Vad är Skolfederation?

Rasmus Larsson

14 september 2022

INTERNET STIFTELSEN

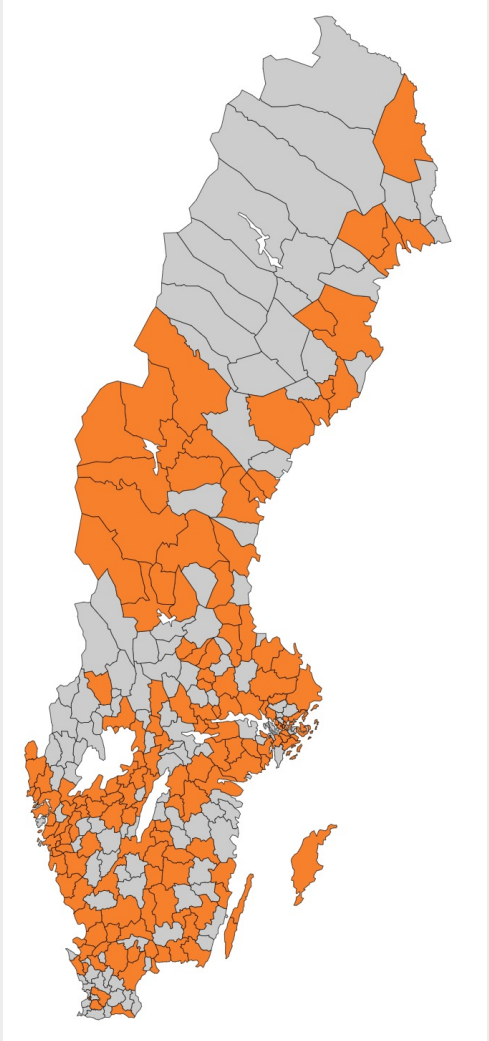
Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi verkar för ett internet som bidrar positivt till människan och samhället.

Skolfederation

- Identitet- och behörighetsfederation (eller: åtkomstfederation) för grund- och gymnasieskola, utbildningsanordnare, myndigheter.
  Kommunala och fristående.

- 384 medlemmar, varav
  - 300 användarorganisationer
  - 84 tjänsteleverantörer

- Över hälften av Sveriges elever går hos en skolhuvudman som är med i Skolfederation



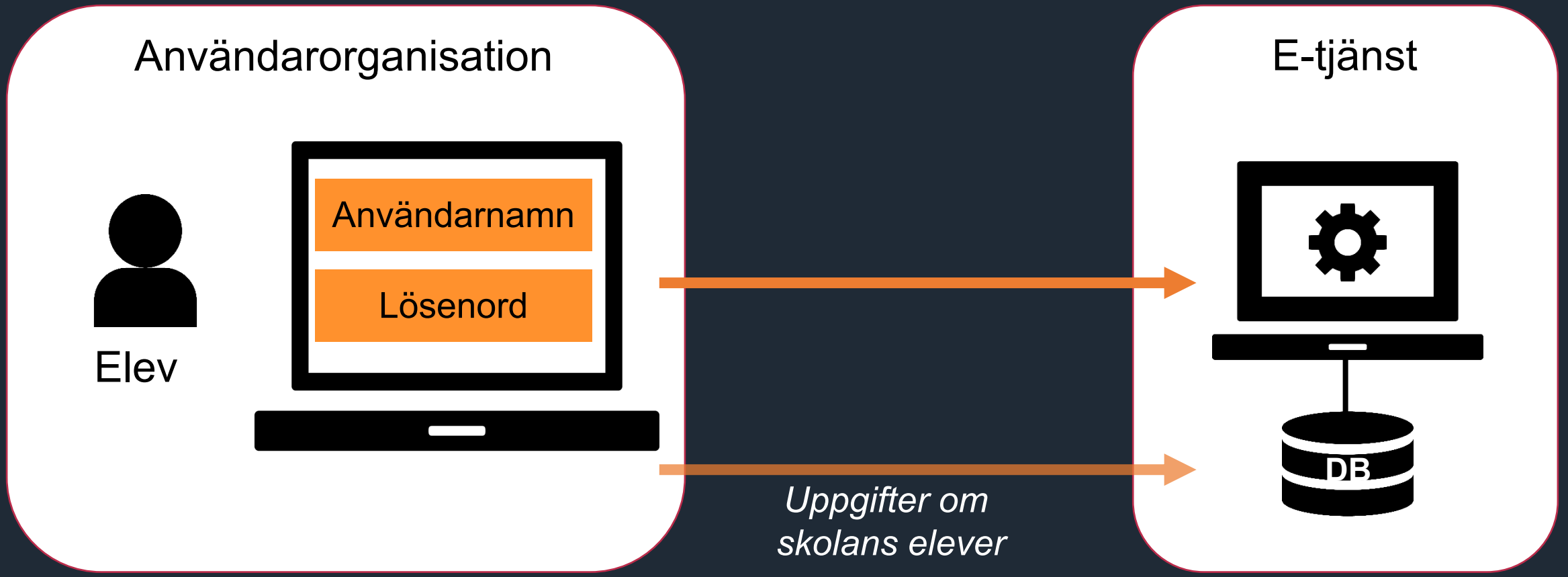
Skolfederation

- Skolor använder Skolfederation för att:
  - Elever och lärare ska få single sign-on (SSO*)
  - Öka säkerheten i inloggning, lösenordshantering, och administration
  - Spara tid och resurser på kravställning och administration av digitala lärresurser. Undvika inlåsningseffekter.
  - Automatiskt överföra (”provisionera”) kontoinformation till lärresurser i Moa
  - Åtkomst till Skolverkets Digitala Nationella Prov (DNP)

**SSO = logga in en gång, komma åt flera tjänster*

Hur fungerar Skolfederation?

Traditionellt inloggningsflöde i skola



Problem 1 – traditionellt inloggningsflöde

Skolhuvudman

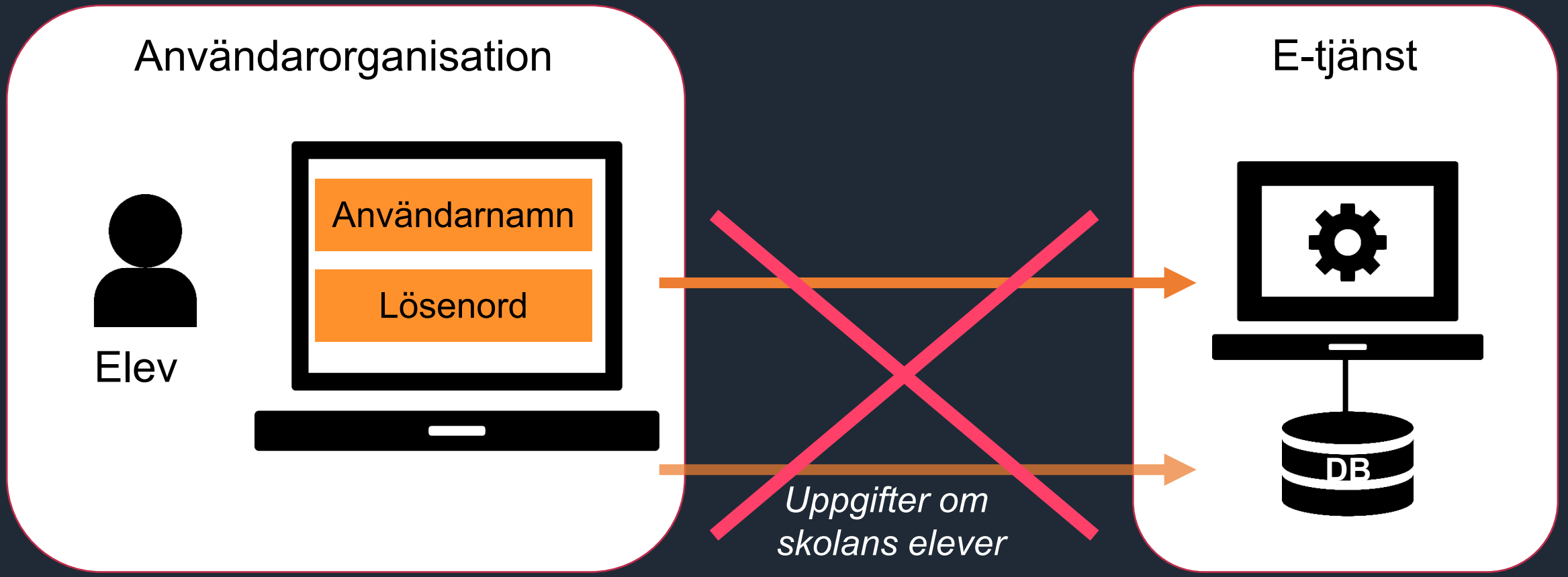
E-tjänst

- Administration av användare
- Kontroll av behörighet
- Integritet för användare
- Tillit

