

Globus Auth

Enabling an extensible, integrated ecosystem of services and applications for the research and education community.

Steve Tuecke

The University of Chicago





Cloud has transformed how platforms and software are delivered

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



NETFLIX



Platform as a service: **PaaS**



Microsoft Azure



Infrastructure as a service: **IaaS**



Microsoft Azure



Google Compute Engine

PaaS enables more rapid, cheap, and scalable delivery of powerful apps—as SaaS



Globus and XSEDE

Extreme Science and Engineering
Discovery Environment

- **XSEDE adopted Globus SaaS early**
 - Much usage of Transfer and Sharing

Research data management simplified.



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

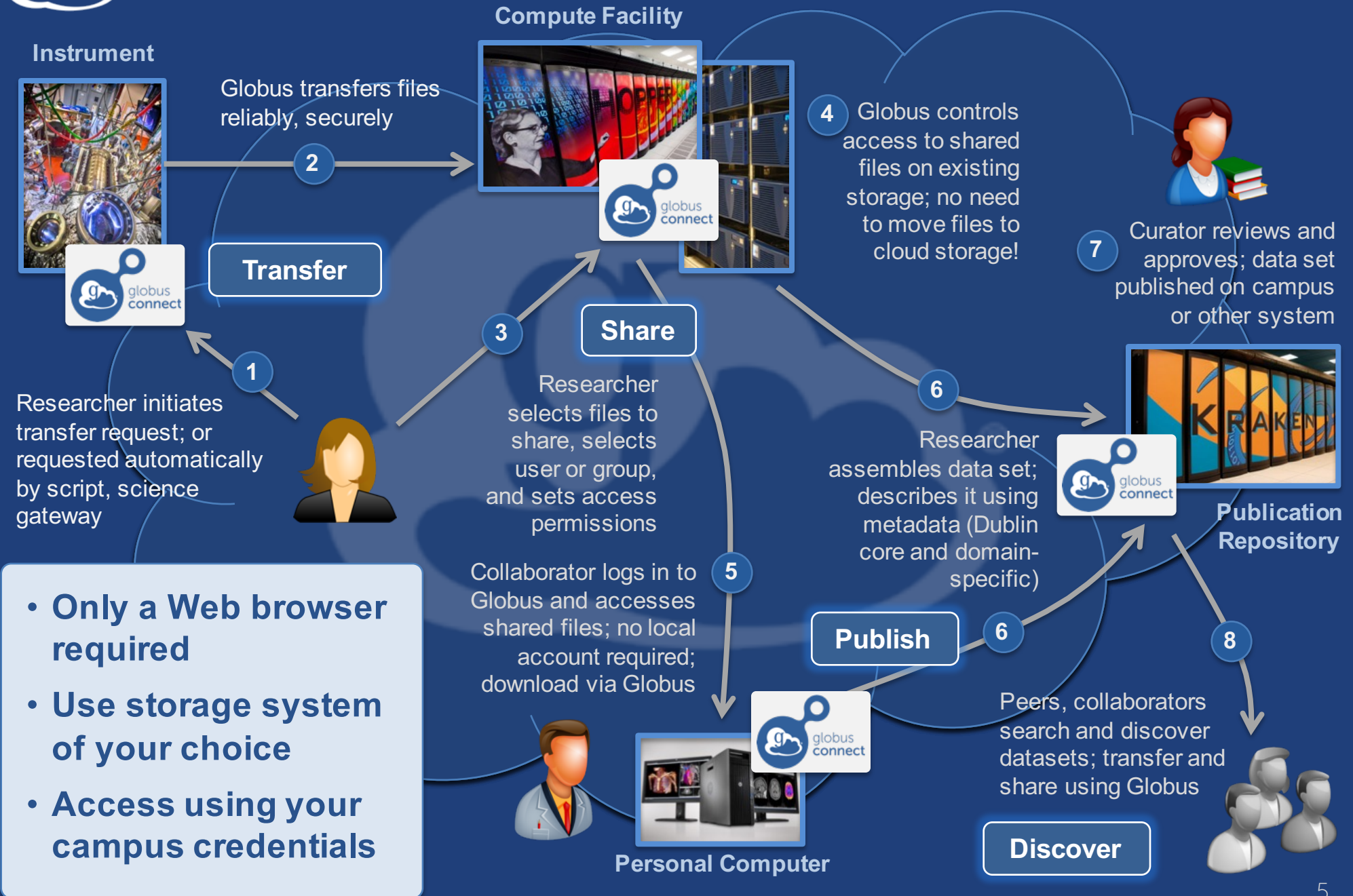
October 16, 2015

 [Webinar: Integrating Globus into the GridChem Gateway](#)

October 16, 2015



Globus SaaS: Research data lifecycle





Globus by the numbers

4

major services

135 PB
transferred

20 billion
files processed

31,000
registered users

13

national labs
use Globus

10,000
active endpoints

~400

active daily users

99.9%
uptime

35+

institutional
subscribers

1 PB

largest single
transfer to date

3 months
longest
continuously
managed transfer

130

federated
campus identities



No Globus usernames required! (coming tomorrow)

- **Globus users no longer require a Globus username & password**
 - Old Globus usernames moved to separate, optional “Globus ID” identity provider
- **Any identity recognized by Globus is now sufficient to access Globus**
- **Globus Account is a primary identity plus a set of linked identities**
 - Verified email address can be a linked identity



Demo

- **Using Globus with any identity**
- **Sharing with any identity**



Globus and XSEDE

Extreme Science and Engineering
Discovery Environment

- **XSEDE adopted Globus SaaS early**
 - Much usage of Transfer and Sharing
- **XSEDE now adopting Globus PaaS as the XSEDE platform**
 - Any science gateway can now integrate trivially with XSEDE services, including Globus transfer



A science CI platform can spur creation of a science CI ecosystem

Software as a service: **SaaS**



(web and mobile apps)

NETFLIX



Platform as a service: **PaaS**



Microsoft Azure



Infrastructure as a service: **IaaS**



EC2



S3



Microsoft Azure



Google Compute Engine

In so doing, we can slash costs, improve quality, and accelerate discovery across the sciences



A science CI platform can spur creation of a science CI ecosystem

Software as a service: SaaS

(web and mobile apps)



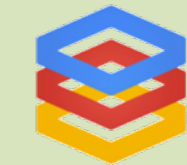
NETFLIX



Platform as a service: PaaS



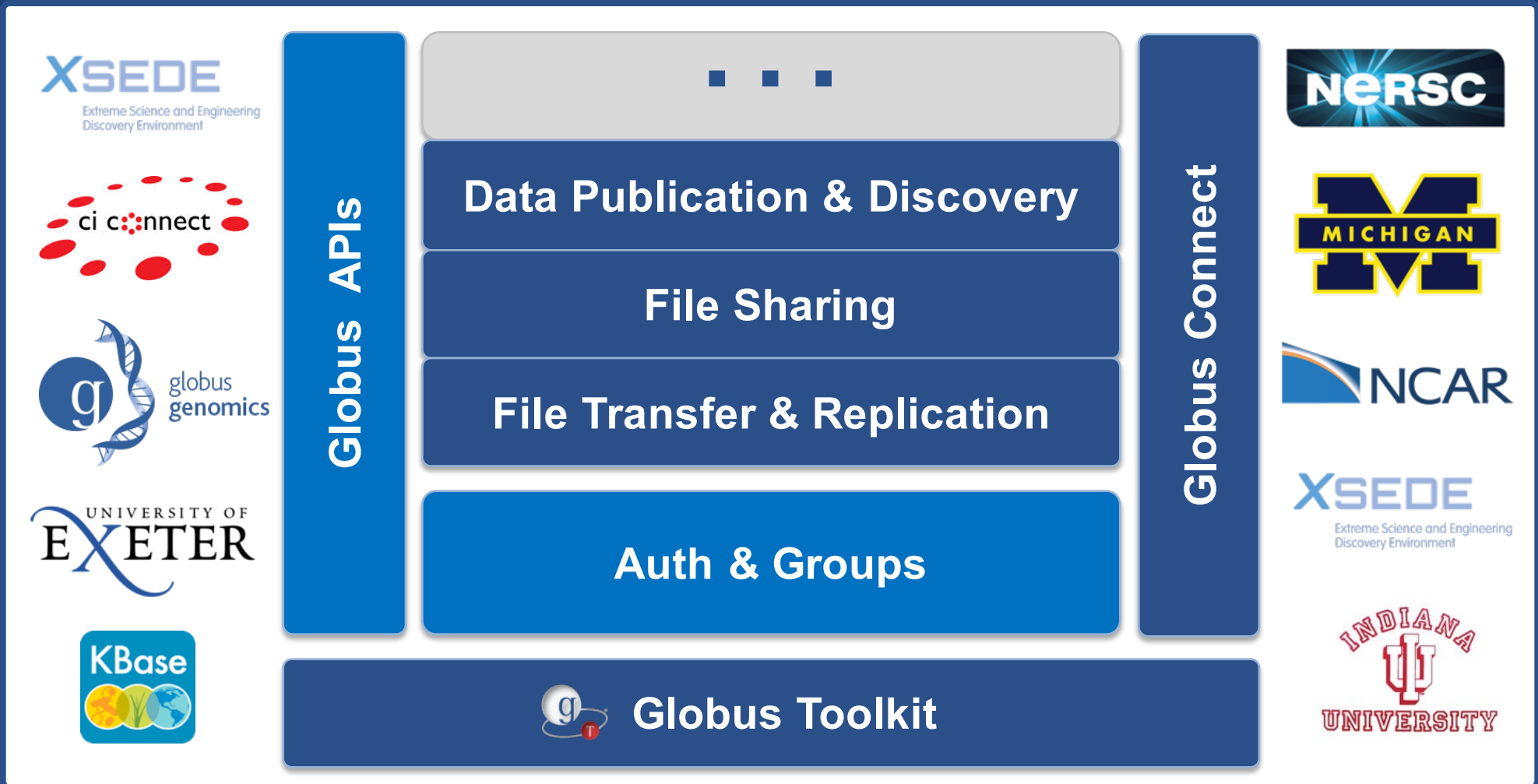
Infrastructure as a service: IaaS



In so doing, we can slash costs, improve quality, and accelerate discovery across the sciences



Globus PaaS: Ecosystem enabler





Globus PaaS at NCAR

- Research Data Archive at NCAR
- Integrate Globus for data downloads
- Shared endpoint with subfolder per request
- Single sign on via streamlined account provisioning

Find Data | Ancillary Services | About/Contact

All Datasets | Recently Added/Updated | Browse the RDA

- GCMD Topic:
 - Agriculture • Atmosphere • Biosphere • Climate
 - Oceans • Paleoclimate • Solid Earth • Spectral/En
- Atmospheric Reanalysis Data:
 - All Reanalysis Datasets • BPRC Arctic System Reanal
 - ECMWF ERA15 Reanalysis (ERA15) • ECMWF ERA40
 - ECMWF Interim Reanalysis (ERA-I) • JMA Japanese 2
 - JMA Japanese 55-year Reanalysis (JRA55) • NCEP Cl
 - NCEP North American Regional Reanalysis (NARR) •
 - NCEP/NCAR Reanalysis Project (NNRP) • NOAA-CIRE
- Station Observations:
 - Land Surface Air Temperature: Hourly, Monthly

Find Platform Observations datasets

CISL Research Data Archive

Managed by NCAR's Data Support Section
Data for Atmospheric and Geosciences Research

RDA





Globus Auth

- **Foundational identity and access management (IAM) platform service**
- **Brokers authentication and authorization interactions between:**
 - end-users
 - identity providers: XSEDE, InCommon, web apps
 - resource servers: services with REST APIs
 - clients: web, mobile, desktop, command line apps
 - resource servers acting as clients to other resource servers

