningen** till aktuella behov och krav

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

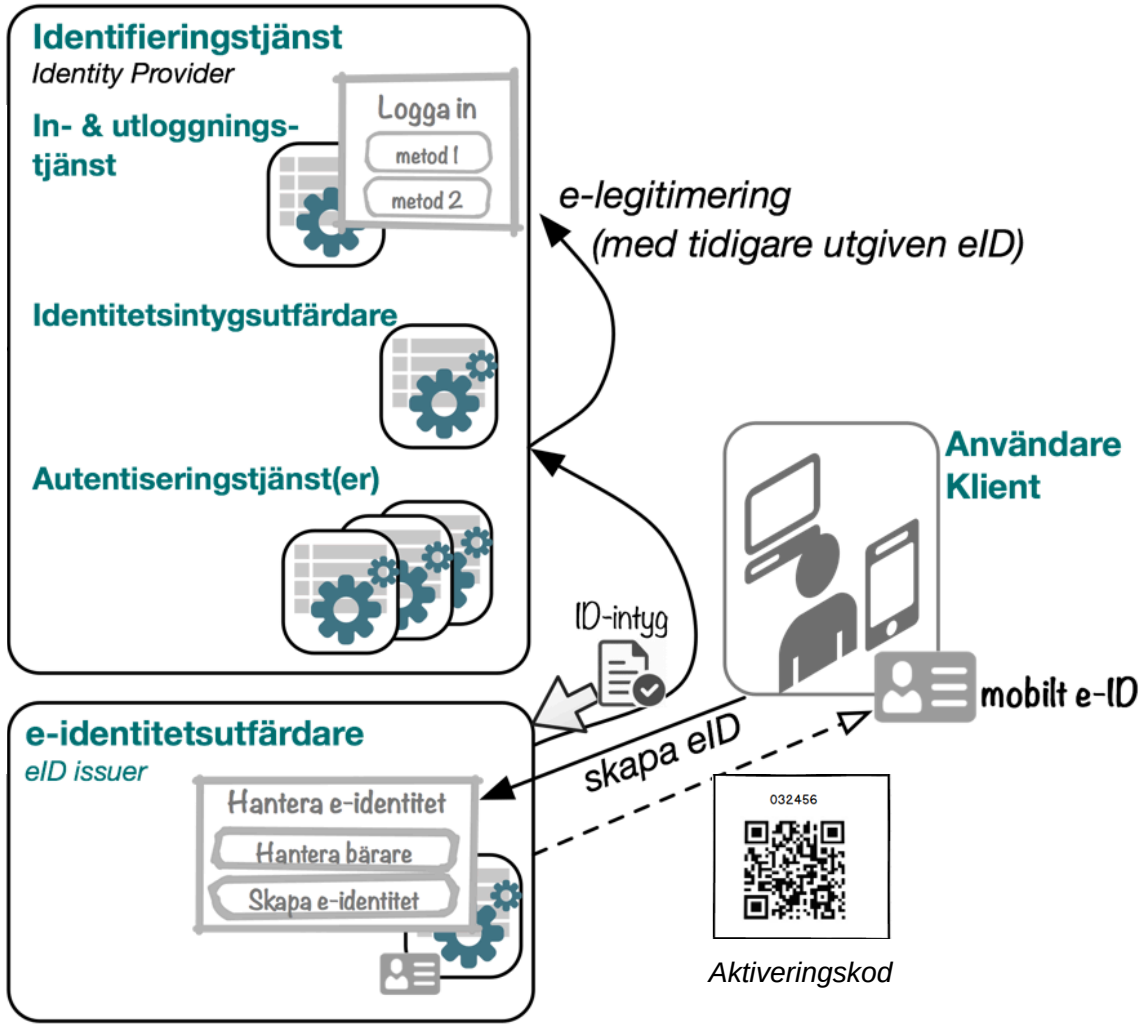
Större flexibilitet med autentisering i separat kanal –
Out-of-bound authentication (OOB)



- ✓ **Större flexibilitet**
- ✓ **Minskat tekniskt beroende** mellan säkerhetstekniken och verktyget för informationsåtkomst

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

Utgivning av eID till mobil bärare, med självservice och ärvd legitimering

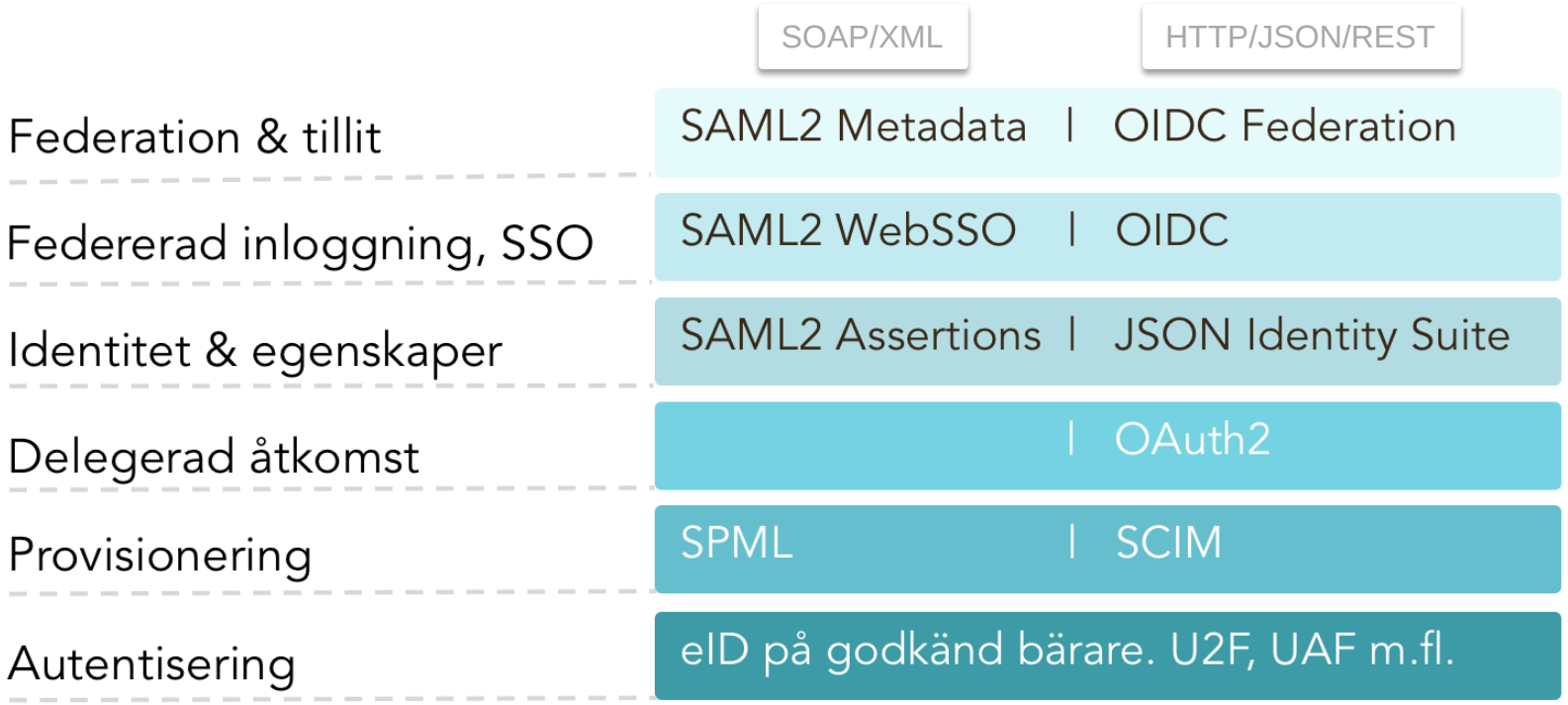


- ✓ **Självservice** ger skalbarheten
- ✓ eID via **ärvd legitimering** som viktigt komplement till direktutfärdade eID

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

Val av tekniska protokoll

Primära tekniska protokoll per förmåga

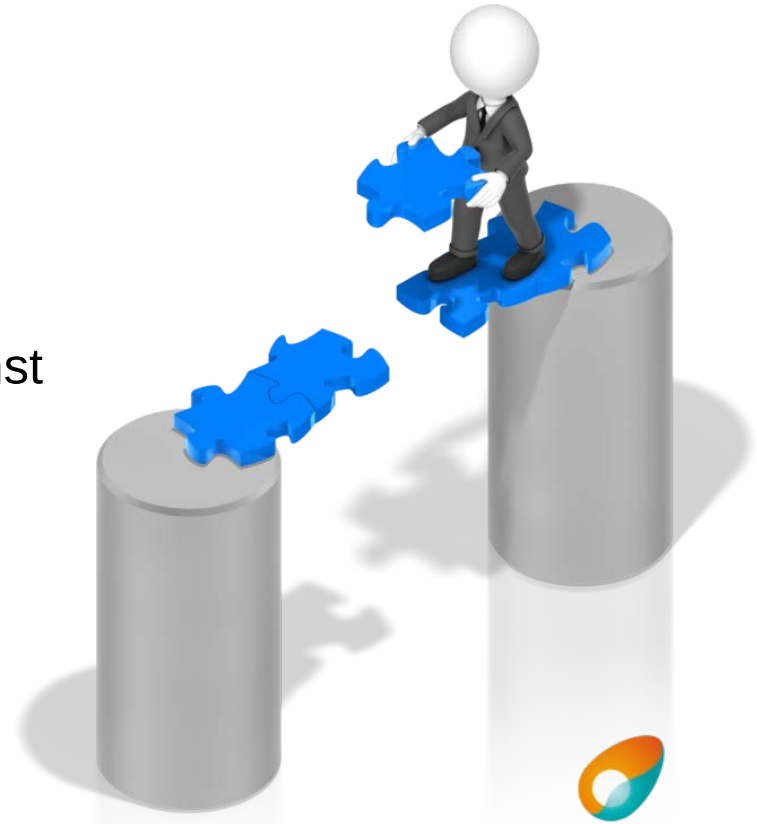


Federationen behöver klara flera protokoll. Teknikvalet för e-tjänsten ska inte begränsa!

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

Sammanfattning

- *Referensarkitektur för Identitet och åtkomst* skapar förutsättningar för bl.a.
  - ✓ **Singelinloggning** och **mobil åtkomst**
  - ✓ **Federativ åtkomst** och **säker api-åtkomst**
  - ✓ **Minskat tekniskt beroende**, **minskad administration** och en **stabilare förvaltning**.
- Viktiga styrande principer i arbetet med identitet och åtkomst inom eHälsa är
  - ✓ **Federativ samverkan**
  - ✓ **Separation av förmågor**
  - ✓ **Öppna standarder** för anslutning av tekniken
  - ✓ **Plattformsneutralitet**



inera
LANDSTING OCH REGIONER
I SAMVERKAN FÖR E-HÄLSA

Tack för uppmärksamheten!

