

*Connecting people and resources to
accelerate discovery by empowering the
science gateway community*



Using Keycloak to Provide Authentication, Authorization, and Identity Management Services for Your Gateway

*Marcus Christie
Science Gateways Research Center
Indiana University
EDS Consultant*



Award Number
ACI-1547611

Overview

- OpenID Connect with CILogon
- Using Keycloak for Authentication and Role-based Authorization
- Integrating Keycloak with Apache Airavata

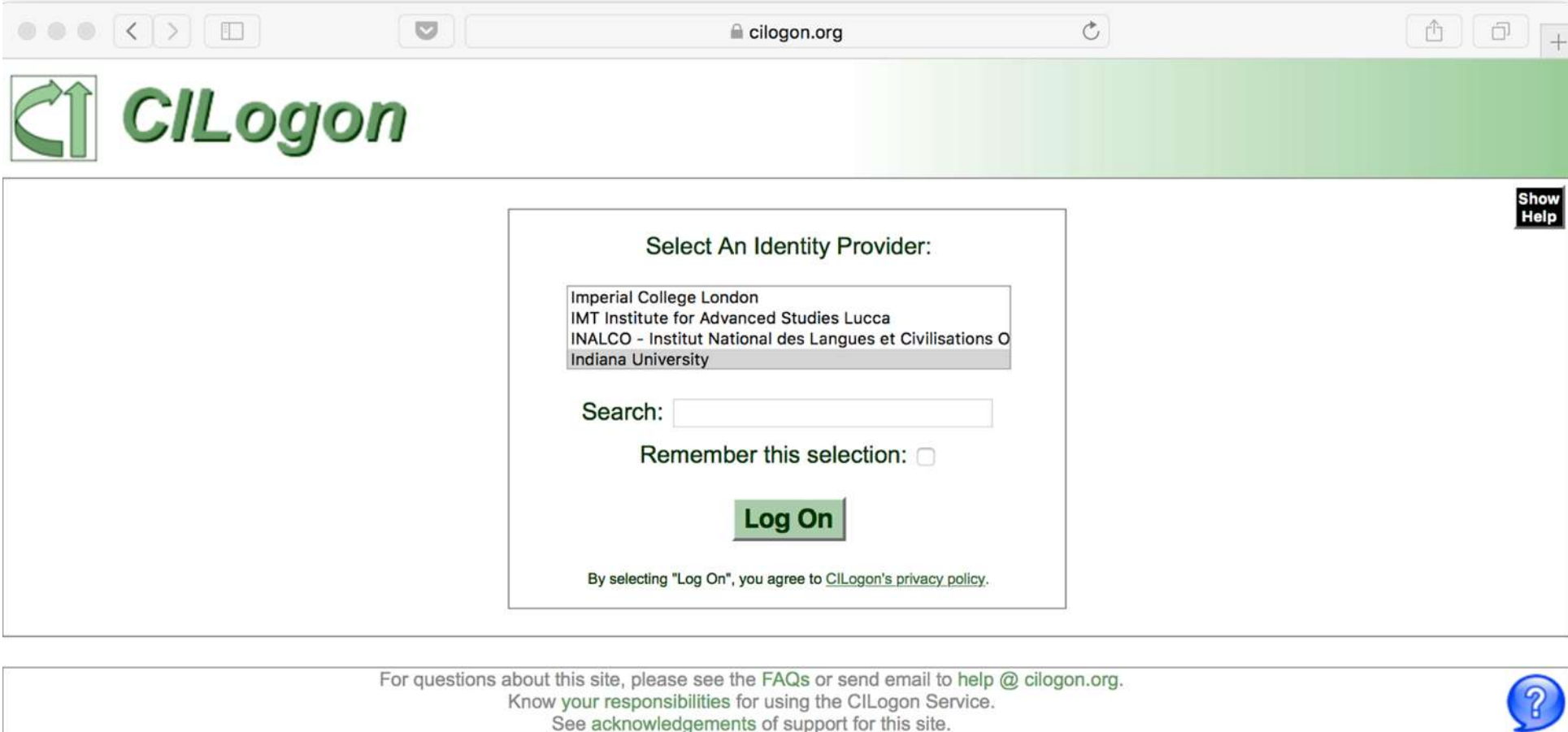
The Problem

- Gateways expose (shared) resources and APIs for manipulating those resources to a diverse set of users
- Authentication – another password to remember?
- Authorization – granting access without too much administrative burden
- Multiple gateways, multiple gateway clients
 - SciGaP (Science Gateway Platform as a Service)
- Campus gateways

Authentication

- Many options here but easiest thing is use an account the user already has
- CILogon
 - A service that allows users to authenticate to their institutions in order to retrieve credentials for accessing cyberinfrastructure.
 - Also provides a **OpenID Connect** (OIDC) interface to this federated authentication
- OpenID Connect
 - Built on top of OAuth2
 - Allows user to sign in with their identity provider
 - User grants client the right to access some of the user's information

