HARVARD UNIVERSITY
Information Technology

IAM Group Services

Nov. 28, 2018 | Overview Presentation | Terry Connolly

Groups Enable Other IT Services

Groups are a critical component of these IT Services	
Access Control (available now) (start in FY19)	• Enable application access for eligible users (authorization) • Authorization options through HarvardKey & API • Automatically removes access as eligibility ends • Authorization options through H-LDAP/AD Groups
Communication (start in FY20)	• Email or texting messaging to targeted audiences • Broadcast Communications
Collaboration (future)	• Simplify document sharing to collaborators • Enable controlled file sharing (individuals and groups)

IAM Group Services Overview

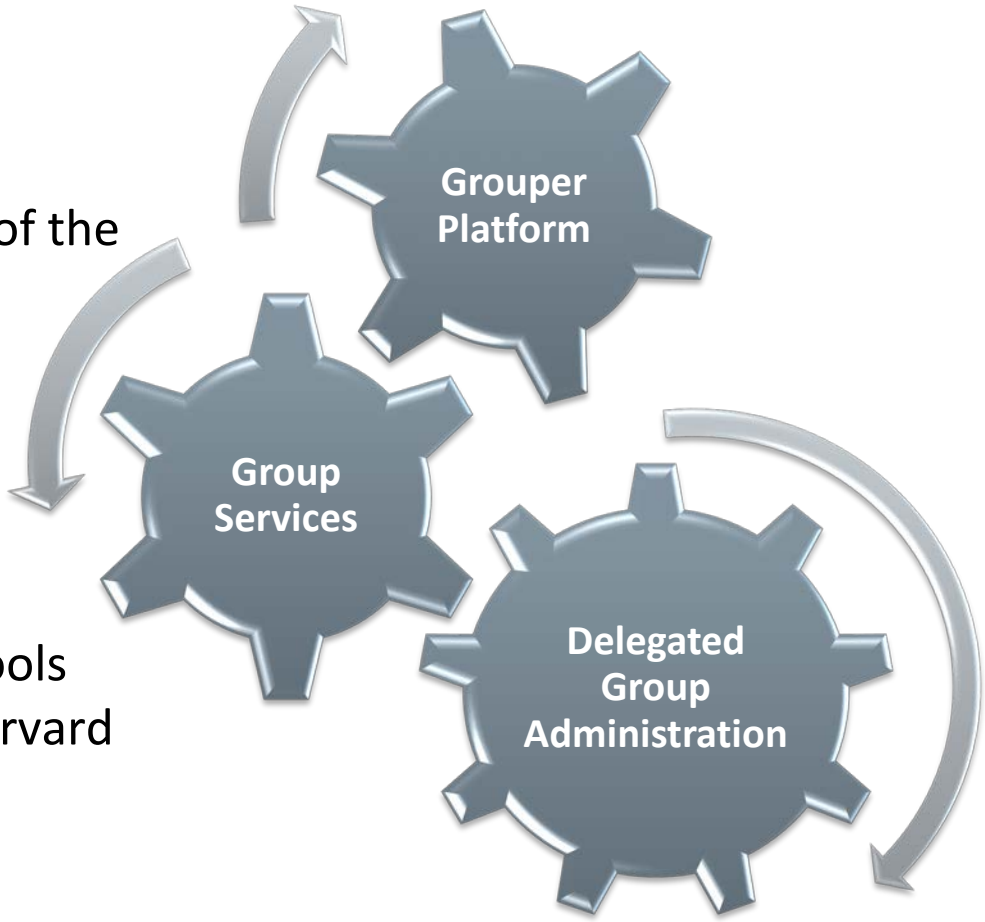
Group Services

…drives the evolution of the

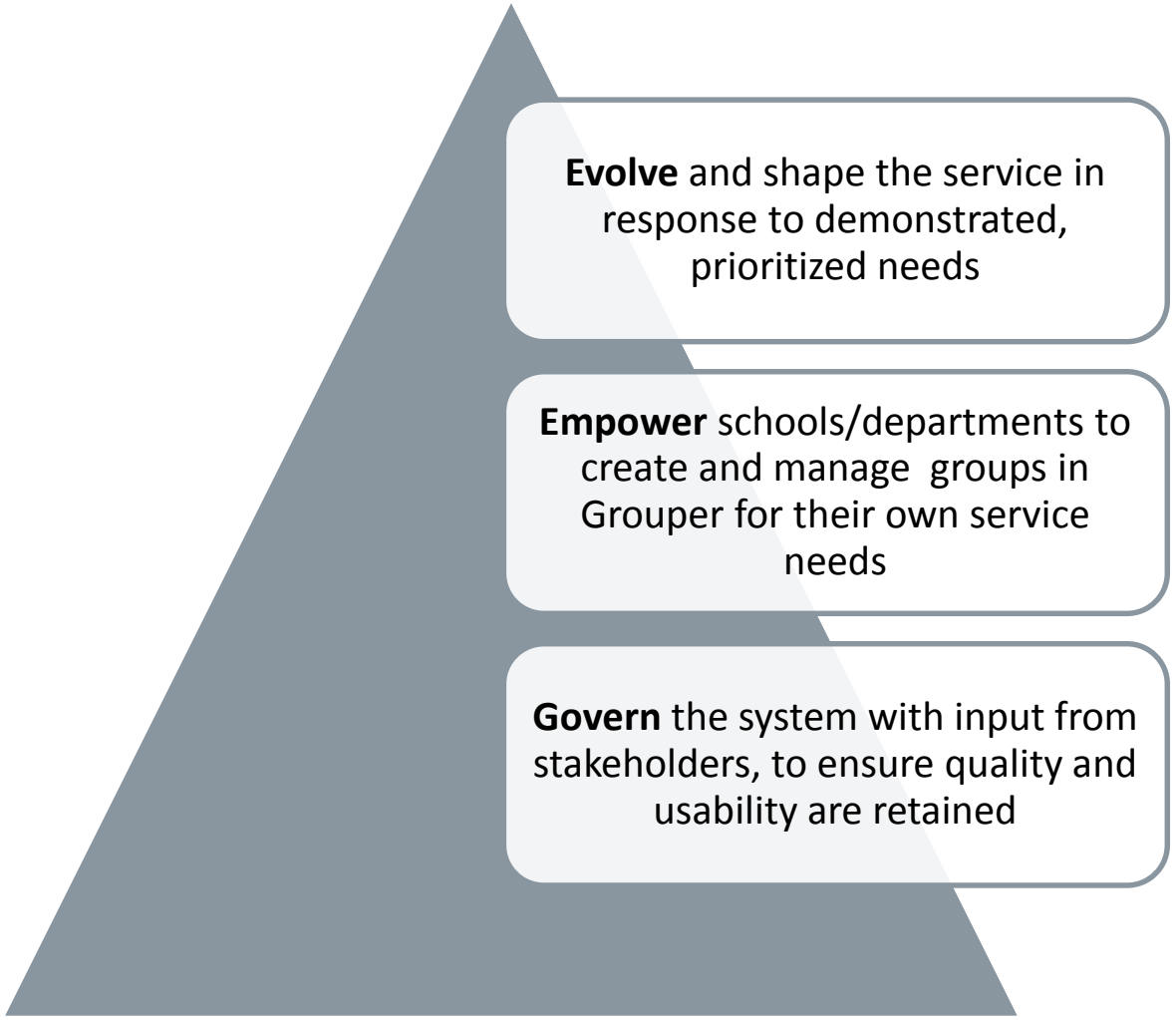
Grouper Platform

…and the adoption of

Delegated Group Administration by schools and departments at Harvard

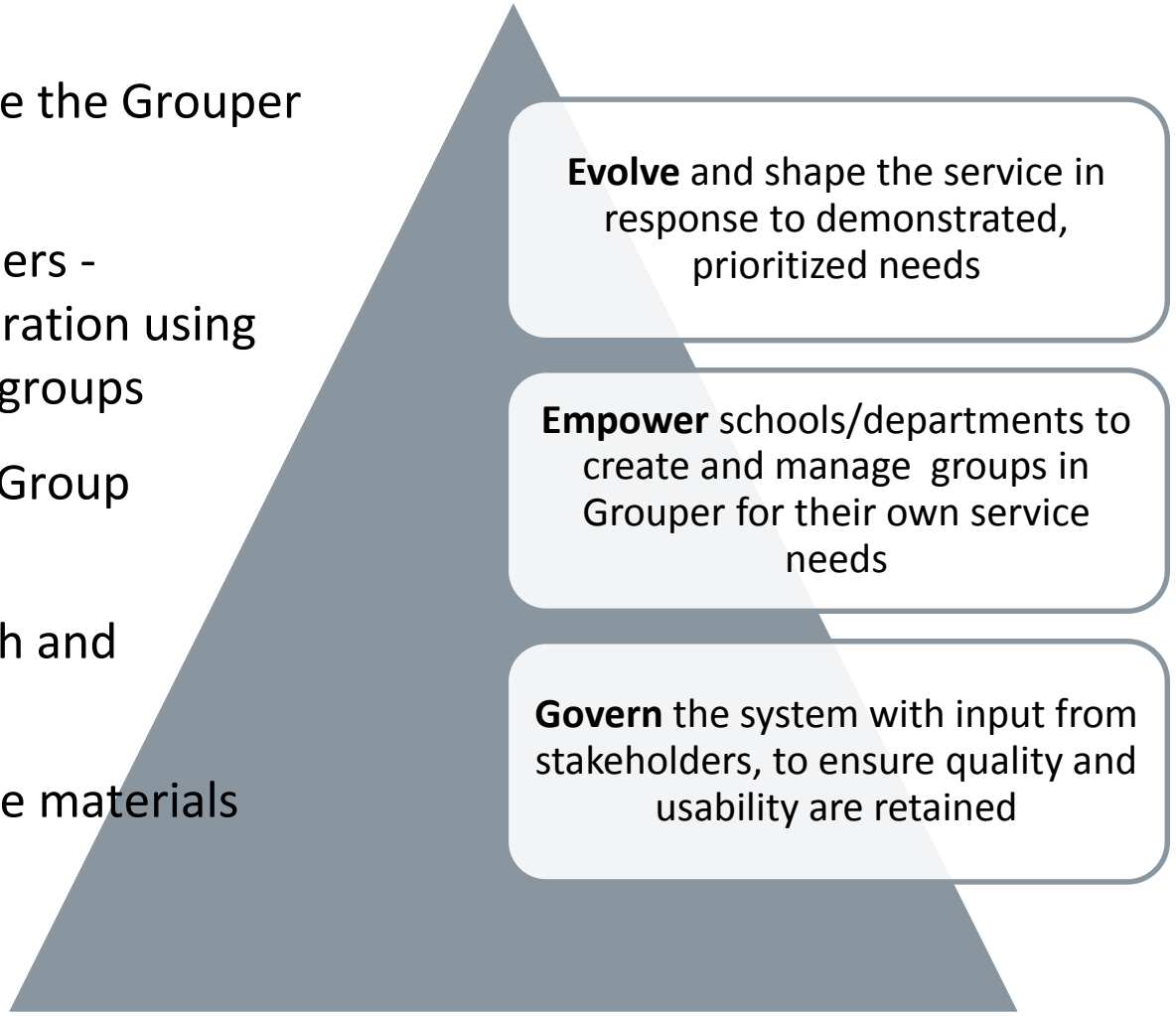


Group Services Guiding Principles

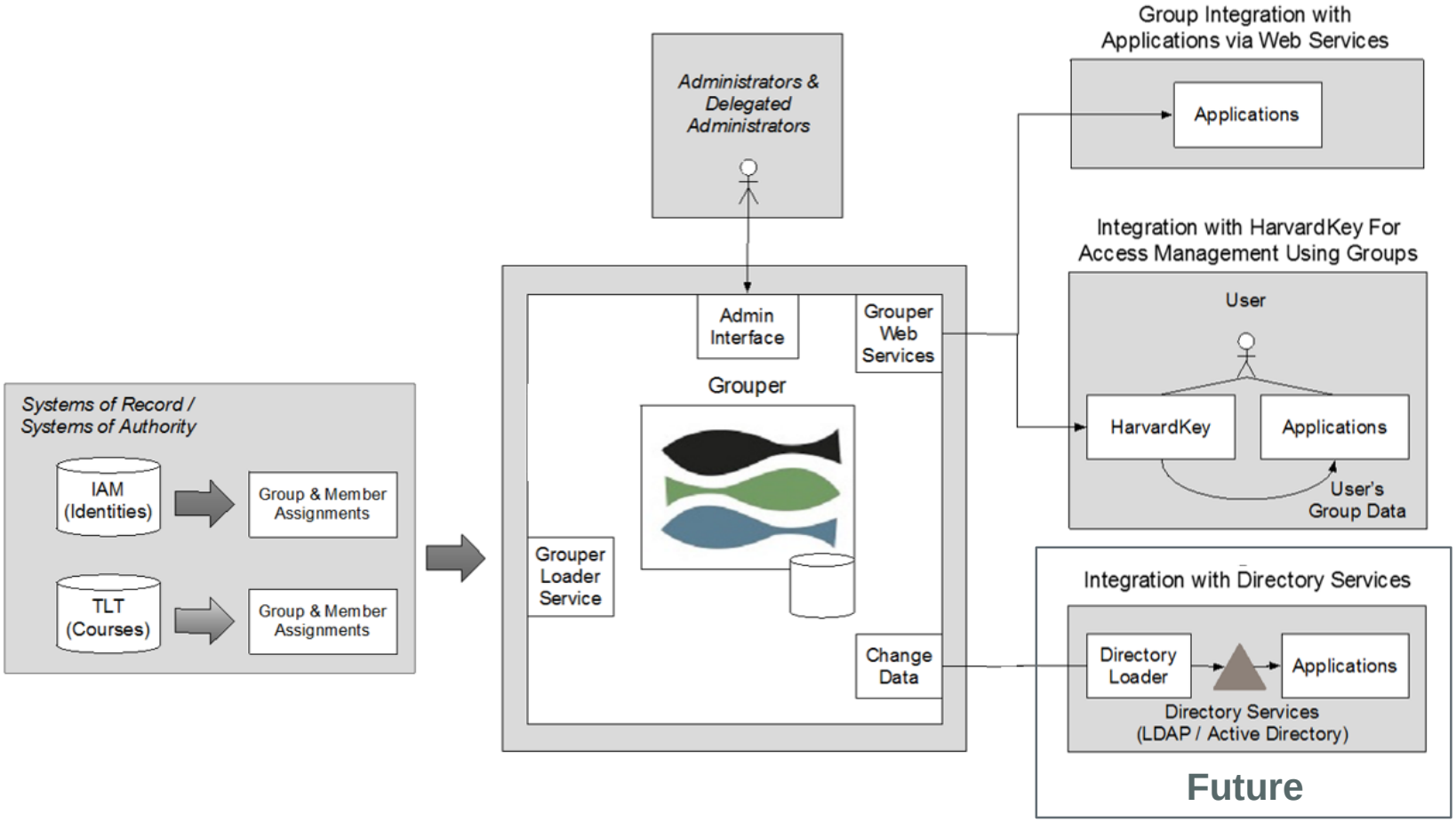


Group Services Guiding Principles and Activities

- Build and operate the Grouper Platform
- Onboard customers - application integration using HarvardKey and groups
- Train Delegated Group Administrators
- Perform outreach and consulting
