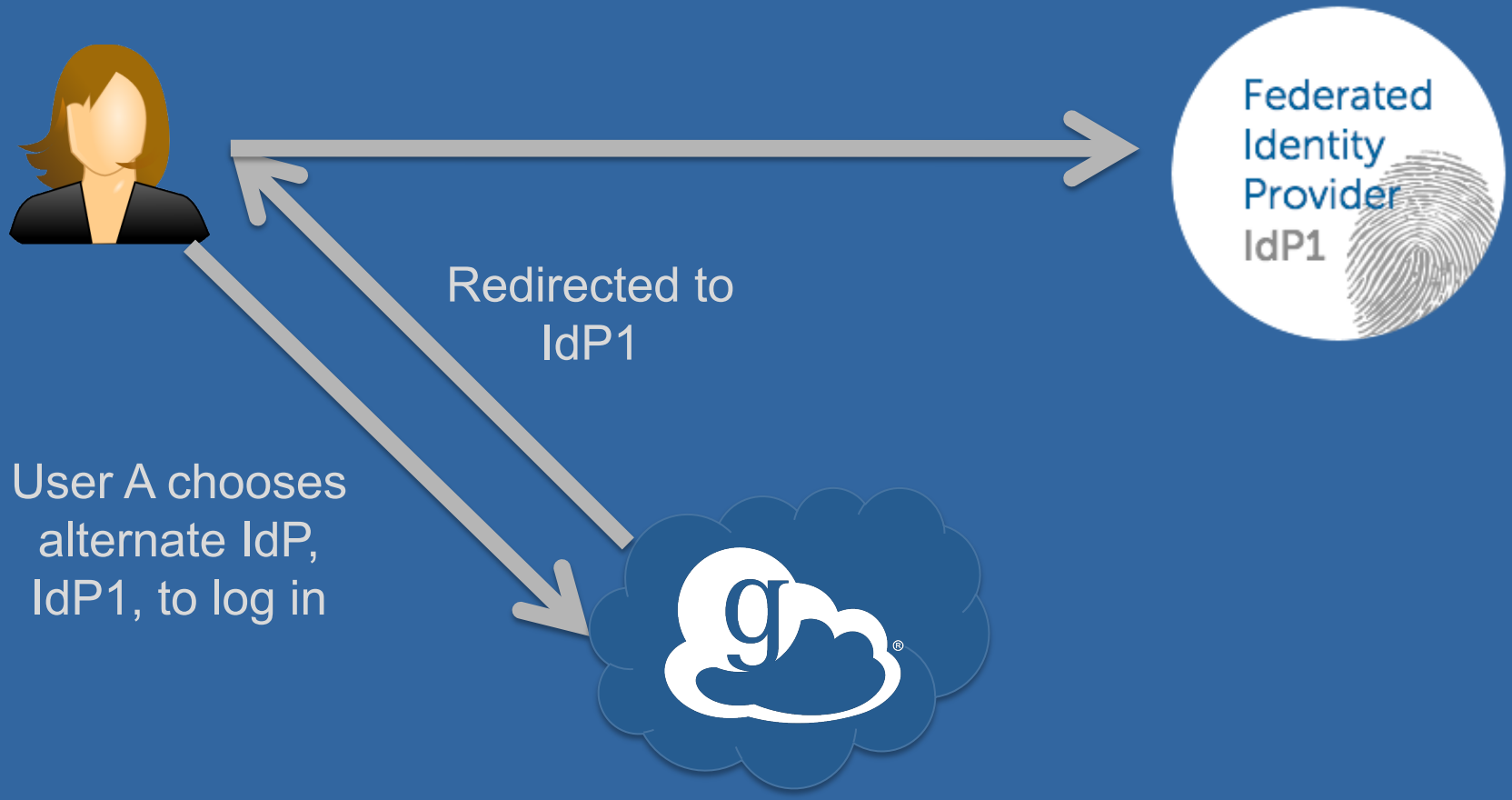
Globus Security Deep Dive

GlobusWorld 2014

Steve Tuecke

Globus Federated Identity Authentication and Linking

Linking a Federated Identity



Linking a Federated Identity

Prompt for login

User A
Authenticates

Federated
Identity
Provider
IdP1

OAuth
interactions

User A's identity:
userA@IdP1.org

userA@IdP1.org

Check for linked
Globus account

Linking a Federated Identity

User A
Authenticates

Prompt for login
with Globus
account

- globususerA@globus.org
- userA@IdP1.org

Linking a Federated Identity

User A chooses alternate IdP, IdP1, to log in

User A logged in as globususerA@globus.org with linked identity

Federated Identity Provider IdP1

- globususerA@globus.org
- userA@IdP1.org

Login with Federated Identity

User A is redirected & authenticates

User A logged in as globususerA@globus.org

OAuth interactions

User A's identity: userA@IdP1.org

User A logs in using alternate IdP: IdP1

- globususerA@globus.org
- userA@IdP1.org

Using Campus IdP (via CILogon)

