INTERNET STIFTELSEN

Målbild för en teknisk implementation och vinster med standarder

14/6 2023

Rasmus Larsson
rasmus.larsson@internetstiftelsen.se

Vad är en federation?

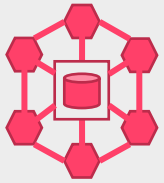
En sammanslutning av organisationer med mål att enas om **identitets- och behörighetsrelaterade frågor**

I Skolfederation handlar det om samverkan avseende:

Regler

Standard

Infrastruktur



Syftet är att underlätta svensk utbildningssektors användning av digitala tjänster och läromedel

Skolfederation

På förra seminariet pratade vi Skolfederation och standarder utifrån ett personuppgiftshanterings-/GDPR-perspektiv

På seminariet presenterades ett implementationsförslag som värnade om den personliga integriteten samtidigt som den är lättare att administrera och kravställa, utifrån standarder

Nu tänkte jag repetera och utveckla lite tankar ur ett tekniskt perspektiv, och ge ett försök att se det långsiktiga resultatet i federationen

Skolfederation

Skolfederation är en **infrastruktur** för skolan baserat på öppna standarder.

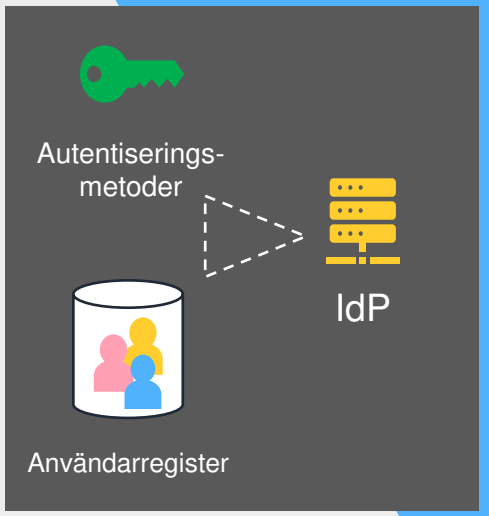
Skolfederation är inte en centraliserad lösning.

Vad betyder det?

Skolfederation

Skolhuvudmannen/skolan tillhandahåller de system och komponenter som krävs för medverkan i en federation.

För att exempelvis inloggning i en federation ska fungera krävs en inloggningslösning, **IdP**, som kan logga in användare med hjälp av **autentiseringsmetoder,** ex användarnamn och lösenord, e-legitimation, och så vidare.



Denna **IdP** måste vara kopplad mot ett **användarregister** där de uppgifter som tjänsterna kräver för inloggningen måste finnas.

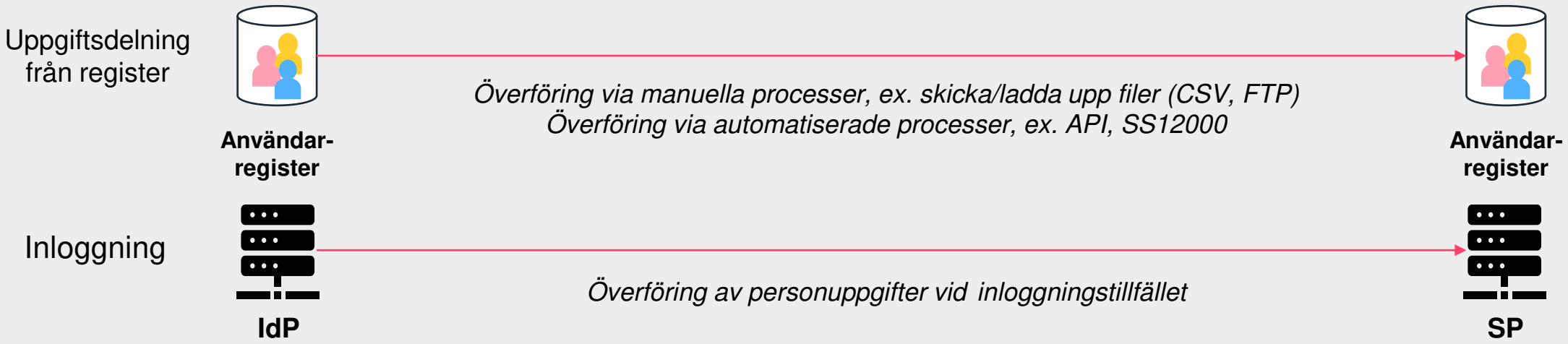
Skolfederation

När var organisation lägger sitt ”pussel” av digitala lösningar blir resultatet ofta annorlunda