- Provide reference materials
- Tier 2-3 support



Groups Services Platform



Grouper

A group management system;

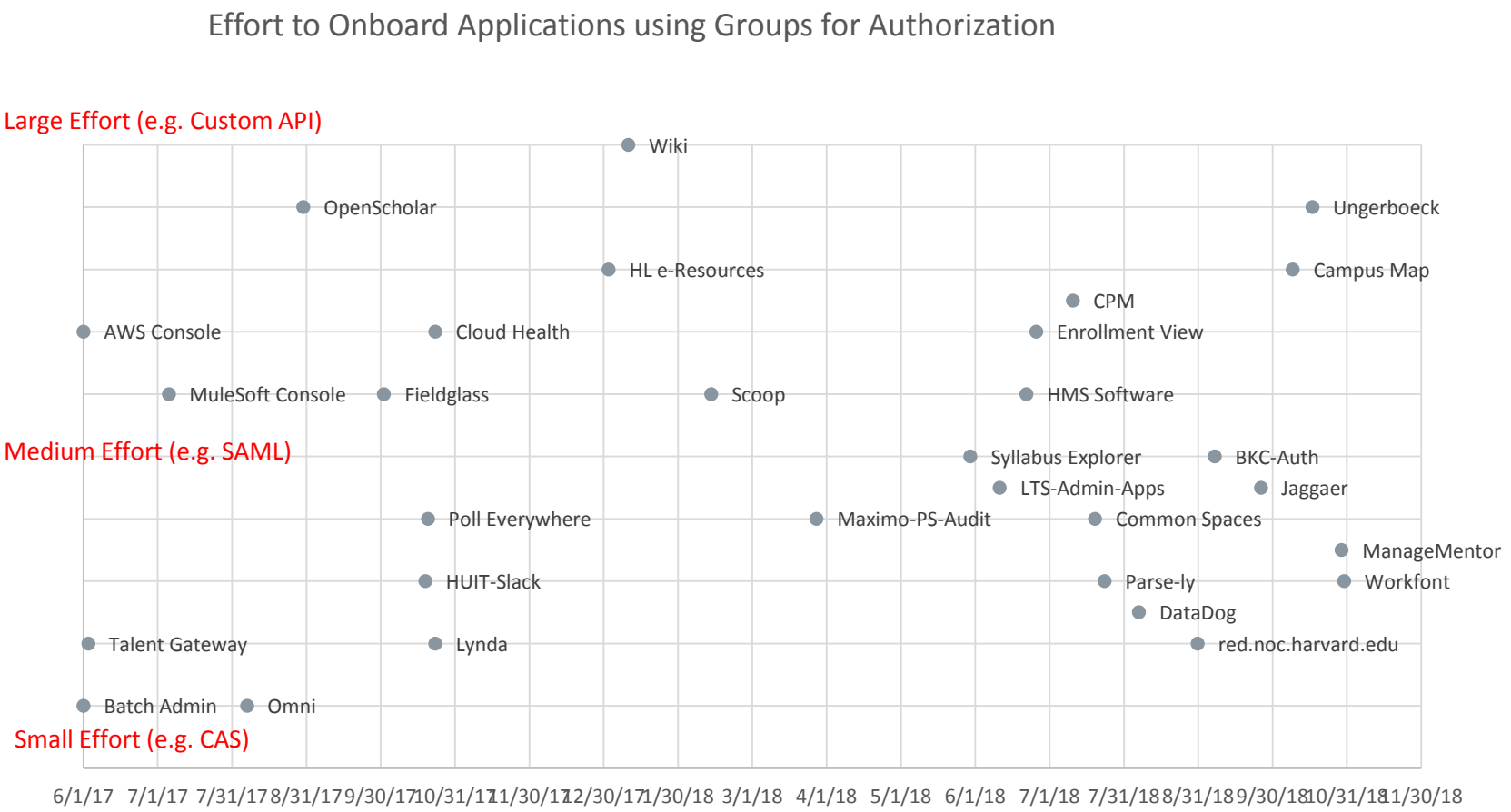
- An open-source application provided by the Internet2 consortium; used widely among universities - https://www.internet2.edu/products-services/trust-identity/grouper/
- Integrated with IAM identity and TLT course data so that group memberships are updated automatically
- Used by school and department IT Service Providers to manage groups directly or via API for application authorization access
- A web tool for delegated group administrators to manage groups for their local needs

