



HARVARD UNIVERSITY
Information Technology

IAM Group Services

April 25, 2018

Overview Presentation

IAM Group Services

Groups Enable Other IT Services

Groups are a critical component of these IT Services

Access Control (available now)	<ul style="list-style-type: none">• Enable application access for eligible users (authorization)• Authorization options through HarvardKey & API• Automatically removes access as eligibility ends
Communication (start in FY19)	<ul style="list-style-type: none">• Email or texting messaging to targeted audiences• Broadcast Communications
Collaboration (future)	<ul style="list-style-type: none">• Simplify document sharing to collaborators• Enable controlled file sharing (individuals and groups)

IAM Group Services Overview

Group Services

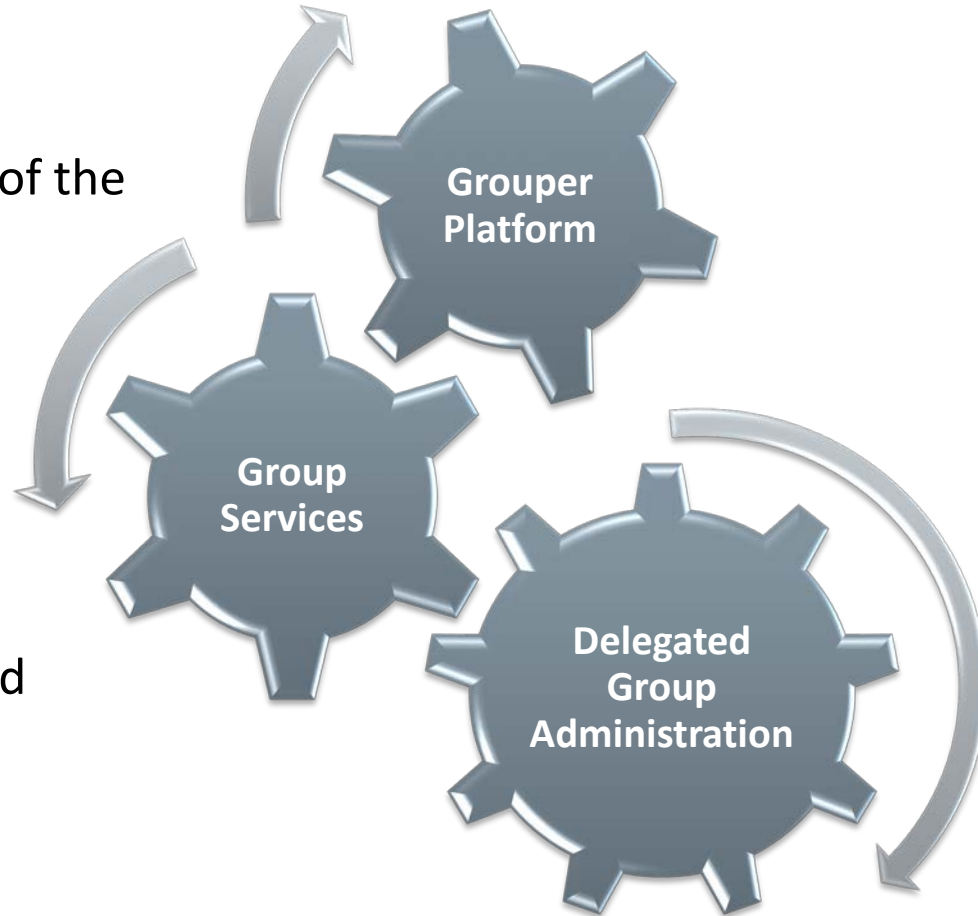
...drives the evolution of the

Grouper Platform

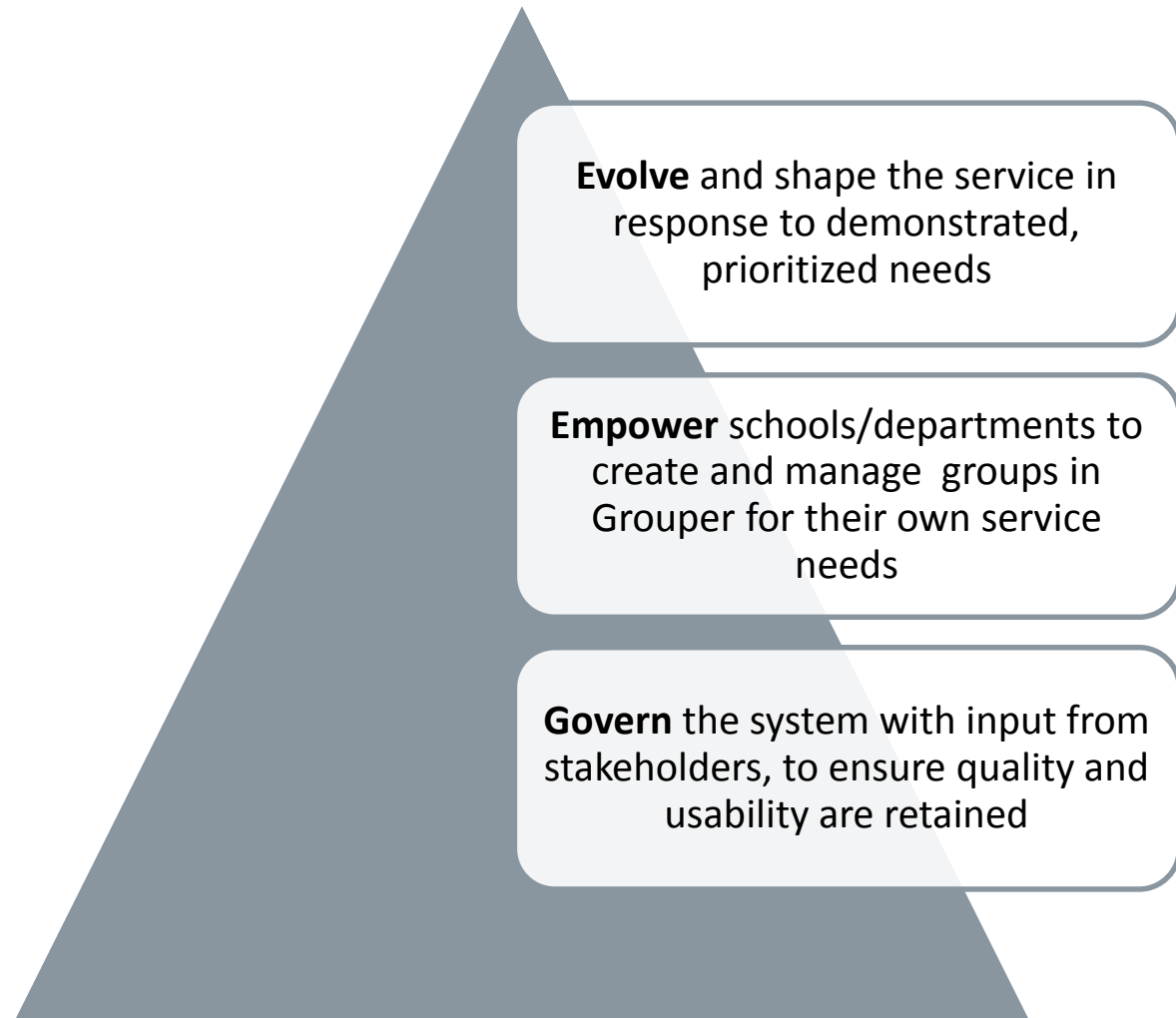
...and the adoption of

Delegated Group Administration