CILogon OpenID Connect

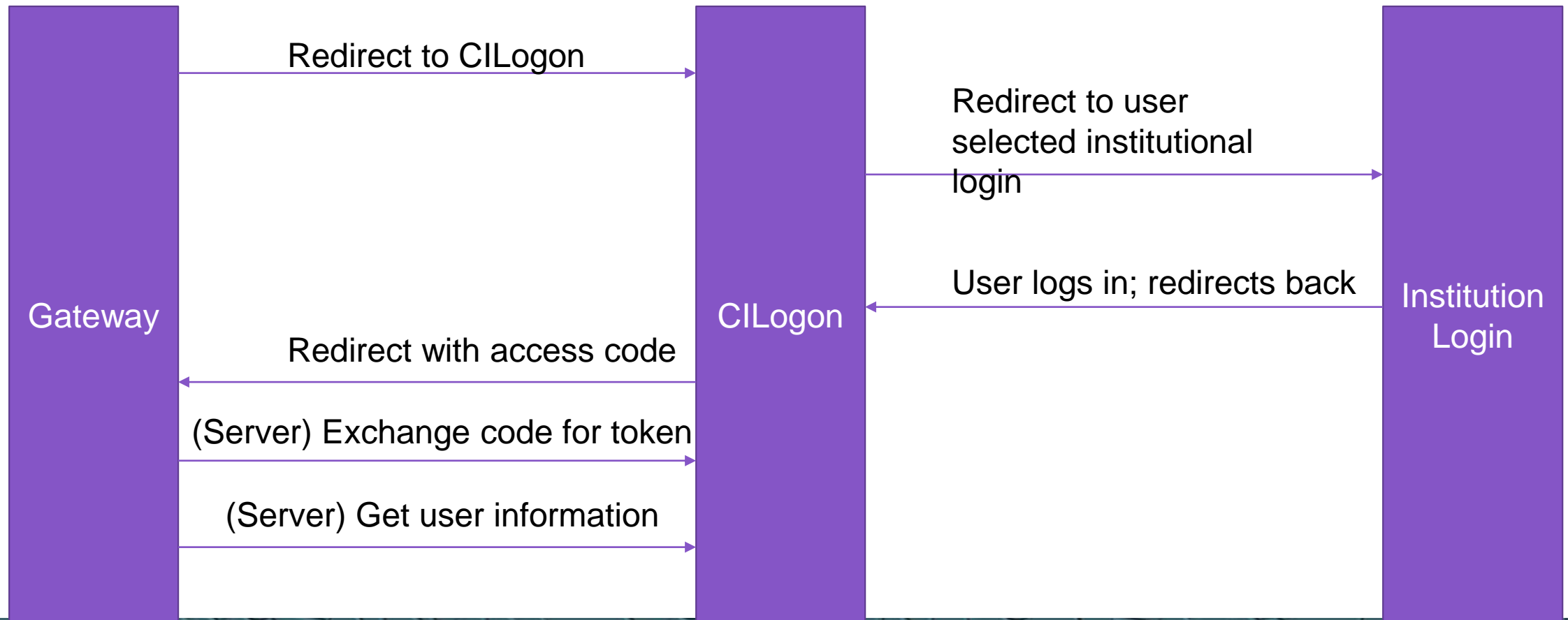


The screenshot shows a web browser window with the address bar displaying "cilogon.org". The page features the CILogon logo in the top left corner. The main content area is titled "Select An Identity Provider:" and contains a list of providers: Imperial College London, IMT Institute for Advanced Studies Lucca, INALCO - Institut National des Langues et Civilisations O, and Indiana University. Below the list is a search input field, a "Remember this selection:" checkbox, and a green "Log On" button. A disclaimer at the bottom of the selection box states: "By selecting 'Log On', you agree to CILogon's [privacy policy](#)." A "Show Help" button is located in the top right corner of the main content area. At the bottom of the page, there is a footer with contact information: "For questions about this site, please see the [FAQs](#) or send email to help@cilogon.org. Know your responsibilities for using the CILogon Service. See [acknowledgements](#) of support for this site." A blue question mark icon is also present in the footer.


OpenID Connect

- One time initial setup
 - Register a client: client id and client secret
- 1 - Redirect to CILogon
 - Parameters: client id, redirect_uri, scope=openid
- 2 - User signs in
- 3 - Redirect back to gateway
 - Exchange access code for authorization token
- 4 - Get user info
 - Use authorization token to call user info endpoint

OpenID Connect flow



One time setup: Registering a client with CILogon



The screenshot shows a web browser window with the address bar displaying "cilogon.org/oauth2/register". The page title is "Welcome to the CILogon OAuth 2 Delegation Service Client Registration Page". Below the title is a paragraph of introductory text. The registration form includes several input fields: "Client Name:", "Contact email:", "Home URL:", and "Refresh Token lifetime:" (with a note "(in seconds - leave blank for no refresh tokens.)"). There is a radio button option "Use Limited Proxy Certificates?". Below this is a large text area for "Callback URLs" with the instruction "Put your callbacks here, one per line.". A "submit" button is located at the bottom left of the form.

Welcome to the CILogon OAuth 2 Delegation Service Client Registration Page

This page allows you to register your client with the CILogon delegation service that supports the OIDC/OAuth 2. To get your client approved, please fill out the form below. Your request will be evaluated for approval. For more information, please make sure you read the [Registering a Client with an OAuth 2 server](#) document.

Client Name:

Contact email:

Home URL:

Refresh Token lifetime: (in seconds - leave blank for no refresh tokens.)

Use Limited Proxy Certificates?

Put your callbacks here, one per line.

Callback URLs:

Step 1: OIDC Redirection

```
https://cilogon.org/authorize?response_type=code  
&client_id=CLIENT_ID  
&redirect_uri=https://mygateway.org/callback  
&scope=openid
```

Step 3: OIDC Exchange code for token

```
https://mygateway.org/callback?  
code=https%3A%2F%2Fcilogon.org%2Foauth2%2FauthzGrant%2F331685b3f...
```

```
POST /oauth2/token HTTP/1.1  
Host: cilogon.org  
Authorization: Basic Base64($client_id + ":" + $client_secret)  
  
grant_type=authorization_code&code=...&redirect_uri=...
```

```
{  
  "access_token": "eyJhbGciOiJ...",  
  ...  
}
```