Grouper is NOT directly accessible to faculty, staff and students at this time

Current Status of Grouper

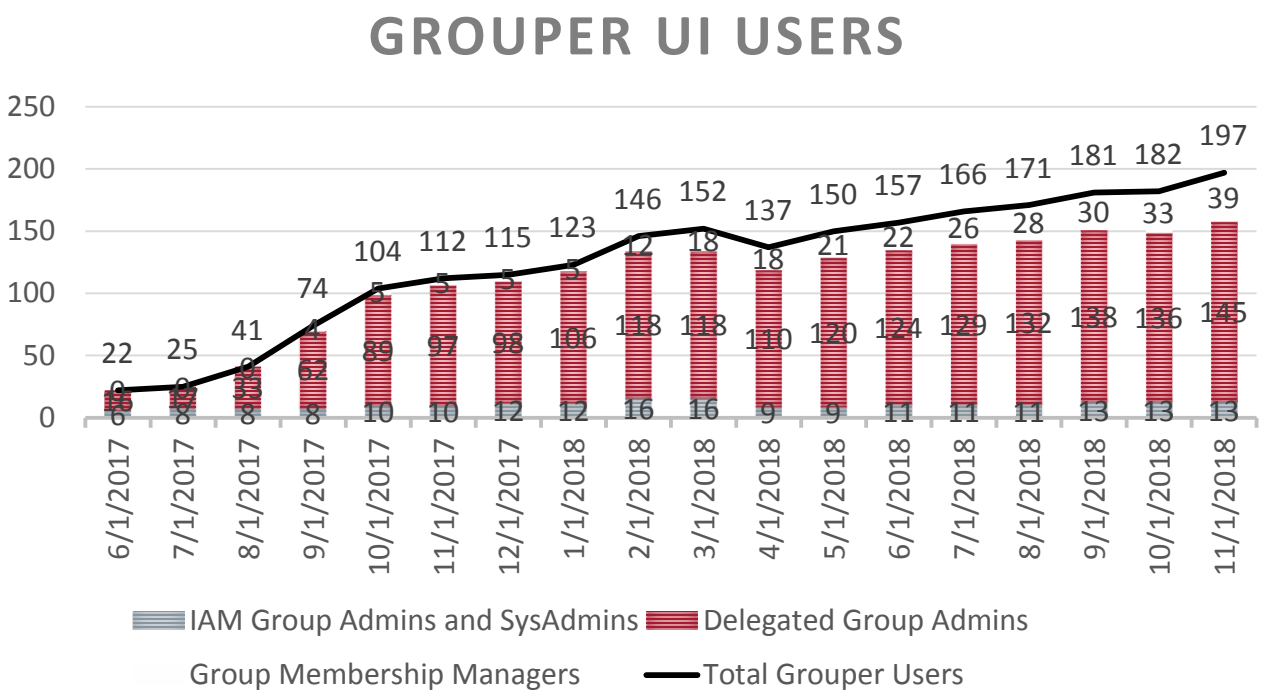
- Approximately 360,000 groups in the system
  - **Reference groups** (800+) automatically update based on current roles/affiliations in IAM Identity Registry
  - **Academic Course groups** (357,000+) automatically update from Academic Technology course database
  - **Managed groups** (900+) ad-hoc or custom groups created and managed by IT Service providers for application-specific needs
  - **Application Authorization groups** (32) applications using Group Services for Authorization
- Monthly Group Services Metrics posted on https://iam.harvard.edu/ along with this presentation.

Application Authorization



Grouper Users

- Limited distribution of the Grouper UI (not a self-service application)
  - **Delegated Group Administrators** (145+) trained by IAM
  - **Group Membership Managers** (39+) self-service guide
  - **IAM Group Administrators** (13)

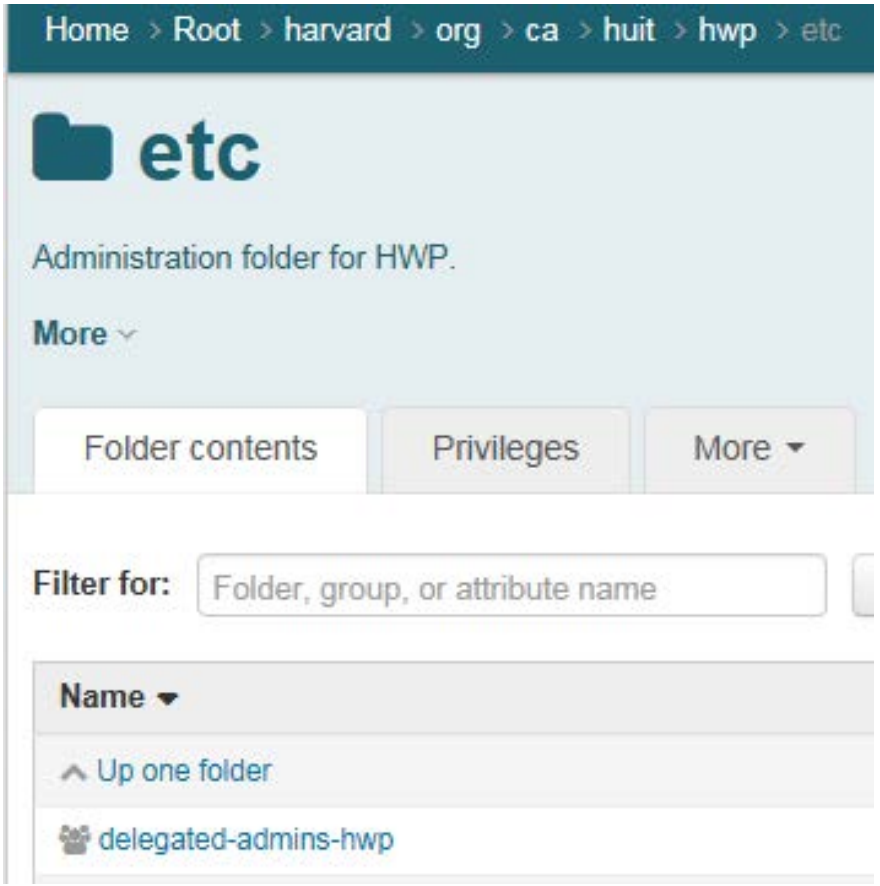


Delegated Group Administration

Grouper is ... designed for the highly ***distributed management environment*** and heterogeneous information technology environment common to universities [Internet2].

