TIER Access Governance and Grouper 2.4

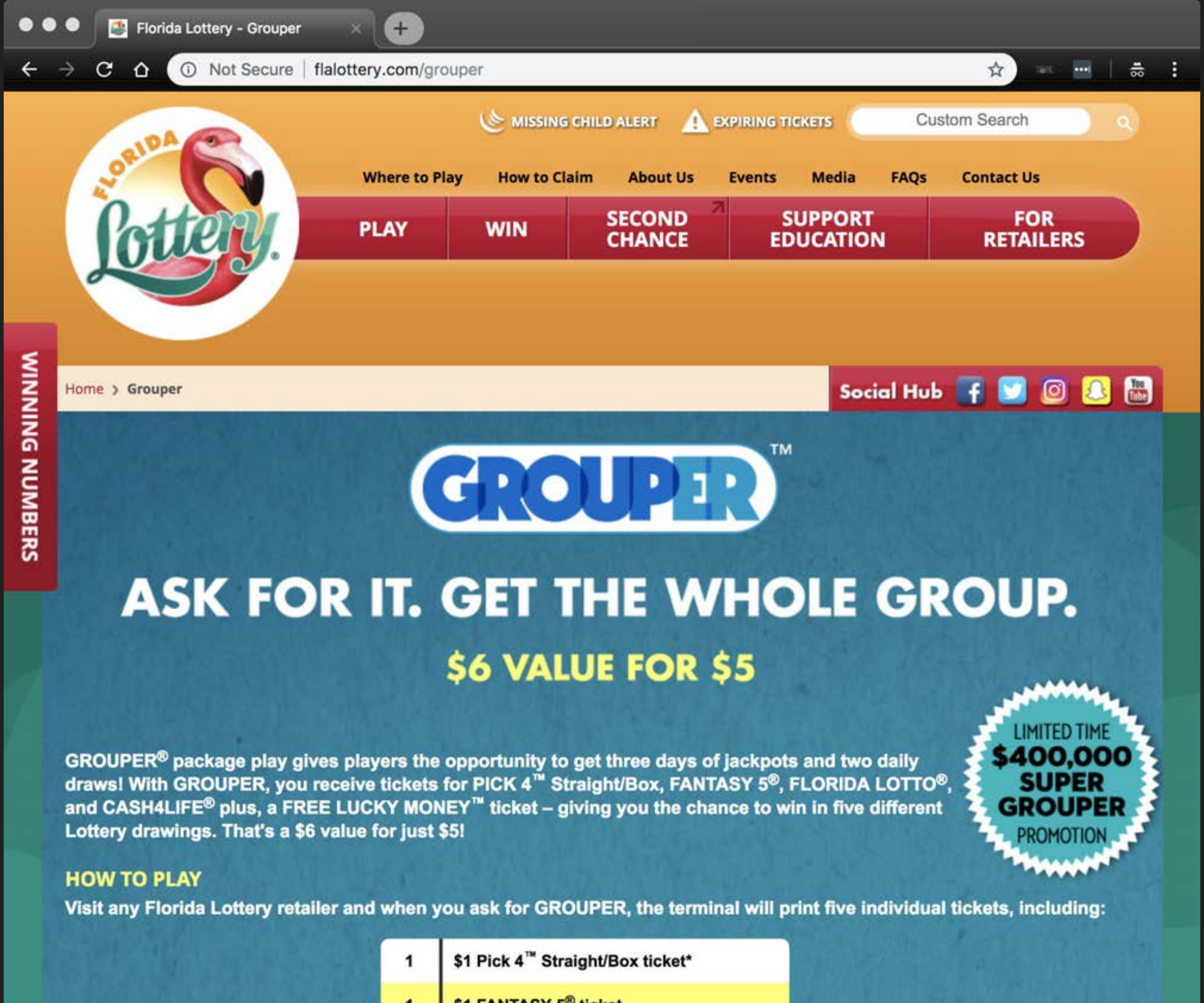
IAM Online

Wednesday, September 12, 2018

Michael Gettes, University of Florida
Chris Hyzer, University of Pennsylvania
Bill Thompson, Lafayette College

What is Grouper?

A lottery?



ASK FOR IT. GET THE WHOLE GROUP.

$6 VALUE FOR $5

GROUPER® package play gives players the opportunity to get three days of jackpots and two daily draws! With GROUPER, you receive tickets for PICK 4™ Straight/Box, FANTASY 5®, FLORIDA LOTTO®, and CASH4LIFE® plus, a FREE LUCKY MONEY™ ticket – giving you the chance to win in five different Lottery drawings. That's a $6 value for just $5!

HOW TO PLAY

Visit any Florida Lottery retailer and when you ask for GROUPER, the terminal will print five individual tickets, including:

1	$1 Pick 4™ Straight/Box ticket*
1	$1 FANTASY 5® ticket

What is Grouper?

Packaged?

In a container?

← yes, that's Grouper!

And now Grouper 2.4 on Slide 2.4

And here’s Chris….

Grouper 2.4 released

- August 2018
- Two years since previous release
- Dozens of substantial enhancements
- Hundreds of small fixes and improvements

Grouper 2.4 features

Release announcement

- Only New UI (other UIs removed)
- Deprovisioning
- Attestation
- Grouper Deployment Guide
- Packaging
- Messaging
- GSH-ng
- Updates to third party packages

Grouper 2.4 upgrade

- Minor upgrade (quick, easy, low risk)
- Please start planning
- Grouper team will focus on 2.4 support and new features
  - Will still fix major bugs and security issues in previous versions
- Upgrade instructions from 2.3
  - Convert some configs
  - Run upgrader

