



# **Apereo Grouper Seminar Part 2 – Penn and Grouper**

Chris Hyzer

University of Pennsylvania and Internet2

# Agenda

- New & improved in latest & upcoming releases
- Qualtrics
- Confluence
- Kuali Rice eDoclite workflow
- Loader and provisioning
- External users and Secure Space

# Roadmap – v2.2

Release	Item	Description
2.2	New Grouper UI	Provide new UI capabilities that better meet community needs.
2.2	Services in Grouper	Tag objects in Grouper so that folders, groups, permissions can be associated with a "service" to make it easier for users to perform tasks in Grouper.
2.2	Improved Grouper configuration	Make Grouper more easily deployable and upgradeable across environments with cascaded config files and expression language in config file entries.
On-going	Grouper Core	Continue adding capabilities to meet requirements from the field.
On-going	Community contributions	Solicit and publicize <u>community contributions</u> of extensions and complements to Grouper.

# Roadmap – v2.2

Release	Item	Description
2.2	Legacy attribute migration	Migrate legacy attributes into the new attribute framework.
2.2	Unix GID management	Built-in support for managing unix GIDs

# Penn and Grouper

- Used Grouper centrally at Penn for 5 years
- 120k groups
- 2.7 million immediate memberships
- 10k permission assignments
- We use: UI, WS, GSH, loader, LDAP, client, external users, workflow with Quali Rice edoclite, heavily delegated

# Penn Grouper project team

- ~20% technical person
- ~20% data analyst
- Small requirements from various other people: manager, sysadmins, ldap admins, etc
- Note: during upgrades time requirements increase, these are average times

# Example application: Qualtrics

- Cloud survey tool which is not licensed to everyone at Penn
- People in various schools or centers see a different branded site
- Loader manages affiliate groups
- Responsible parties can add ad hoc members
- Shib entitlements communicate rights to qualtrics cloud application on login

# Example application: Qualtrics (continued)

Search results for: qualtrics

- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsBsd
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsBsd\_systemOfRecord
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsDental
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsDental\_systemOfRecord
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsDesign
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsDesign\_systemOfRecord
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsGse
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsGse\_systemOfRecord
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsInstResearch
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsInstResearch\_systemOfRecord
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsIsc
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsLaw
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsLaw\_systemOfRecord
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsNotMember
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsNotMember\_systemOfRecord
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsNursing
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsNursing\_systemOfRecord
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsSas
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsSas\_systemOfRecord
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsSeas
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsWharton
- 👤👤 penn:evp:businessServices:apps:qualtrics:qualtricsWharton\_systemOfRecord
- 👤👤 penn:gse:apps:qualtrics:qualtricsUsers
- 👤👤 penn:gse:apps:qualtrics:qualtricsUsers\_systemOfRecord
- 👤👤 penn:seas:security:qualtrics:qualtricsUsers
- 👤👤 test:seas:wsk:qualtricsUsers



# Example application: custom app admin console

- Custom app framework does groups (pre-dated Grouper), though not centrally
- Integrated so groups could be linked externally to Grouper
- For admins (all powerful), it is required that users be in the admins group

# Example application: custom app admin console (continued)

## Membership list

- Show DIRECT members of this group
- Show INDIRECT members of this group
- Show ALL members of this group (direct and indirect)

**Change display**

First name  **Change sort attribute**

This group has no direct members

- This is a composite group

 **penn:isc:ait:apps:fast:fastAdmins system of record intersection**

 **penn:community:employee:org:91XX - Information Systems and Computing Parent:91XX - Information Systems and Computing Parent**

[Remove composite group](#) [Replace composite factors](#) [Back to group summary](#)

# Example application: Confluence wiki
















- Confluence (our version at least) can have external groups (hopefully ldap)
- We externalized users and groups so we have single signon, and ability to use Grouper features:
  - Loader - Auto-deprovisioning
  - Reuse groups in other apps
  - Central report to see who has what
  - Decentralized management

