Identity Access and Management with Globus

IAM Online Webinar Series

Steve Tuecke
University of Chicago - Globus
tuecke@globus.org

Moderator: Tom Barton, University of Chicago and Internet2
Common solutions to common problems

*Problem: I need to protect application X. Some requirements:*

- Users are inside and outside of our org
  - Federation + Social IDs
  - 2FA too?
- Access by web and mobile clients, ssh for some users
- Automated integrations (CLI or APIs)
- Several different security roles to which users and automatons are assigned
- OAuth2/OIDC is supported natively
Is this a Research IT problem or an Enterprise IT problem?

- Yes! These requirements occur in both.
- Yes! Research instances have Enterprise dependencies.
- Research! The research IT community is addressing these needs.
- Enterprise! The enterprise IT community is addressing these needs.

hmmm…

- So let’s talk
Some things to listen for/think about

- What problems are being addressed by Globus Auth?
  - Insulation of application from changes in user affiliation, authentication/federation technology, sources of authority for access to security roles, else?
- What’s the right operational architecture?
  - Who should run what, how should it/they be sustained?
- What parts of the Globus work can/should be leveraged in solutions to other problems?
- What other work might benefit Globus Auth?
Cloud has transformed how software and platforms are delivered

Software as a service: SaaS
(web & mobile apps)

Platform as a service: PaaS

Infrastructure as a service: IaaS

PaaS enables more rapid, cheap, and scalable delivery of powerful (SaaS) apps
Globus and the research data lifecycle

1. Researcher initiates transfer request; or requested automatically by script, science gateway.

2. Globus transfers files reliably, securely.

3. Researcher selects files to share, selects user or group, and sets access permissions.

4. Globus controls access to shared files on existing storage; no need to move files to cloud storage!

5. Collaborator logs in to Globus and accesses shared files; no local account required; download via Globus.

6. Researcher assembles data set; describes it using metadata (Dublin core and domain-specific).

7. Curator reviews and approves; data set published on campus or other system.

8. Peers, collaborators search and discover datasets; transfer and share using Globus.

- Access via web browser or command line
- Use any storage system
- Use existing identity
Example use of Globus PaaS

• The Modern Research Data Portal: A Design Pattern for Networked, Data-Intensive Science
  – Example web app
  – Jupyter notebook
  – Technical article

https://docs.globus.org/modern-research-data-portal/
Security PaaS challenges

• **How to provide:**
  – Login to apps
    o Web, mobile, desktop, command line
  – Protect all REST API communications
    o App → Globus service
    o App → non-Globus service
    o Service → service

• **While:**
  – Not introducing even more identities
  – Providing least privileges security model
  – Being agnostic to programming language and framework
  – Being web friendly
  – Making it easy for users and developers
Globus Auth

- Identity and access management (IAM) platform-as-a-service
- Simplifies creation and integration of advanced apps and services
- Brokers authentication and authorization interactions between:
  - End-users
  - Identity providers: InCommon, XSEDE, Google, portals
  - Services: resource servers with REST APIs
  - Apps: web, mobile, desktop, command line clients
  - Services acting as clients to other services

[docs.globus.org/api/auth](http://docs.globus.org/api/auth)
Based on widely used web standards

- **OAuth 2.0 Authorization Framework**
  - aka OAuth2

- **OpenID Connect Core 1.0**
  - aka OIDC

- **Uses various OAuth2 and OIDC libraries**
  - Google OAuth Client Libraries (Java, Python, etc.), Apache mod_auth_openidc, etc.
  - Globus Python SDK
Globus Python SDK

- Python client library for the Globus Auth and Transfer REST APIs
  
  [GitHub](https://github.com/globus/globus-sdk-python)

- Jupyter (iPython) notebook demonstrating use of Python SDK
  
  [GitHub](https://github.com/globus/globus-jupyter-notebooks)
Use Case: Log in with Globus

• Similar to: “Log in with Google” “Log in with Facebook”
• Using existing identities
• Providing access to community services
Adding your identity provider

• InCommon identity providers that release Research & Scholarship attributes to CILogon *(free)*

• Any other OpenID Connect identity provider *(subscription)*
Use Case: App calling services on user’s behalf

• **Example:**
  – App starting transfer for user

• **Authorization Code Grant**
  – With service scopes
  – Can also request OIDC scopes

• **Confidential client**

• **Globus SDK:**
  – To get tokens: ConfidentialAppAuthClient
  – To use tokens: AccessTokenAuthorizer
Example: Research automation

https://github.com/globus/automation-examples

- README for install instructions
- `globus_folder_sync.py`, `cli-sync.sh`
  - Replication
- `share_data.py`, `share-data.sh`
  - Data distribution using sharing
- `cleanup_cache.py`
  - Monitor and clean up
Use Case: Native apps

• **Examples**
  – Command line, desktop apps
  – Mobile apps
  – Automation scripts
  – Any client that cannot keep a secret (downloaded)

• **Native app is registered with Globus Auth**
  – Not a confidential client

• **Native App Grant is used**
  – Variation on the Authorization Code Grant that uses PKCE

• **Globus SDK:**
  – To get tokens: NativeAppAuthClient
  – To use tokens: AccessTokenAuthorizer
Use Case: Apps that need access tokens for a long time

• **Examples:**
  – Portal checks for transfer status when user is not logged in
  – Run command line app from script

• **App requests refresh tokens**

• **Globus SDK:**
  – To get token: ConfidentialAppClient or NativeAppClient
  – To use tokens: RefreshTokenAuthorizer
Example: Command Line Interface

$ globus
Usage: globus [OPTIONS] COMMAND [ARGS]...