...by schools and departments at Harvard

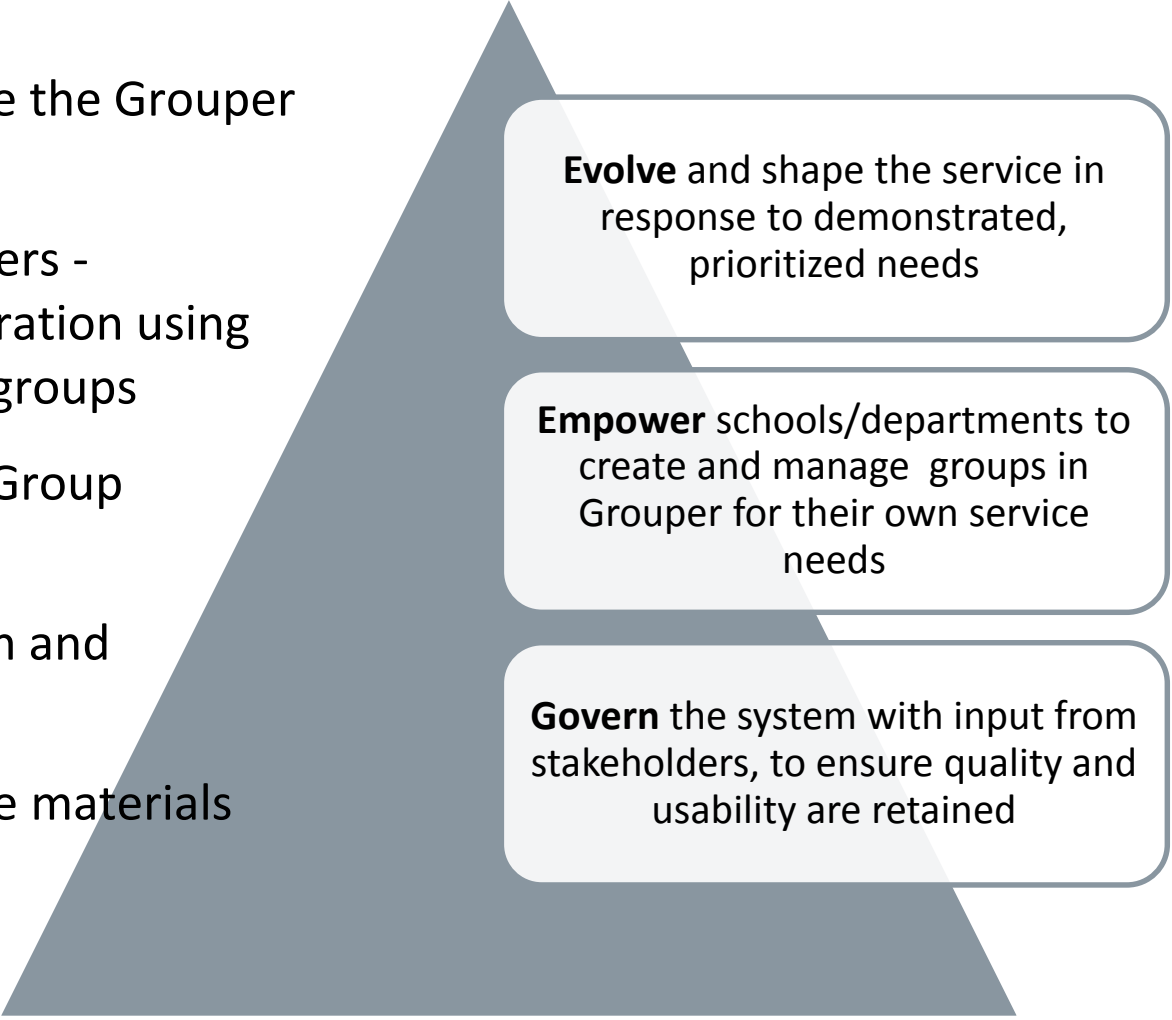


Group Services Guiding Principles



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

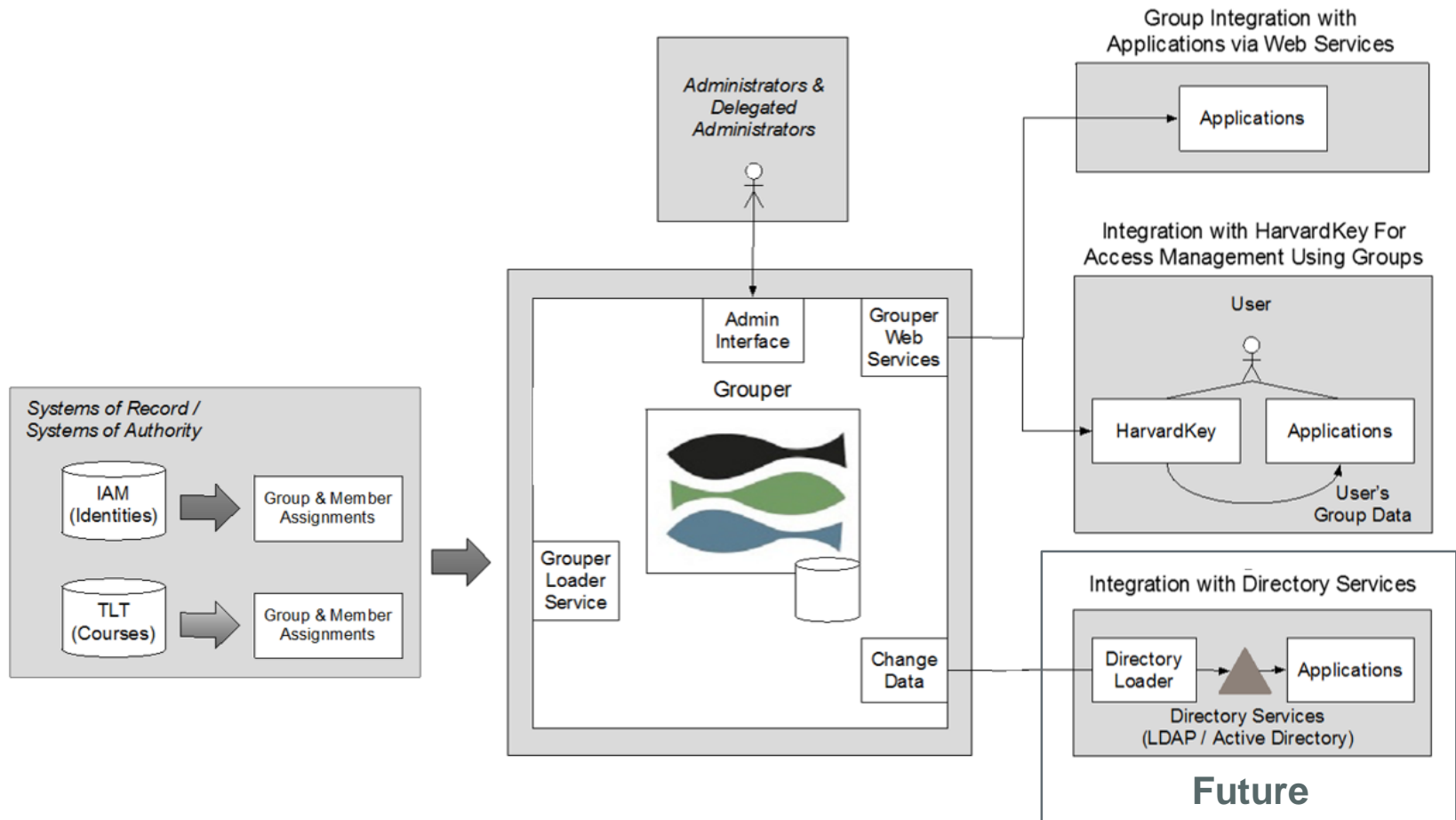


Evolve and shape the service in response to demonstrated, prioritized needs

Empower schools/departments to create and manage groups in Grouper for their own service needs

Govern the system with input from stakeholders, to ensure quality and usability are retained