# Example application: Confluence wiki

- Note: we have a rule for auto-assigning privileges

**Error: Too many results returned by one or more data sources - displaying truncated result set. Please narrow your search**

Search results for: confluence

 penn:isc:ait:apps:atlassian:groupsConfluence:direct\_lending\_admin  
 penn:isc:ait:apps:atlassian:groupsConfluence:direct\_lending\_contributors  
 penn:isc:ait:apps:atlassian:groupsConfluence:direct\_lending\_viewers  
 penn:isc:ait:apps:atlassian:groupsConfluence:dw\_refresh\_admin  
 penn:isc:ait:apps:atlassian:groupsConfluence:dw\_refresh\_contributors  
 penn:isc:ait:apps:atlassian:groupsConfluence:era\_admin  
 penn:isc:ait:apps:atlassian:groupsConfluence:era\_contributors  
 penn:isc:ait:apps:atlassian:groupsConfluence:era\_viewers  
 penn:isc:ait:apps:atlassian:groupsConfluence:harts  
 penn:isc:ait:apps:atlassian:groupsConfluence:international\_activities\_contributors  
 penn:isc:ait:apps:atlassian:groupsConfluence:isc\_admin  
 penn:isc:ait:apps:atlassian:groupsConfluence:isc\_ait  
 penn:isc:ait:apps:atlassian:groupsConfluence:isc\_contributors  
 penn:isc:ait:apps:atlassian:groupsConfluence:isc\_finance\_hr  
 penn:isc:ait:apps:atlassian:groupsConfluence:isc\_nt

# Grouper loader

- Daemon that periodically sync'ed external sources with Grouper
- Can work for groups or permissions (e.g. org chart)
- SQL or LDAP sources (note: PSP does LDAP too)
- Grouper admins can configure jobs based on attributes

## Grouper loader (continued)

- Can sync multiple groups from one query/filter (e.g. courses or orgs)
- Penn has 92 SQL Grouper Loader jobs
- Generally we run these daily, though some run a handful of times throughout the day

# Provisioning

- Grouper PSP can provision grouper data to LDAP or AD (other targets can be created)
- Grouper change log can send notifications to XMPP, ESB, etc (other targets can be created)
- Generally we aim for periodic full refresh, with near real time updates

# Auditing

- “User audit” will audit who does what
- Point-In-Time auditing will keep track of the history of the repository
  - Who was in this group at a point in time (or time range) in the past
  - Who are all the people who have been in this group
  - What groups was this person in at a point in the past (or time range)



# Grouper Kualiti Rice edoclite workflow

# Paper form screenshot

- In 2009 Penn wanted to convert paper access management forms to eForms

**Part I Identification Information** (please print) Check one:  New ID  Change privs.  Remove privs.

Full Name (include middle initial): \_\_\_\_\_

Phone Number: \_\_\_\_\_ - \_\_\_\_\_ Organization Name: \_\_\_\_\_

Address: \_\_\_\_\_

Email Address: \_\_\_\_\_ @ \_\_\_\_\_ PennCard ID Number: \_\_\_\_\_

PennNet ID (network ID): \_\_\_\_\_ Oracle ID (for changes, deletions): \_\_\_\_\_

As an individual whose position requires interaction with any or all of the University's administrative information systems, I may be provided with direct access to confidential and valuable data and/or use of data systems. In the interest of maintaining the integrity of these systems and of ensuring the security and proper use of University resources, I will maintain the confidentiality of my password for all systems to which I have access. I will maintain in strictest confidence the data to which I have access. Any confidential information will not be shared in any manner with others who are unauthorized to view such data. I will use my access to the University's systems for the sole purpose of conducting official business of the University. I understand that the use of these systems and their data for personal purposes is prohibited. I understand that any abuse of access to the University's systems and their data, any illegal use of copying of software, any misuse of the University's equipment may result in disciplinary action, loss of access to the University's systems, and possible sanctions consistent with the University Policy on Adherence to University Policy.

