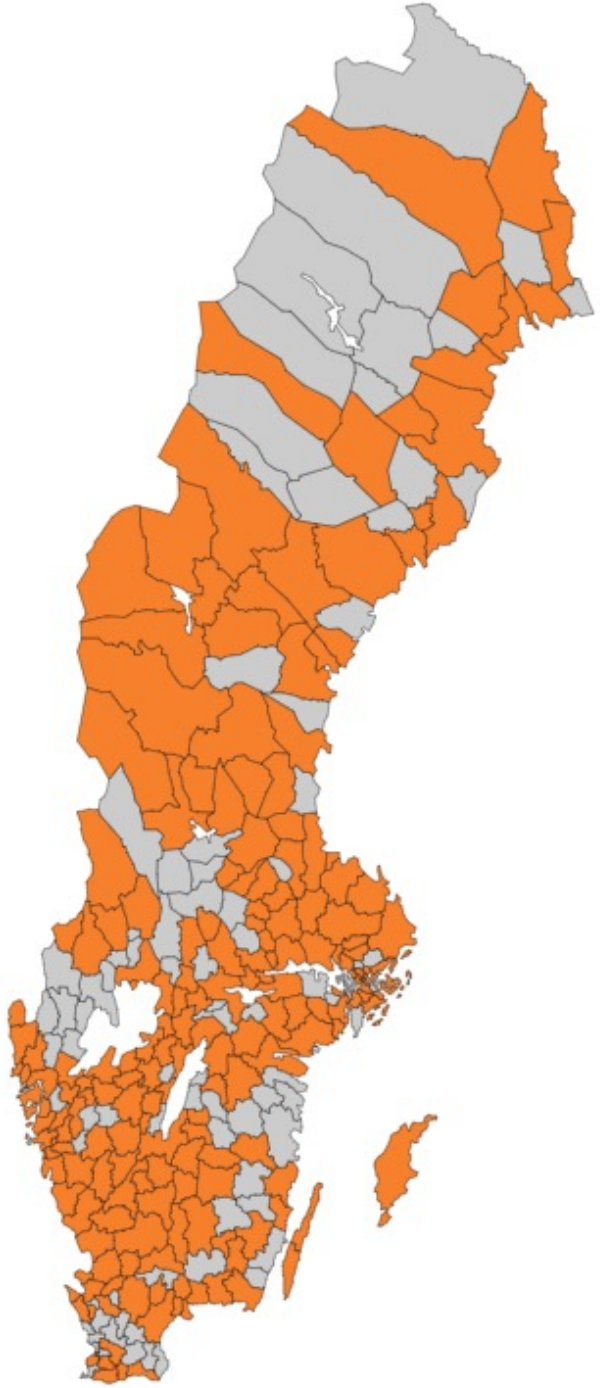
INTERNET STIFTELSEN

Säker identitetshantering med Skolfederation

24/5 2023

Rasmus Larsson
rasmus.larsson@internetstiftelsen.se



Skolfederation

Identitet- och behörighetsfederation för grund och gymnasieskola, utbildningsanordnare, myndigheter. Offentliga och fristående.

Totalt 440 medlemmar

- 358 är användarorganisationer, varav 207 kommunala skolhuvudmän (se karta)
- 82 är tjänsteleverantörer

Ungefär fyra av fem elever går hos en skolhuvudman som är medlem i Skolfederation

Vad är en federation?

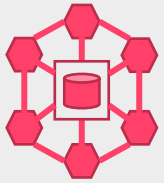
En sammanslutning av organisationer med mål att enas om **identitets- och behörighetsrelaterade frågor**

I Skolfederation handlar det om samverkan avseende:

Regler

Standard

Infrastruktur



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

Regler

Vilka lagar och regler behöver vi förhålla oss till?

GDPR
Skollag- och förordningar
Branschspecifika överenskommelser
→
Tillitsramverk
Informationssäkerhet
Identitetshantering

Standard

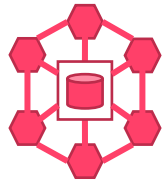
Vilka gemensamma lösningar och standarder ser vi kan lösa utmaningarna?