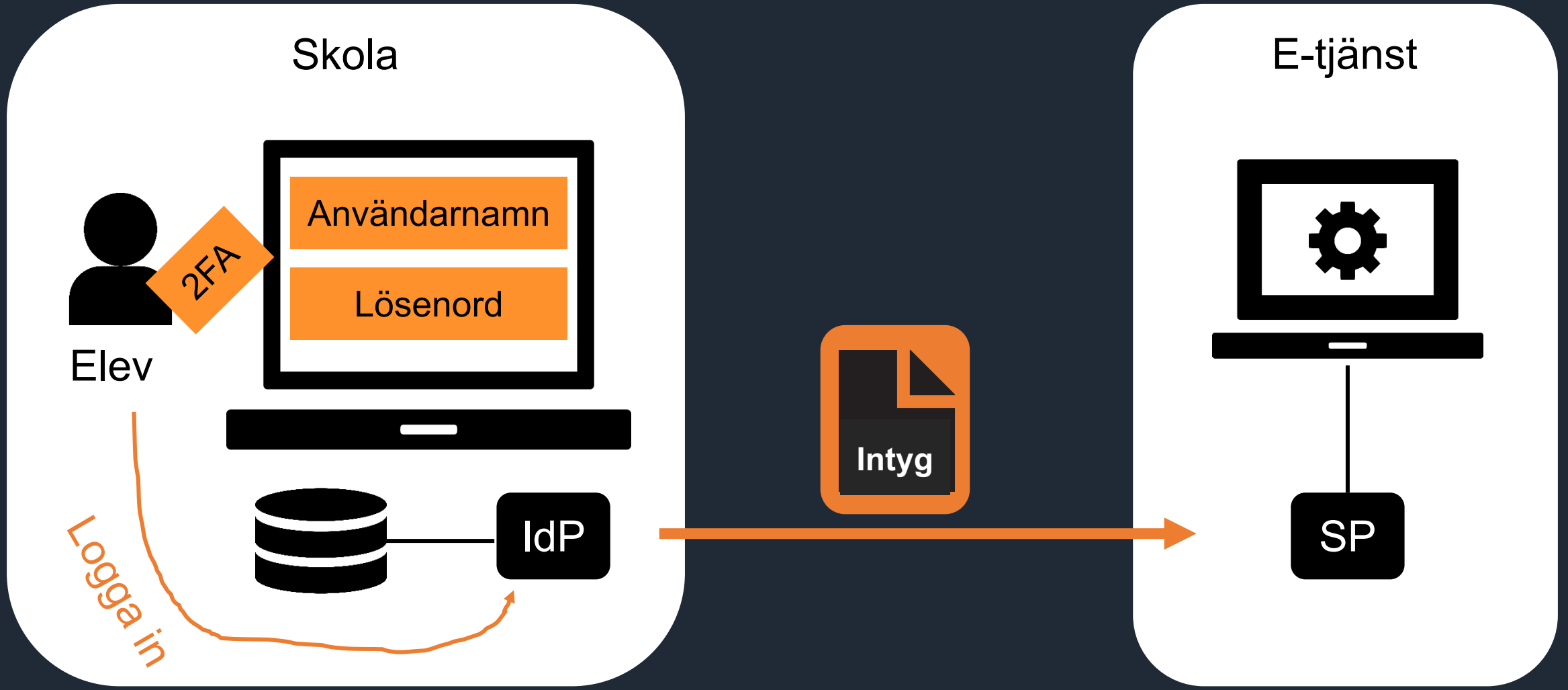
- En inloggning per tjänst
- Ett lösenord per tjänst
- Integritet
- Tillit

- Administration av användare
- Inloggningssupport
- Integritet för användare
- Säkerhet
- Tillit

Traditionellt inloggningsflöde - lösning



Federerat inloggningsflöde i skola



Kort om akronymer och betydelser

SAML – teknisk standard för federerad inloggning

IdP – Identity Provider – ”inloggningslösningen”, hanterar autentisering av användare till tjänster, tillhandahålls av användarorganisation

SP – Service Provider – tjänsteleverantör, skyddar en tjänst och kräver att IdP autentiserar användare

Intyg – IdP ställer ut ett intyg som skickas till SP när åtkomst till SP’s tjänst begärs av användaren

Federerad inloggning

Skolhuvudman

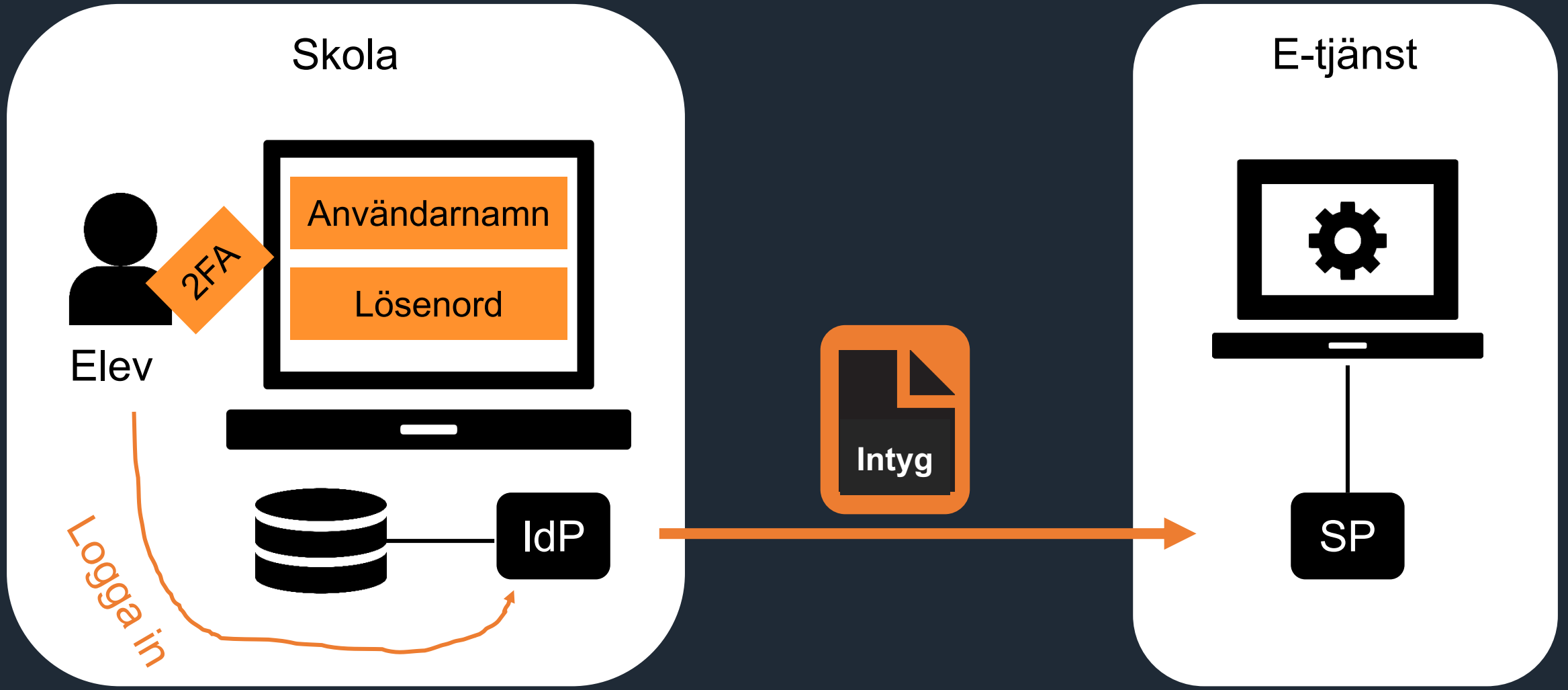
E-tjänst

- Administration av användare ✓
- Kontroll av behörighet ✓
- Integritet för användare ✓
- Tillit ?

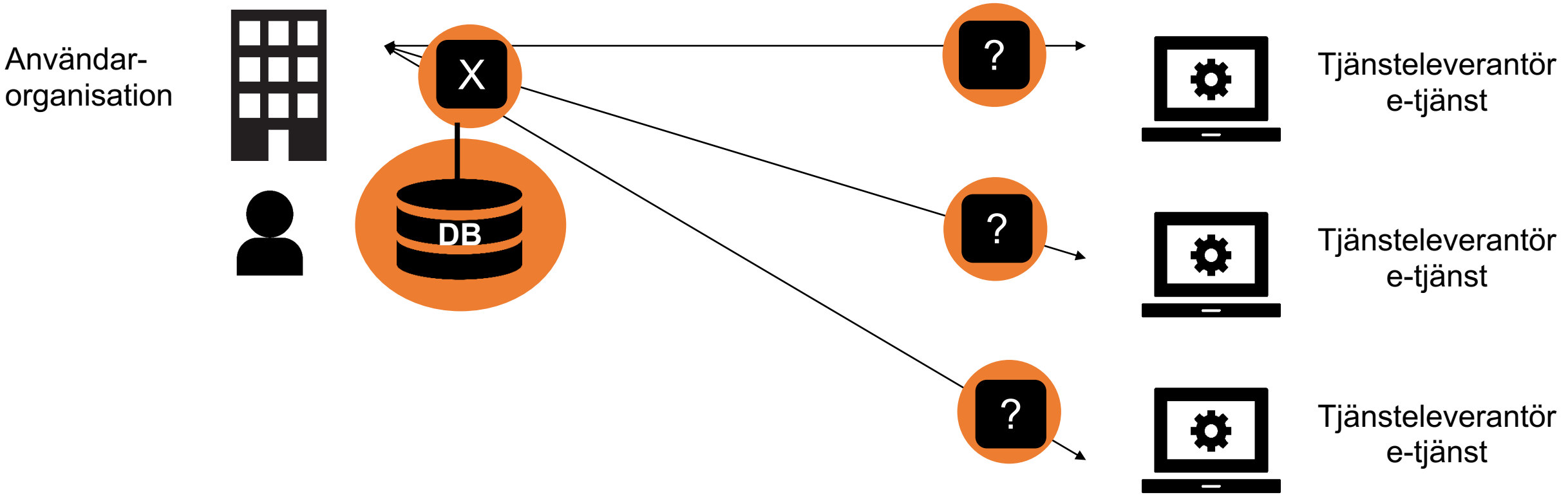
- ~~En inloggning per tjänst~~
- ~~Ett lösenord per tjänst~~
- Integritet ✓
- Tillit ?