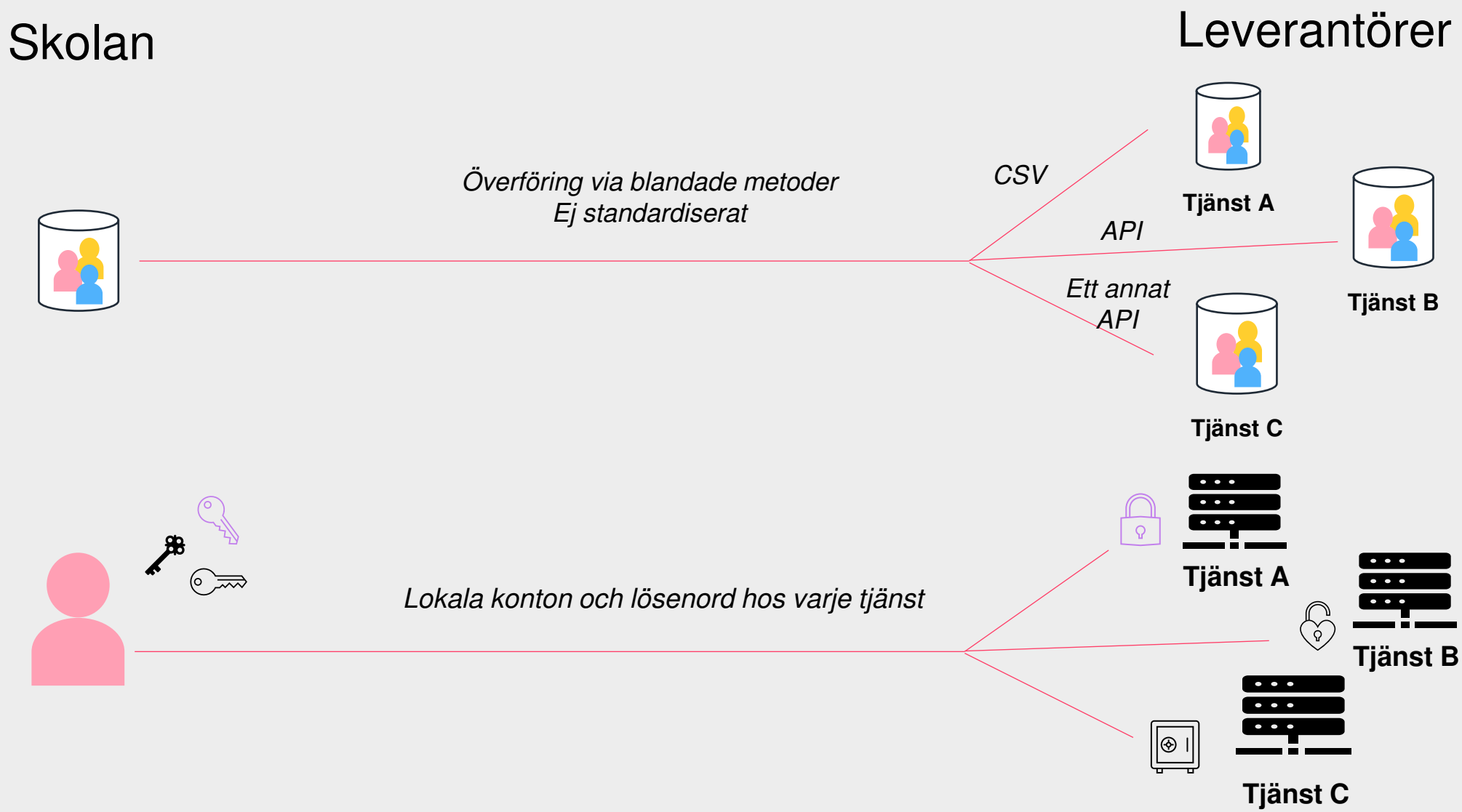
Det finns standard idag, finns det etablerad god praxis?

Går den att formalisera? Vem gör det?

Typiska (person)uppgiftsflöden från skola till leverantör



Vad vi försöker gå ifrån:



INTERNETSTIFTELSEN

Problem

- Flera tjänster – flera lösenord
- Höga säkerhetskrav ställs på leverantör i hantering av säkerhetsgränssnitt
  - Inloggning
  - Lagring av inloggningsuppgifter
  - Gränssnitt för överföring av personuppgifter
- Svårare administration av personuppgifter för skolan
  - Exempelvis när elev/personal slutar, eller byter klass/skola, eller ändrar andra personuppgifter, måste denna förändring inom rimlig tid speglas ut i tjänsterna (livscykelhantering)