User A is redirected to Campus IdP

User A logs in using Campus IdP

User A is redirected to CILogon

CILogon

globususerA@globus.org

userA@uchicago.edu

Using Campus IdP (via CILogon)

Prompt for login

User A
Authenticates

Campus IdP
UChicago

SAML
interactions

User A's identity:
userA@uchicago.edu
(optional attributes)

CILogon

User A logs
in using
Campus IdP

- globususerA@globus.org
- userA@uchicago.edu

Using Campus IdP (via CILogon)

User A logged in as
globususerA@globus.org

User A logs
in using
Campus IdP

OAuth
interactions

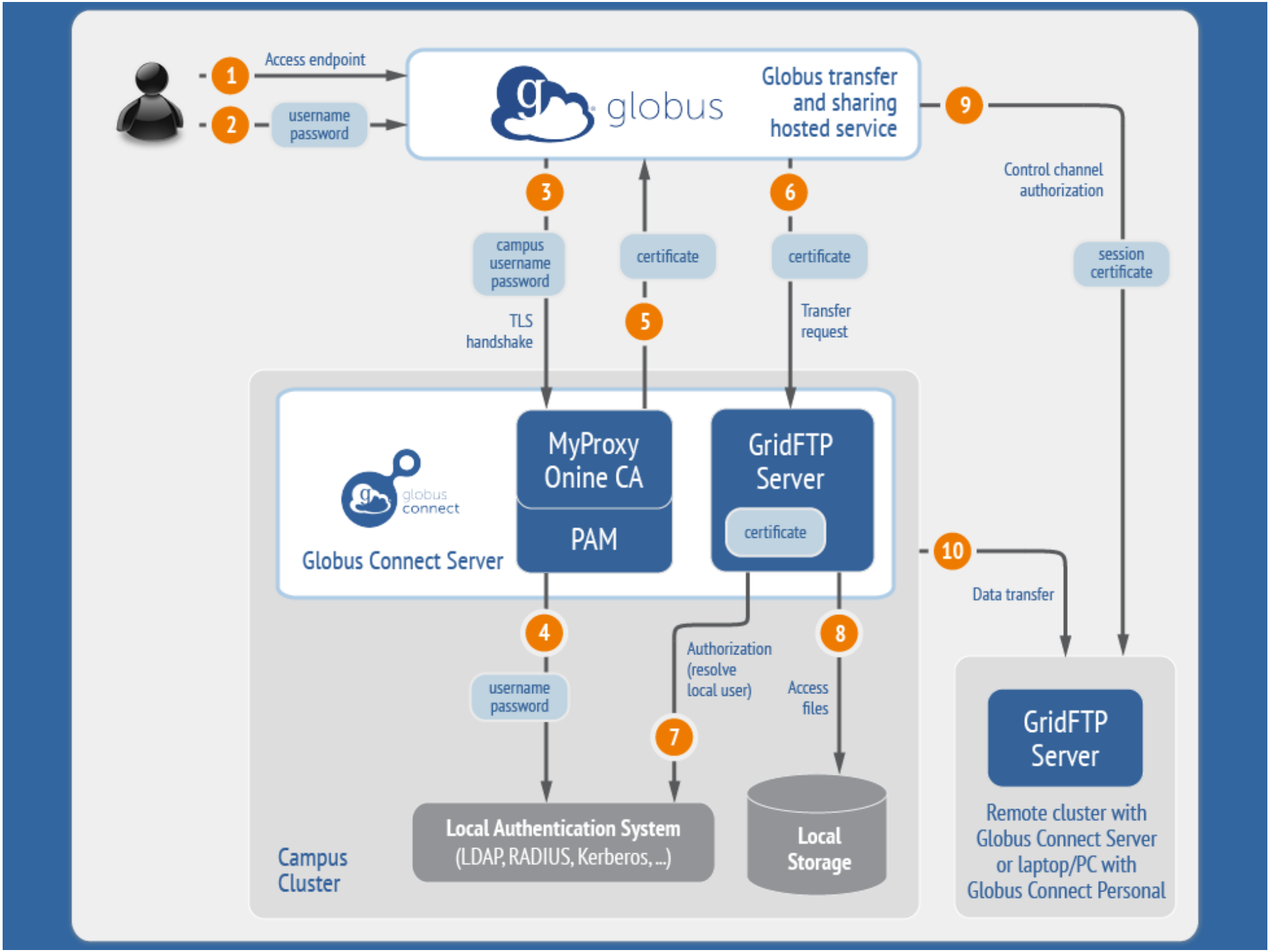
User A's credentials with
identity :userA@uchicago.edu
(optional attributes)