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

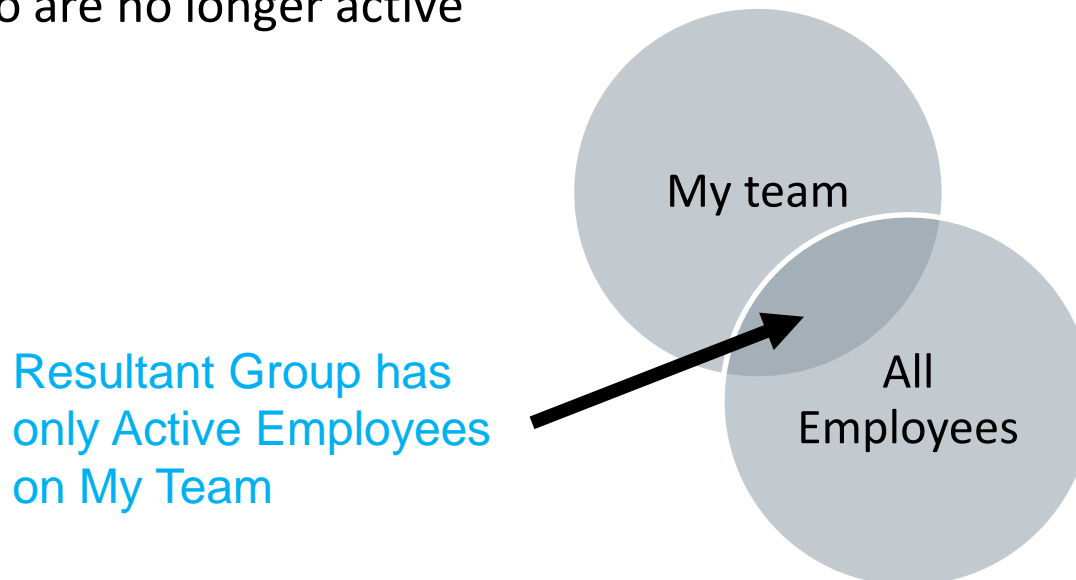
Current Status of Grouper - Monthly Group Services Metrics

- Approximately 290,000 groups in the system
 - **Reference groups** (400+) - automatically update based on current roles/affiliations in IAM Identity Registry
 - **Academic Course groups** (285,000+) - automatically update from Academic Technology course database
 - **Managed groups** (100+)– ad-hoc or custom groups created and managed by IT Service providers for application-specific needs
 - **Application Authorization groups** – (14) applications using Group Services for Authorization e.g. AWS, Talent Gateway, Lynda, Huit-Slack, Poll Everywhere, OpenScholar, Wiki
- Limited distribution of the Grouper UI
 - **Delegated Group Administrators** (125+) trained by IAM
 - **Group Membership Managers** (30+) self-service guide

The Value of Reference Groups

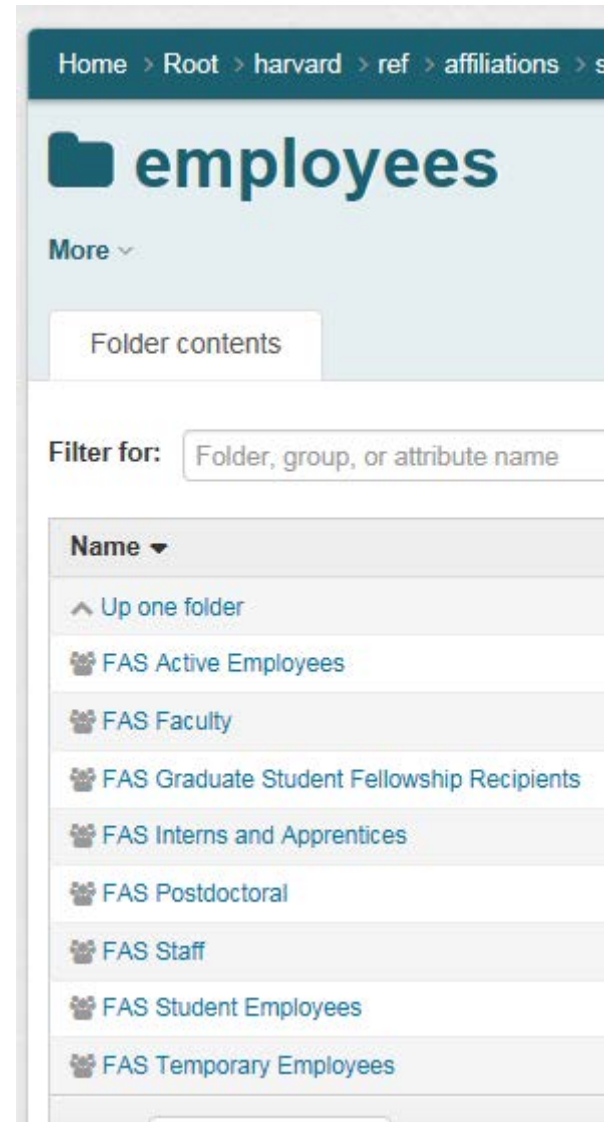
Reference groups are automatically updated daily based on the system of record feeds to IAM and TLT

- 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



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 400+ reference groups available today
- Additional reference groups are built out upon request (e.g. at the department level)



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 - Key Features

1- HarvardKey Authentication

The current authentication service provided by HarvardKey, using a user ID, password, and the Duo two-step process, continue as before.