Step 4: OIDC fetch userinfo using access token

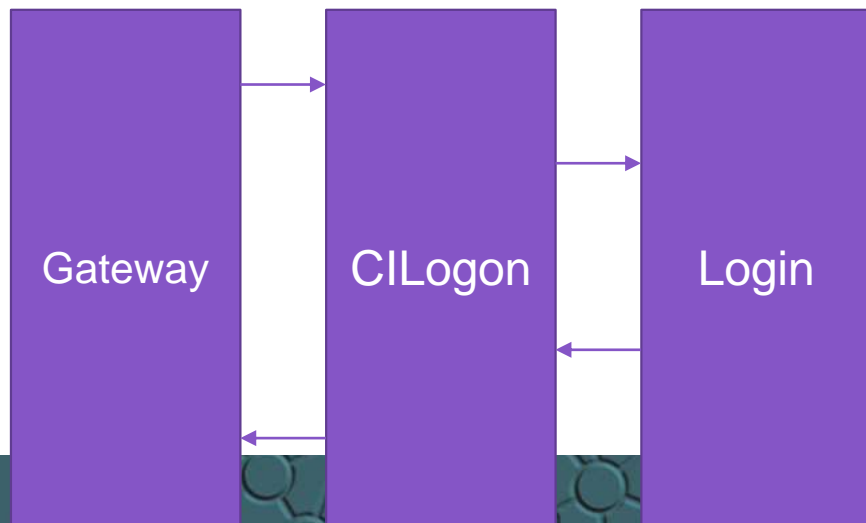
```
GET /oauth2/userinfo HTTP/1.1
Host: cilogon.org
Authorization: Bearer $access_token
```

```
{
  "sub": "http://cilogon.org/serverA/users/123",
  "name": "Marcus Christie",
  "given_name": "Marcus",
  "family_name": "Christie",
  "email": "machrist@iu.edu",
  ...
}
```

Integrating gateway with CILogon

- Direct integration
- Indirect integration through an Identity and Access Management (IAM) Server (for example, Keycloak)

Direct approach



Indirect approach



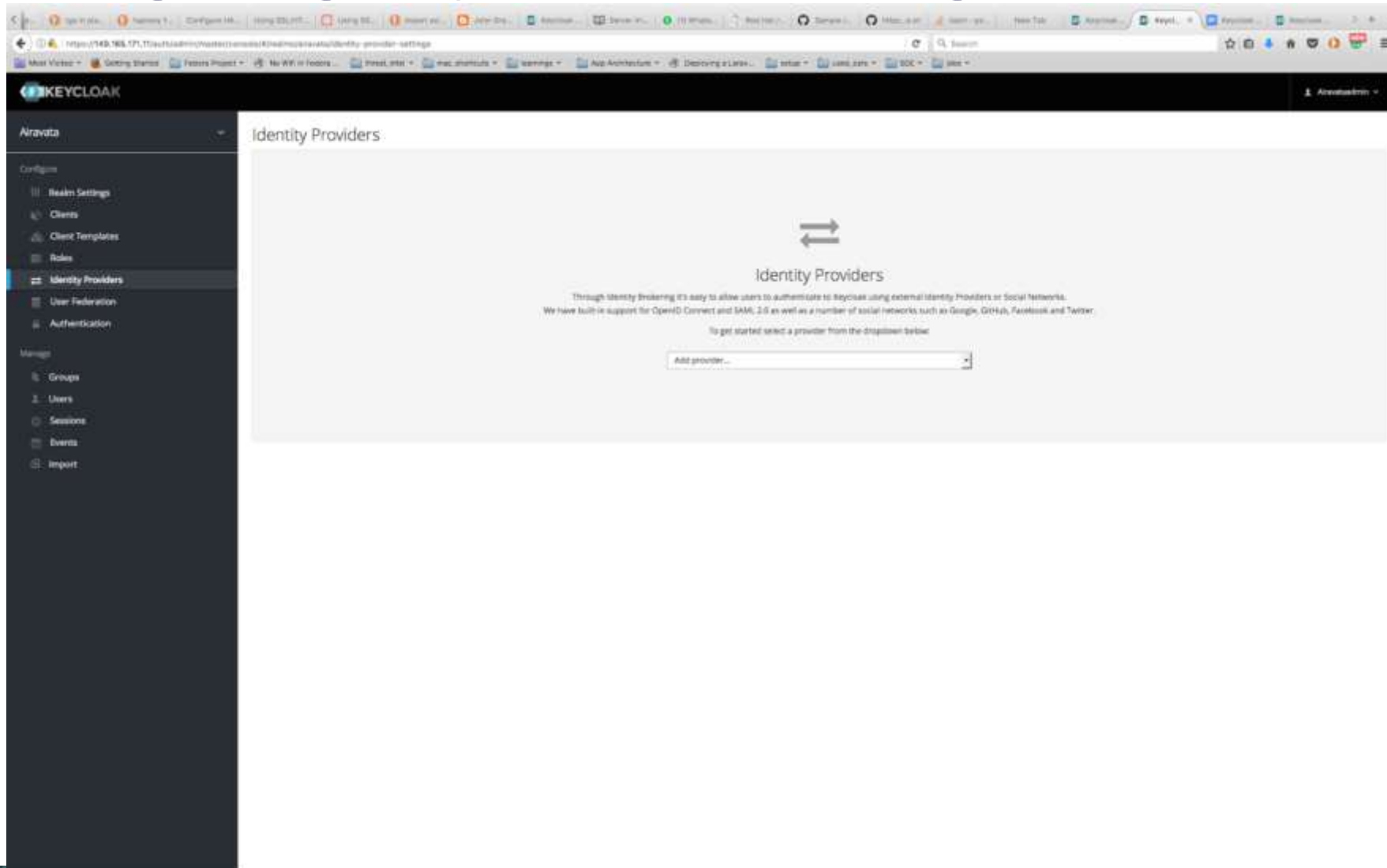
Advantages of using IAM server

- Flexible Authentication options
- Gateway client software integration is done once
- Authorization services

Keycloak

- <http://www.keycloak.org/>
- Red Hat, 200+ contributors on GH, 4,500+ merged PRs
- Open source (ALv2) identity and access management server
- Identity brokering; pluggable authentication mechanisms
- Authorization services: attribute-based, role-based, group-based, etc.
- Multi-tenanted
- Complete, well-documented REST API

Configuring Keycloak for CILogon



Configuring Keycloak for CILogon

The screenshot shows the Keycloak administration console interface. The browser address bar displays `iam.scigap.org/auth/admin/master/console/#/realms/accord.scigap.org`. The left sidebar contains navigation options: Authentication, Manage, Groups, Users, Sessions, Events, and Import. The main content area is titled "Trust Email" and "OpenID Connect Config".