Requestor signature: \_\_\_\_\_ Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

Expiration Date: \_\_\_\_/\_\_\_\_/\_\_\_\_



# Paper form screenshot (continued)

<p><b>Part 2A Requested Access for:</b></p> <p><input type="checkbox"/> <b>Financial Balances</b></p>	<p><b>Part 2B Access Level:</b></p> <p>BEN Financials ID*: _____ (Access to Financial Balances will be granted with the same organization access as BEN Financials)</p> <p>*If you do not have a BEN Financials ID, specify level of access desired. Chart of Accounts training is the prerequisite for users without access to BEN Financials.</p> <p><input type="checkbox"/> University Wide <input type="checkbox"/> School -- School Number: _____ <input type="checkbox"/> Org Number: _____</p>
<p><b>Part 3A Requested Access for:</b></p> <p><input type="checkbox"/> <b>Salary Management</b></p>	<p><b>Part 3B Access Level: Specify <i>one</i> level of access required.</b></p> <p><input type="checkbox"/> University Wide <input type="checkbox"/> School -- School Number: _____ <input type="checkbox"/> Org Number: _____ <input type="checkbox"/> Employee General only* (no salary information)</p>
<p><b>Part 4A Requested Access for:</b></p> <p><input type="checkbox"/> <b>Position Inventory</b></p>	<p><b>Part 4B Access Level: Specify <i>one</i> level of access required.</b></p> <p><input type="checkbox"/> University Wide <input type="checkbox"/> School -- School Number: _____</p>

# Paper form screenshot (continued)

(continued on second page)

## Part 5A Requested Access for:

**Sponsored Projects**  
(use this form ONLY if you really need the old Sponsored Projects data... otherwise, please use the regular Data Warehouse Access form for Financial Data, and request access to PennERA Proposals)

**Part 5B Access Level:** Access to Sponsored Projects will be granted with the same organization access as BEN Financials. If you do not have a BEN Financials ID, please specify *one* level of access:

- University Wide  
 School -- School Number: \_\_\_\_\_  
 Org Number: \_\_\_\_\_

## Part 6 Type of Access

Business Objects Full Client?  Windows 98  Win2000/XP

OR

InfoView-only?

(If neither of the above, please specify method of access: \_\_\_\_\_)

# Paper form screenshot (continued)

## Part 7 Authorizing signatures

*The person named above has my approval for the requested warehouse access.*

Authorizing (ie., supervisor) Signature: \_\_\_\_\_ Date: \_\_\_\_/\_\_\_\_/\_\_\_\_  
(Required for all the data collections listed above)

School/Center Sr. BA Signature: \_\_\_\_\_ Date: \_\_\_\_/\_\_\_\_/\_\_\_\_  
(Required for all the data collections listed above)

Trainer Signature: \_\_\_\_\_ Date: \_\_\_\_/\_\_\_\_/\_\_\_\_  
(Required *only* for General Ledger access for non-BEN Financials users, to certify Chart of Accounts training)

Human Resources Signature: \_\_\_\_\_ Date: \_\_\_\_/\_\_\_\_/\_\_\_\_  
(Required for Salary Management\* and Position Inventory only)

Payroll Signature: \_\_\_\_\_ Date: \_\_\_\_/\_\_\_\_/\_\_\_\_  
(Required for Salary Management\* and Position Inventory only)

\*Human Resources and Payroll signatures are *not* required for requests for Salary Management – Employee General access.

# Paper form screenshot (continued)

**Part 8 To be completed by Security Administrator**

ID assigned: \_\_\_\_\_

Initial password assigned: \_\_\_\_\_

Data Administration initials: \_\_\_\_\_

Authorizations in order. Date received: \_\_\_/\_\_\_/\_\_\_

Authorization incomplete. Return to sender.