Mer information

inera.se, *sambi.se*

inera
LANDSTING OCH REGIONER
I SAMVERKAN FÖR E-HÄLSA

inera

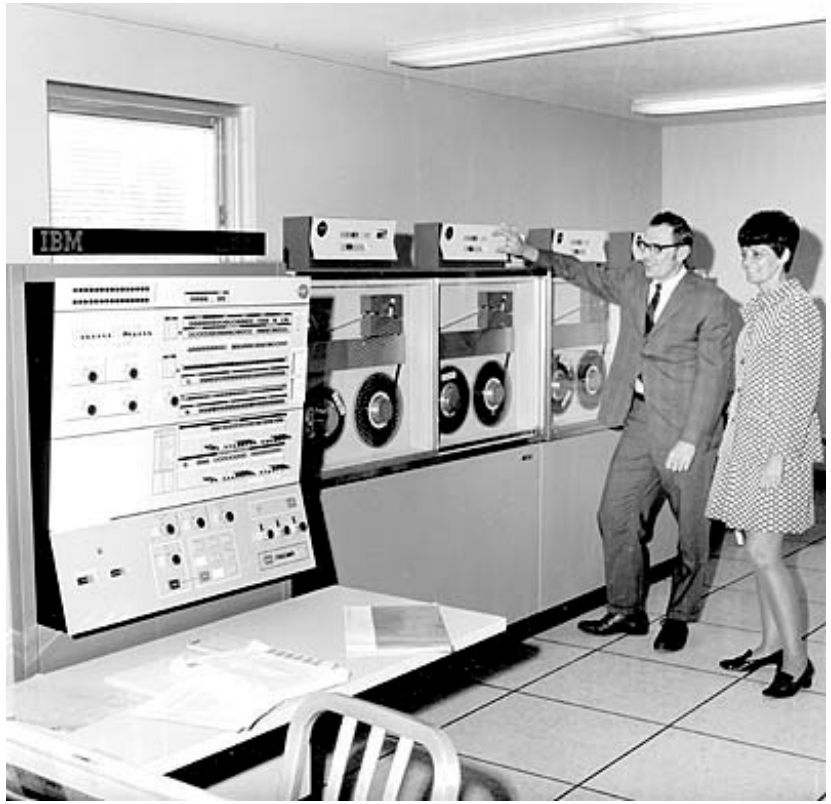
LANDSTING OCH REGIONER
I SAMVERKAN FÖR E-HÄLSA

Federation inom Polisen

2016-11-21, Johanna Mannung, Säkerhetsarkitekt, IT-säk

Newbies

Federationslösningar sedan hedenhös



Att börja med federationer

Tillitsramverk? Eller förordningar, föreskrifter och tillsyn?

- Polisdatalagen anger vilka uppgifter som får lämnas ut via direktåtkomst
- Polisdataförordningen ger Polismyndigheten föreskriftsrätt kring säkerhetskrav vid direktåtkomst
- Rikspolisstyrelsens föreskrifter och allmänna råd om behandling av personuppgifter i Polisens brottsbekämpande verksamhet
- Rikspolisstyrelsens föreskrifter om säkerhet vid Polisens informationsbehandling med stöd av IT
- Tillsyn: Datainspektionen, SIN, SÄPO

Vem får federera med oss?

- **Polisdatalagen: Direktåtkomst**
- **8 §** Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket får medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.
- En myndighet som medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.
- Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.*Lag (2014:597)*.

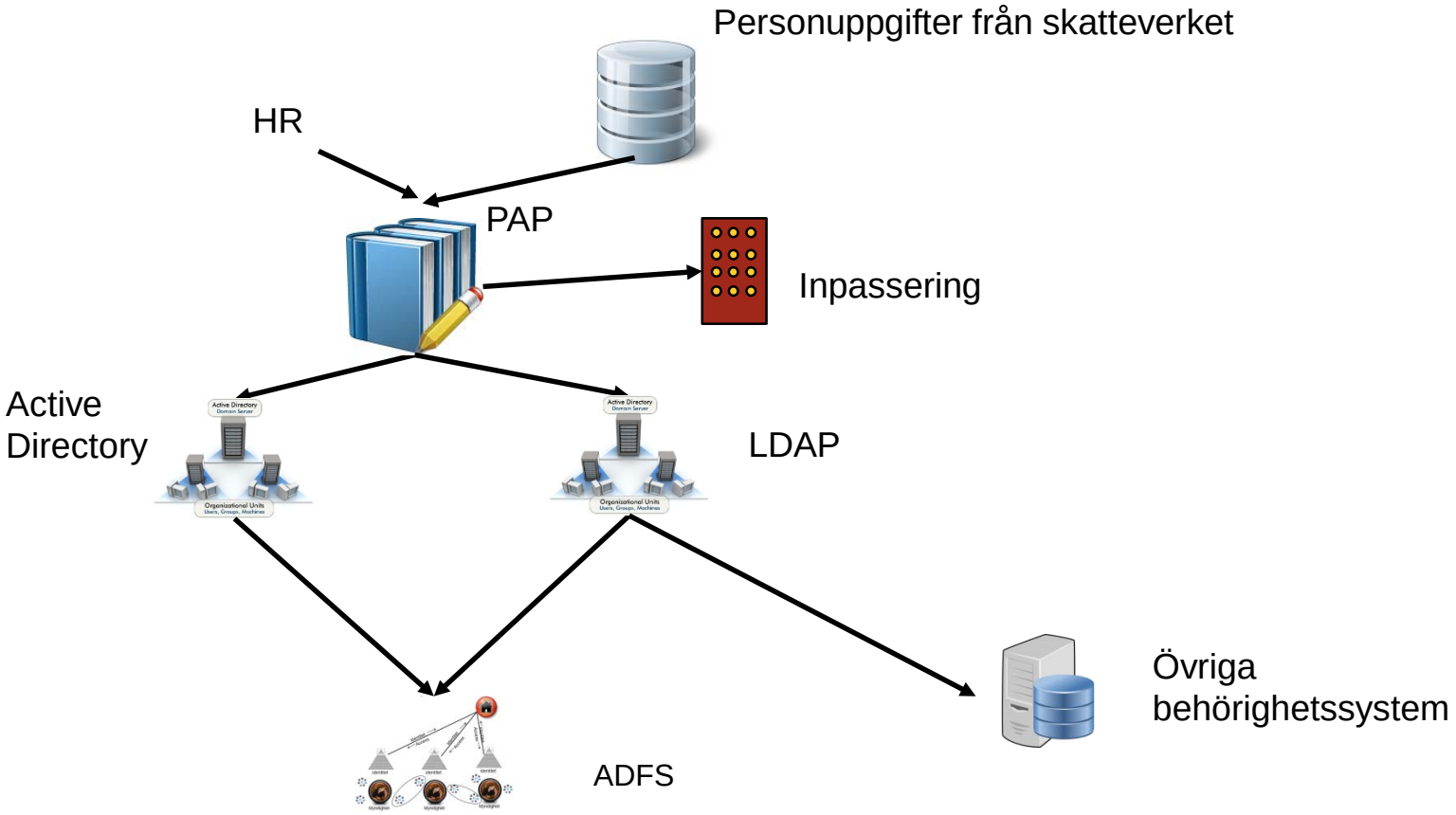
Uppifrån och ner? Eller nerifrån och upp?