2- User's Groups

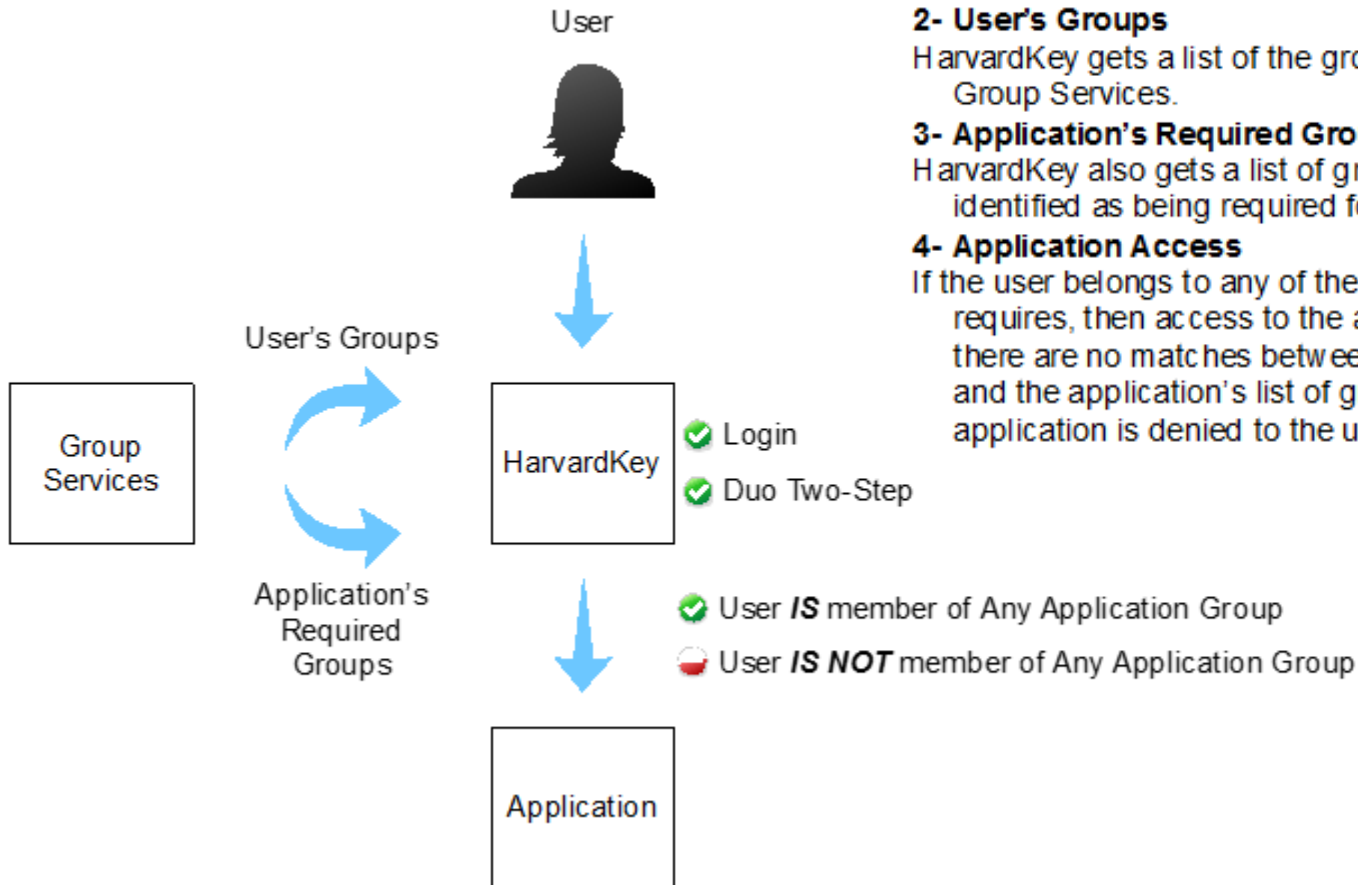
HarvardKey gets a list of the groups a user belongs to from Group Services.