Date returned to Security Administrator: \_\_\_/\_\_\_/\_\_\_ Date completed: \_\_\_/\_\_\_/\_\_\_

Remarks:

**Send completed forms to:**

Data Administration - W.H. Access

██████████ Street/6228

**To request additional forms:**

URL <http://██████████forms.html>

# Paper form existing list

To request authorization and access, you must submit a Data Warehouse Access Request Form for each data collection you need. Be sure to check the appropriate check box on each form if you plan to use Business Objects or InfoView only. Select the form from these data collections:

- [Advancement Data Collection](#) (information from ATLAS)
- [Assets Data Collection](#) (property management asset information from the BEN Assets module of BEN Financials)
- [BRIM Data Collection](#) (Office of Research Services' Billing and Receivables Management)
- [Express Mail Collection](#) (access to Express Mail detail data)
- [Faculty Data Collection](#) (information from the Faculty Information System)
- [FRES Work Requests Data Collection](#) (information from Facilities and Real Estate Services Facility Focus System)
- [General Ledger , Salary, Position Inventory and PennERA Proposals Data Collections](#)

(Note: You may also this form to request access only to EMPLOYEE\_GENERAL and related tables, for the purposes of viewing basic employee and primary appointment information with no salary or job details.)

- [Sponsored Projects version](#) of the financial collection form (used only for access to old Sponsored Projects data, *not* Proposals)
- [Graduate Admissions](#) (for graduate and professional school reporting)
- [ISC Billing Data Collection](#) (access to Network billing, Telecommunications, and

# Requirements

- Autofill personal information
- Common includes (privacy statement)
- Fill out form on behalf of someone else
- Org chart picker for data access
- Person picker from group (employee)
- Notification to requester when complete
- Report on form data
- Should require no Java to create forms



