Federated AAI and the World of Tomorrow

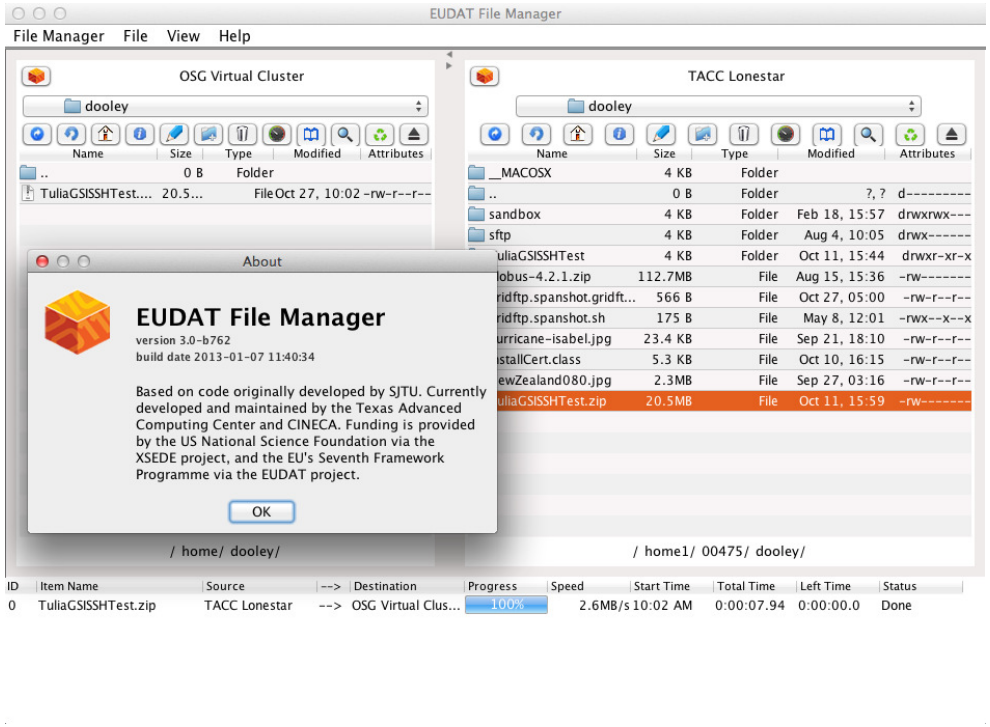
Rion Dooley

Who is this guy?

- Systems provider @ TACC
- Infrastructure provider @ iPlant/XSEDE
- Service provider @ Agave
- Application developer @ GatewayDNA
- Support staff @ all of the above
- Community advocate @ SGW-I
- Authz/n practitioner @ SGW Security

Why is he here?

- XSEDE File Manager
  - Move data
  - Manage data
  - Manage metadata
  - Multiple sources
  - Multiple protocols
  - Used by EUDAT



…and how this is a FAAI talk?

- File manager is the “Hello world!” federation scenario
  - Desktop app
  - User supplied credentials
  - Fully delegated authz/n
  - In-memory cache
  - Disappears when the app closes

Stop, we've heard this before!

- Windows SAM Registry Hive
- Apple Keychain
- SSH Keys
- …

Yes, but…times are changing

- It's not a desktop driven world anymore

Desktops
Notebooks
Tablets
Phones
Televisions

Cable consoles
Gaming consoles
Handheld games
Appliances
Automobiles
"Music players"

But we've solved this already

- Lastpass
- Passbook
- Firefox password manager
- …

…and when that doesn't work

- Login with Facebook
- Login with Twitter

Thank you

It’s not really that easy

- Multiple identities
- Multiple protocols
- Multiple credential servers and flows
- Knowing what and when to apply them
- Still has to be easy to use

Things are getting cloudy

- Now the apps are in the cloud
- Many have only a programmatic interface (API)
- Tons of services providers, tons of services
- Everyone has their own IdP
- You're still you
- Admins still don't trust anyone
- Apps now need to interact with systems as well as services.

Pick your problem

- **Identity:** Who are you?
- **Authentication**: Are you who you say you are?
- **Authorization**: Do you have permission to do what you want to do?
- **Federation**: Are these two different identities the same person?
- **Delegation**: How do I allow another to do something on my behalf?