3- Application's Required Groups

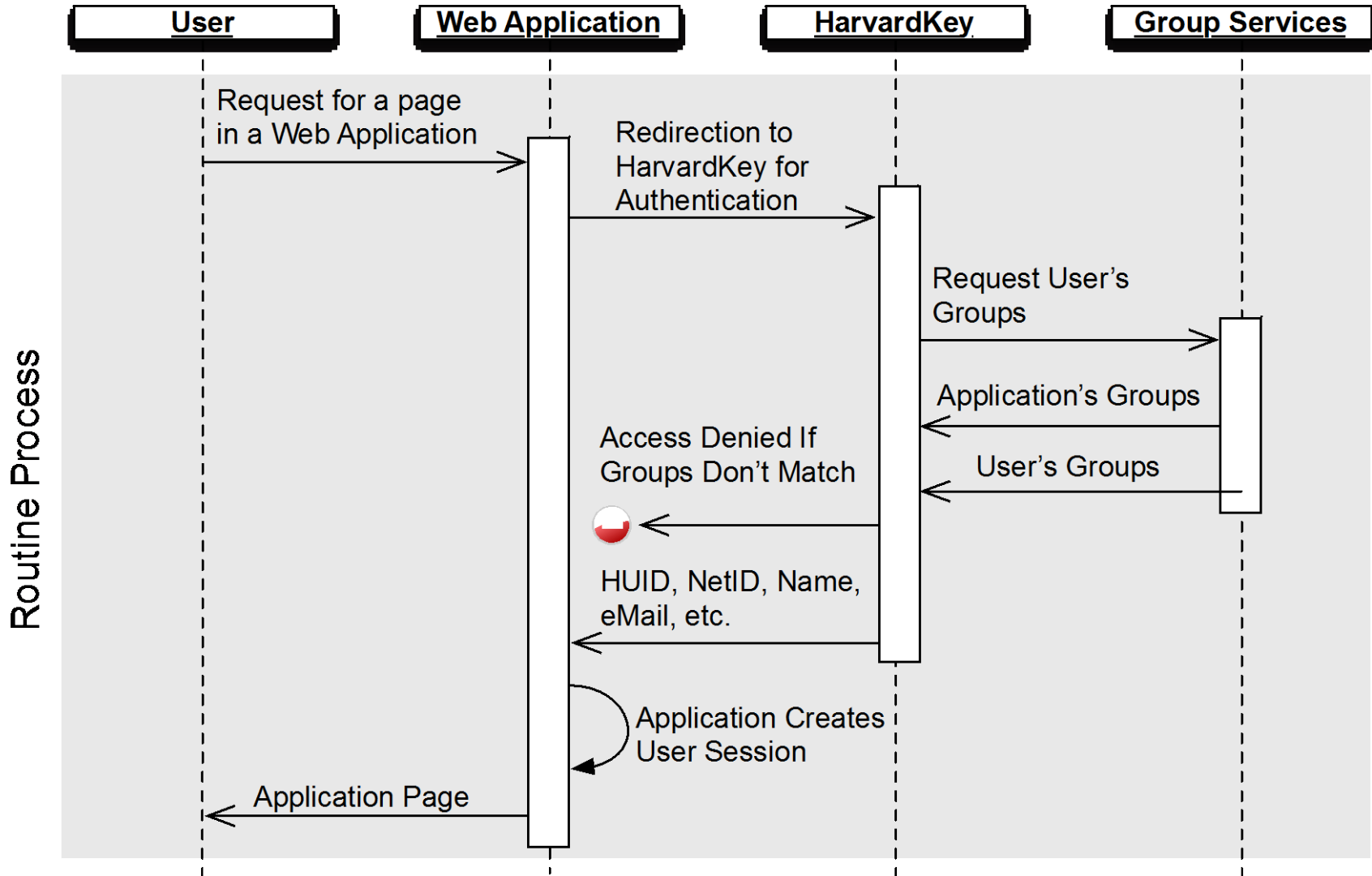
HarvardKey also gets a list of groups the application has identified as being required for the user belong.

4- Application Access

If the user belongs to any of the groups that the application requires, then access to the application is granted. If there are no matches between the user's list of groups and the application's list of groups, access to the application is denied to the user.

