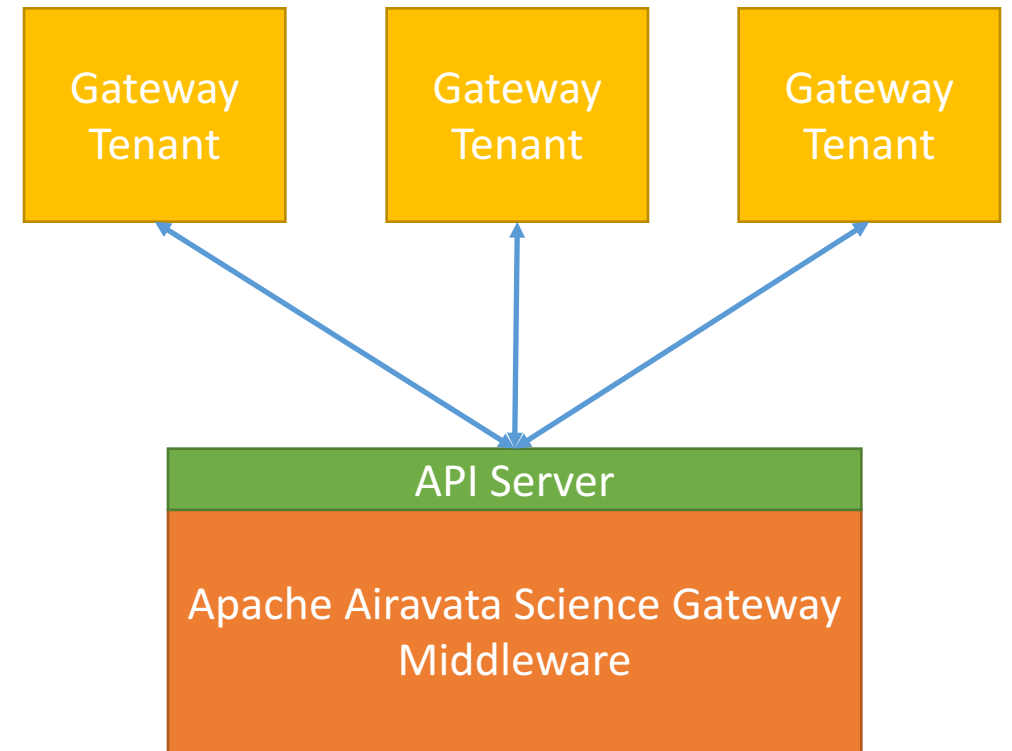


OAuth2, OpenID Connect and Science Gateway API Servers

What You Need to Know for Project Milestone 2

General Gateway Issues

- Science Gateways use middleware for common, generic functions.
 - Execute jobs, manage data and metadata
- **Authentication as a Service:**
Science gateways need a way to authenticate users.
- **Authorization as a Service:**
Middleware (Airavata) needs a scalable way to establish trust with numerous science gateway tenants.
 - Gateway tenants can be Web clients but also desktop clients.
 - These have very different security concerns.



Authentication as a Service

Using an IdP centralizes authentication and user management across your organization.