Delegated Group Administrators

- Interacts directly with Grouper to set up sub-folder structure, and to create and manage groups
- Receives training and observes IAM group conventions
- Provides Tier 1 support for their school/department
- May designate additional delegated administrators
- Schools/Departments should designate an point-person to interact with IAM Group Services

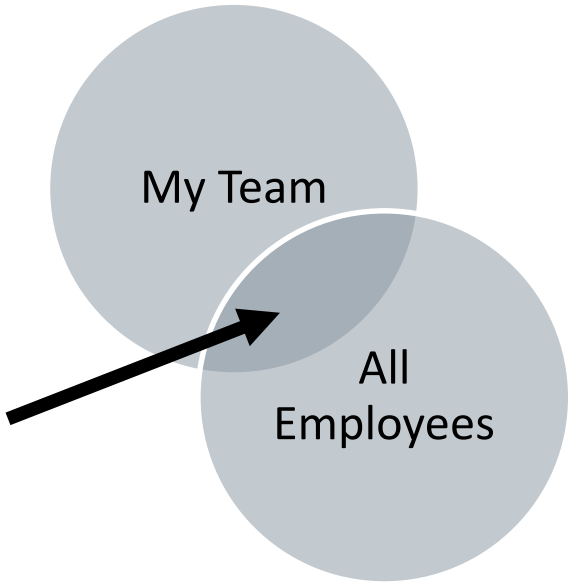


The Value of Reference Groups

Reference groups are automatically updated daily based on the system of record feeds to IAM and TLT

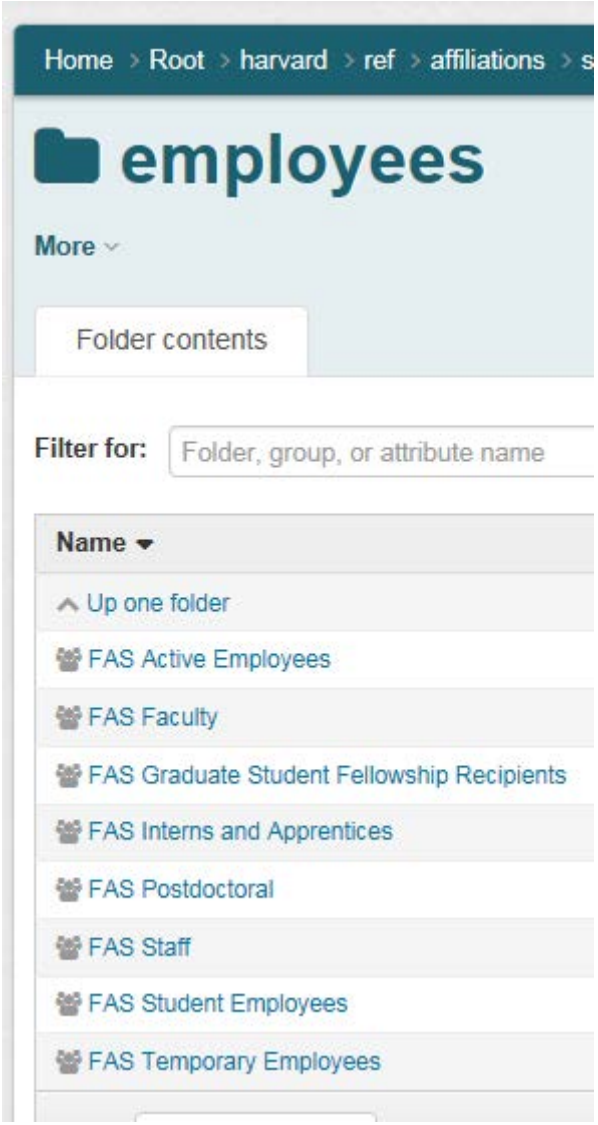
- Using reference groups, you get “only current members” and this supports authorization objectives
- By intersecting reference groups with your own managed (custom) groups, you can ensure that the membership of your managed groups are automatically updated to remove people who are no longer active

Resultant Group has only Active Employees on My Team



Reference Groups Build-out

- Reference groups are automatically updated daily based on the system of record feeds to IAM and TLT
- Today reference groups are only built out to the school – high level department depth
- We have 750+ reference groups available today
- Additional reference groups are built out upon request (e.g. at the department level)
- 2-4 week service level objective



HarvardKey Integrated with Group Services

Application Authorization Filter –

After authentication, HarvardKey checks if the person is in a particular group, e.g., authorized-users-omni. If so, then access to the application is granted.

MemberOf Group Attribute Release –

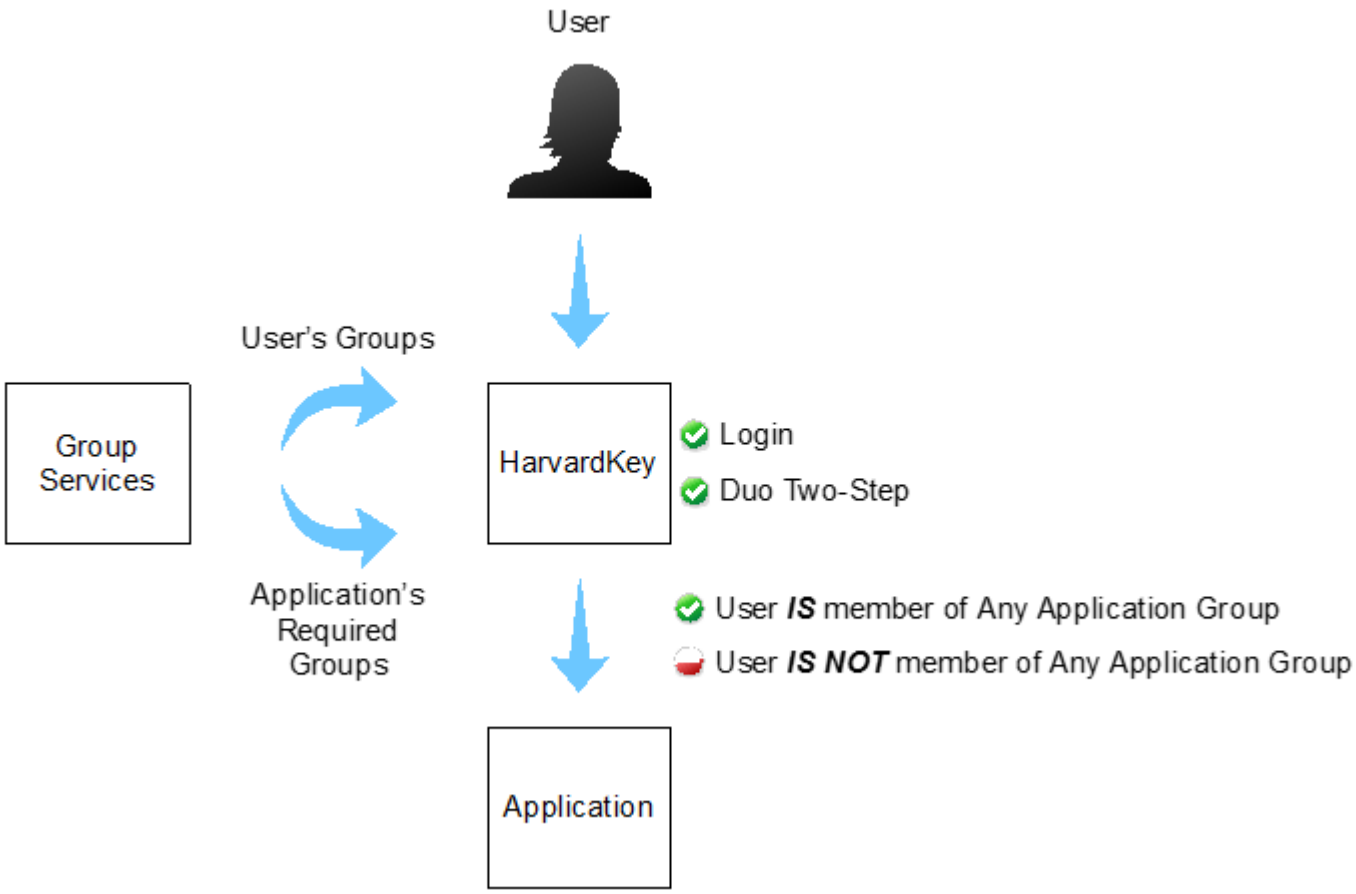
CAS or SAML release the groups a person is a member of in their response back to the application. The application then determines what to do with that information. Can be used for more granular level of permissions, e.g. standard or superuser permission.

