Using Globus Auth to Streamline the Creation, Integration, and Use of Research Services

Steve Tuecke

tuecke@globus.org

globus

Cloud has transformed how software and platforms are delivered

Software as a service: **SaaS**

(web & mobile apps)

Tripit from Concur

NETFLIX

salesforce

Platform as a service: **PaaS**

amazon web services

Microsoft Azure

force.com cloud platform

Infrastructure as a service: **IaaS**

amazon web services EC2

amazon web services S3

Microsoft Azure

Google Compute Engine

PaaS enables more rapid, cheap, and scalable delivery of powerful (SaaS) apps

globus

Products News About Support Quick Links kyle

Research data management simplified.

135,196,155,372 MB TRANSFERRED

Researchers

Focus on your research, not IT problems. We make it easy to move, manage, and share big data.

LEARN MORE

GET STARTED

Resource Providers

Globus gives you more control over your data infrastructure, while providing excellent ease-of-use for your researchers.

LEARN MORE

GLOBUS PROVIDER PLANS

Our Users

Researchers and resource providers are our greatest inspiration and we love it when they say nice things about Globus.

USER QUOTES

CASE STUDIES

Fast, Reliable, Secure File Transfer

Move files between your laptop, lab server, research computing center, national supercomputing facility, or any other storage system, using just a browser.

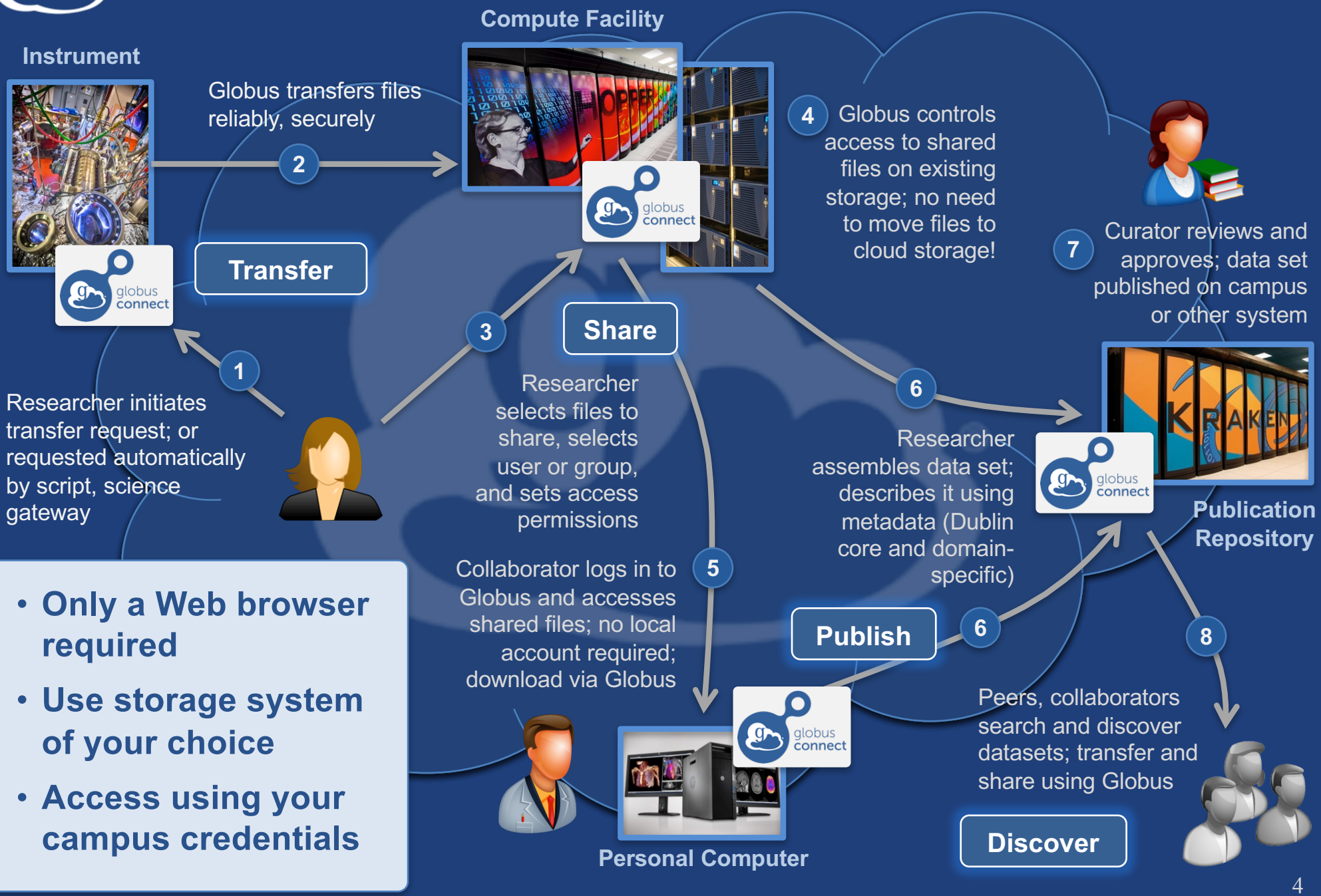
LEARN MORE ABOUT FILE TRANSFER WITH GLOBUS

UPCOMING EVENTS

October 16, 2015

Webinar: Integrating Globus into the GridChem Gateway

Globus SaaS: Research data lifecycle



- **Only a Web browser required**
- **Use storage system of your choice**
- **Access using your campus credentials**

Platform Questions

- **How do you leverage Globus services in your own applications?**
- **How do you extend Globus with your own services?**

- **How do we empower the research community to create an integrated ecosystem of services and applications?**

Example: NCAR RDA

NCAR UCAR | Research Data Archive
Computational & Information Systems Lab

weather • data • climate

Go to Dataset: nnn.n

Home | Find Data | Ancillary Services | About/Contact | Data Citation | Web Services | For Staff

NCEP Climate Forecast System Version 2 (CFSv2) Monthly Products

ds094.2

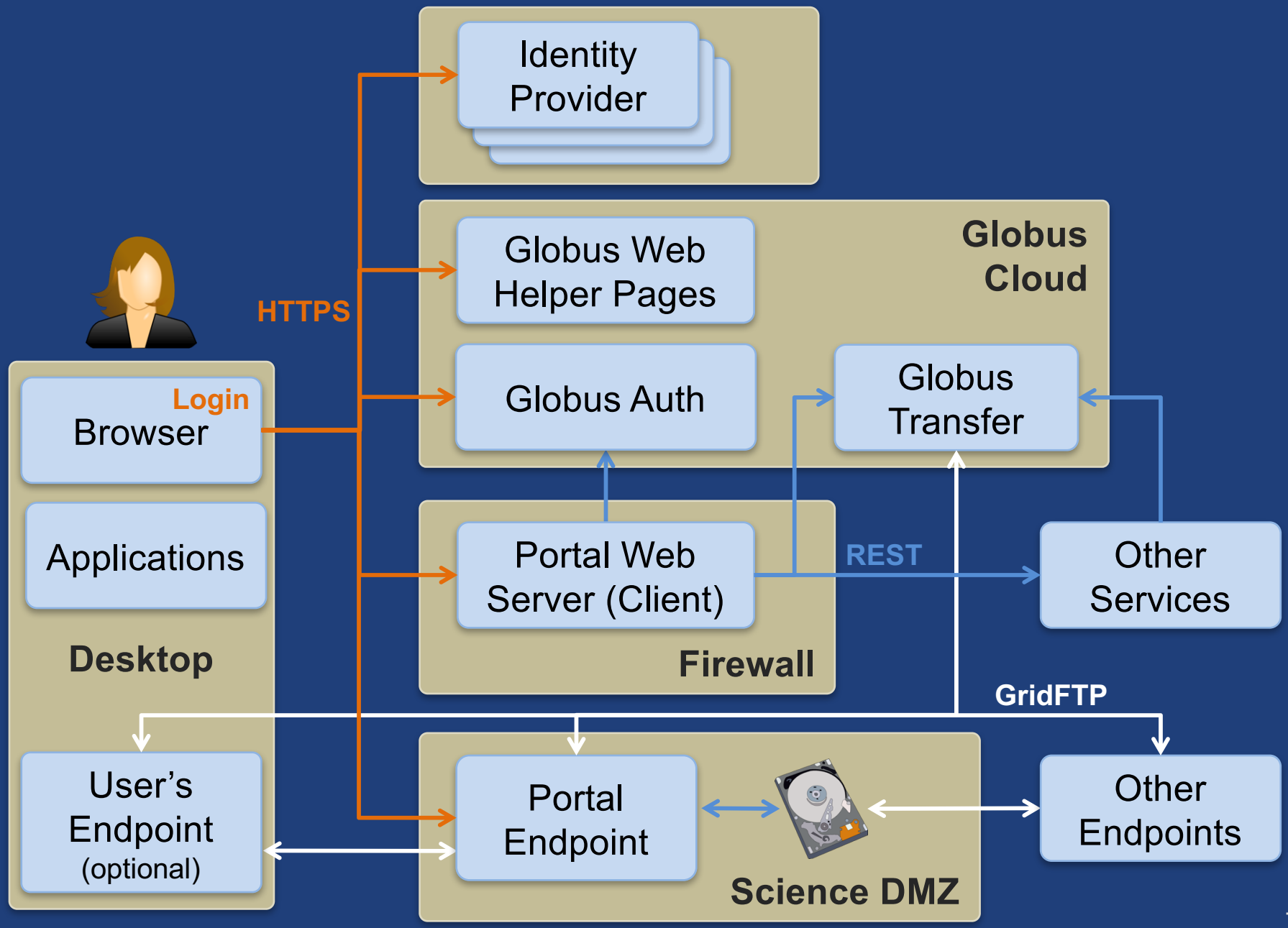
For assistance, contact Bob Dattore (303-497-1825).

Description | Data Access

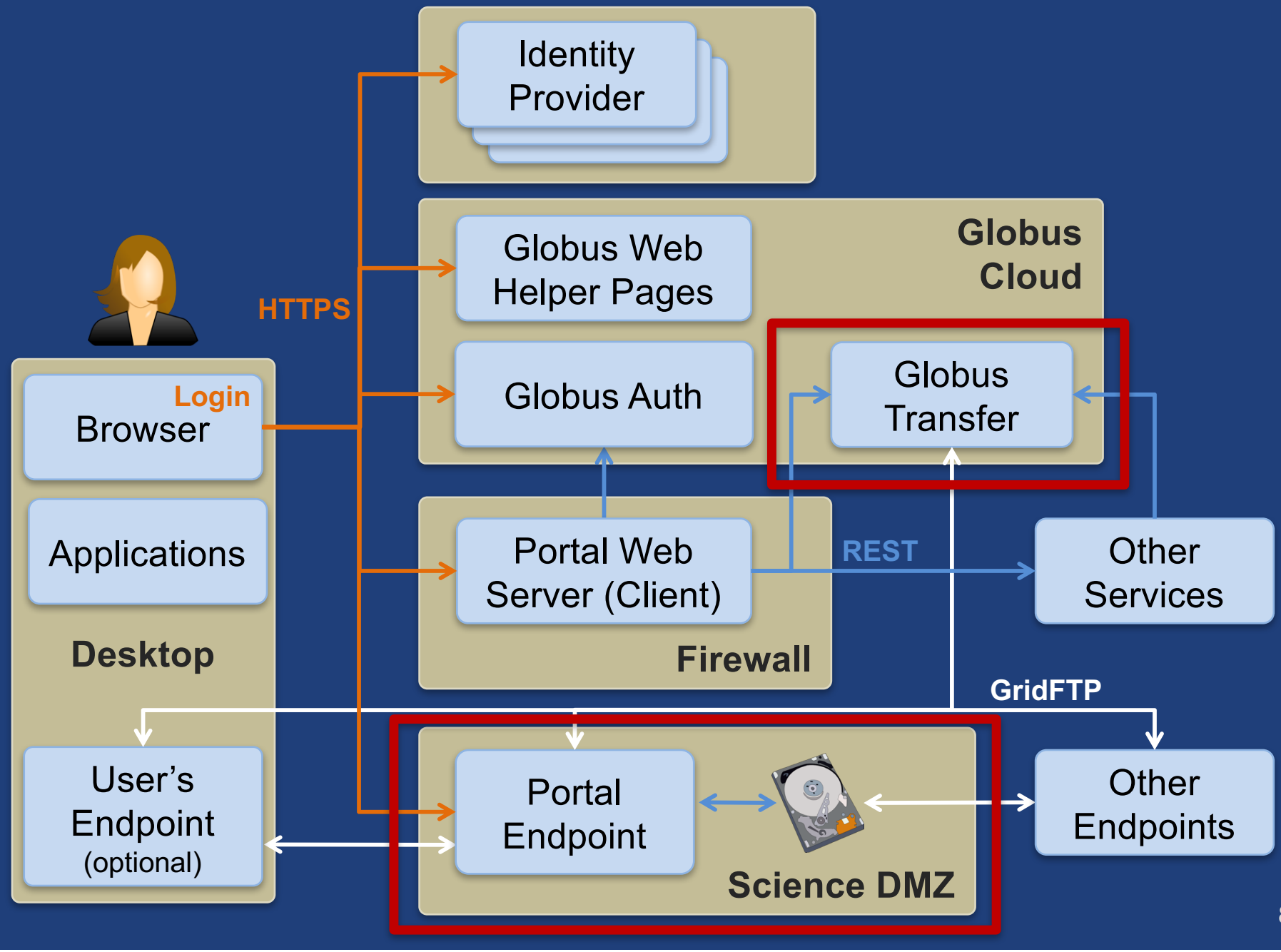
Mouse over the table headings for detailed descriptions