User + Browser

(2) User Authenticates

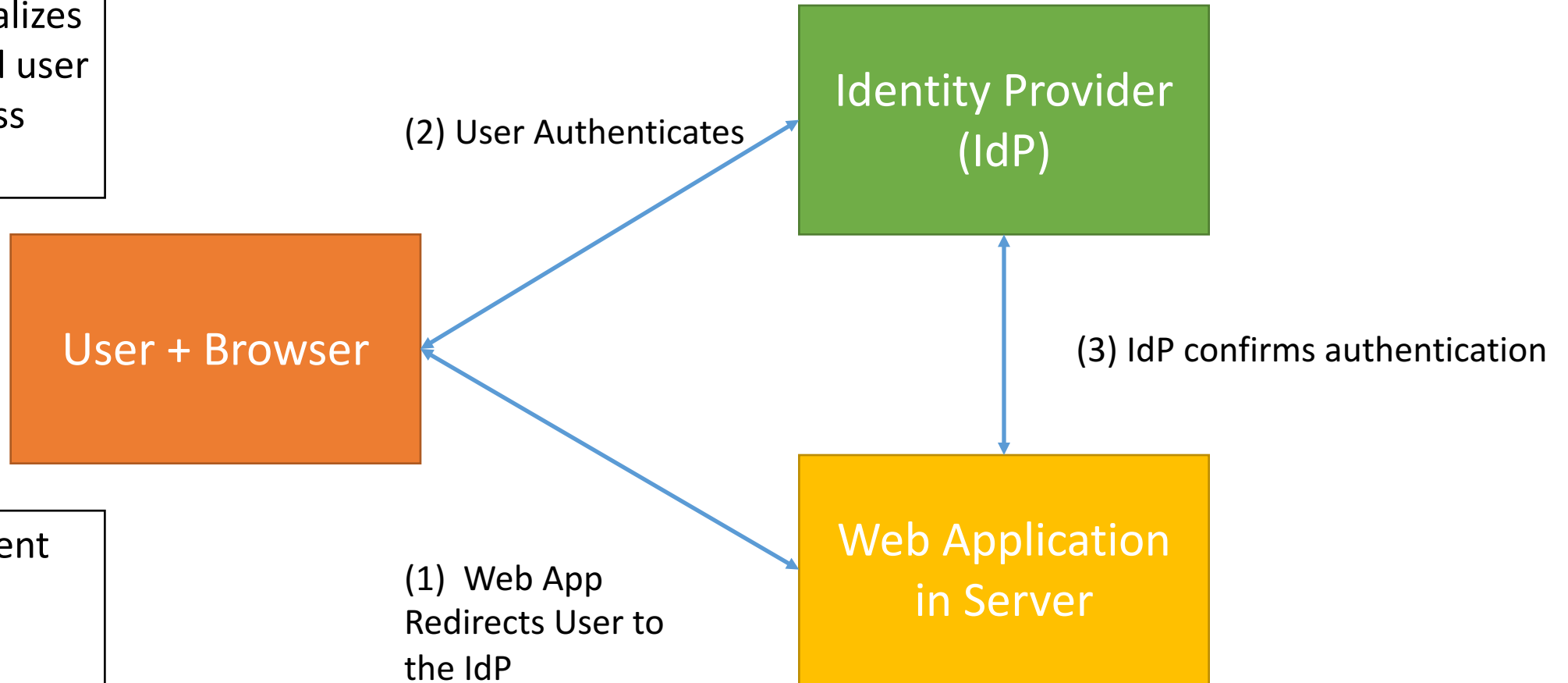
Identity Provider
(IdP)

(3) IdP confirms authentication

Good IdPs implement best practices for managing user information.

(1) Web App
Redirects User to
the IdP

Web Application
in Server



Create a Trello Account

https://trello.com/signup?returnUrl=%2F

Create a Trello Account

Name

Email


Password

Create New Account

Do you have a Google Account?

Sign up with Google

Let's sign up





One account. All of Google.

Sign in with your Google Account



Next

[Find my account](#)

[Create account](#)