- ~~Administration av användare~~
- ~~Inloggningssupport~~
- Integritet för användare ✓
- Säkerhet ✓
- Tillit ?

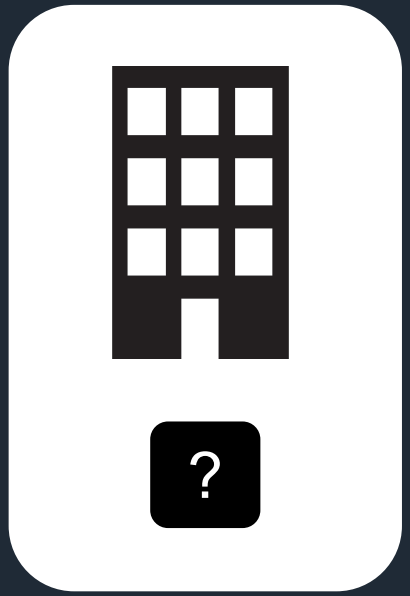
Federerat inloggningsflöde i skola



Problem 2 – bilaterala överenskommelser

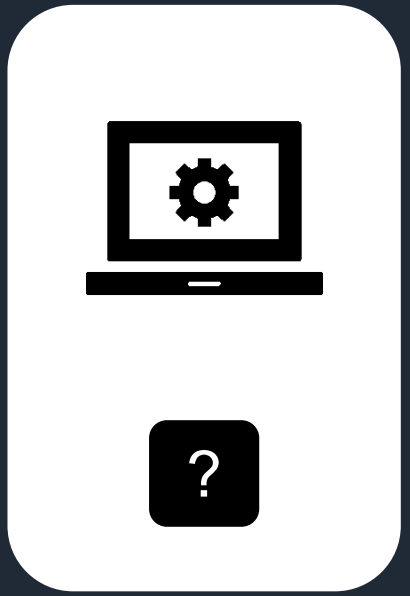


En närmare titt på problem 2



Förutsätter att parterna <u>enats</u> om:

- Teknik/standard
- Tillämpning
- Information
- Format
- Tillit/säkerhet
- Rutiner
- …

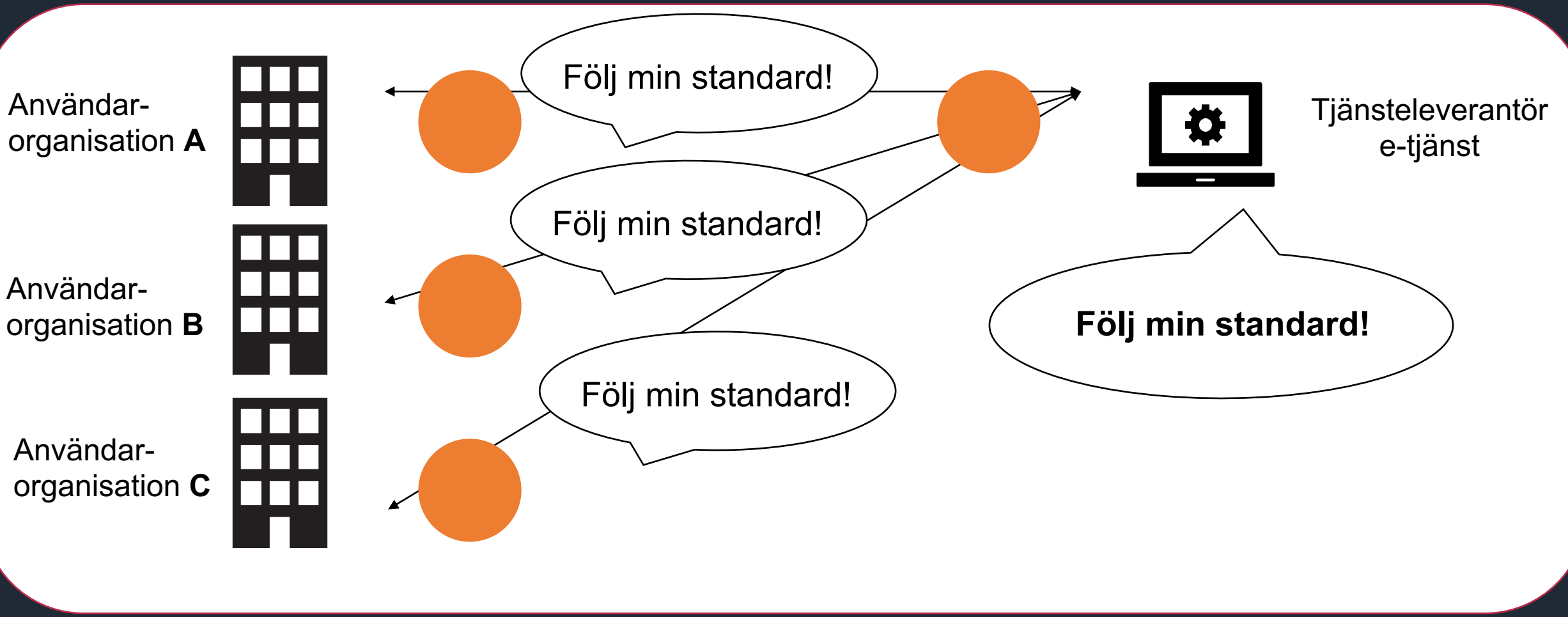


Mer akronymer och betydelser

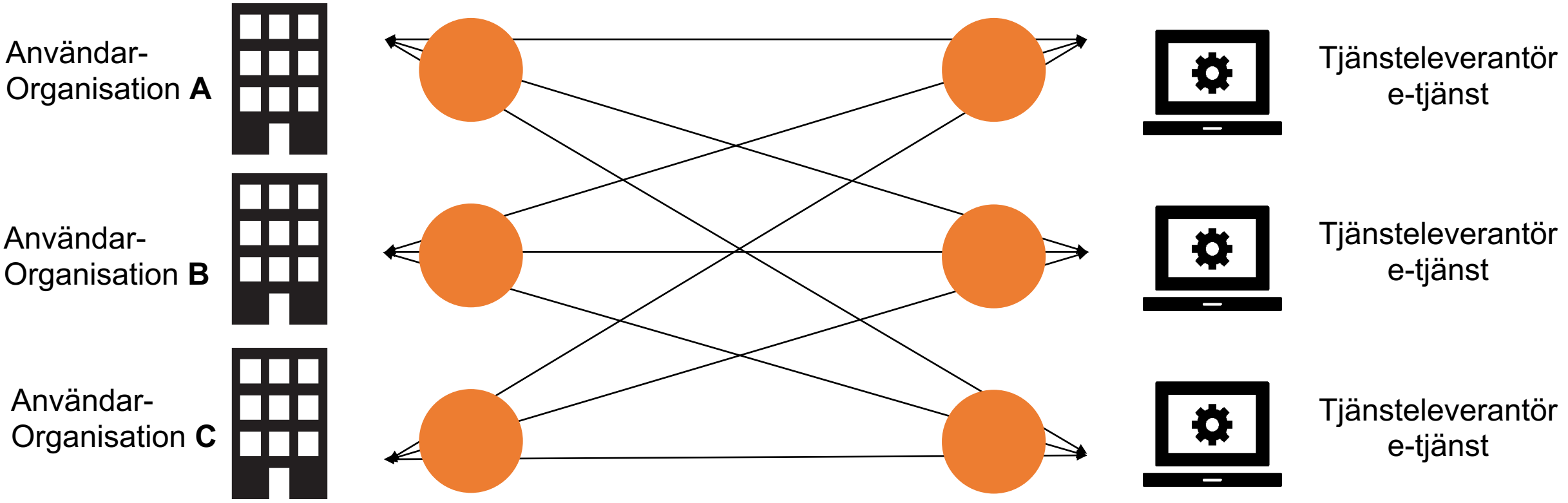
Metadata – ”data om data”, beskriver IdP/SP med tekniska termer, används för inloggning och anslutning i federation. Ett ”tekniskt medlemsregister”