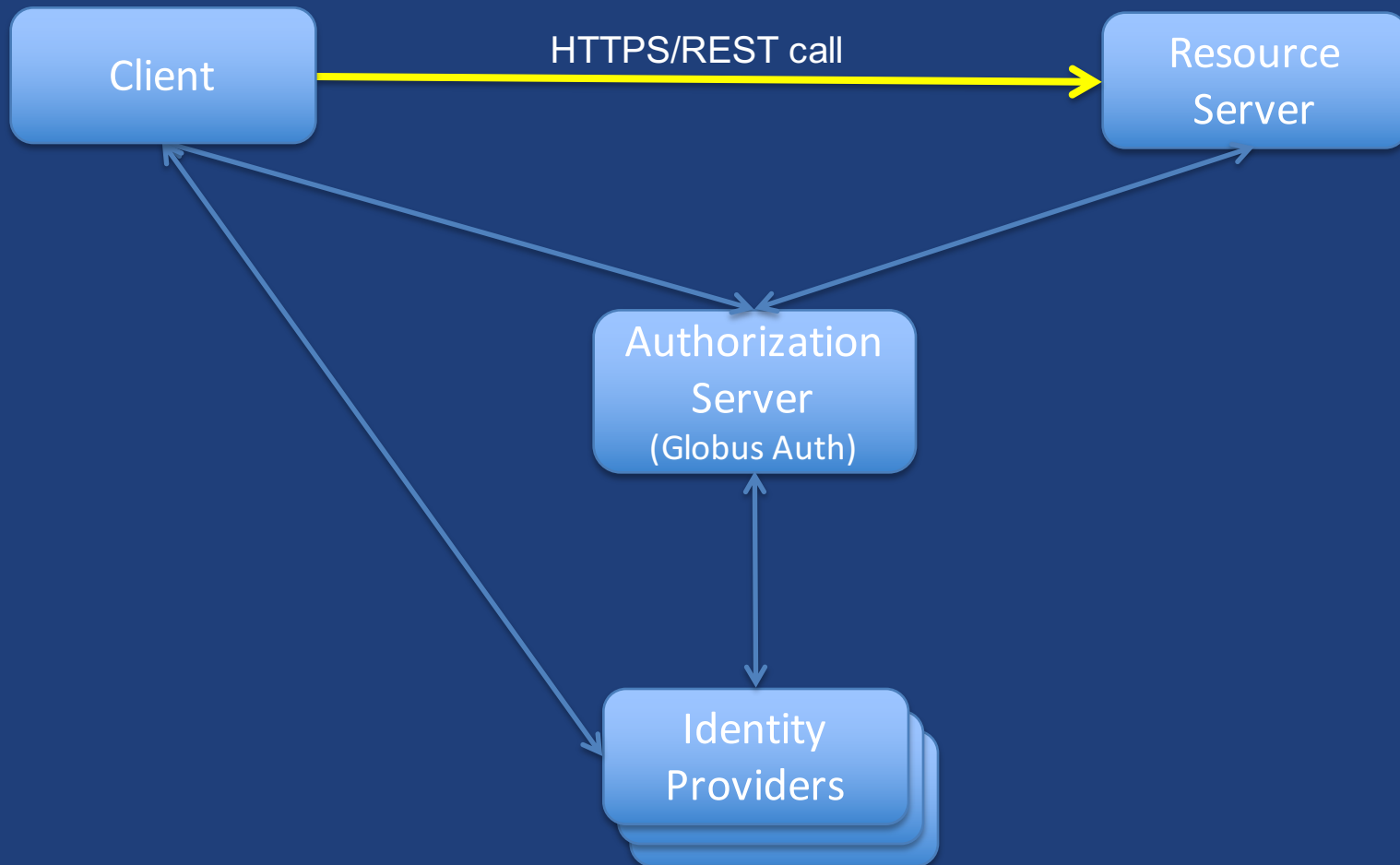


Based on widely used web standards

- **OAuth 2.0 Authorization Framework**
 - aka OAuth2
- **OpenID Connect Core 1.0**
 - aka OIDC
- **Allows use of standard OAuth2 and OIDC libraries**
 - E.g., Google OAuth Client Libraries (Java, Python, etc.), Apache mod_auth_openidc

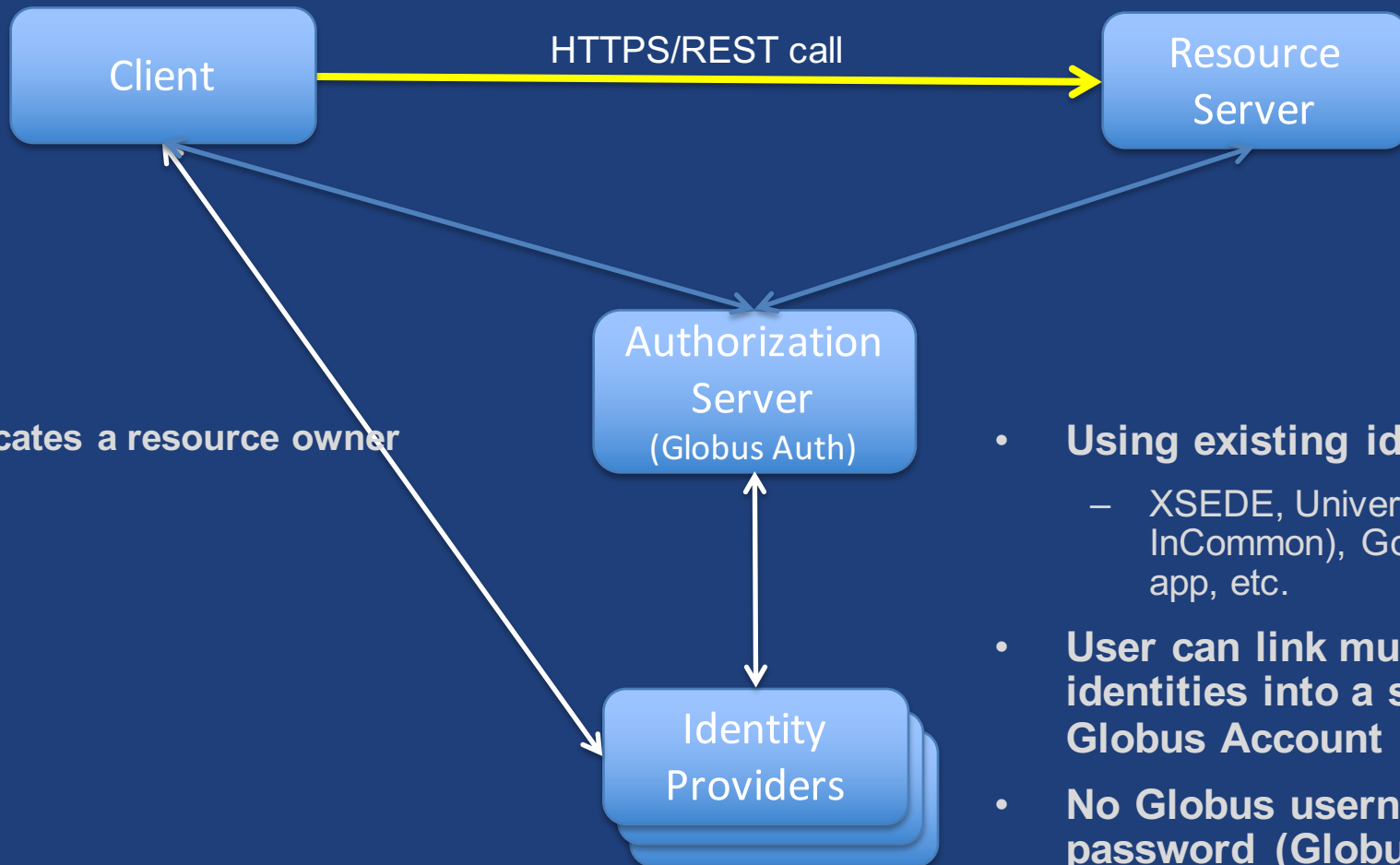


Globus Auth is “authorization server”





Globus Auth is “authorization server”

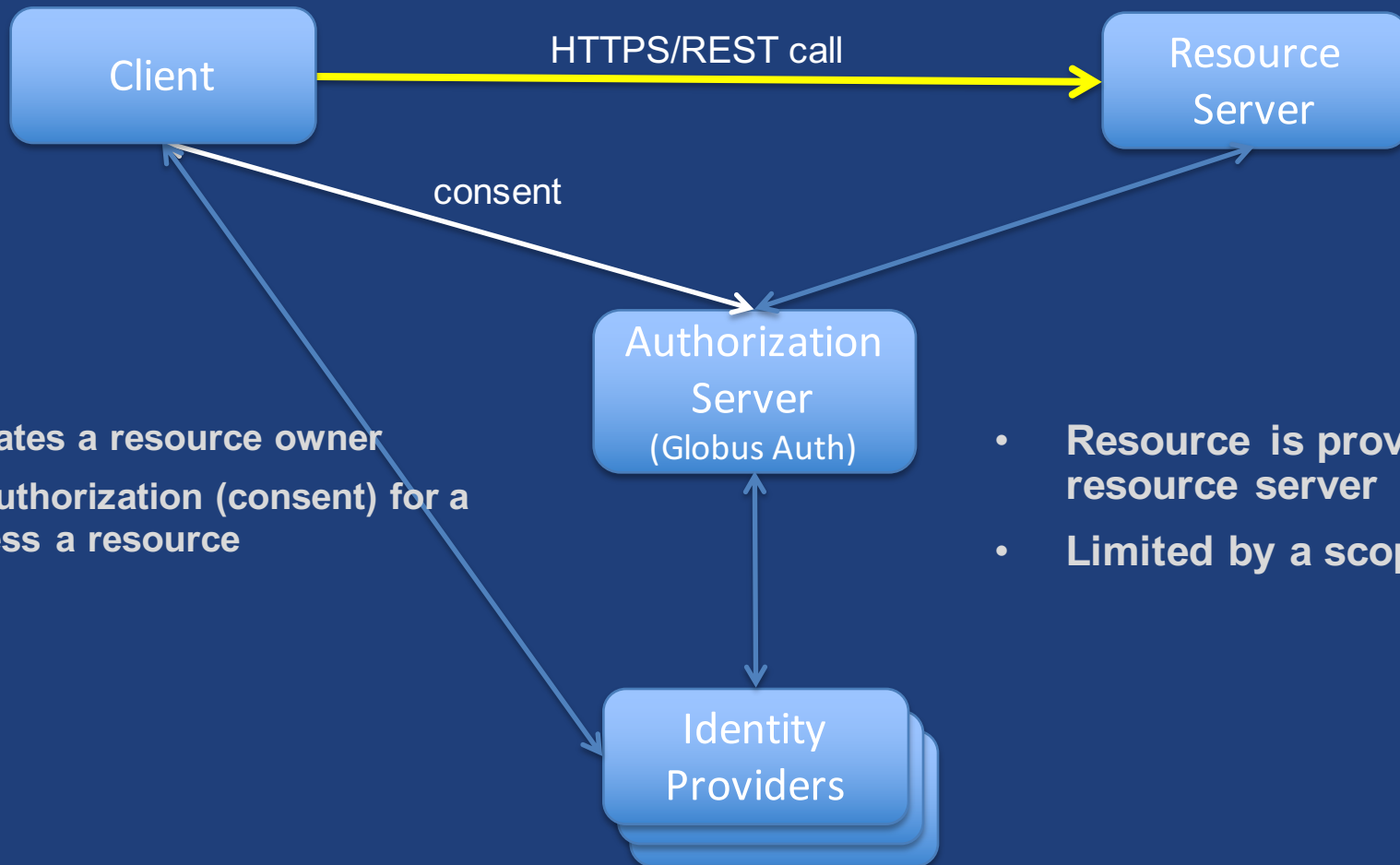


(1) Authenticates a resource owner

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



Globus Auth is “authorization server”