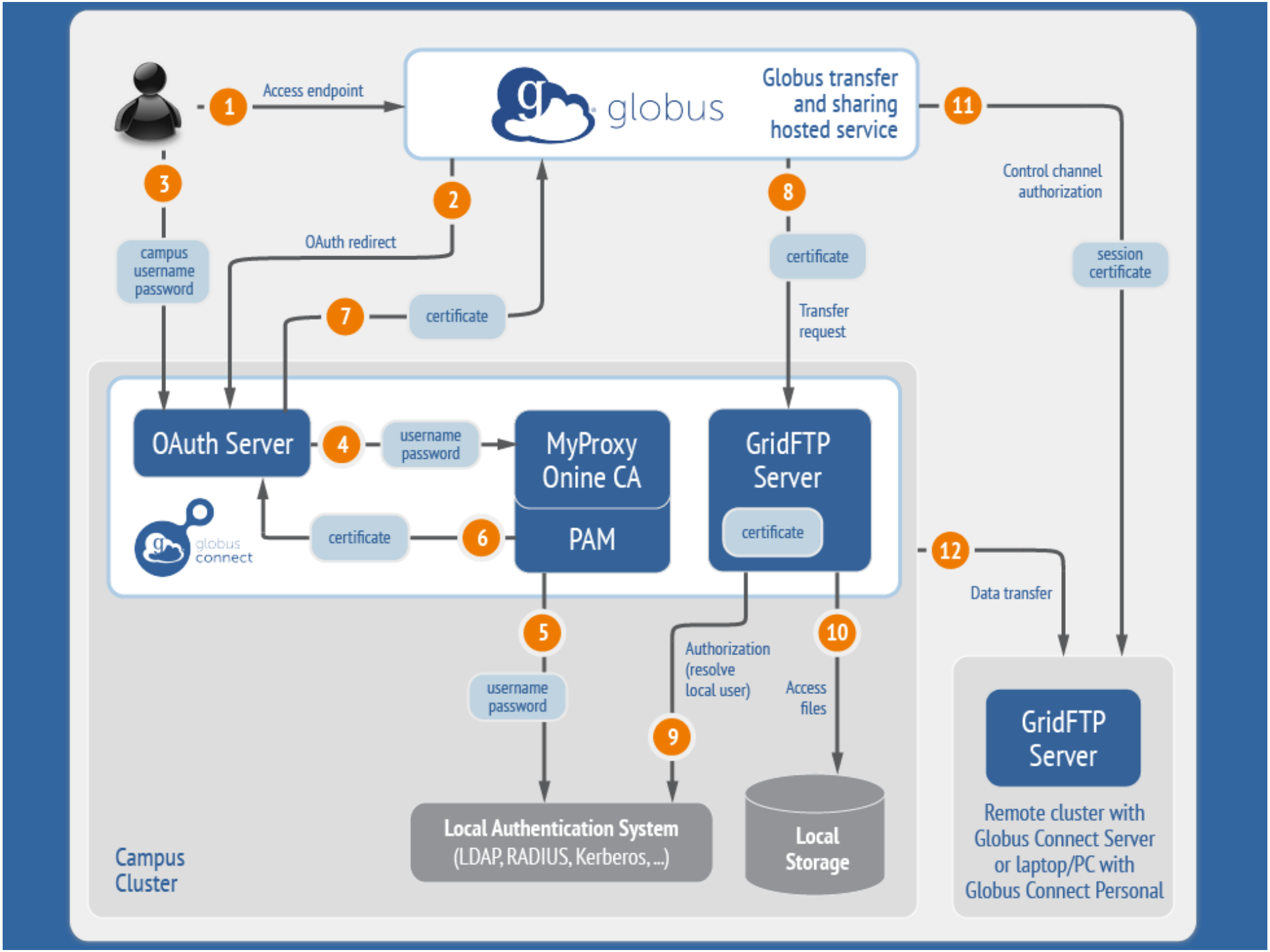
- globususerA@globus.org
- userA@uchicago.edu

Future Identity Directions

- **Move to user@domain user names**
  - Current Globus usernames become user@globus.org
  - Users not required to have @globus.org name
- **Auto-provision accounts from other identity domains**
- **XSEDE identities will fold into this**