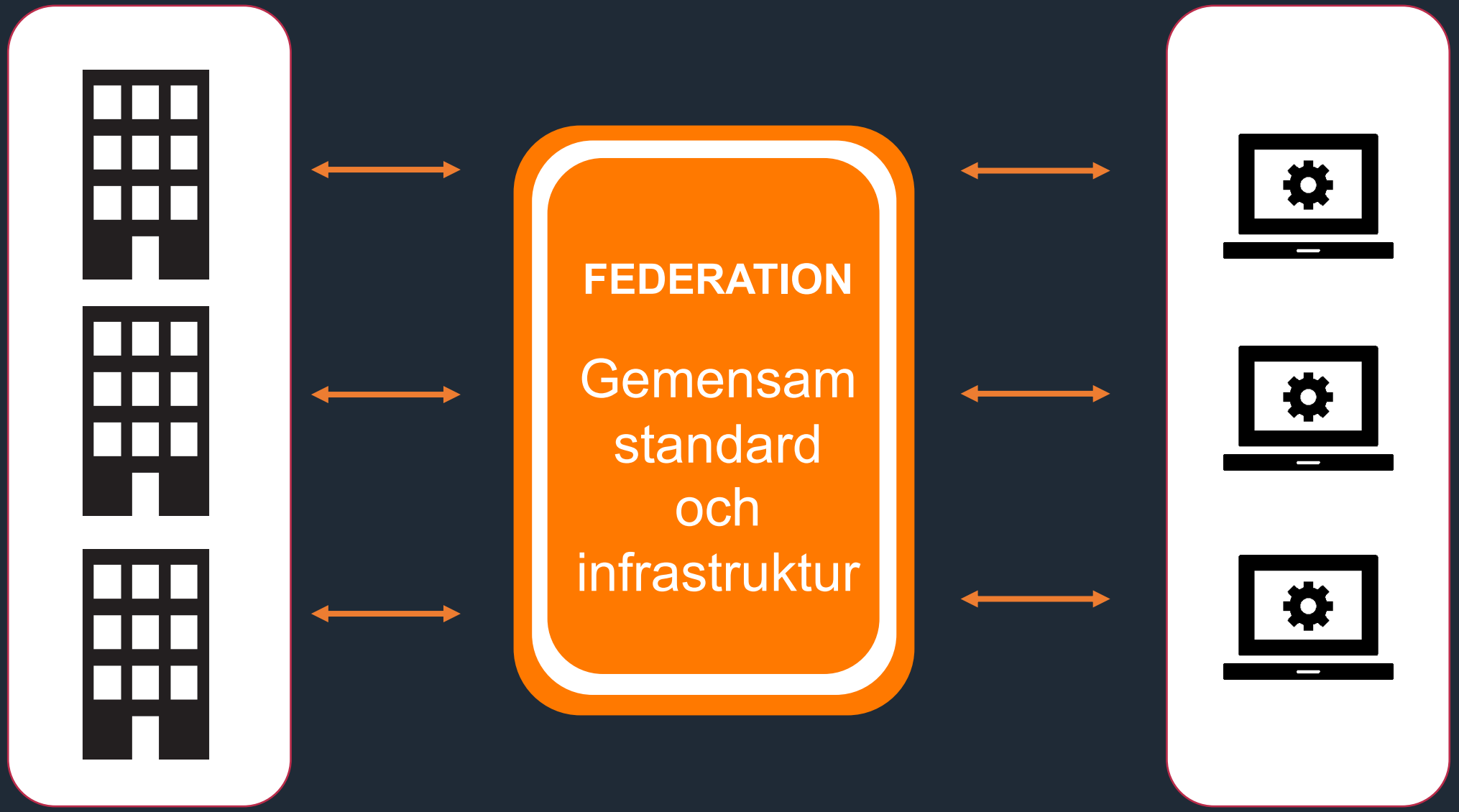
Certifikat/nyckel – för säkerhet i federation används signering och kryptering mellan parter. För detta behöver medlemmar publicera säkerhetscertifikat/”nycklar” i sitt metadata

Problem 2

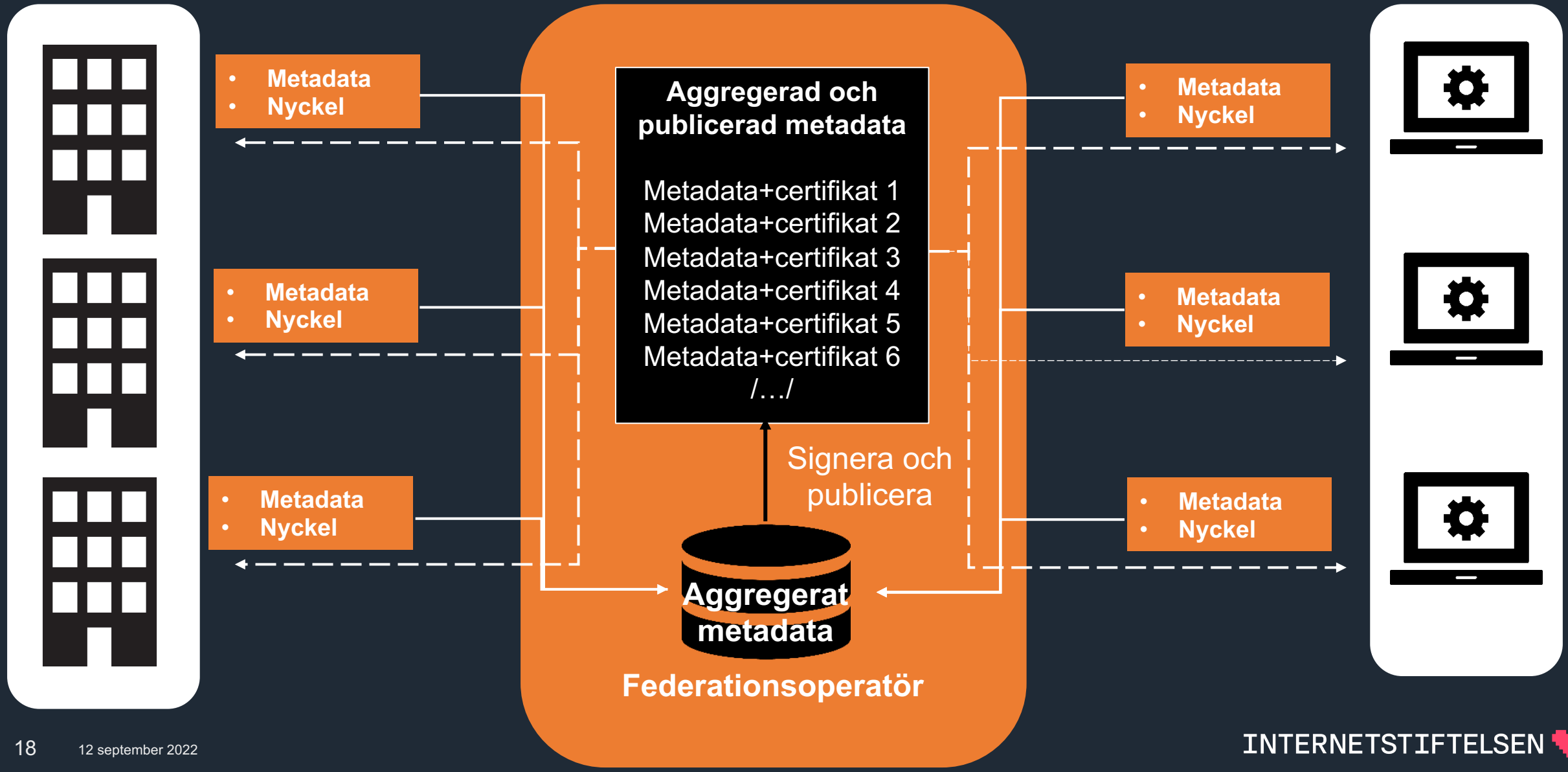

Användar-
organisation **A**
Användar-
organisation **B**
Användar-
organisation **C**
Följ min standard!
Följ min standard!
Följ min standard!
Tjänsteleverantör
e-tjänst
Följ min standard!

Problem 2


Användar-
Organisation **A**
Användar-
Organisation **B**
Användar-
Organisation **C**
Tjänsteleverantör
e-tjänst
Tjänsteleverantör
e-tjänst
Tjänsteleverantör
e-tjänst

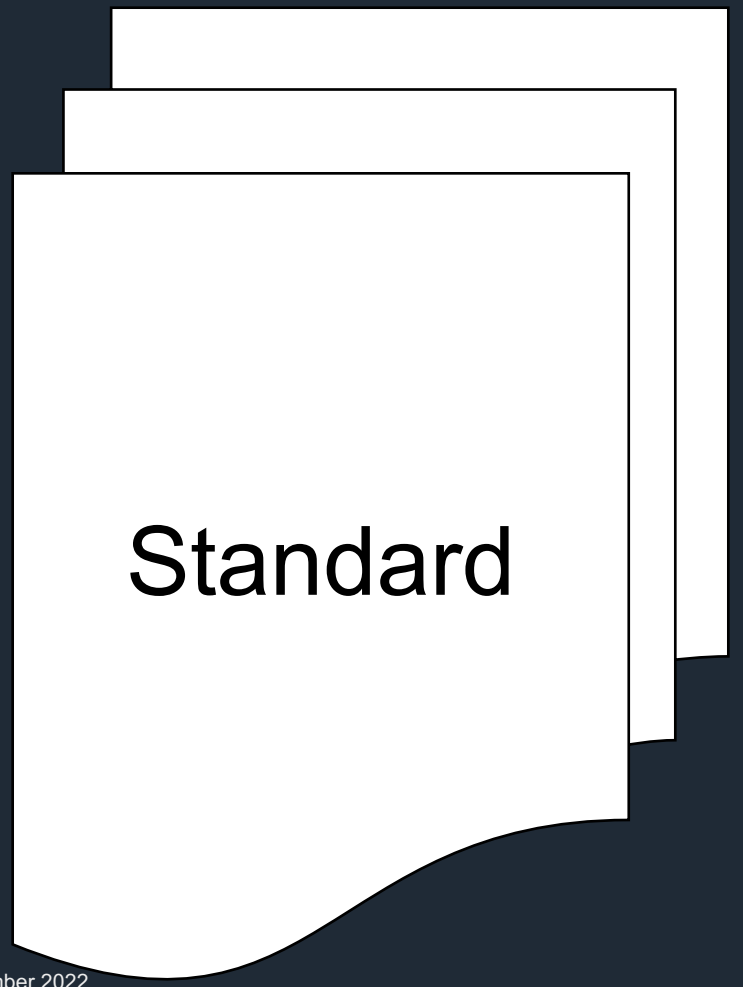

FEDERATION
Gemensam standard och infrastruktur

Federationens infrastruktur



INTERNETSTIFTELSEN

Federation



och

Och…

Tillit!