Enkel och säker inloggning - SAML 2.0

Provisionering och informationsöverföring - SS12000, EGIL

Beställning och leverans av digitala läromedel - BOL

Infrastruktur



Hur tillämpas dessa?

Metadataregister SAML 2.0

Metadataregister Moa

Skolfederation

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

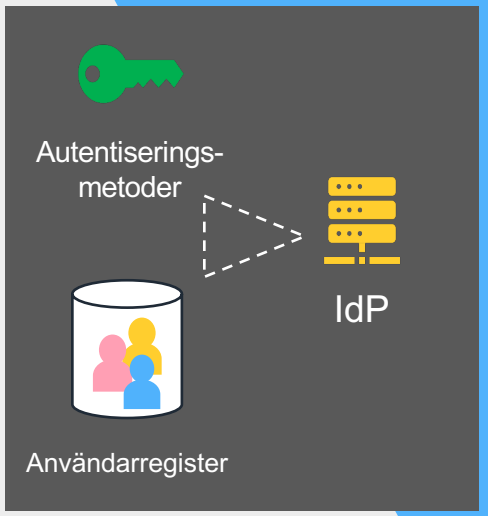
Skolfederation är inte en centraliserad lösning.

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

Avtal krävs mellan parterna, precis som vanligt

Skolan behöver ha affärsavtal med de leverantörer vars tjänster de vill utnyttja

Skolan behöver ha personuppgiftsbiträdesavtal (**PUBA**) med leverantörerna i fallet personuppgifter behandlas

Avtal

Vilka tjänster...

Skolan

$

Leverantören

PUBA

Vilken personuppgiftsbehandling...

Metod

Uppgiftsdelning från register

Användar-register

Överföring via manuella processer, ex. skicka/ladda upp filer (CSV, FTP)
Överföring via automatiserade processer, ex. API, SS12000