Data Description		Data File Downloads		Customizable Data Requests	Other Access Methods	NCAR-Only Access	
		Web Server Holdings	Globus Transfer Service (GridFTP)	Subsetting	THREDDS Data Server	Central File System (GLADE) Holdings	Tape Archive (HPSS) Holdings
Union of Available Products		Web File Listing	Request Globus Invitation	Get a Subset	TDS Access	GLADE File Listing	HPSS File Listing
PRODUC	Diurnal monthly means	Web File Listing		Get a Subset		GLADE File Listing	HPSS File Listing
	Regular monthly means	Web File Listing		Get a Subset		GLADE File Listing	HPSS File Listing
	Selected Parameter/Level Time Series	Web File Listing		Get a Subset	TDS Access	GLADE File Listing	HPSS File Listing

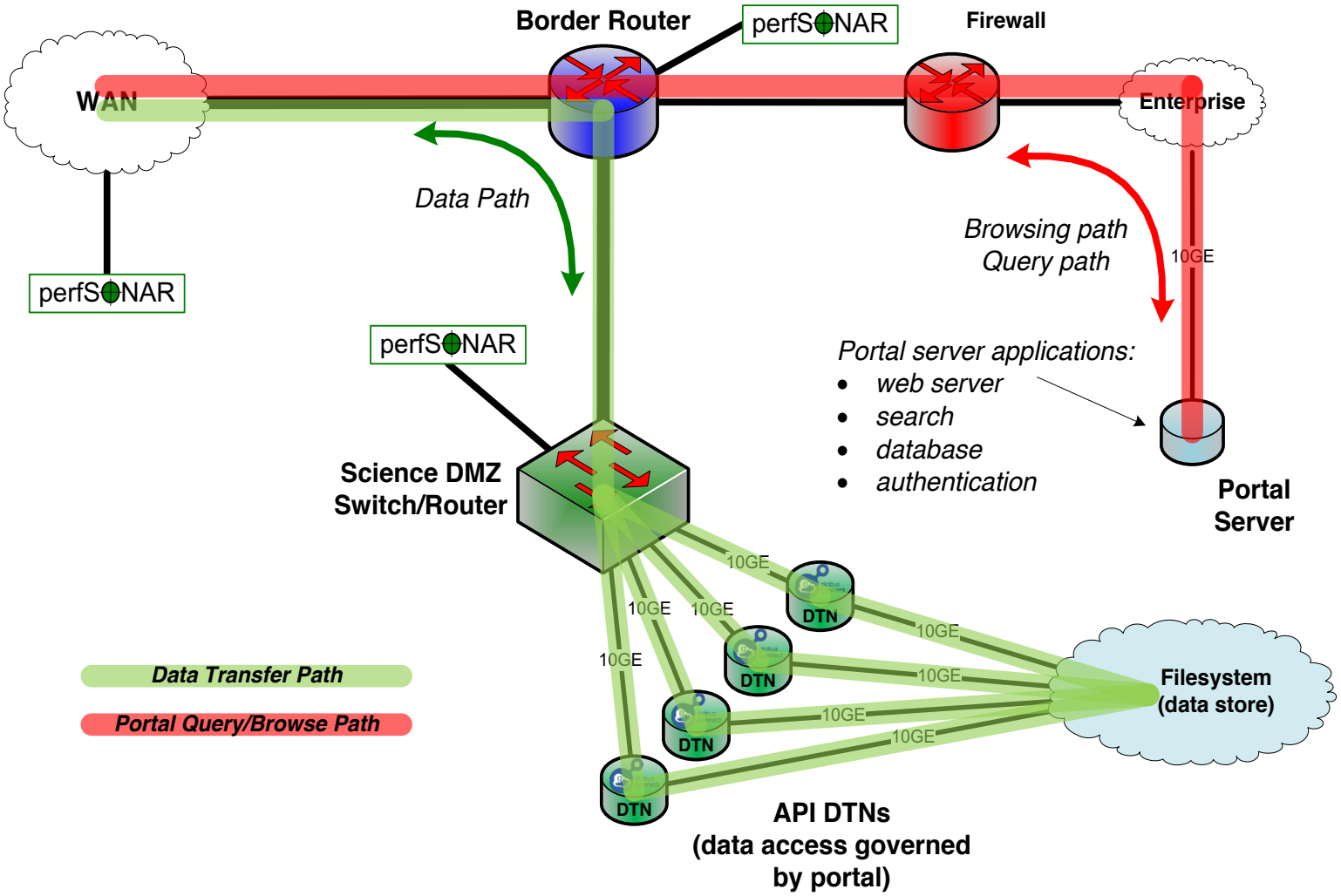
Prototypical research data portal



Prototypical research data portal



Next-Generation Portal Leverages Science DMZ



https://fasterdata.es.net/

Globus Transfer API

- **Nearly all Globus Web App functionality implemented via public Transfer API**

docs.globus.org/api/transfer

- **Requests authorized via OAuth2 access token**
  - Authorization: Bearer asdflkqhafsdafeawk

Transfer API Functionality

- Endpoint search
- Endpoint management
- Endpoint activation
- File operations
- Task submission
- Task management
- Bookmarks
- Shared endpoint access rules (ACLs)
- Management console

Globus Python SDK

- **Python client library for the Globus Auth and Transfer REST APIs**

globus.github.io/globus-sdk-python

- **Public beta, likely to change some**
- **Open source**

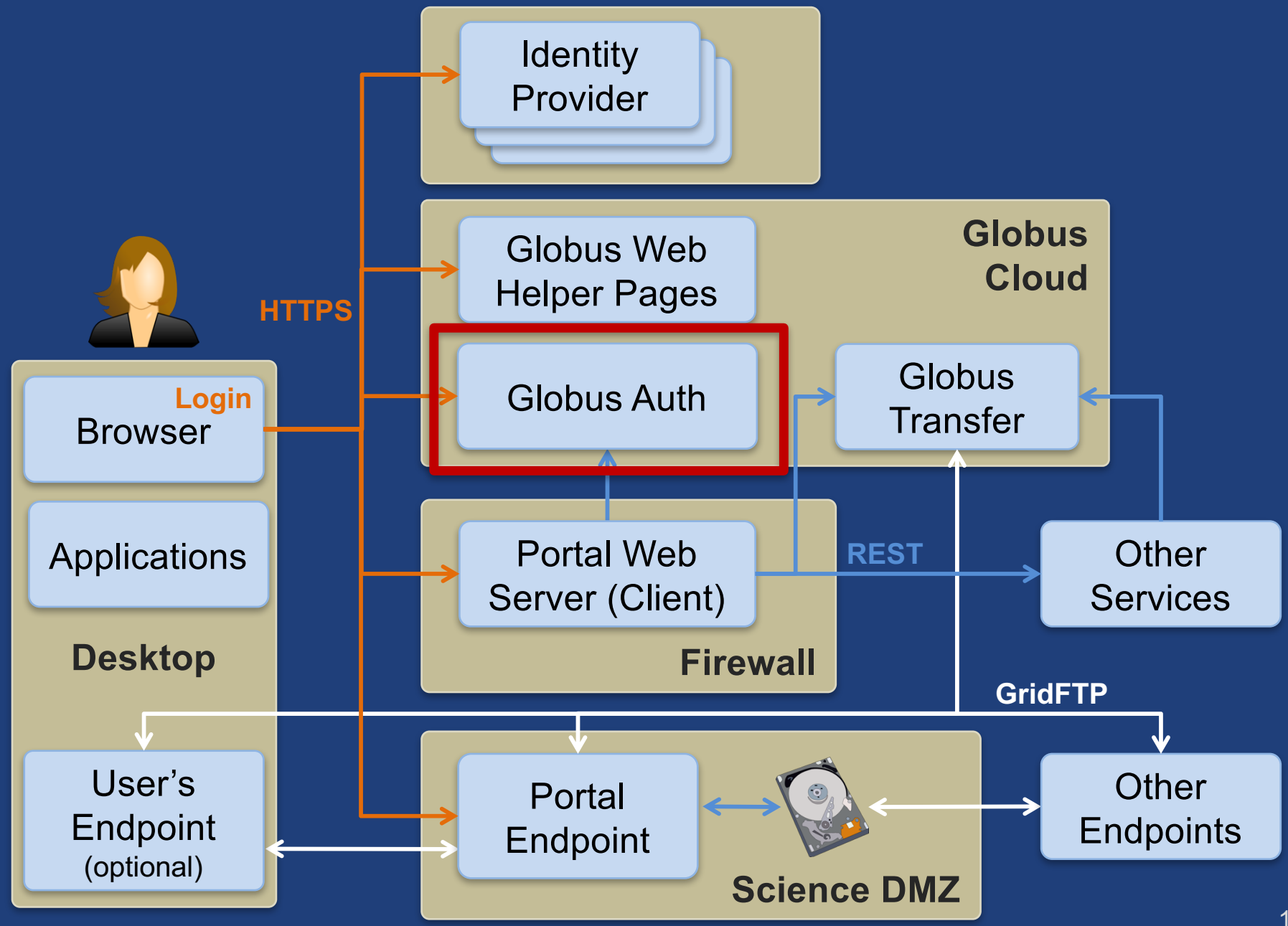
Python SDK Jupyter notebook

- **Jupyter (iPython) notebook demonstrating use of Python SDK**

github.com/globus/globus-jupyter-notebooks

- **Overview**
- **Open source**

Prototypical research data portal



Challenge

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

- **Foundational identity and access management (IAM) platform service**
- **Simplify 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

Globus Auth

- **Identity and access management PaaS**

docs.globus.org/api/auth

- **Introduction**
- **Developer Guide**
- **Reference**

Based on widely used web standards

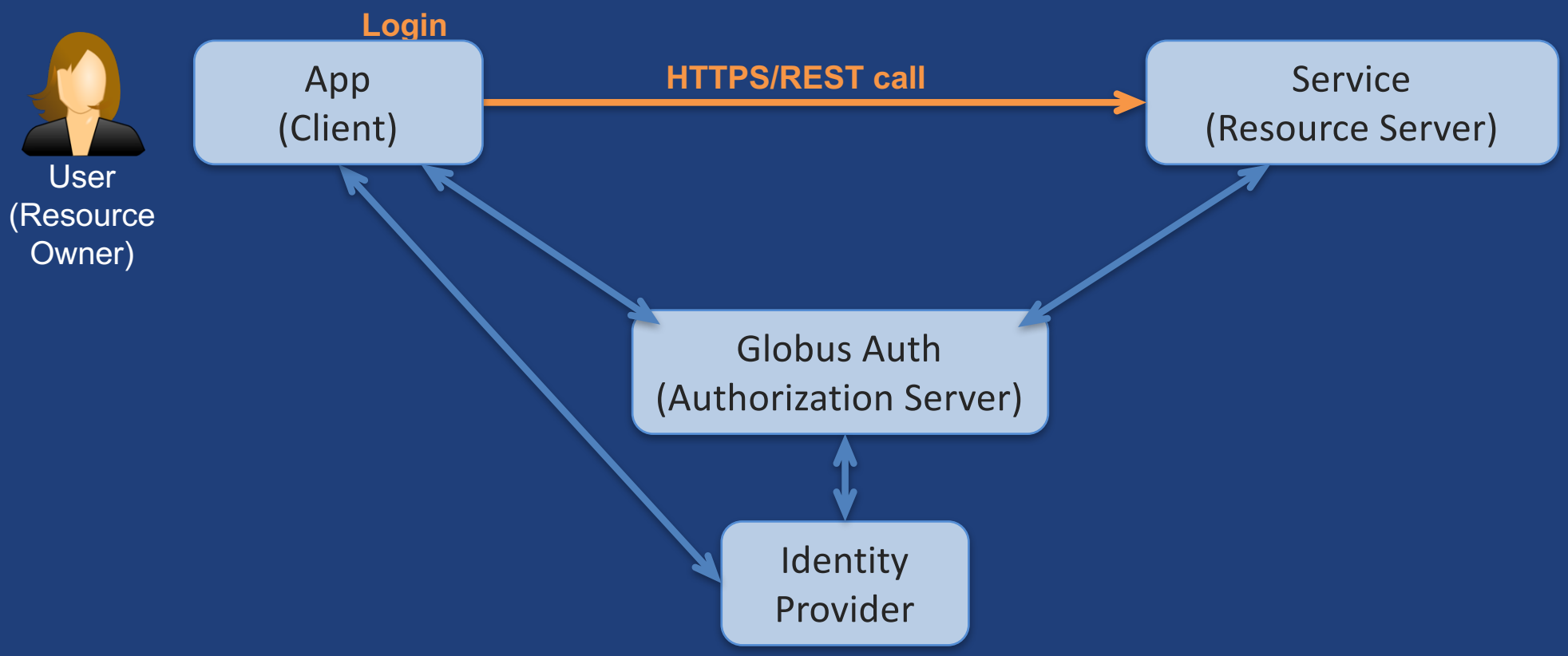
- **OAuth 2.0 Authorization Framework**
  - aka OAuth2
- **OpenID Connect Core 1.0**
  - aka OIDC