- För att en federation ska fungera behöver medlemmar ha *tillit* till federationen
- Tillit upprätthålls genom så kallade *tillitsramverk*
- I Skolfederation behöver medlemmarna ha tillräcklig koll på sin informationssäkerhet, identitetshantering, sina organisatoriska aspekter med mera


BILAGA 2
Säkerhetsföreskrifter för Användarorganisationer anslutna till Skolfederation
Version 2.3
Skolfederation

- Granskningar/revisioner av medlemmars uppfyllnad görs typiskt inte i Skolfederation (ev. vid kända avvikelser som kommit upp till ytan).
  I systerfederationen Sambi (inom vård och omsorg) är vikten av granskning däremot större.

Federation - samverkan

Regler

Standard

Infrastruktur

Skolfederation och DNP

Skolfederation

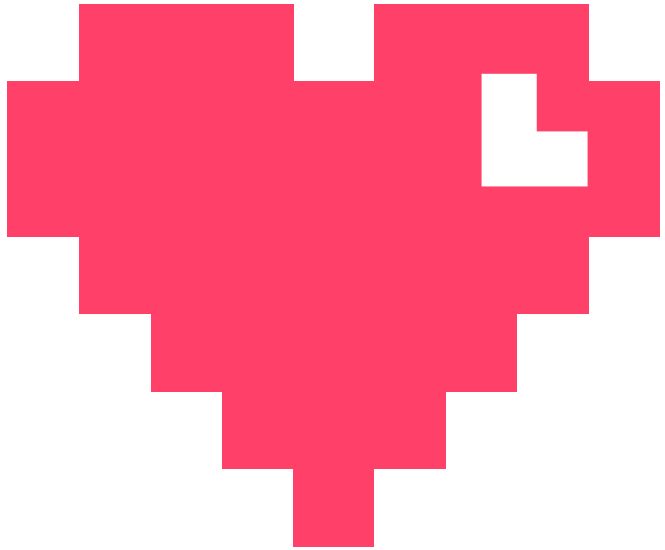
Skolfederation är en **infrastruktur** för skolan.

Skolfederation är inte en centraliserad lösning.

Skolan behöver erhålla egen IdP, hantera sina användare med egna rutiner, tillgodose användarna med inloggningsmetoder som är tillräckligt säkra för ändamålet

Skolfederation

För vissa hög initial tröskel – men väl på plats kommer däremot varje ny integration till tjänst bli enklare och enklare, mer kostnadseffektiv och hållbar i administrationen.



Skolfederation

Vad krävs för en lyckad anslutning?

Samarbete mellan IT och verksamhet för att täppa igen gapet mellan teknik och funktion.

Know-how. Om kunskapen ej finns inom organisationen så är det guld värt att prata med en IT-partner/konsult/integratör.

Hör gärna av er till oss på Skolfederation om ni vill komma igång.
Jag och mina kollegor träffas gärna för att prata igenom era förutsättningar för vägledning och rådgivning.

Skolfederation

Anslutningsprocessen:

Checklista finns här

1. Ta del av avtalet och fyll i webbformuläret
2. Firmatecknare signerar **(i kommun är det)**
3. Åtkomst till hantering av metadata i Skolfederation

Skolfederation

Pris för medlemskap Användarorganisation:

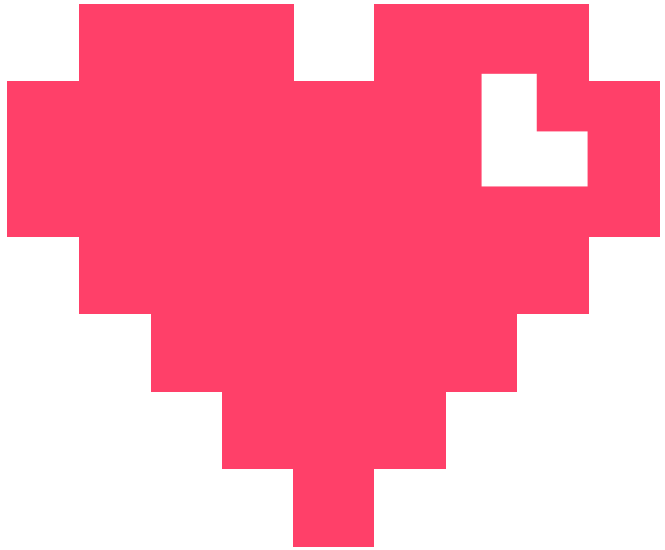
Mycket liten användarorganisation (upp till 100 elever):	1 000 SEK/år
Liten användarorganisation (upp till 500 elever):	5 000 SEK/år
Mellanstor användarorganisation (upp till 5 000 elever):	10 000 SEK/år
Stor användarorganisation (mer än 5 000 elever):	20 000 SEK/år

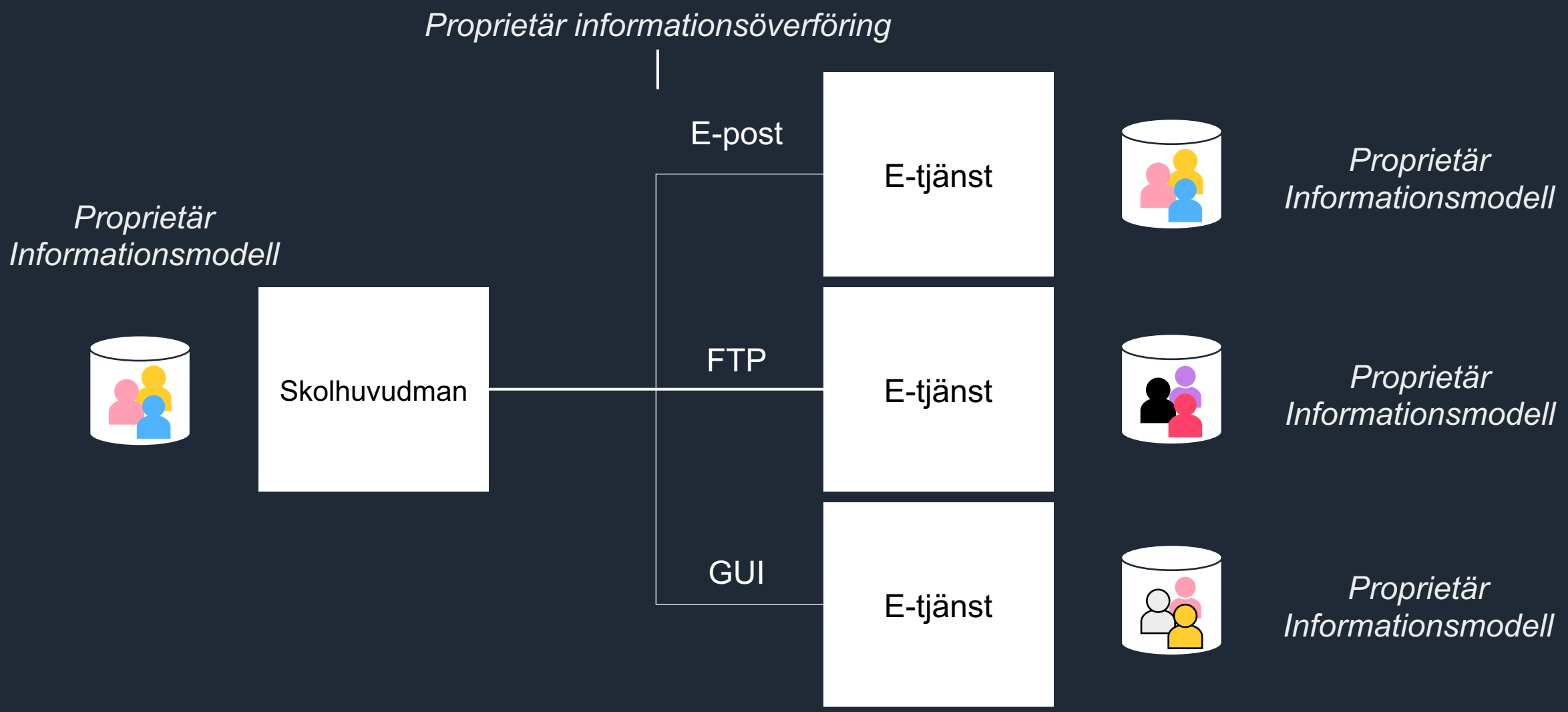
Skolfederation Mini: kostnadsfritt (enbart för Skolverkets tjänster)