Användar-register

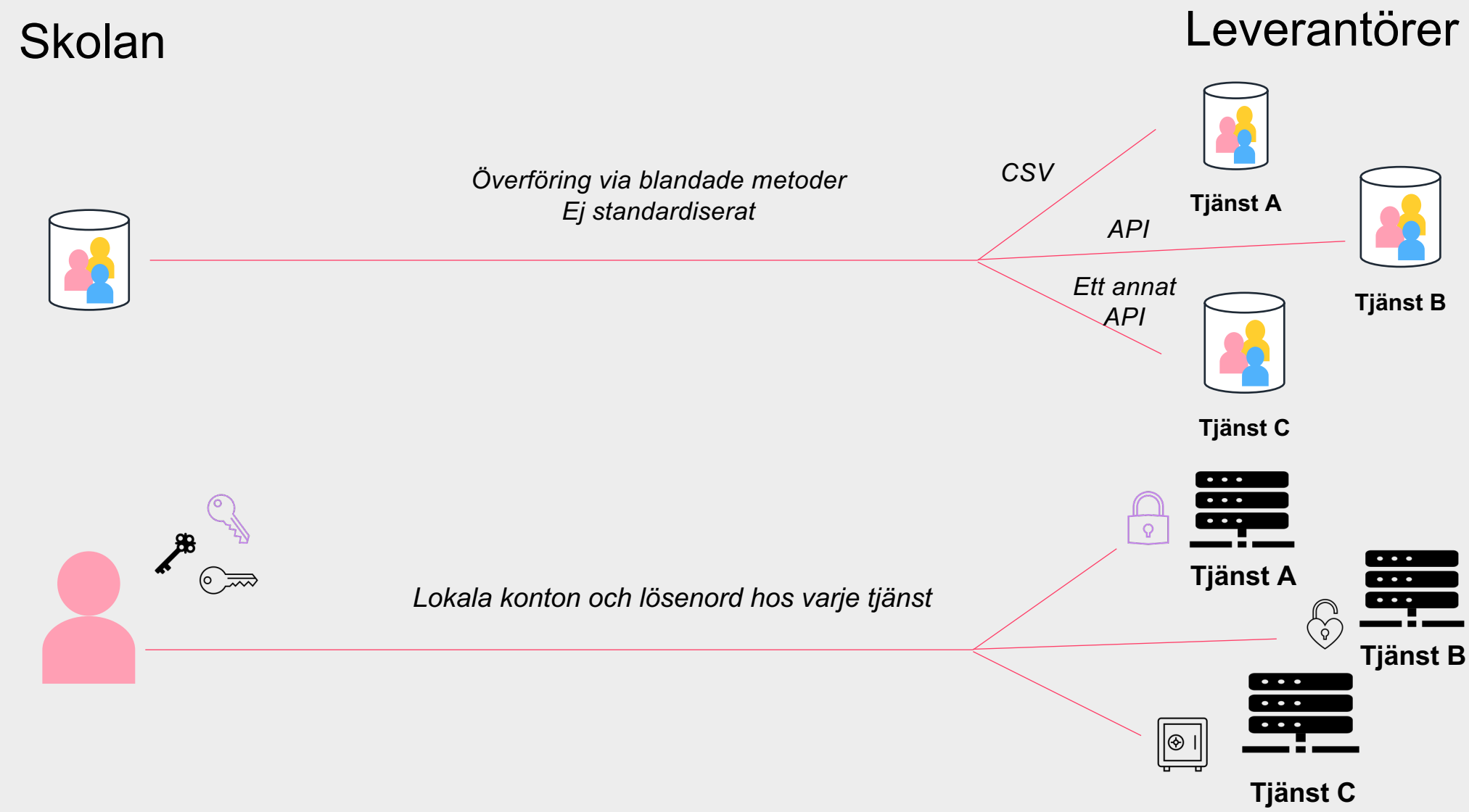
Inloggning

IdP

Överföring av personuppgifter vid inloggningstillfället

SP

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 och GDPR

- Först presenteras *en* integritetsskyddande uppsättning för hantering av identiteter och personuppgifter
  - Det finns säkert flera sätt att göra goda lösningar när pusslet läggs
- Vi går sedan igenom de grundläggande principerna i GDPR och ger exempel på fördelar som Skolfederation kan innebära om ni ansluter er och använder tjänsten på ett integritetsskyddande sätt
- Kom ihåg att Skolfederation inte gör att ni per definition efterlever GDPR
  - Det är hur era rutiner, processer, och hur ni och tjänsteleverantörerna sätter upp era tekniska lösningar samt till exempel vilka attribut ni faktiskt kräver eller skickar som avgör om ni arbetar på ett integritetsskyddande sätt eller inte. Ansvaret ligger hos personuppgiftsansvarig.