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

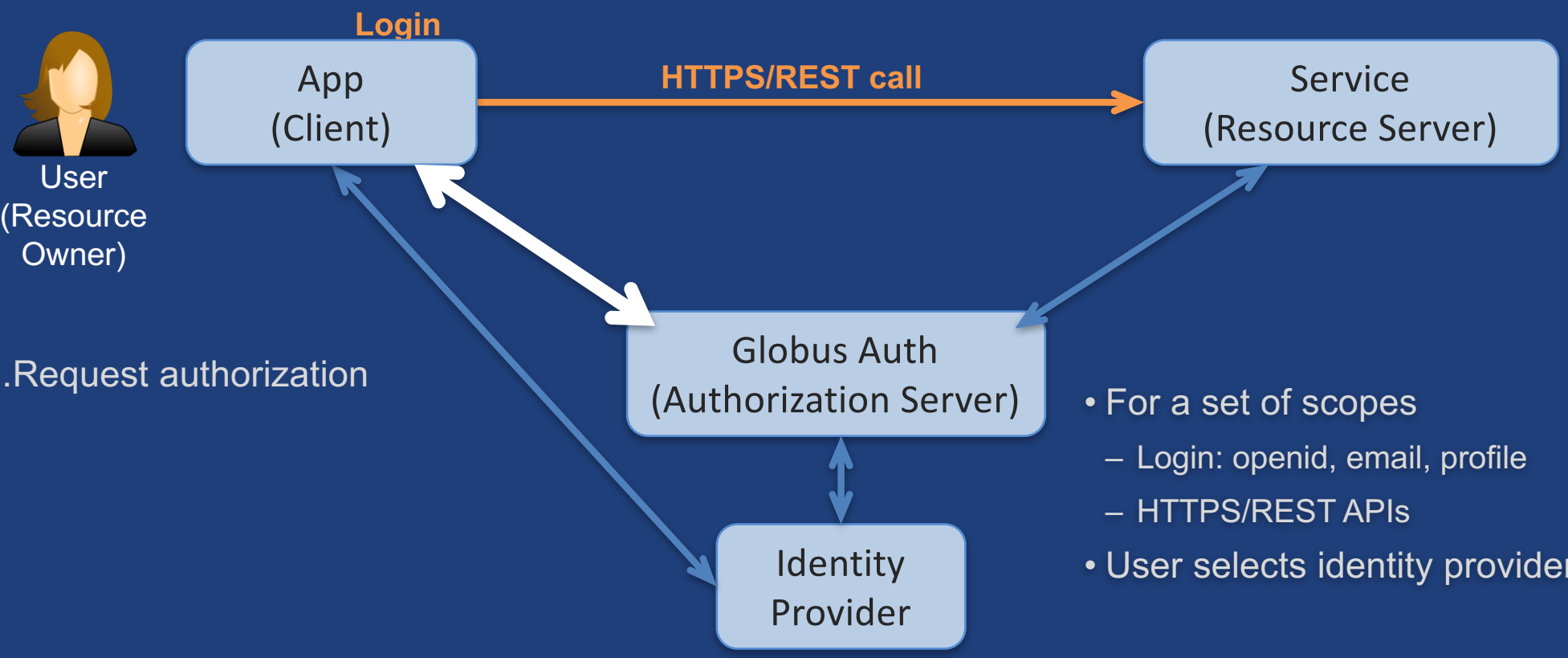
Globus account

- **A Globus account is a set of identities**
  - A *primary identity*
    - Identity can be primary of only one account
  - One or more *linked identities*
    - Identity can (currently) be linked to only one account
- **Account does not have own identifier**
  - An account is uniquely identified using its primary identity

Globus Auth interactions



Globus Auth interactions



1.Request authorization

- For a set of scopes
  - Login: openid, email, profile
  - HTTPS/REST APIs
- User selects identity provider

Globus Auth interactions

User (Resource Owner)

Login

App (Client)

HTTPS/REST call

Service (Resource Server)

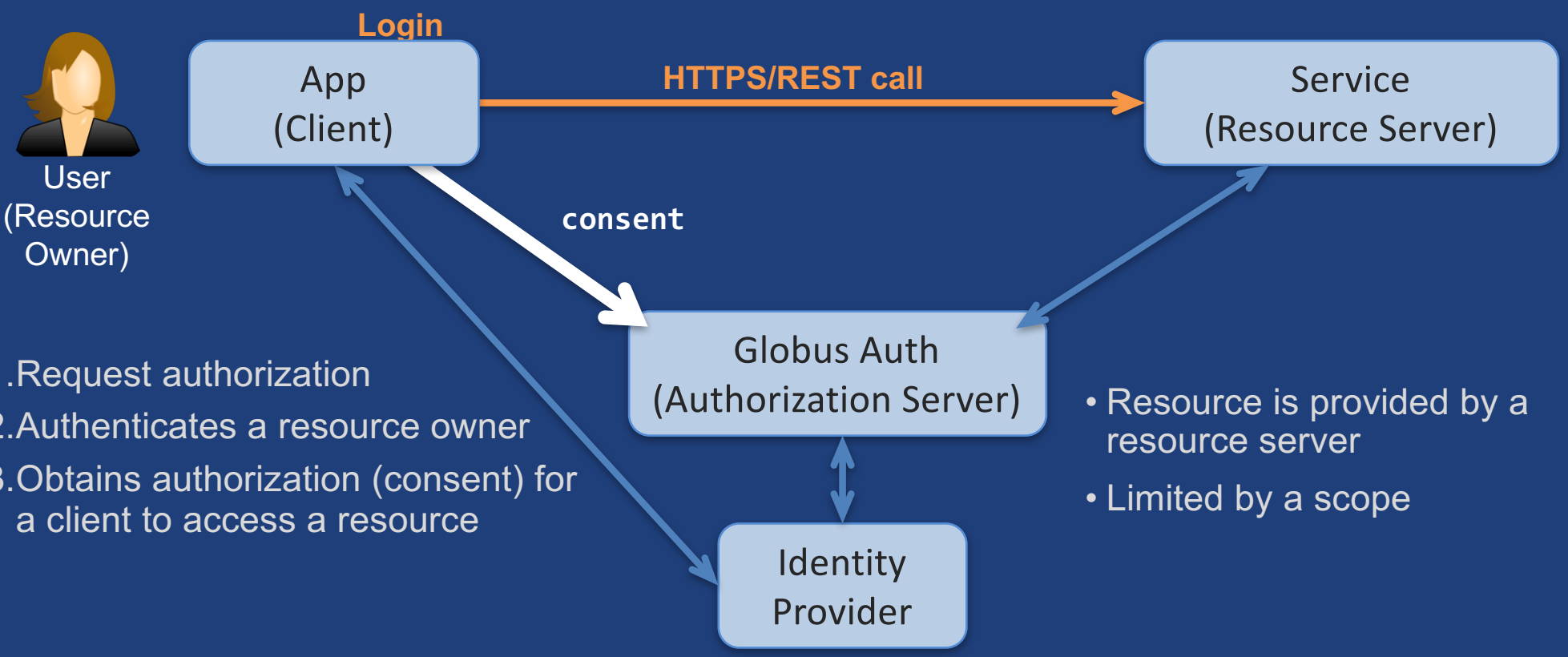
Globus Auth (Authorization Server)

Identity Provider

1. Request authorization
2. Authenticates a resource owner

- Using existing identities
  - XSEDE, University (via InCommon), Google, web app, etc.
- User can link multiple identities into a single Globus Account
- No Globus username (Globus ID) required
- Globus Auth handles naming details, e.g., ePPN vs ePTID

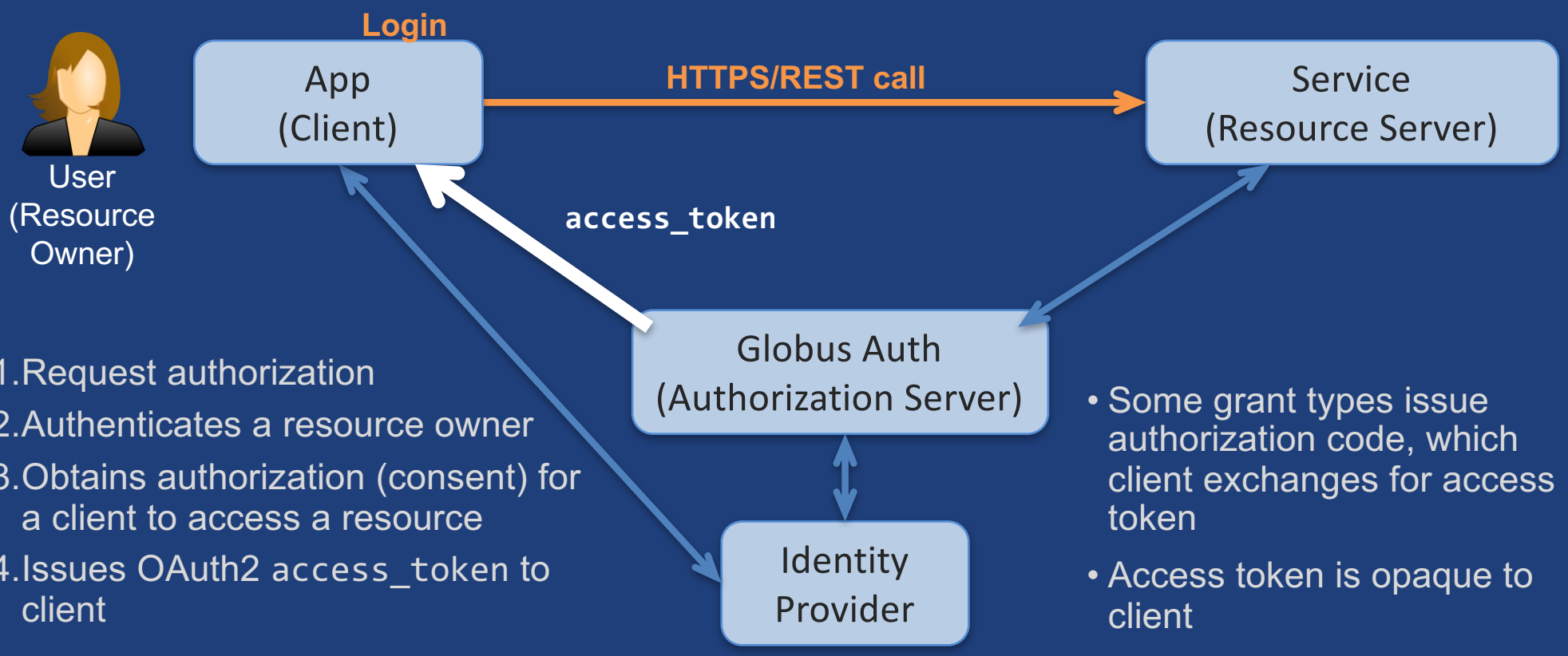
Globus Auth interactions



1. Request authorization
2. Authenticates a resource owner
3. Obtains authorization (consent) for a client to access a resource