Options:
- `v`, `--verbose` Control level of output
- `h`, `--help` Show this message and exit.
- `F`, `--format [json|text]` Output format for stdout. Defaults to text
- `--jmespath`, `--jq TEXT` A JMESPath expression to apply to json output. Takes precedence over any specified '---format' and forces the format to be json processed by this expression
- `--map-http-status TEXT` Map HTTP statuses to any of these exit codes: 0,1,50-99. e.g. "404=50,403=51"

Commands:
- `bookmark` Manage Endpoint Bookmarks
- `config` Modify, view, and manage your Globus CLI config.
- `delete` Submit a Delete Task
- `endpoint` Manage Globus Endpoint definitions
- `get-identities` Lookup Globus Auth Identities
- `list-commands` List all CLI Commands
- `login` Login to Globus to get credentials for the Globus CLI
- `logout` Logout of the Globus CLI
- `ls` List Endpoint directory contents
- `mkdir` Make a directory on an Endpoint
- `rename` Rename a file or directory on an Endpoint
- `task` Manage asynchronous Tasks
- `transfer` Submit a Transfer Task
- `version` Show the version and exit
- `whoami` Show the currently logged-in identity.

docs.globus.org/cli
Use Case: App invoking services as itself

• **Examples**
  – Sample portal invoking graph service and accessing endpoints as itself
  – Robots, agents, services

• **Every app is/has an identity in Globus Auth**
  (\(<\text{client\_id}\>@\text{clients.auth.globus.org}\))

• **App registers with Globus to get client id/secret**
  – Native app cannot do this (no client_secret)

• **Client Credential Grant is used**

• **Can use the client_id just like any other identity_id**
  – Sharing access manager role, permissions, group membership, etc.

• **Globus SDK:**
  – To get tokens: ConfidentialAppAuthClient
  – To use tokens: AccessTokenAuthorizer
Use Case: Securing your service’s REST API

- Outsource all identity management and authentication
  - Federated identity with InCommon, Google, etc.
- Outsource your REST API security
  - Consent, token issuance, validation, revocation
  - You provide service-specific authorization
- Apps use your service like all others
  - It’s standard OAuth2 and OIDC
- Your service can seamlessly leverage other services
- Other services can leverage your service
- Implement your service using any language and framework

Add your service to the science cyberinfrastructure platform
Example: SSH with Globus Auth

• **Goal:** Use unmodified SSH server and client binaries to allow SSH login using Globus Auth

• **Who:** XSEDE, research computing

• **Approach:** SSH server is a Globus Auth / OAuth2 resource server
  – Pass access token as user password
  – PAM module to validate
  – Globus CLI wrapper around SSH client
  – Local account mapping service?
Use Case: Dependent services

• **Your service can act as client to other services (scopes)**
  – Globus Transfer and Auth
  – XSEDE (e.g., Jetstream, XUP)
  – Other community services
  – Future: Commercial services (e.g., Google Drive)

• **Entire service call tree consented by user and service owners**
  – Rescinding consent revokes all dependent tokens

• **Dependent tokens are restricted to a particular client, calling a particular scope, on behalf of a particular resource owner (e.g., user)**
  – Restricted delegation!
Summary

• Globus Auth makes it easy to:
  – add user login to your applications
  – integrate with Globus, XSEDE, and other services
  – add OAuth2 support to your service’s REST API
  – create services to leverage other services

Globus enables an integrated ecosystem of services and applications for the research community
Thank you to our sponsors!

U.S. DEPARTMENT OF
ENERGY

THE UNIVERSITY OF
CHICAGO

NATIONAL INSTITUTES
OF HEALTH

NIST

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

Argonne
NATIONAL LABORATORY

powered by
amazon
web services
Thanks for attending.

• Steve Tuecke
tuecke@globus.org

• Was this session helpful?
• Want to discuss how Globus Auth might help you?
Evaluate Today’s IAM Online

https://www.surveymonkey.com/r/IAMOnline-Sept2017
Upcoming Events

Internet2 Technology Exchange – October 14-19, 2017 – San Francisco, CA
meetings.internet2.edu/2017-technology-exchange/
• Two Trust and Identity tracks Monday and Tuesday morning
• Working Groups and Birds of a Feather Tuesday afternoon
• Advance CAMP (ACAMP) unconference Wednesday and Thursday (noon finish)

InCommon Shibboleth Installation Workshop (incommon.org/shibtraining)
November 7-8, Bethesda, Maryland [Starting with this session, the curriculum will shift to Shibboleth incorporated with TIER]
October IAM Online

How to (Re-)Do an IAM Program for Your Institution:
Two Case Studies
October 11, 2017
2 pm ET

Michael Corn, Chief Information Security Officer
University of California-San Diego

Sharon Pitt, Chief Information Officer
Binghamton University