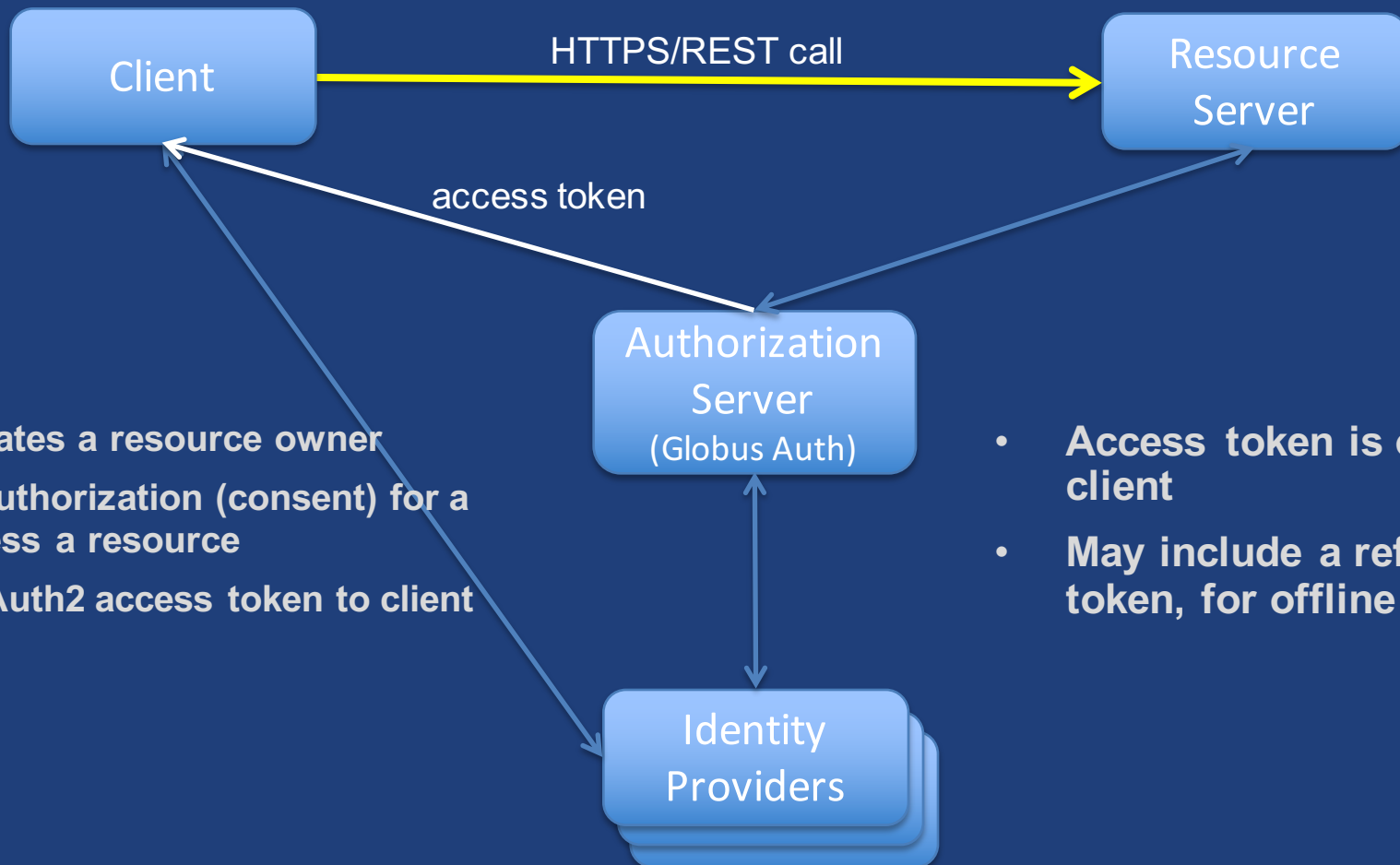


- (1) Authenticates a resource owner
- (2) Obtains authorization (consent) for a client to access a resource

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



Globus Auth is “authorization server”

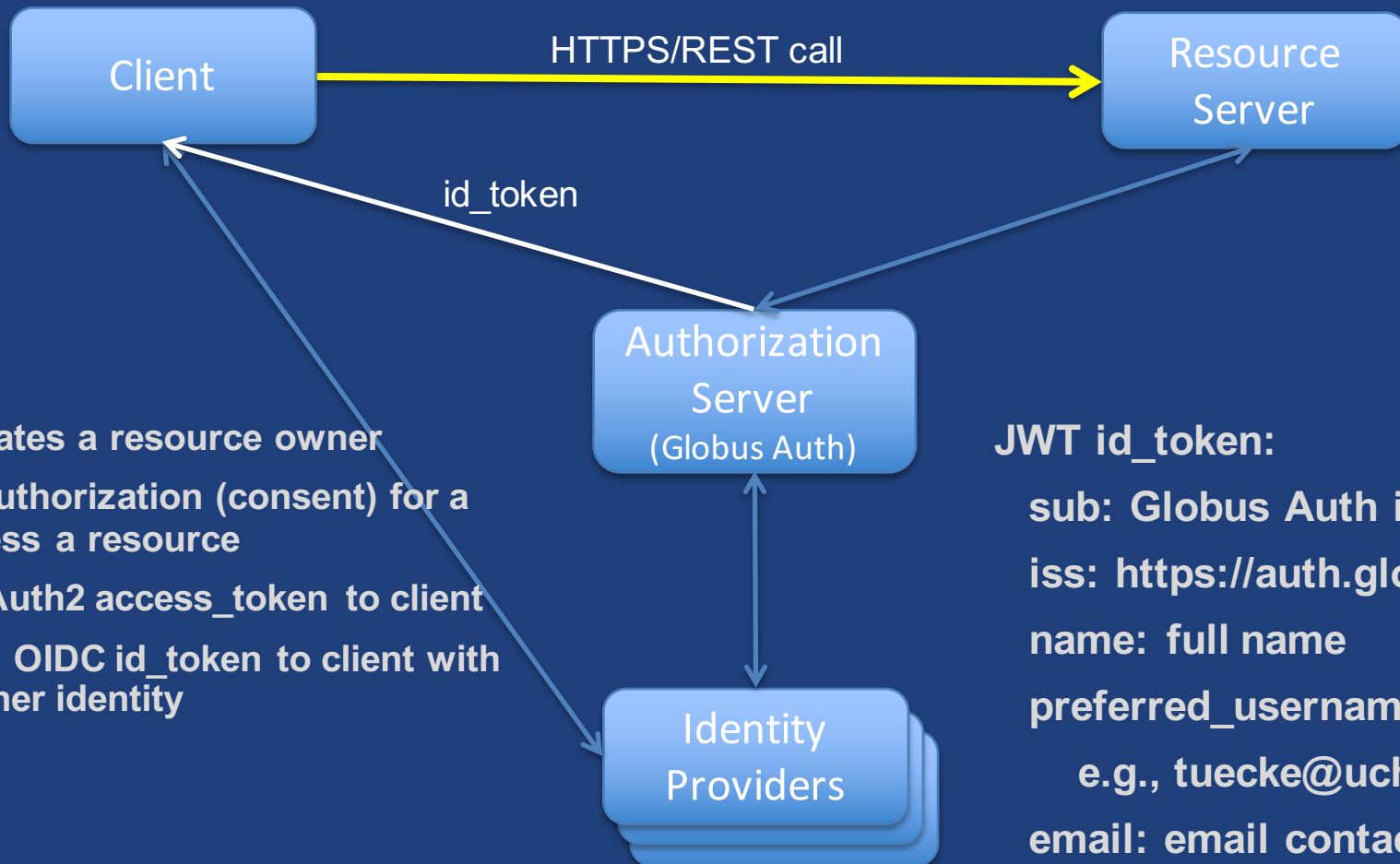


- (1) Authenticates a resource owner
- (2) Obtains authorization (consent) for a client to access a resource
- (3) Issues OAuth2 access token to client

- Access token is opaque to client
- May include a refresh token, for offline access



Globus Auth is “authorization server”



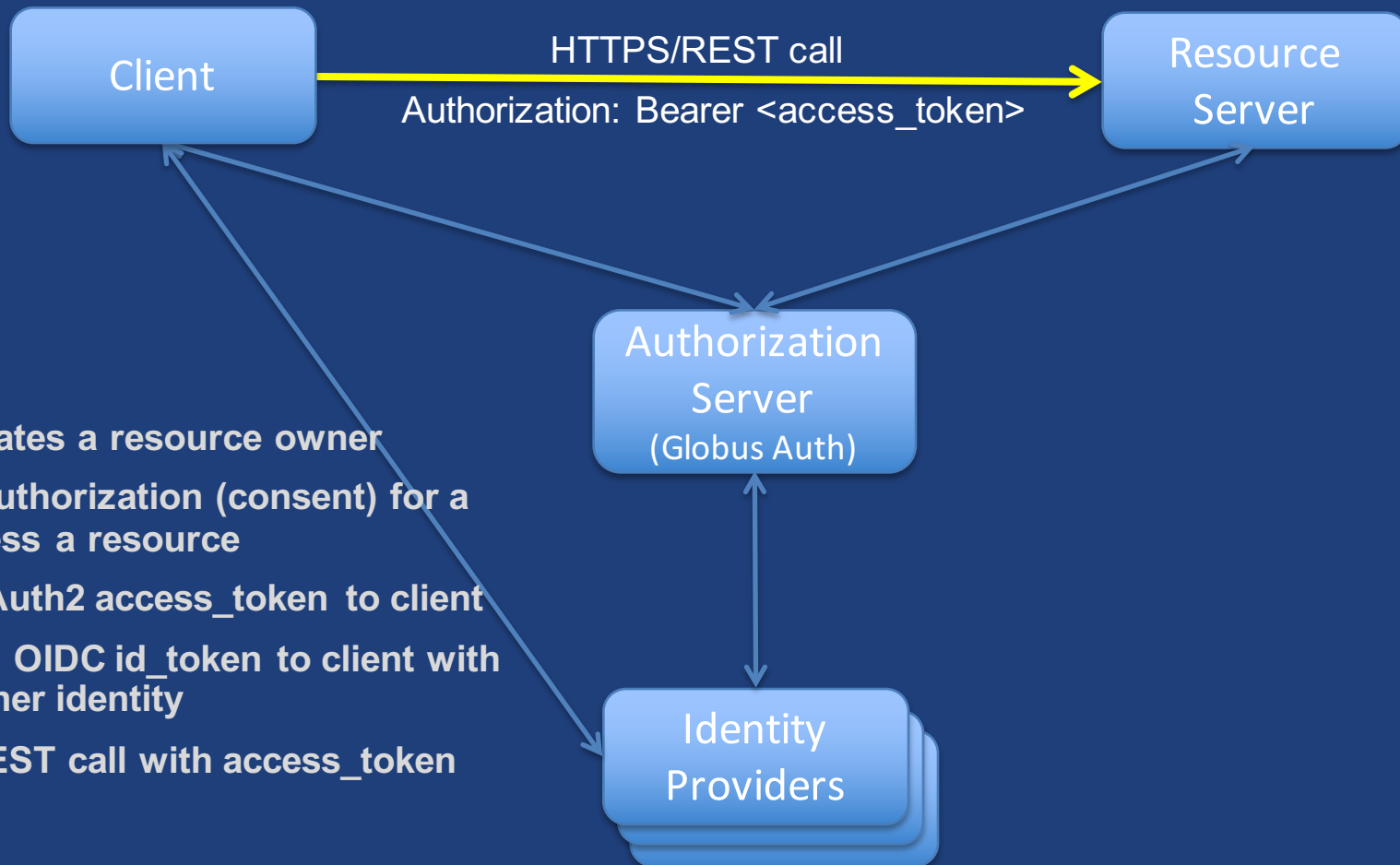
- (1) Authenticates a resource owner
- (2) Obtains authorization (consent) for a client to access a resource
- (3) Issues OAuth2 access_token to client
- (4) May issue OIDC id_token to client with resource owner identity

