Identity Access and Management with Globus

Rachana Ananthakrishnan
rachana@globus.org
Globus Auth: Foundational IAM service

• Protects REST API communications between and among apps and services
• Federated login for diverse app ecosystem
• Based on OAuth2 and OpenID Connect
  – Least privileges security model: scopes/consents
  – Access via OAuth2 and OIDC libraries of your choice
  – Programming language and framework agnostic
Globus Auth: Identity broker for research apps

Brokers authentication and authorization among...

- End-users
- Identity providers: enterprise, external (e.g. Google)
- Services: resource servers with REST APIs
- Apps: web, mobile, desktop, command line clients
- Services acting as clients to other services
Use Case: Log in with Globus

- Similar to: “Log in with Google” “Log in with Facebook”
- Using existing identities
- Providing access to community services
Use Case: App calling service on user’s behalf

Authorization Code Grant

Welcome to the GPCR Data Explorer. The GPCR Data Explorer contains data generated during the process of GPCR structure determination. These data will represent the entire process of GPCR structural biology including all associated constructs and related experimental data generated from three leading academic sites: the University of Southern California in Los Angeles, iHuman Institute at ShanghaiTech University, and Shanghai Institute of Materia Medica, a member of the Chinese Academy of Sciences.

Click one of the links below to start exploring GPCR data.

Comprehensive craniofacial data and resources
Your curated, one-stop shop for facial development and research.
Use Case: Native Apps calling services

Native App Code Grant

Globus command line client application

High performance, high throughput, computing workflows
Use Case: Apps that need offline access

Refresh tokens

Copy /ingest Daily @ 3:30am

Recurring transfers with sync option

High performance, high throughput, computing workflows

```python
from parsl.data_provider.files import File

@python_app
def sort_numbers(inputs=[]):
    with open(inputs[0].filepath, 'r') as f:
        strs = [n.strip() for n in f.readlines()]
        strs.sort()
        return strs

unsorted_globus_file = File('globus://03d7d06a-cb6b-lle8-8c6a-0ald4c5c824a/unsorted.txt')

f = sort_numbers(inputs=[unsorted_globus_file])
print(f.result())
```
Use Case: Apps invoking service as itself

Client Credential Grant
Examples: Securing service’s REST API

Outsource all IAM, authorization on your own

workflow-execution-service-schemas

Global Alliance for Genomics & Health

Collaborate. Innovate. Accelerate.

Workflow Execution Service (WES) API

The Global Alliance for Genomics and Health is an international coalition, formed to enable the sharing of genomic and clinical data.

Cloud Work Stream

The Cloud Work Stream helps the genomics and health communities take full advantage of modern cloud environments. Our initial focus is on "bringing the

Object Resolution Service

The Object Resolution Service (ORS) registers and resolves GUIDs and Core Metadata for DCPPC digital objects. It creates and assigns persistent GUIDs for digital objects: Archival Resource Keys (ARKs), Datacite Digital Object Identifiers (DOIs), or Minids (implemented as ARKs). It also provides a landing service endpoint where Core Metadata for these objects in human and machine readable format (JSON-LD) may be retrieved, including the cloud provider endpoints.

Terms of service

Contact Max Levinson

Apache 2.0

Authorize
Use case: Invoking dependent services

Restricted delegation down the call chain

FAIR Research Data Portal

Concierge Service

Manage data bags

Identifier

Mint persistent identifiers

Groups

Manage groups

Transfer

Transfer data
High Assurance support in Globus Auth

• Determine which identities in a user’s identity set have been used to authenticate and when
• Session context = app instance, device
• Information returned via token introspection
• Services make access control decisions
• Failed operation → app generates specific redirect URL

[link to documentation] docs.globus.org/api/auth/sessions
Services using high assurance features

- **Globus transfer and groups**
- **Additional authentication assurance**
  - Enforce user authentication with specific identity within session with specific timeframe
- **Application instance isolation**
  - Authentication context is per app, per session
Additional authentication assurance

Welcome!

Please log in to JAGGAER Production Environment.

To securely logout, you must quit your browser.

CNetID / UCHIDID: [blank]

Password: [blank]

Forgot your password? [link]

LOG IN

Need help with your CNetID or UCHIDID? If you are a University of Chicago faculty member, student, or staff member you may use myaccount.uchicago.edu to change your password, re-enter your...
Additional authentication assurance
Re-authentication timeout

userX@anl.gov
userX@uchicago.edu

Globus File Manager
RECENTLY USED ENdPOINTS
ucr1cago RCC Mapped Collection
Ol Home Shares - Vas
Sandbox - Vas
Amazon S3 Gateway - Vas
ESnet Read-Only Test DTN at Sunnyvale
Vas Laptop
POSIX Sandbox - Vas
Globus Tutorial Endpoint
NCAR RDA Dataset Archive
Global Tutorial Endpoint

Globus File Manager
RECENTLY USED ENdPOINTS
ucr1cago RCC Mapped Collection
Ol Home Shares - Vas
Sandbox - Vas
Amazon S3 Gateway - Vas
ESnet Read-Only Test DTN at Sunnyvale
Vas Laptop
POSIX Sandbox - Vas
Globus Tutorial Endpoint
NCAR RDA Dataset Archive
Global Tutorial Endpoint

File Manager
Panel
Bookmark Manager

Panel
Bookmark Manager

Collection
NCAR RDA Dataset Archive

Path

Permissions
Transfer or Sync to...
New Folder
Rename
Delete Selected
Preview Limited
Download (https)
Get Link
Show Hidden Items

Permissions
Transfer or Sync to...
New Folder
Rename
Delete Selected
Preview Limited
Download (https)
Get Link
Show Hidden Items
Application instance isolation

Authenticated in browser session (app instance 1)

Re-authentication required in different app, same browser (app instance 2)

Authentication Failed

Your credentials do not provide sufficient access to this endpoint. If you have alternative credentials you may need to deactivate this endpoint and try again.

userX@uchicago.edu
Application Instance Isolation

Authenticated in browser session (app instance 1)

userX@uchicago.edu

Re-authentication required in CLI session (app instance 2)

userX@uchicago.edu

File Manager

Collection: GCSv5.2 Globus Demo HA Mapped Collection

Options:
- -v, --verbose: Control level of output
- -h, --help: Show this message and exit.
- -F, --format [unix|json|text]: Output format for stdout. Defaults to text.
- --jmespath, --jq TEXT: 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"
More information

- **Documentation**
  - docs.globus.org

- **Globus Auth documentation**
  - docs.globus.org/api/auth/

- **Python SDK**

- **Support**
  - support@globus.org

- **Subscribe to blog posts and news/announcements**
  - www.globus.org/contact-us
"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov