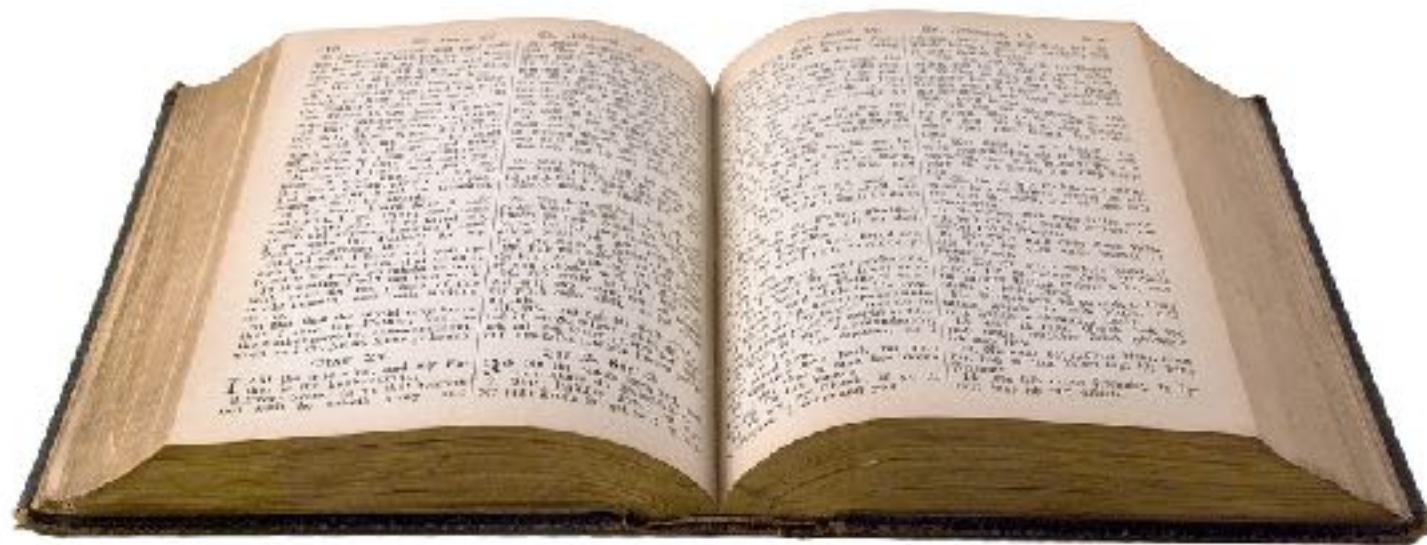


SCIM för digitala läromedel

Jakob Schlyter & Palle Girgensohn







Bakgrund & frågeställningar

Vem har köpt vad?

Hur överförs informationen?

Vad för information överförs?

Hur underhålls informationen?

Hur raderas informationen?

Möjliga lösningar

Centraliserad dataöverföring

- En gemensam integrationstjänst hämtar/får uppgifter från skolhuvudmän
 - ▶ Lokala kataloger, administrativa system, molntjänster
- Läromedelsföretagen hämtar uppgifter från den gemensamma integrationstjänsten

Distribuerad dataöverföring

- Direkt utbyte av data mellan skolhuvudmän och läromedelsföretagen
- Hur man kommunicerar ("protokoll") och identifierar varandra standardiseras
- Inget beroende av centralpunkt

SCIM för digitala läromedel

Förslag till lösning

- SCIM som protokoll för dataöverföring mellan skolhuvudmän och läromedelsföretag.
- Autentisering med stöd av Skolfederation.
- Lokal auktorisation baserat på beställningar.

Protokoll

- SCIM – System for Cross-domain Identity Management – enligt RFC 7642

Säkerhetsfunktioner

- SCIM över HTTPS enligt RFC 7644
 - ▶ Krav på protokoll och chifferuppsättningar
- Ömsesidig autentisering via TLS
 - ▶ Federering av certifikat via metadata publicerad av Skolfederation

Attribut

- Attribut enligt RFC 7643
 - ▶ SCIM Core
- Attribut enligt SS 12000
 - ▶ SIS/TK 450 (IT standarder för lärande) AG9
 - ▶ Elever, lärare, undervisningsgrupper, skolor

Vad behövs?