Börja uppifrån, med ramverk och samarbetsorganisation

Börja nerifrån, med ett enskilt system

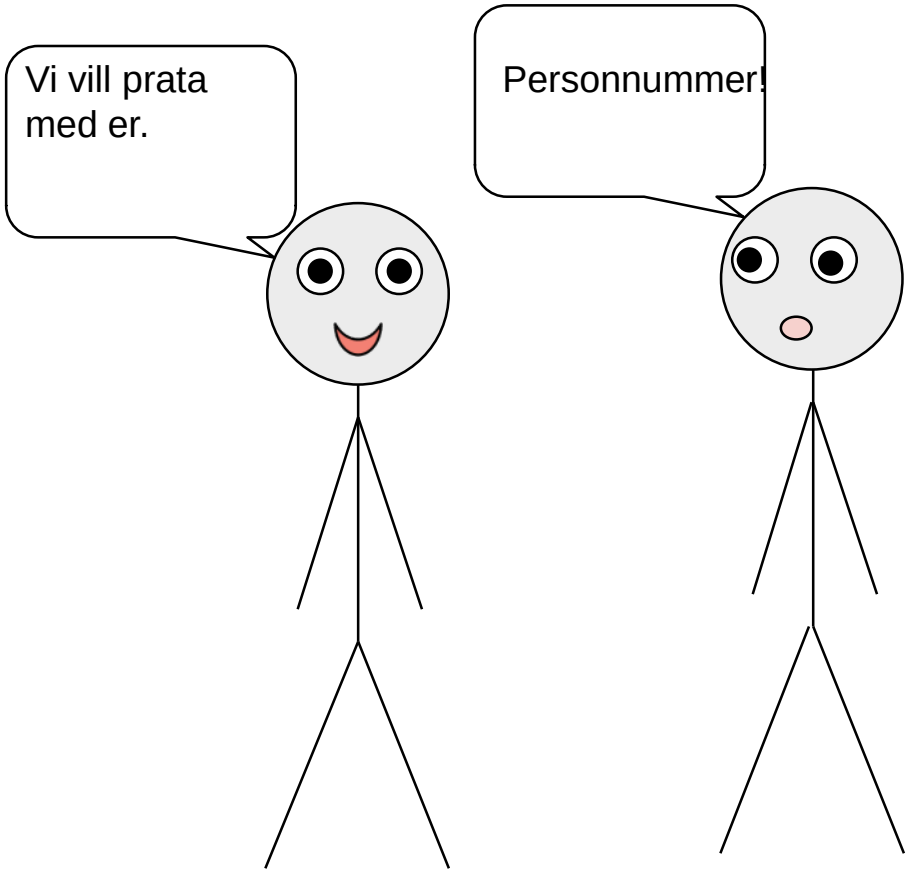
Att nå varandra

Krav på behörighetsadministration

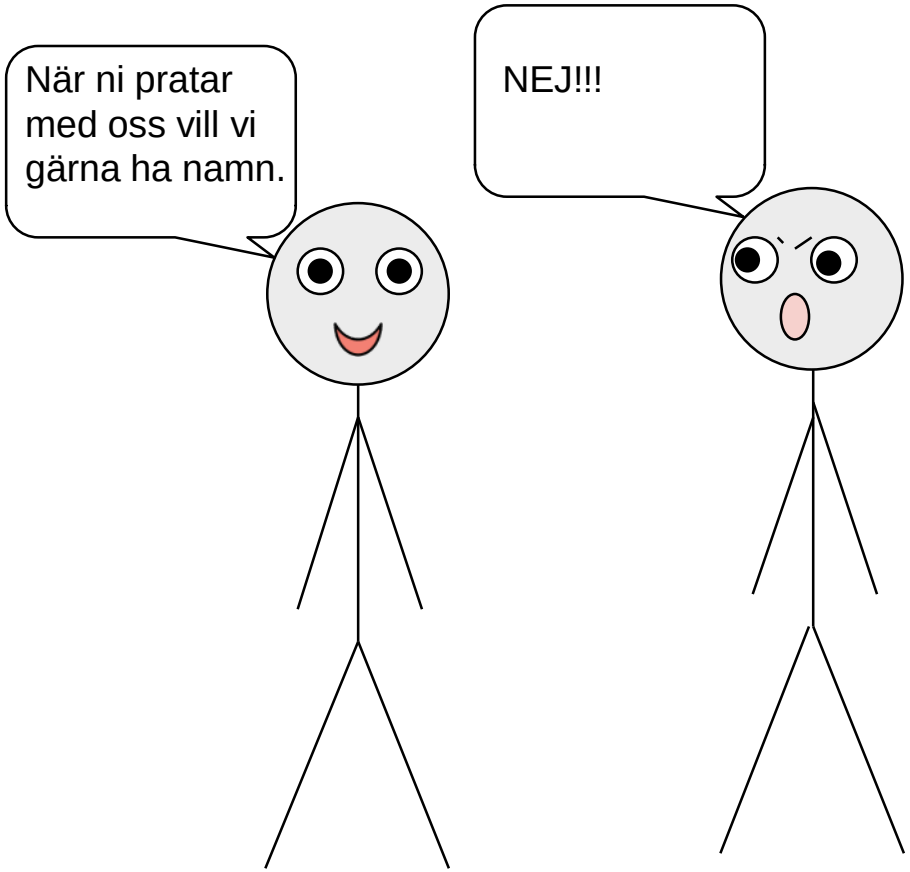


Spårbarhet

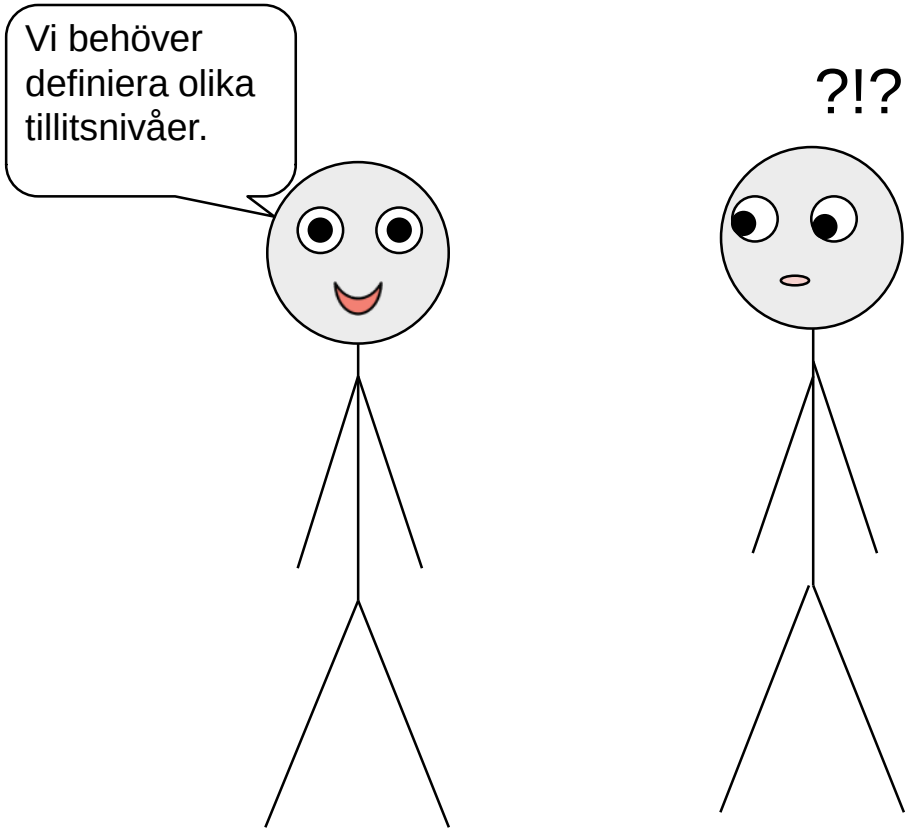
Polisen – en resonlig partner



Polisen – en resonlig partner



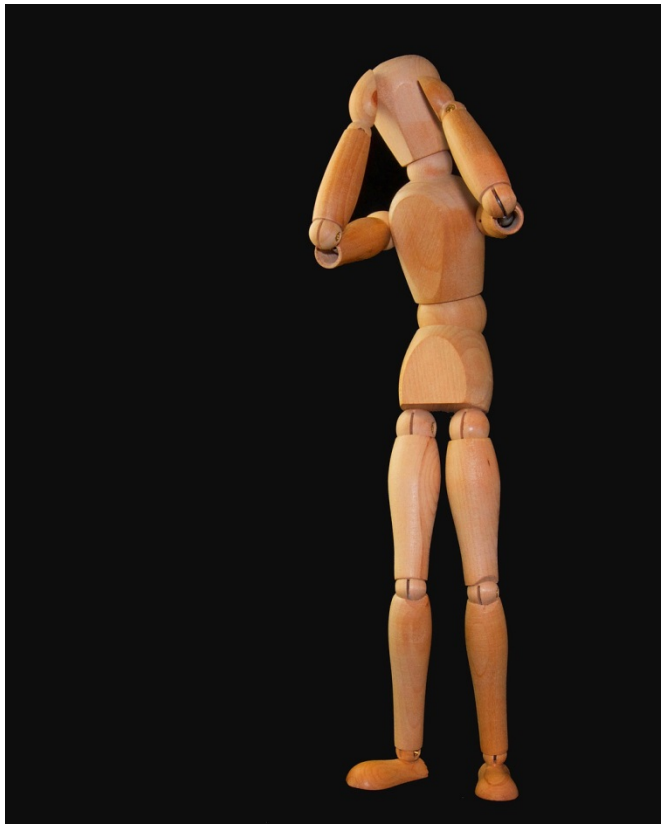
LOA lite högre tack!



Varifrån ska systemet nås?

Polisen

Devices utan kortläsare

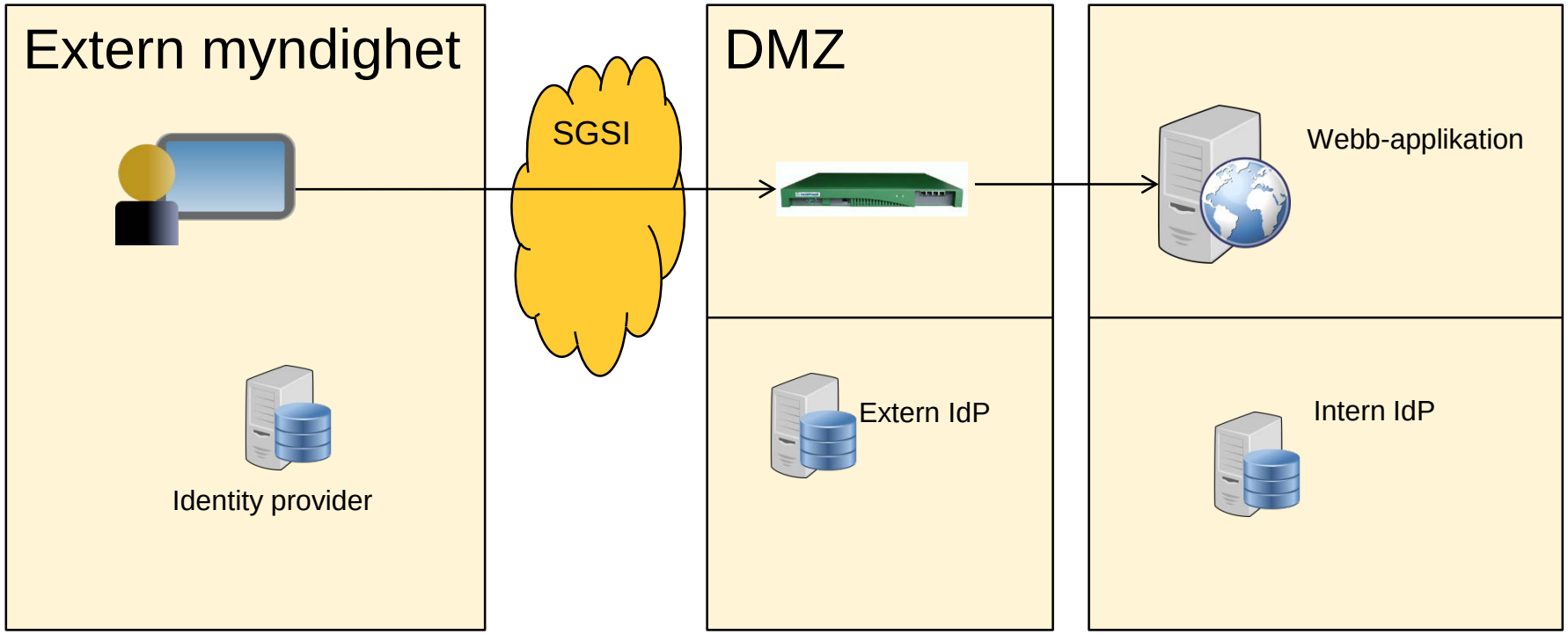


SAML eller OIDC?

- Vi började med SAML.
- Men vi tittar på OIDC.

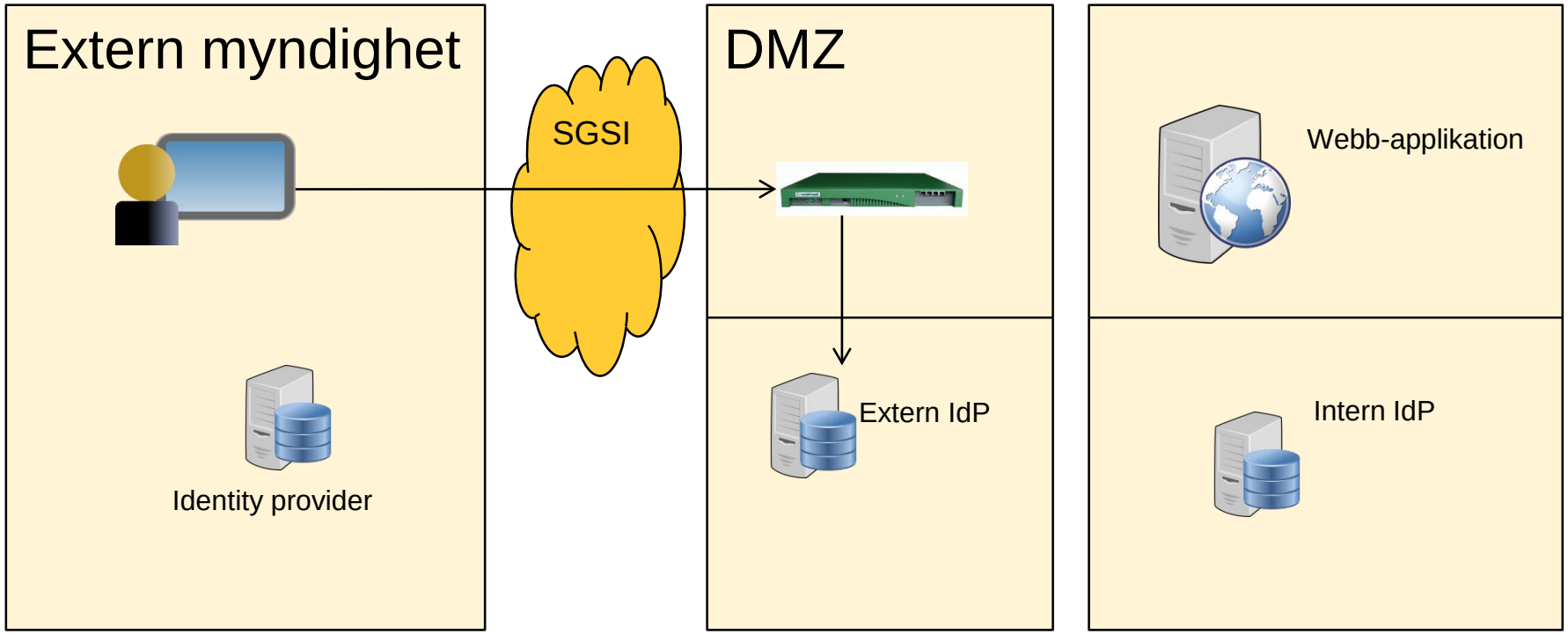
Hur har vi jobbat?

Hur ser det ut rent praktiskt?



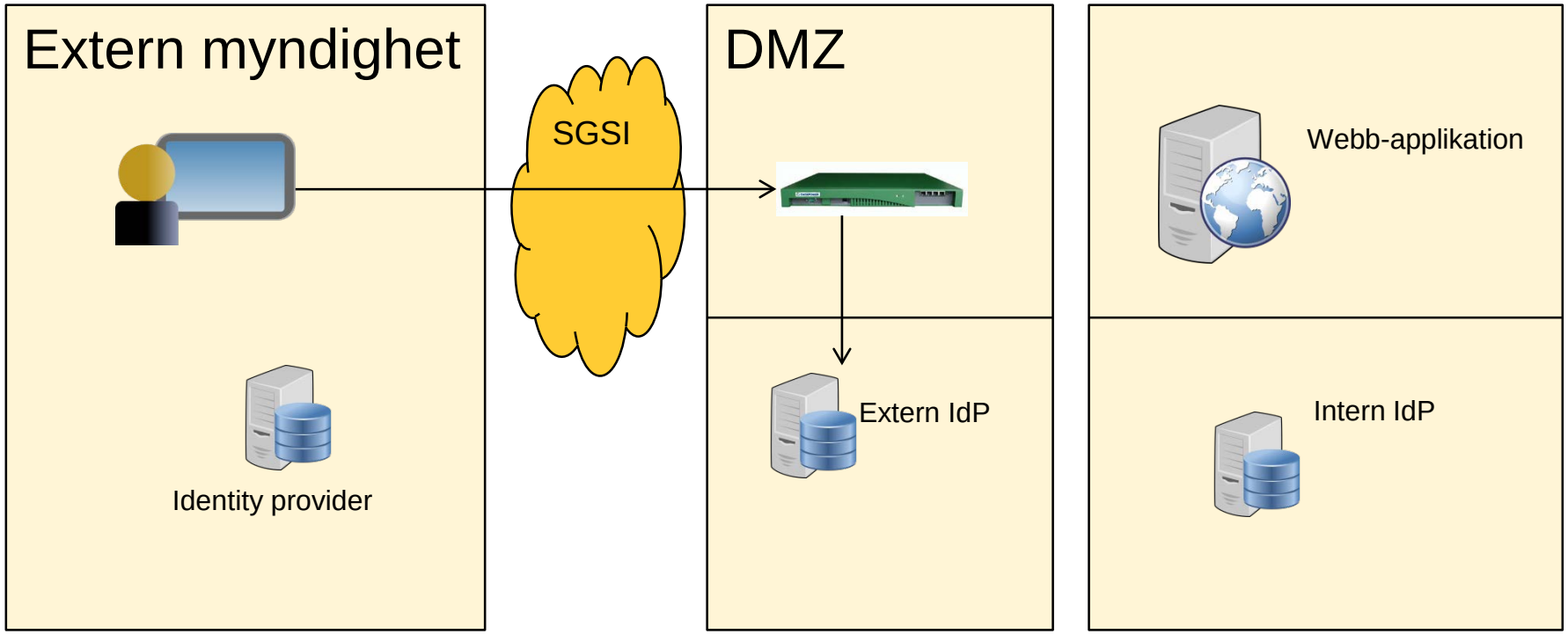
En användare hos en extern myndighet surfat mot vår webbapplikation via webbläsaren. Trafiken går via SGSI.

Hur ser det ut rent praktiskt?



Externa användare skickas till vår externa IdP, som låter användaren välja bland anslutna IdP:er.

Hur ser det ut rent praktiskt?



På vägen tillbaka översätts biljetten i vår externa IdP, för att externa användares biljetter inte ska kunna ha fel behörigheter och för att vi alltid ska veta varifrån användaren kommer.

Sammanfattning

- Då mycket fanns på plats började vi i den lättaste änden
- Samarbete mellan bara två organisationer är svårt.
- Täta avstämningar är en nyckelfaktor

Frågor?

Diskussion

Vilka är likheterna, skillnaderna för federationerna?

Vad är av generellt intresse för alla federationer?

Några viktiga parametrar

- Antal medverkande parter
- Styrande lagar
- Olika syn på vad som ska uppnås, olika framgångsfaktorer
- Utövande av tillsyn
- …

Svenskt federationsforum

Paus

Åter kl 15.30

Tillit i federationer

Pågående arbeten

Diskussion - Hur skapa tillit bland federationens medlemmar?

Björn Hesthamar, Post- och telestyrelsen

TILLITSMODELLEN FÖR BETRODDA TJÄNSTER ENLIGT EIDAS

Tillitsmodellen för betrodda tjänster enligt eIDAS

Björn Hesthamar
Nätsäkerhetsavdelningen

Dagens glosor

- eIDAS
- Betrodd tjänst
  - Kvalificerad
  - Icke-kvalificerad
- Trusted List
- Tillitsmodell

https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

eID AS

Gränsöverskridande erkännande av elektronisk identifiering

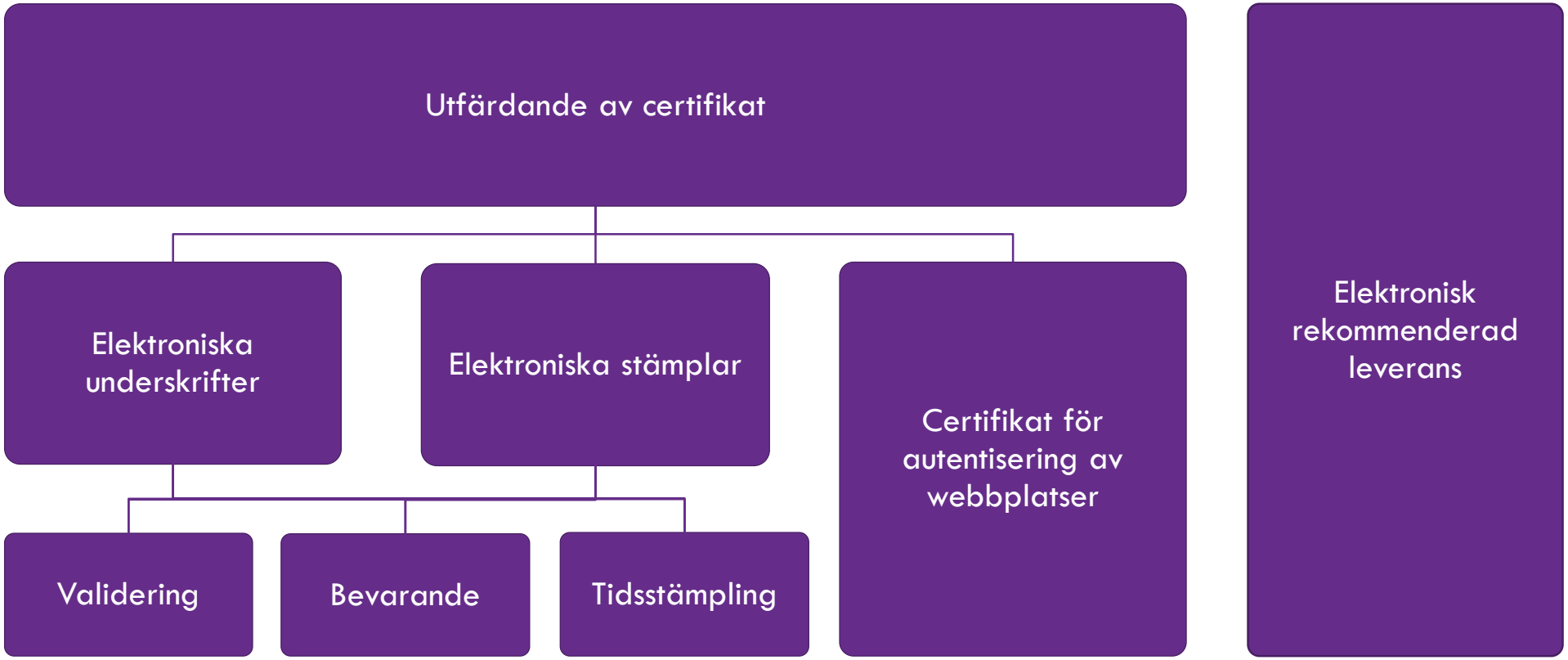
Betrodda tjänster för elektroniska transaktioner på den inre marknaden

EUs förordning 910/2014

E-LEGITIMATIONS NÄMNDEN

PTS

Vilka betrodda tjänster?