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



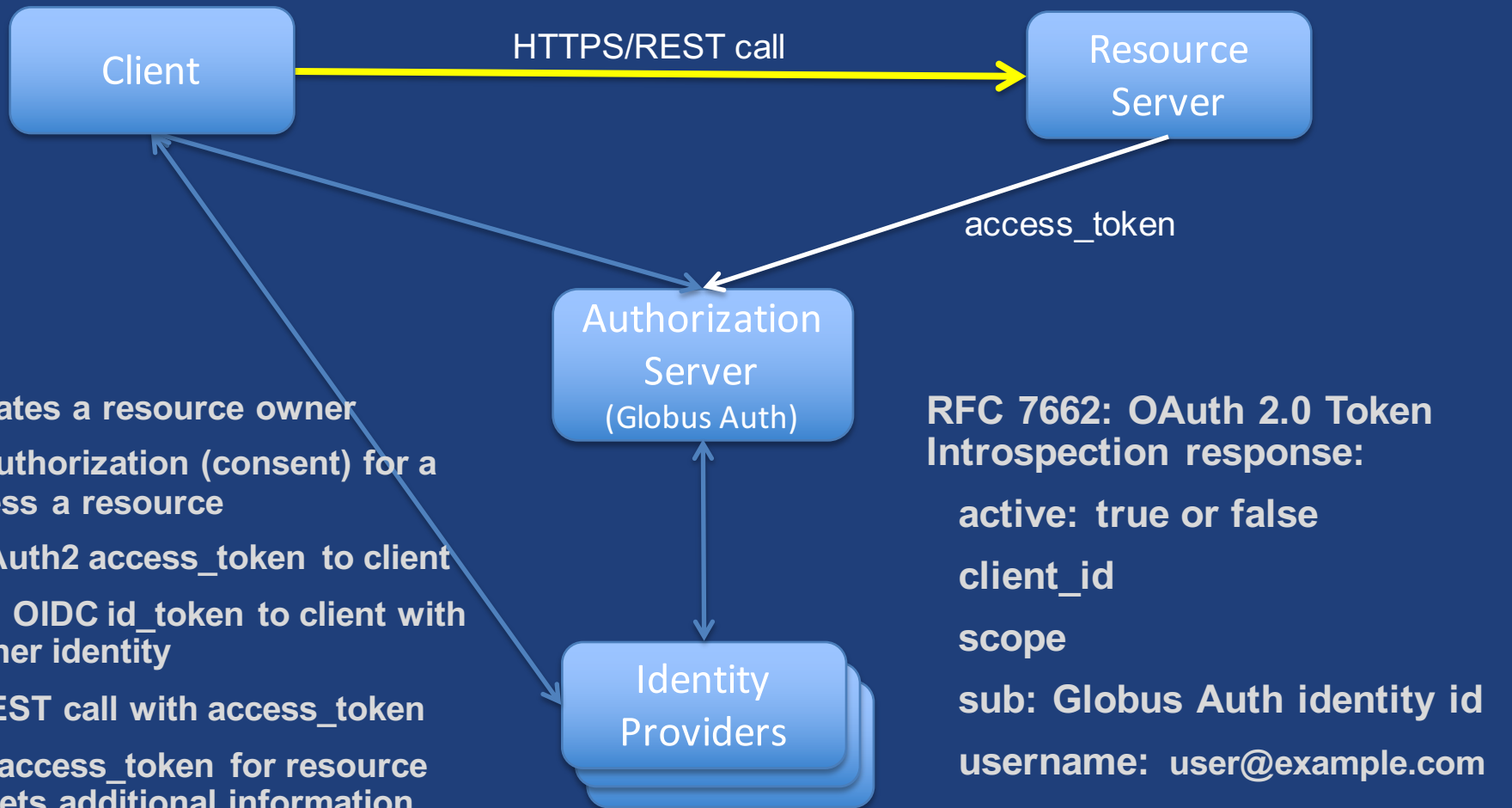
Globus Auth is “authorization server”



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



Globus Auth is “authorization server”



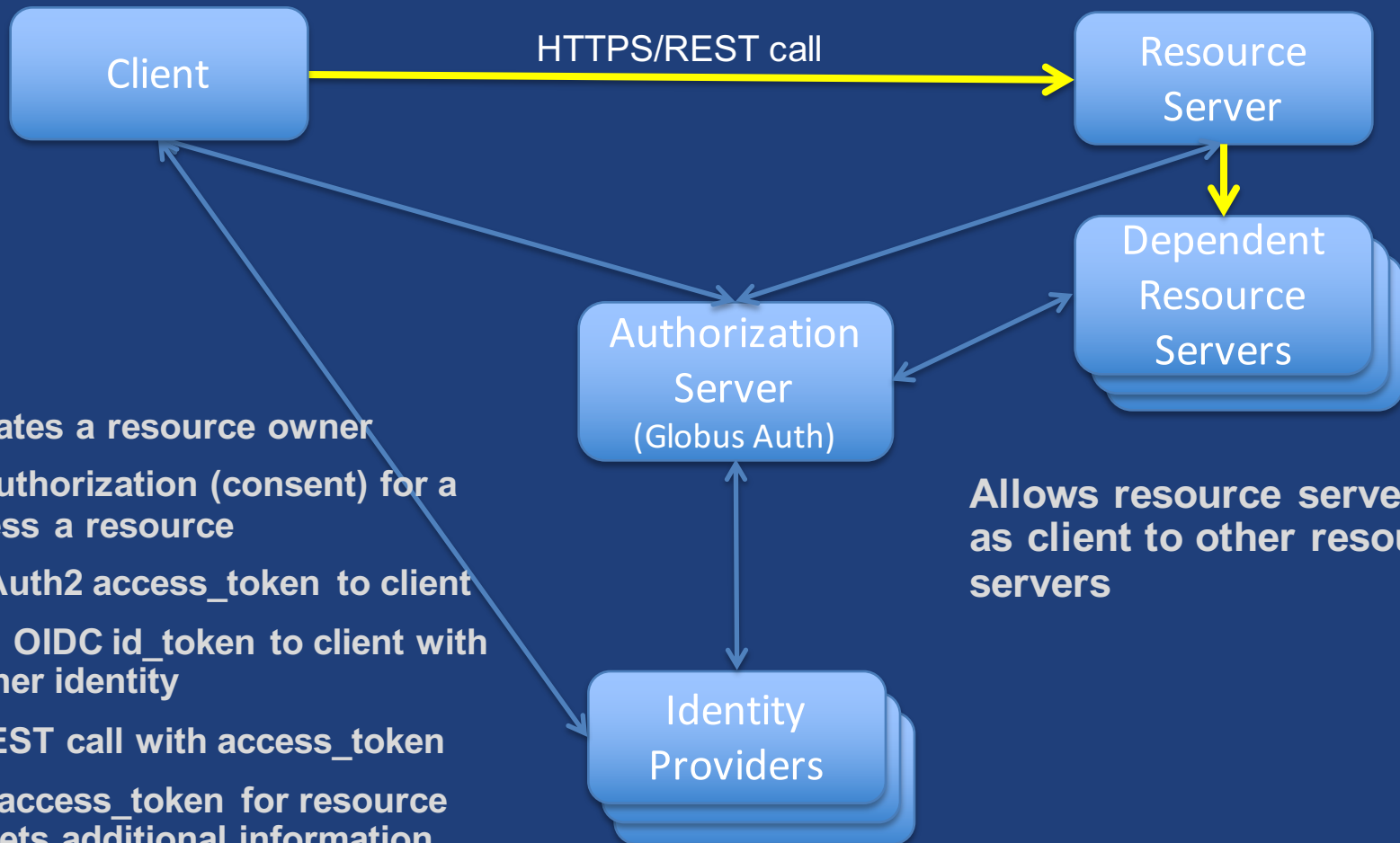
- (1) Authenticates a resource owner
- (2) Obtains authorization (consent) for a client to access a resource
- (3) Issues OAuth2 access_token to client
- (4) May issue OIDC id_token to client with resource owner identity
- (5) HTTPS/REST call with access_token
- (6) Validates access_token for resource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

RFC 7662: OAuth 2.0 Token Introspection response:

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



Globus Auth is “authorization server”



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

Allows resource server to act as client to other resource servers



Simple web app server login



KBBase
PREDICTIVE BIOLOGY

About ▾

Data & Tools ▾

Docs ▾

Help ▾

Sign Up

Sign In

Search our site



Maintenance Window - February 13, 2016 in 2 days

Sat Feb 13 from 10:00am to 3:00pm

KBBase: The Department of Energy Systems Biology Knowledgebase

Analyze your data with KBBase apps

APPS & METHODS



BUILD FLATIL METABOLIC MODEL
v0.1.0



Compare Genomes from
Pangenome
v0.1.0



Insert Genomes into Species Tree
v0.1.0



Propagate Genome-scale Model to
Close Genome
v0.1.0



Reconstruct Community Metabolic
Model

Insert Genomes into Species Tree

Determine evolutionary relationships between organisms by calculating a tree with closely related public genomes in KBBase. [more...](#)

The "Insert Genomes into Species Tree" app allows a user to determine evolutionary relationships on the differences in their genomic sequences. In this app, the user may either upload existing genomes already in KBBase. KBBase will then recruit these genomes into a specified number of phylogenetically close genomes from the KBBase reference genome. The tree object may be exported or viewed in KBBase.

Step 1 - Insert Genome Into Species Tree

Add one or more genomes to the KBBase species tree. [more...](#)

Genome Genome to species tree

KBBase apps are ready-to-use workflows consisting of a set of chained methods that together perform some useful analysis.



New to KBBase?



Search Data

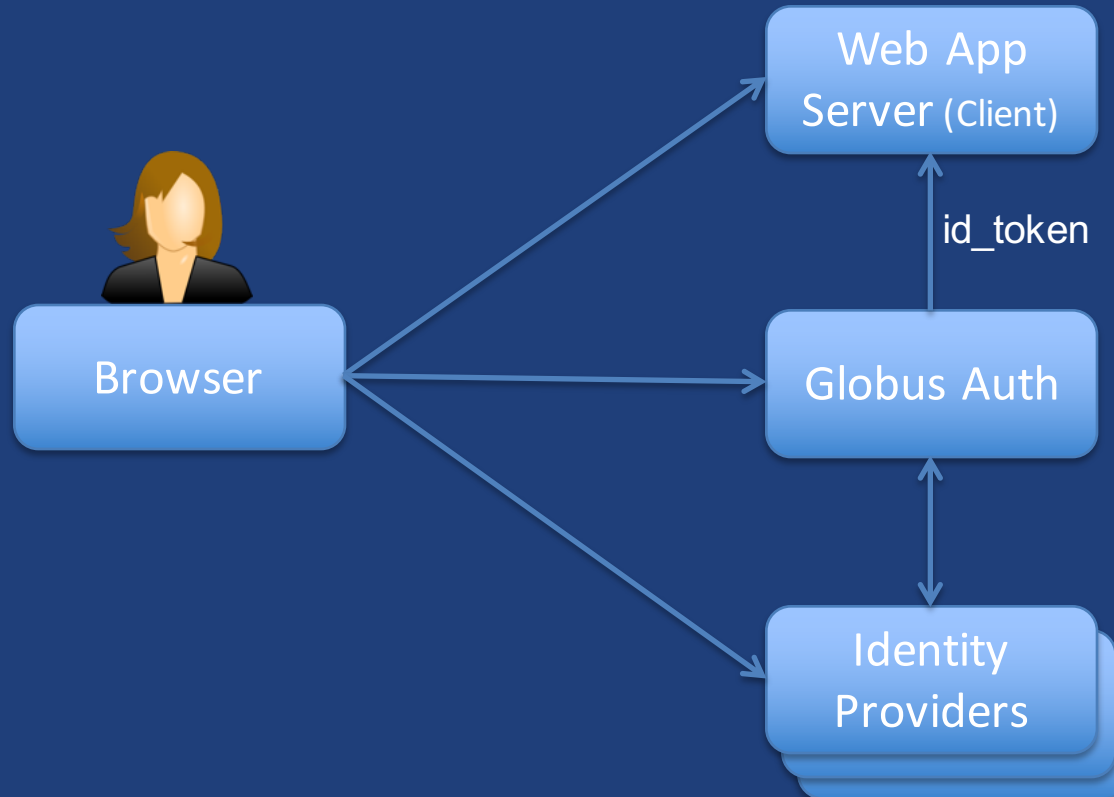


Sign In

KBBase is an open platform for comparative functional genomics and systems biology for microbes, plants and their communities, and for sharing results and methods with other scientists.