Grouper roadmap - currently working on

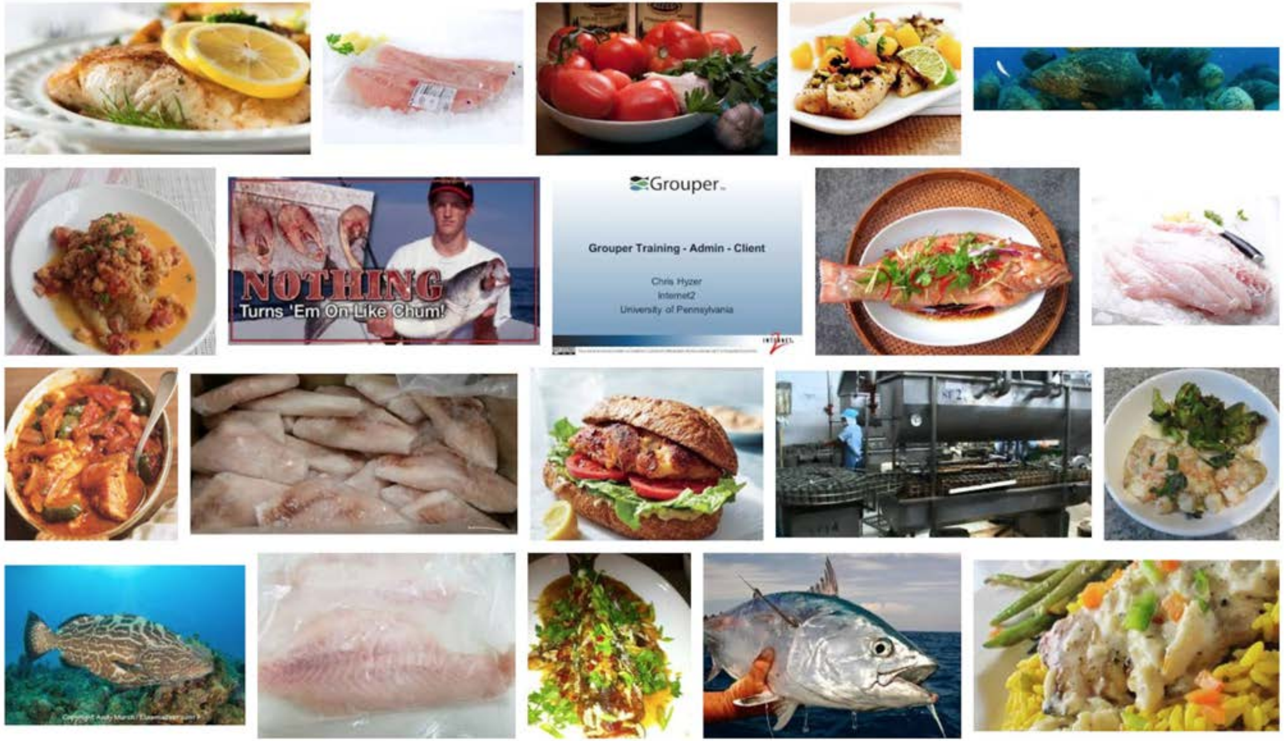
Roadmap

- Supporting 2.4
- Configuration stored in database
- Templates to create services and TIER structure
- Real time LDAP loader
- Provision to BMC Remedy

Grouper roadmap - next priorities

- Tag TIER objects (ref, basis, authz, etc)
- Configure which objects to provision in UI
- Add ability to disable loader jobs
- Subject source configuration wizard
- Permission role hierarchy in UI
- Membership reports

- Please email grouper-core@internet2.edu with Roadmap feedback



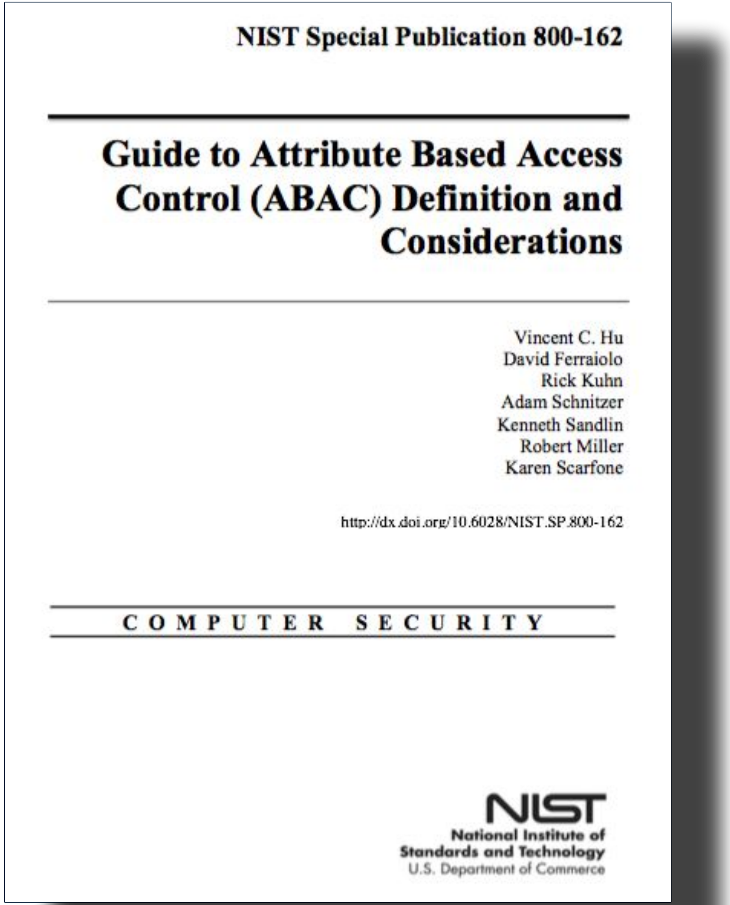
Grouper

Grouper Training - Admin - Client

Chris Hyzer
Internet2
University of Pennsylvania

Access Management Strategies for Higher Education and Research
TIER Grouper Deployment Guide

Bill Thompson, Director, Digital Infrastructure
Lafayette College



NIST Special Publication 800-162

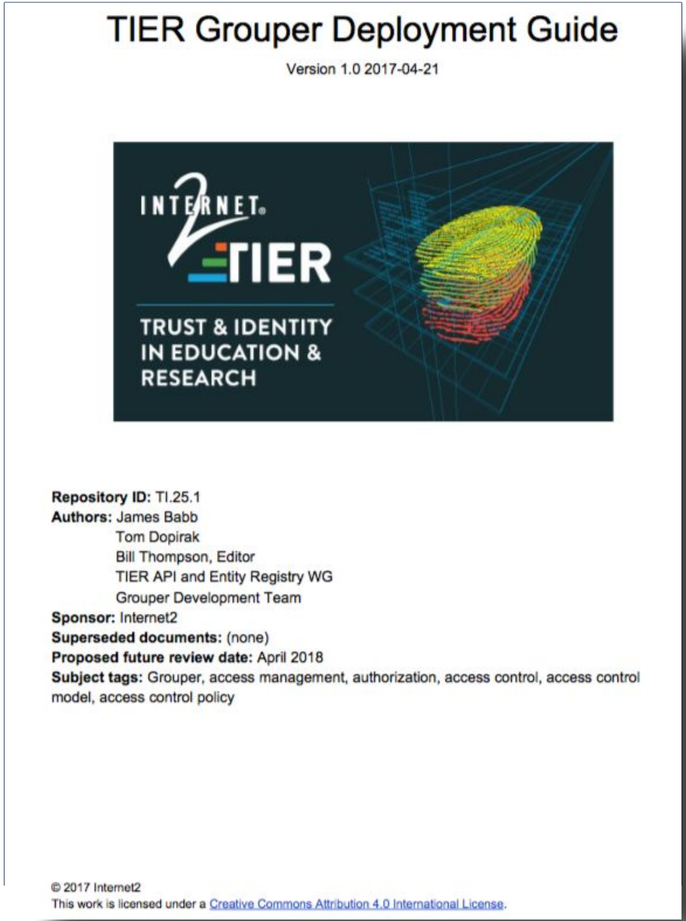
Guide to Attribute Based Access Control (ABAC) Definition and Considerations

Vincent C. Hu
David Ferraiolo
Rick Kuhn
Adam Schnitzer
Kenneth Sandlin
Robert Miller
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-162

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



TIER Grouper Deployment Guide

Version 1.0 2017-04-21

Repository ID: TI.25.1
Authors: James Babb
Tom Dopirak
Bill Thompson, Editor
TIER API and Entity Registry WG
Grouper Development Team
Sponsor: Internet2
Superseded documents: (none)
Proposed future review date: April 2018
Subject tags: Grouper, access management, authorization, access control, access control model, access control policy

Why do we need a guide?

- “Better documentation will make your project more successful” – Daniele Procida

- Four distinct types/purposes:
  - Tutorials – learn by doing, getting started, repeatable, concrete
  - How-to guides – series of steps, specific real goal/problem, some flexibility
  - Reference – technical description, information oriented, accuracy
  - **Discussions – context, explaining why, multiple examples**

- https://www.divio.com/en/blog/documentation/

TIER Grouper Deployment Guide

"The goal of this document is to help you come up to speed on Grouper concepts, how they relate to identity and access management, and how they can be deployed to implement effective access control in a wide variety of situations."