Dessa tjänster kan valideras med hjälp av trusted list.

Två olika tillitsnivåer av betrodda tjänster

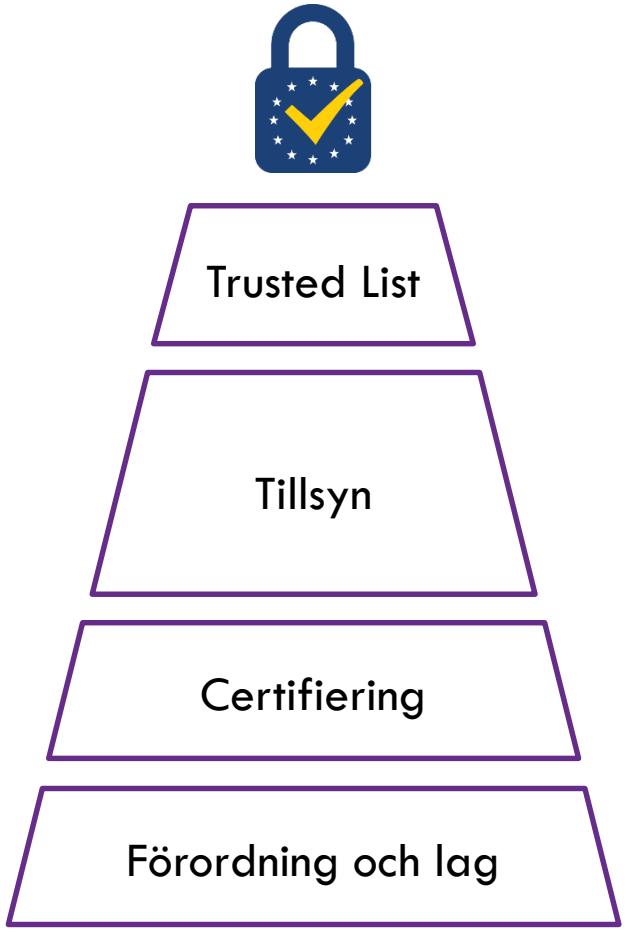
	Icke-kvalificerade	Kvalificerade
Anmälning	Ingen anmälningsplikt	Anmälningsplikt
Säkerhetskrav	”vidta lämpliga säkerhetsåtgärder med hänsyn till teknik och kostnad”	Detaljerade säkerhetskrav på policy, process och rutin. Återkommande krav på överenstämmelsesbedömning hos ackrediterat organ.
Skadestånd	Ja, bevisbörda på drabbad part	Ja, bevisbörda på tillhandahållare. Finansiell förmåga att bära sin risk.
Incidentrapportering	Ja	Ja
Tillsyn	Händelsestyrd efter inträffande	Årlig, planlagd och händelsestyrd
Juridisk verkan	Får inte diskrimineras enbart för att den har elektronisk form och erkänns på samma villkor i alla medlemsstater	Har motsvarande rättslig verkan som en icke-kvalificerad tjänst, men med en högre tillitsnivå och erkänns på samma villkor i alla medlemsstater

Ett sätt att se på tillit

As humans, we find ways
to lower uncertainty about one another,
so that we can exchange value.

Bettina Warburg

Vad ger tillit för en kvalificerad betrodd tjänst?



Trusted List

Förmedlar aktuell teknisk och juridisk status i ett maskinläsbart format

Tillsyn

Tillhandahållare står under årlig tillsyn

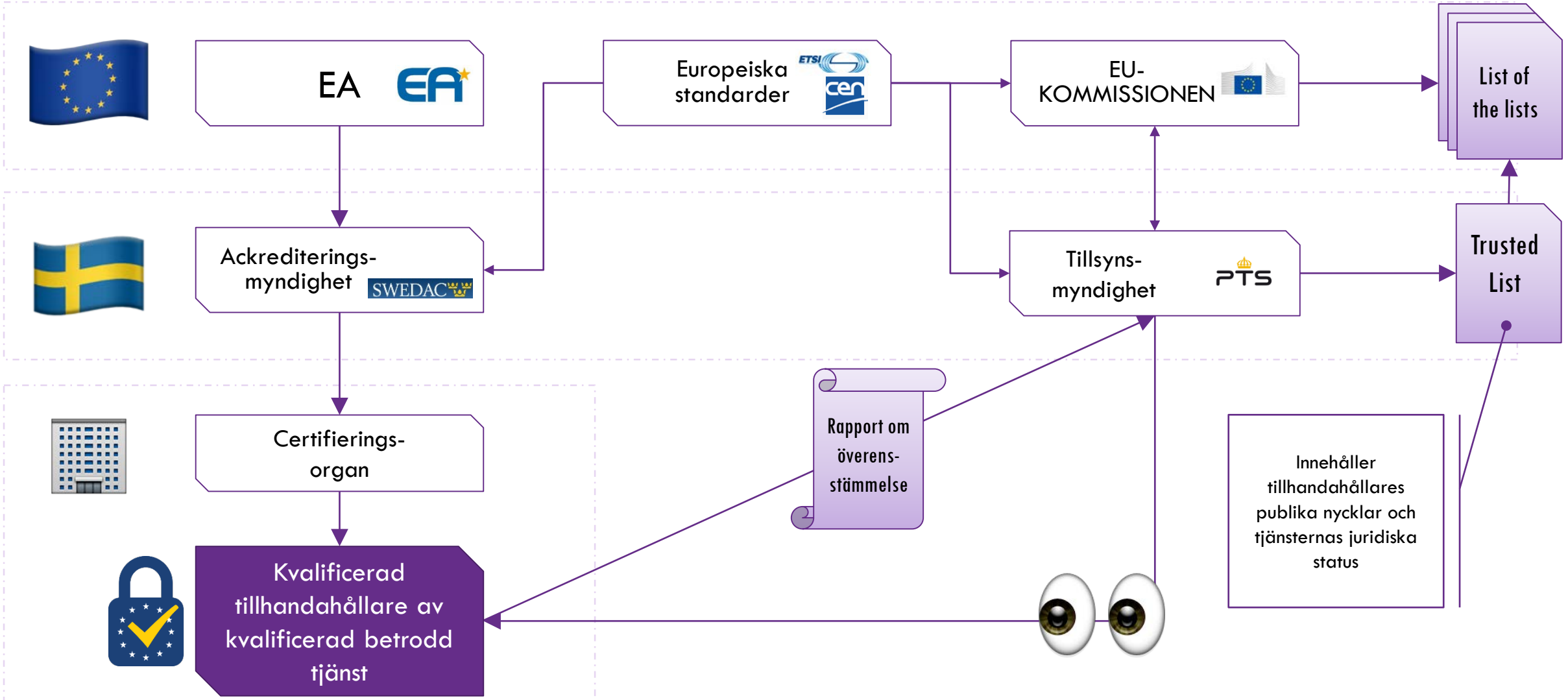
- Planlagd
- Händelsestyrd

Lärande organisation

Certifiering

- IT-produkter (HSM-modul etc.)
- Bedömning av överensstämmelse

Tillitsmodell för kvalificerade betrodda tjänster



Sammanfattning

- eIDAS är tvådelat, eID och betrodda tjänster
- Det finns två nivåer av betrodda tjänster
  - Icke-kvalificerade
  - Kvalificerade
- Kvalificerade tillhandahållare och tjänster står under mer omfattande tillsyn med klar ansvarsfördelning mellan olika organ.
- Tjänster får inte diskrimineras för att de är elektroniska
- Trusted List förmedlar alltid status

För mer information om betrodda tjänster

http://pts.se/eidas

- Faktablad för tillhandahållare
- Vägledning för betrodda tjänster i Sverige enligt eIDAS

http://trustedlist.pts.se/

- Sveriges nationella förteckning över kvalificerade tillhandahållare och kvalificerade betrodda tjänster

Tack för uppmärksamheten!

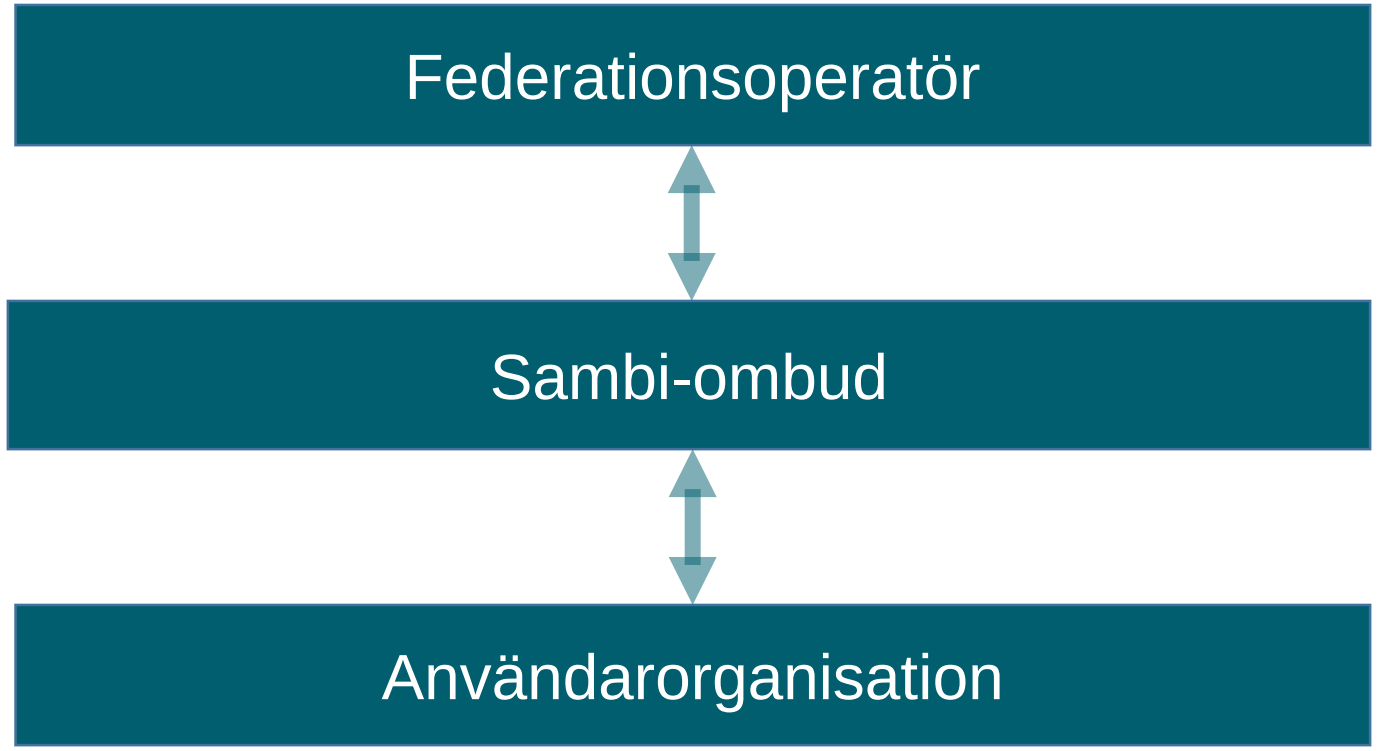
Frågor?