One Google Account for everything Google



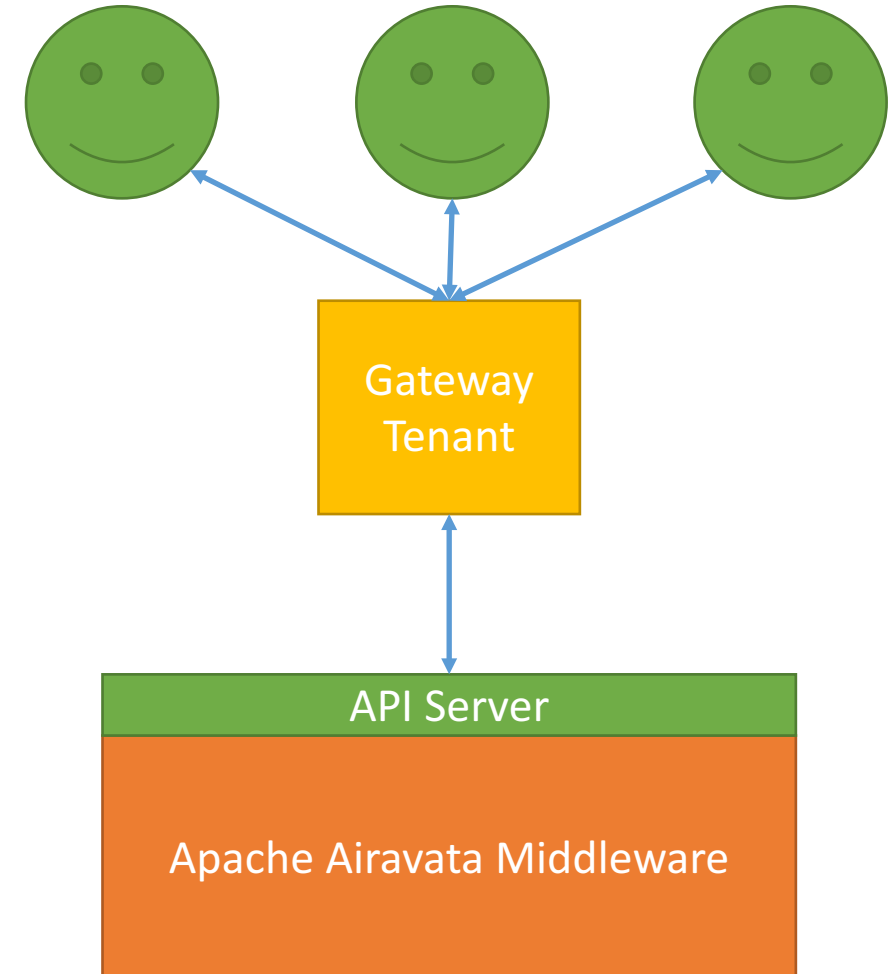
Look at the URL On the Sign Up Page

https://accounts.google.com/ServiceLogin?passive=1209600&continue=https://accounts.google.com/o/oauth2/auth?openid.realm%3Dhttps://trello.com%26scope%3Dopenid%2Bemail%2Bprofile%26response_type%3Dcode%26redirect_uri%3Dhttps://trello.com/auth/callback%26state%3DreturnUrl%253D%25252F%2526locale%253Den-US%2526csrf%253D0GeVBUY02zhGDH%25252BMUOASfk%25252FYnOXQavsNtqW2bW05Ab4%25253D%26client_id%3D28300235456-b801aqbc1i8luet9arr7sgll09t6eep9.apps.googleusercontent.com%26from_login%3D1%26as%3D-84d8dbf64644636&oauth=1&sarp=1&scc=1#identifier

OK, don't look too long...

Security Issue #1: User Authentication

- Gateway users must authenticate themselves.
 - You need to provide identity management
- User sessions in the gateway will be archived
 - Use the Registry for this.
- This is analogous to Amazon's shopping cart and order history.