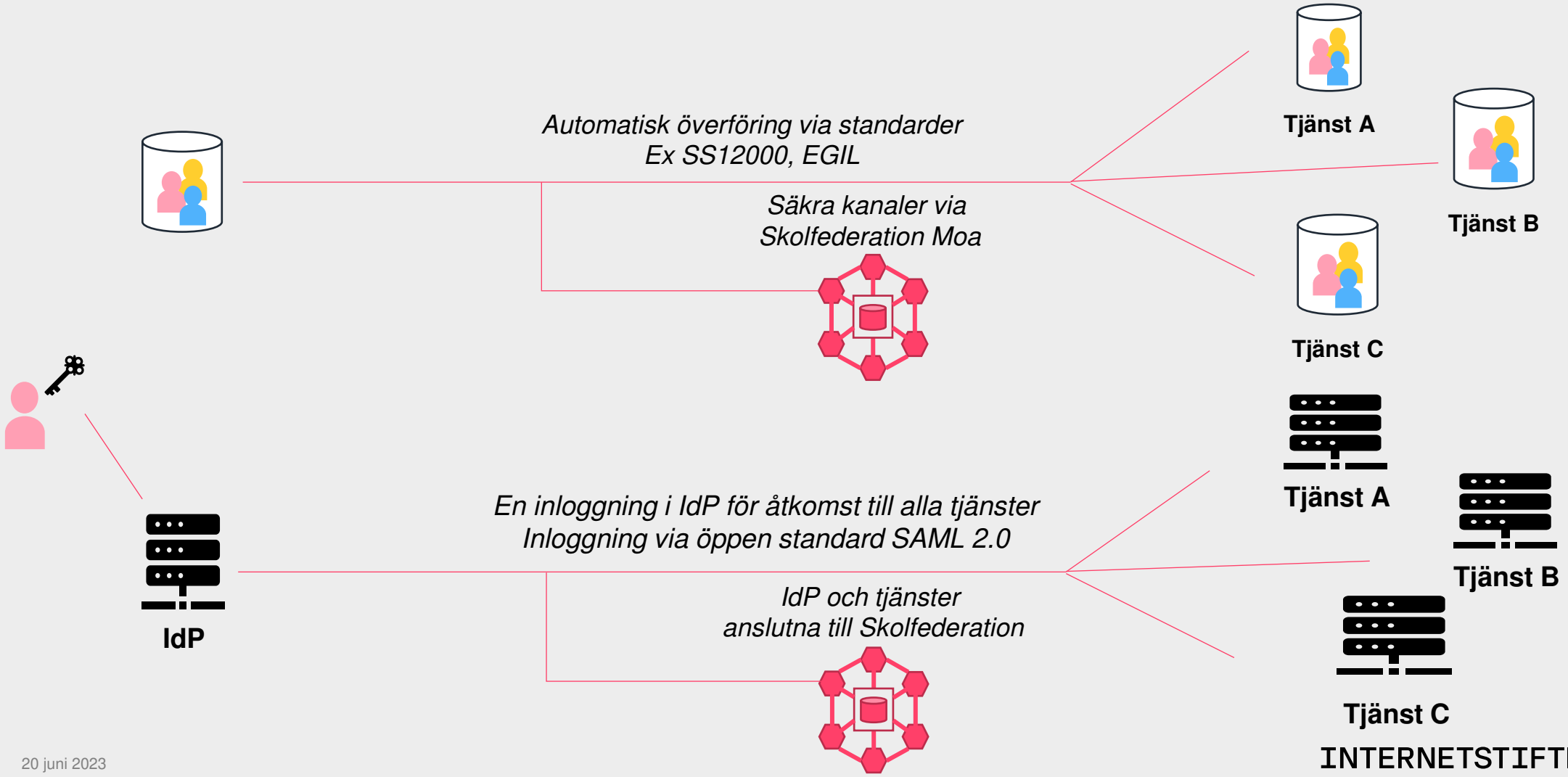
Skolfederation

En bra lösning

Skolan

Överblick

Leverantörer



INTERNETSTIFTELSEN

Skolfederation

En bra lösning

Skolan

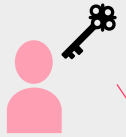
Personuppgiftsflöden

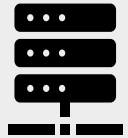
Leverantörer

Personuppgifter skickas via standardiserad provisionering

Namn
Roll
Undervisningsgrupper/klass
Behörigheter
...
ePPN

En pseudonym identifierare, ePPN, skickas
Denna används för att koppla ihop inloggning
med provisionerad användare





IdP

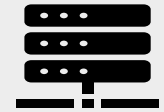
I inloggningen skickas inga personuppgifter