Globus Endpoint Authentication


Access endpoint
1
2
username
password
globus
Globus transfer
and sharing
hosted service
9
Control channel
authorization
session
certificate
3
6
campus
username
password
certificate
certificate
TLS
handshake
5
Transfer
request
globus
connect
Globus Connect Server
MyProxy
Onine CA
PAM
GridFTP
Server
certificate
10
Data transfer
4
8
Authorization
(resolve
local user)
Access
files
username
password
7
Local Authentication System
(LDAP, RADIUS, Kerberos, ...)
Local
Storage
Campus
Cluster
GridFTP
Server
Remote cluster with
Globus Connect Server
or laptop/PC with
Globus Connect Personal


Access endpoint
globus
Globus transfer and sharing hosted service
Control channel authorization
OAuth redirect
campus username password
certificate
session certificate
Transfer request
OAuth Server
username password
MyProxy Onine CA
GridFTP Server
globus connect
certificate
PAM
certificate
Data transfer
Authorization (resolve local user)
Access files
username password
Local Authentication System (LDAP, RADIUS, Kerberos, ...)
Local Storage
GridFTP Server
Remote cluster with Globus Connect Server or laptop/PC with Globus Connect Personal
Campus Cluster

Globus Sharing Security

Globus Sharing

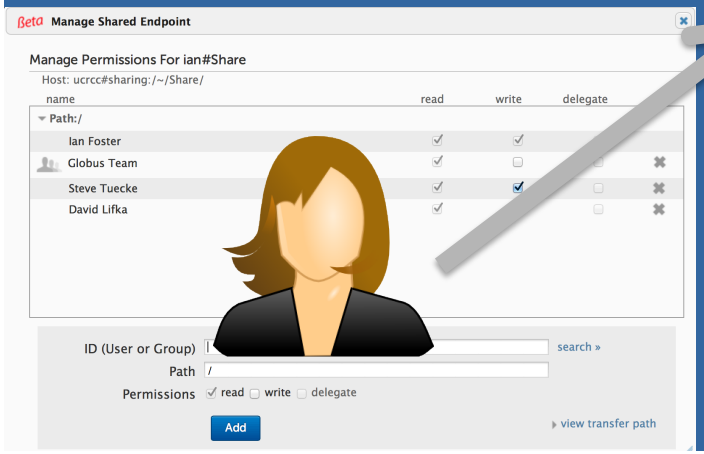
2 Globus manages ACLS on shared files; no need to move files to cloud storage!

Data Source

globus connect

1 User A selects file(s) to share, selects user or group, and sets permissions

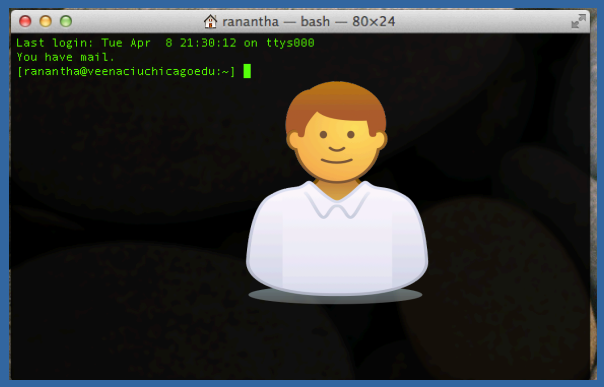
3 User B logs in to Globus and accesses shared file



Configuring a Managed Endpoint for Sharing

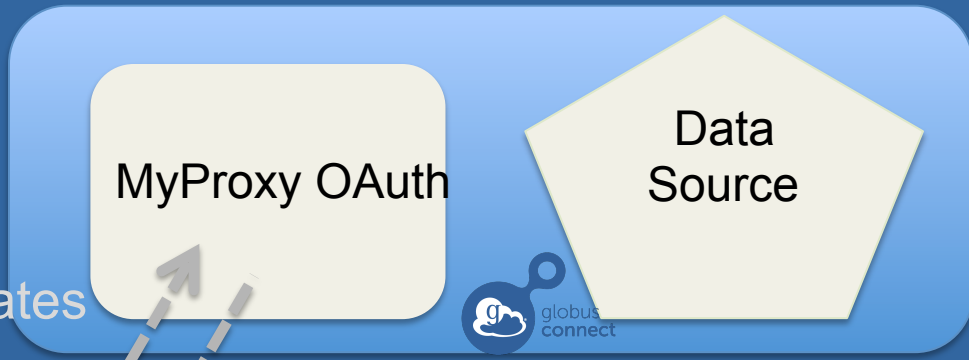
Configurable policies:

- Enable share
- Share restricted path
- Read only or Read/Write
- Local users that can share



Admin configures Managed Endpoint
/etc/globus-connect-server.conf

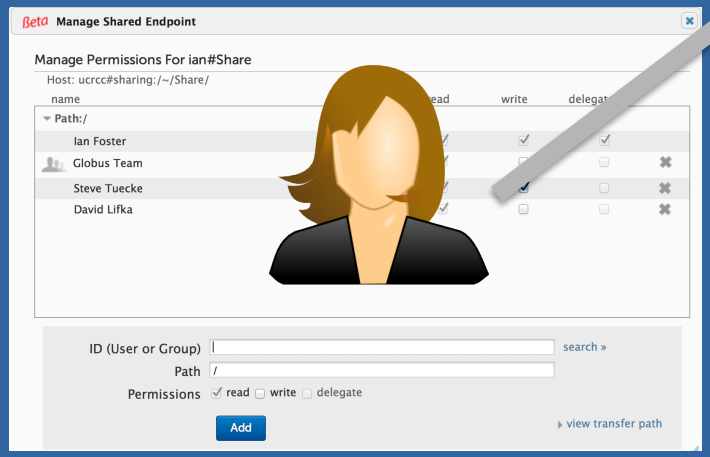
Activate Endpoint



User A authenticates using resource credentials

User A's credentials returned to Globus

User A selects endpoint to activate



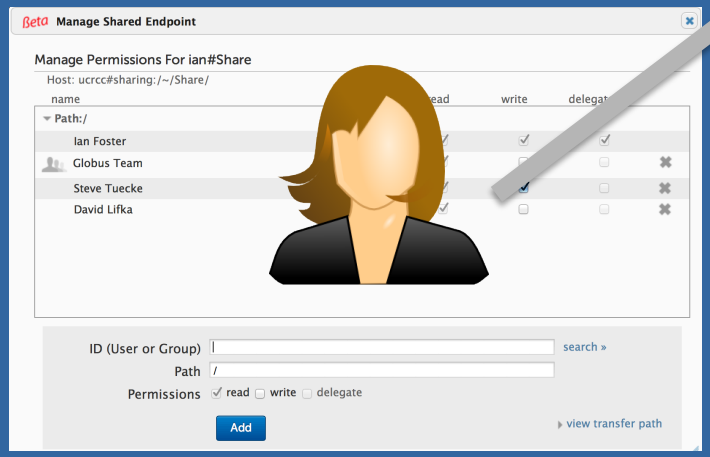
User A's credentials

Create Share

Data Source

globus connect

User A creates a shared endpoint, userA#share for path /projects/



User A's credentials

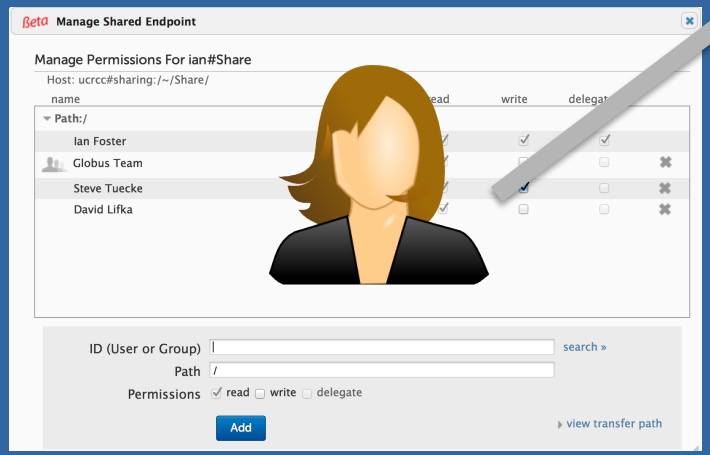
Create Share

Data Source

globus connect

Authenticate as User A

User A creates a shared endpoint, userA#share for path /projects/



User A's credentials

Create Share

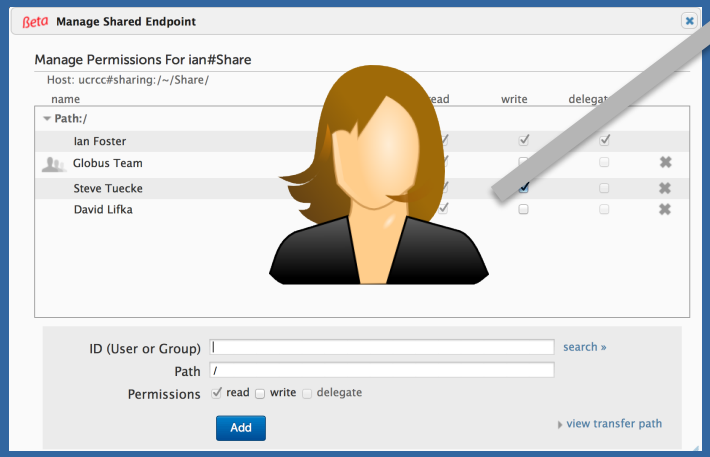
Does the endpoint allow shared endpoint for path /projects/?