- Resource is provided by a resource server
- Limited by a scope

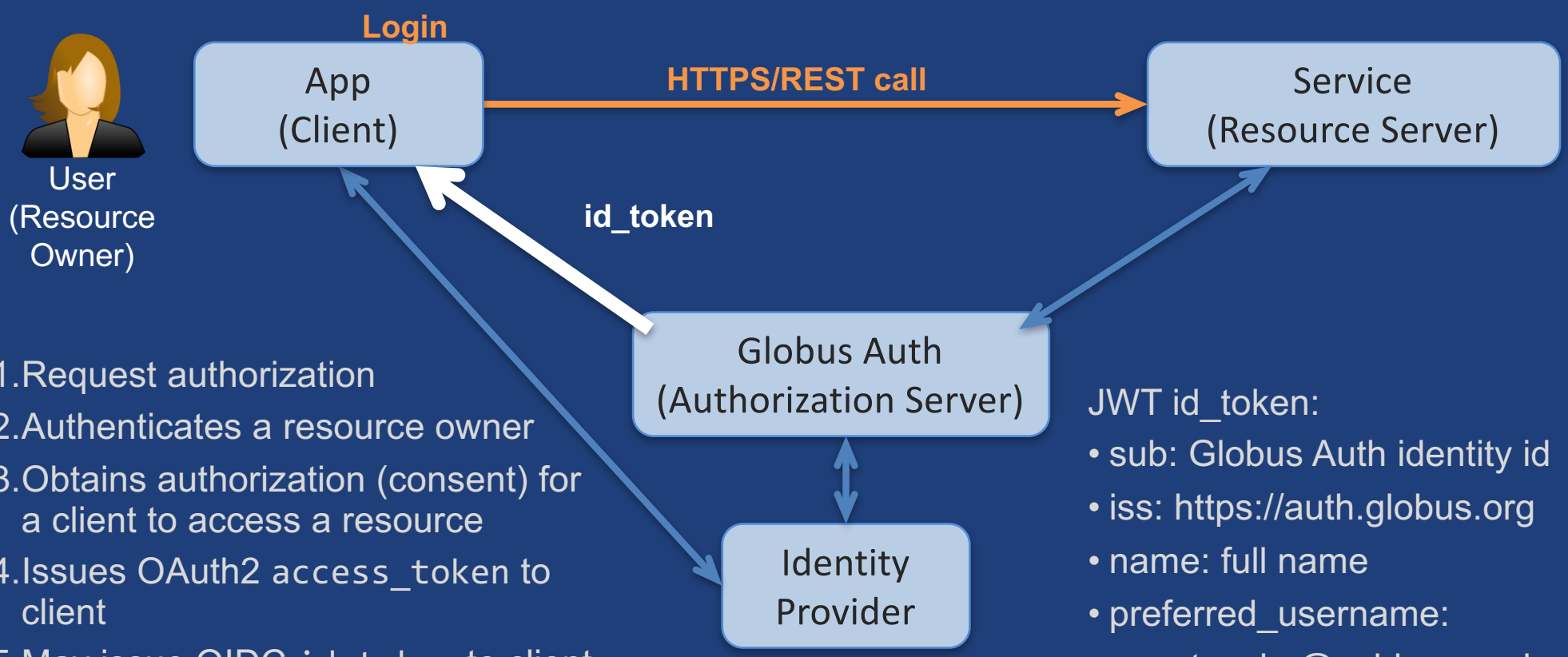
Globus Auth interactions



1. Request authorization
2. Authenticates a resource owner
3. Obtains authorization (consent) for a client to access a resource
4. Issues OAuth2 `access_token` to client

- Some grant types issue authorization code, which client exchanges for access token
- Access token is opaque to client
- May include a refresh token, for offline access

Globus Auth interactions

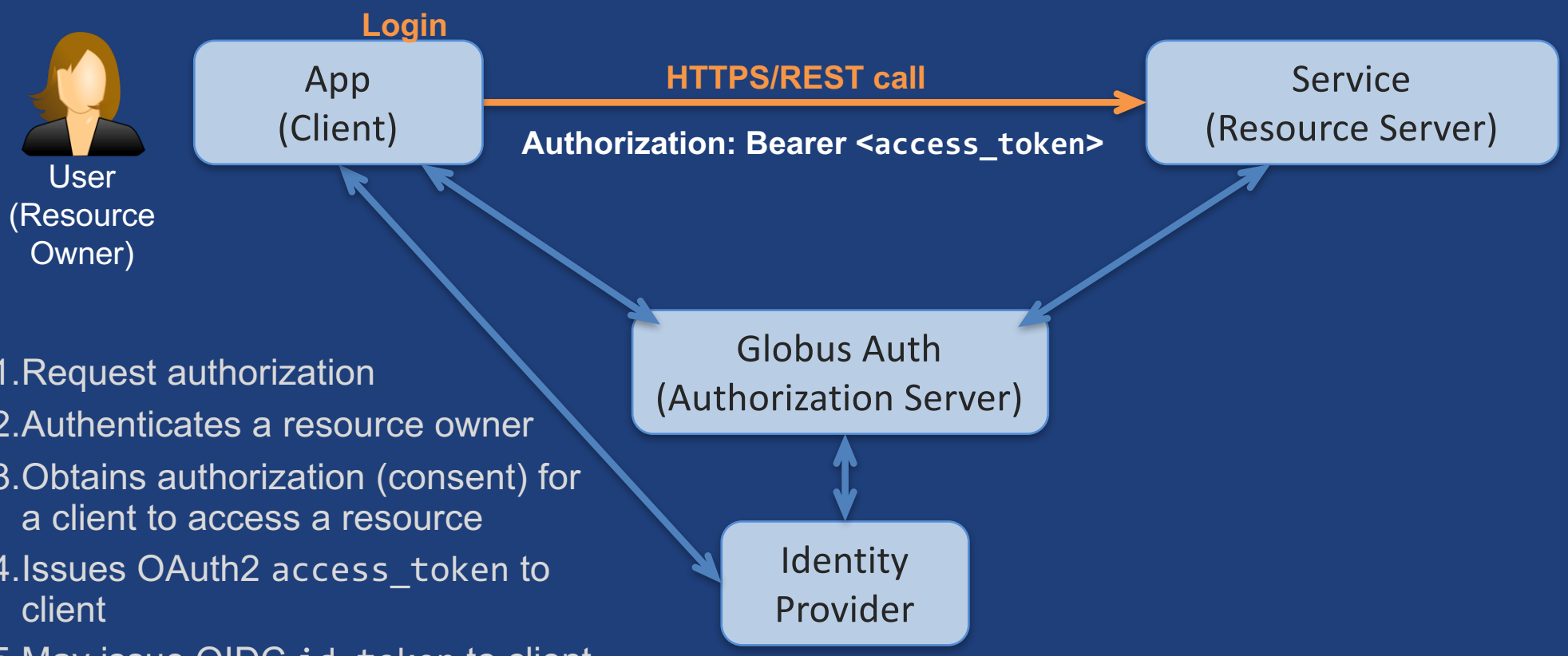


1. Request authorization
2. Authenticates a resource owner
3. Obtains authorization (consent) for a client to access a resource
4. Issues OAuth2 `access_token` to client
5. May issue OIDC `id_token` to client with resource owner identity

JWT id_token:

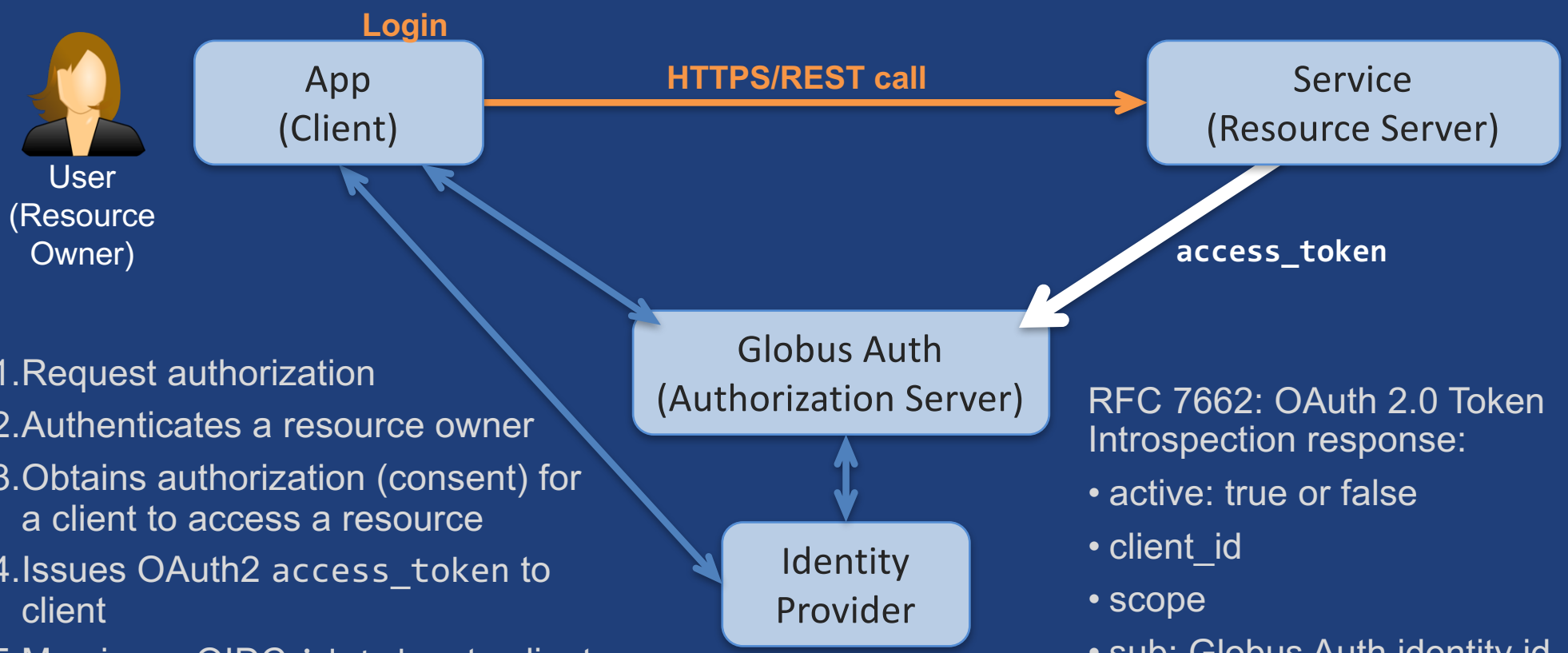
- sub: Globus Auth identity id
- iss: https://auth.globus.org
- name: full name
- preferred_username:
- e.g., tuecke@uchicago.edu
- email: email contact
- other standard OIDC claims

Globus Auth interactions



1. Request authorization
2. Authenticates a resource owner
3. Obtains authorization (consent) for a client to access a resource
4. Issues OAuth2 `access_token` to client
5. May issue OIDC `id_token` to client with resource owner identity
6. HTTPS/REST call with `access_token`

Globus Auth interactions

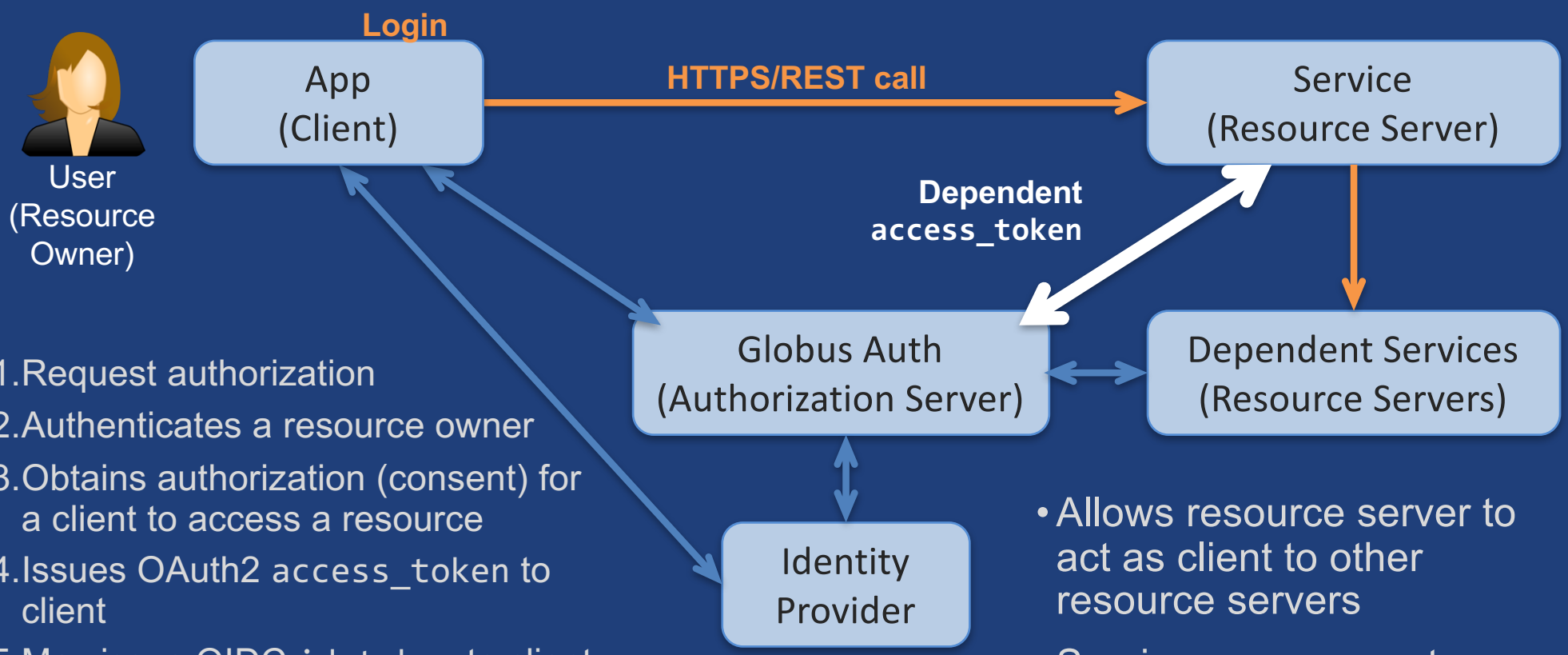


1. Request authorization
2. Authenticates a resource owner
3. Obtains authorization (consent) for a client to access a resource
4. Issues OAuth2 `access_token` to client
5. May issue OIDC `id_token` to client with resource owner identity
6. HTTPS/REST call with `access_token`
7. Validates `access_token` for resource server, gets additional info