Enbart ePPN

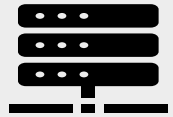
Tjänst A

Tjänst B

Tjänst A



Tjänst B



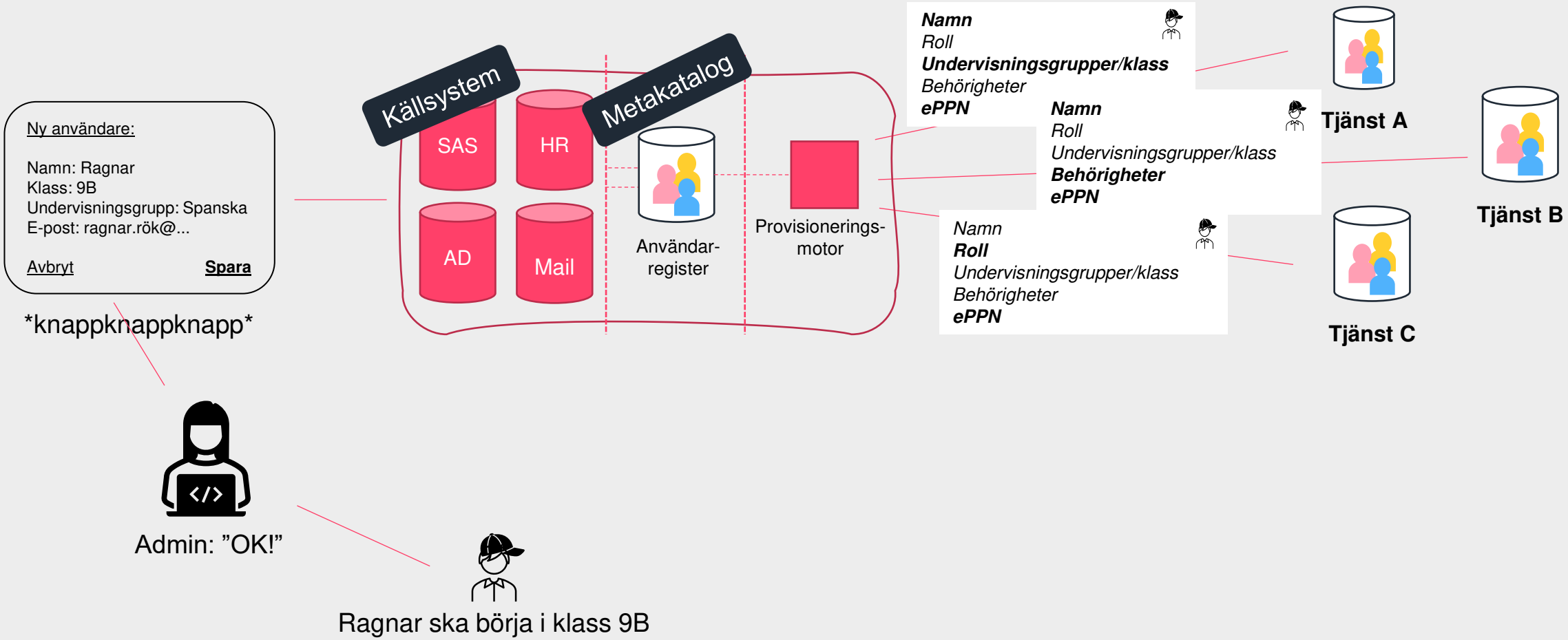
Tjänst C

As made famous by Skolverket

INTERNETSTIFTELSEN

Skolfederation

En bra lösning

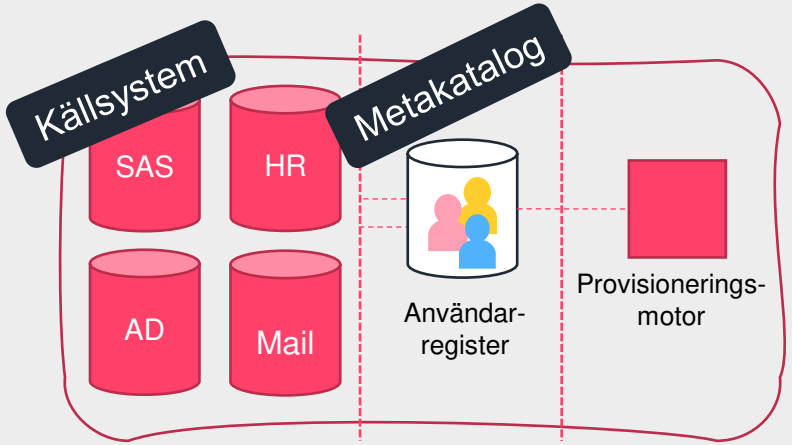


INTERNETSTIFTELSEN

Skolfederation

En bra lösning

Hur en registerlösning kan se ut hos skolan kan variera och delas i olika bitar



Det kan vara separata system:
Provisioneringsmotorn är kopplad till ett användarregister (”metakatalog”), som föds av källsystemen.