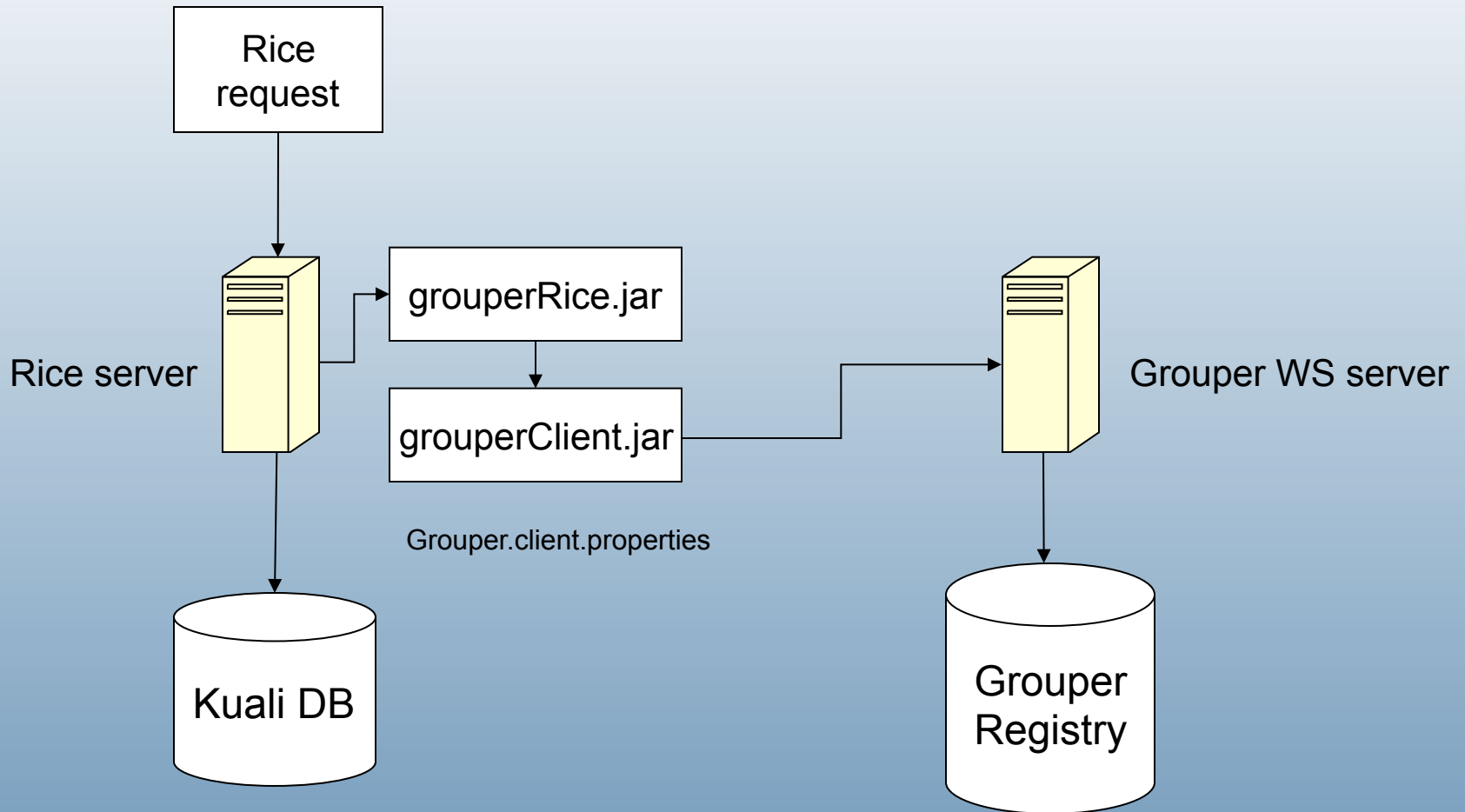
# Routing requirements

- Route to members of Groupers group
- Route to selected group (pick school)
- Ability to return to previous route node
- Route to multiple groups at once
- Conditional routing
- Dynamic routing to someone entered on form