Section 3 Understanding Grouper
Section 4 Installing Grouper
Section 5 TIER Folder and Group Design
Section 6 Access Control Models
Section 7 Provisioning
Section 8 Operational Considerations
Section 9 Conclusion
Appendix A Example policies
Appendix B Acknowledgements

Terminology

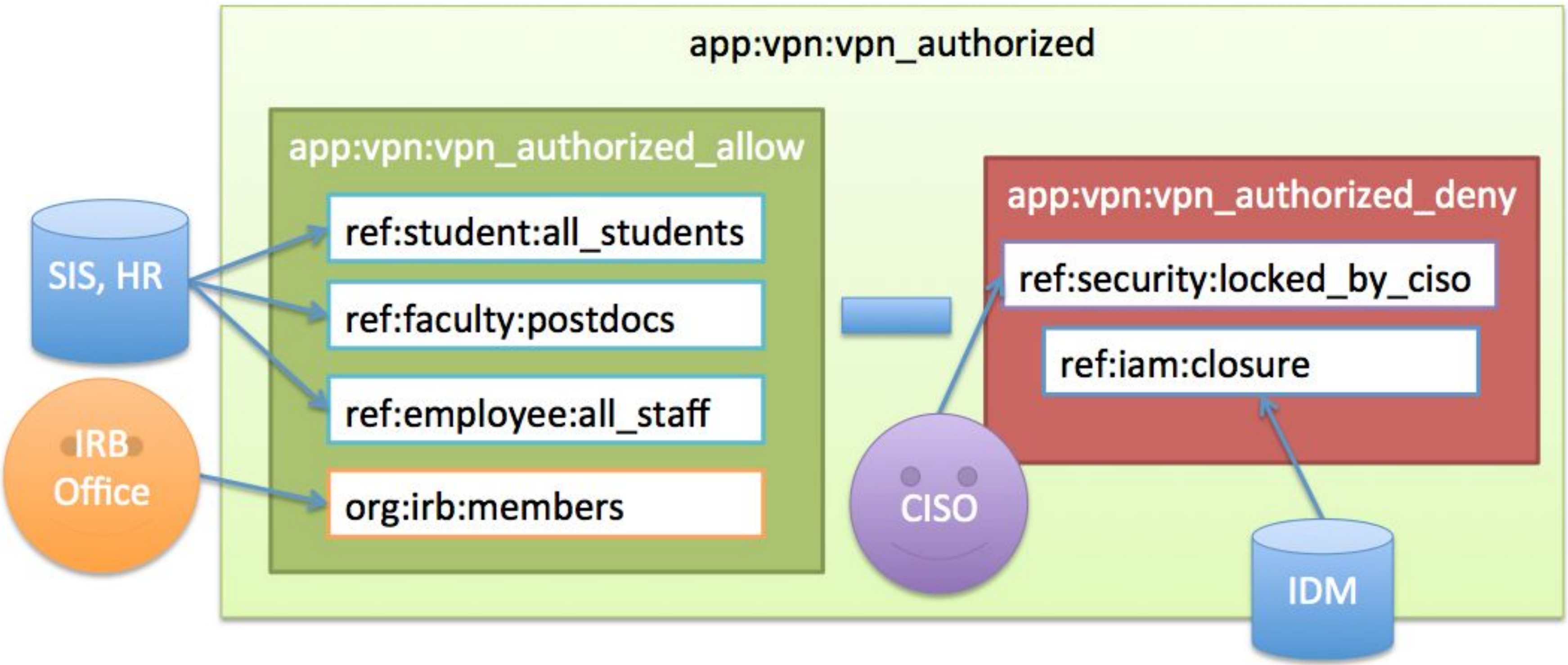
- NIST 800-162 ABAC
- Grouper glossary
- Grouper UI terminology

Grouper Specific

- **Direct membership** – subject added directly to a group's membership list
- **Indirect membership** – subject is a member by virtue of membership in another group
- **Composite group** - combining two other groups to form a third group

TIER Access Management

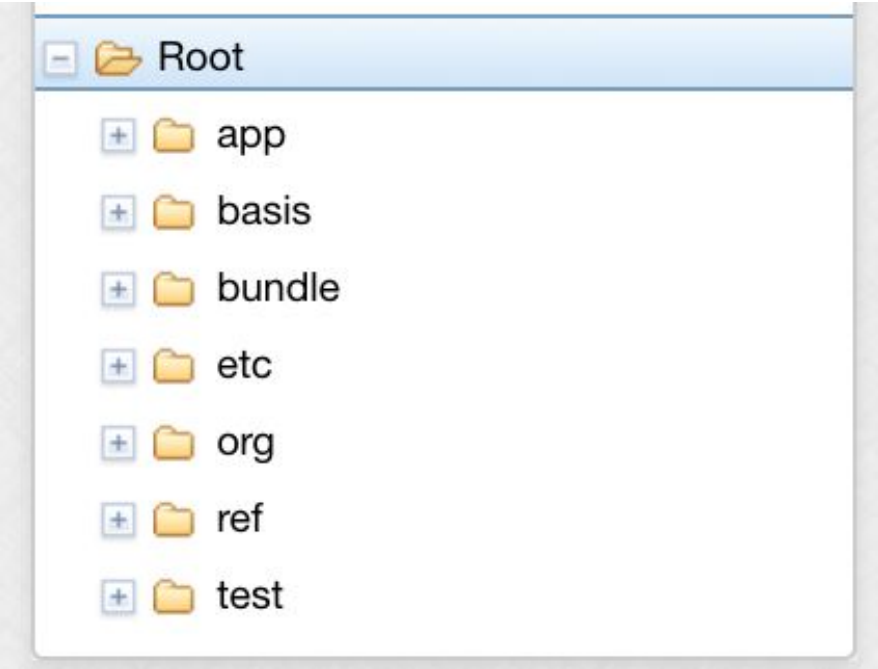
- **Basis group** – direct subject membership, low level, "raw" groups
- **Reference group** – institutionally meaningful cohorts - aka subject attributes
- **Access/Account policy group** – pre-computed policy decision



"All students, staff, postdocs, and members of the IRB have access to VPN unless their account has been locked by the CISO or is in the closure process."

TIER Folder and Group Design

"***Just having a plan or standard has been quite helpful, as it allows implementers to get on with real work without having to stumble on how to name things or where to stick them.***"
- Tom Barton



- Root
  - app
  - basis
  - bundle
  - etc
  - org
  - ref
  - test

TIER Folder and Group Design

Basis Groups - Systems of record codes (hidden away from access policy)

- **basis:hris:{employee_codes}**
- **basis:sis:{student_codes}**

Reference Groups - Institutionally meaningful cohorts – "truth" (aka subject attributes)