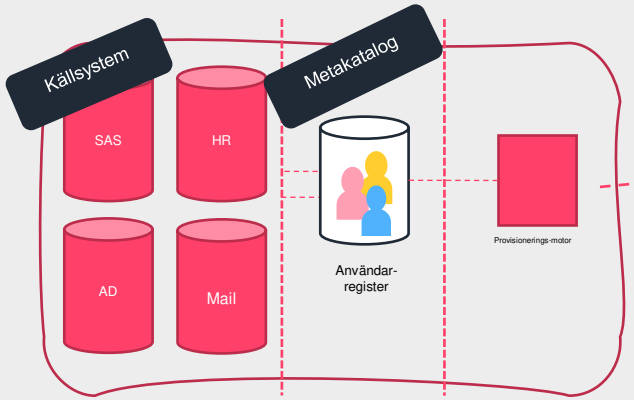
Det kan vara samma system:
Ex. ett SAS vara källsystem, och den kan i sin tur inkludera en provisioneringsmotor (lager metakatalog inte tillämpbart)

INTERNETSTIFTELSEN

Skolfederation

Inloggning

Tjänst A kopplar ePPN med tidigare överförda ePPN och kan logga in Ragnar



Namn
Undervisningsgrupper/klass
...
ePPN

Tjänst A

IdP skickar ePPN till Tjänst A

ePPN

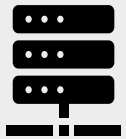
Inga personuppgifter skickas vid inloggningen