RFC 7662: OAuth 2.0 Token Introspection response:

- active: true or false
- client_id
- scope
- sub: Globus Auth identity id
- username: user@myu.edu
- identity_set: linked identities
- email
- name
- other standard claims

Globus Auth interactions



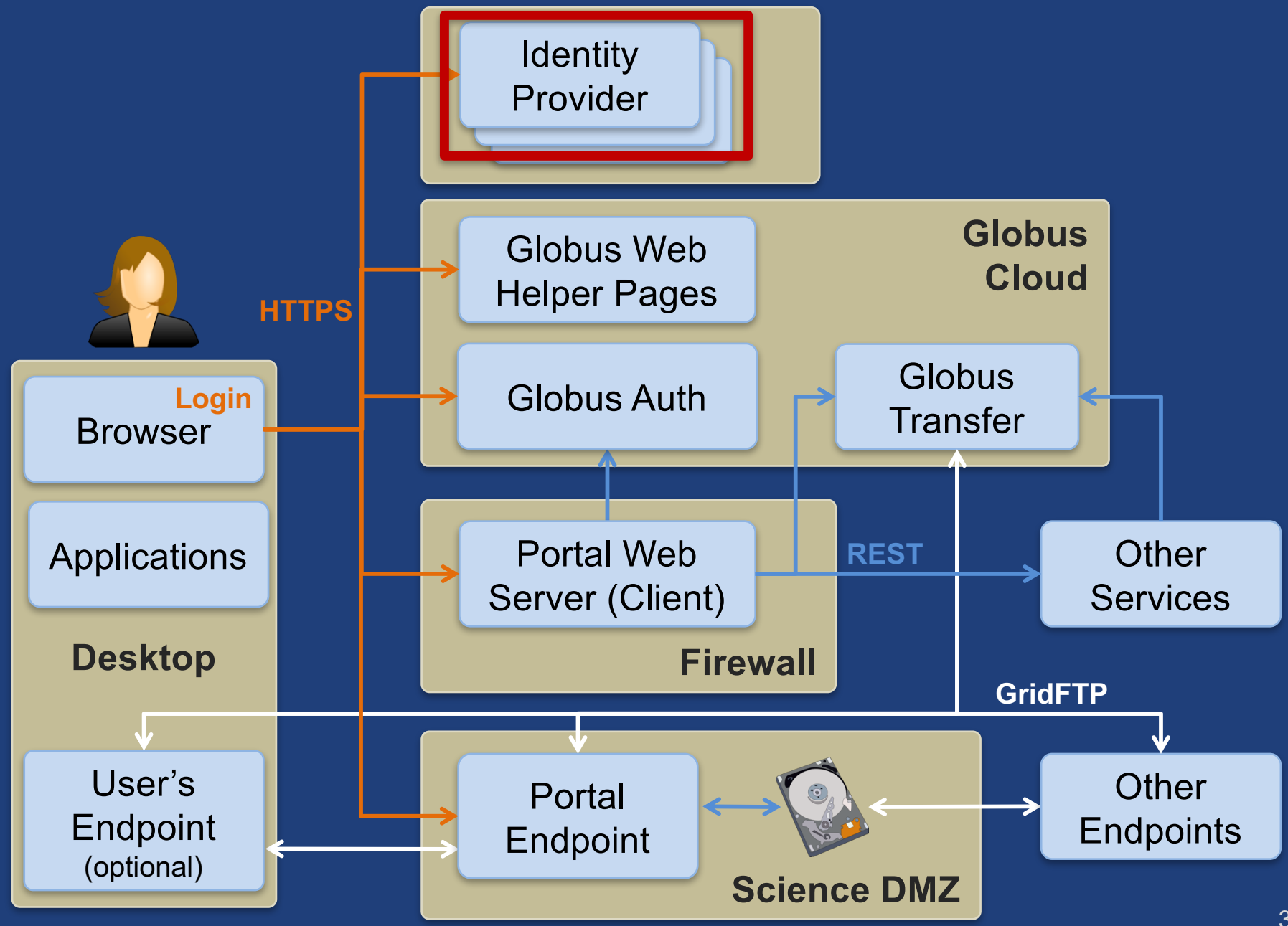
1. Request authorization
2. Authenticates a resource owner
3. Obtains authorization (consent) for a client to access a resource
4. Issues OAuth2 `access_token` to client
5. May issue OIDC `id_token` to client with resource owner identity
6. HTTPS/REST call with `access_token`
7. Validates `access_token` for resource server, gets additional info
8. Issues dependent access tokens to resource server

- Allows resource server to act as client to other resource servers
- Service uses request `access_token` to get a *dependent* `access_token` for each dependent service
- Service acts as client to its dependent services

User identity vs portal identity

- **User logging into portal results in portal having user's identity and access token**
  - Used to make requests on the user's behalf
  - Use OAuth2 Authorization Code Grant
  - User authenticates using their portal identity
- **Portal may also need its own identity**
  - Access and refresh tokens for this identity
  - Used to make requests on its own behalf
  - Use OAuth2 Client Credentials Grant to authenticate the portal client identity and secret

Prototypical research data portal



Adding your identity provider

- **InCommon identity providers that release research & scholarship attributes to CILogon** ***(free)***

- **Any other OpenID Connect identity provider** ***(subscription)***

Adding portal as identity provider

- **If your portal has identities already:**
  - Deploy OIDC server in front of it
    - Globus Python OIDC (coming soon)
    - Any standard OIDC server should work
    - Requires claim that can map to username
    - Optional claims: name, email, organization
  - Can register apps and services with an effective identity policy
    - Requires account to have identity from your identity provider when logging into your app

Remove RDA Username & Password

Hello Guest! Register Now | Sign In | Forgot Password?

Email/Username: Password: Sign In

Remember me on this computer

Archive

Computational & Information Systems Lab

weather • data • climate

Go to Dataset: nnn.n

Home | Find Data | Ancillary Services | About/Contact | Data Citation | Web Services | For Staff

First-time visitor to our site?

Please take a video tour of our home page

Dataset Search:

Keyword(s) Search Advanced Options

Look For Data:

All Datasets	Variable/Parameter	Type of Data
Time Resolution	Platform	Spatial Resolution
Topic/Subtopic	Project/Experiment	Supports Project
Data Format	Location	Recently Added/Updated

Recently Added Datasets: (within the last 6 months)

- United Kingdom Hadley Centre Climate Model Version 3 Output
- Cross-Calibrated Multi-Platform Ocean Surface Wind Vector Analysis Product V2, 1987 - ongoing
- An Ensemble of Atmospheric Forcing Files from a CAM reanalysis
- ECMWF IFS CY41r2 High-Resolution Operational Forecasts
- International Comprehensive Ocean-Atmosphere Data Set (ICOADS) Release 3, Individual Observations
- International Comprehensive Ocean-Atmosphere Data Set (ICOADS) Release 3, Monthly Summaries
- EarthScope USArray Transportable Array (TA) Surface Pressure Observations Sampled at 1 Hz Frequency
- Coordinated Ocean-ice Reference Experiments - Phase II

Get Help:

- Frequently Asked Questions
- Reset your password
- A-Z Site Index
- RDA Users Email List
- RDA Blog
- RDA video tutorials
- Email Us

From Our Blog:

- NCAR RDA Partial Outage Aug 2, 2016
- What spatial resolution can I expect when using gridded dataset products?
- NCAR RDA Partial Outage July 12, 2016
- NCAR RDA System Outage June 28, 2016

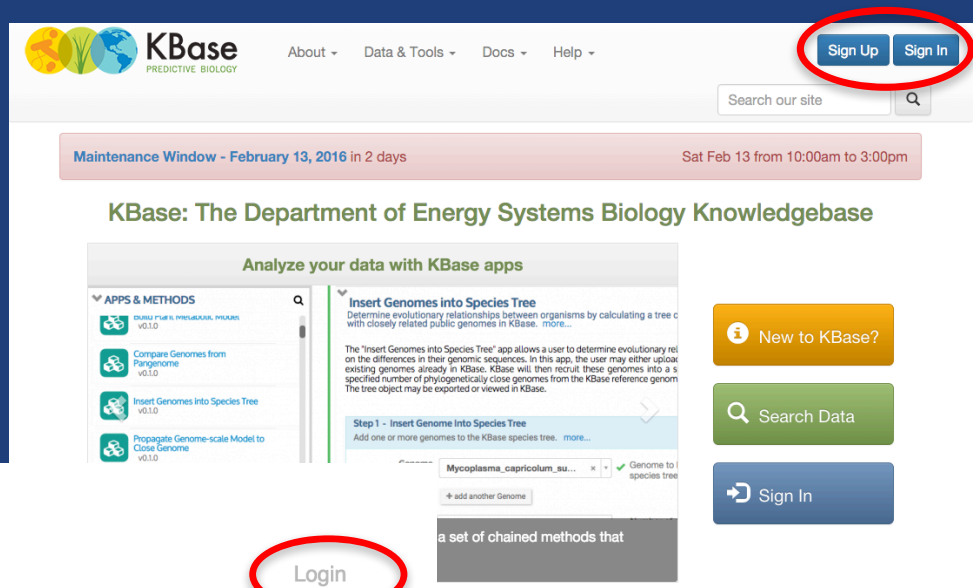
More blog posts ...

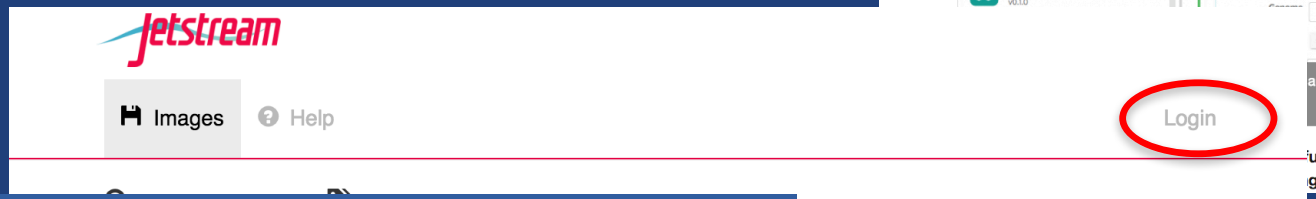
GLADE Users:

ucar.edu

Log in with Globus

- **Similar to Log in with Google and Log in with Facebook**
- **Using existing identities**
- **Providing access to community services**





Log in to Jetsteam app

https://use.jetstream-cloud.org/application/images

jetstream | Images | Help | Login

SEARCH | TAGS

Search across image name, tag or description

Showing 27 of 27 images

List | Grid

Featured Images

Centos 7 (7.2) Development
Jun 24th 2016 10:27 pm CEST by **jfischer**
CentOS | development | Featured

Based on Centos 7 Cloud 1601 Image, Development tools added, Patched up to date as of 6/23/16.

Ubuntu 14.04.3 Development GUI
Jun 24th 2016 09:57 pm CEST by **jfischer**
desktop | development | Featured | gui | Ubuntu | vnc

Based on Ubuntu 14.04.3 Development Patched up to date as of 5/12/16 Base Ubuntu 14.04.3 + Xfce + Xfce-goodies, firefox, icon sets and themes

©2016 Jetstream-Cloud Feedback & Support

Globus Auth login page

https://auth.globus.org/p/login?access_type=online&authentication_hint=xsede&state=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZnAiOiJ5Vnho...

globus Globus Account Log In

XSEDE
Extreme Science and Engineering Discovery Environment

Log in to use Jetstream Web App

Use your existing organizational login

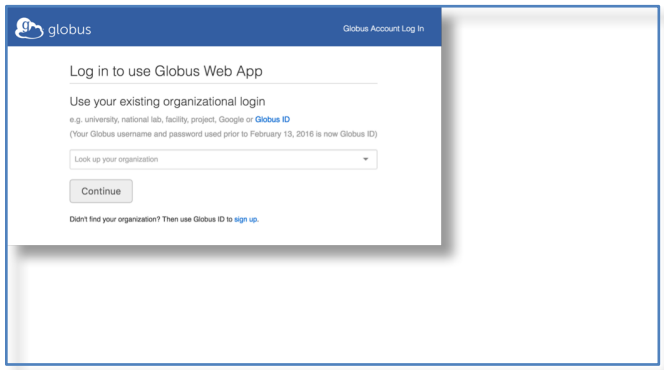
e.g. university, national lab, facility, project, Google or Globus ID

(Your Globus username and password used prior to February 13, 2016 is now Globus ID)

XSEDE

Continue

Didn't find your organization? Then use Globus ID to sign up.



Campus login via InCommon

THE UNIVERSITY OF CHICAGO

CILogon

Sign In

Login to **CILogon**
CILogon facilitates secure access to CyberInfrastructure (CI).

CNetID / UCHADID: tuecke

Hospital Employee?

Password: ••••••••••••••

Forgot your password?

Login

Signing in allows you to access multiple University of Chicago web applications while entering your CNetID and password only once. To end your session, simply close your browser.