HARVARDKEY

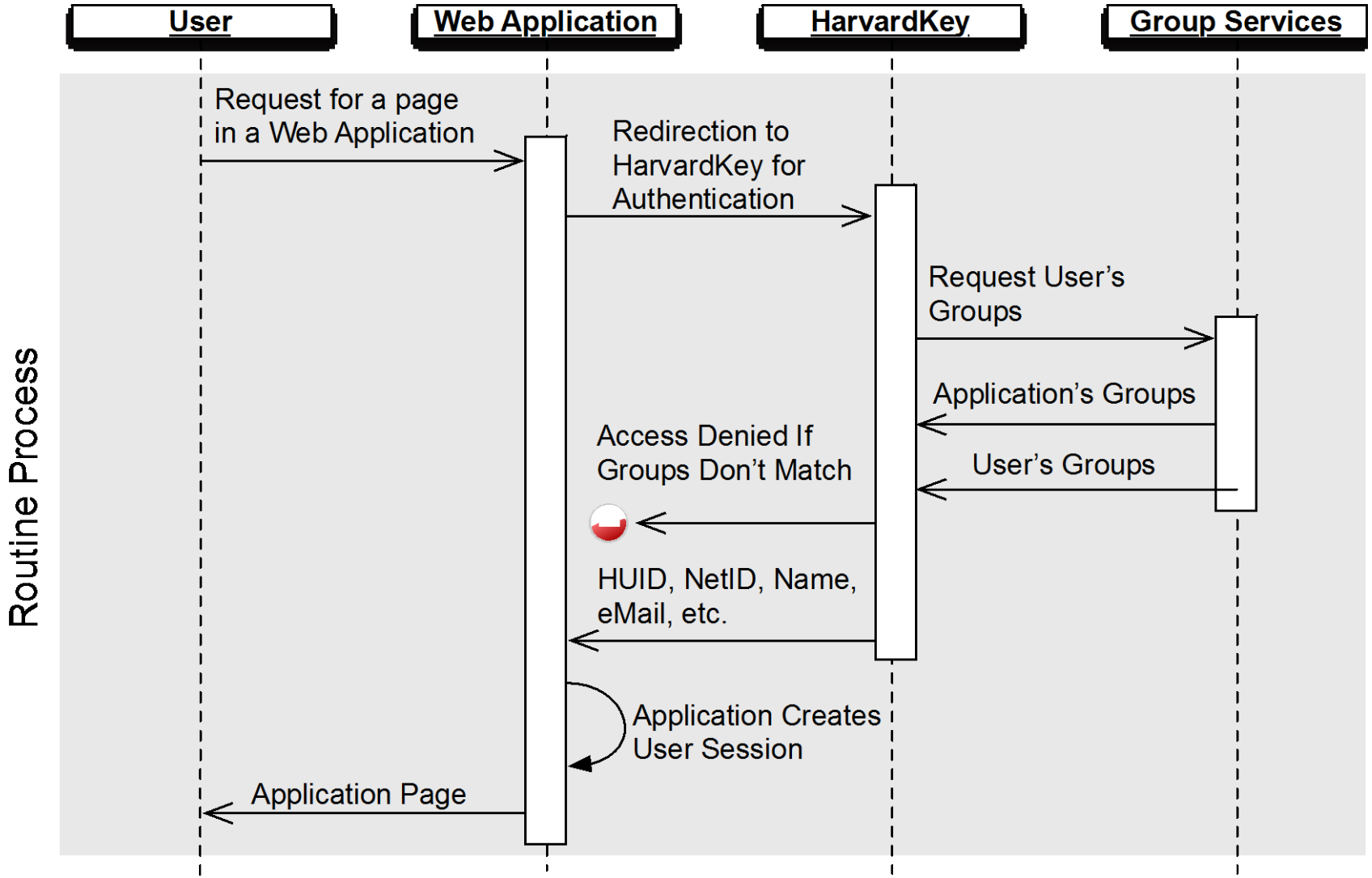
- Used for web-based application using **CAS or SAMLs** protocols.
- The two methods which can be used alone or together.
- Each requires one-time process: IAM setups up Application Authorization groups in Grouper and adds one or both methods to the application's HarvardKey integration.