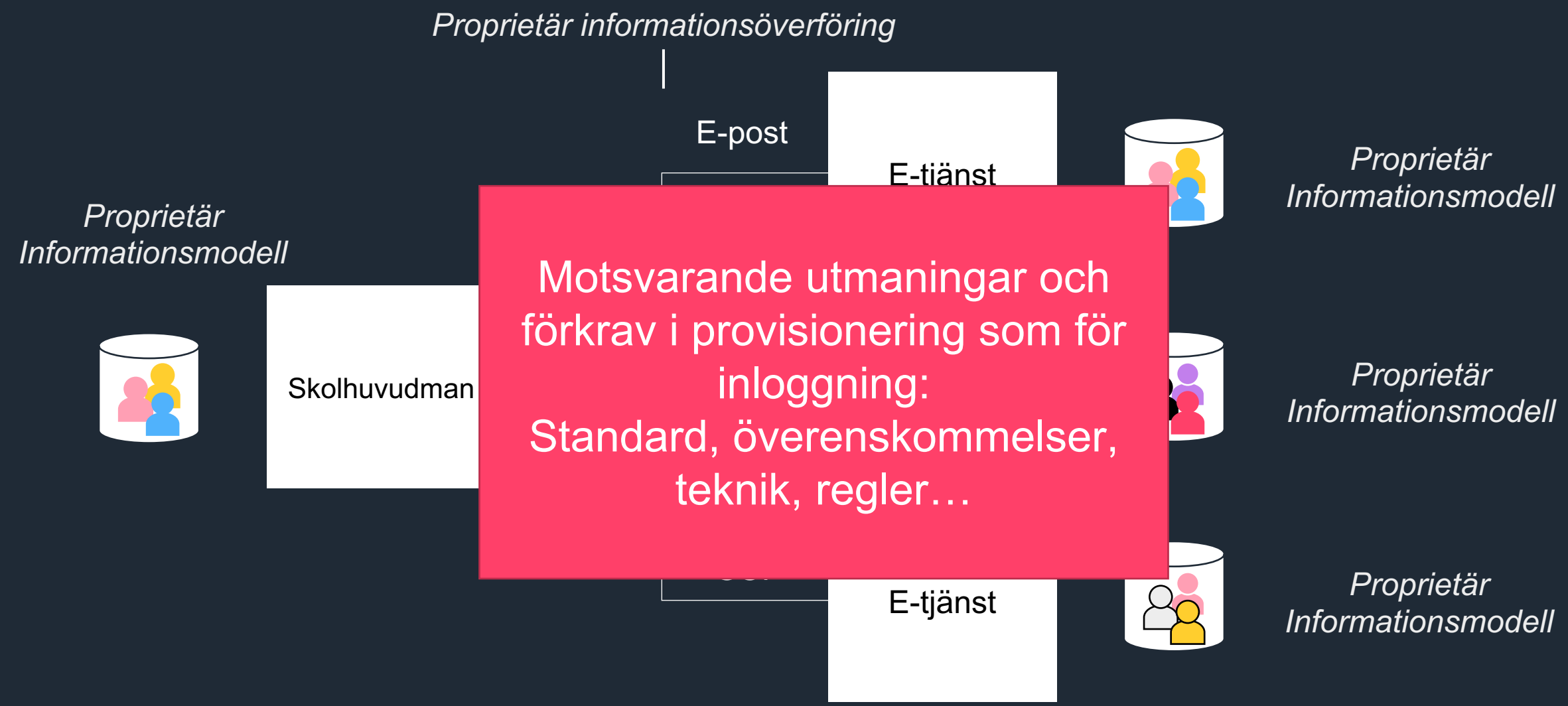
Skolfederation

Federerad provisionering i Moa

Skolfederation har inte stöd enbart för inloggningsflödet, utan även för flödet för automatisk hantering av ”kontouppgifter”, så kallad provisionering.



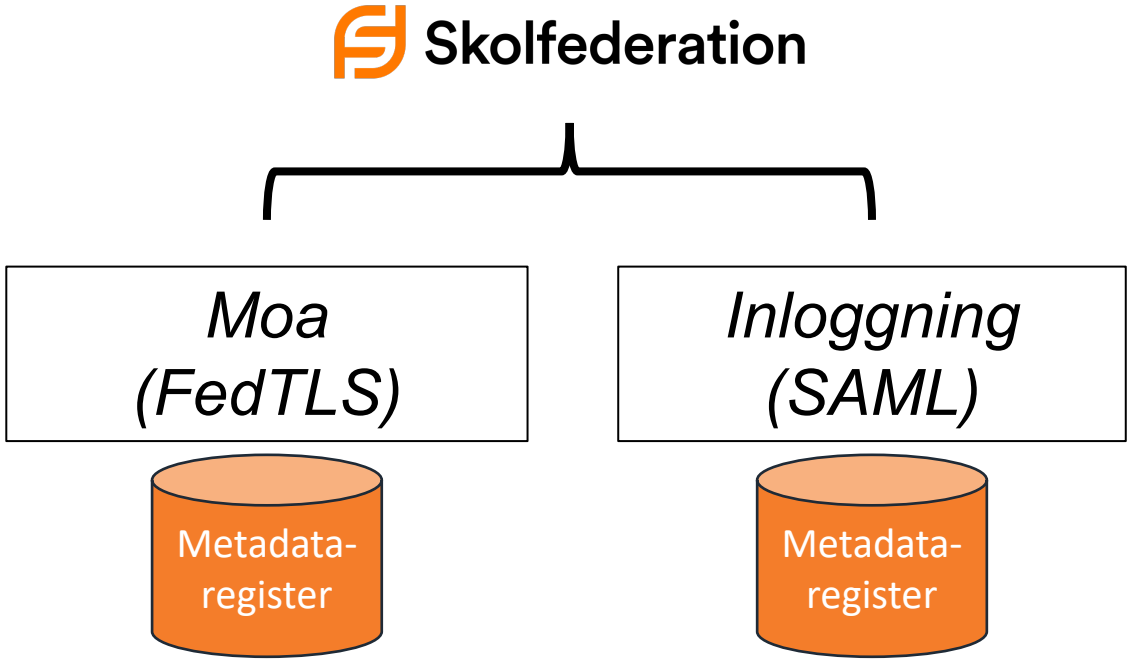

Proprietär informationsöverföring
E-post
FTP
GUI
Proprietär Informationsmodell
Skolhuvudman
E-tjänst
E-tjänst
E-tjänst
Proprietär Informationsmodell
Proprietär Informationsmodell
Proprietär Informationsmodell


Proprietär informationsöverföring
E-post
E-tjänst
Proprietär Informationsmodell
Proprietär Informationsmodell
Skolhuvudman
Motsvarande utmaningar och förkrav i provisionering som för inloggning:
Standard, överenskommelser, teknik, regler…
Proprietär Informationsmodell
Proprietär Informationsmodell
E-tjänst

Skolfederation

Federerad provisionering i Moa

Moa är en teknisk federation som ingår i Skolfederation.