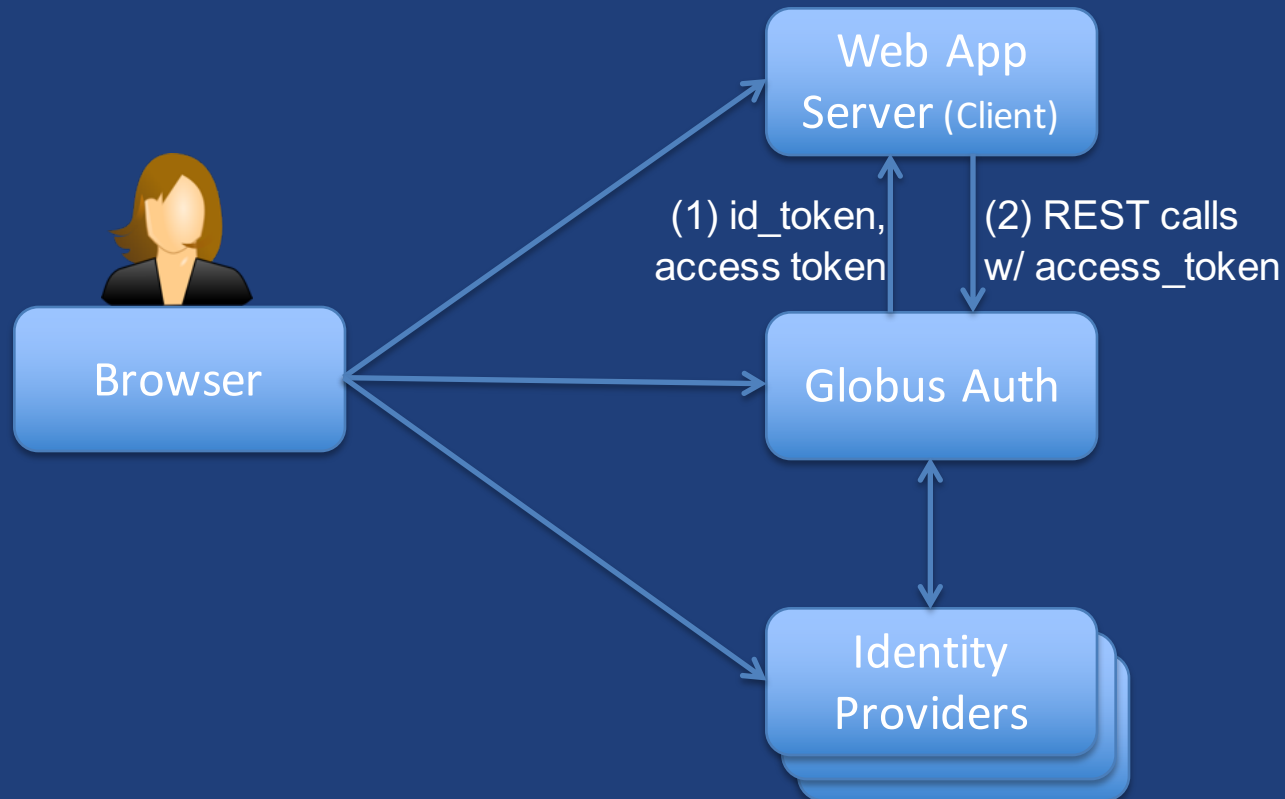
Simple web app server login



- **OAuth2 Authorization Code Grant with Globus Auth**
 - With OIDC scopes: openid email profile
- **User logs into Globus account using their favorite identity provider**
- **Globus Auth returns OIDC id_token to the web server**
 - With identity sub (unique id), name, preferred_username, email
- **Client policy can require identity from a particular identity provider**



Login + Globus Auth REST API



- **OAuth2 Authorization Code Grant with Globus Auth**
 - With OIDC scopes: openid email profile
 - And scope: [urn:globus:auth:scope:auth.globus.org:view_identities](#)
- **Globus Auth returns OAuth2 access token to Web App Server (OAuth2 client) for use with Globus Auth REST API**
- **Web App Server calls Globus Auth REST API with access token**
 - Authorization: Bearer <access_token>
 - Get identity information, including full set of linked identities



Browser-based web app login



[Manage Data](#) ▾

[Publish](#)

[Groups](#) ▾

[Support](#) ▾

[Account](#)

Account

[Manage Your Consents](#)

[Logout](#)

Identities

[Manage These Identities](#)

[Add Linked Identity](#)

Steven Tuecke via University of Chicago

Name: Steven Tuecke

Username: [tuecke@uchicago.edu](#)

E-mail: tuecke@uchicago.edu

This is your **primary** identity.

services@tuecke.com via Email Address

Username: [services@tuecke.com](#)

E-mail: services@tuecke.com

This is a **linked** identity.

Steve Tuecke via Globus ID

Name: Steve Tuecke

Username: [tuecke@globusid.org](#)

E-mail: tuecke@uchicago.edu

Organization: University of Chicago

This is a **linked** identity.

Globus Plus

Globus Plus gives you [enhanced features](#) on your Globus Connect Personal endpoints.

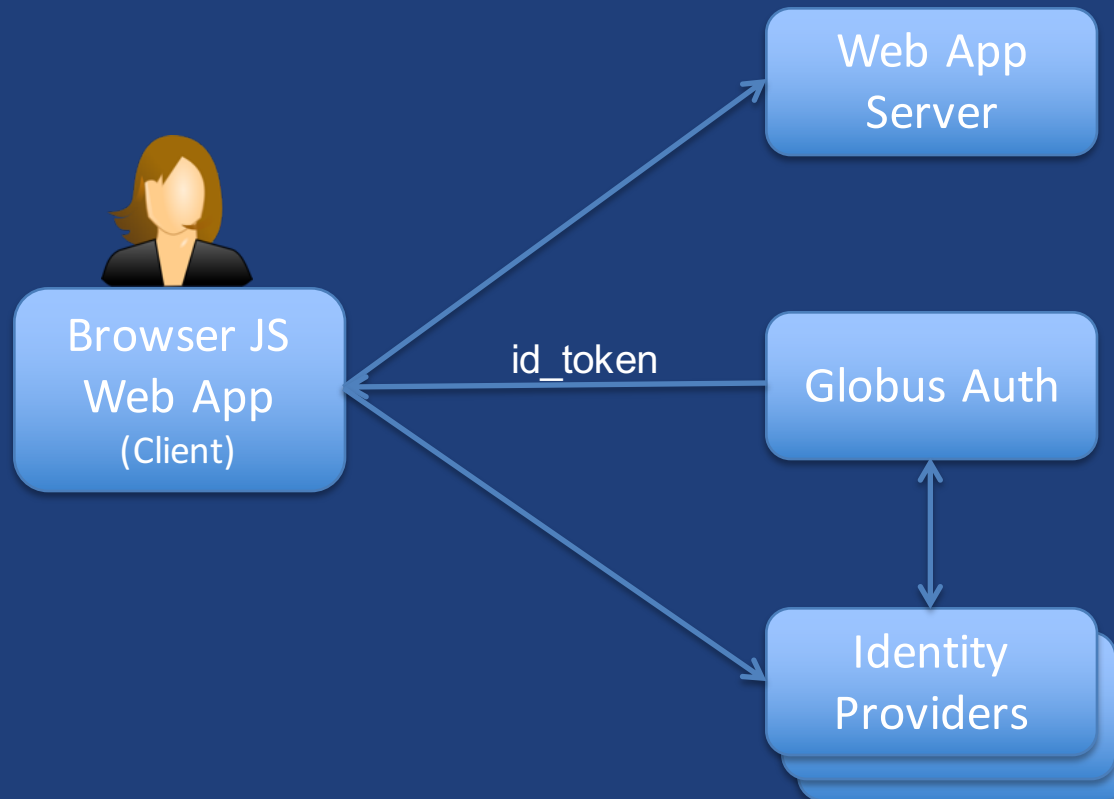
You have Globus Plus, because you are a member of the following groups:

[Globus Team Plus Sponsor](#)

[Tutorial Users](#)



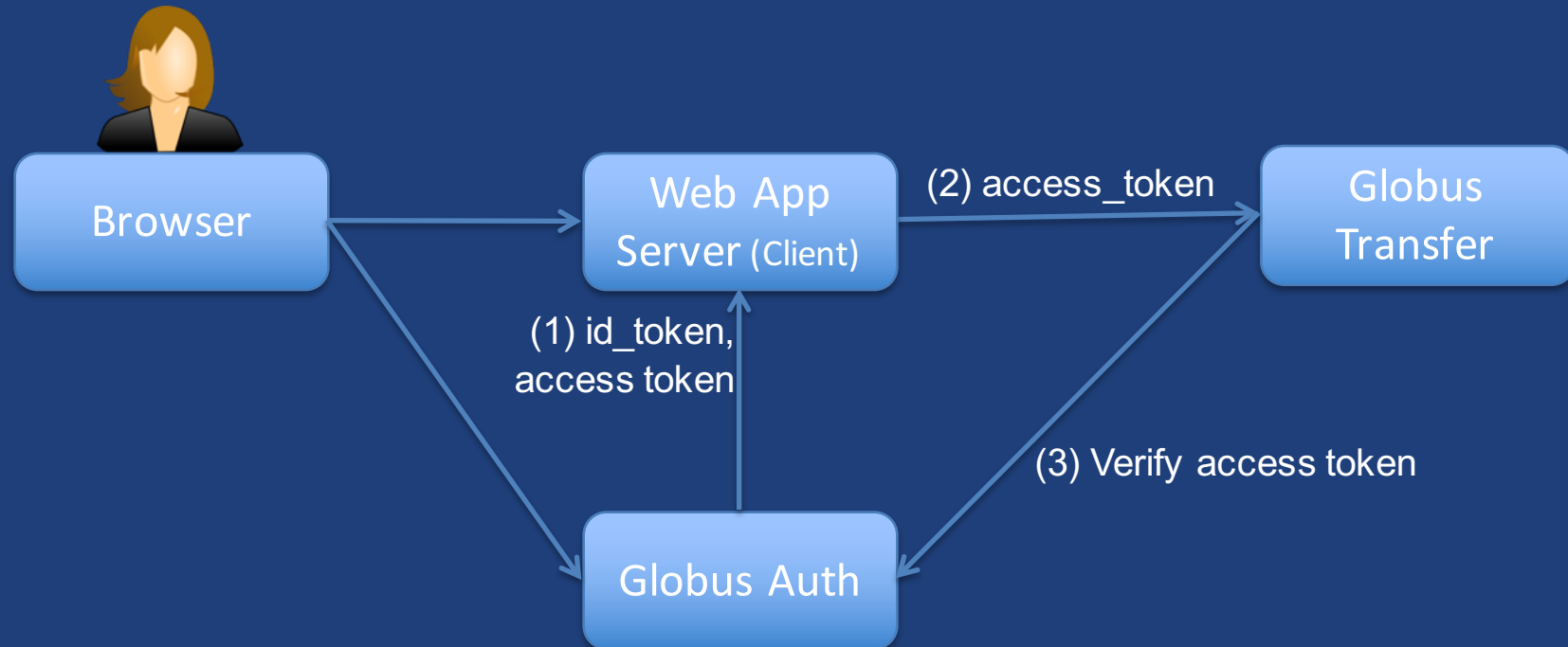
Browser-based web app login



- **OAuth2 Implicit Grant**
 - With OIDC scopes: openid email profile
- **Globus Auth returns OIDC id_token to the browser-based Javascript client**
 - With identity sub (unique id), name, preferred_username, email
 - Client policy can require identity from a particular identity provider