Granskning av medlemmar anslutna via ombud

Staffan Hagnell, IIS

2016-11-21

Sambi-ombud?



Kravställning

Säkerhetskraven måste vara pragmatiska. T.ex. en liten kommun eller vårdgivare har inte möjlighet att själv kontroll sin tekniska lösning. Men centralt för Sambi är:

- Det ska alltid framgår vilken organisation som en individ representerar även när ombud används.
- En användarorganisation ska alltid ha ett eget avtal med federationen.
- Om ett ombud inte sköter sig ska det kunna hanteras.
- En användarorganisation ska fortsatt ha ett tydligt ansvar för sina identiteter och behörighetsstyrande attribut.

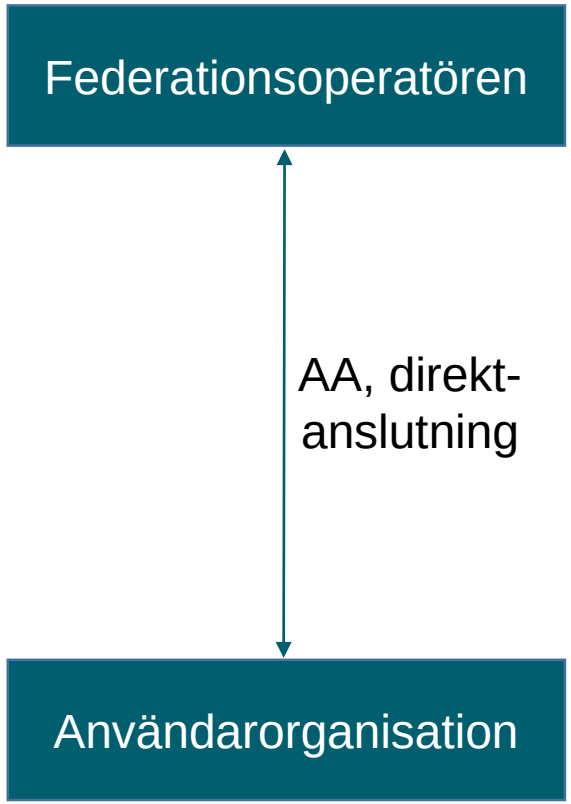
Att göra

Nya anslutningsavtal för

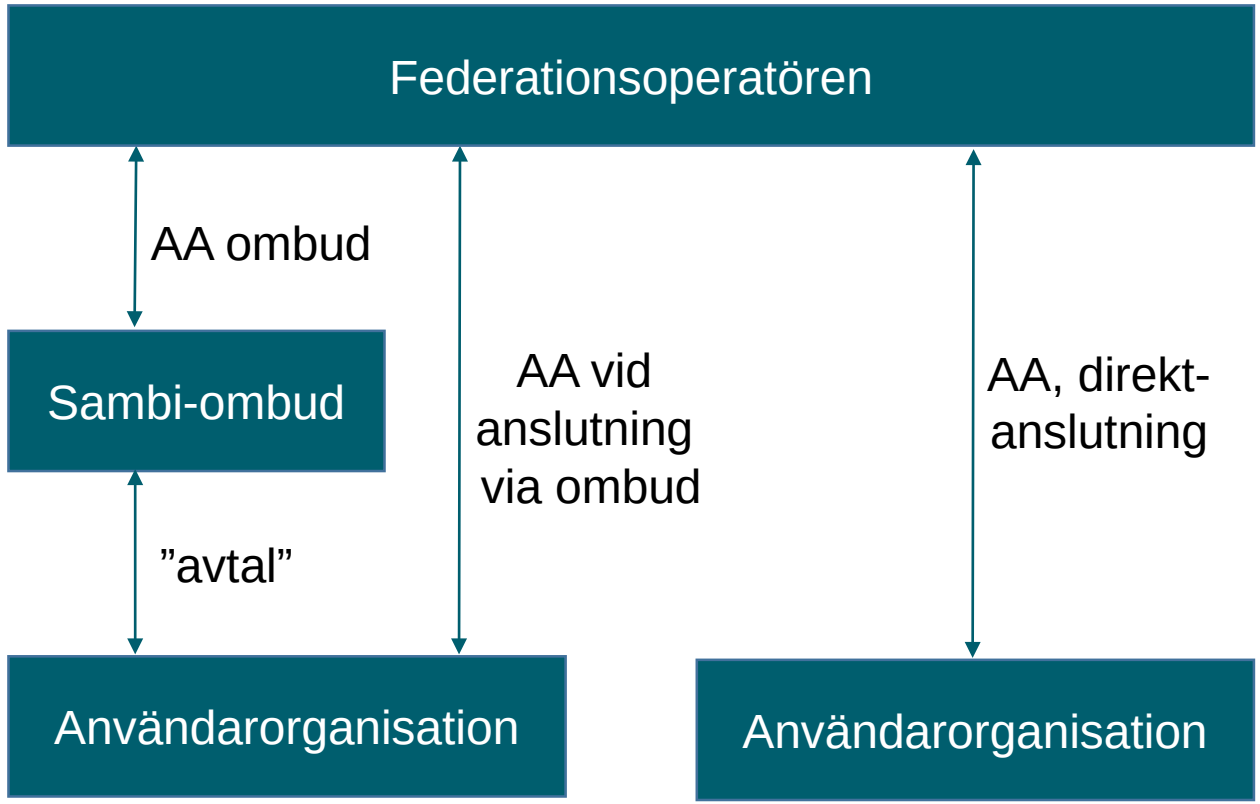
- Användarorganisation ansluten via Sambi-ombud
- Sambi-ombud

Vidareutveckla Tillitsgranskningstjänsten

Olika Anslutningsavtal (AA)



Olika Anslutningsavtal (AA)



Hur anpassa Sambis Tillitsgranskning?