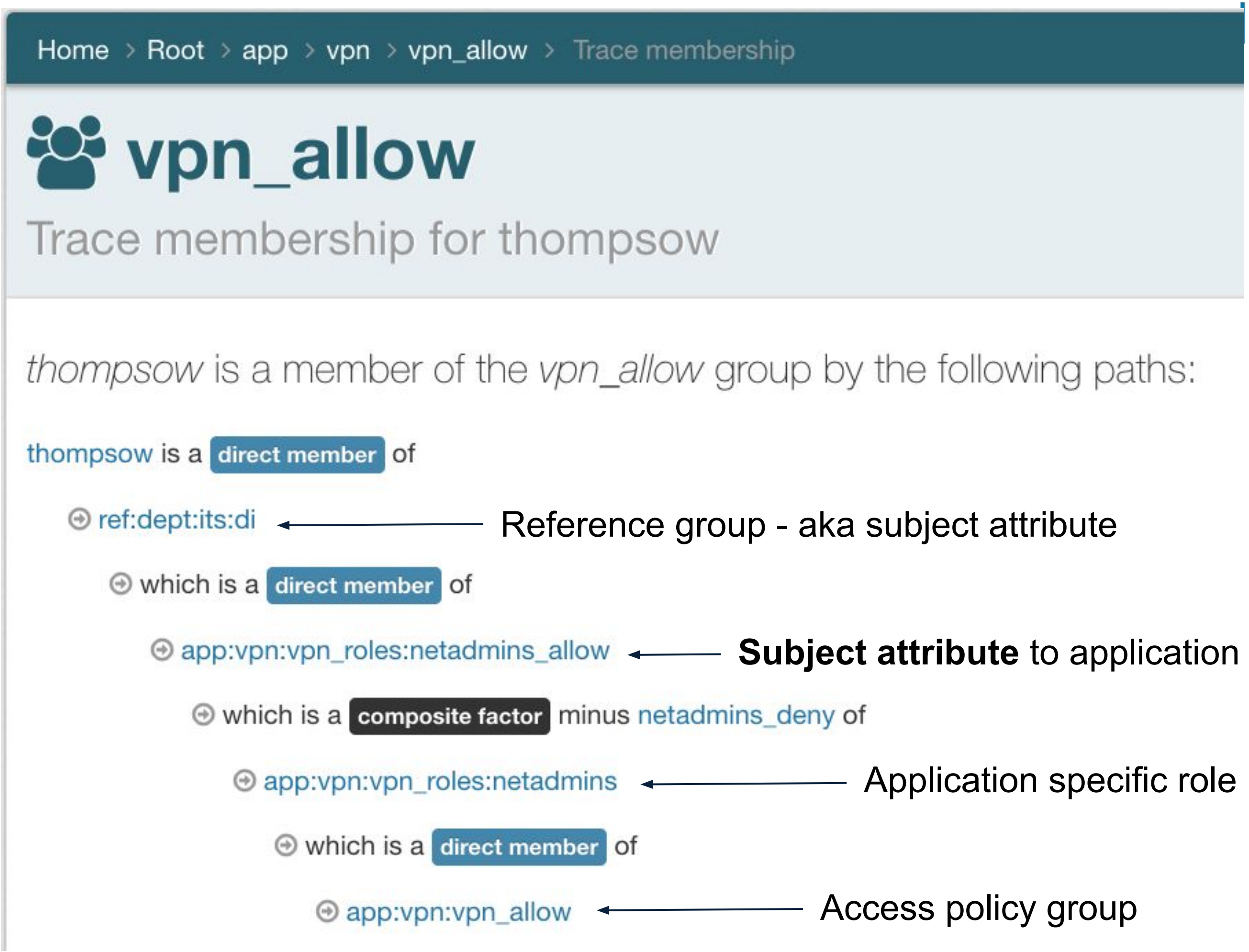
- **ref:role:** - institutional scope roles (e.g. president, provost, chaplain...)
- **ref:employee:** - types of employees (faculty, staff, part-time, full-time...)
- **ref:student:** - types of students

Access Policy Groups - digital policy based on subject attributes

- **app:vpn:vpn_allow** - allow policy for vpn access

Bundle Groups - Sets of reference groups (cohorts) used to drive access policy

- **bundle:employee_services** - cohorts that get employee-like access



Home › Root › app › vpn › vpn_allow › Trace membership

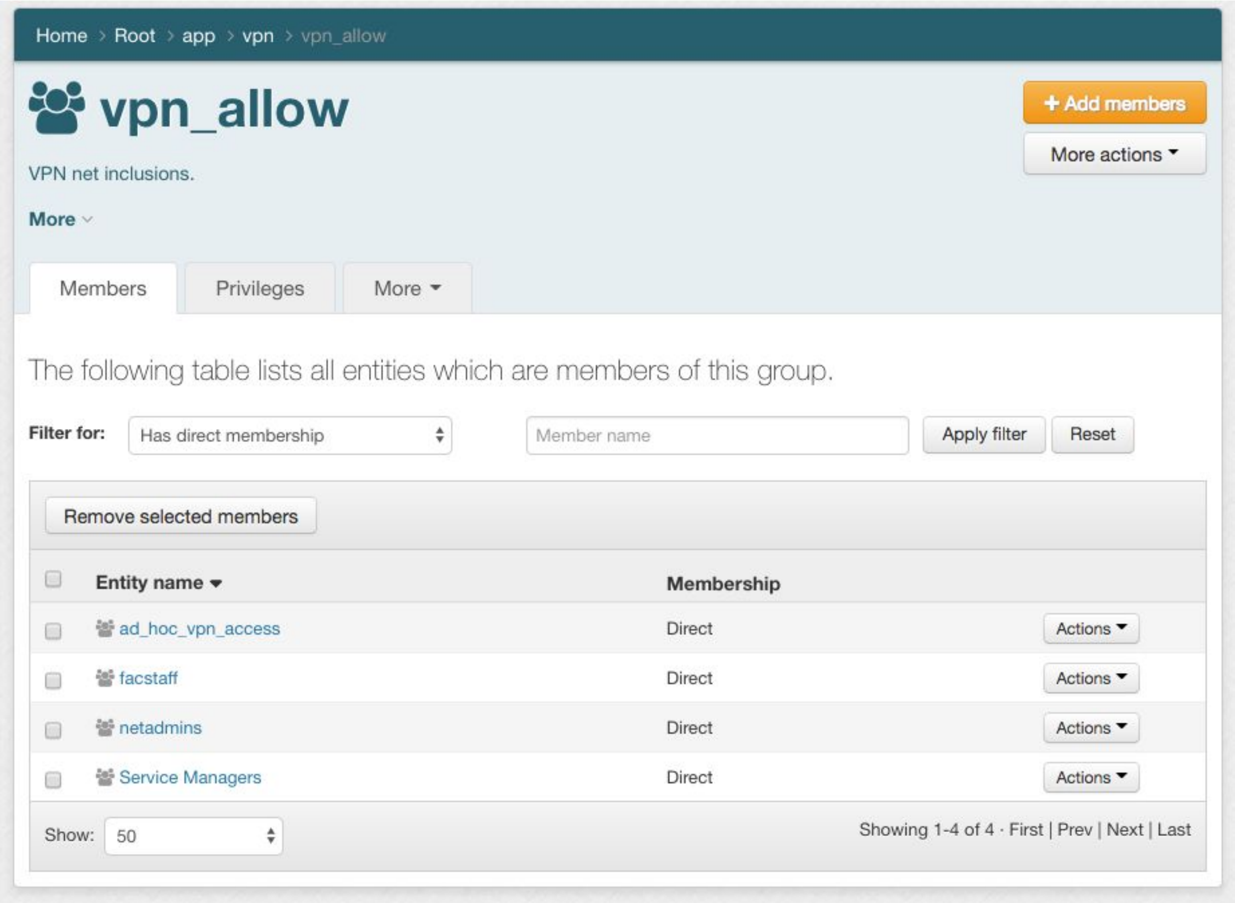
vpn_allow

Trace membership for thompsow

thompsow is a member of the *vpn_allow* group by the following paths:

thompsow is a **direct member** of

- ref:dept:its:di ← Reference group - aka subject attribute
  - which is a **direct member** of
    - app:vpn:vpn_roles:netadmins_allow ← **Subject attribute** to application role mapping
      - which is a **composite factor** minus netadmins_deny of
        - app:vpn:vpn_roles:netadmins ← Application specific role
          - which is a **direct member** of
            - app:vpn:vpn_allow ← Access policy group