Data Source

globus connect

Yes

User A creates a shared endpoint, userA#share for path /projects/



User A's credentials

Create Share

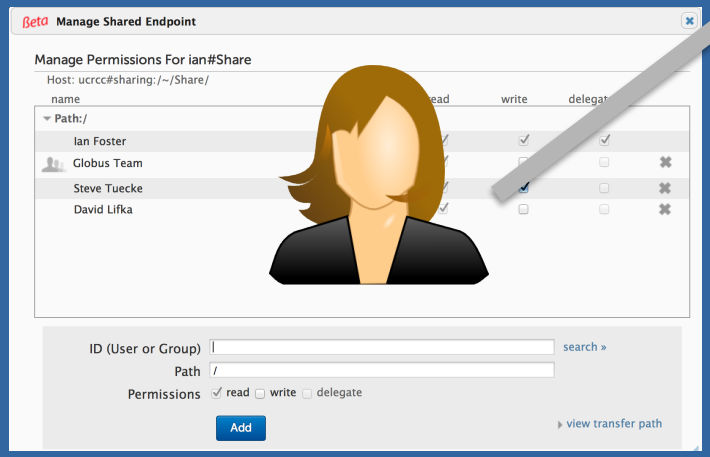
Data Source

globus connect

Create share: UUID and /projects/

For User A, file share.UUID with path /projects/

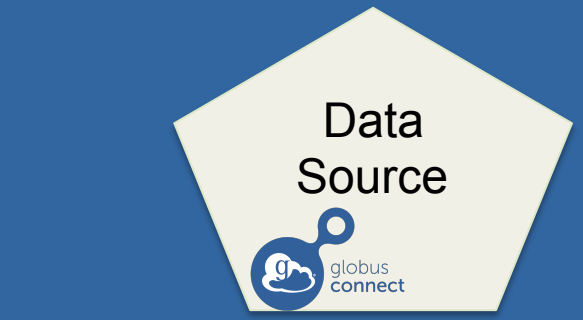
User A creates a shared endpoint, userA#share for path /projects/



User A's credentials

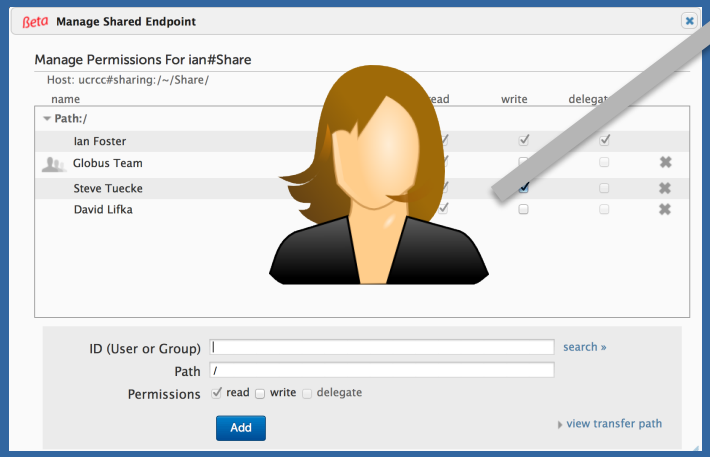
userA#share, UUID, User A's credentials, /projects/

Set permissions



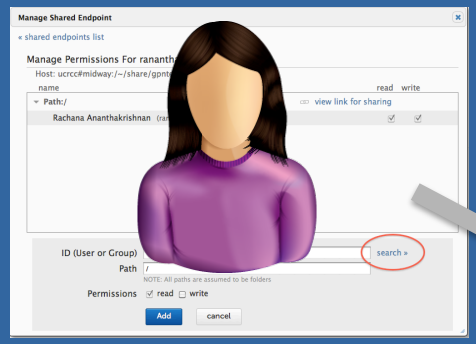
- For User A, file share.UUID with path /projects/

User A sets permissions for User B to read path userA#share:/dir1



- User A's credentials
- userA#share, UUID, User A's credentials, /projects/
- ACL: userA#share:/dir1, read, User B