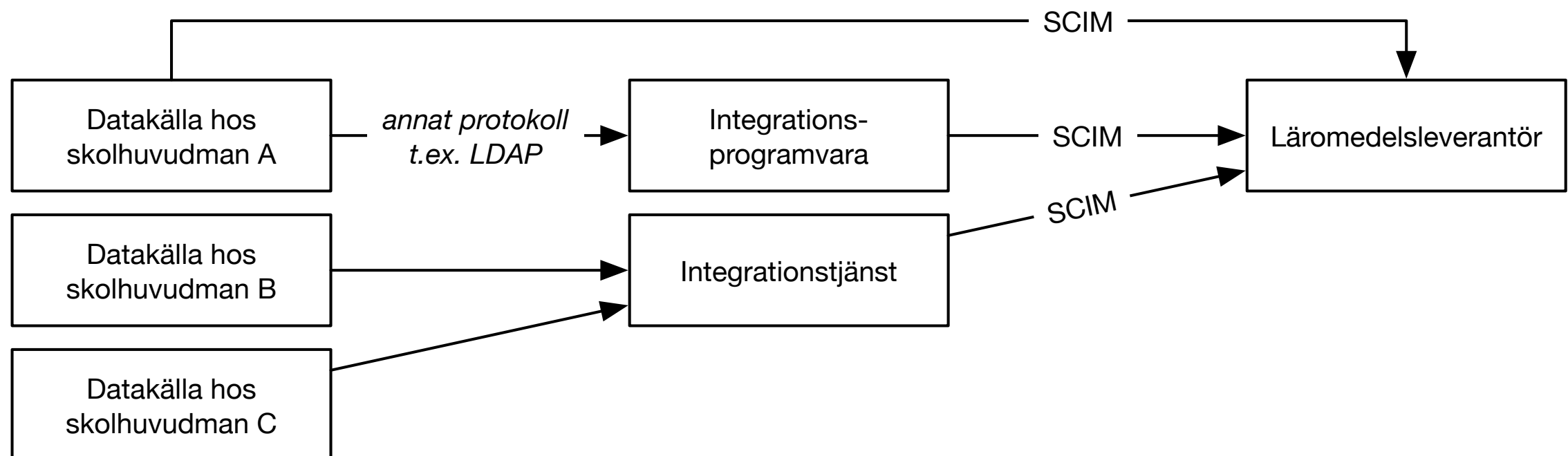
Skolhuvudmän

- Programvara för att synkronisera vald data från elevregister till leverantörer.
- Integrationstjänster kan användas förutsatt att de anpassas till SCIM.

Läromedelsföretag

- Implementation av SCIM-gränssnitt

Dataflöde



Persondataskydd

Dataminimering

- Vilka uppgifter **måste** läromedelsföretaget ha för att leverera tjänsten?
 - ▶ Adam Bertil Carlsson 20100211-9999 i 2 A
 - ▶ Bertil i 2 A
- Vad krävs för att pedagogerna skall kunna identifiera eleven?

Datamaximering

- Integrationstjänster medför koncentration av data från flera parter och därmed större exponering
- Vad innebär en läcka hos en integrationstjänst?
 - ▶ Personuppgiftsbiträden enligt PUL/GDPR
 - ▶ Är anslutna läromedelsföretag underentreprenörer?

Inloggning

- Hur kopplas inloggningsuppgifter till redan överförda personuppgifter
 - Användarnamn (t.ex. EPPN)
 - SAML NameID

Nästa steg

Förslaget på remiss

Testmiljö

<https://www.kirei.se/tmp/scim20170602/>

jakob@kirei.se

girgen@pingpong.net