Trust Email ON

GUI order

First Login Flow

Post Login Flow

OpenID Connect Config

* Authorization URL

* Token URL

Logout URL

Backchannel Logout OFF

Disable User Info OFF

User info URL

* Client ID

* Client Secret

Issuer

Default Scopes

Prompt

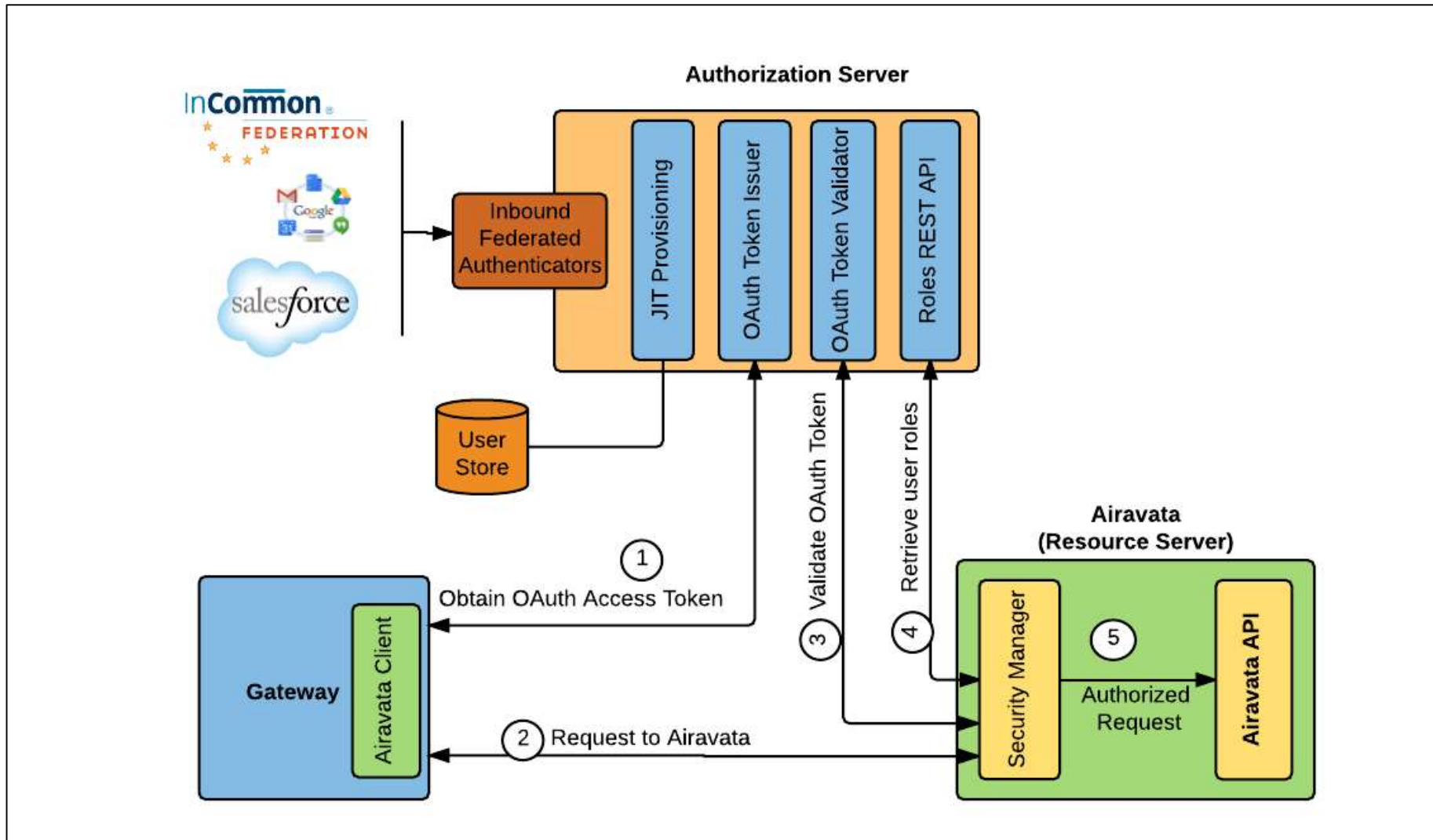
Validate Signatures OFF



How to integrate Keycloak

- Multi-tenanted: create a “realm” for each gateway
 - configure authentication options, like CILogon
- Web portal to use OpenID Connect for authentication
 - Redirect user to Keycloak to log in
- REST API for administrative and authorization integration
 - <http://www.keycloak.org/docs-api/3.0/rest-api/index.html>
 - E.g., Manage what roles a user has