Questions? Contact the IT Services Service Desk by phone at 2-5800 (773-702-5800), via email at itservices@uchicago.edu, or get walk-in help at the TECHB@R on the first floor of Regenstein Library during reference desk hours http://hours.lib.uchicago.edu/.

Alumni account holders may contact alumnitechsupport@uchicago.edu or call 1-877-292-3945 between 9 AM and 3 PM CST with any

Consent

https://auth.globus.org/v2/oauth2/authorize?access_type=online&authentication_hint=xsede&redirect_uri=https%3A%2F%2Fuse.jetstream-cloud.or...

globus Account

XSEDE
Extreme Science and Engineering Discovery Environment

Jetstream Web App would like to:

- Access all Jetstream resources

By clicking "Allow", you allow **Jetstream Web App** (this client has not provided terms of service or a privacy policy to Globus) to use the above listed information and services. You can rescind this and other consents at any time.

Allow Deny

globus Account

Globus Web App would like to:

- View your identities on Globus Auth
- Manage your Globus Groups
- Transfer files using Globus Transfer

To work, the above will need to:

- View your identities on Globus Auth
- Manage your Globus Groups

By clicking "Allow", you allow **Globus Web App**, in accordance with its terms of service and privacy policy, to use the above listed information and services. You can rescind this and other consents at any time.

Allow Deny

Logged in

https://use.jetstream-cloud.org/application

jetstream

Dashboard | Projects | Images | Providers | Help | tuecke

Getting Started

Launch New Instance

Browse Atmosphere's list of available images and select one to launch a new instance.

Browse Help Resources

View a video tutorial, read the how-to guides, or email the Atmosphere support team.

Change Your Settings

Modify your account settings, view your resource quota, or request more resources.

Resources in Use *Need more?*

Jetstream – Indiana University | Jetstream – TACC

100

80

60

Allocation Used

0 Instances

0 Volumes

©2016 Jetstream-Cloud | Feedback & Support

https://use.jetstream-cloud.org/application#

Identity id vs. username

- **Identity id:**
  - Guaranteed unique among all Globus Auth identities, and will never be reused
  - UUID
  - Always use this to refer to an identity
  - Similar to ePPID
- **Identity username:**
  - Unique at any point in time
    - May change, may be re-used
  - Case-insensitive user@domain
  - Can map to/from id, for user experience
  - Similar to ePPN
- **Auth API allows mapping back and forth**

Scopes

- **APIs that client is requesting access to**
- **Scope syntax:**

  urn:globus:auth:scope:<service-name>:<scope-name>
- **If client requests multiple scopes**
  - Token response has tokens for first scope
  - other_tokens field in response has list of token responses for other scopes
  - Client must use correct token with each request

Effective identity

- **App can choose to operate only with identities from a particular identity provider**
  - Globus Auth login will require an identity from that provider to be linked to user's account
  - OIDC id_token uses this "effective identity"
- **If app does not set an effective identity policy, then the primary identity of the account is used as the effective identity for that app**

App registration

developers.globus.org

- **Client_id and client_secret for service**
- **App display name**
- **Declare required scopes**
  - Need long-term, offline refresh tokens?
  - May require authorization from scope admin
- **OAuth2 redirect URIs**
- **Links for terms of service & privacy policy**
- **Effective identity policy (optional)**

Consent

- **Resource owner authorization that a client can request access to a service on the resource owner's behalf within a limited scope**
  - If service has dependent scopes, they are part of the consent
- **User can rescind a consent at any time**
  - Invalidates all access, dependent, and refresh tokens originating from the client

