

# Solving Identity Management Challenges with Community-Built Software

Case Studies from the 2020 CSP  
IAM Online - March 11, 2020

- ❖ Tommy Doan, Southern Methodist University
- ❖ Ethan Kromhout, University of North Carolina at Chapel Hill
- ❖ Lacey Vickery, University of North Carolina at Charlotte
- ❖ Keith Hazelton, Internet2



InCommon®

# University of North Carolina at Chapel Hill

Ethan Kromhout

## Project Overview: Identity and Lifecycle Management

UNC previously embraced Grouper and Shibboleth  
Main CSP goal rollout midPoint as provisioning engine  
Initial provisioning target is Google  
midPoint to provision based on Grouper access policy

# Strong CSP overlap with Incommon Collaboration Platform

InCommon®

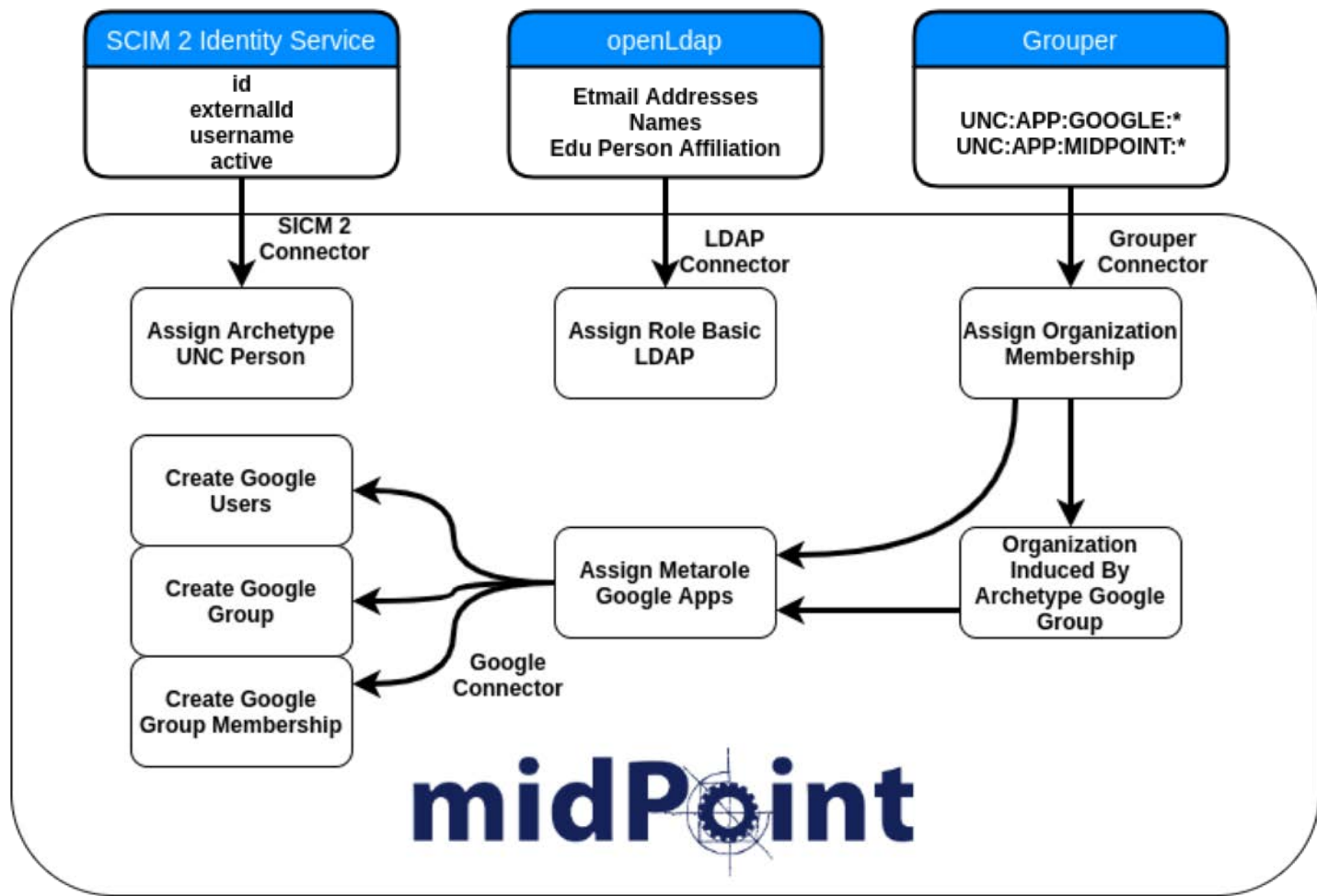


midPoint



midPoint







InCommon®

# University of North Carolina at Charlotte

Lacey Vickery

# Project Overview: Access Management



Shibboleth.



UNC Charlotte's current group management strategy consists of home grown scripts and Ad Hoc groups being maintained in Active Directory.

Access management use case: GitHub Enterprise utilizes just in time provisioning with no method to check attributes for access control. This means a license seat is taken for any user with the ability to authenticate.

Our goal for the Collaboration Success Program is to have Grouper provision groups to AD and use the PEP (policy enforcement point) access control model to block access to GitHub at the IdP.

## Project Overview: Access Management

Access to training and subject matter experts through the Collaboration Success Program has allowed us to implement Grouper on an accelerated timeline.

The use of Docker has streamlined the install process and removed the burden of server configuration and management.

Grouper will eventually handle application access decisions as well as provisioning determination based on attributes.

