Integrating Applications with NetID Login, Manifest and Person Data Delivery Services

Charlie Calderón <charles.calderon@wisc.edu>
Tom Jordan <tom.jordan@wisc.edu>
Jon Miner <jon.miner@wisc.edu>
Applications generally need a few things:

1. A way to define and populate user data within the application (provisioning)

2. A way to prove a user's claim of identity (authentication)

3. A way to determine what roles and permissions a user should have (authorization)
Defining an identity lifecycle

Defining a provisioning strategy:

● Who are the users of the application?
● What data does the application need to know about them?
● When does the application need to know? (Pre-provisioning vs. JIT)

Understanding identity lifecycle:

● When do they become eligible for the application?
● When do they stop being eligible?
● What data drives eligibility?
● What do the onboarding and offboarding processes need to accomplish?
Authentication Considerations

Who are the users?

- All from UW-Madison? Other campuses? Other HE institutions?

Who’s doing the authenticating?

- Are we allowing other institutions’ users to log in?

What’s the required security context?

- Do we require any special security considerations (forced-reauth, MFA, etc)?
Authorization Considerations

Determining application roles:

- What are the different roles / access levels within the application?
- What data drives them, and where is it maintained?
- How does the application need to consume role data?

Defining an authorization / grouping strategy:

- Data-driven grouping
- Ad-hoc group information
- Intersection ("in my ad-hoc group and also still employed")
An integrated SAML web application

Person data:
- Unique identifiers
- Preferred Name
- Official Email
- Etc.

Group Memberships:
- Authorized for App X
  - Current Employee
- Admins of App X
  - Employee of UDDS Y
  - Ad Hoc Admins
Other tools in the toolkit..

Not every app is well heeled. Sometimes we need other tools for integration:

- Integration with directory service (AD, LDAP) for authentication, group membership, or person data

- Direct provisioning via flat file, database view, etc

- Scripted deprovisioning to look up eligibility data and perform batch deprovisioning
Questions?