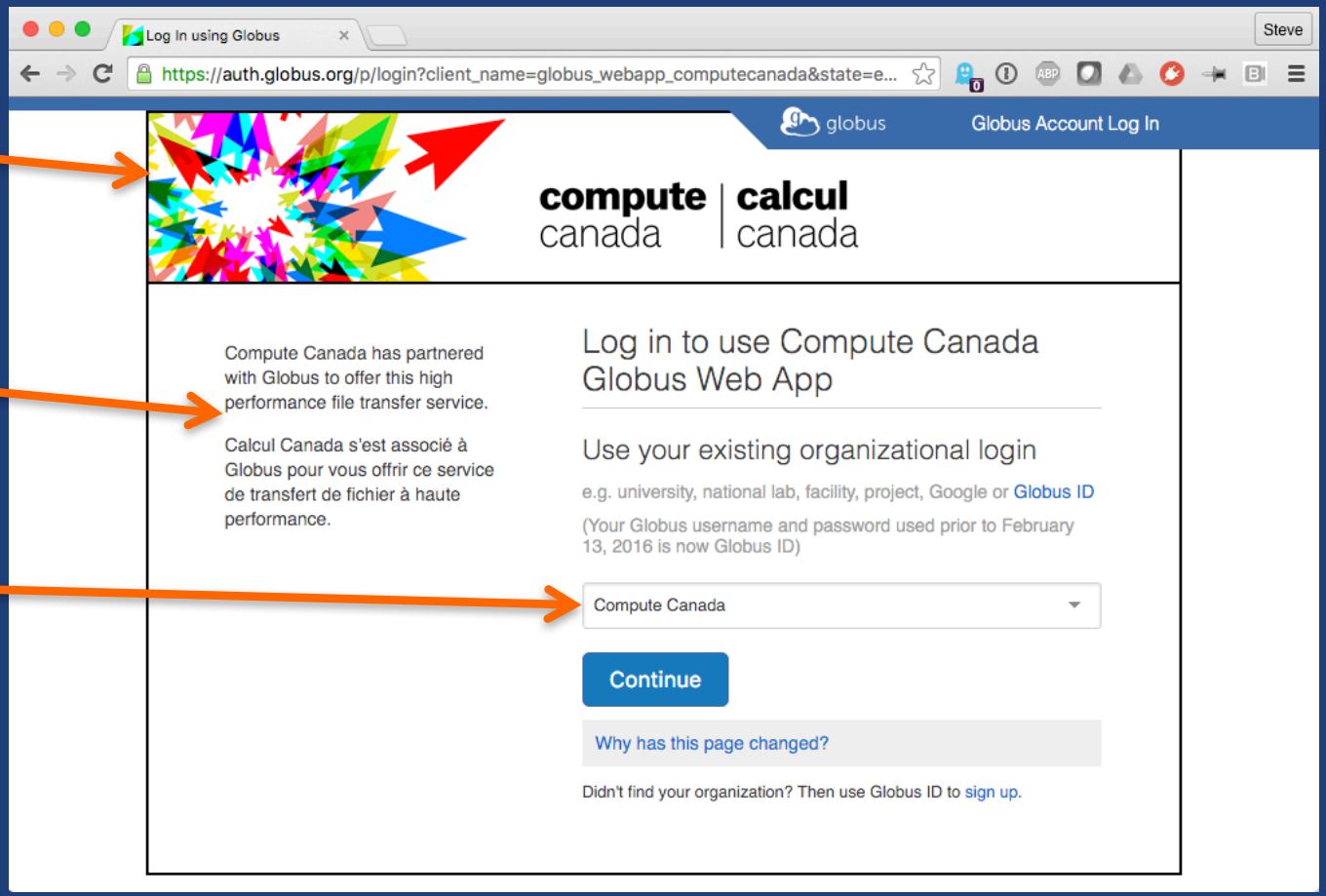
Branding

- **Can skin Globus Auth pages**

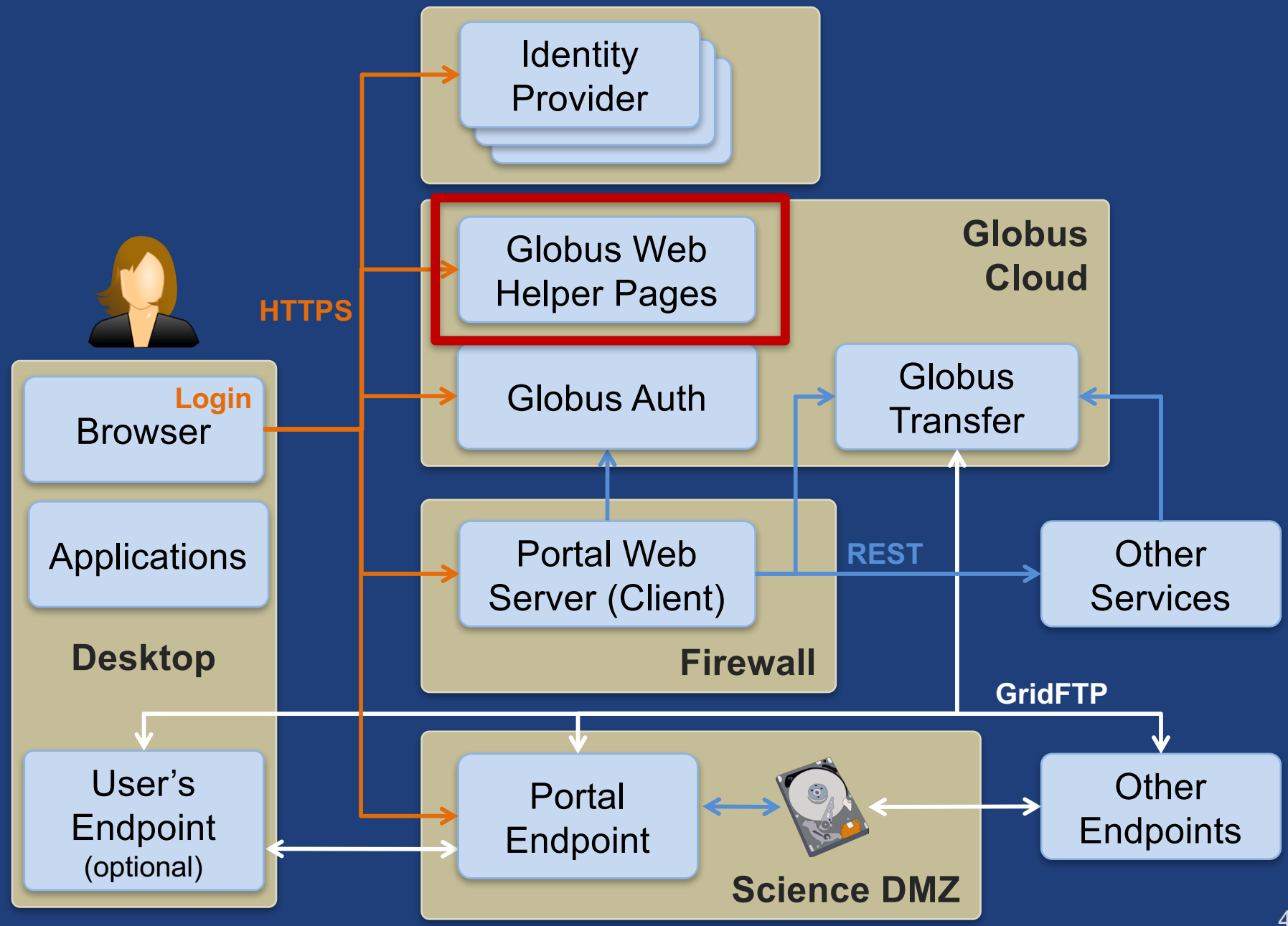
Header

Text

Default IDP

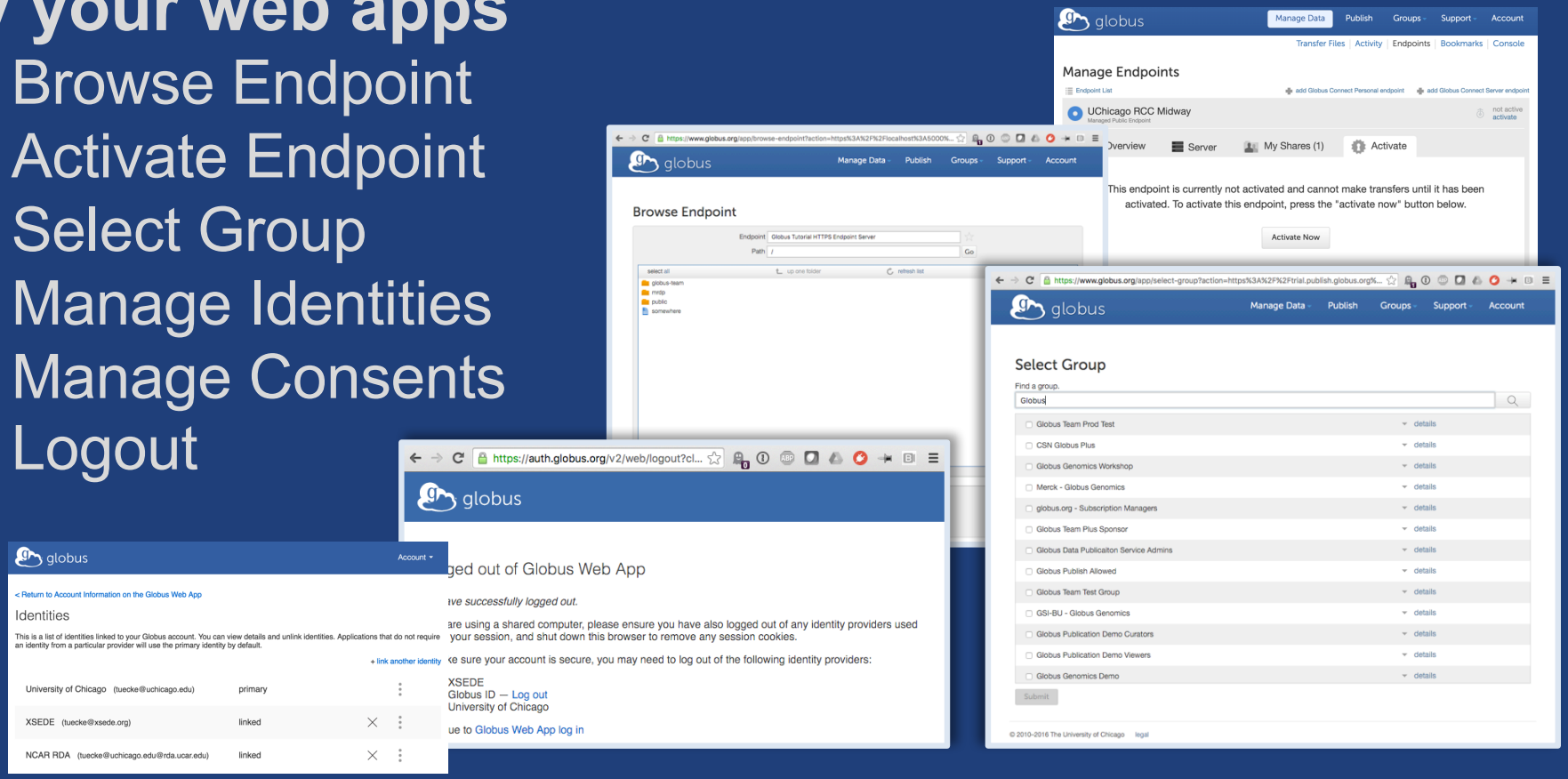


Prototypical research data portal



Globus Helper Pages

- **Globus provided web pages designed for use by your web apps**
  - Browse Endpoint
  - Activate Endpoint
  - Select Group
  - Manage Identities
  - Manage Consents
  - Logout

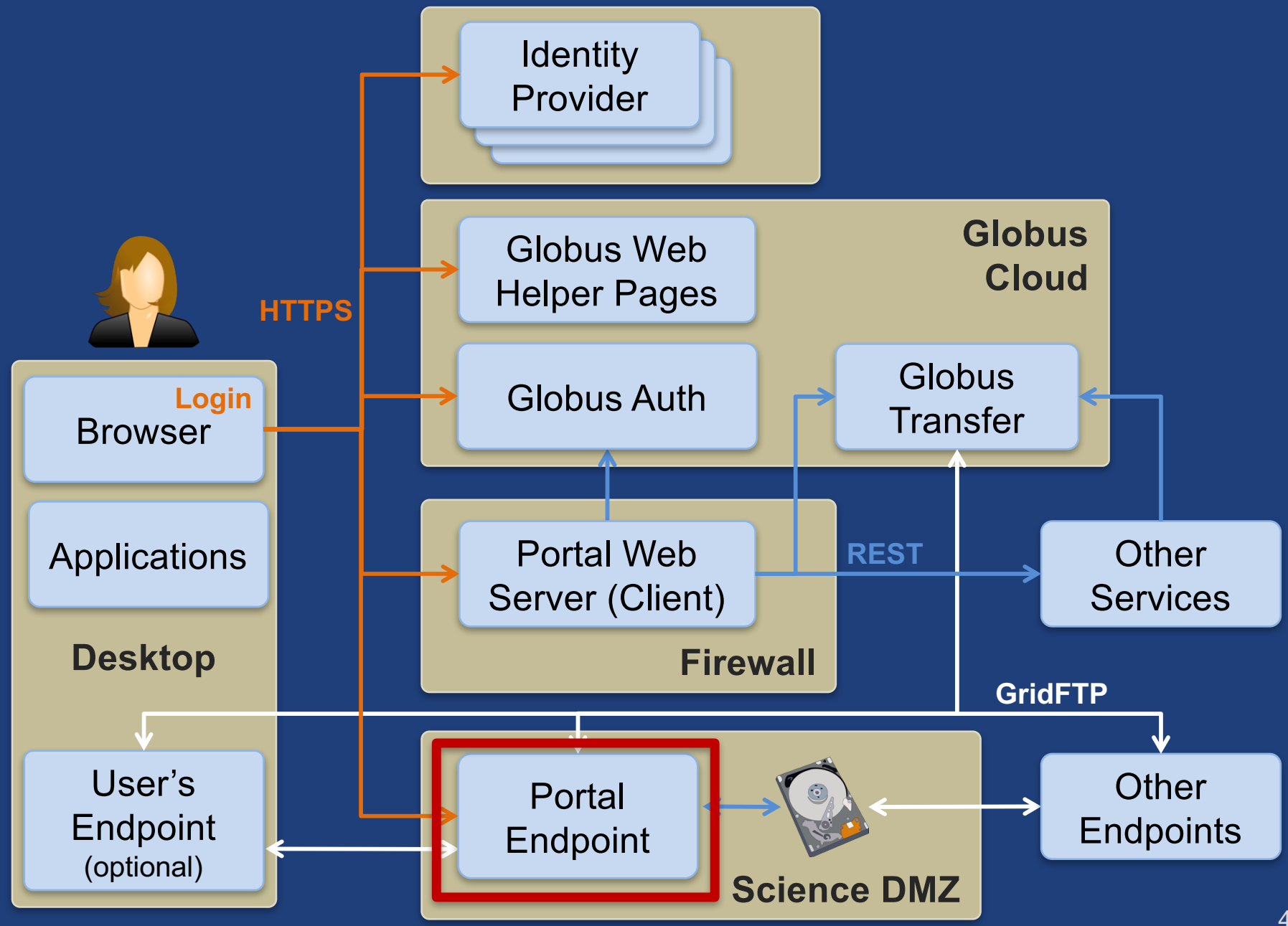


docs.globus.org/api/helper-pages

Client Logout

- **Call token revocation on access tokens**
  - https://auth.globus.org/v2/oauth2/token/revoke
  - Doc: **docs.globus.org/api/auth/reference**
  - Note: Does not revoke dependent tokens
- **Delete access tokens**
- **Redirect to logout helper page**
  - https://auth.globus.org/v2/web/logout
  - Doc: **docs.globus.org/api/helper-pages**

Prototypical research data portal

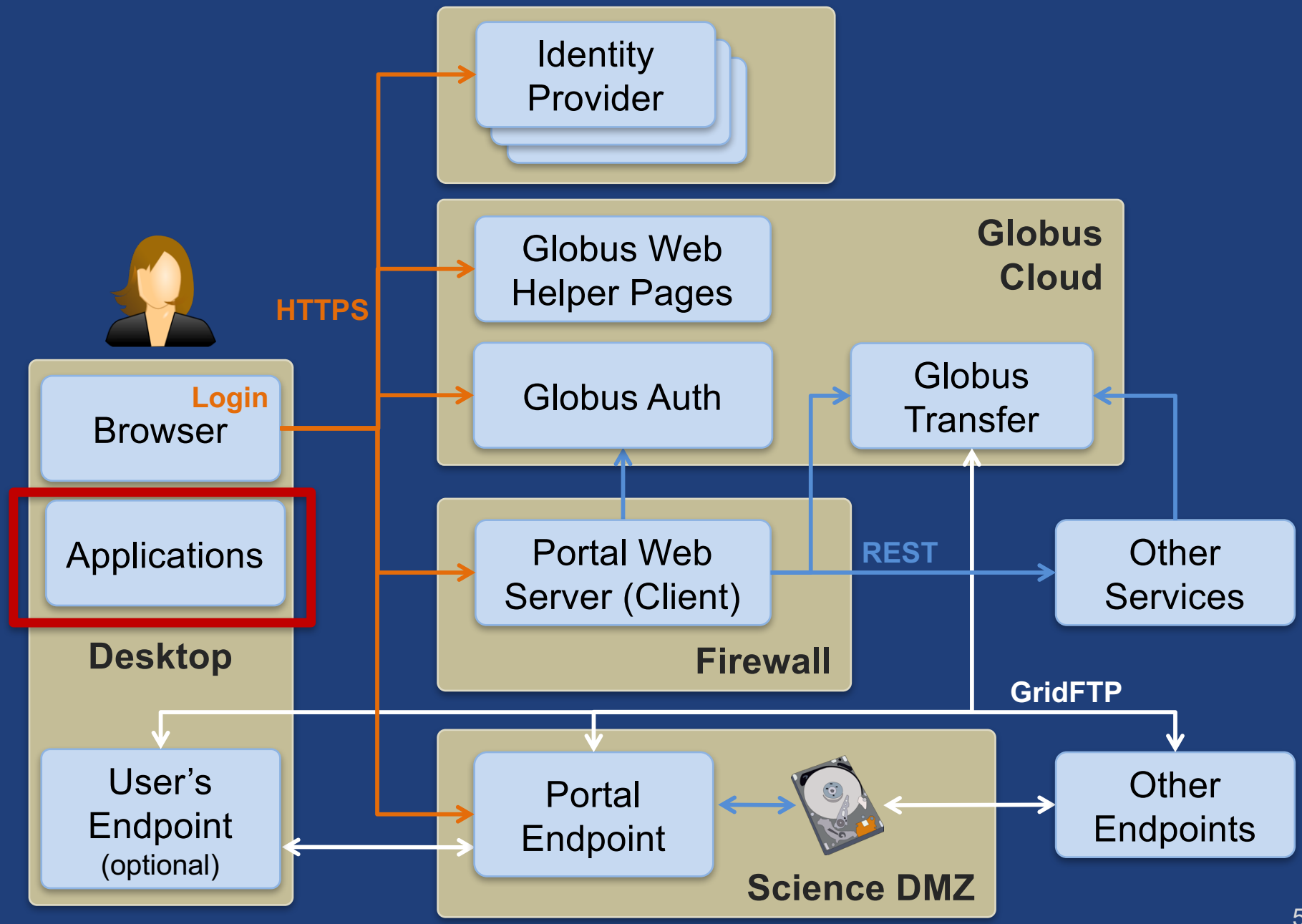


HTTPS to Endpoints

- **Each endpoint HTTPS server is a Globus Auth service (resource server)**
  - HTTPS requests authorized via Globus Auth issued OAuth2 access tokens
- **Web page can link to file on server**
  - Browser GET will cause HTTPS server to authorize request via Globus Auth (note SSO)
- **Portal (client) can request scope for endpoint resource server**
  - Use access token in requests

“A single global information space”

Prototypical research data portal



Mobile apps

- **Globus Auth supports mobile apps**
  - "Log in with Globus" in mobile apps
    - RFC 7636: Proof Key for Code Exchange by OAuth Public Clients (PKCE, pronounced "pixy")
    - Extension to OAuth2 to allow OAuth2 Authorization Code Grant to work from mobile apps
  - Uses mobile browser for web-based login
  - Mobile apps can call any service REST APIs that use Globus Auth
  - iOS and Android
  - Same approach as used by Google, Facebook, etc.