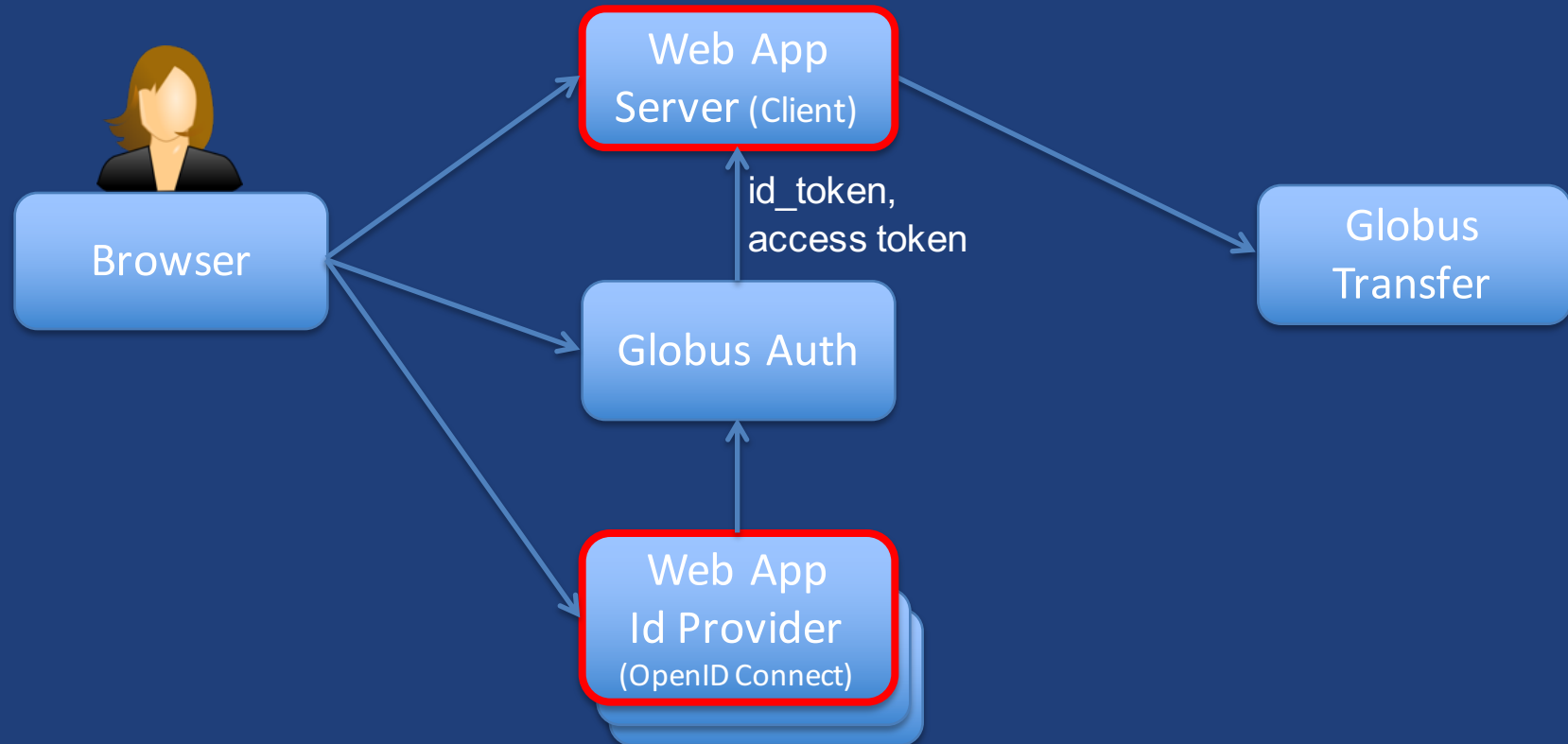
Globus transfer integration



- **OAuth2 Authorization Code Grant with Globus Auth**
 - Scopes: openid email profile [urn:globus:auth:scope:transfer.api.globus.org:all](https://globus.org/docs/transfer-api/authorization-scopes)
- **Globus Auth returns OAuth2 access token to Web App Server (OAuth2 client) for use with Globus Transfer REST API**
- **Web App Server (OAuth2 client) calls Globus Transfer REST API**
 - Authorization: Bearer <access_token>



Using existing web app identities



- **Web App Server does OAuth2 Authorization Code Grant with Globus Auth**
 - Scopes: openid email profile urn:globus:auth:scope:transfer.api.globus.org:all
- **Globus Auth does OIDC login with Web App Identity Provider**
- **Results in Web App Server having:**
 - User login information from own Web App Id Provider
 - Access token(s) that it can use with REST APIs for Globus Transfer, XSEDE, etc.
- **SSO to your web app and Globus using only your web app identities!**



Research data portal

UCAR NCAR

Closures/Emergencies

Locations/Directions

Find People

Hello tuecke@uchicago.edu [dashboard](#) [sign out](#)

NCAR
UCAR



Research Data Archive
Computational & Information Systems Lab

weather • data • climate

Go to Dataset:

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

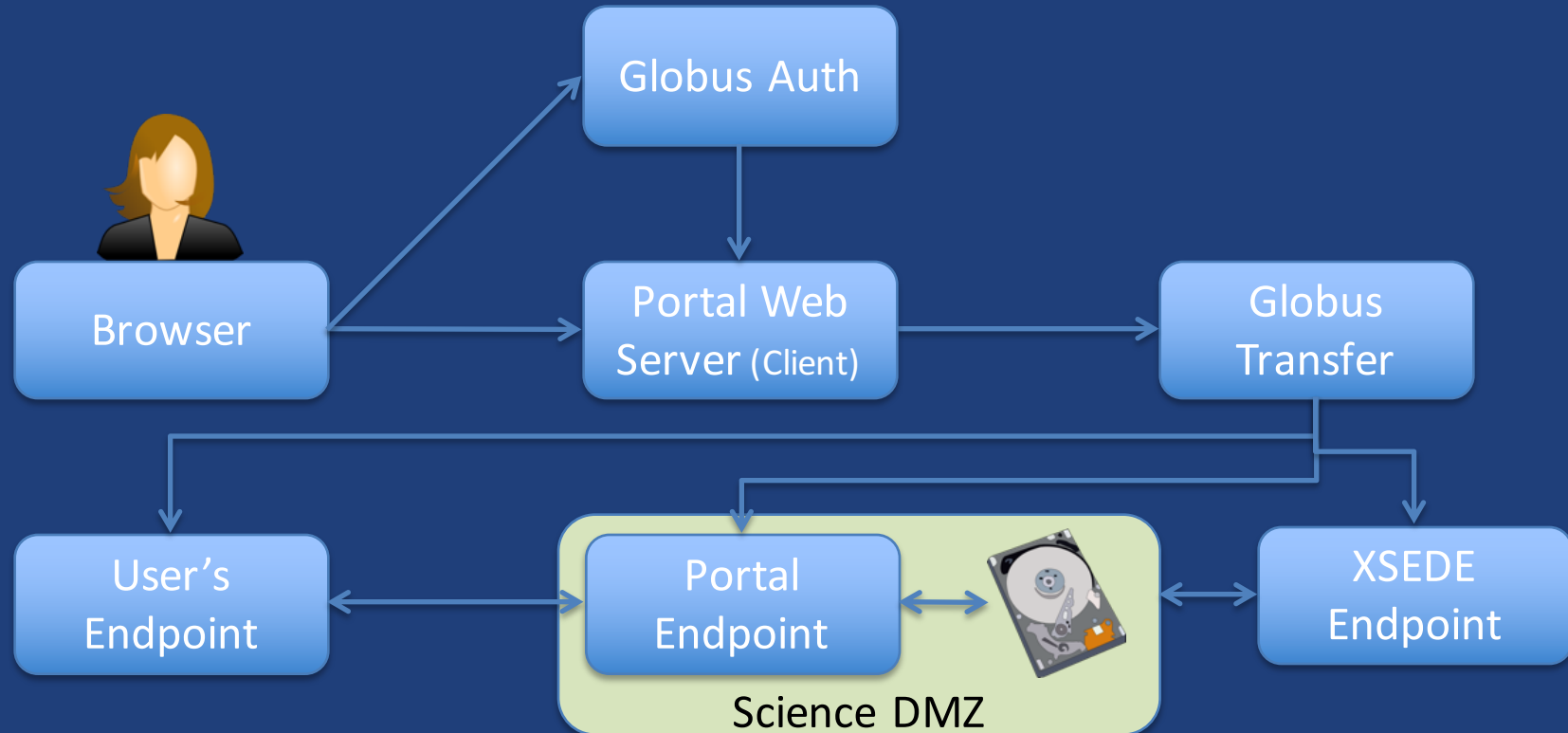
Data Access

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
P R O D U C	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



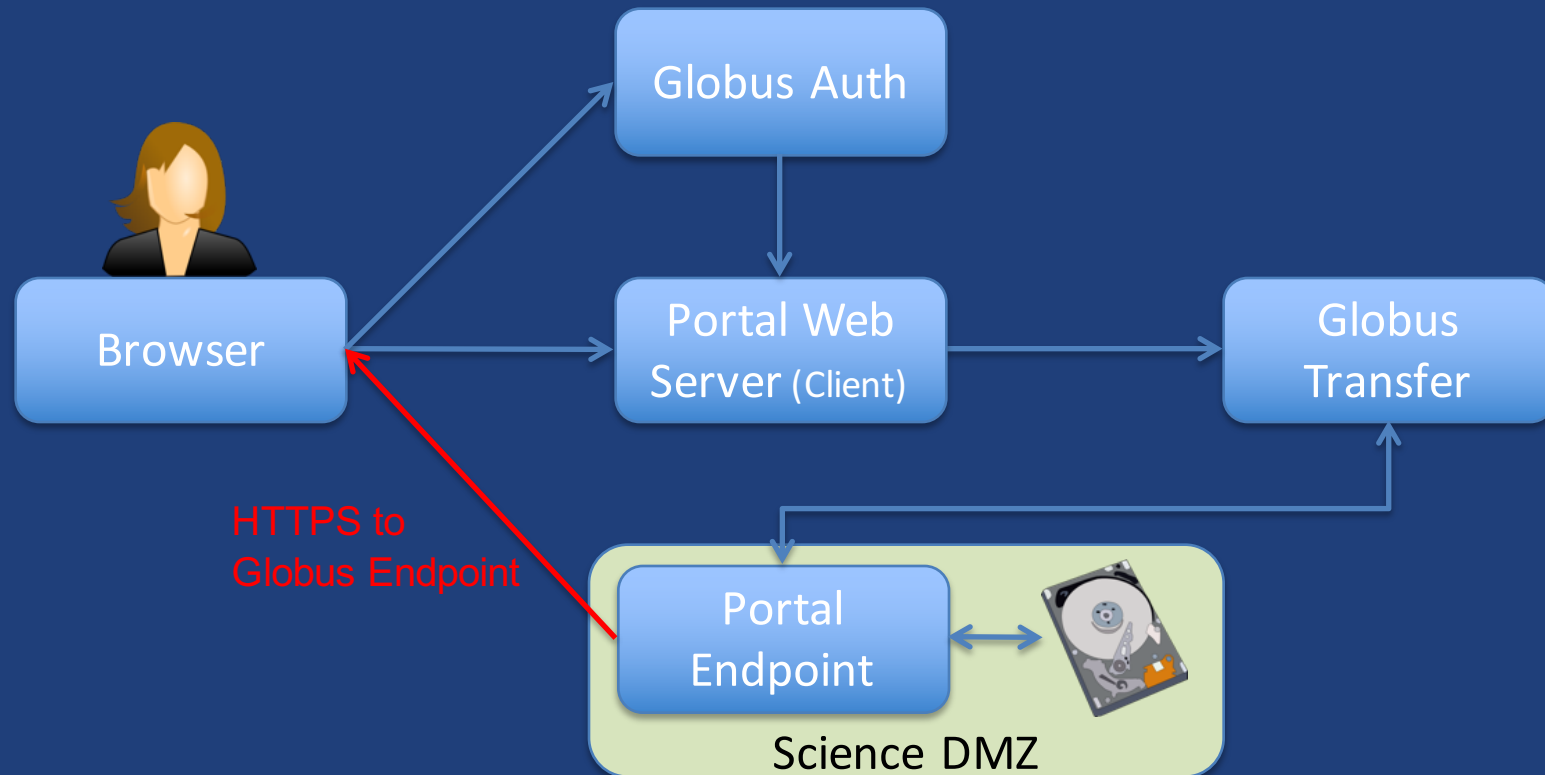
Research data portal



- **Move portal storage into Science DMZ, with Globus endpoint**
 - High performance, managed storage
- **Leave Portal Web server behind firewall**
- **Globus handles the data heavy lifting**