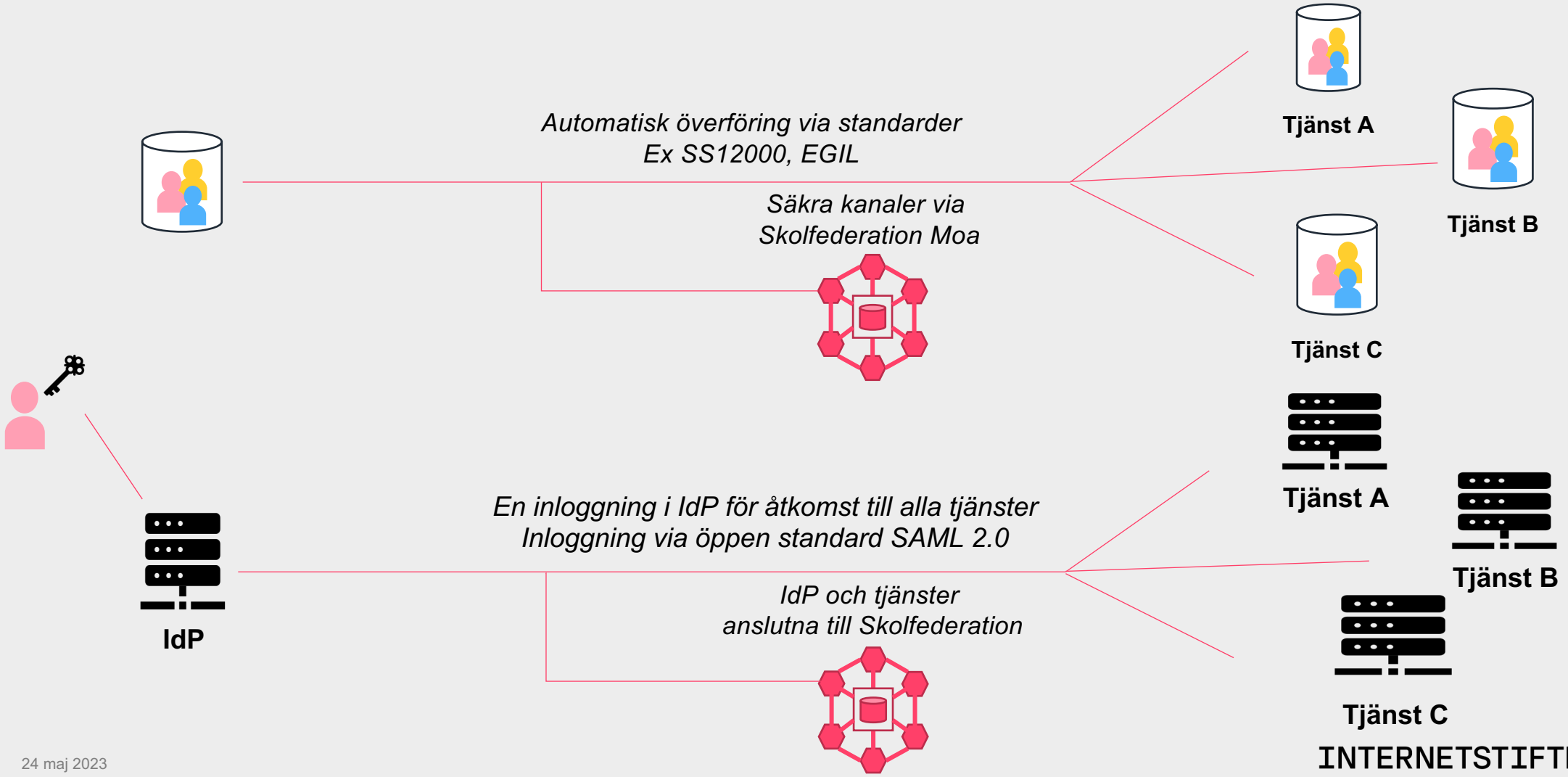
Skolfederation

En bra lösning

Skolan

Överblick

Leverantörer



INTERNETSTIFTELSEN

Skolfederation

En bra lösning

Skolan

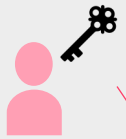
Personuppgiftsflöden

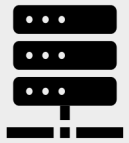
Leverantörer

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





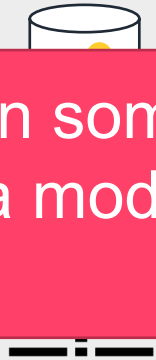
IdP

I inloggningen skickas inga personuppgifter

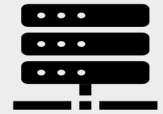
Enbart ePPN

Tjänst A

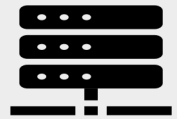
Tjänst B



Tjänst A



Tjänst B



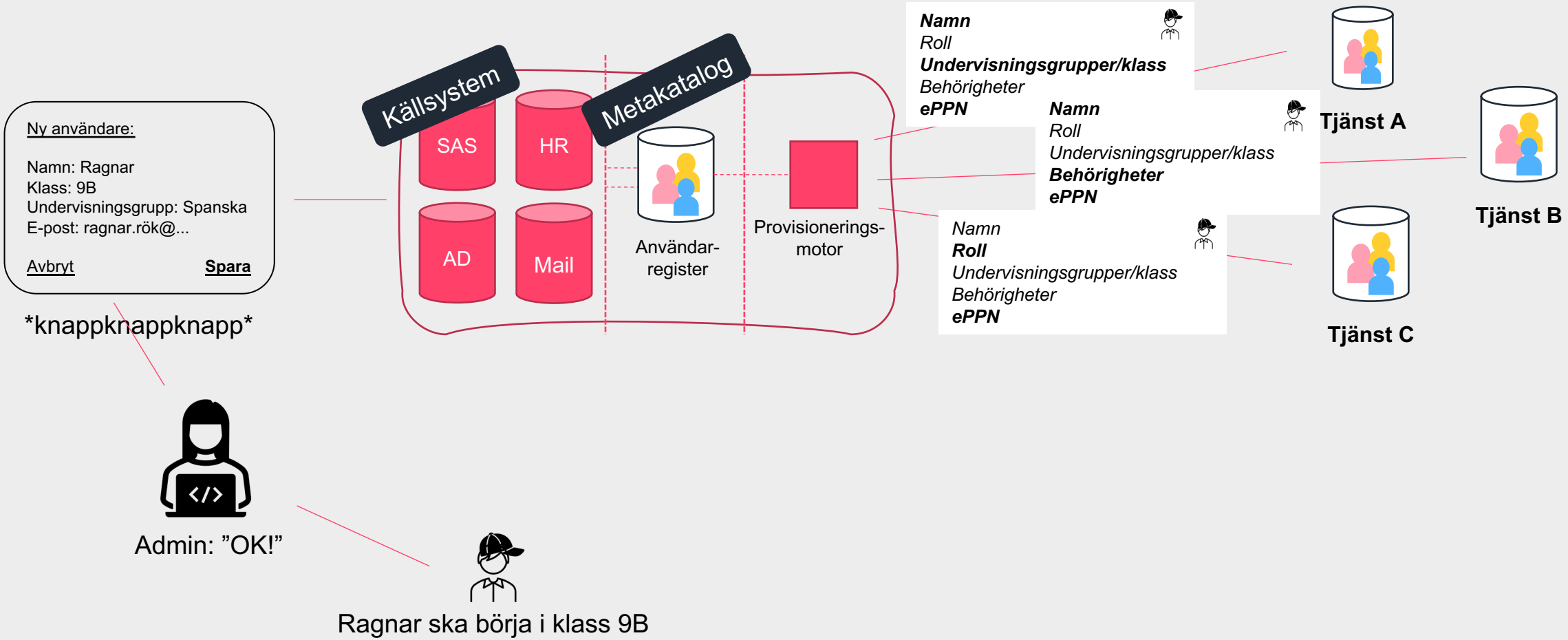
Tjänst C

Någon som känner igen denna modell? Varifrån?
☺

INTERNETSTIFTELSEN