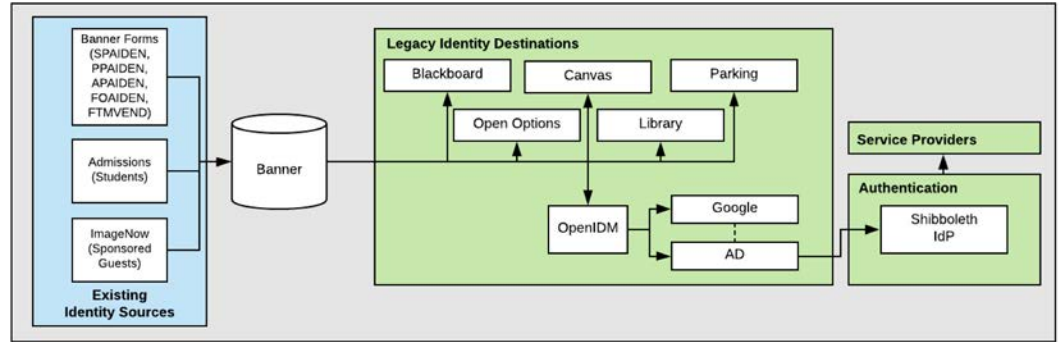
We are also looking at other TAP components, specifically MidPoint, to replace our current proprietary provisioning system.



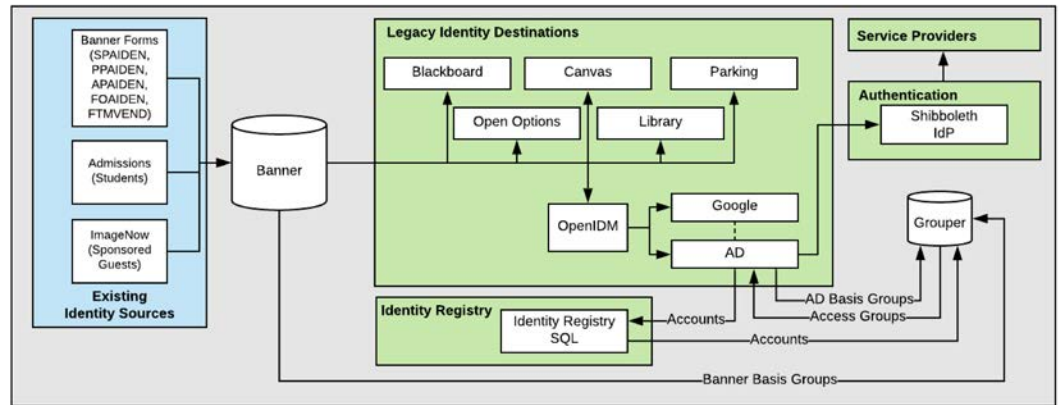


# Project Overview: Access Management

## Current Model



## Phase 1: Access Management CSP





# Southern Methodist University

Tommy Doan

# Project Overview: Long-Term IAM Roadmap

## **Where we are:**

Existing custom-built provisioning system built on PeopleSoft.

University members are managed quite well.

Sponsored users are managed relatively well, but there are problems.

PeopleSoft is currently the only Source of Record for identities.

# Project Overview: Long-Term IAM Roadmap

## What's coming up:

Motivation to move IAM to its own independent system.

Additional constituents from new Sources of Records are coming very soon:

- Non-credit SIS
- Donor management system
- Rec Center management system
- Sponsored user (aka guest) management system

# Project Overview: Long-Term IAM Roadmap

## Challenges we face:

Matching "new" incoming users to existing identities.

Grouping users into meaningful populations for access control, etc.

Enhancing our sponsorship model to better support:

- Real-time guest enrollments
- Transient guests who require IT services for a few days
- Longer-term users who require a sponsor
- Employee-equivalent users hired through a contracting agency

# Project Overview: Long-Term IAM Roadmap

## **The major components we lack are:**

- Central person registry
- Grouping system
- Guest management system
- A replacement provisioning system

# Project Overview: Long-Term IAM Roadmap

## What we are considering:

1. Commercial IAM solutions.
  - a. We have concerns about:
    - i. Their management of various sponsored user populations
    - ii. Their grouping mechanism
2. Open source opportunities.
  - a. The CSP has opened our eyes to the viability of Grouper and COmanage.
3. Some combination of commercial solutions and open source solutions.

Interested in Learning More?

Keith Hazelton



# Interested in Learning More about the CSP?

1. Complete a brief expression of interest form at <https://www.surveymonkey.com/r/CSP2021> by June 30th
2. Talk to us about your plans in a scheduled call
3. Review the training opportunities at <https://www.incommon.org/academy/library/>
4. Learn about the program details and fees at: <https://www.incommon.org/academy/cspdetails/>
5. Other questions? Email [help@incommon.org](mailto:help@incommon.org) or visit <https://www.incommon.org/academy/csp/> for more information



Questions?

# InCommon Trusted Access Platform Training



May 19-20            COmanage (virtual)

June 2-3             Grouper (virtual)

July/August         Shibboleth (virtual - dates TBA)

Details and registration at [www.incommon.org/academy](http://www.incommon.org/academy)

# BaseCAMP 2020



InCommon BaseCAMP - June 23-25 - Milwaukee, Wisconsin

For those new to IAM, Federation, and/or the InCommon Trusted Access Platform

Program and registration links: <https://meetings.internet2.edu/2020-basecamp/>

# IAM Online Evaluation



<https://www.surveymonkey.com/r/IAMOnline-March2020>