



Bedework v Identity Services

Gary Schwartz

Communications & Middleware Technologies,

Rensselaer Polytechnic Institute

Bedework project manager

Advanced CAMP: Identity Services Summit for Higher Ed

Open/Community-Source Projects

June 18–19, 2009

Philadelphia, Pennsylvania

Copyright Michael A. Douglass, Arlen D.H. Johnson and Gary Schwartz 2009. This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this written permission from the author.



I'm a Bedework-er,

- **not a psychiatrist**
- **not an escalator**
- **not a bricklayer**
- **not a mechanic**
- **not an engineer**
- **not a coal miner**

Or

a Federated Identity expert



Overview of Bedework





What Is Bedework?

- **Comprehensive calendaring/events**
 - **open source, *and* exploits/assumes other OSS - Mozilla Lightning, OpenConnector, ical4j, CalDAV4j, Hibernate, Lucene**
 - **platform independent (Java)**
 - **modular & extensible**
 - **higher education aware**

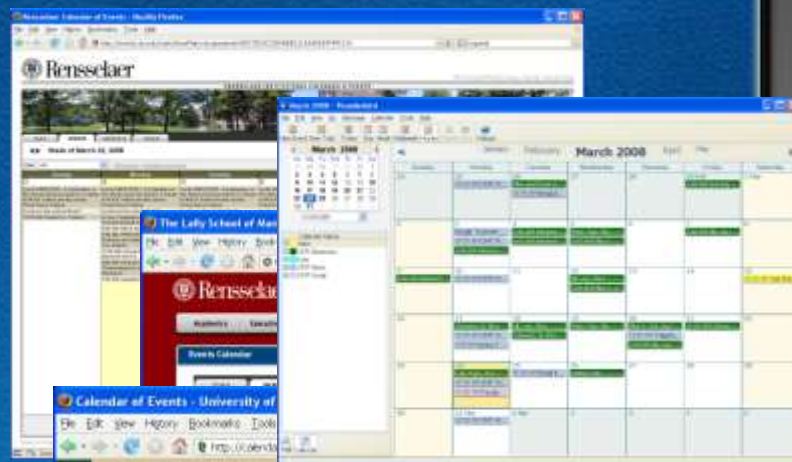


Bedework at this meeting

- **Brown**
- **Chicago**
- **Cornell**
- **Duke**
- **Maryland**
- **RPI**
- **UBC**



- Five main components:
 - public suites & data feeds
 - administrative client
 - event submission client
 - personal client
 - CalDAV





calendar bedework

Duke Buzz

Duke Student Calendar - Windows Internet Explorer

http://buzz.duke.edu/bedework/calendar-nb

buzz | Duke Student Calendar | FEBRUARY 22, 2009 | HELP

Calendar Views: DAY WEEK MONTH YEAR

Calendar Views

Sunday, February 22, 2009

All

- Official Duke Academic Calendar
- Arts
- Activities/Recreation
- Lectures/Conferences
- Religious/Spiritual
- University Events
- Volunteer/Community Service
- Workshop/Short Course
- Other
- Free Food and Beverages
- Guests
- Search Multiple Categories
- Search by Group

ADDITIONAL FUNCTIONS

- Manage Events
- Submit an Event

Events@Duke

Sunday, February 22, 2009

Men's Golf at Jacksonville, Fla.
Location: See description
Categories: Athletics/Recreation

Women's Golf at Mexico
Location: See description
Categories: Athletics/Recreation Sports/Volleyball

Sunday Morning Catholic Mass
Location: White 117 Lecture Hall
Categories: Religious/Spiritual

Madagascar: Escape 2 Africa (2008)
Location: Bryan Center Griffin Film Theater
Categories: Movies/Film

Duke Democratic General Body Meeting
Location: Bryan Center Griffin Board Room
Categories: Meetings

Priority One
Location: McClellan 2nd Floor Media Room
Categories: Religious/Spiritual

Women's Basketball at Maryland
Location: See description
Categories: Athletics/Recreation Sports/Volleyball

Men's Basketball vs. Wake Forest
Location: Cameron Indoor Stadium
Categories: Athletics/Recreation Sports/Volleyball

Sunday Evening Catholic Mass
Location: Duke Chapel
Categories: Religious/Spiritual

2009 Ethics Film Series

"The Axe in the Attic"
7 p.m. Feb. 24
Bryan Center Griffin Film Theater

"What is Grand Strategy?"
Lecture by John Lewis Gaddis
9:30 p.m. Feb. 26
Sanford Hall Duke Freshman Commons

"Infection in the Sentence Breeds"
A Festival of Poetry

Events@Duke

February 22, 2009

Calendar Views

Sunday, February 22, 2009

All

- Official Academic Calendar
- Arts
- Activities/Recreation
- Lectures/Conferences
- Religious/Spiritual
- University Events
- Workshop/Short Course
- Other
- Free Food and Beverages
- Guests
- Search Multiple Categories
- Search by Group