Skolfederation Moa

Autentiserade och säkrade kanaler

Informationsmodell enligt SS12000

Skolhuvudman

Överföringsgränssnitt Enligt SS12000

E-tjänst

E-tjänst

E-tjänst

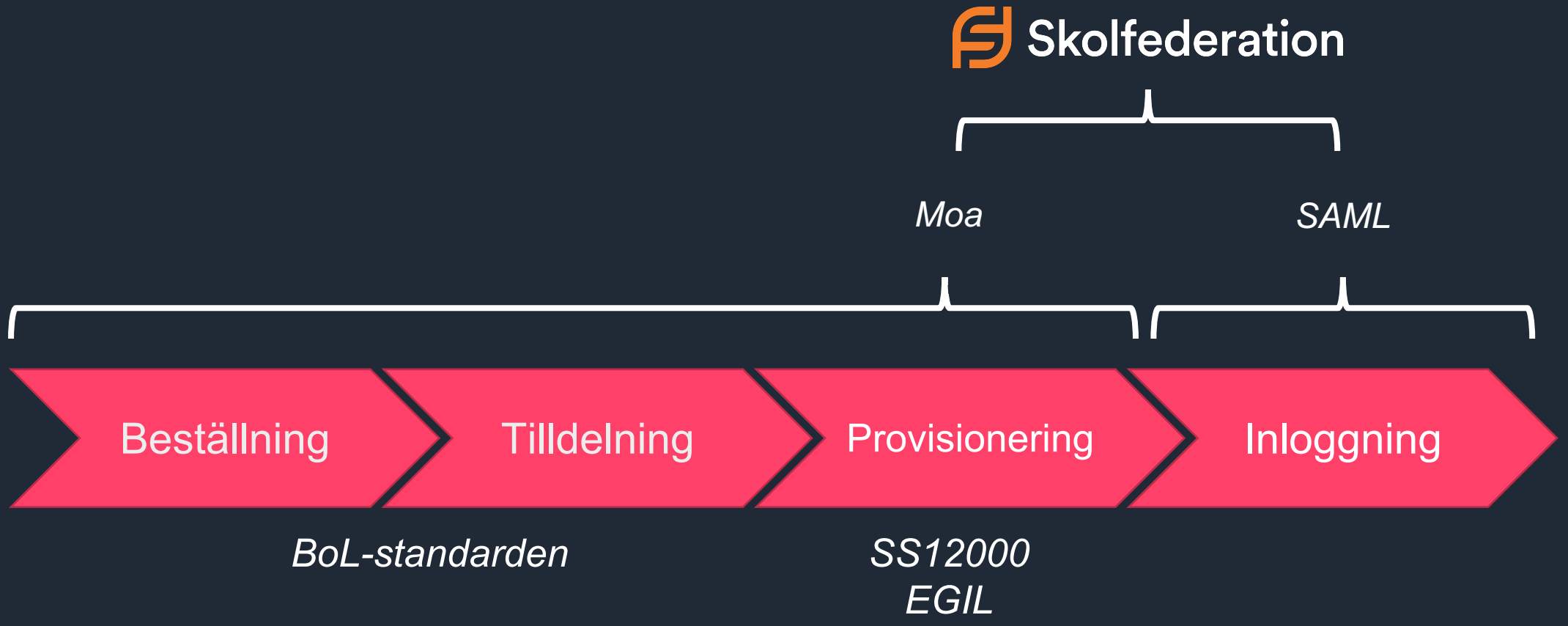
Informationsmodell enligt SS12000

Informationsmodell enligt SS12000

Informationsmodell enligt SS12000

INTERNETSTIFTELSEN

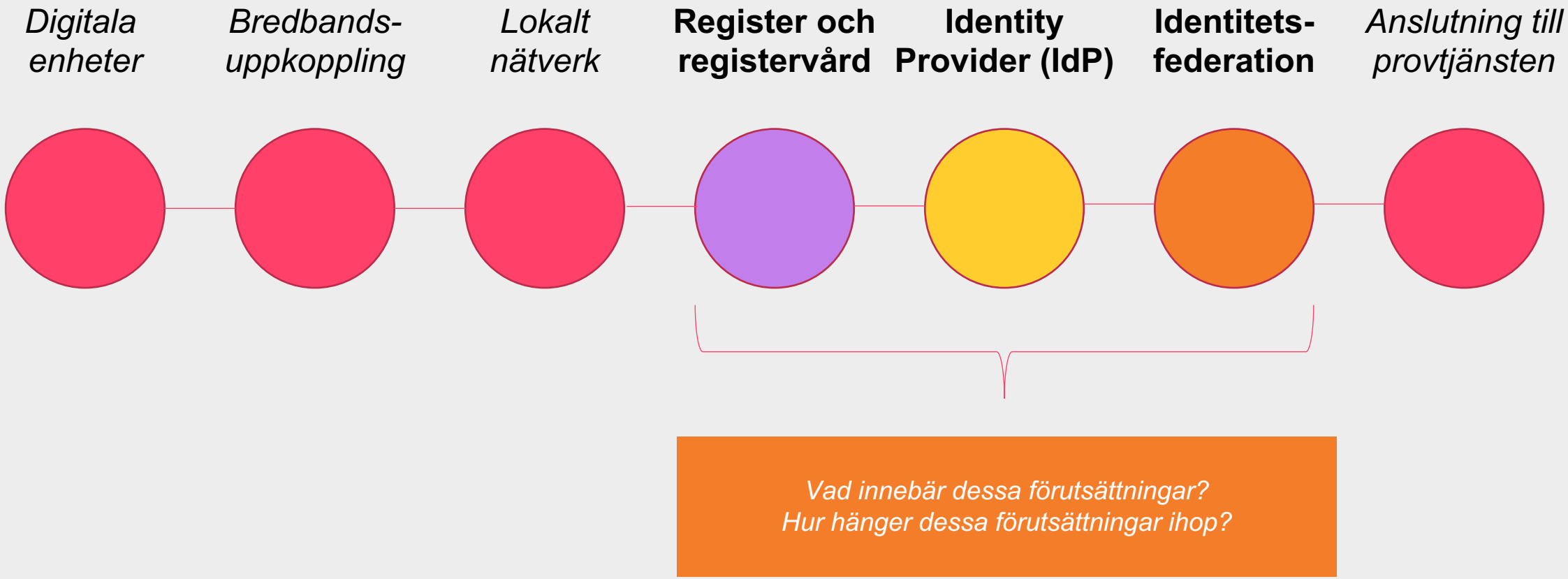
Elektroniska läromedel från ax till limpa



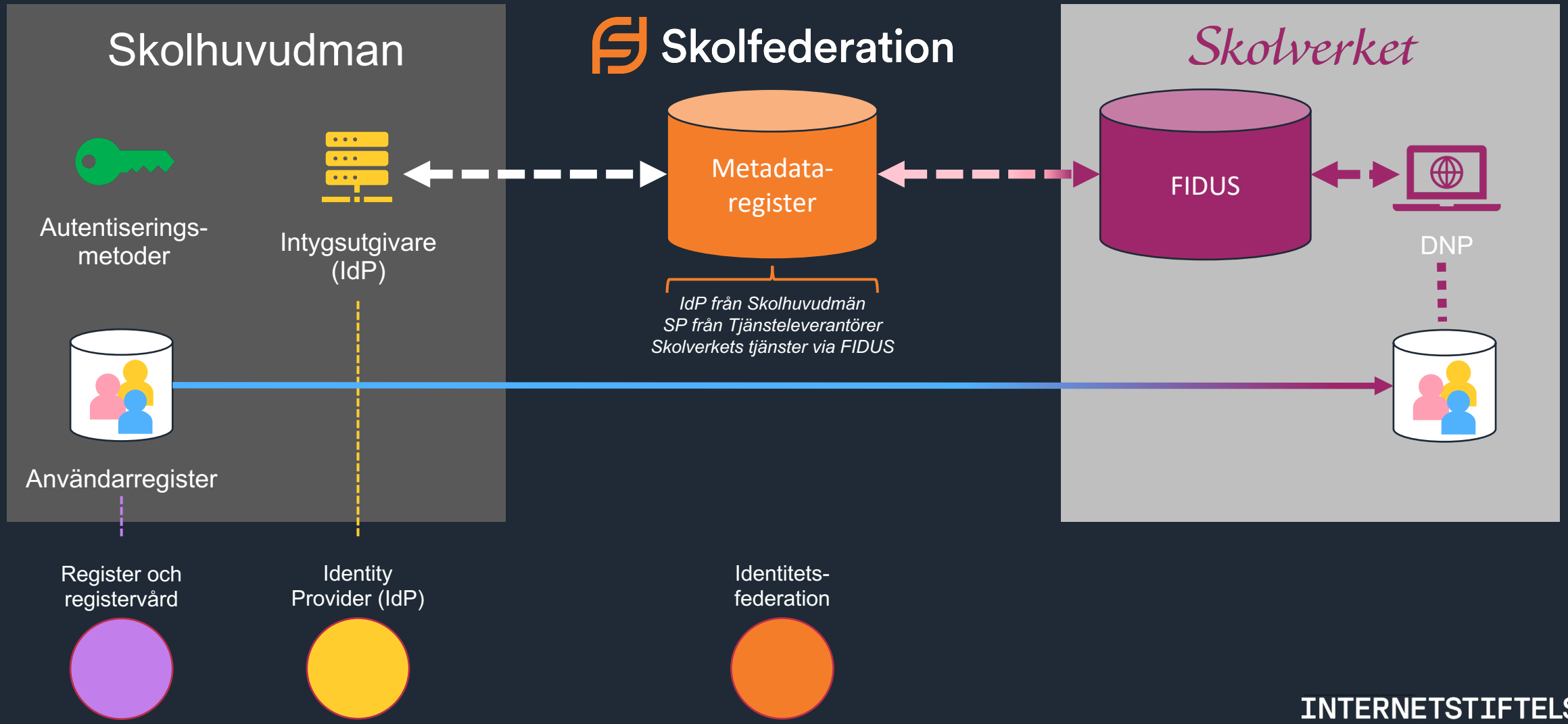
Skolfederation

Digitala Nationella Prov

Tekniska förutsättningar enligt Skolverket



Hur ser lösningen ut?



Identitetsfederation

- Skolfederation är en identitets- och behörighetsfederation (åtkomstfederation)

- Definierar vilka **standarder och krav** som medlemmar måste förhålla sig till – tekniska som organisatoriska

Organisatoriska krav:
Informationssäkerhet
Identitetshantering

Tekniska krav** (bl.a.)**:
saml2int
eGov2

Standarder och krav

Vad berörs av saml2int och eGov2? Jo,

Beskriver ***vad*** som ska användas och ***hur*** det ska användas

Identity Provider (IdP)

Syfte:

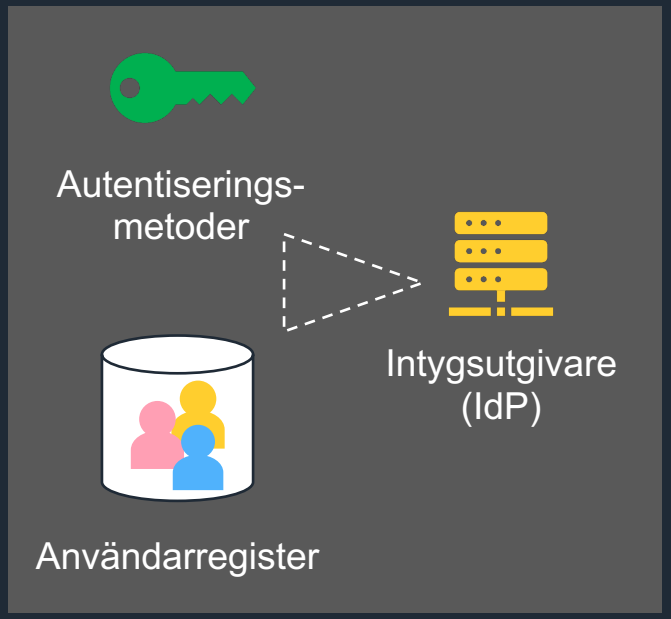
Standarder och krav

Vilka IdP'er har det stödet som krävs?