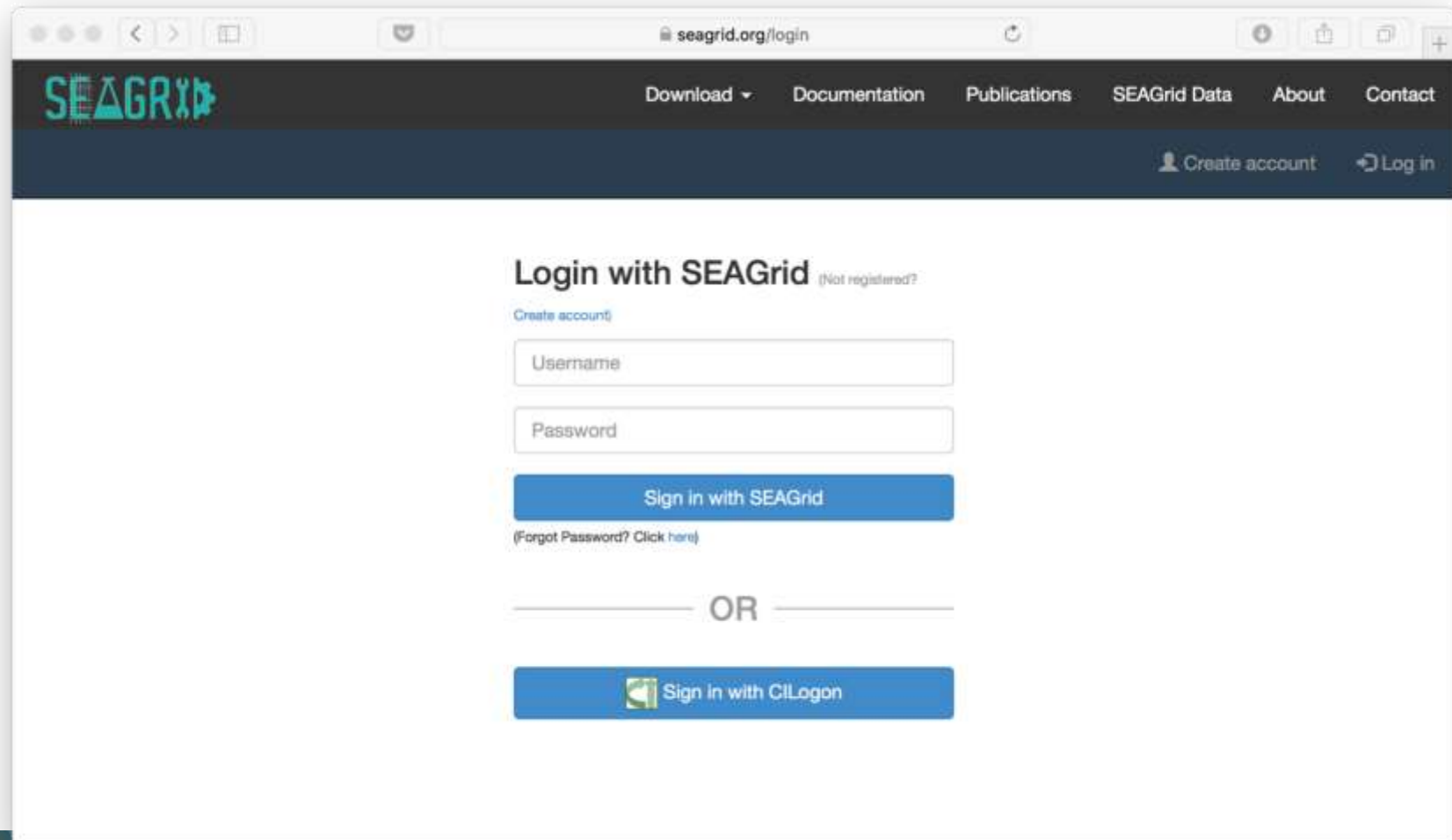
Securing Airavata



Apache Airavata – Profile Service

- Integrates with Keycloak REST API for tenant and user management
- Tenant Management
 - createTenant
 - Keycloak REST API: create Realm, create Realm Roles, create Admin user for Realm, create default client for web application
- User Management
 - createUser – Keycloak REST API: create User
 - enableUser – Keycloak REST API: update User
 - resetUserPassword – Keycloak REST API: update User with updated password
 - addRoleToUser – Keycloak REST API: add Realm Roles to User

User logs in



The screenshot shows a web browser window with the address bar displaying "seagrid.org/login". The page features a dark blue header with the SEAGRID logo on the left and navigation links for "Download", "Documentation", "Publications", "SEAGrid Data", "About", and "Contact" on the right. Below the header, there are links for "Create account" and "Log in". The main content area is titled "Login with SEAGrid" with a "(Not registered?)" link. Below this, there is a "Create account" link, followed by input fields for "Username" and "Password". A blue button labeled "Sign In with SEAGrid" is positioned below the password field. A link for "(Forgot Password? Click here)" is located below the button. A horizontal line with "OR" in the center separates the SEAGrid login section from the "Sign In with CILogon" section, which includes a CILogon logo and a blue button.

seagrid.org/login

SEAGRID

Download Documentation Publications SEAGrid Data About Contact

Create account Log in

Login with SEAGrid (Not registered?)