List Share



User B lists
userA#share:/dir1

Check ACLs
for User B

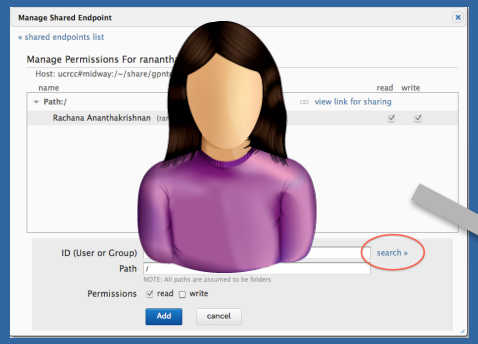
Data Source

globus connect

- For User A, file share.UUID with path /projects/

- User A's credentials
- userA#share, UUID, User A's credentials, /projects/
- **ACL: userA#share:/dir1, read, User B**

List Share



User B lists userA#share:/dir1

Authenticate as Globus

Data Source

globus connect

- For User A, file share.UUID with path /projects/

- User A's credentials
- userA#share, UUID, User A's credentials, /projects/
- ACL: userA#share:/dir1, read, User B

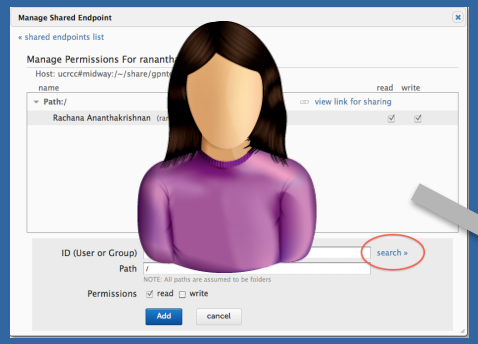
List Share

Get User A's local account

Data Source

globus connect

Request sharing from UUID with User A's credentials

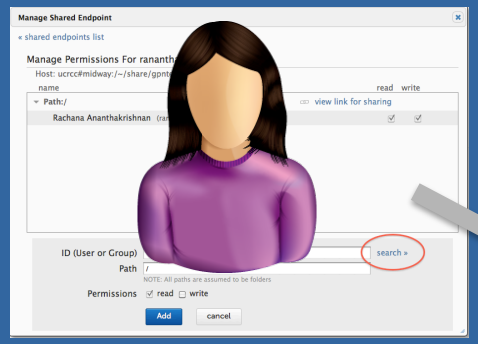


User B lists userA#share:/dir1

- For User A, file share.UUID with path /projects/

- User A's credentials
- userA#share, UUID, User A's credentials, /projects/
- ACL: userA#share:/dir1, read, User B

List Share



User B lists userA#share:/dir1

Request sharing from UUID with User A's credentials

Check for User A's share.UUID file

Data Source

globus connect

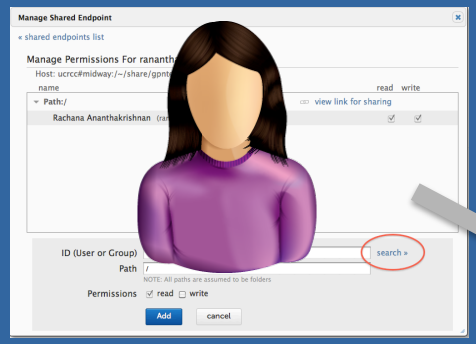
- For User A, file share.UUID with path /projects/

- User A's credentials
- userA#share, UUID, User A's credentials, /projects/
- ACL: userA#share:/dir1, read, User B

List Share

Load and enforce sharing restricted path

Request sharing from UUID with User A's credentials



User B lists userA#share:/dir1

Data Source

globus connect

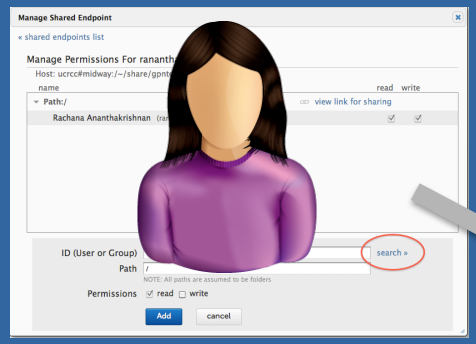
- For User A, file share.UUID with path /projects/

- User A's credentials
- userA#share, UUID, User A's credentials, /projects/
- ACL: userA#share:/dir1, read, User B