HTTPS to endpoints (coming soon)



- **Globus Connect Server will soon allow HTTPS access to endpoint storage**
- **Your web application can directly link to files on the Portal Endpoint**
- **Globus Auth and Transfer mediated security**
 - Restrict HTTPS access to files by particular users and groups



Globus Web App Integration



Manage Data ▾

Publish

Groups

Support ▾

tuecke ▾

Browse & Discover

Data Publication Dashboard

Communities & Collections

...knowledge and accept
that datasets you submit to this trial collection: (1)
will be

Input Form*

Datcite Mandatory + R ▾

Submission
Workflow*

Default ▾

Curation Type*

Edit Metadata ▾

Collection Permissions

Submitters

- All Users
- Restricted to Group...

Access to Data

- All Users
- Restricted to Group...

Curation Group

null

Change...



Manage Data ▾ Publish Groups Support ▾ tuecke ▾

Select Group

Find a group.

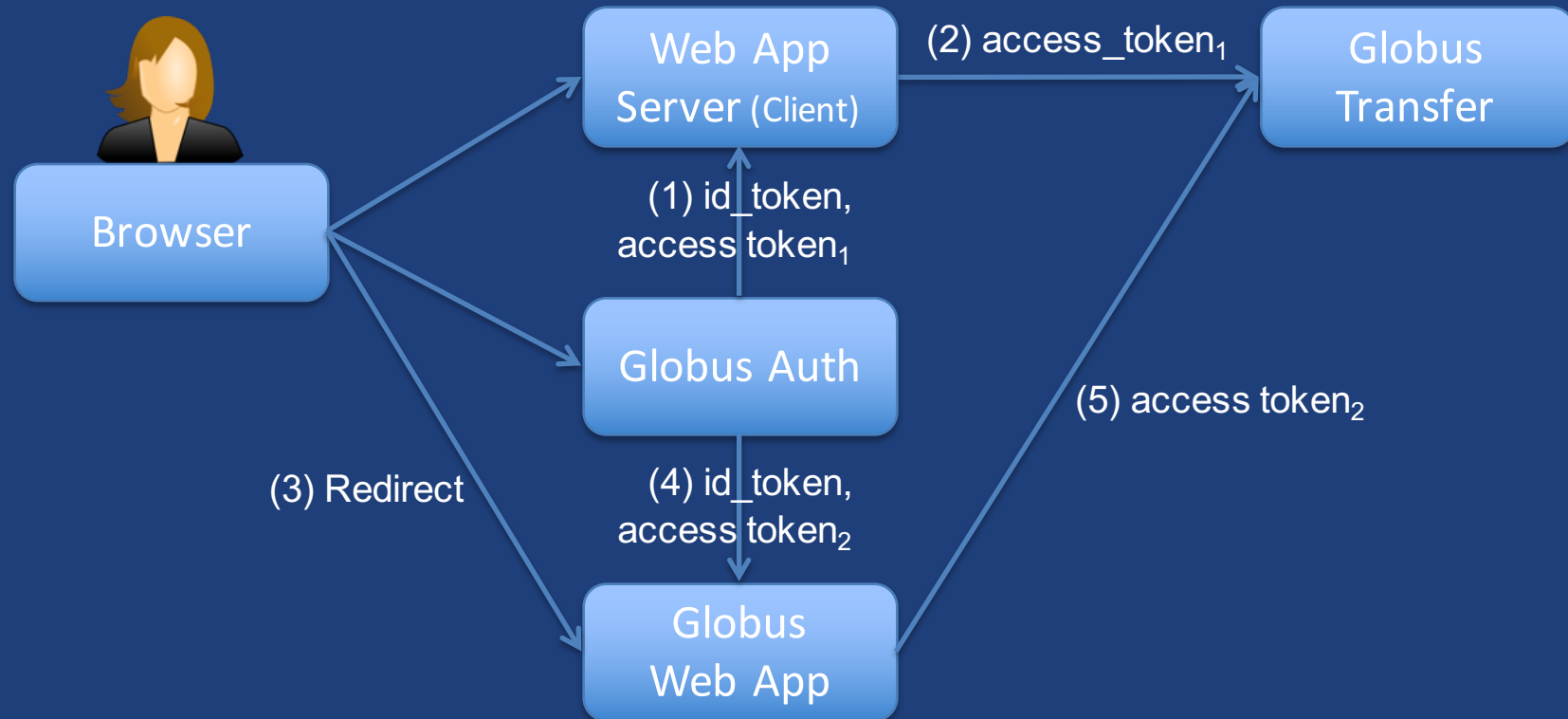
Globus Team

- Globus Team Prod Test ▾ details
- Globus Team - Development ▾ details
- Globus Team - User Services ▾ details
- Globus Team Plus Sponsor ▾ details
- Globus Team ▾ details
- Cir-Lab Globus Publication Users ▾ details
- go#s3 access ▾ details
- Wellcome Trust Sanger Institute Scientific Users ▾ details

Submit



Globus Web App integration



- **OAuth2 Authorization Code Grant with Globus Auth**
 - Scopes: openid email profile urn:globus:auth:scope:transfer.api.globus.org:all
 - Globus Auth returns OIDC id_token & OAuth2 access token to client
- **Web App Server can redirect browser to Globus Web App pages**
 - Globus Web App can be skinned to look like Web App Server
 - Globus Web App provides special pages for **selecting files** and **selecting a group**
- **Globus Auth provides single sign-on across multiple apps**



Other resource servers

js Atmosphere x Steve

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

Jetstream DEMO

Images Help Login


SEARCH TAGS


Search across image name, tag or description

Showing 5 of 5 images List Grid

Featured Images

All Images

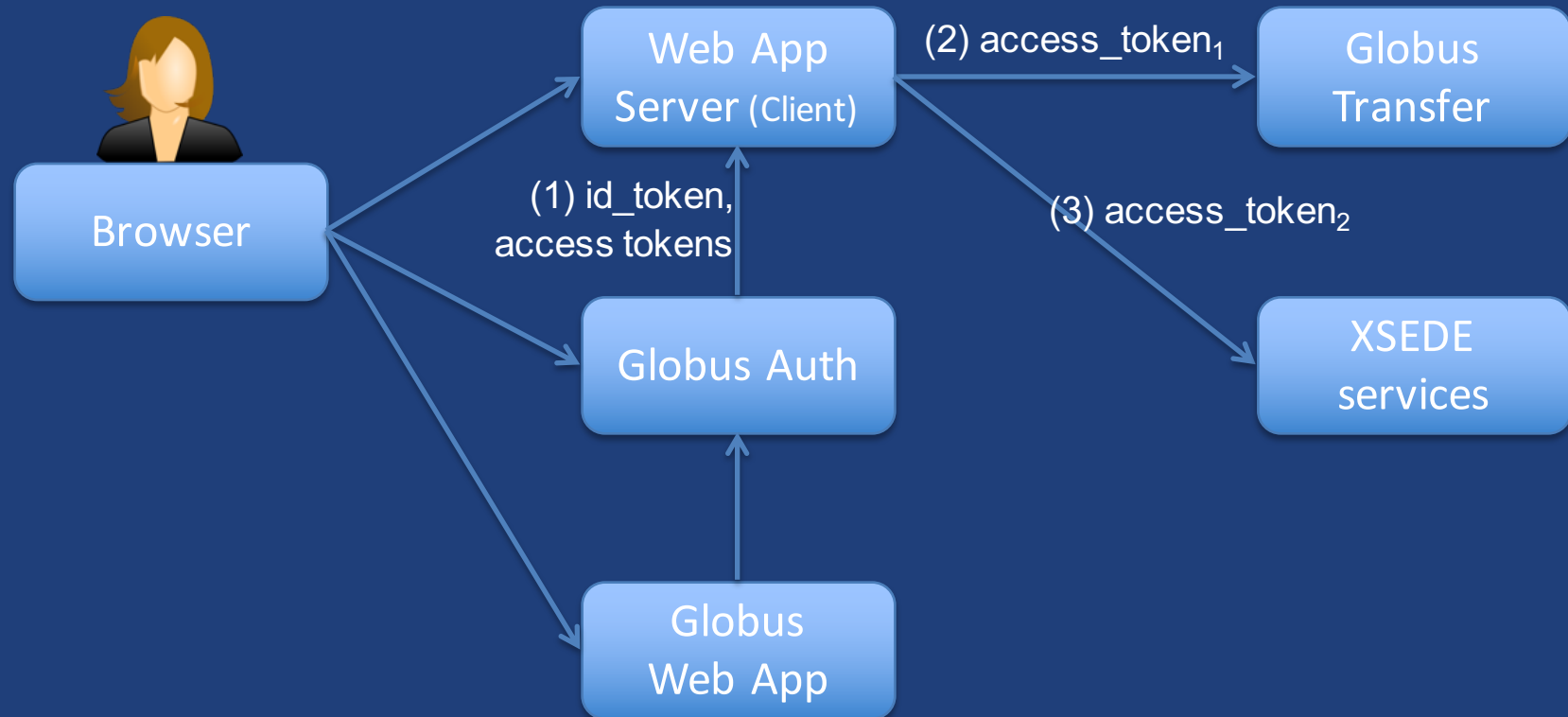
 [CentOS 7 Stock 1601](#)
Feb 1st 2016 08:31 am CST by admin
Imported Application - CentOS 7 Stock 1601

 [CentOS 6 Stock 1601](#)
Feb 1st 2016 08:31 am CST by admin

©2016 Jetstream [Feedback & Support](#)