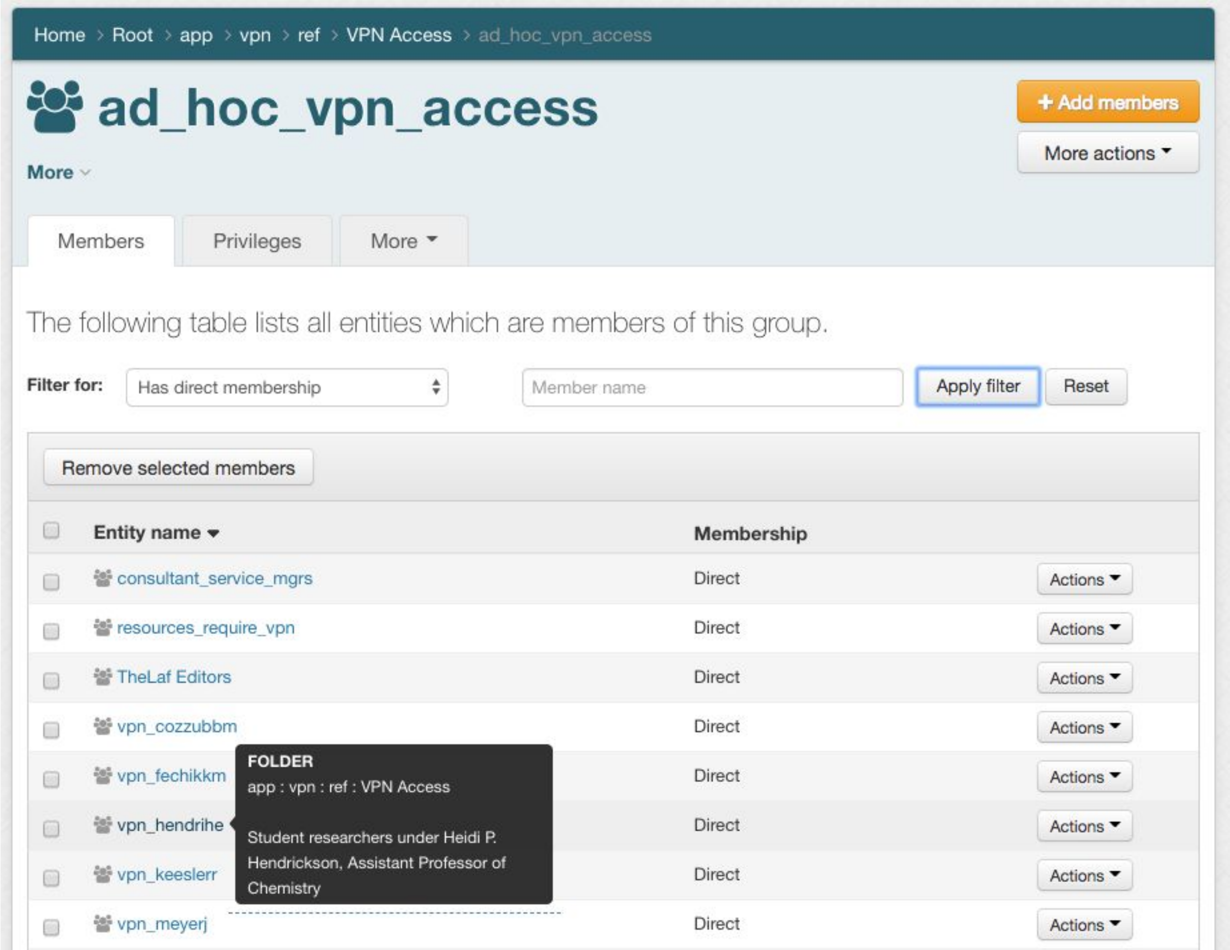
vpn_allow

VPN net inclusions.

The following table lists all entities which are members of this group.

□	Entity name	Membership	
□	ad_hoc_vpn_access	Direct	Actions
□	facstaff	Direct	Actions
□	netadmins	Direct	Actions
□	Service Managers	Direct	Actions

VPN access is granted to all faculty, staff, network administrators, service managers, and...exceptions.



Home › Root › app › vpn › ref › VPN Access › ad_hoc_vpn_access

ad_hoc_vpn_access

The following table lists all entities which are members of this group.

Filter for: Has direct membership | Member name

□	Entity name	Membership	
□	consultant_service_mgrs	Direct	Actions
□	resources_require_vpn	Direct	Actions
□	TheLaf Editors	Direct	Actions
□	vpn_cozzubbm	Direct	Actions
□	vpn_fechikkm	Direct	Actions
□	vpn_hendrihe	Direct	Actions
□	vpn_keeslerr	Direct	Actions
□	vpn_meyerj	Direct	Actions

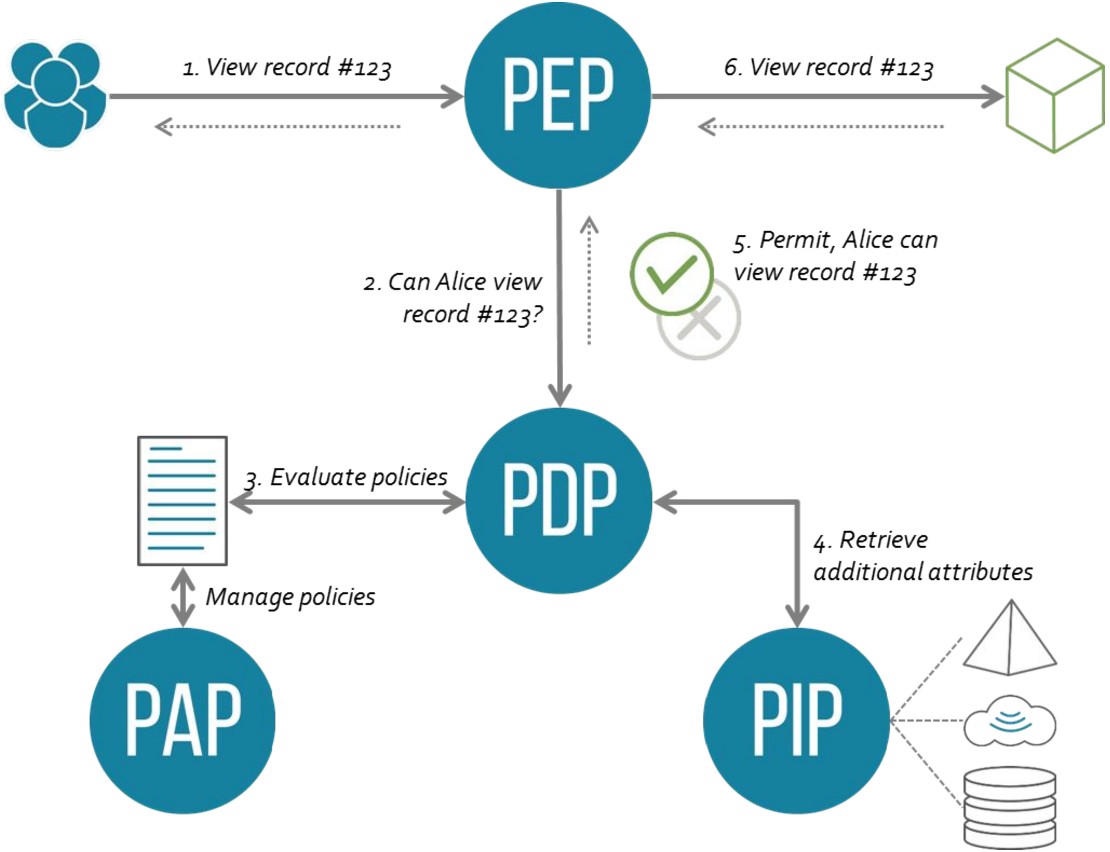
FOLDER
app : vpn : ref : VPN Access

Student researchers under Heidi P. Hendrickson, Assistant Professor of Chemistry

Managed exceptions. Delegated to appropriate people.