Skolfederation

En bra lösning

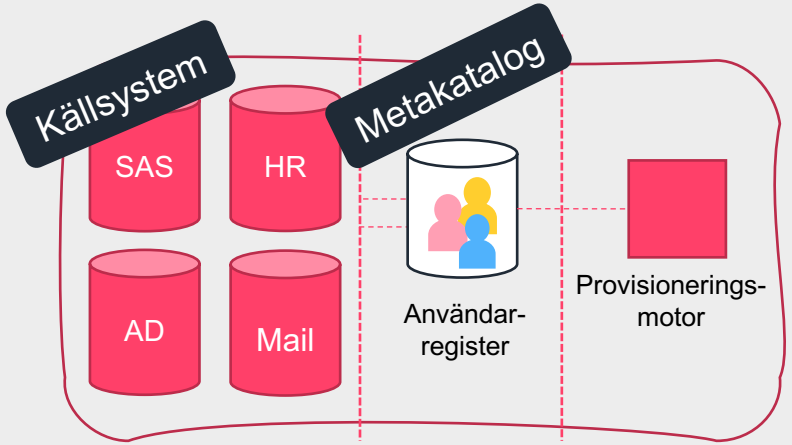


INTERNETSTIFTELSEN

Skolfederation

En bra lösning

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



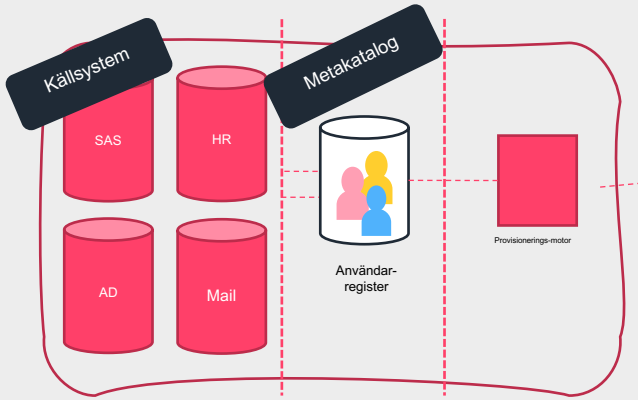
Det kan vara separata system:
Provisioneringsmotorn är kopplad till ett användarregister (”metakatalog”), som föds av källsystemen.

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



Namn
Undervisningsgrupper/klass
...
ePPN

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

Tjänst A

IdP skickar ePPN till Tjänst A

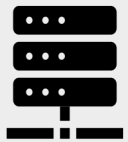
ePPN

Inga personuppgifter skickas vid inloggningen

Lätt att administrera åtkomst till alla tjänster i skolans IdP