De flesta moderna IdP-lösningar
- Kommersiella
- Öppen källkod

Kontakta din IT-avdelning (eller leverantör) för att se om er lösning har det stöd som krävs.

Har ni ingen IdP? Kravställ på saml2int och eGov2 vid upphandling. Glöm inte autentiseringsmetoder och anslutning till användarregister.



Google och Microsoft

Vi använder G Suite / MS Azure AD / ADFS, fungerar det?

Ja, men med vissa avsteg eller anpassningar.

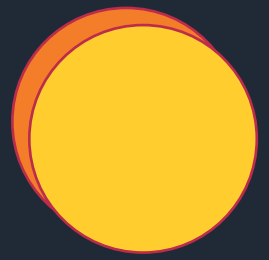
G Suite kräver manuell hantering av metadata.
Skolfederation har en guide för konfiguration av G Suite,
https://gidp.swefed.se

Video finns här!

MS Azure AD / ADFS kan stödja automatisk metadatahantering med extern anpassning via tredjepartsprogram.

Video finns här!

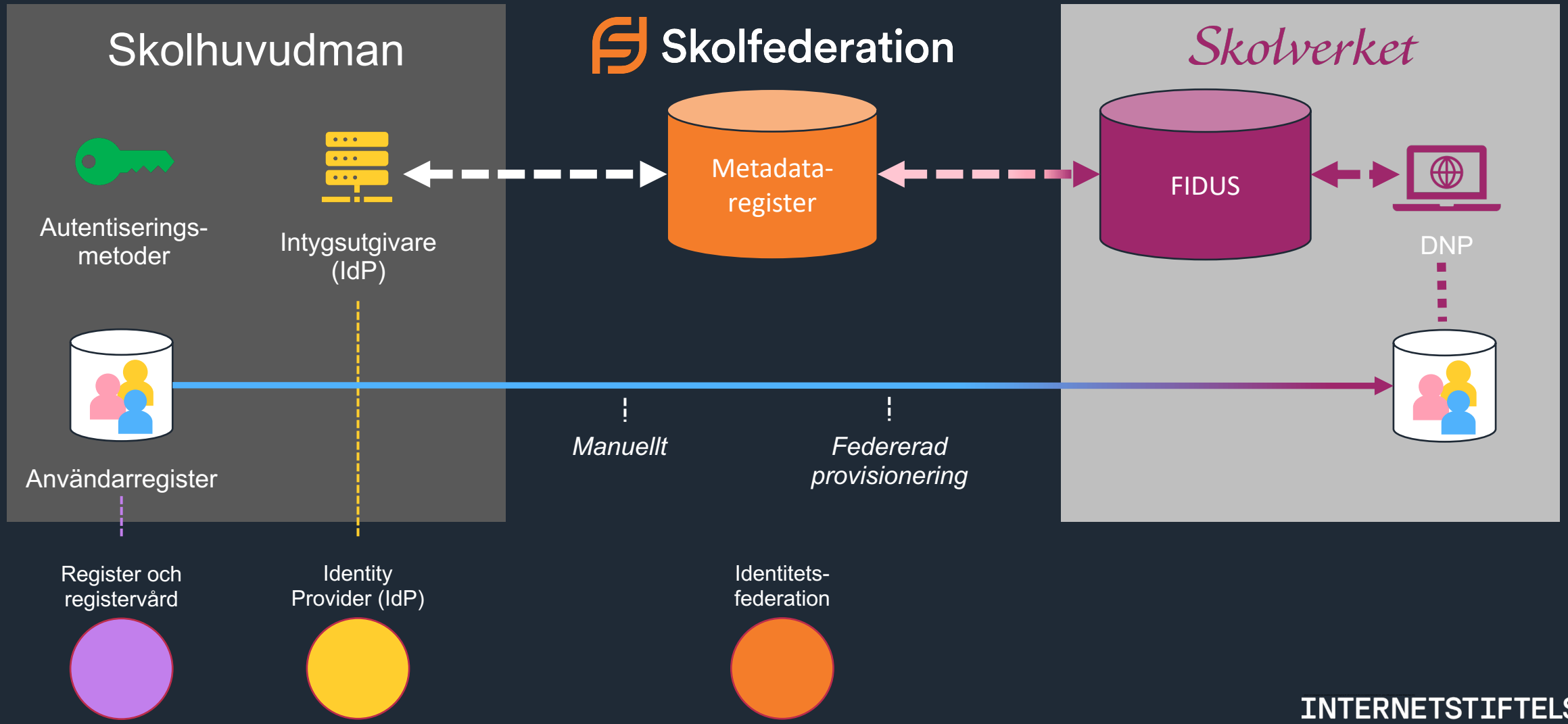
Båda kan lösas med proxy-IdP / SAML-proxy,
det vill säga en komponent mellan federationen och sin lokala IdP



Google och Microsoft

Gör det inte själv. Ta hjälp av er partner!

Registervård

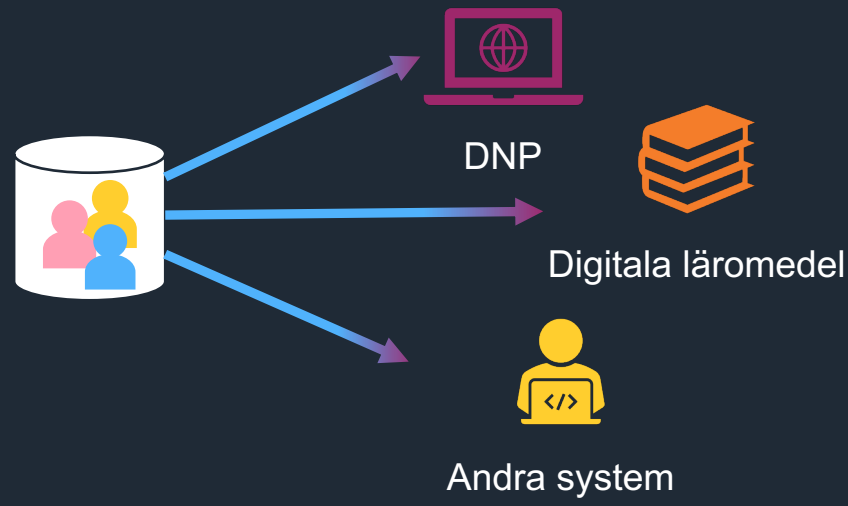


Federerad provisionering

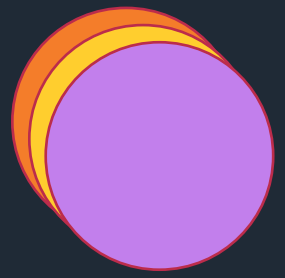
En lösning för att överföra aktuella uppdateringar om elever och personal till medlemmar i en federation

Vid uppdateringar av användare i källsystem sker uppdateringar hos beroende motparter automatiskt

I Skolfederation heter federationslösningen Moa



- För en genomgång av de tekniska grunderna så finns video här.



Federerad provisionering Moa

När bör vi använda federerad provisionering till DNP och andra lärresurser?

När manuell administration av elever och lärare blir för tidskrävande och kostsamt.

När ni vill ha en säkrare lösning (maskiner är mer noggranna än människor)

Manuell hantering

När bör vi hantera användarna manuellt?

När ni är skola där manuell hantering av användarna inför varje provtillfälle känns acceptabelt.

Igen: prata med er IT, leverantör, partner, konsult…

Avslutningsvis…

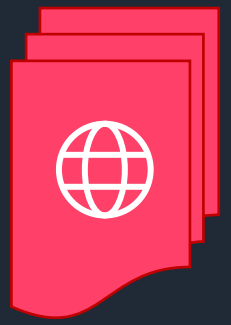
- I vilka register finns de uppgifter som Skolverket kräver?
- Kan ni använda er befintliga IdP? Om inte – erhåll en bra IdP!
  - Kravställ på saml2int (eller ”anslutning till Skolfederation”)
- Gå med i Skolfederation om ni inte är medlemmar - och börja testa

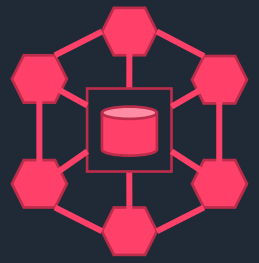
Federation - samverkan

Regler

Standard

Infrastruktur





Frågor?

Tack för att ni lyssnade!

rasmus.larsson@internetstiftelsen.se
info@skolfederation.se

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

INTERNET STIFTELSEN