BILAGA 3 – Tillitsramverk

Version: 1.3.1

Innehåll

Allmänt 2

1) **A. Generella krav** 2

Övergripande krav på verksamheten 2

Säkerhetsarbete 3

Granskning och uppföljning 3

Kryptografisk säkerhet 3

Ansvar för användning av Leverantörer 4

Handlingars bevarande 4

Information 4

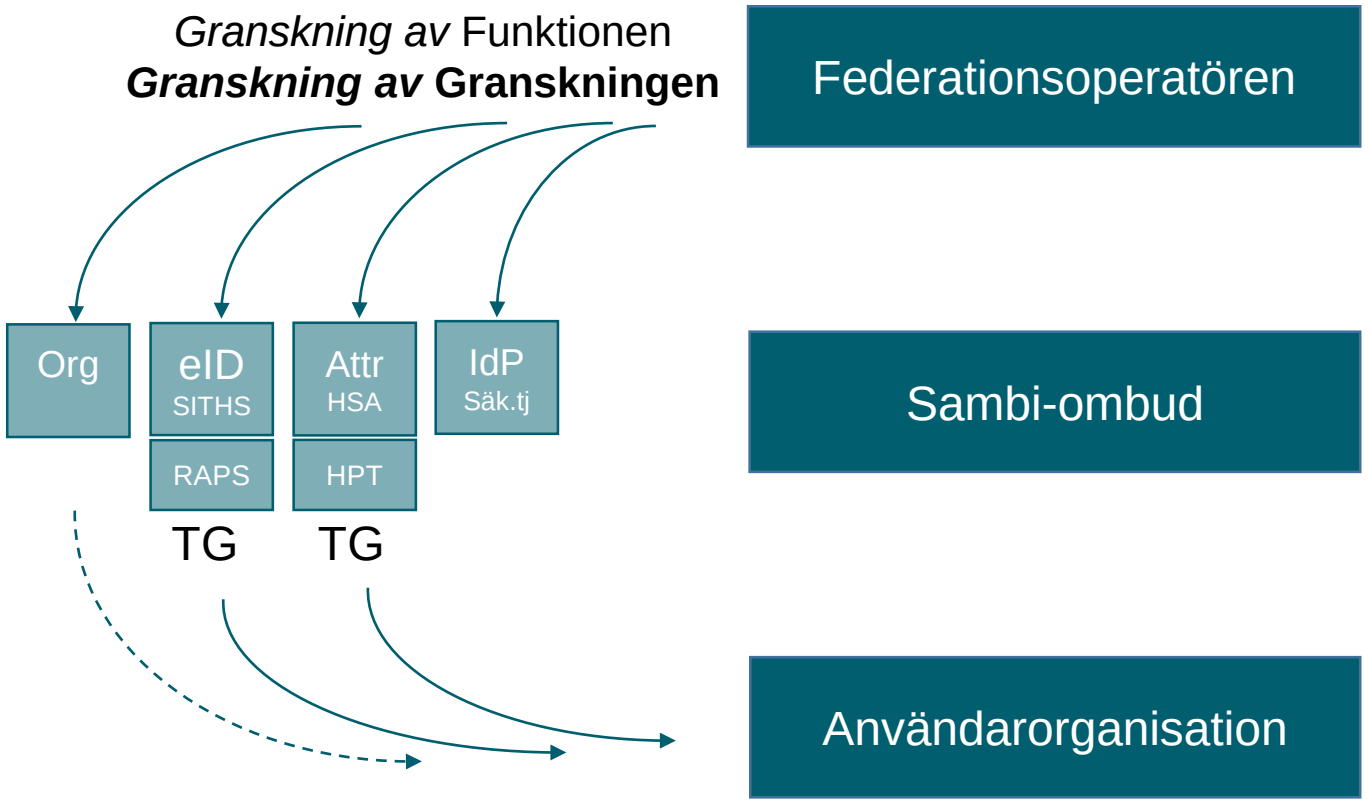
2) **B. E-legitimationsutfärdare** 5

3) **C. Attribututgivare** 5

4) **D. Identitetsintygsutgivare** 5

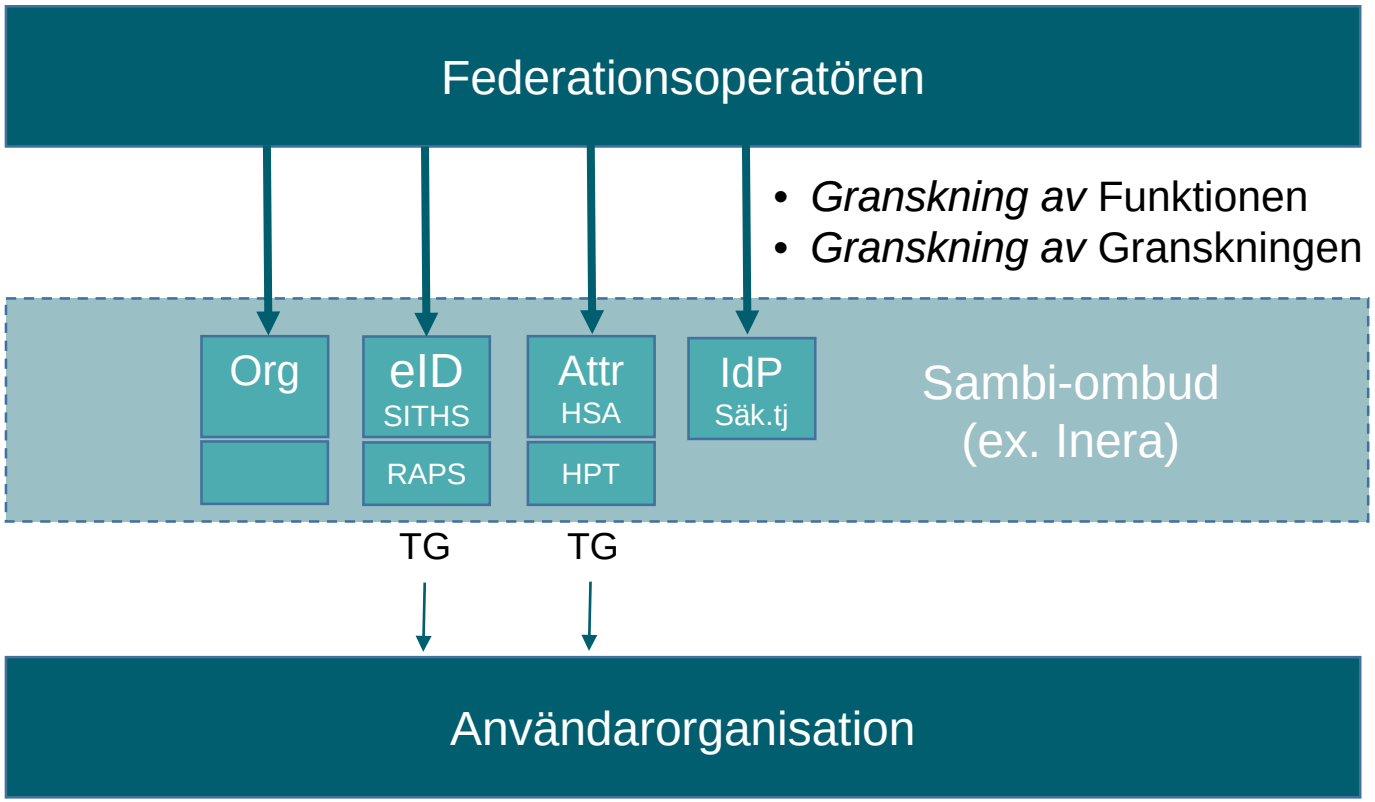
E. Tjänsteleverantör 6

De 4 olika ”delarna” granskas idag separat



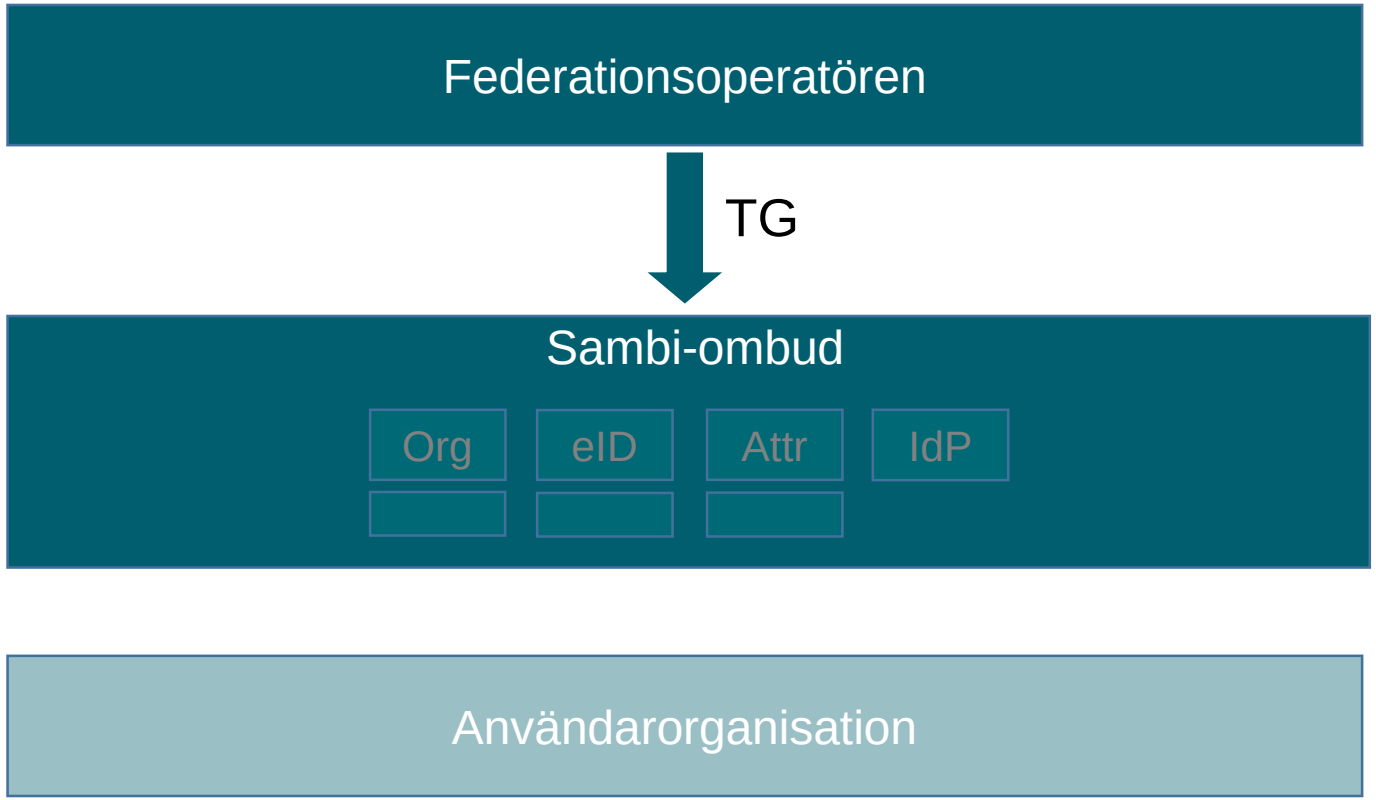
TG: Tillitsgranskning

Ett ombuds tjänst byggs med redan granskade moduler



TG: Tillitsgranskning

…och tillitsgranskning av Sambi-ombudet



Vidareutveckling av Tillitsgranskningstjänsten

1. Hanteringen Tillitsramverkets Generella krav
2. Granskning av Leverantörer som tillhandahåller granskningstjänst
3. Granskning av Sambi-ombud

Hur hantera Tillitsramverkets Generella krav?

- Vad krävs för att vara en ”vårdgivare”?
  - Samordning med kommande centrala register över vårdgivare?
  - Hur kan ett ombud utföra denna granskning i väntan på att centralt register över vårdgivare finns?

Hur granska Leverantör som tillhandahåller granskningstjänst?

- Vägledning finns i ISO/IEC 27007 (guideline for auditing information security management systems)!

Granskning av ombud

1. Fastställ kraven som ska ställas på ett ombud
2. Tag fram en granskningstjänst för granskning av ombud

Förslag till lösning

ska presenteras i februari 2017

Pål Axelsson, Swamid

STATUS FÖR SWAMID GRANSKNING AV AL1 OCH AL2

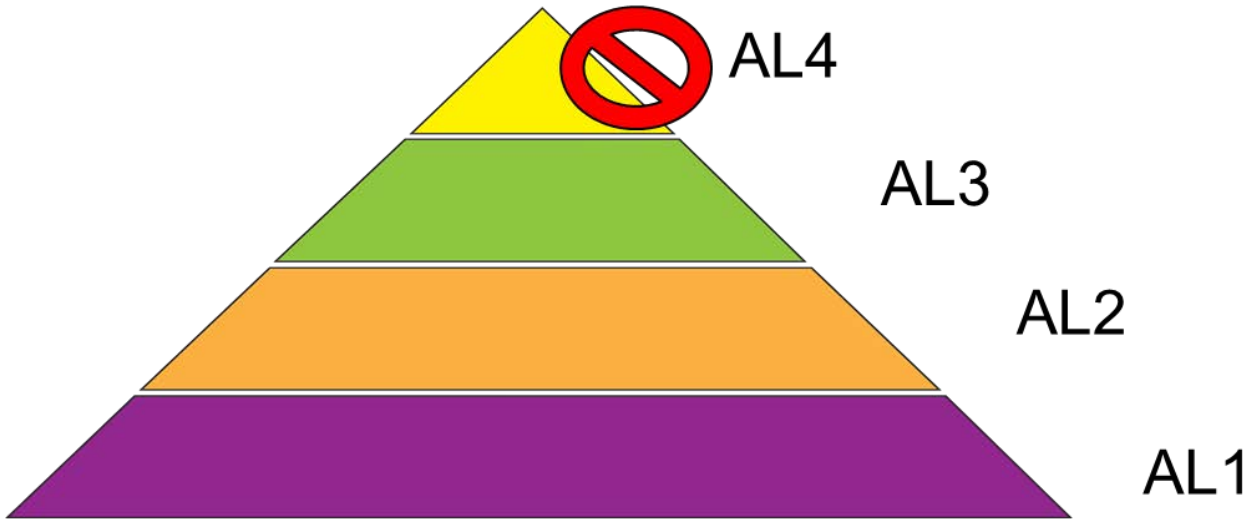

SWAMID
Swedish Academic Identity Federation

Varför tillitsprofiler i SWAMID

- SWAMID är en sektorsfederation med 57 medlemsorganisationer inom högre utbildning och forskning i Sverige
- Det har funnits en tilltro bland lärosätena om att andra lärosäten gör ungefär som vi själva när det gäller kontohantering men det har i själva verket funnits en stor variation
  - Exempel på spridning för kontoaktivering: Kraven har varierat mellan att några lärosäten har skicka ut ett e-post med användaridentitet och lösenord till den e-postadress som studenterna använt vid ansökan till att studenterna vid några lärosäten har varit tvungna att vissa legitimation för kontohandläggare för att få tillgång till sitt studentkonto.
- Med utökad mängd sektorsgemensamma system behövs gemensam tillit

SWAMID

Tillitspyramiden för användare



***AL4:** Går ej att använda i federation!*

AL3: Vet mycket väl vem personen är *(verifierad)*. Personen har uppvisat legitimation och personuppgifter är delvis hämtade från annan källa.