Identity

- **Rank of Difficulty:** 4
- **Approach**:
  - Use existing trust relationships to verify the person from campus, service provider, or email validation
- **Policy Issues**:
  - Establishing the trust relationship
  - Software stack at IDP
- **Technical Issues**:
  - Creates inconsistent UX
  - Inadequate information

Authentication

- **Rank of Difficulty:** 5
- **Approach**:
  - Ask the remote identity provider
  - Cache/persist the response (profile, token, cert)
- **Policy Issues:**
  - How do we accessing the identity provider
- **Technical Issues**:
  - Performance
  - Namespace conflicts (see resolution)

Authorization

- **Rank of Difficulty:** 1
- **Approach:**

  UNIX groups and permissions
  VOMS
  AD/LDAP
  Grouper
  SAML
  SCIM
  CDMI
  Roll your own
- **Policy Issues:**
  - Decisions made at a high level
  - Change must occur there as well
  - Economics of interoperability (i.e. Quid pro No-Go)

Authorization

- **Technical Issues:**
  - Very few approaches interoperate
  - Concepts don't always map over well (states, roles, etc)
  - How to administer federated identities control
  - How to recognize and apply contextual ACL
  - Mismatched degrees of granularity (groups, shared accounts, user accounts, application accounts, etc)

Federation

- **Degree of difficulty:** 2
- **Approach:**
  - Pick your supported IdP
  - Set up a database
  - Define your flows
  - Get to mapping
- **Policy Issues:**
  - Getting permission from the IdP
  - Credential policies
  - Disparate vetting processes
  - What is the mechanism for feedback?
  - When to force resolution?

Federation

- **Technical Issues:**
  - Namespace conflicts
  - ”Dead" accounts can be reused
  - Shared accounts can map to multiple people rather than one
  - Man in the middle
  - Mismatching information
  - Lack of desire
  - Requires human intervention
  - Implementing levels of assurance
  - Tough for legacy systems with a lot of duplicate accounts
  - Accounting and billing become a game
  - Users WILL try to game the system
  - What level/kind of reporting is required?

Delegation

- **Degree of difficulty:** 3
- **Approach:**
  - Verify permission
  - Record answer
  - Create appropriate delegation credential
  - Log everything
- **Policy Issues:**
  - Service providers may not allow this
  - IdP may forbid this
  - Users generally all want this
  - What is the feedback loop for revoked users/accounts/permissions?

Delegation

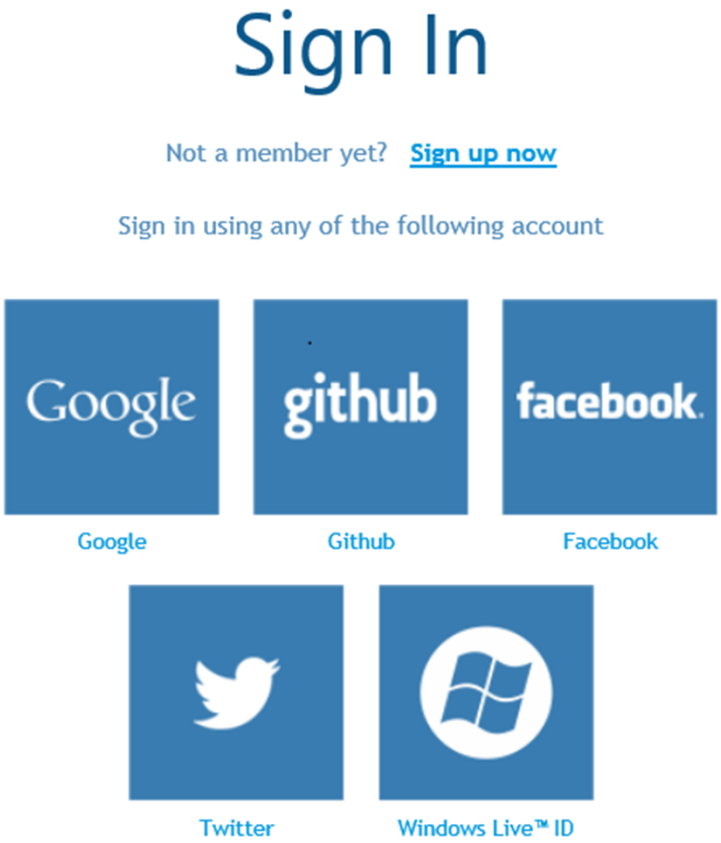
- **Technical Issues:**
  - security implications are obvious
  - What does delegation across protocols look like?
  - Is it even possible?
  - Will credentials be stored? is that ok?
  - How to control scope of delegation? warehouse or hotel?
  - How to expire delegated authorization
  - Policy problem: stored credentials, scope
  - What about degrees of delegation?
  - Wind up implementing your own full permission model

Who wants to deal with this mess?