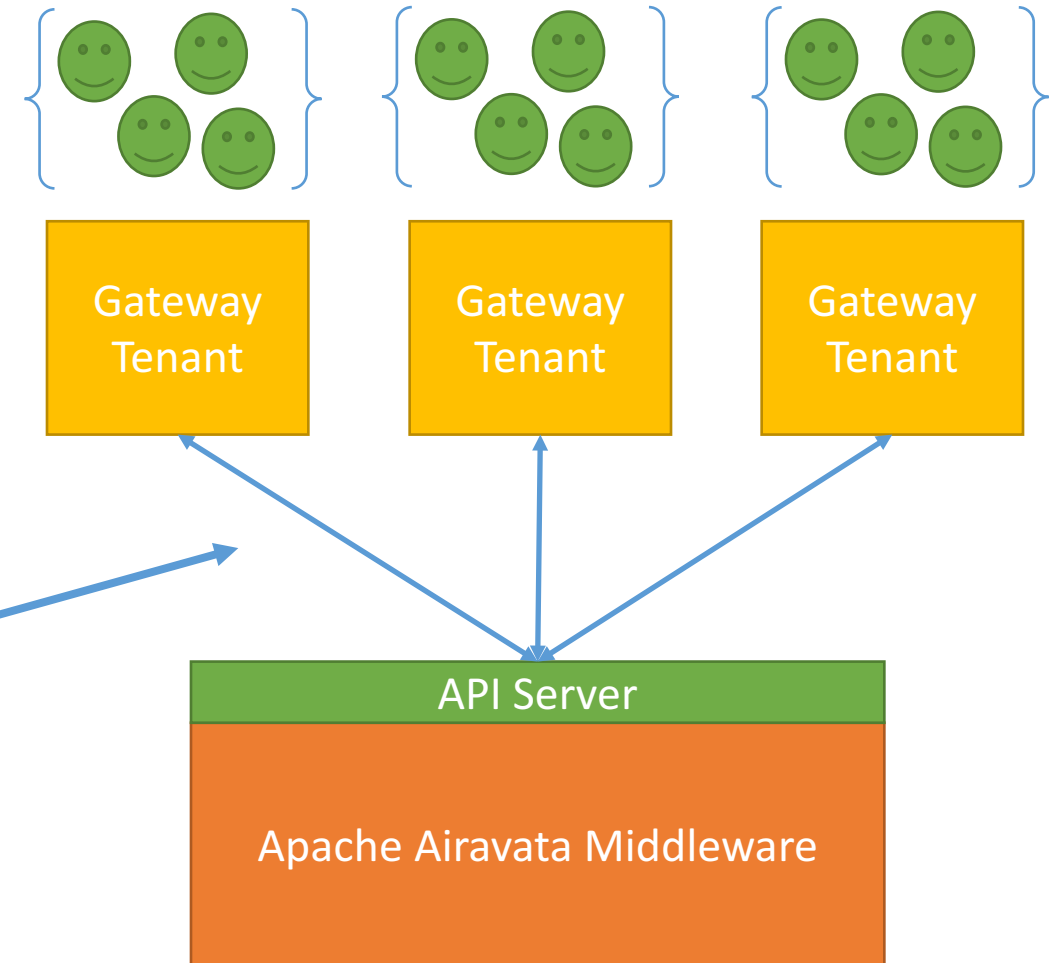
Authentication and Project Milestone 2

- For Project Milestone 2, you will use OpenID Connect to authenticate users.
- If you already have a login mechanism from Project Milestone 1 (optional), add OIDC login.
- Pick an option
 - Google: <https://developers.google.com/identity/protocols/OAuth2>
 - Auth0: <https://auth0.com/>
 - Stormpath: <https://stormpath.com/>
- Want to use another provider? Discuss with us.
- Discuss with TA Anuj Bhandar

Security Issue #2: Tenant to Middleware Security

- You DO NOT need to do this for Milestone 2.
- Using HTTPS is all that is required
- We may include it in a future milestone.

General Problem: how does a gateway tenant itself authenticate to the API server?



Let's Look at Some Real Examples

I'll show Pinterest and Zapier. Can you think of some?



Getting started

Users

Boards

Pins

SDKs

Overview

iOS

Android

Javascript

Add-ons

Getting started

Save button

Follow button

Pin widget

Board widget

Profile widget

Rich Pins

Getting started

Article Pins

Pinterest platform

The Pinterest Developers Platform is a suite of tools that help you reach Pinners in new ways. Right now, there are 3 ways to use the platform to increase your reach: through the API, add-ons and Rich Pins.

The Pinterest API

We use a RESTful API that lets you access users' Pinterest data, like their boards, Pins, followers and more. The Pinterest API uses OAUTH and allows both read and write permissions when interacting with a user's content.

To start, you'll need to set up an app. Get all the info you need over at [Getting started](#). The easiest way to access our API is to use one of our SDKs: we currently provide [iOS](#), [Android](#) and [JavaScript](#). If you don't want to use




Authentication

Pinterest uses [OAuth 2.0](#) to authenticate requests between your app and your users. With OAuth, users can give you access to their Pinterest content without giving up their passwords. Here's how it works:

1. **Get authorization from your user.** Your app will redirect your user to Pinterest and ask for their permission to read or change their account.
2. **Get an authorization code.** If your user approves your request, you'll receive temporary credentials (known as an authorization code) for your user's Pinterest account.
3. **Exchange for an access token.** Your app will call the API to exchange the authorization code for an access token, which is a

Formstack (OAuthV2 & REST Hooks Example)

← → ↺ 🔒 https://zapier.com/developer/documentation/v2/rest-hooks-example/ ☆ 📄 ⋮

 we're hiring!

EXPLOREAPP DIRECTORYPRICINGLOG INSIGN UP

Documentation

Version 1Version 2 (beta)

YOUR APPSSHARED ZAPSDOCUMENTATION

Developer Platform Docs

Search All

Platform

[Getting Started](#)[How Does it Work?](#)[Style Guide](#)[Scripting](#)[Reference \(Full Guide\)](#)

App Lifecycle

[1. Planning](#)[2. Development](#)[3. Activation](#)[4. Marketing Launch](#)[5. Ongoing Support](#)

Example Apps

<https://zapier.com/developer/documentation/v2/rest-hooks-example/>

Formstack (OAuthV2 & REST Hooks)

This example will walk you through creating a developer app that uses [REST Hooks](#) for a trigger that subscribes and unsubscribes a callback and waits for the data to come in. To make the example real, we'll be implementing the actual **Formstack** API. Let's get started!