Hjälper med kravställning

Ragnar vill komma åt Tjänst A



IdP

Inloggning görs i skolans IdP

ePPN

Tjänst C

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

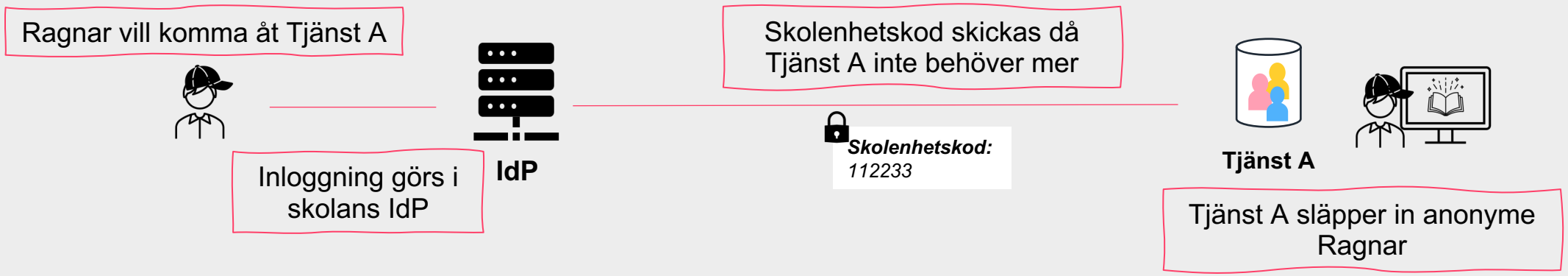
- Tjänsten får inte kännedom om användaren inte längre ska ha tillgång till tjänsten – exempelvis om en elev slutar, byter klass/undervisningsgrupp, och så vidare – svårare att hålla uppgifterna korrekta och uppdatera.

Skolfederation

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



Självklart behövs en bedömning av personuppgiftsansvarige för att se om ”anonyma” attribut tillsammans med någonting annat eller i särskilda omständigheter kan utgöra personuppgifter