- Exempel: Svensk E-legitimation

AL2: Vet vem personen är *(bekräftad)*. Uppgifterna är delvis hämtade från annan källa.

- Exempel: Universitet eller högskola

AL1: Vet att det är en person *(obekräftad)*. Personuppgifterna är självuppgivna.

- Exempel: Facebook och Google

SUNET

21 medlemmar uppfyller idag SWAMID AL1

SWAMID

SWAMID Identity **A**ssurance **L**evel **1** Profile

Tillitsprofilen SWAMID AL1 innebär:

- att det är en person som innehar och använder kontot (obekräftad användare)
- att informationen knuten till kontot ofta är uppgiven av och ansvaras för av användaren själv
- att medlemsorganisationens identitetshanteringssystem uppfyller minst kraven i SWAMID AL1 och visar detta genom en Identity Management Practice Statement (IMPS)
- att granskning sker genom årlig egenkontroll

SUNET

https://www.swamid.se/policy/assurance/al1/

7 medlemmar uppfyller idag SWAMID AL2

SWAMID

SWAMID Identity **A**ssurance **L**evel **2** Profile

Tillitsprofilen SWAMID AL2 innebär:

- att lärosätet vet vem personen är som innehar och använder kontot (bekräftad användare)
- att lärosätet ansvarar för personinformationen
- att det finns högre krav på inloggningssäkerhet än i SWAMID AL1
- att SWAMID granskar att IMPS uppfyller kraven i SWAMID AL2
- att SWAMID genomför årlig kontroll av att IMPS fortfarande gäller
- i övrigt en utökning av SWAMID AL1 med några få tilläggskrav

SUNET

https://www.swamid.se/policy/assurance/al2/

SWAMID

Utmaningar för medlemsorganisationerna

- Medlemmarna har aldrig skrivit något liknande en Identity Management Practice Statement (IMPS)
- En del lärosäten har rationaliserat bort användarreglerna och säger istället bara att användarna ska följa svensk lag
- Att göra utländska distansstuderande till bekräftade användare är inte helt enkelt
  - Lösningen är att tillåt att användare kan vara antingen bekräftade eller obekräftade
- Lösenordsåterställning är svårt att få till på ett tillräckligt säkert sätt
  - Microsofts lösenordsåterställning via Microsoft Identity Manager (tidigare FIM) och en webbsida är inte tillräckligt bra för SWAMID AL2

Mer information…

- Allmänt om SWAMIDs federationspolicy
  - https://www.sunet.se/swamid/policy/
- Praktisk hjälp till SWAMIDs medlemmar gällande tillitsprofiler
  - https://wiki.swamid.se/display/SWAMID/SWAMID+Identity+Assurance
- Kontakta SWAMID
  - https://www.sunet.se/swamid/kontakt/

Diskussion

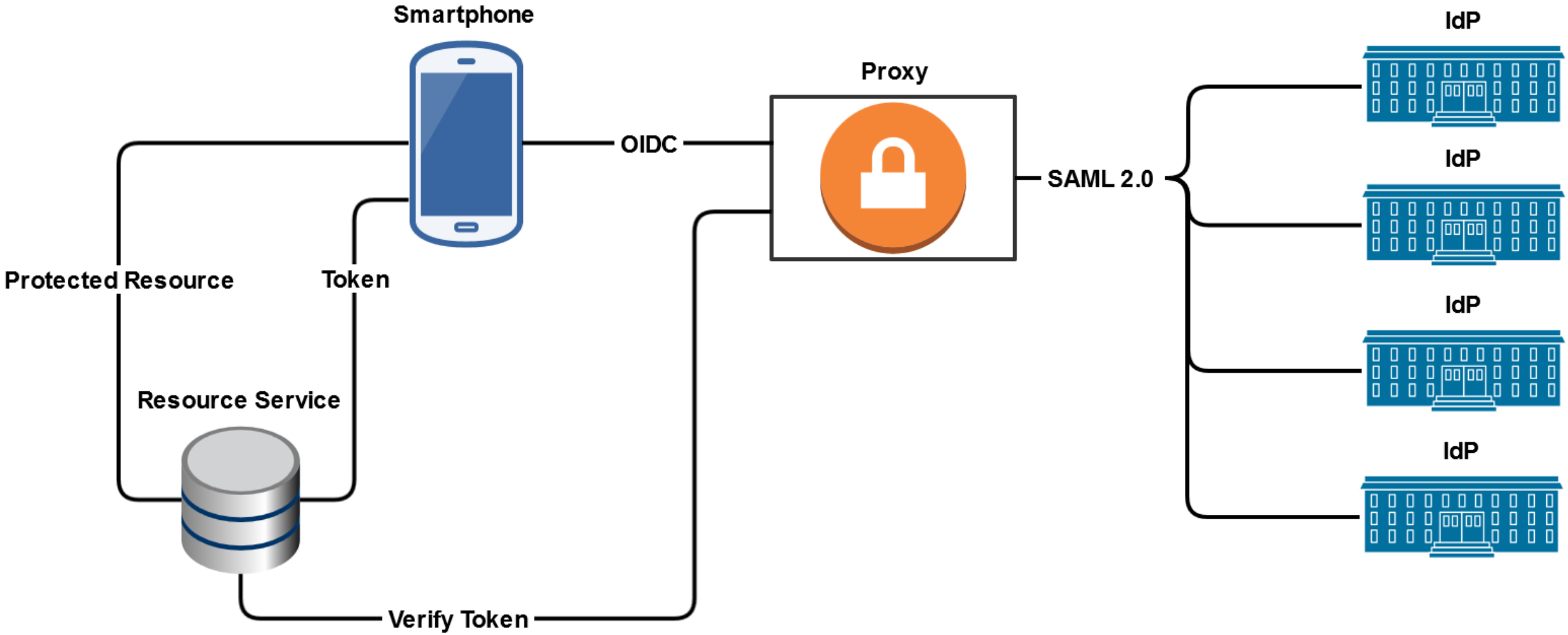
- Ändras en federation behovet av tillit mellan parterna?
- Hur bör tillsyn ske av medlemmarna i en federation?
- Vad kan göras för att vidareutveckla säkerheten i federation?

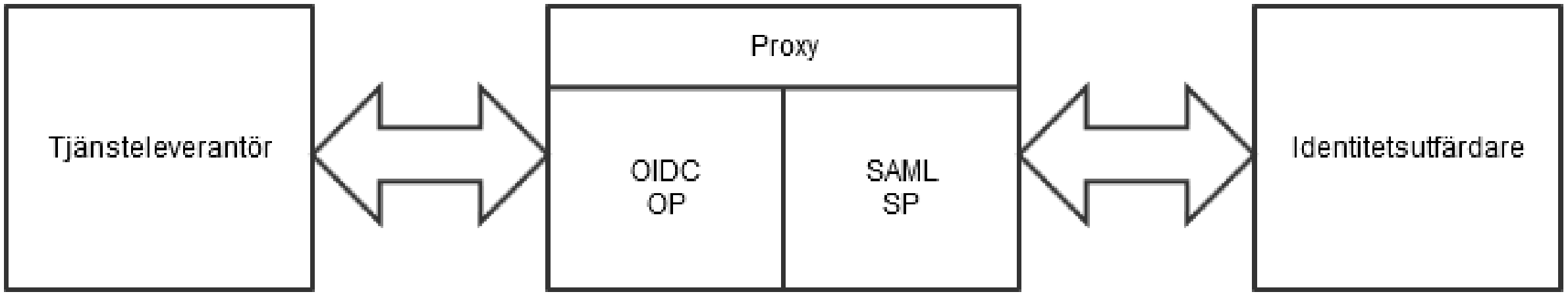
plan för fortsatt arbete

FRÅGOR AV GEMENSAMT INTRESSE

Stefan Halen

HANTERING AV APPAR


Smartphone
OIDC
Proxy
SAML 2.0
IdP
IdP
IdP
IdP
Protected Resource
Token
Resource Service
Verify Token


Tjänsteleverantör
Proxy
OIDC
OP
SAML
SP
Identitetsutfärdare

Utvecklingsfrågor från tidigare möte	Utveckling
En POC för federativ hantering av appinloggning och IoT	En OIDC/SAML-gateway har utvecklats och tester kan nu startas.
Gemensamma federerade infrastrukturtjänster	Arbete pågår för att utveckla Sunets erbjudande
Säkerhetskrav och tillitsarbeten	Pågående arbeten behandlades under dagen
Samordnad kravställning på de stora molntjänsternas federativa anpassning	Kontakter med Google, men önskemålet är eduGAIN tar frågan med att finna en gemensam lösning
Entitetskategorier	Har implementerats och används av Swamid
Livscykelhantering av användare	SIS/TK450 har påbörjat ett standardiseringsarbete för Skolfederation
Standardisering	Ett samordnat standardiseringsarbete diskuterades inte
Anvisningstjänst	Behovet diskuterats inte vidare
Nyckelhantering och krypto	Behovet diskuterats inte vidare
Onbording för användarutrustning	Behovet diskuterats inte vidare
Test och testverktyg	Arbete bedrivs av Roland Hedberg

Några frågor av gemensamt intresse för fortsatt arbete

- OIDC/SAML GW – Hitta lämplig pilot
- Stöd för federationer i MS ADFS
- Lärdomar från CERN Certified – Uppföljning vid ID-kapning
- Gemensamt metadataregister hos E-legitimationsnämnden
- Sammanställning och översikt över alla federationer
- Mobila klienter
- Resultatet av SIS/TK450:s arbete med livscykelhantering
- Behörighetsmodeller

Former för fortsatt arbete

- Skapa ett samarbetsforum eller mejllista för löpande utvecklingsfrågor
- Fortsatt 1 till 2 möten per år

Svenskt federationsforum

Tack för idag och på återseende!