- InCommon/I2 - lots of tools if you're willing to work
- OpenStack Keystone - still a ways off
- On premise identity providers – Forge Rock, ws02, Oracle, IBM, CAS - roll up your sleeves
- API Management companies: Mashery, Layer7, Apigee - great if you have up front and subscription cash
- Commercial cloud identity providers - Amazon, Ping, Janrain, Atlassian - great if you have subscription cash
- Globus Nexus - implements a subset of the above. good choice when GSI is required
- 2 Factor – DUO, Google Authenticator, RSA SecurID – goodbye APIs

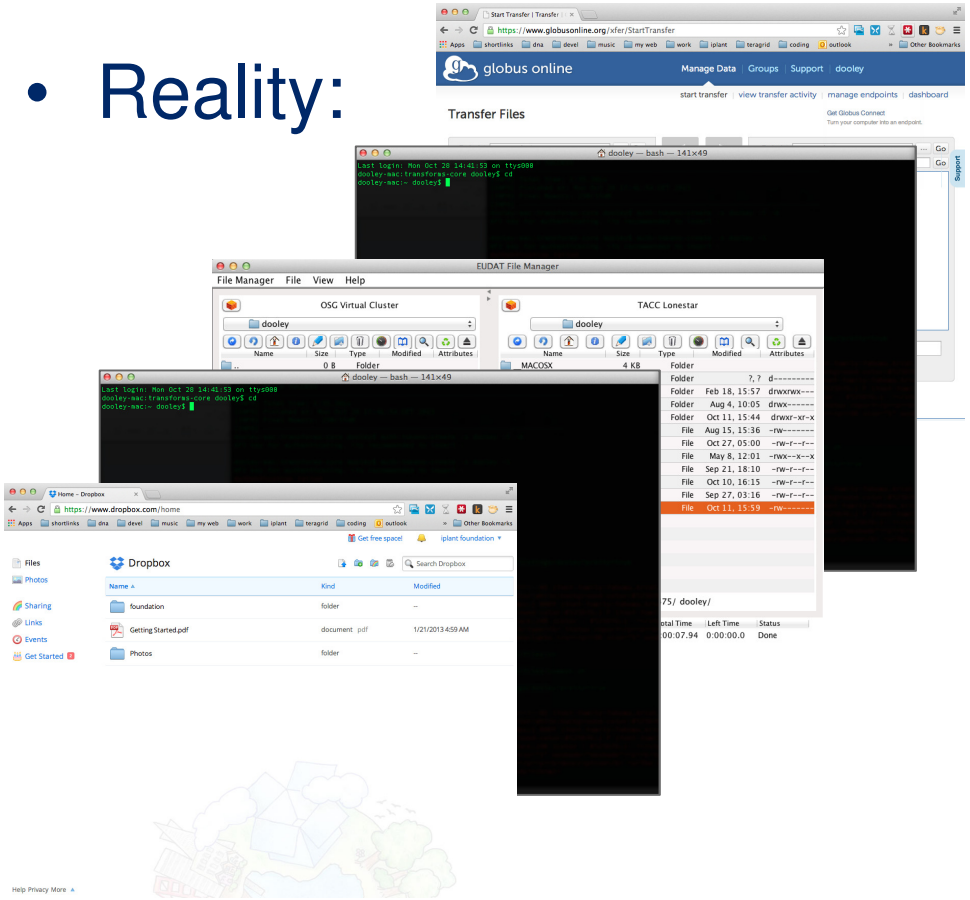
What about the users?

- Expectation



What about the users?

- Reality:



What about the users?

- Pros:
  - Juggling a few logins instead of dozens
  - Some SSO at the web layer
  - Possibility of piecing together a solution
- Cons:
  - Still duck taping together technologies to do basic things
  - Users will and are reusing passwords
  - Systems are exposed
  - No way to disable from point of compromise
  - No way to disable user on a shared accounts

What's the solution

```
while (!found(solution))
    prompt("What's the solution?")
```

Ideas

- Bind identities to physical identifiers
- Federalize identities, federate at a national level
- Establish and build on trust relationships:
  - InCommon
  - IETF
- Less re-invention, more adoption.
  - OGF
  - W3C
  - etc

Ideas

- Full stack integration
- Create a cause
- Be part of the solution

Thank you

http://bit.ly/1g8Grze

Rion Dooley

dooley@tacc.utexas.edu

For more information:

www.tacc.utexas.edu

www.sciencegatewaysecurity.org

www.sciencegateways.org