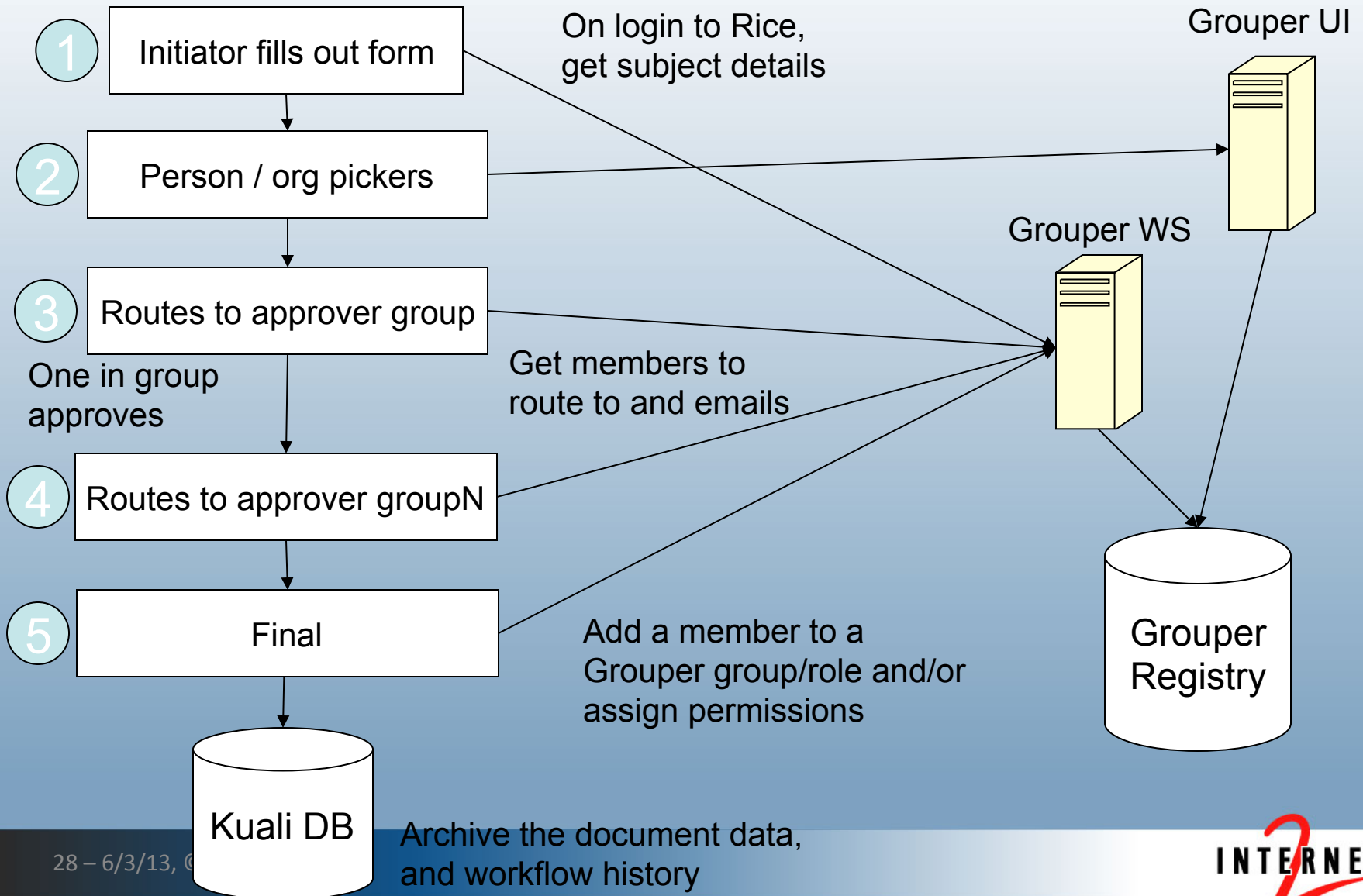
# Security requirements

- Submitters can see current and past forms
- Approvers can see current and past forms
- Certain people can edit certain forms

# Kuali Rice overridable services



# eForms workflow with Grouper



# Salary management eForm

Form name:	Salary Management access
Form status:	INITIATED
Create date:	07:50 PM 11/07/2010
Document ID:	3196

## Access Request Form: Data Warehouse Salary Management Collection

### Requester Information:

Please complete the fields below, and then click the **route** button to initiate your request. Fields with an asterisk (\*) are required.

**On behalf of Penn ID\***

**On behalf of (auto filled from above)** Michael Christopher Hyzer (m-123456789, 3-123456789) (active) Staff - Isc Administrative Systems Tools And Technologies - Programmer Analyst Sr (also: Alumni)

**Privilege change\***  New ID  Change privs  Remove privs **Oracle ID (for changes or deletions)**

**Name** Michael Christopher Hyzer (m-123456789, 3-123456789) (active) Staff - Isc Administrative Systems Tools And Technologies - Programmer Analyst Sr (also: Alumni)

**Expiration date (yyyy-Mon-dd)**

**Type of access\***  Business Objects  InfoView only  Other (please specify)

**Supervisor Penn ID\***

**Supervisor (auto filled from above)**

# Salary management eForm (continued)

Please specify level of access desired by selecting ORGs in the fields provided below.

Org*	<input type="text" value="0107"/>	<input type="button" value="Find org"/>	<input type="text" value="UNIV:USCH:02XX:FBBA:ENGL:0107"/>
Org	<input type="text"/>	<input type="button" value="Find org"/>	<input type="text"/>
Org	<input type="text"/>	<input type="button" value="Find org"/>	<input type="text"/>
Org	<input type="text"/>	<input type="button" value="Find org"/>	<input type="text"/>
Org	<input type="text"/>	<input type="button" value="Find org"/>	<input type="text"/>

[More orgs](#)

As an individual whose position requires interaction with any or all of the University's administrative information systems, I may be provided with direct access to confidential and valuable data and/or use of data systems. In the interest of maintaining the integrity of these systems and of ensuring the security and proper use of University resources, I will maintain the confidentiality of my password for all systems to which I have access. I will maintain in strictest confidence the data to which I have access. Any confidential information will not be shared in any manner with others who are unauthorized to view such data. I will use my access to the University's systems for the sole purpose of conducting official business of the University. I understand that the use of these systems and their data for personal purposes is prohibited. I understand that any abuse of access to the University's systems and their data, any illegal use of copying of software, any misuse of the University's equipment may result in disciplinary action, loss of access to the University's systems, and possible sanctions consistent with the University Policy on Adherence to University Policy.