TIER Access Control Models

- Access Control Model 1 – Grouper Subject Attributes
- Access Control Model 2 – Grouper as PAP and PDP
- Access Control Model 3 – Application RBAC User to Role Mapping
- Access Control Model 4 – WebSSO Short-circuit


1. View record #123
PEP
6. View record #123
2. Can Alice view record #123?
5. Permit, Alice can view record #123
3. Evaluate policies
PDP
4. Retrieve additional attributes
Manage policies
PAP
PIP

By Axiomatics (Axiomatics) [CC BY 3.0 (http://creativecommons.org/licenses/by/3.0)], via Wikimedia Commons

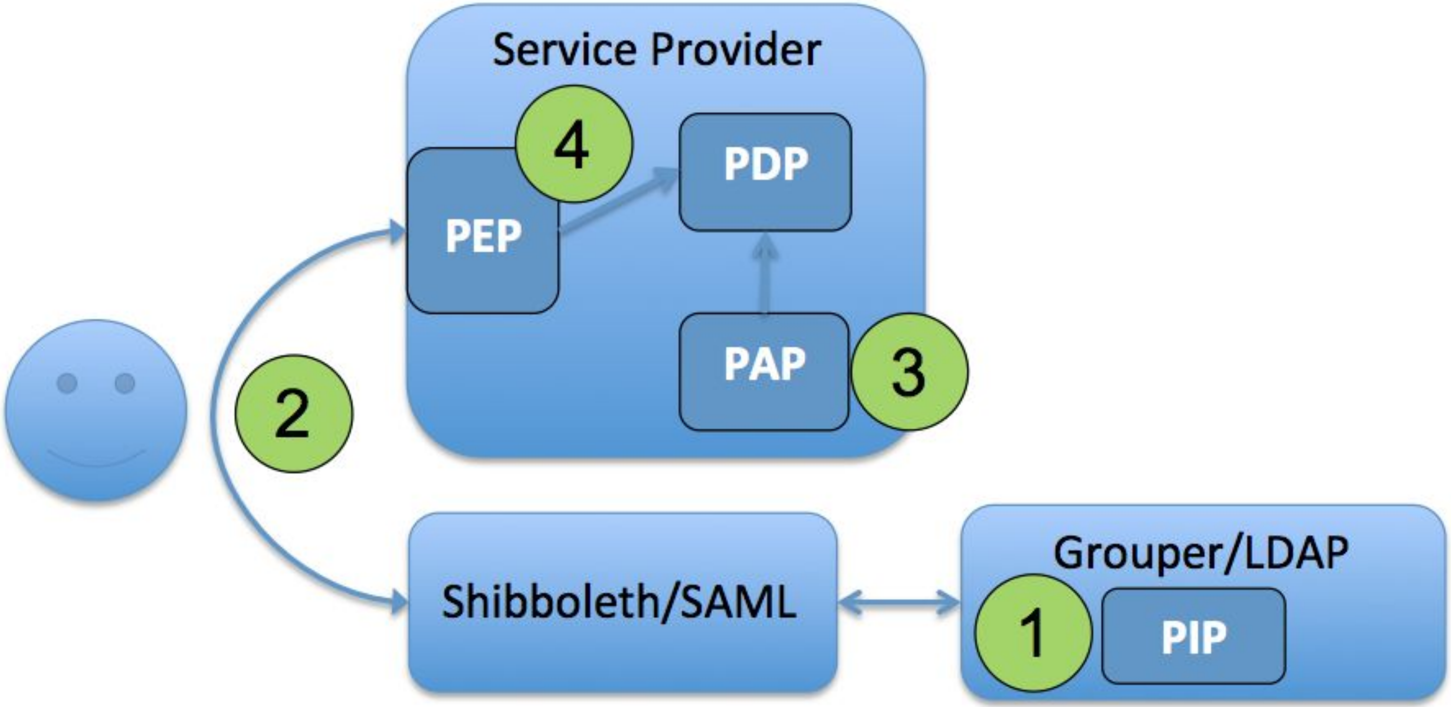
PAP - Policy Administration Point

PDP - Policy Decision Point

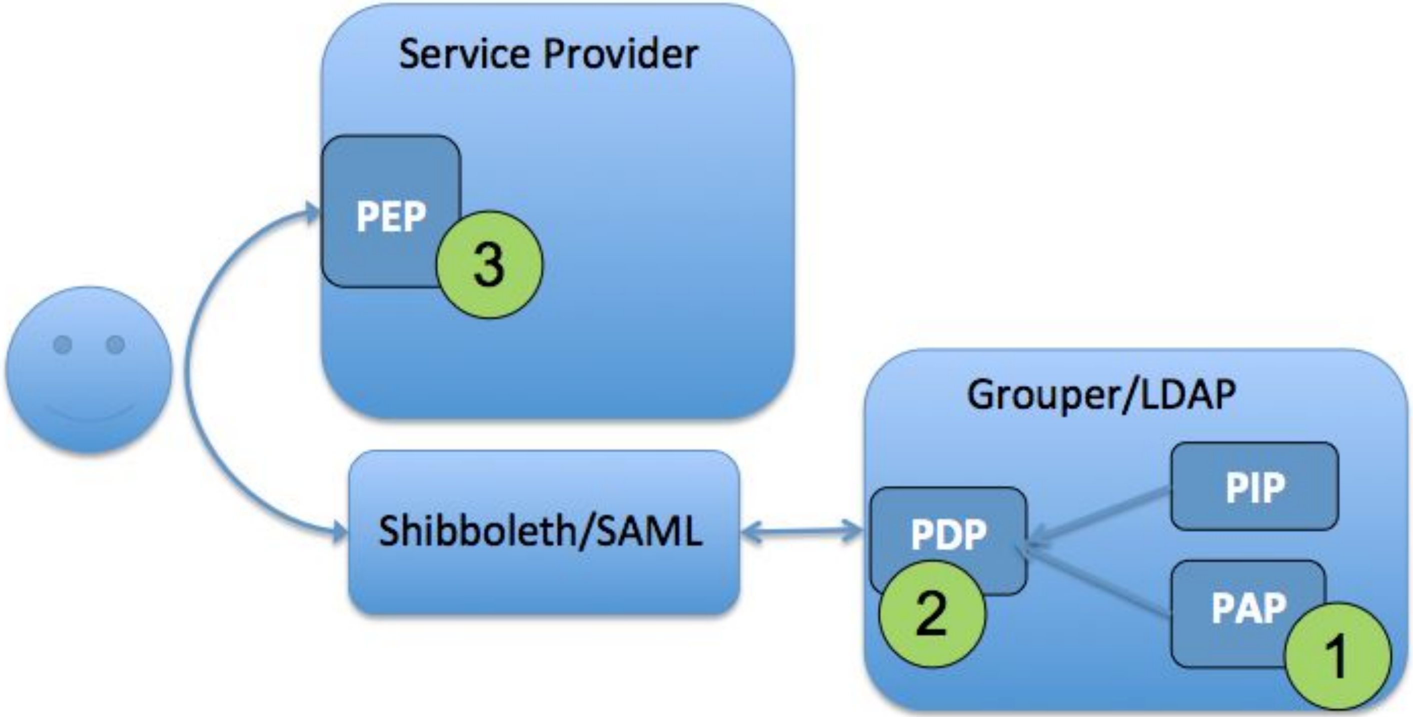
PEP - Policy Enforcement Point

PIP - Policy Information Point

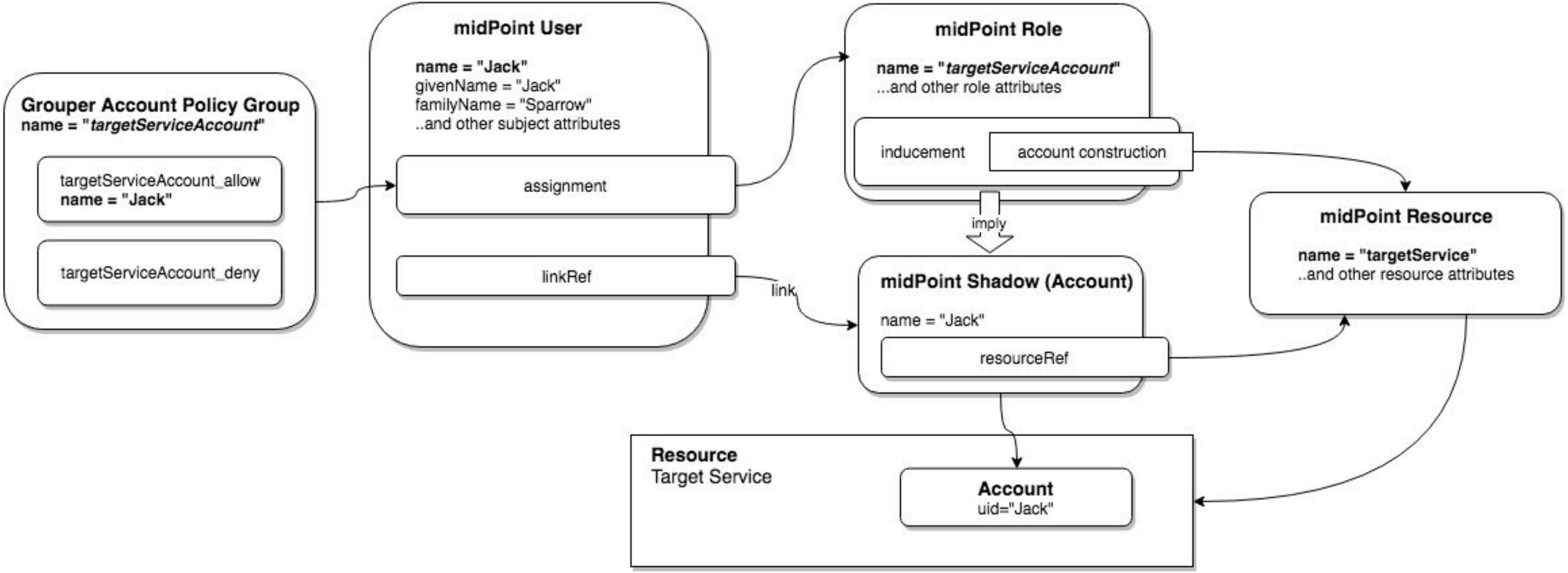
Access Control Model 1 – Grouper Subject Attributes - eduPersonAffiliation



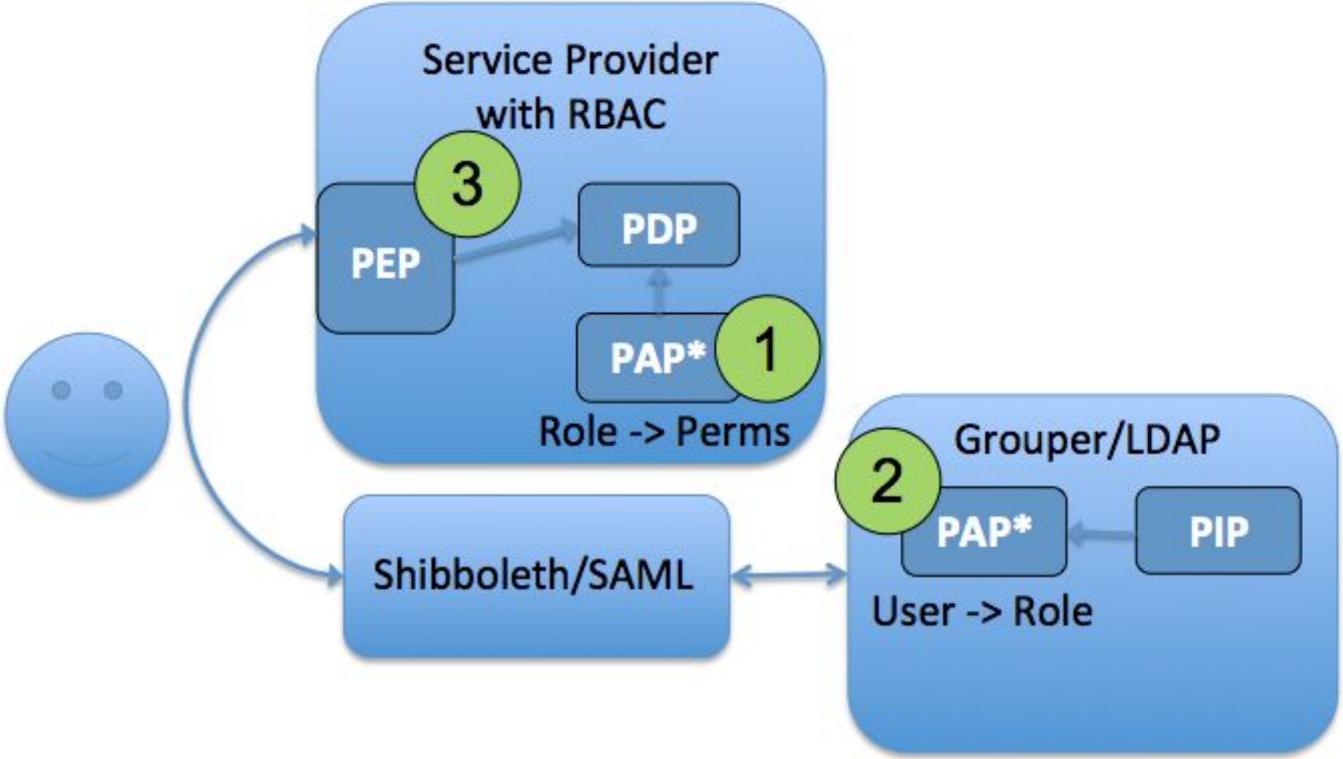
Access Control Model 2 – Grouper as PAP and PDP - eduPersonEntitlement