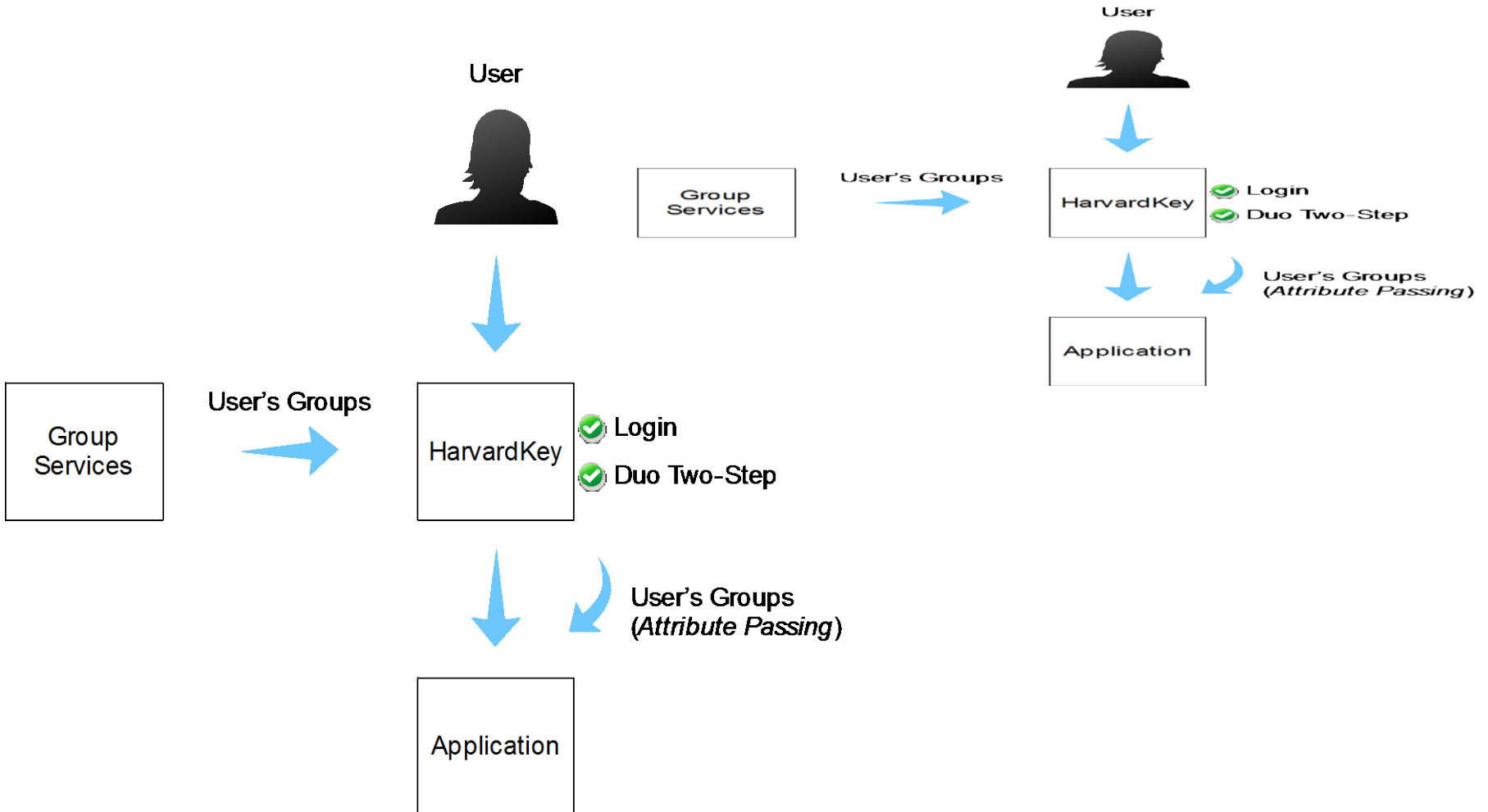


Application Authorization Filter - Sequence Diagram

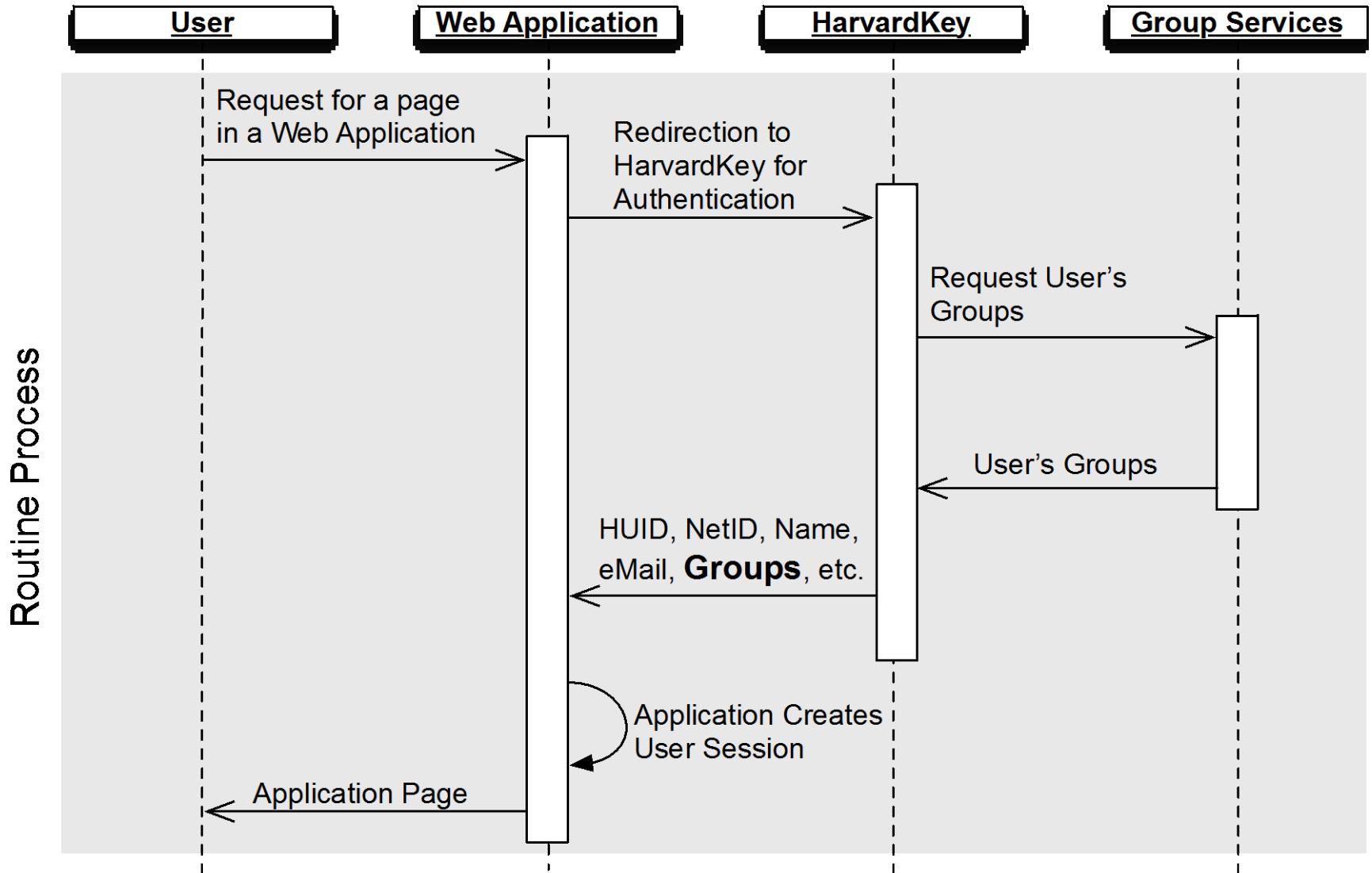


MemberOf Group Attribute Release - Key Features

Provides User's Group Memberships to Applications



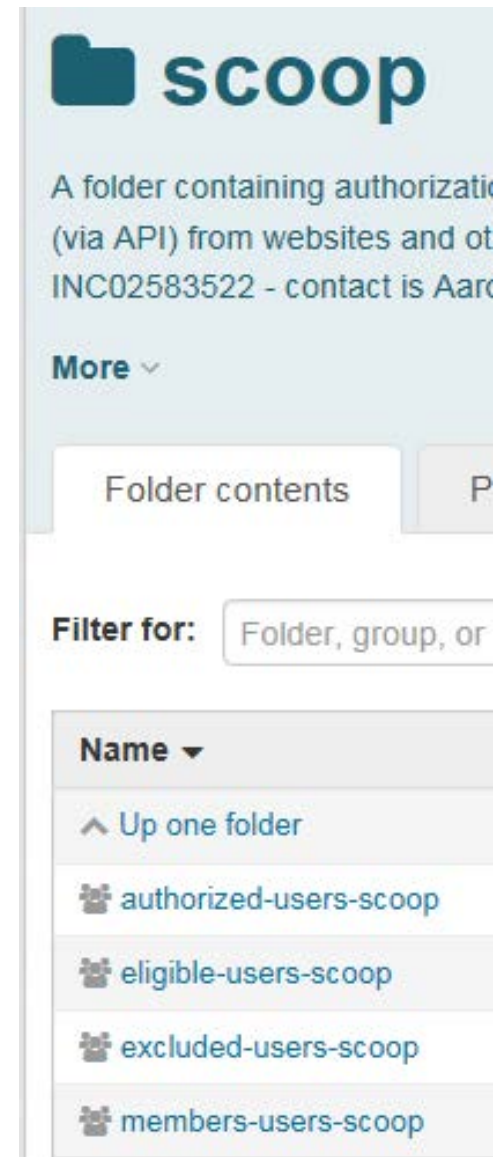
MemberOf Group Attribute Release - Sequence Diagram



Application Authorization Groups

A set of groups 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.

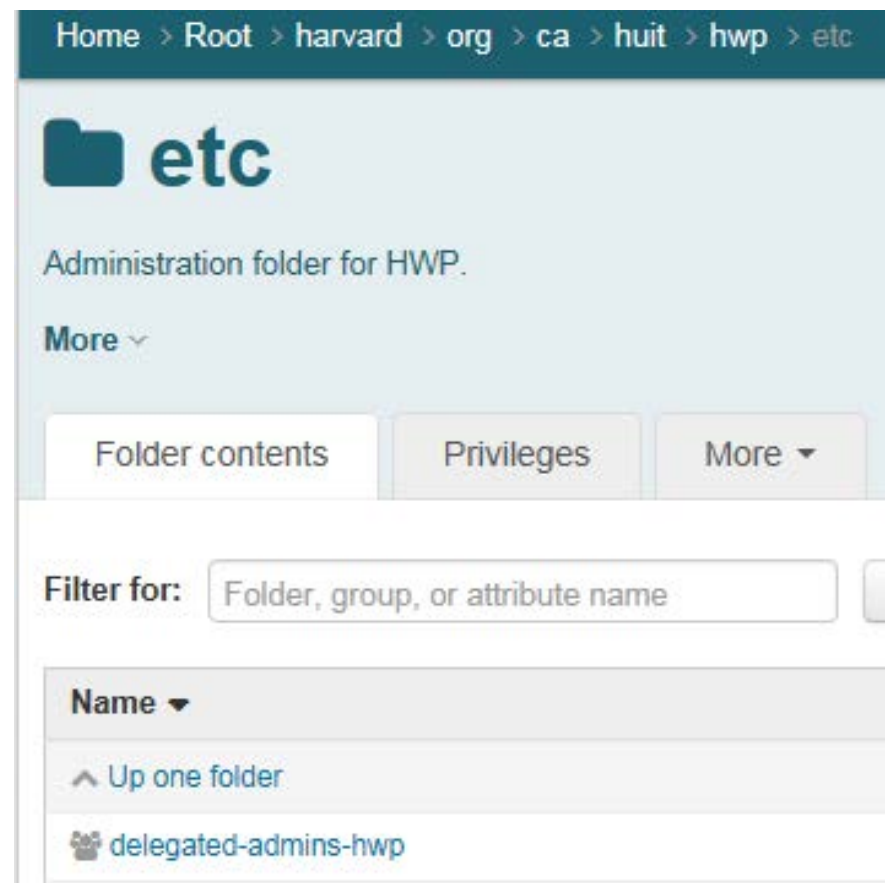


Delegated Group Administration

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



How Can I Use The Service?

Group Service	How To Use The Service
Access Control for Web Applications using HarvardKey and Groups	<p>IAM help@harvard.edu</p> <p>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</p>
Delegated Group Administration	<p>IAM will provide consultation, training and onboarding for you to manage groups as you need. Submit your request to iam_help@Harvard.edu.</p> <p>Requests are managed by the IAM Accounts team and Group Services Owner, Terry Connolly at terry_connolly@harvard.edu</p>
Need Groups?	<p>Contact the delegated group administrators for your school/department at https://harvard.servicenow.com/ithelp?id=kb_article&sys_id=f8b58eb2db7e4304a914fff31d9619aa on the IT Help Knowledge Portal.</p>