ADDITIONAL FUNCTIONS

- Manage Events
- Submit an Event

Events@Duke

Sunday, February 22, 2009

Men's Golf at Jacksonville, Fla.
Location: See description

Women's Golf at Mexico
Location: See description

Sunday Morning Catholic Mass
Location: White 117 Lecture Hall

Service of Worship
Location: Duke Chapel

Madagascar: Escape 2 Africa (2008)
Location: Bryan Center Griffin Film Theater

Duke Democratic General Body Meeting
Location: Bryan Center Griffin Board Room

Women's Basketball at Maryland
Location: See description

Men's Basketball vs. Wake Forest
Location: Cameron Indoor Stadium

2009 Ethics Film Series

"The Axe in the Attic"
7 p.m. Feb. 24
Bryan Center Griffin Film Theater

"What is Grand Strategy?"
Lecture by John Lewis Gaddis
9:30 p.m. Feb. 26
Sanford Hall Duke Freshman Commons

"Infection in the Sentence Breeds"
A Festival of Poetry

"The students said they liked Events@Duke, but they needed something more 'student-friendly' that filtered events relevant to students," said Johnson, who led a student focus group that advised a team of representatives from the Offices of IT, Student Activities, and Undergrad Education. Students came up with the name and categories such as "free food".



- **Jasig has officially accepted Bedework as an Incubating Project.**





Bedework Project Survey



- **public calendar & data feeds**
- **web-based clients for**
 - administration,
 - event submission
 - personal calendaring,
- **servers for**
 - CalDAV,
 - CardDAV,
 - and Timezones.



Technology Stack

- **Java**
- **Struts**
- **Hibernate**
- **Ehcache**
- **iCal4j**
- **Lucene**
- **jQuery**
- **Xalan-Java**
- **Apache Commons.**



Bedework is implemented as fully standard (JSR 154) collection of servlets, and as such relies on the container for authentication



- **Bedework implements interfaces which provide basic LDAP support to obtain principal group information and principal attributes.**
- **Shibbolized instances of Bedework have been deployed, but there are compatibility issues with CalDAV and Shibboleth.**



- **Authorization within Bedework services is based on DAV access control using ACLs.**
 - **This is proving to be complex for users, and inadequate in that the assignment of roles to a principal needs to affect multiple services, e.g. CalDAV and CardDAV.**



- **Shibboleth implements Web Browser Single-Sign On profile of SAML, which requires a full web-browser to run.**
 - **Virtually no *-DAV clients are full web browsers. We need something else to base federated identity authorization for *-DAV (CalDAV, CardDAV, WebDAV, etc).**



calendar bedework

In detail



- **Bedework is largely a consumer of directory information through an abstract interface.**
- **We need to map LDAP information onto the principal hierarchies expected in the DAV world, e.g.**
 - **id=douglm,ou=accounts,d=rpi,r=edu <--> /principals/users/douglm**
 - **and similarly for groups.**
 - **groups need to be multi-level, e.g. /principals/groups/dotcio/cmt**
 - **Groups can be members of groups**
 - **Apple assume that user principals are also groups - this is how they make people proxies, they create 2 groups (1 for read, 1 for read/write) that are members of the user principal group and then add principals to those groups.**



- **Maintained distinctly because there is an account associated with the group.**
- **Could do in LDAP but many Bedework deployers have no privilege to modify site LDAP schema.**
- **In next release, groups may be fully fledged principals,**
 - **i.e. they can own things, at which point it becomes easier to move the admin groups into LDAP.**
 - **we may no longer have to implement group management in Bedework, using the packaged directory server instead**



- **At start of a session, Bedework obtains group membership for current user**
- **if you're a member of /rpi/dotcio and also /rpi/dotcio/cmt**
 - **any specific rights for /rpi/dotcio/cmt should override those for /rpi/dotcio.**
- **Need to ensure that user X logging into the admin client doesn't get the same group membership as when X logs in to the personal client**
 - **Lest they have write access to the public tree when doing personal calendaring.**



- **“We should all be concerned about the future because we will have to spend the rest of our lives there.” – Charles Kettering**



- **iSchedule** - <https://www.ietf.org/mailman/listinfo/ischedule>
 - a binding from (iTIP) to (HTTP) to enable interoperability between calendaring and scheduling systems over the Internet.
 - specifies how a calendar service (iSchedule Sender) transmits scheduling messages (iTIP messages) to another calendar service (iSchedule Receiver)
 - Server-server trust model



- **Federated/cloud/aggregation**
- **Workflow, Authentication, Discovery**
- **Social networking**
- **Semantic Web**
- **Handheld/mobile**
- **Massive scalability**
- **Pervasive internationalization/localization**
- **Event aggregators / harvesters**
- **Calendaring as a platform**



Yes, we speak of things that matter,

With words that must be said,

Can analysis be worthwhile?

Is the desktop client really dead?



- **We need new, closer, more pervasive collaborations between Middleware / IDM developers/practitioners and calendaring developers / practitioners.**