Desktop & command line apps

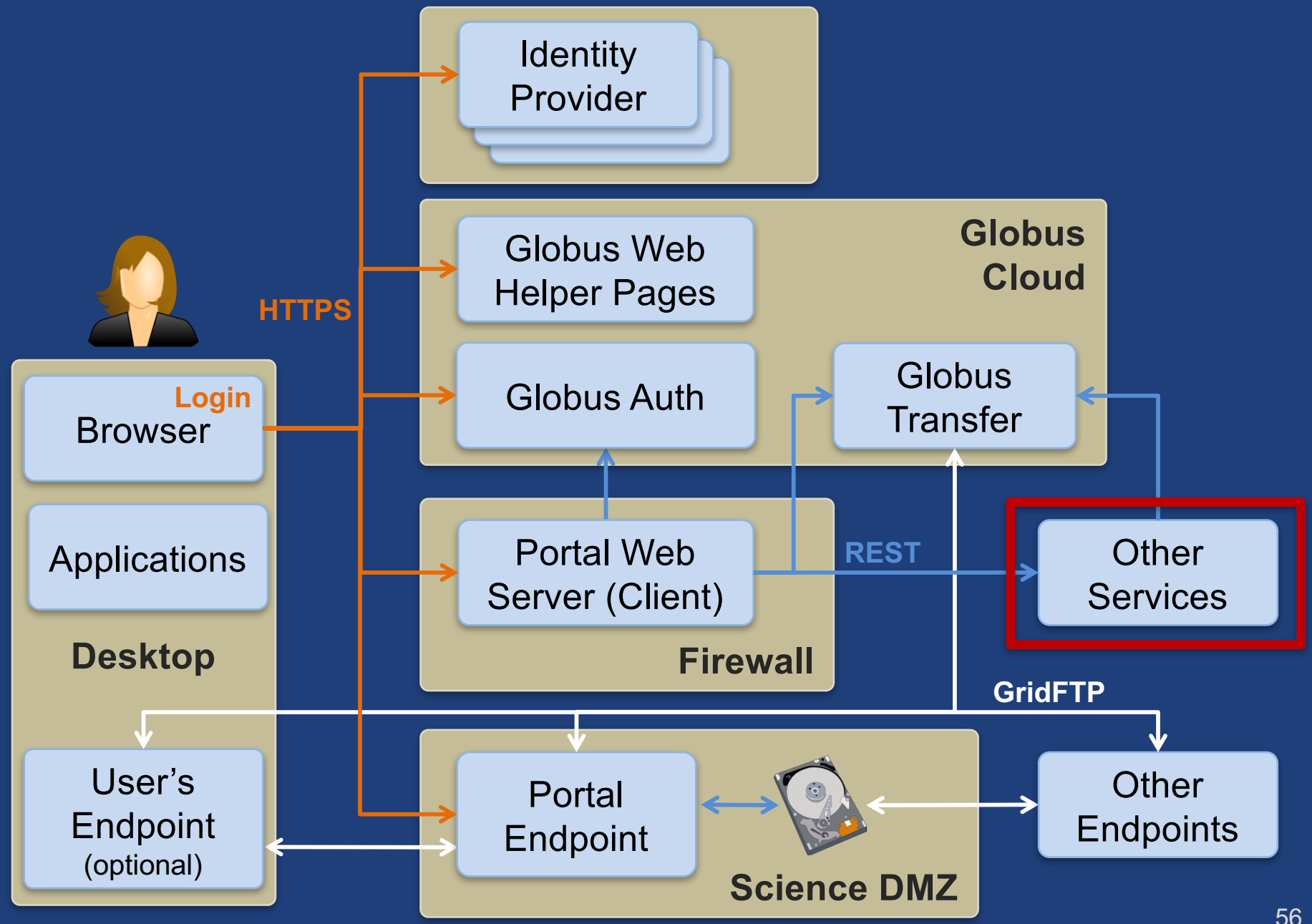
- **Globus Auth "Native App" PKCE support**
- **Use browser if possible**
  - "OAuth 2.0 for Native Apps"
    - draft-ietf-oauth-native-apps-02
    - Use external browser if possible
    - Embed browser in app
    - Embed mini web server in app
- **Allows copy-n-paste of authorization code**
  - A little like app passwords, but OAuth2 compliant
- **Globus Python SDK and CLI support Native App login**
- **Limited support for username/password authentication**
  - Not recommended

Register your app

- **Self-help registration of apps (clients) with Globus Auth**

developers.globus.org

Prototypical research data portal



Why create your own services?

- **Front-end / back-end within your portal**
  - Remote backend for portal
  - Backend for pure Javascript browser apps

- **Extend your portal with a public REST API, so that other app and service developers can integrate with and extend your portal**

Why Globus Auth for your service?

- **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**
  - Its 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

Typical service interactions

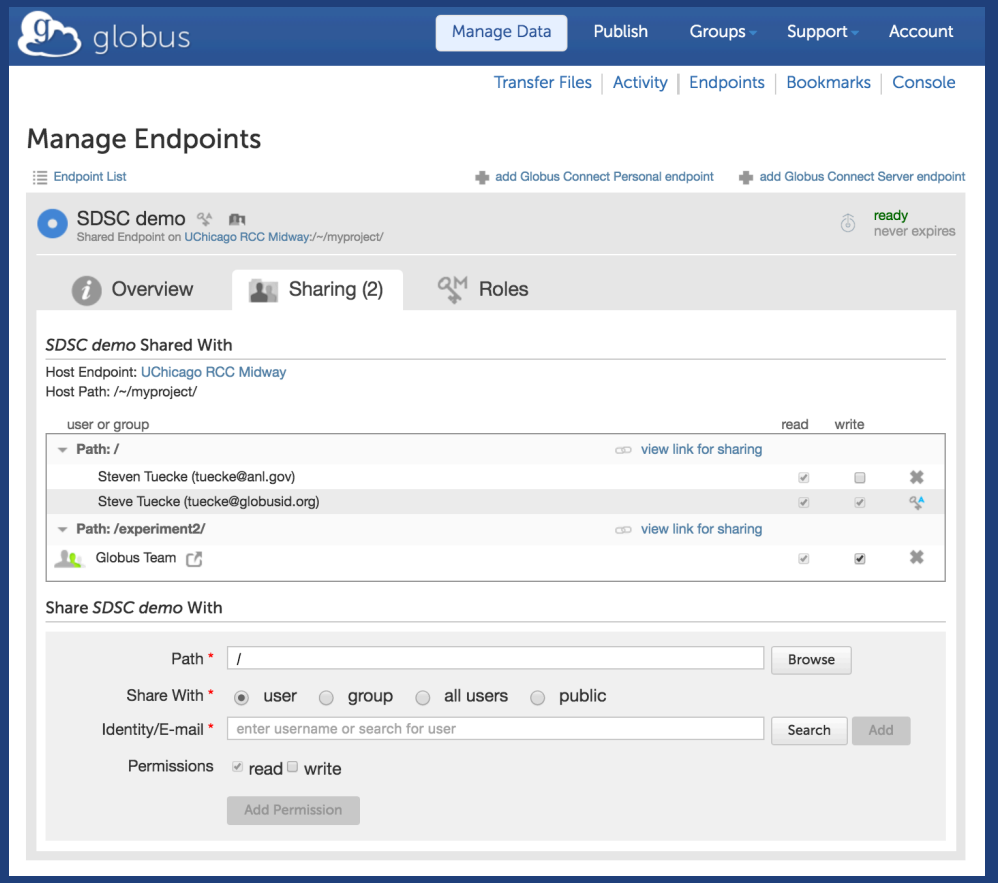
- **Service receives HTTPS request with header**
  - Authorization: Bearer <request-access-token>
- **Introspects the request access token**
  - Auth API: POST /v2/oauth2/token/introspect
  - Authorized by client_id and client_secret
  - Returns: validity, client, scope, effective_identity, identities_set
- **Verifies token info**
- **Authorizes request**
- **If service needs to act as client to other services:**
  - Calls Globus Auth Dependent Token Grant
    - Returns a token for each dependent service
  - Uses correct dependent token for downstream REST call
- **Responds to client HTTPS request as appropriate**

Authorization based on identity set

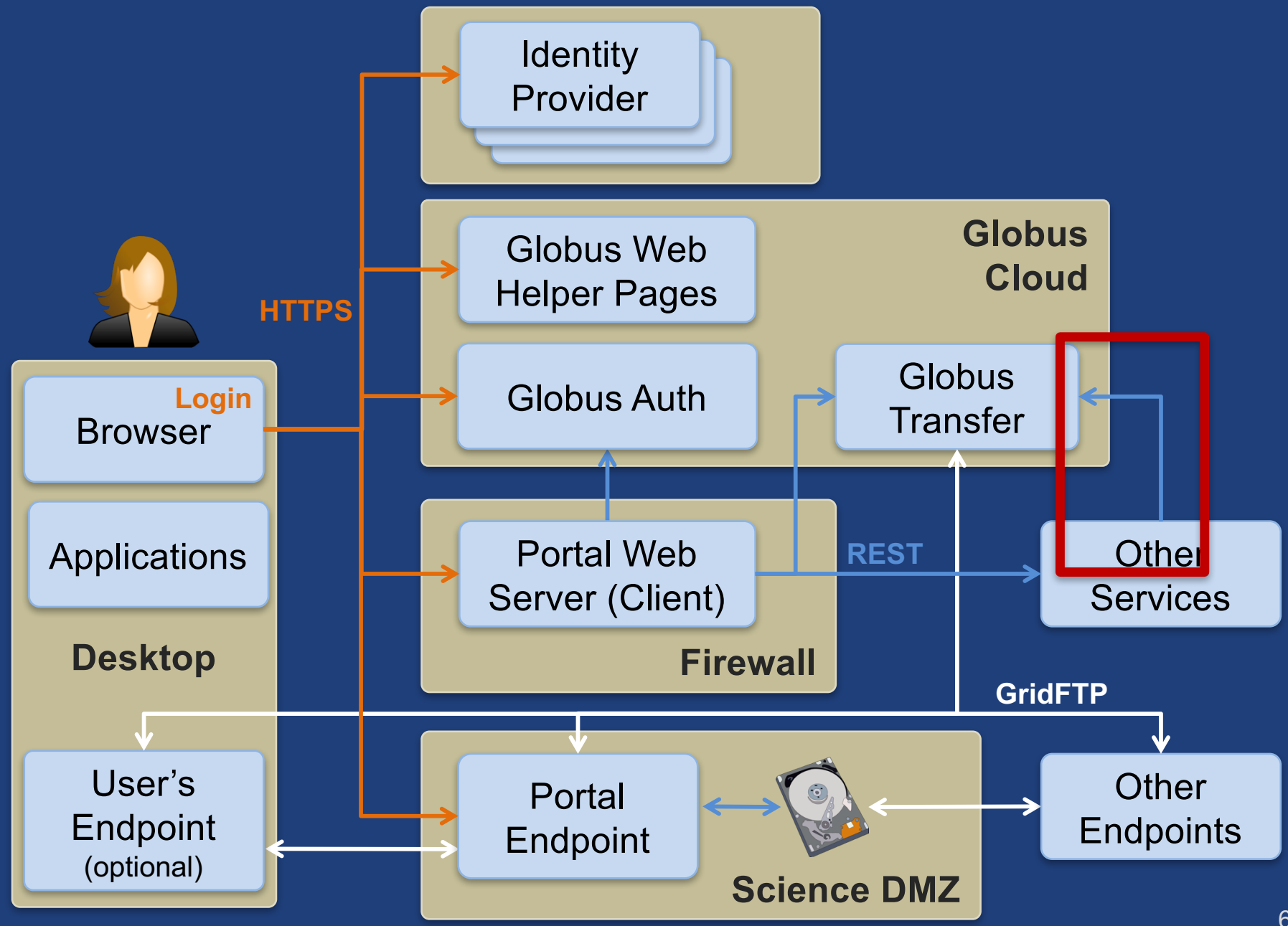
- **Use identities_set when authorizing a request based on the resource owner associated with an access token**
  - E.g., ACLs on Globus shared endpoints
- **Authorizing based on set of identities is same complexity as authorizing based on group membership set**

Groups

- **Globus group service is identity set aware**
  - "Tell me all groups for all identities of the logged in user"
- **Services can leverage this for authorization**



Prototypical research data portal



Dependent tokens

- **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!

Refresh tokens

- **For "offline services"**
  - E.g., Globus transfer service working on your behalf even when you are offline
- **Refresh tokens issued to a particular client for use with a particular scope**
- **Client uses refresh token to get access token**
  - Client_id and client_secret required
- **Refresh token good for 6 months after last use**
- **Consent rescindment revokes resource token**

Globus Platform Summary

- Globus platform makes it easy to:
  - Integrate Globus data transfer and sharing with your apps and services
  - Add (federated) login and REST API security to your apps and services
  - Leverage ScienceDMZ storage

Together we can create an integrated ecosystem of services and applications for the research community

Sample Data Portal

- **Sample Python code demonstrating use of most of the Globus platform**

github.com/globus/globus-sample-data-portal.git

- **Open source**

GlobusWorld Developer Workshops

The globusworld TOUR

Home | Register | Program | Contact Us

Welcome to the GlobusWorld Tour!

We're presenting a series of Globus tutorials and developer workshops across the US, building on the success of the workshop held at GlobusWorld 2016. These workshops are made possible by the various hosting institutions that generously provide meeting space and other financial support.

The following workshops are currently scheduled:

- **September 13-14, 2016 - LBNL, Berkeley, CA**
- **October 12-13, 2016 - Yale University, New Haven, CT**
- **October 25-26, 2016 - NCAR, Boulder, CO**
- **Dates TBD - NIH, Washington D.C.**

If you would like to host a workshop at your institution please contact us.

Motivation: New high-speed networks make it possible, in principle, to transfer

Why Attend?

- Learn how the Globus platform simplifies development of web applications for researchers
- Experiment with new Globus services and APIs
- Exchange ideas with peers on ways to apply Globus technologies
- Expand your knowledge of Globus administration features

Workshops are free to attend and open to all,

https://www.globusworld.org/tour/

Join the Globus developer community

- **Join developer-discuss@globus.org mailing lists: globus.org/mailing-lists**
- **Python SDK is open source**
  - **github.com/globus/globus-sdk-python**
  - Submit issues, pull requests
  - Discussions on **developer-discuss@globus.org**
- **Jupyter notebook, sample data portal and native applications are open source on github**
- **Documentation: docs.globus.org**
- **We're hiring: globus.org/jobs**

Thank you to our sponsors!

U.S. DEPARTMENT OF ENERGY

NSF

THE UNIVERSITY OF CHICAGO

NATIONAL INSTITUTES OF HEALTH

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

ALFRED P. SLOAN FOUNDATION 1934

Argonne NATIONAL LABORATORY

powered by amazon web services