Lätt att administrera åtkomst till alla tjänster i skolans IdP

Hjälper med kravställning

Ragnar vill komma åt Tjänst A

Inloggning görs i skolans IdP



IdP

ePPN

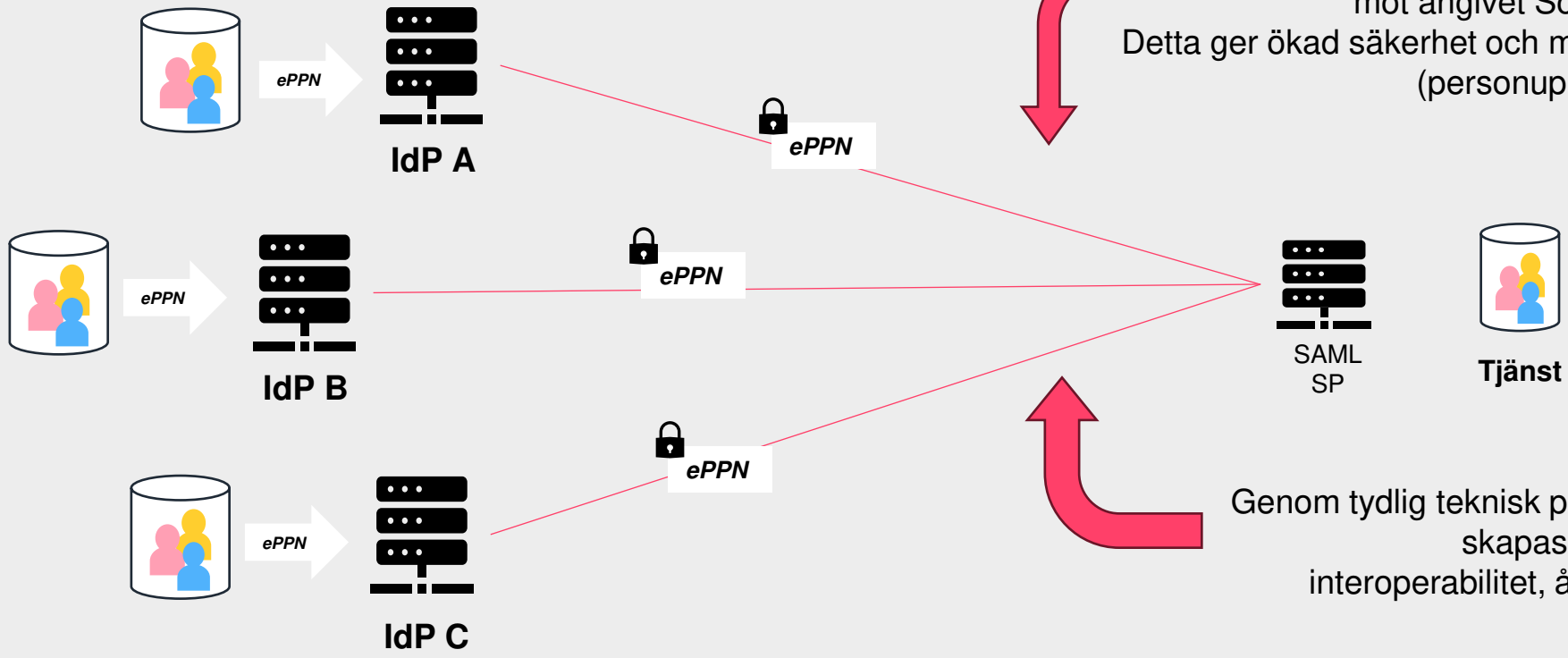
Tjänst C

INTERNETSTIFTELSEN

Skolfederation

Bra för tjänsteleverantörer med!

Genom att minimera attributhantering vid inloggningstillfället till enbart identifiering, och dessutom till ett attribut för identifiering som är standard, blir nya uppsättningar och hantering av inloggningsgränssnittet enkelt



Tjänsteleverantörer validerar Scope-delen i EPPN
mot angivet Scope i IdP-metadata.
Detta ger ökad säkerhet och minskar risken för identitetsförväxling
(personuppgiftsincidenter)

Genom tydlig teknisk profil (WebSSO Technology Profile)
skapas förutsättningar för
interoperabilitet, återanvändbarhet, automation

INTERNETSTIFTELSEN

Skolfederation

Varför inte överföra alla personuppgifter i inloggningen? Varför enbart ePPN?

Personuppgifter, och andra behörighetsstyrande attribut, kan överföras vid inloggningen utan en provisionering

Skolfederation har en Attributprofil som beskriver hur dessa attribut då ska formas och hanteras.

Med detta ställs dock vissa praktiska utmaningar.

- Samtliga av tjänsten önskade personuppgifter skickas vid varje åtkomsttillfälle (oftare än inloggningstillfälle – tänk att inloggning kan ske en gång i IdP men personuppgifter skickas först en användare önskar nå och saknar en session hos en extern tjänst)

- Tjänsten får inte kännedom om användaren innan den har loggat in första gången – krångligare att administrera för skolpersonal och administratörer

- Tjänsten får inte kännedom om användaren inte längre ska ha tillgång till tjänsten – exempelvis om en elev slutar, byter klass/undervisningsgrupp, och så vidare – svårare att hålla uppgifterna korrekta och uppdatera.

Skolfederation

Men hur gör jag egentligen med ePPN?

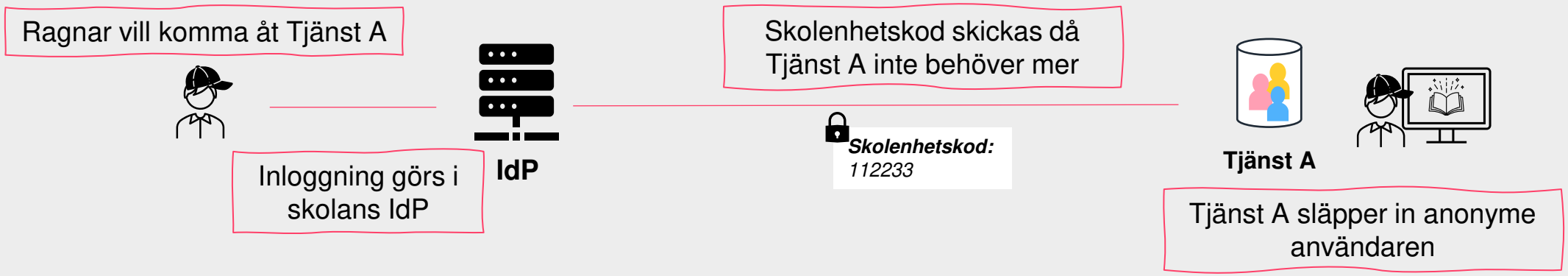
Stanna kvar för Stefan Haléns presentation alldeles strax.

Skolfederation

I vissa fall krävs inte personuppgifter för åtkomst

Vissa tjänster är inte intresserade av **vem** användaren är, utan det räcker att veta att användaren är behörig att få åtkomst

Ofta regleras detta genom affärsavtal mellan skolan och leverantören, ex om licenser är på skolhuvudmanna- eller skolenhetsnivå



INTERNETSTIFTELSEN

Skolfederation

Nationella betygsdatabasen (Beda)

I september 2023 flyttar Universitets- och högskolerådet (UHR) den nationella betygsdatabasen till en ny teknisk plattform, med en ny inloggningstjänst (varken inrapportering av betyg våren 2023 eller skolor som skickar in betyg till Beda via en centralleverantör kommer att påverkas av plattformsflytten).

