# New person from institutional source, midPoint variant

- midPoint would be fed “System of Record” (SoR) data over SCIM RESTful APIs

    a. First iteration will rely on the self-registration UI already running in the original testbed VM as the demo System of Record.
    b. For now we will use a midPoint “connector” that maps from SCIM to native midPoint RESTful APIs. The connID framework will be the basis for building connectors. Eventually we expect midPoint to speak SCIM natively.

- midPoint would be configured to provision person information into LDAP (using its delivered LDAP connector)

- Grouper would be configured to use midPoint as a person subject source (using either a to-be-developed a SCIM-based Subject API implementation or LDAP or SQL)

    a. Hook up the PSU SCIM server?
    b. Overhead of REST….killer? LDAP/SQL as subject source is faster (and can be tuned)
    c. Grouper assumes millisecond-level responses, if API is 200 milliseconds, that’s not gonna fly; with SQL, searches are slow over 800K, with a text string

- Provisioning rules in midPoint would also use SoR data to determine which “base” or “reference” groups people belong to (faculty or student in this scenario)

    a. Idea or role based group is different than service eligibility groups.
        i. E.g. consider “faculty” category - could have different definitions amongst business/enterprise vs. academia (for example, professors emeritus might not be considered faculty by businesses)

- Use the delivered Grouper UI to create and manage membership of groups other than the base set.

- Person attributes and group memberships would be reflected into LDAP from midPoint and Grouper respectively. Might allow access to Grouper, LDAP and SQL

- To construct attribute assertions, the Shibboleth IdP will pull attribute values from one or more of LDAP, midPoint and Grouper (design decision point). UDub: LDAP and Group API; Hawaii: LDAP; UW-Madison: LDAP, HA Database (groups are filtered per SP)

- The demo web-SSO “LMS” application will be a simple web app running on an Apache httpd server on paths protected by a Shib

- Configure the sample Service Provider application to use Shibboleth as its Web SSO mechanism

  2) Configure requested attributes element on Shib session protected endpoints, ask for displayName and isMemberOf

  3) Have registered users browse to the protected application

  4) Users authenticate at their IDP

  5) Depend on LDAP for the initial user authentication behind the IDP, Release attributes X, Y, Z to the SP application

  6) If authenticated user isMemberOf the Instructor Group, show a hello {name} “Course Design” page

  7) If authenticated user isMemberOf the Learner Group, show a hello {name} “Course Catalog” page

---

Include/exclude, Eligibility and Authorization Groups also have a part to play. Check with Bill Thompson

[Keith] Create midpoint.testbed.tier.internet2.edu dashboard with LDAP info, mySQL info, etc. as shared cheat sheet for multiple developers.