Quick Preparation Checklist

If you plan to follow along, it is recommended you set up everything beforehand and keep these resources open and ready for quick access.

- You must have a [Zapier account](#).
- You must have a [Formstack account](#) and are ready to create a [Formstack Developer App](#).
- Read the [Getting Started with the Zapier Developer Platform](#) section to familiarize yourself with some of

Get help

Try It Out Yourself

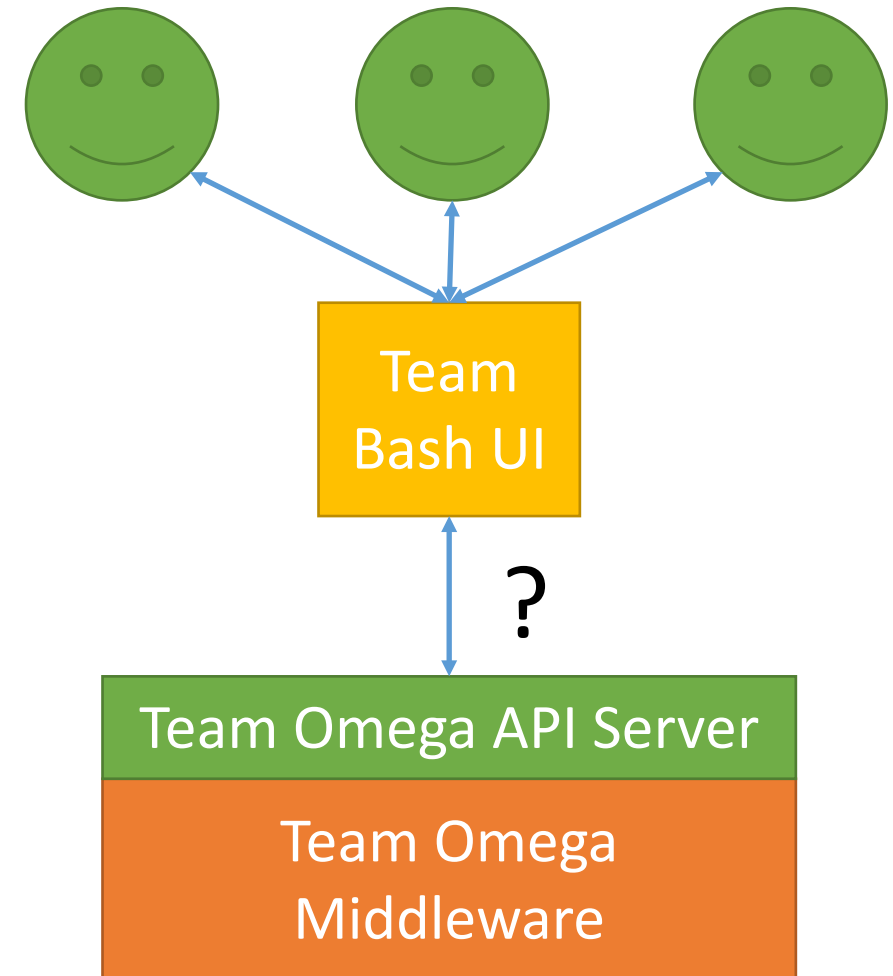
- Follow the Zapier documentation to make an OAuth2 app.
 - <https://zapier.com/developer/documentation/v2/rest-hooks-example/>
- Your app is an OAuth2 client.
- Have your friends use it.
 - They are the Resource Owners.
 - Their Zapier accounts are OAuth2 Resource Services.