**I will abide by this policy\***

# Salary management eForm (continued)

## Supervisor Action:

Please select the appropriate School/Center Access Administrator from the list.

School/Center Access Administrator\*

## Form Routing:

To add a comment to your request or approval action, enter it in the Note field provided and click the **save** button.  
Click the appropriate button (**route**, **approve**, **disapprove**, etc.) to submit the form for continued processing in the workflow.

Create Note			
Author	Date	Note	Action
Michael Christopher Hyzer (n [REDACTED]) (active) Staff - Isc Administrative Systems Tools And Technologies - Programmer Analyst Sr (also: Alumni)	11/07/2010	<input type="text"/>	<input type="button" value="save"/>

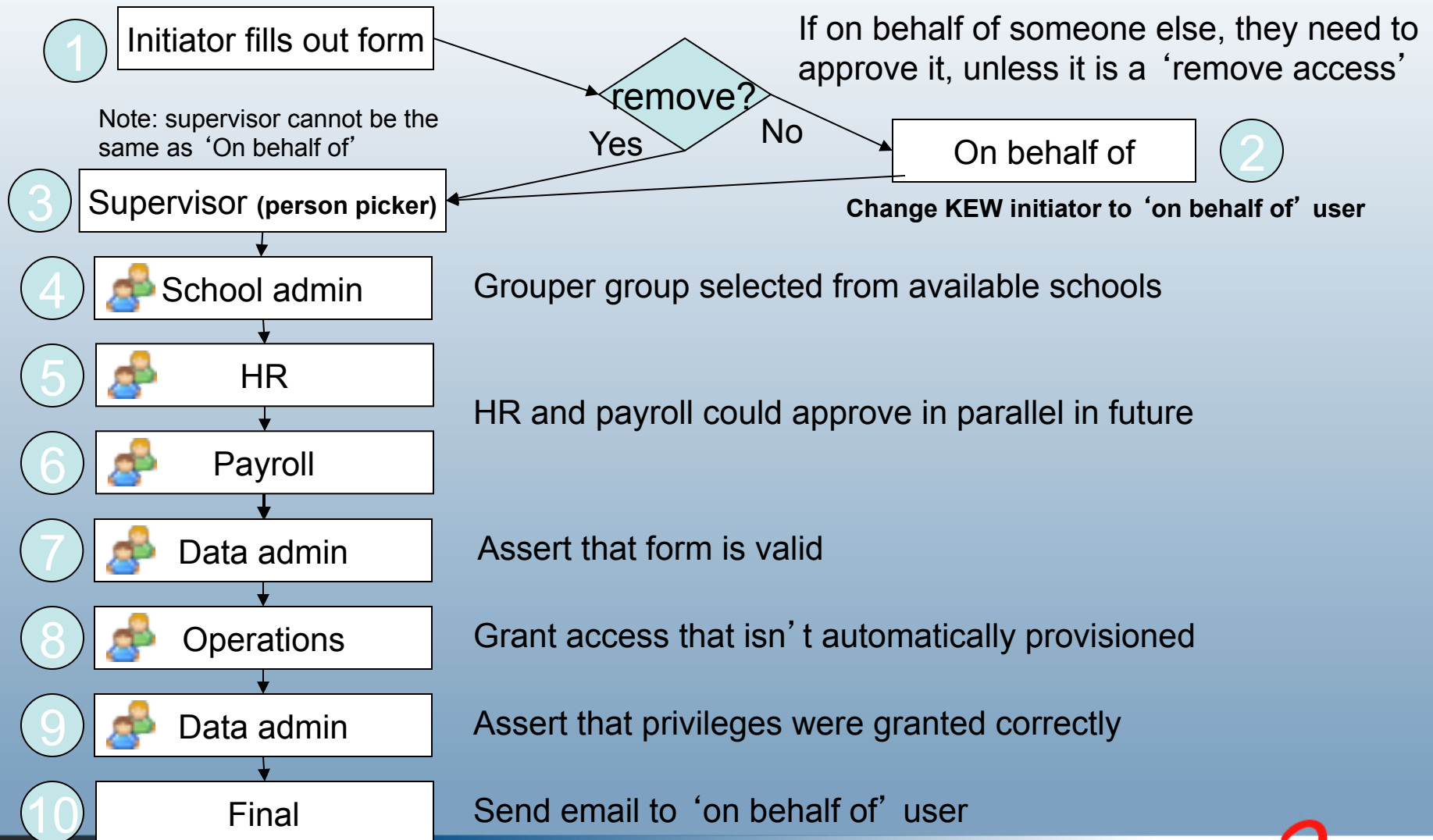
## Implementation Notes:

For internal ISC use only. The following implementation actions are complete:

- Oracle ID assigned
- Data Warehouse access
- Listserv membership(s)
- Business Objects access

Form template last revised 08/04/2010

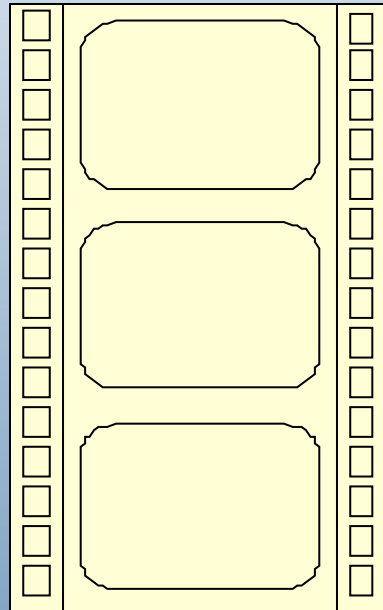
# eForms demo workflow





# Grouper Rice demo

- Demo movie



# Grouper Rice group provisioning

- Grouper can provision groups and permissions when forms are complete, but generally Penn does not use it that way

# Grouper and external users

# Penn' s Secure Space

- Penn launched Secure Space in Fall 2010
- Initially it was for PennKey holders only
- 2011 we enabled external users
- 2013 we will retire this service in favor of Box.net

# Penn' s Secure Space (continued)

- Secure Space is built on Grouper with three groups per space: admins, users, readonly
- When logging in, the grouper client / WS is used to cache the list of groups for user
- On create/delete space, GC/WS is used to create/delete groups
- Group memberships are managed via the membership lite UI screen

# Penn' s Secure Space (continued)

- Penn' s Grouper has rules to only allow external users in certain SS folders
- Penn' s Grouper external users must be invited to be able to register
- SecureSpace uses InCommon
- EPPN is required for external users
- External users self-register their name, email, institution

# Penn' s Secure Space (continued)

- Penn installed Shibboleth Discovery Service (DS/WAYF), customized:
  - Pennify
  - Support channel
  - Make it easy for Penn users
  - Recommend ProtectNetwork for users who don' t have an InCommon account which releases EPPN

# Penn' s Secure Space (continued)

- Grouper shows external users with different icon, and description:
- [unverifiedInfo] First Last - institution  
[externalUserId] userId@institution.suf
- External users do not show in results for groups which do not allow external users
- Demo



# Thanks!

## Further information:

Infosheets, mail lists, wiki, downloads, etc:  
[www.internet2.edu/grouper](http://www.internet2.edu/grouper)

Grouper demo server:  
<https://grouperdemo.internet2.edu/>