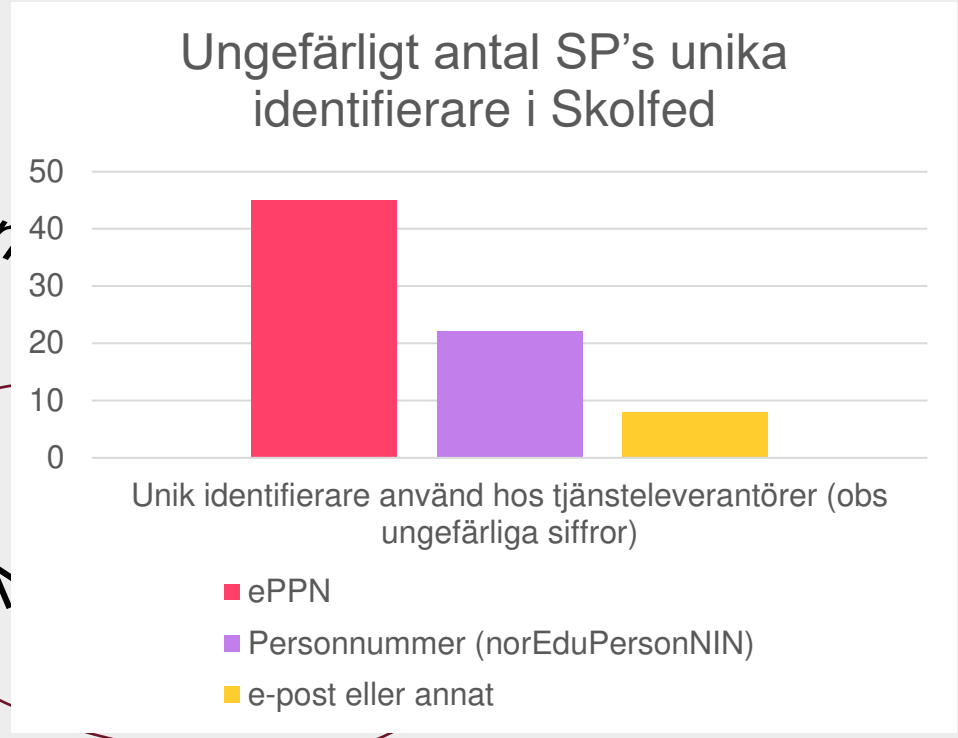
Skolor kommer kunna logga in till Beda genom sin federationsanslutna IdP – likt Skolverkets provplattform för DNP 👍
(eduID är ett alternativ för de som saknar IdP)

Beda kräver attributet ePPN som identifierare – Skolor kan återanvända sitt ePPN-arbete 👍

Information relaterat till det ”federationsspecifika” kommer vi publicera på webbplatsen vartefter. För mer info, kolla in https://www.uhr.se/beda