Thought Experiment

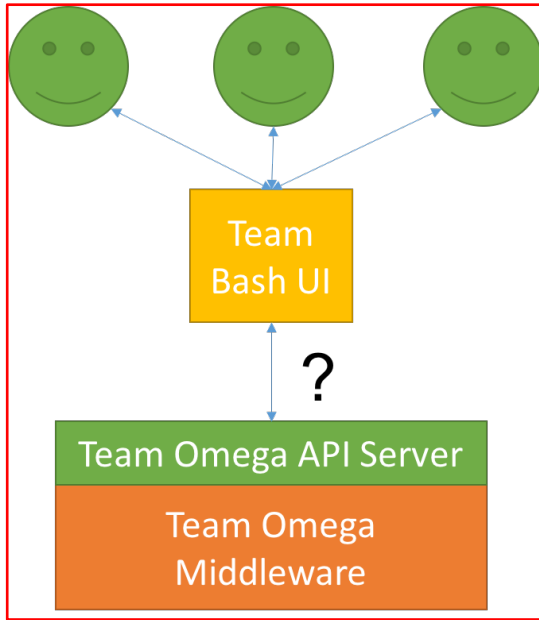
How Would You Use OAuth2 for Security Issue #2?

OAuth2 and Multiple Gateway Tenants

- What if Team Bash wants its gateway UI to use Team Omega's API Server.
- Team Bash will need to modify its UI client to use the API, of course.
- But how does Team Omega decide to allow this?
- And what if Team CodeRing and Team Aviato also want to use Team Omega's API server?