Create account

Username

Password

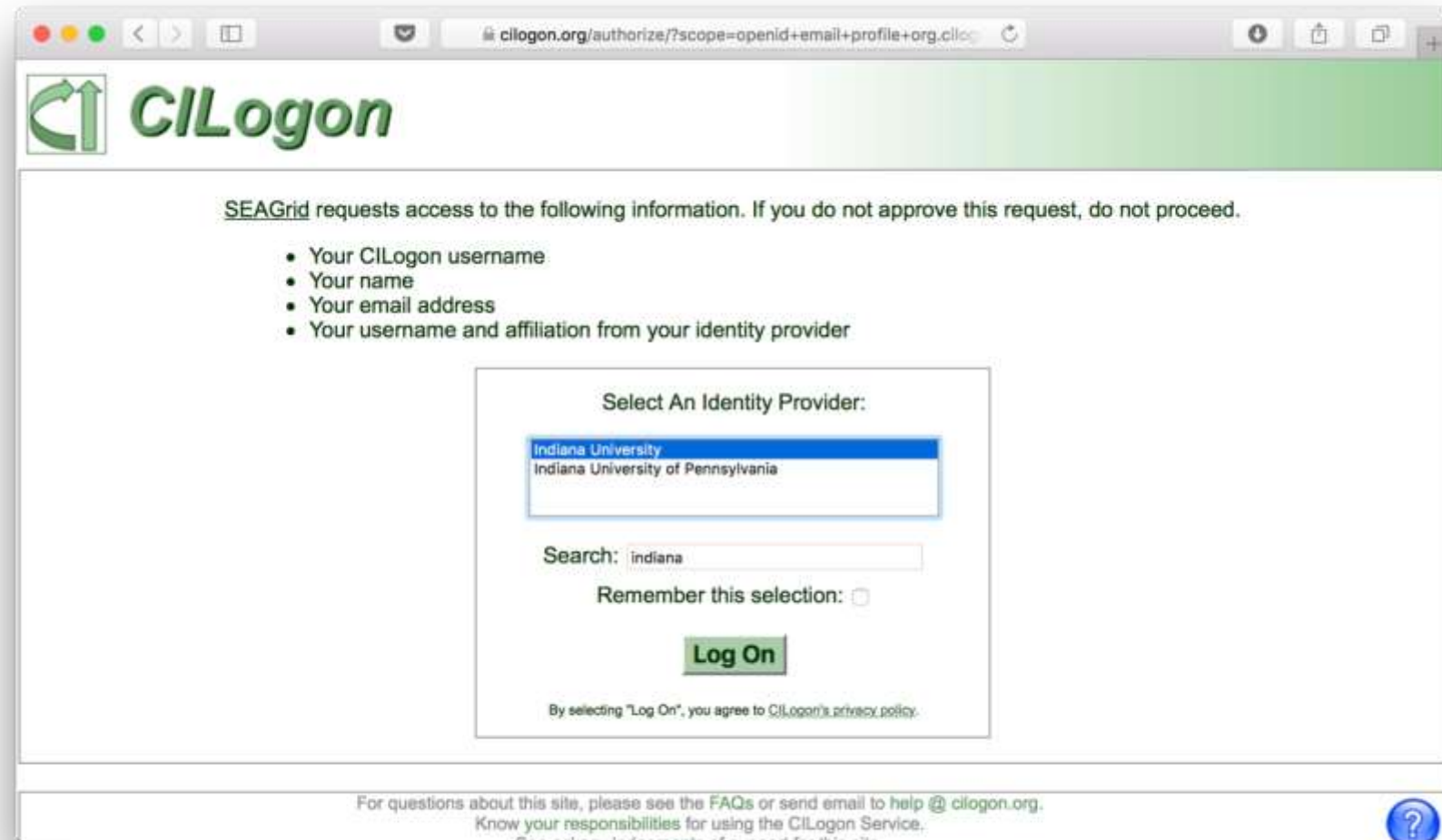
Sign In with SEAGrid

(Forgot Password? Click here)

OR

Sign In with CILogon

User logs in



The screenshot shows a web browser window with the URL `clilogon.org/authorize/?scope=openid+email+profile+org.cilogon.org`. The page header features the CILogon logo. The main content area contains a consent request from SEAGrid, listing the requested information: CILogon username, name, email address, and identity provider affiliation. Below this is a 'Select An Identity Provider' section with a dropdown menu showing 'Indiana University' selected and 'Indiana University of Pennsylvania' as an option. A search box contains the text 'indiana', and there is a 'Remember this selection' checkbox. A green 'Log On' button is present, with a note below it stating: 'By selecting "Log On", you agree to CILogon's privacy policy.' The footer includes contact information for help and a privacy policy link.

SEAGrid requests access to the following information. If you do not approve this request, do not proceed.

- Your CILogon username
- Your name
- Your email address
- Your username and affiliation from your identity provider

Select An Identity Provider:

Indiana University
Indiana University of Pennsylvania

Search: indiana

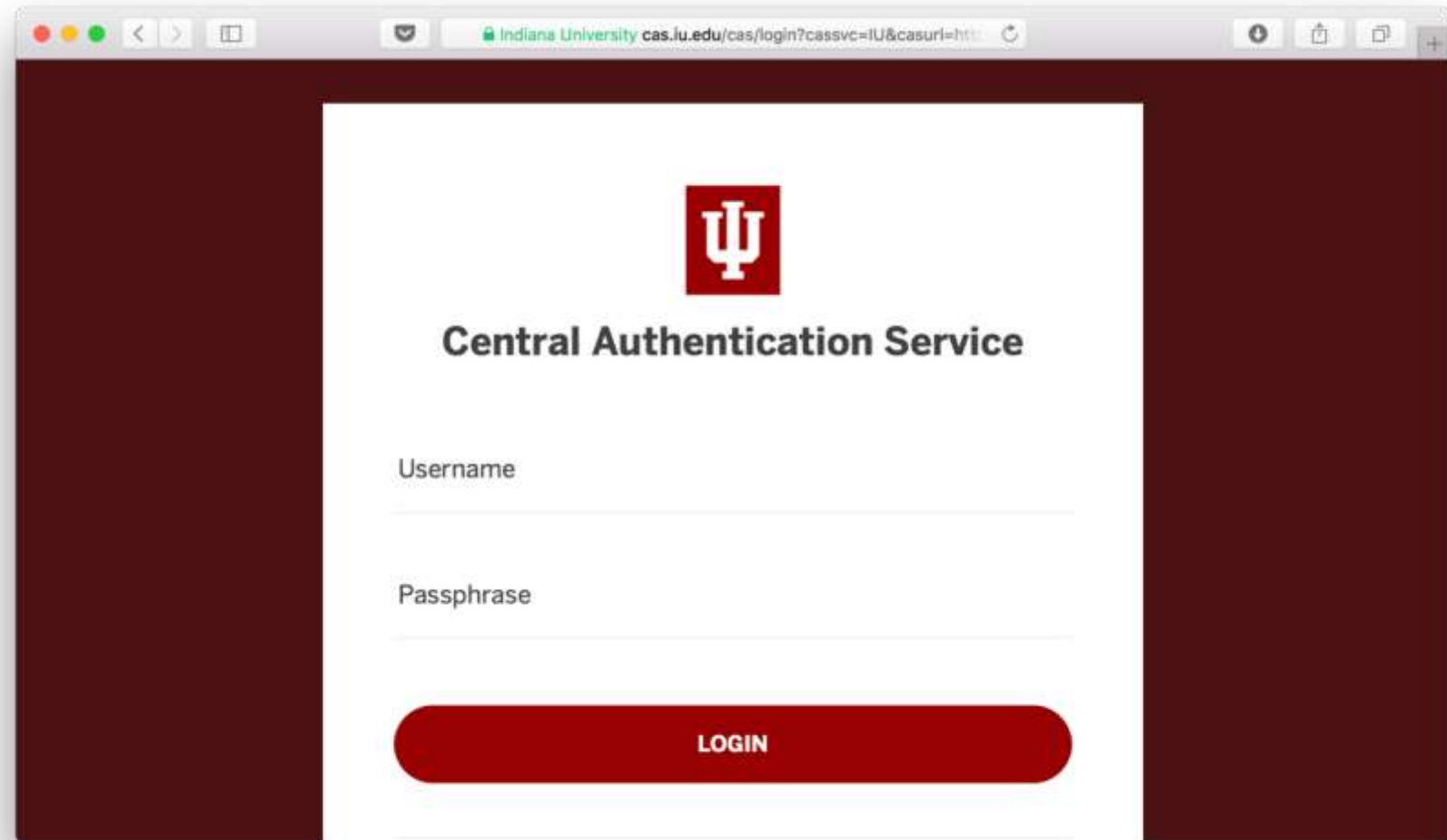
Remember this selection:

Log On

By selecting "Log On", you agree to CILogon's privacy policy.

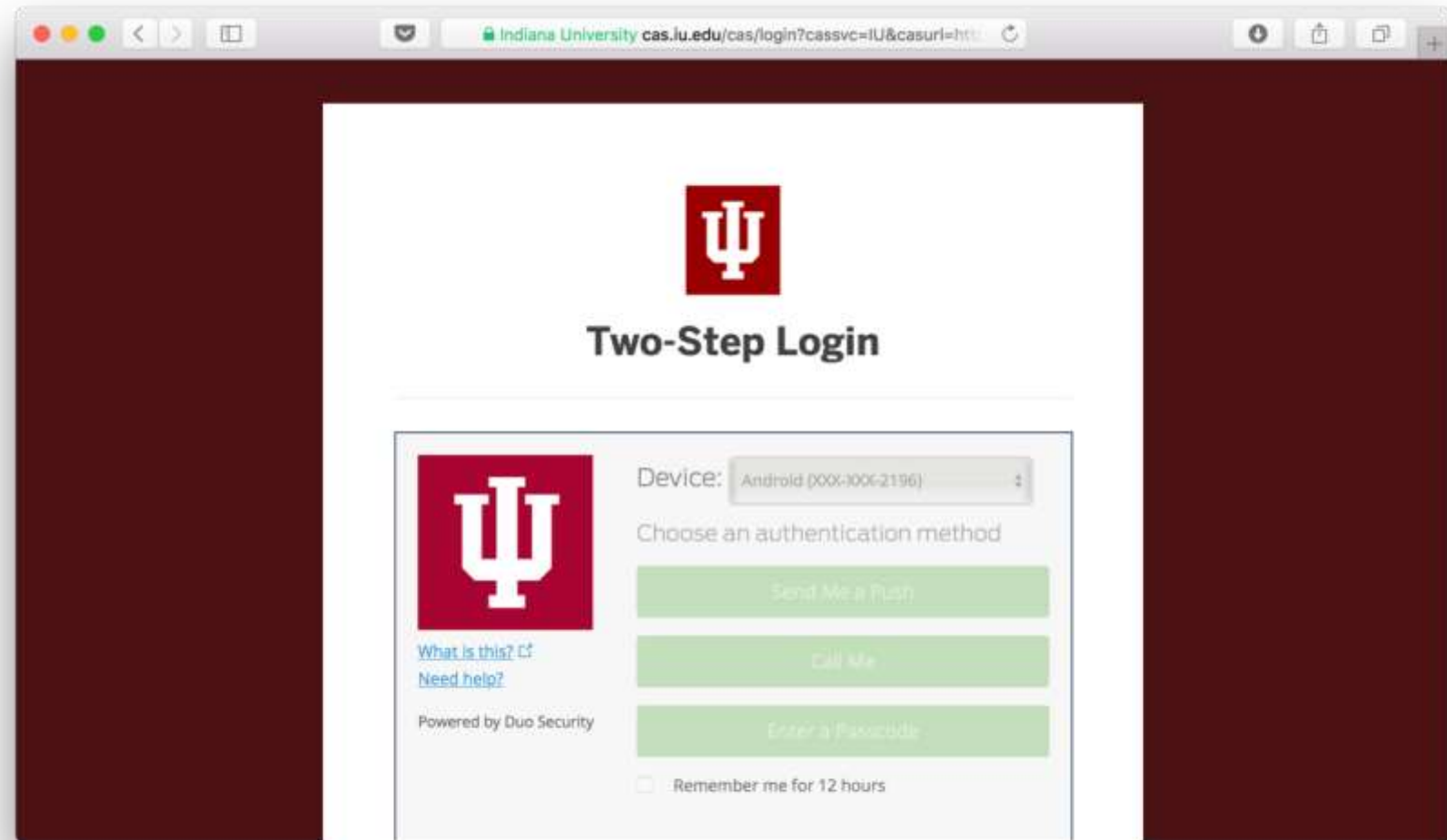
For questions about this site, please see the [FAQs](#) or send email to help@clilogon.org.
Know your responsibilities for using the CILogon Service.