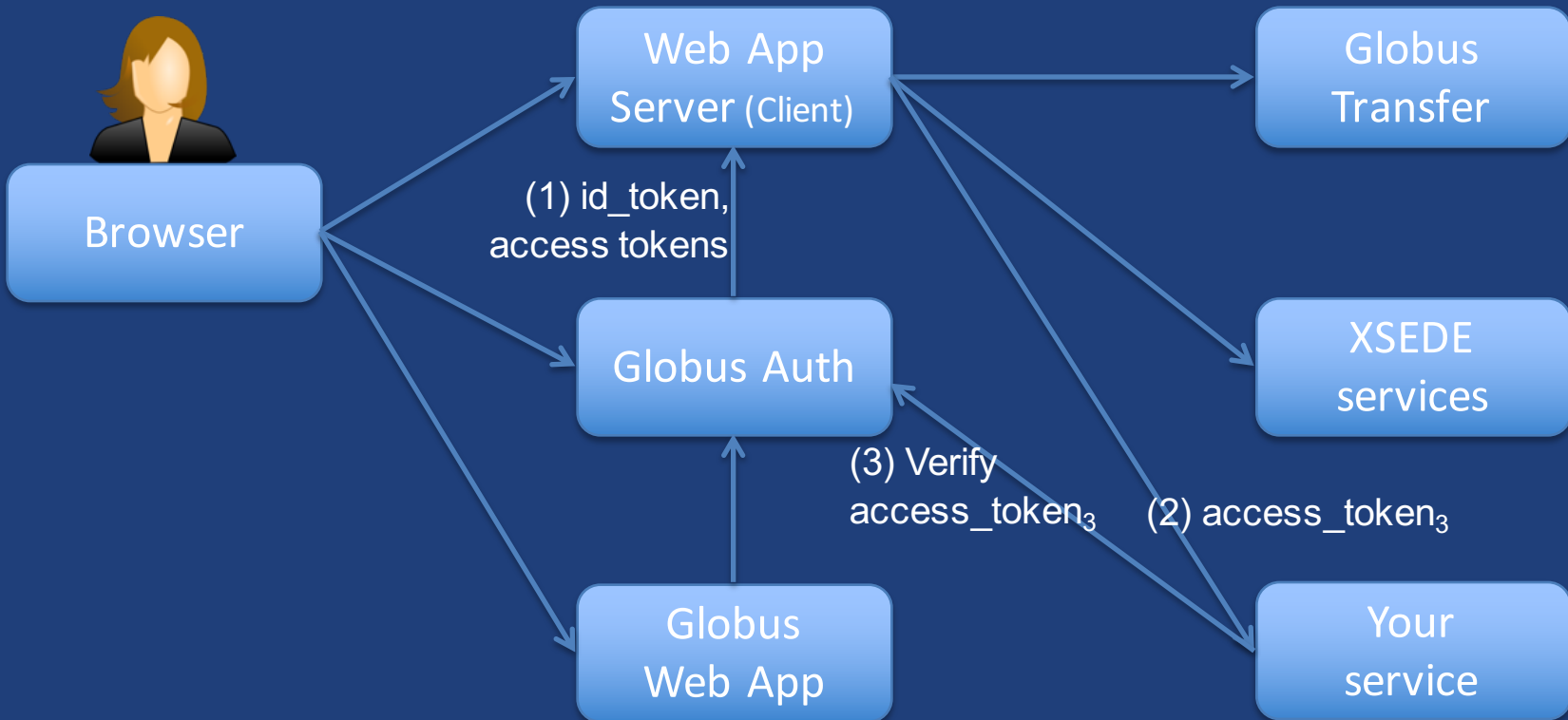
XSEDE services integration



- **OAuth2 Authorization Code Grant with Globus Auth**
 - Scopes: openid email profile urn:globus:auth:scope:transfer.api.globus.org:all
[urn:globus:auth:scope:api.xsede.org:all](#)
 - Globus Auth returns OIDC id_token & OAuth2 access tokens to client
- **Globus Auth returns different access tokens for different resource servers**
- **Web App Server calls each resource server with appropriate access token**



Add your own resource servers



- **OAuth2 Authorization Code Grant with Globus Auth**

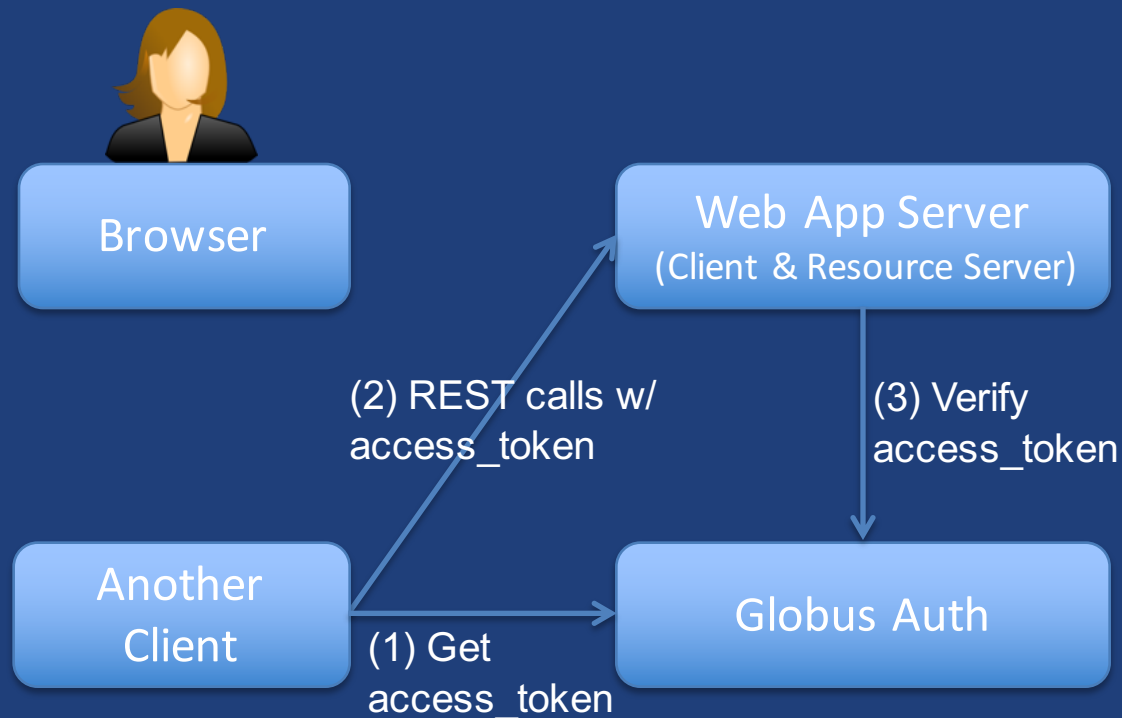
- Scopes: openid email profile urn:globus:auth:scope:transfer.api.globus.org:all urn:globus:auth:scope:api.xsede.org:all **urn:globus:auth:scope:api.example.com:all**
- Globus Auth returns OIDC id_token & OAuth2 access tokens to client

- **Resource Server must register with Globus Auth**

- Resource server policy can require identity from a particular identity provider



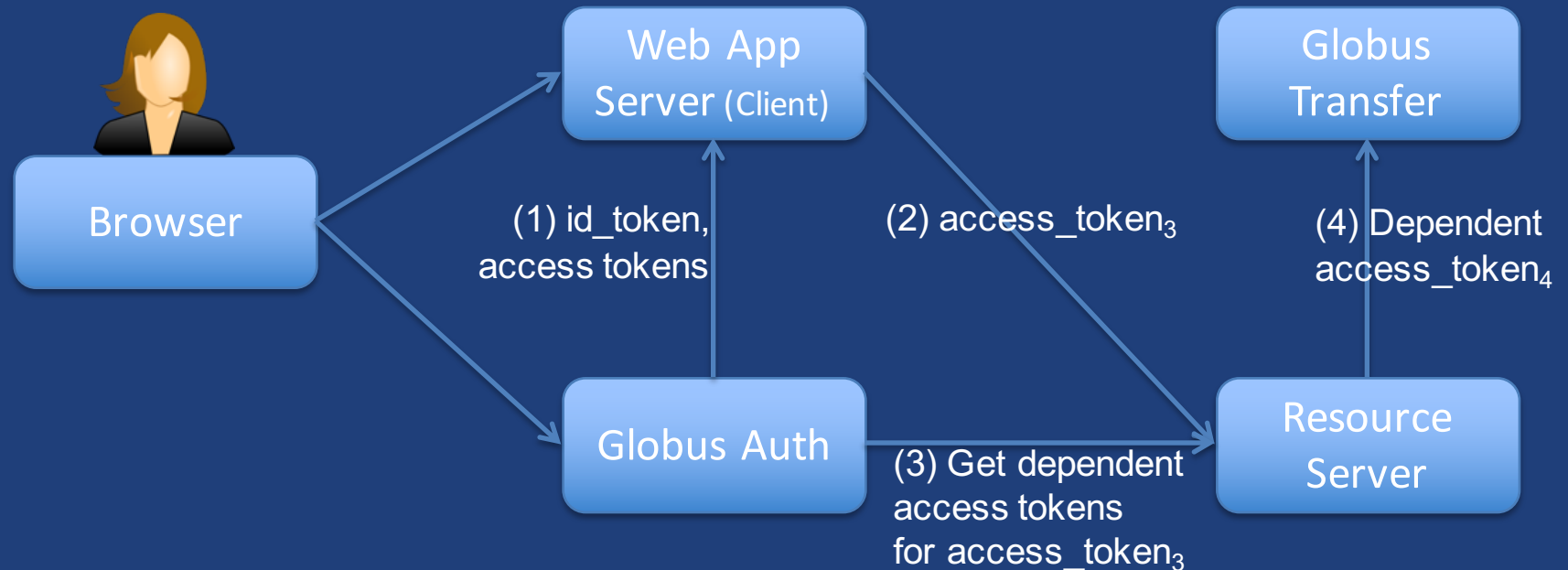
Both client and resource server



- **Web App Server can be both a client and a resource server**
- **Another Client can use any OAuth2 grant with Globus Auth to get access_token for your Web App Server**
 - Scope: `urn:globus:auth:scope:api.example.com:all`



Dependent resource servers



- **OAuth2 Dependent Token Grant with Globus Auth**
 - Scopes: openid email profile [urn:globus:auth:scope:api.example.com:all](#)
- **Resource Server registers its Globus Transfer dependency with Globus Auth**
- **Resource Server uses request access token to get dependent access tokens**
- **Resource Server uses dependent access token to call Globus Transfer**



Mobile applications

- **Globus Auth will be adding support for mobile apps**
 - “Log in with Globus” in mobile apps
 - RFC 7636: Extension to OAuth2 to allow OAuth2 Authorization Code Grant to work from mobile apps
 - Mobile apps can call any resource server REST APIs that use Globus Auth
 - iOS and Android



An extensible platform for CI

Apps

Domain-independent and domain-specific services

AWS, Google, Azure services

Foundation services: Globus Auth, Groups, etc.

- Globus provides foundation and other services
- Community can extend to meet domain-specific and domain-independent needs

Developer Workshop: Building the Modern Research Data Portal

New high-speed networks make it possible, in principle, to transfer and share research data at tremendous speeds and scales—but have also proved challenging to use in practice. Two new technologies now allow us to translate this potential into reality: Science DMZ architectures provide frictionless end-to-end network paths; and Globus APIs allow programmers to create powerful research data portals that leverage these paths for data distribution, synchronization, and other useful purposes.

Introduction, Concepts, and Components

IMPERIAL 2

Led by: TBD

We will introduce the Modern Research Data Portal and set the context for how Globus and the ScienceDMZ combine to deliver unique data management capabilities. This will include:

- Overview of use cases: Common patterns like data publication/distribution, orchestration of data flows, etc.
- Overview of the Globus platform: Architecture and brief overview of available services
- Introduction to the Globus Auth API: Authenticating and authorizing a client
- Introduction to the Globus Transfer API: Make your first call and move data with Globus
- Introduction to the Python SDK for using Globus Auth and Transfer

Come to Chicago in April to learn more!



Summary

- Globus no longer requires a Globus username and password
- Globus Auth makes it easy to:
 - add user login to your web app
 - integrate with Globus, XSEDE, and other services
 - add OAuth2 support to your service's REST API
 - create services to leverage other services



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



Thank you to our sponsors!



U.S. DEPARTMENT OF
ENERGY



THE UNIVERSITY OF
CHICAGO



NIST

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



Argonne
NATIONAL LABORATORY



powered by
amazon
web services