INTERNETSTIFTELSEN

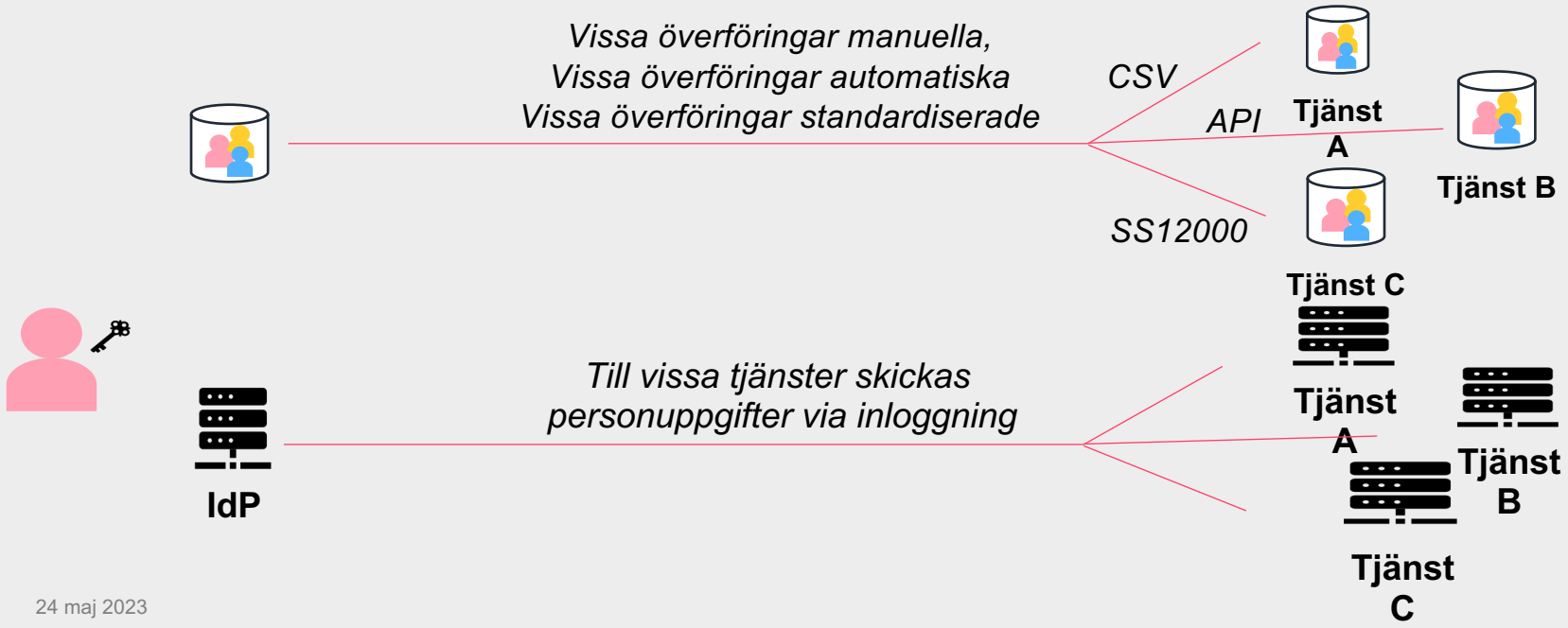
Skolfederation

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 och GDPR

Laglighet, korrekthet och öppenhet

- Med Skolfederation är det lättare att hålla personuppgifterna uppdaterade och korrekta. Det är hos skolan som inloggningen sker och skolan väljer vilka uppgifter som skickas till tjänsteleverantörerna. Skolan har då möjlighet att ha större kontroll över personuppgifterna, hålla en bättre ordning på uppgifterna samt hålla dem uppdaterade.

- Att använda Skolfederation innebär att alla medlemmar i federationen följer en och samma standard vilket skapar öppenhet och förenklar för skolorna att vara transparenta i sin personuppgiftsbehandling.

- Att leverantören måste ange vilka attribut som krävs innebär också en ökad transparens och skolan kan då, för att skydda användarnas integritet, välja en leverantör som inte kräver mer än nödvändigt.

Uppgiftsminimering

- Vid användande av Skolfederation behöver användaren endast logga in en gång för att komma åt alla tjänster. Detta minskar personuppgiftsbehandlingen väsentligt jämfört med att användaren behöver logga in i varje individuell tjänst den ska använda.

- Skolfederation innebär att skolan på ett enkelt och säkert sätt kan ha kontroll på vilka personuppgifter som skolan lämnar ifrån sig till sina tjänsteleverantörer. Skolan kan på ett enkelt sätt uppgiftsminimera personuppgiftsbehandlingen genom att endast skicka nödvändiga attribut till tjänsteleverantörerna.