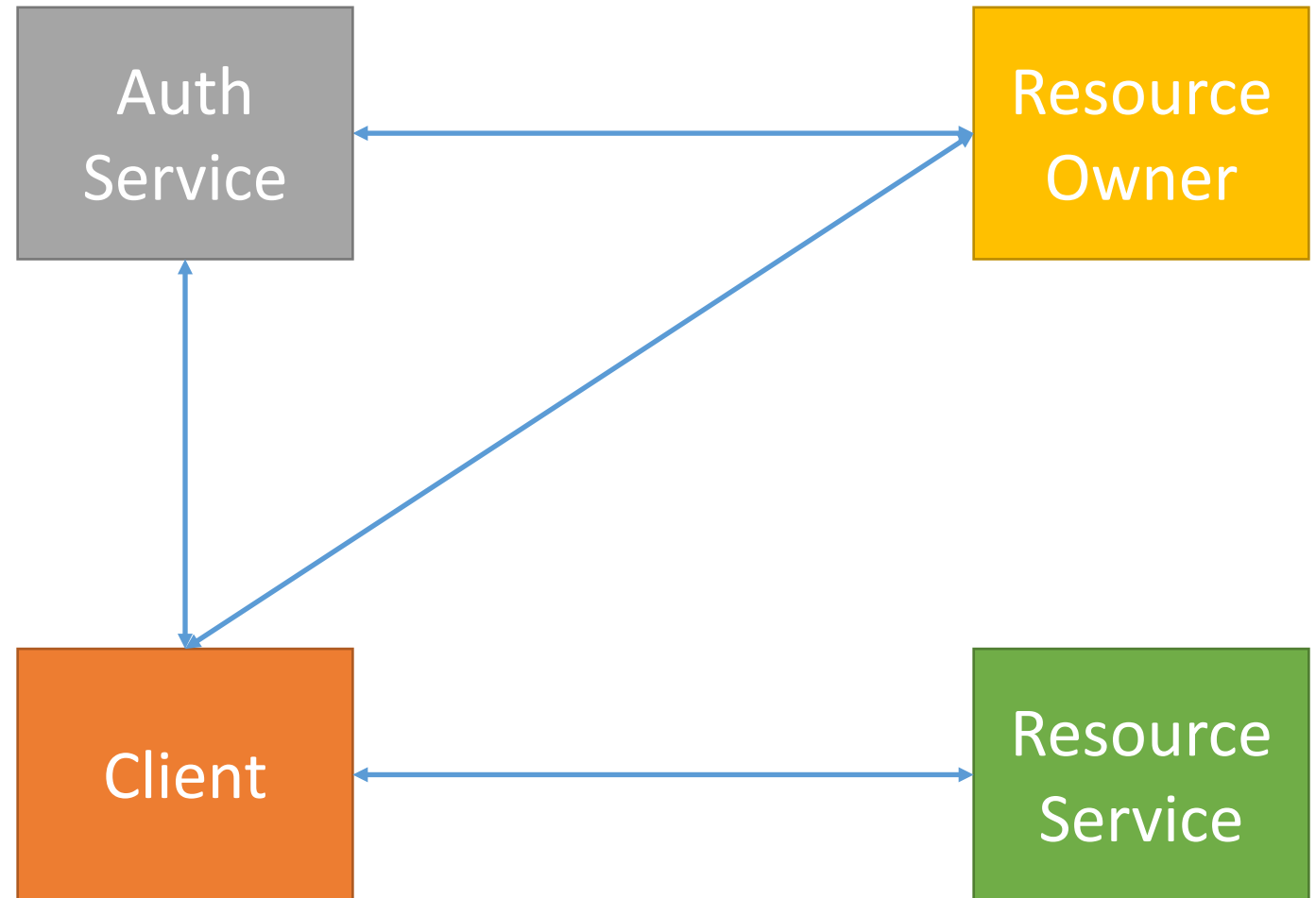


Map the Gateway Entities to OAuth2



For Science Gateways,

- Who is the Resource Owner?
- Who is the Client?
- What is the Resource Service?



OAuth2 Entities

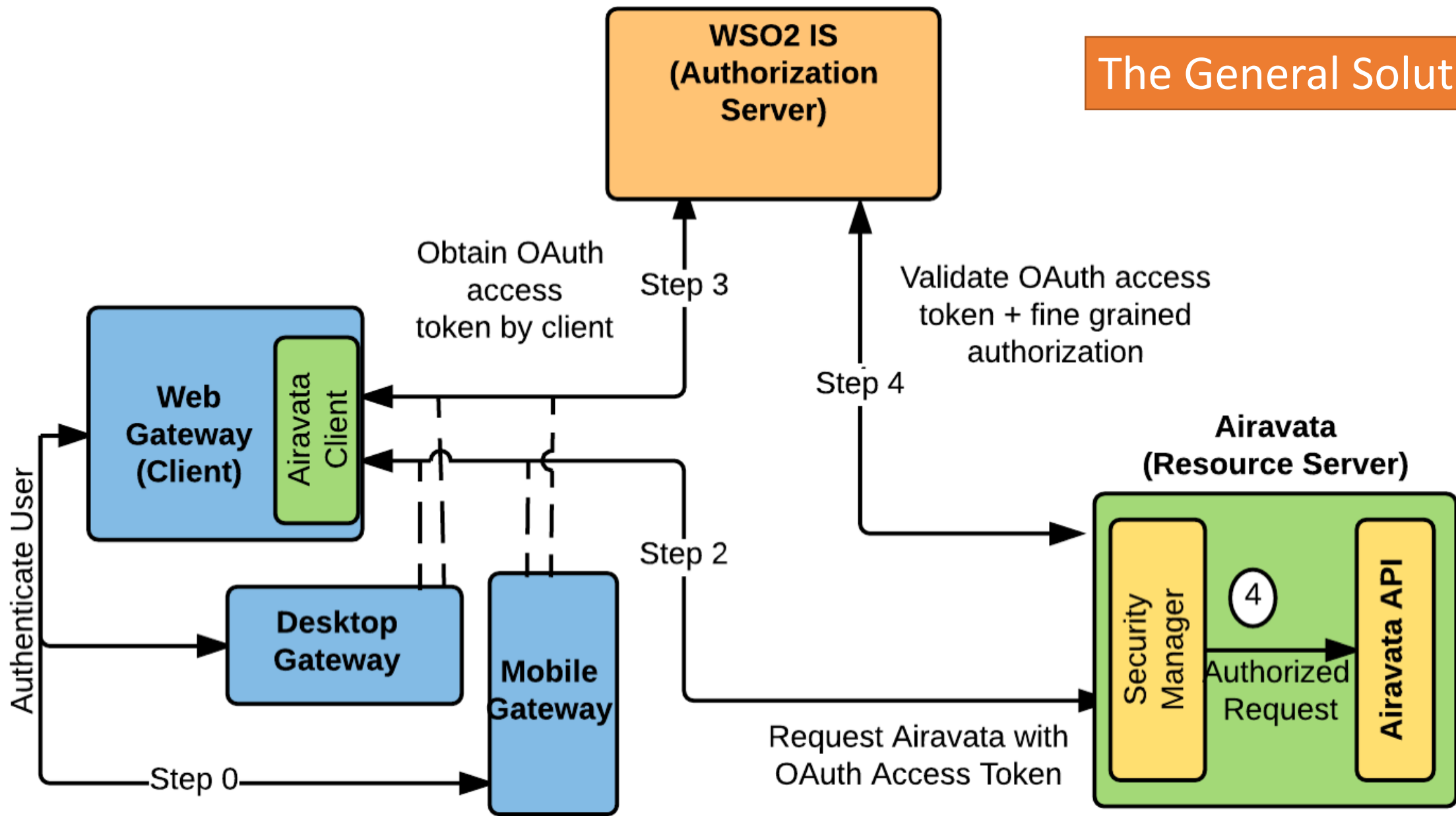
OAuth2 Entity	Gateway Entity
Resource Owner	Team that develops the API Server (Team Omega)
Resource Service	The API Server
Client	Team Bash's Gateway UI Client