Skolfederation

ePPN en nyckel som identifierare



Frår

Grund- och gymnasieskola

Skoladministrativa system

Digitala läromedel

Andra digitala lärresurser

DN

ePPN

Skolorganisationer

INTERNETSTIFTELSEN

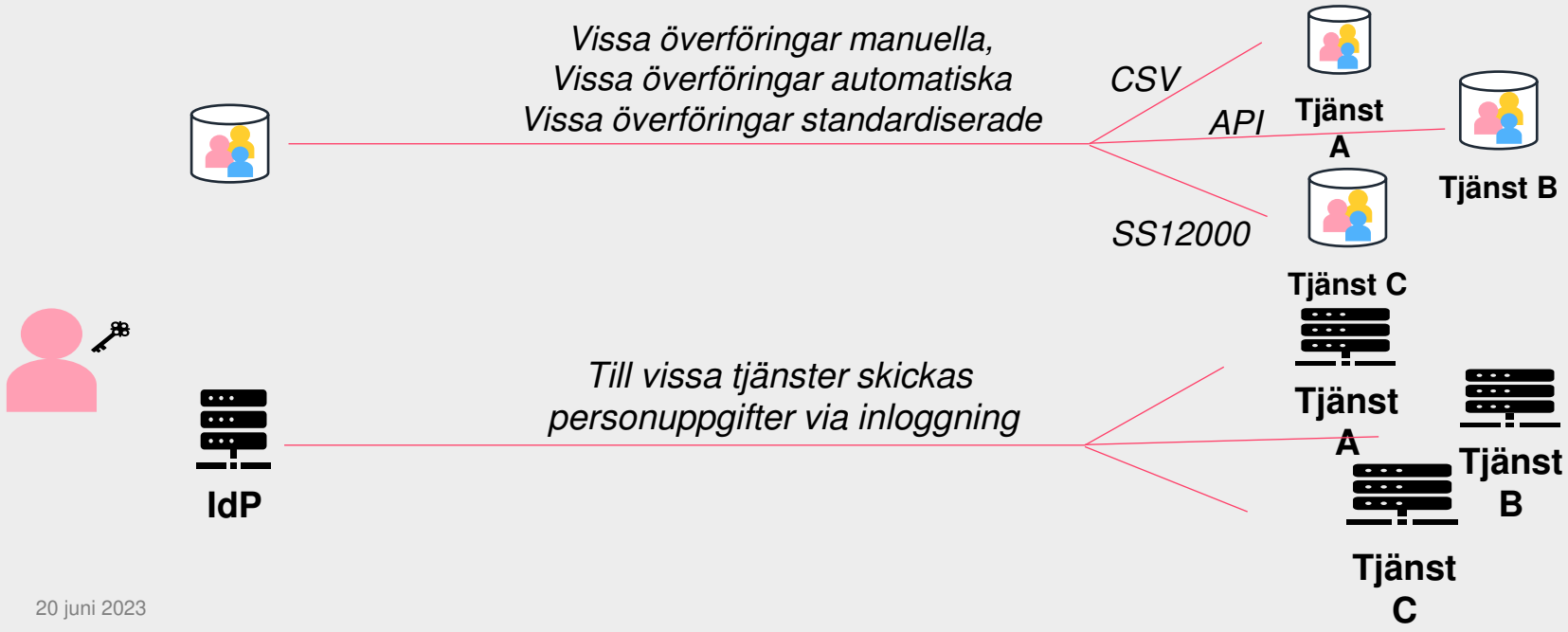
Skolfederation

En förändring som kan ta lite tid

Även om många huvudmän och tjänsteleverantörer kan sträva efter en enhetlig standardiserad lösning så tar en transition från ”en sämre lösning” till ”en bra lösning” tid.

I Sverige har vi tusentals skolor och hundratals leverantörer som behöver samspela för att komma förbi initiala hinder

Skolhuvudmän och leverantörer behöver i resan mot standarder vara anpassningsbara till att personuppgifter och behörighetsstyrande uppgifter hanteras på olika sätt beroende på parter.



INTERNETSTIFTELSEN

Skolfederation

Ytterligare saker att ta i beaktande

- Vi har nu bara zoomat in på provisionering och inloggning för att se en god(eller?) symbios
- Andra processer viktiga: beställning och leverans av digitala läromedel, elev byter skola, framtida utveckling och standarder
- E-legitimationer och autentiseringsmetoder, signalering av tillitsnivå och IdP- samt SP-stöd

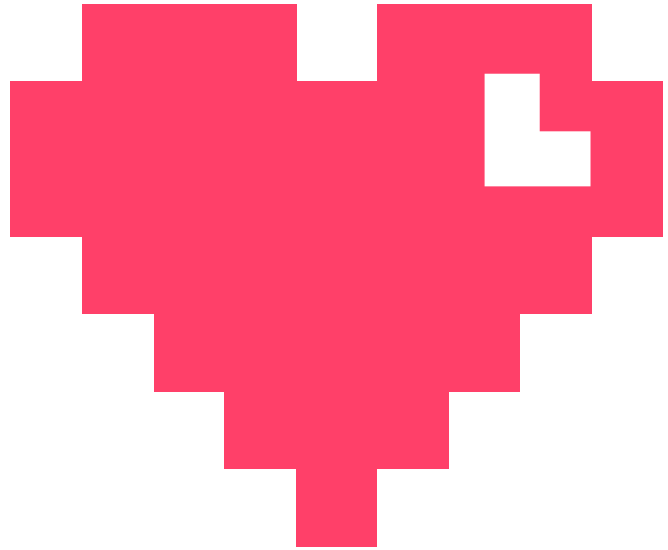
Kommentera gärna!

- Jag tror att den här modellen kommer vara gällande för stora till mellanstora skolhuvudmän i Sverige, och leverantörer kommer följa efter

- DNP (och ev andra tjänster som Beda) normerande

- I en övergångstid kommer det vara blandade implementationer

- För små till de minsta huvudmännen kommer paketerade lösningar IdP+SS12k men full täckning kommer vara svårt att nå



Tack!

rasmus.larsson@internetstiftelsen.se

Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi verkar för ett internet som bidrar positivt till människan och samhället.

INTERNET STIFTELSEN