Uppgiftsminimering

- Om båda både skolan och tjänsteleverantören stödjer det kan också en inloggning med hjälp av Skolfederation faktiskt ske utan att tjänsteleverantören får ta del av information som kan identifiera den som loggar in. Tjänsteleverantören får bara ett pseudonymiserat attribut. Skolan kan alltså samla in personuppgifterna för inloggning från eleverna men behöver inte exponera dem för sina tjänsteleverantörer.

- Kom ihåg grundregeln att det inte är tillåtet att samla in personuppgifter bara för att ”de är bra att ha” och det gäller såväl skolan som tjänsteleverantörerna

Lagringsminimering

- Personuppgifter får inte heller behandlas längre än vad som är nödvändigt för ändamålet. Personuppgifter som inte längre är nödvändiga för ändamålet ska gallras. Det vanligaste sättet att gallra är att radera personuppgifterna.

- Skolfederation kan underlätta gallring och underlätta lagringsminimering, särskilt vid användning av Skolfederation Moa, detta eftersom skolan då själv kontrollerar provisioneringen av konton och behörigheter. Skolan kan centralt i sina register ta bort användare som inte längre ska ha konton eller behörighet hos skolans tjänsteleverantörer.

Integritet och konfidentialitet

- Den som behandlar personuppgifter ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna, detta gäller så klart också vid inloggning i olika tjänster

- I Skolfederation behöver skolan bara skapa en säker inloggning för sina användare på skolan (inloggning i skolans IdP). Det är skolan som själv har kontroll på säkerheten i inloggningen och inloggningen kan då ske med hjälp av till exempel två-faktorsinloggning eller annan, ännu säkrare inloggning

- Inloggningen på skolan kan sedan användas för att koppla upp sina användare mot alla tjänsteleverantörer inom Skolfederation. Skolorna behöver då inte granska och kvalitetssäkra en mängd olika inloggningsmetoder för olika tjänsteleverantörer

Integritet och konfidentialitet

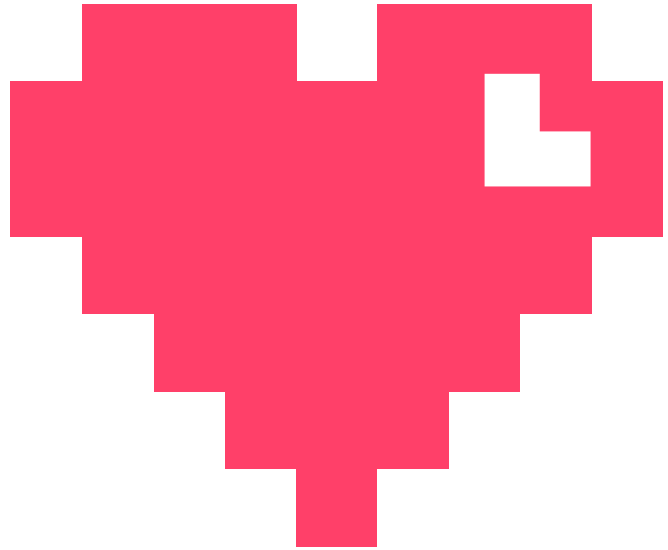
- Om både tjänsteleverantören och skolan stödjer det i sina tekniska lösningar och i sina implementationer av Skolfederation kan inloggningen ske helt utan exponering av personuppgifter för tjänsteleverantören.

- Med hjälp av provisionering genom Skolfederation Moa skickas kontoinformation och behörigheter på ett säkrare sätt. Idag skickas nämligen dessa uppgifter till varje separat tjänsteleverantör med hjälp av till exempel mejl eller excel-filer. Att skicka en mängd listor och dokument på olika sätt till olika leverantörer ökar också risken för att personuppgifterna ska skickas fel eller komma i orätta händer

Summering

- Skolfederation ger personuppgiftsansvarig organisation en bra verktygslåda för att underlätta administration av identiteter och personuppgifter

- God personuppgiftshantering är ingen quick fix, det är ett krav för att digitaliseringen av skolan ska fungera långsiktigt



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