User logs in

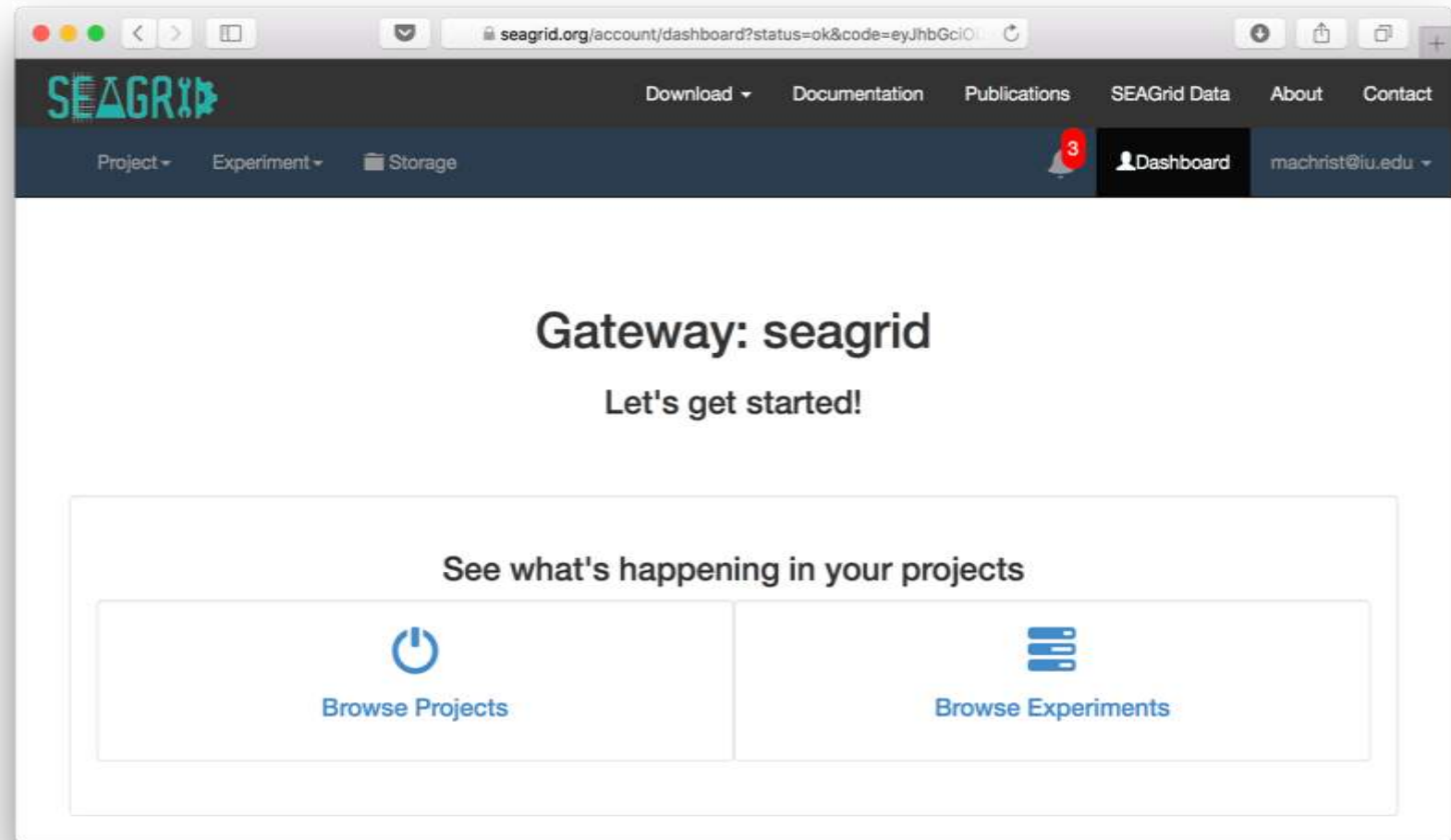


The image shows a web browser window displaying the login page for the Central Authentication Service (CAS) at Indiana University. The browser's address bar shows the URL: `cas.liu.edu/cas/login?casvc=IU&casurl=ht...`. The page features a dark red background with a white central box. At the top of the white box is the Indiana University logo, a red square with a white Greek letter Psi (Ψ). Below the logo, the text "Central Authentication Service" is displayed in a bold, black font. Underneath, there are two input fields: "Username" and "Passphrase", each with a horizontal line for text entry. At the bottom of the white box is a prominent red button with the word "LOGIN" in white, uppercase letters.

User logs in



User logs in



First login: user is assigned a default role

- At this point, the user is logged in but can't do anything yet
- User is assigned to 'user-pending' role
- Gateway admin gets an email about a new gateway user

Admin grants role

The screenshot shows a web browser window at `seagrid.org/admin/dashboard/users`. The page title is "User Roles". The user being managed is "machrist@iu.edu". A search box contains "gateway-user". A list of roles is displayed: "admin", "admin-read-only", "gateway-user", and "user-pending". A blue "Add Roles" button is visible next to the list. A "Close" button is at the bottom right of the modal. The background shows the SEAGrid navigation menu with items like "Download", "Documentation", "Publications", "SEAGrid Data", "About", and "Contact". The footer features the IU logo and "GCI".

seagrid.org/admin/dashboard/users

User Roles

User : machrist@iu.edu

gateway-user

admin
admin-read-only
gateway-user
user-pending

Add a new roles to the user

Add Roles

Close

How does the role get used?

- Portal – show/hide functionality based on role
- Airavata API server – each API method is restricted to certain roles
 - Uses OIDC endpoints to verify access token
 - Uses Keycloak REST API to get user's roles
 - Mapping from role to API methods accessible by that role

Questions?

- Feel free also to email me at machrist@iu.edu