kirei

Rapport

2017-06-01

Svenska Läromedel
Kirei 2017:30 (R.20797)

SCIM för digitala läromedel

Introduktion

Den kommande standarden SS12000 specificerar hur verktyg och system för skolor kan utbyta information om elever, lärare, utbildningsgrupper, klasser, ämnen, kurser och skolschema. Syftet med den standarden är förvisso att kommunicera skolans schema, men den grund av klasser och utbildningsgrupper som den kräver är i stort desamma som de behov ett vanligt digitalt läromedel har.

Syftet med detta dokument är att presentera en gemensam profil av SS12000 som läromedel och elevregister kan använda för att på ett skalbart sätt göra det möjligt att koppla olika elevregister med läromedel från olika leverantörer med samma underliggande teknik och samma gränssnitt (API). Profilen beskriver också ett antal säkerhetsfunktioner för att säkerställa korrekt identifiering av de kommunicerande parterna, samt en gemensam lägsta nivå för transportskydd. Protokoll

SCIM enligt RFC 7642 används för all kommunikation. För datatransport används SCIM över HTTP (HTTP/1.0 eller HTTP/2) enligt RFC 7644.

Säkerhetsfunktioner

Autentisering

Säker kommunikation mellan klienter och servrar implementeras genom TLS med ömsesidig autentisering enligt separat specifikation, https://github.com/kirei/scim-fed-auth/. Den metadata som krävs för att implementera detta föreslås koordineras och hanteras av Skolfederation. Det bör dock påpekas att metadata för SCIM hanteras separat från den metadata som används för t.ex. SAML, och att det inte finns något direkt beroende på Skolfederation.

Transportskydd

All kommunikation skall skyddas av HTTPS med TLS version 1.2 eller senare, och endast chifferuppsättningar som resulterar framtida sekretesskydd (Perfect Forward Secrecy, PFS), t.ex. ECDHE/DHE, får användas.

Auktorisation

Denna specifikation definierar inte mekanismer för att styra vem som får åtkomst till vilken information. Säkerhetsfunktionerna möjliggör för de kommunicerande parterna att autentisera sig mot varandra, och efter det är det upp till mottagande system att auktorisera ett sändande system baserat på befintliga affärsmässiga avtal.

Persondataskydd

De ökade kraven på persondataskydd inom EU (GDPR) påverkar överföring av personuppgifter mellan skolhuvudmän och läromedelsleverantörer. För att möta dessa krav rekommenderas att den information som överförs är så begränsad som möjligt (“dataminimering”) samt att olika former av pseudonymisering används för att minska behovet av känsliga personuppgifter.

I många fall räcker det att användare beskrivs med kortare namn (t.ex. “Adam” eller “Eva N”), dvs det namn som normalt sett används i klassrummet och därmed är tillräckligt för att en pedagog skall kunna identifiera eleven i verksamheten. Det kortare namnet kan fördel överföras genom attributet “displayName”. Fullständigt namn och/eller personnummer (“civicNo”) bör inte användas om inte särskilda skäl föreligger.

Då system för läromedel i de allra flesta fall inte är konstruerade för att hantera skyddade personuppgifter får användare med skyddad identitet inte överföras utan pseudonymisering. Den pseudonymiserade identiteten anses i detta fall inte vara skyddad.

Inloggning

Vid en federerad inloggning överförs oftast någon form av identitet på användaren. Denna identitet kan vara tillfällig eller permanent, och är i många fall unik per e-tjänst.

Förutom användaridentiteten överförs ofta ett antal attribut för att kunna knyta användaren till bakomliggande system. Ett vanligt förekommande attribut för att koppla användare är EPPN (“eduPersonPrincipalName”) som kan motsvara attributet “userName” i SCIM, men det finns även lösningar där mer pseudonyma attribut kan användas för att koppla samman identiteter.

Attribut

Följande attribut, hämtade från RFC 7643 och SS12000, används av SCIM för svenska läromedel. Notera att vissa attribut har begränsningar vad gäller användning.

Användare

Följande schemata och attribut som beskriver individuella användare (User Resource) används:

- urn:ietf:params:scim:schemas:core:2.0:User
  - userName
  - name
  - displayName
  - nickName
  - preferredLanguage
  - locale
  - timezone
  - active
  - emails
  - phoneNumbers
  - groups
  - entitlements
  - roles
- urn:scim:schemas:extension:sis:school:1.0:User
  - enrolments

Attributet "password" *får inte* användas – användare måste logga in med federerade identiteter via Skolfederation eller annan fristående infrastruktur för autentisering.