Access to Amazon cloud costs money. Access to XSEDE supercomputers requires effort by the Resource Owner to acquire an allocation. Access to IU's Big Red and Karst are restricted to IU researchers. This is why the providers of the API server are OAuth2 Resource Owners.

In Summary, for Project Milestone 2

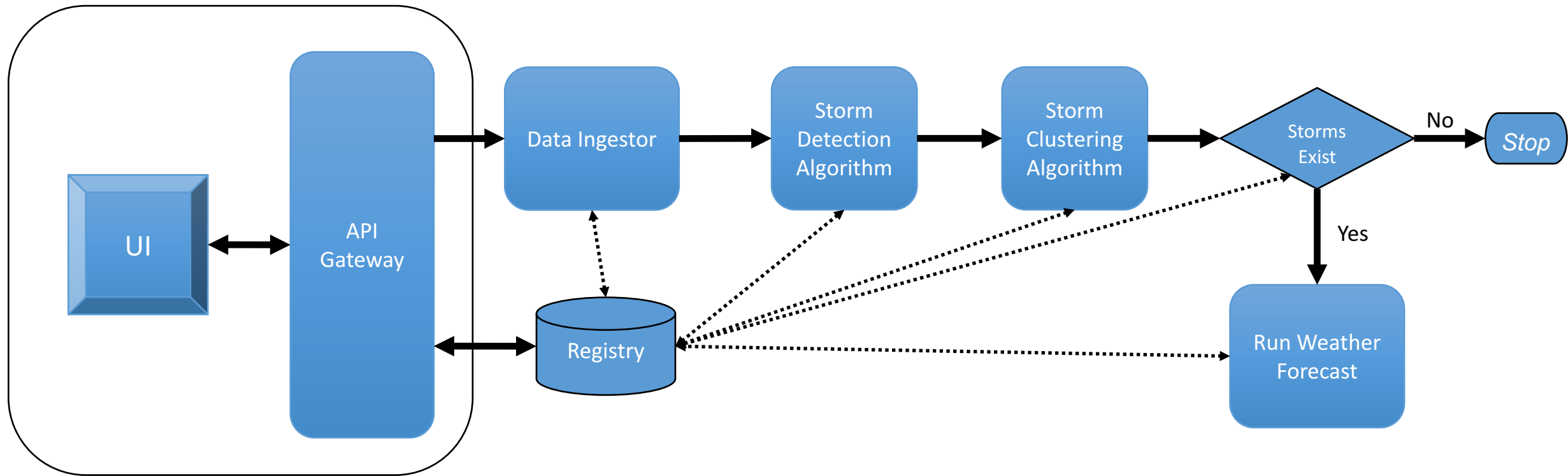
- Use an OpenID Connect provider to authenticate users and manage accounts.
- Set up HTTPS security between the Gateway Tenant and the API Server.

The General Solution



Our Conclusions About OAuth2 and Gateways

OAuth2 Grant Type	Science Gateway
Authorization Code	Web-based, server side gateway implemented with PHP, JSP/servlets, Django, etc. The Airavata client SDK is on the server under the gateway operator's control
Implicit	Client is a browser using JavaScript client SDKs to make direct connections to the Airavata server; no Web server in the middle
Resource Owner Password	Client is a trusted non-browser application under the user's control, such as a mobile device or a desktop application.
Client Credential	Machine-to-machine authentication



Science Gateways use OAuth2+OpenID Connect to establish trust between gateway clients and the API server.

- API Server is multi-tenanted. It's a platform.
- Gateways are clients to the API server
- Gateways have separate user bases.
- Gateways can be Web servers, desktop applications, or browser clients.