List Share

Setuid to User A local account, change root to path

Request sharing from UUID with User A's credentials



User B lists userA#share:/dir1

Data Source

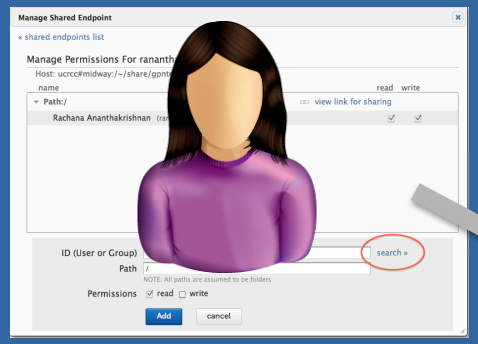
globus connect

- For User A, file share.UUID with path /projects/

- User A's credentials
- userA#share, UUID, User A's credentials, /projects/
- ACL: userA#share:/dir1, read, User B

List Share

Combine user path restrictions, & sharing restricted path



User B lists userA#share:/dir1

Path restrictions for User B

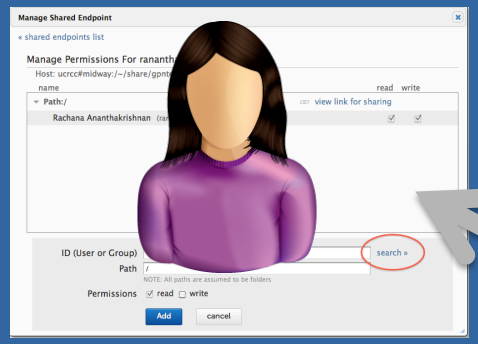
Data Source

globus connect

- For User A, file share.UUID with path /projects/

- User A's credentials
- userA#share, UUID, User A's credentials, /projects/
- ACL: userA#share:/dir1, read, User B

List Share



User B lists userA#share:/dir1

Directory listing

Data Source

globus connect

- For User A, file share.UUID with path /projects/

- User A's credentials
- userA#share, UUID, User A's credentials, /projects/
- ACL: userA#share:/dir1, read, User B

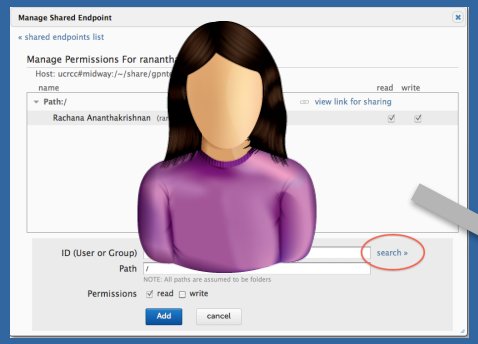
Transfer from share

- For User A, file share.UUID with path /projects/

Data Source

globus connect

Enforce share permissions



User B transfer from userA#share:/dir1

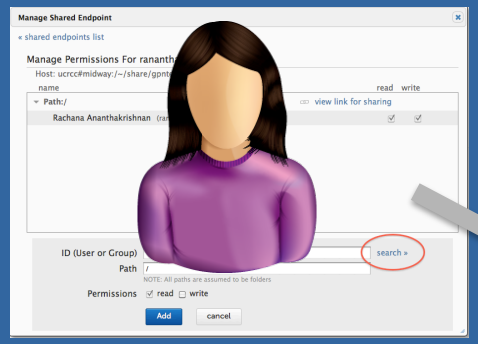
- User A's credentials
- userA#share, UUID, User A's credentials, /projects/
- ACL: userA#share:/dir1, read, User B

Data Destination

globus connect

Transfer from share

- For User A, file share.UUID with path /projects/



User B transfer from userA#share:/dir1

Data Source

globus connect

Globus moves the files

- User A's credentials
- userA#share, UUID, User A's credentials, /projects/
- ACL: userA#share:/dir1, read, User B

Data Destination

globus connect

Future Possible Sharing Directions

- **Share to users by email address**
- **Level of Assurance policies**
  - E.g., In order to write to a shared endpoint, user must have authenticated with one of these IdPs, in the last N minutes, within this browser session.
- **Time-based shared endpoints**
- **Time-based ACLs**
- **Periodic re-validation of shared endpoints**

Operational Security

Operational Security

- **Separate AWS security groups for:**
  - Nexus vs Transfer, Production vs Test and QA
  - Check ports hourly
- **Central logging with Nagios monitoring**
- **OSSEC intrusion detection**
- **Globus root CA for sharing access on offline hardware security module**

Who has access to what?

- **Access to production backends restricted to only those ops staff who need it to operate the service.**
- **Globus Connect Server endpoint restrictions prevent Globus ops access**

What data does Globus see?

- **User profile: email, name, etc.**
- **Linked identities: no secrets stored**
  - With OAuth, we never see passwords
- **Temporary user credentials**
- **File paths, but NOT file contents**
- **File level transfer logs retained for 1 month**
- **Summary level transfer history retained indefinitely**
- **Publication metadata**