Attributet "civicNo" *bör inte* användas utan särskilda skäl.

Användare som hanteras enligt denna profil får inte vara sekretessmarkerade via attributet "securityMarking" (se avsnittet om persondataskydd).

Grupperingar

Attribut som beskriver grupper av användare (Group Resource) och undervisningsgrupper, t.ex. klasser (Student Group Resource) hämtas från följande schemata:

- urn:ietf:params:scim:schemas:core:2.0:Group
- urn:scim:schemas:extension:sis:school:1.0:Group
- urn:scim:schemas:extension:sis:school:1.0:StudentGroup

Skolor och skolenheter

Attribut som beskriver skolor (School Resource) och skolenheter (SchoolUnit Resource) hämtas från följande schemata:

- urn:scim:schemas:extension:sis:school:1.0:SchoolUnit
- urn:scim:schemas:extension:sis:school:1.0:School

Aktiviteter

Aktiviteter beskriver en aktivitet för en studentgrupp, med ämne eller kurs, samt vilken eller vilka som är lärare för just det ämnet. Lärare kopplas dessutom till aktiviteten via en anställning.

- urn:scim:schemas:extension:sis:school:1.0:Activity
- urn:scim:schemas:extension:sis:school:1.0:Employment
- urn:scim:schemas:extension:sis:school:1.0:Course
- urn:scim:schemas:extension:sis:school:1.0:Subject

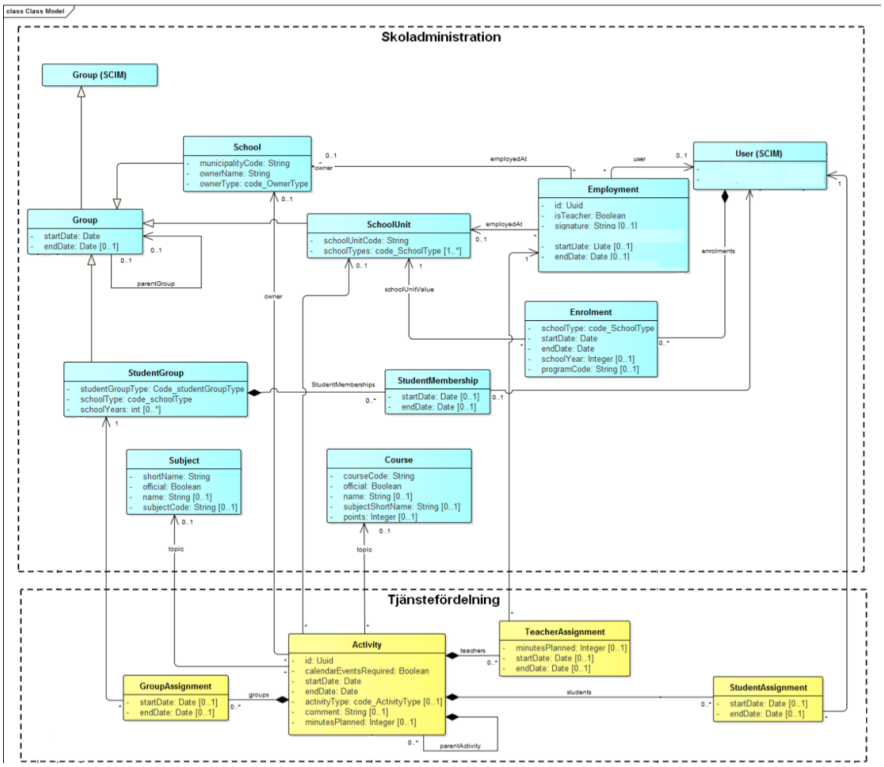
Inskrivning i skola

En elev ska vara inskriven vid exakt en skolenhet vid en given tidpunkt. Det beskrivs med en inskrivning:

- urn:scim:schemas:extension:sis:school:1.0:Enrolment

Domänmodell

De resurser och attribut som används i SS12000 sammanfattas i nedanstående domänmodell:



Figur 1 – Domänmodell