Application Authorization Filter

Front Door Authorization via HarvardKey

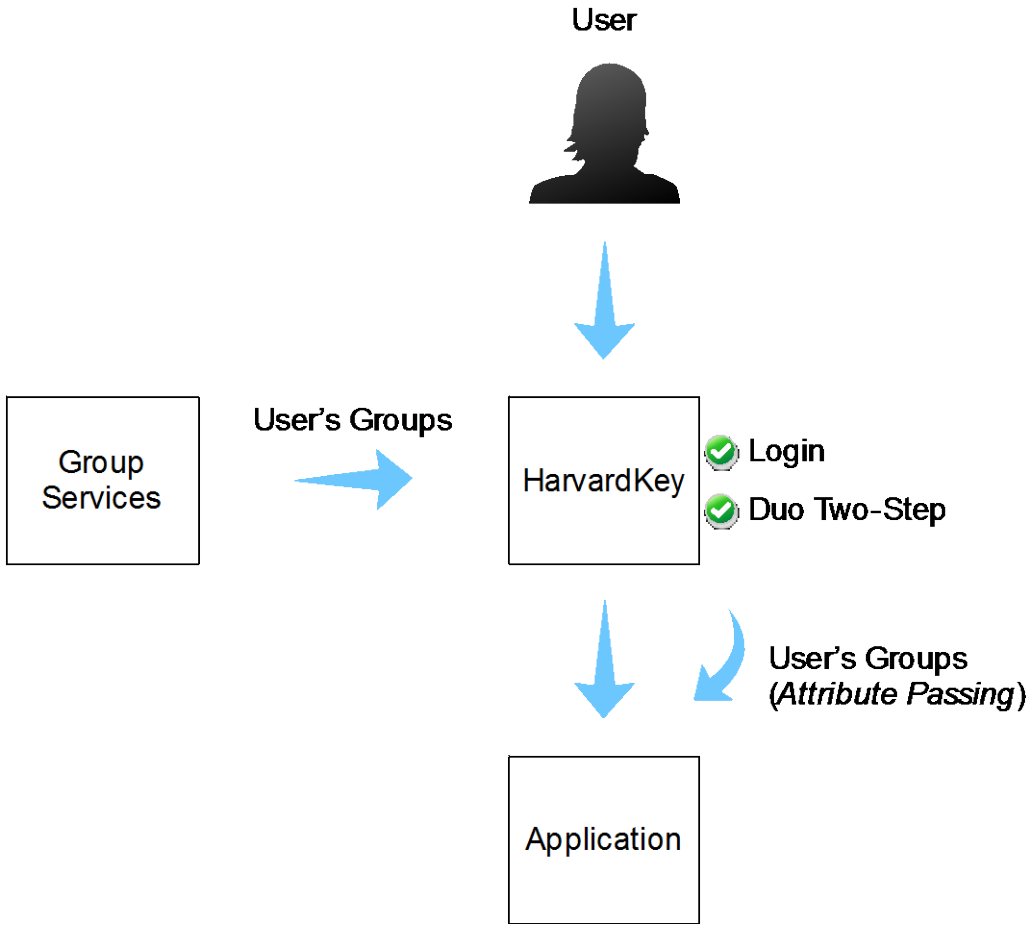


Application Authorization Filter - Sequence Diagram

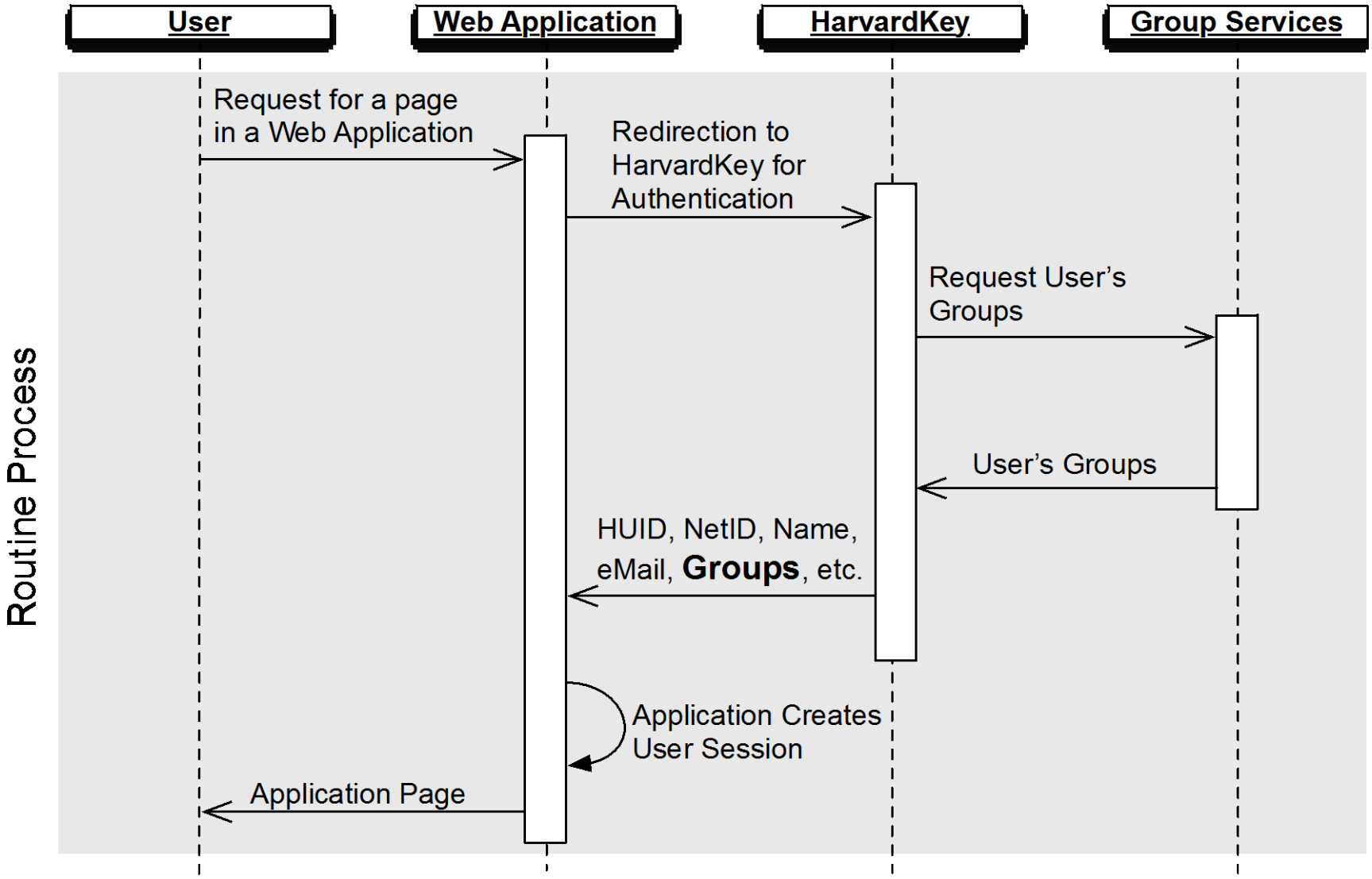


MemberOf Group Attribute Release

HarvardKey proides User's Group Memberships to Applications



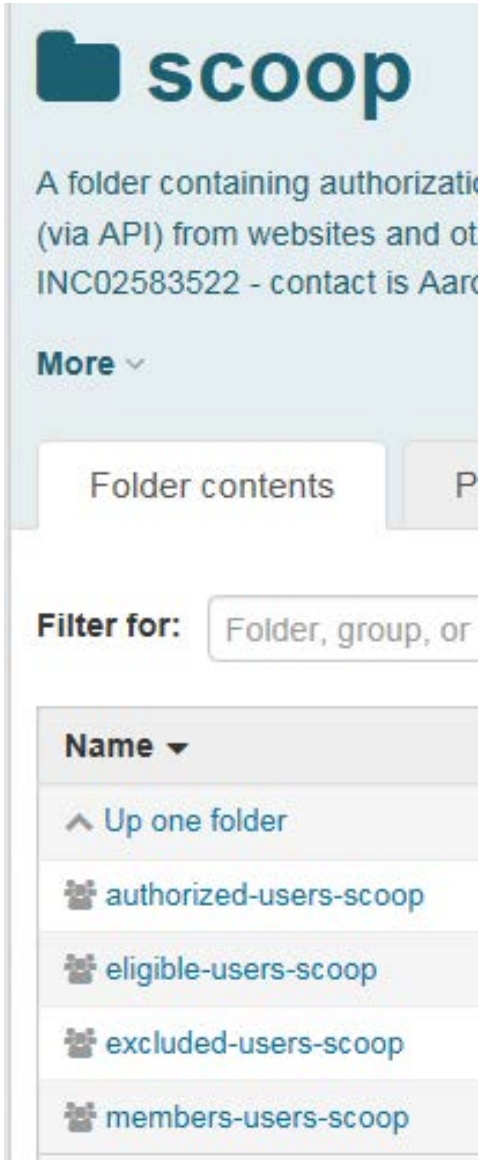
MemberOf Group Attribute Release - Sequence Diagram



Application Authorization Groups

A set of group s which are used to derive one resultant group whose members are authorized to access an application.

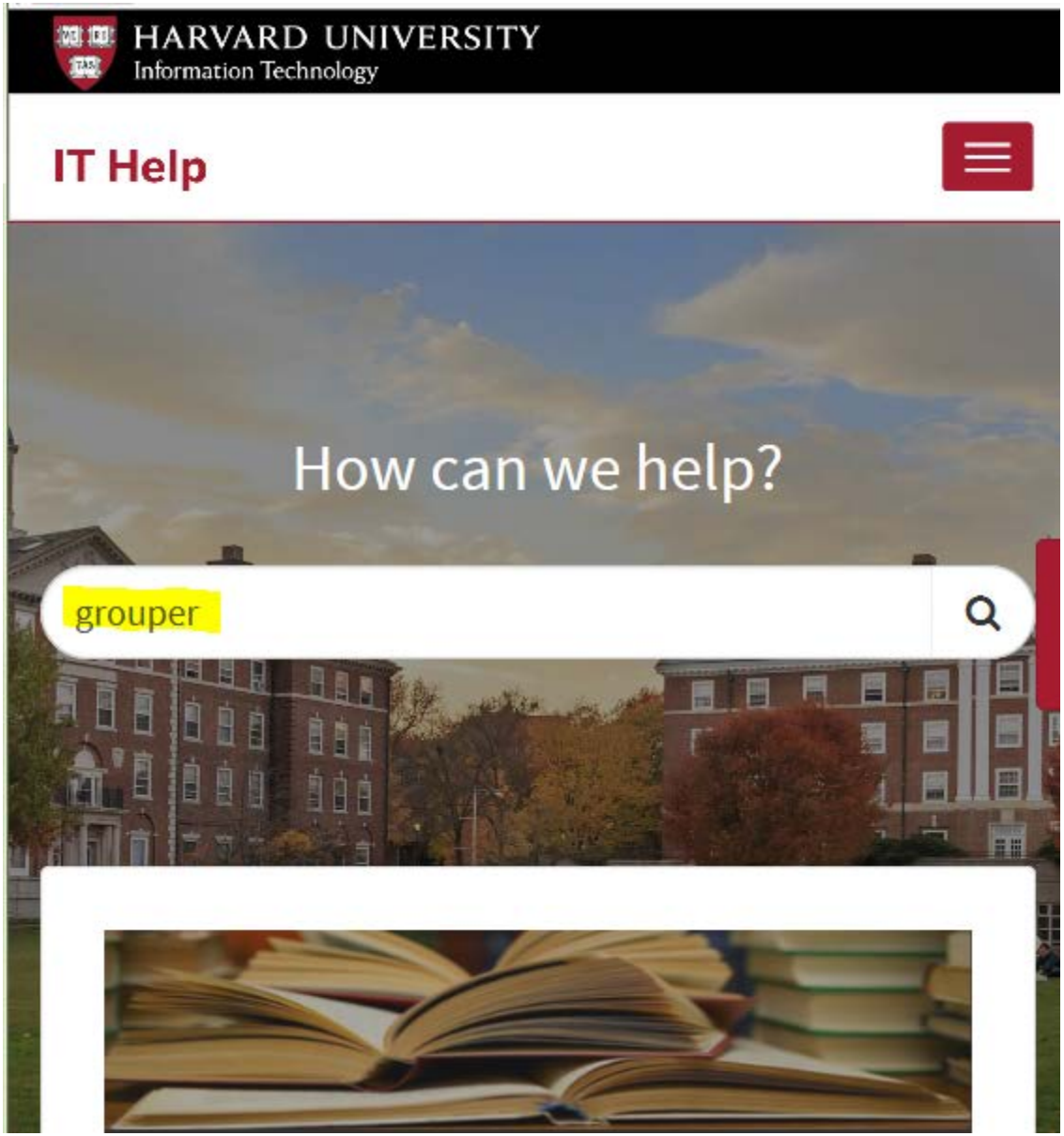
- **Authorized-users** = final resultant group after subtracting excluded-users from eligible-users (eligible-excluded)
- **Eligible-users** = resultant group intersecting members-users with a reference group (members X reference group)
- **Excluded-users** = list of people to exclude and the university excluded users group
- **Members-users** = list of people, reference groups and or other managed groups who are the intended users of the application before removing inactive and excluded users.



https://harvard.service-now.com/ithelp

Group Service

- Knowledge Articles
- Guides
- Q&A



How Can I Use The Service?

Group Service	How To Use The Service
Access Control for Web Applications using HarvardKey and Groups	IAM_help@harvard.edu Submit a request to integrate an application with HarvardKey. Submit this form with your request: http://iam.harvard.edu/files/iam/files/cas-saml-spusagerequest-form.pdf
Delegated Group Administration	IAM will provide consultation, training and onboarding for you to manage groups as you need. Submit your request to iam_help@Harvard.edu. Requests are managed by the IAM Accounts team and Group Services Owner, Terry Connolly at terry_connolly@harvard.edu
Need Groups?	Contact the delegated group administrators for your school/department at https://harvard.service-now.com/ithelp?id=kb_article&sys_id=f8b58eb2db7e4304a914fff31d9619aa on the IT Help Knowledge Portal.