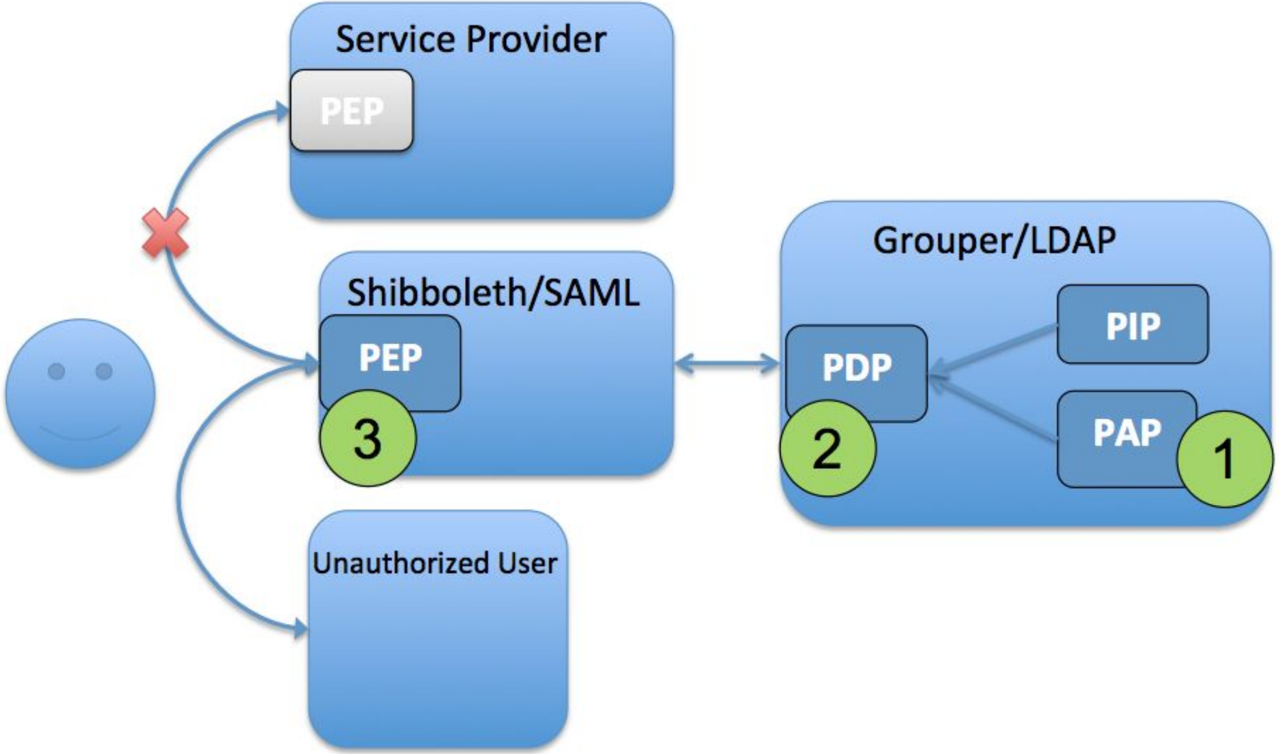
TIER Account Provisioning via Grouper and midPoint

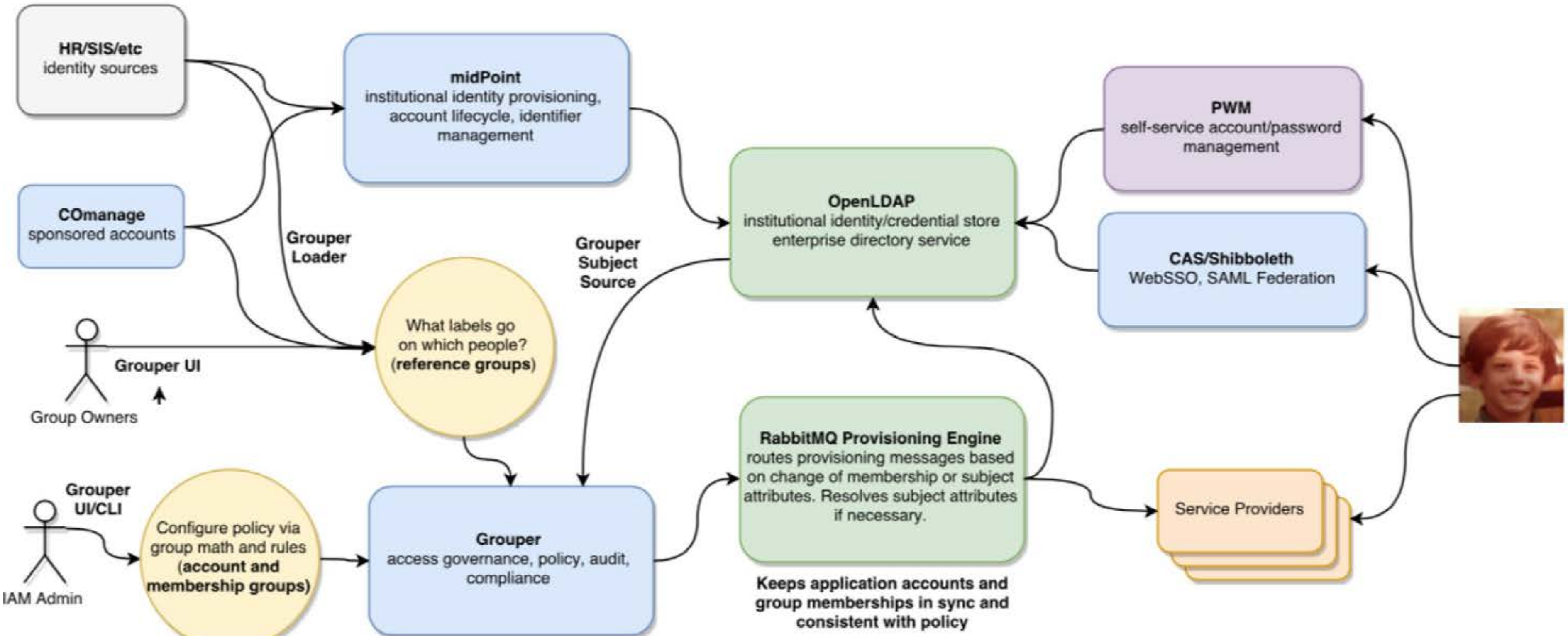

Grouper Account Policy Group
name = "targetServiceAccount"
targetServiceAccount_allow
name = "Jack"
targetServiceAccount_deny
midPoint User
name = "Jack"
givenName = "Jack"
familyName = "Sparrow"
..and other subject attributes
assignment
linkRef
link
midPoint Role
name = "targetServiceAccount"
...and other role attributes
inducement
account construction
imply
midPoint Shadow (Account)
name = "Jack"
resourceRef
midPoint Resource
name = "targetService"
..and other resource attributes
Resource
Target Service
Account
uid="Jack"

Access Control Model 3 – RBAC User to Role Mapping



Access Control Model 4 – WebSSO Short-circuit





HR/SIS/etc
identity sources

midPoint
institutional identity provisioning, account lifecycle, identifier management

COmanage
sponsored accounts

Grouper Loader

Grouper Subject Source

OpenLDAP
institutional identity/credential store enterprise directory service

PWM
self-service account/password management

CAS/Shibboleth
WebSSO, SAML Federation

What labels go on which people? (**reference groups**)

Grouper UI

Group Owners

Grouper UI/CLI

IAM Admin

Configure policy via group math and rules (**account and membership groups**)

Grouper
access governance, policy, audit, compliance

RabbitMQ Provisioning Engine
routes provisioning messages based on change of membership or subject attributes. Resolves subject attributes if necessary.

Service Providers

Keeps application accounts and group memberships in sync and consistent with policy

Account and membership groups represent authorization policy. Effective membership configured via group math or rules generates change notifications.

Reference groups represent the current state of membership for all subjects as known to the enterprise. They are used to configure access management policy and provide the means for automated provisioning of groups and accounts as well as audit and compliance.

TIER Subject Attribute Management and Access Governance

- Consistent model and terminology
  - Basis –> reference –> policy
  - Reference groups = subject attributes (institutionally meaningful cohorts)
  - Policy groups can implement ABAC, RBAC, and ACLs
- Strategy applies to all four access control models

- Policy is more organized, discoverable, manageable, and auditable
- Management of policy is consistent, easy, flexible, and can be delegated
- Improved security posture and ability to onboard new services quickly

TIER Access Governance with Grouper and Friends
https://meetings.internet2.edu/2018-technology-exchange/detail/10005135/
2018 Technology Exchange - Monday, September 28, 8am - 5pm

Please evaluate today’s session

https://www.surveymonkey.com/r/IAMOnline-Sept2018

2018 Internet2 Technology Exchange (TechEx)

October 15-19, 2018 - Orlando, Florida

https://meetings.internet2.edu/2018-technology-exchange/

- Two full tracks for Trust and Identity topics
- Advance CAMP (ACAMP)
- Pre-meeting tutorials

InCommon Shibboleth Workshop: Making Federation Easier

Brown University, Providence, Rhode Island
November 13-14, 2018

www.incommon.org/shibtraining