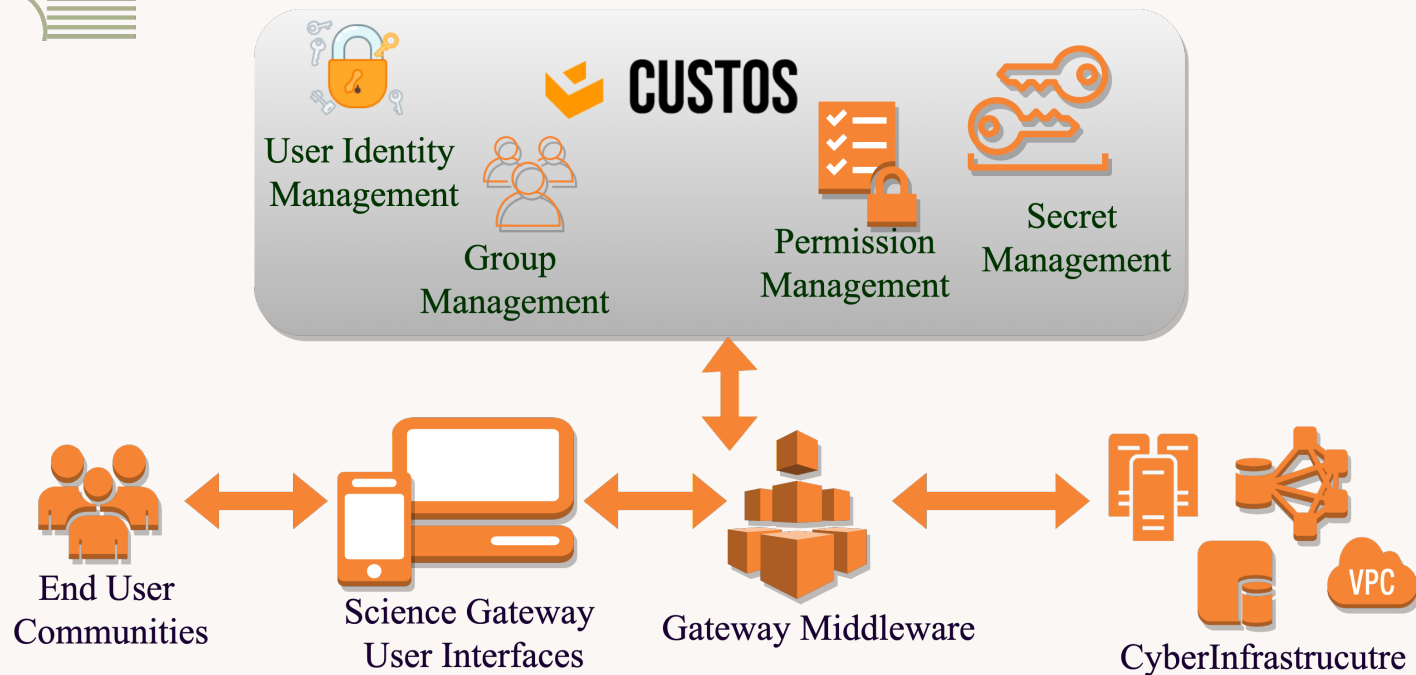# Science Gateway Integration Examples with the Custos Security Service

Isuru Ranawaka, Samitha Liyanage, Dannon Baker, Alexandru Mahmoud, Juleen Graham, Terry Fleurry, Dimuthu Wannipurage, Yu Ma, Enis Afgan, Jim Basney, Suresh Marru, Marlon Pierce
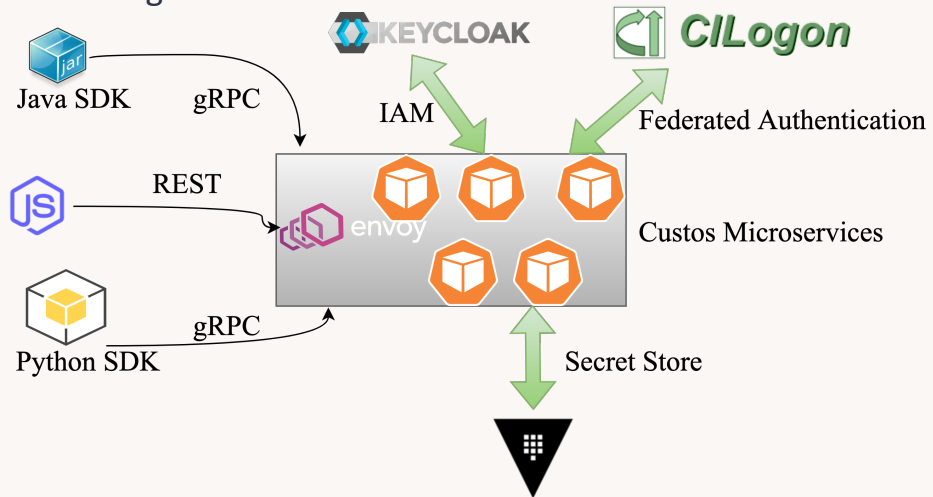
Science Gateways: Science-centric views to Cyberinfrastructure
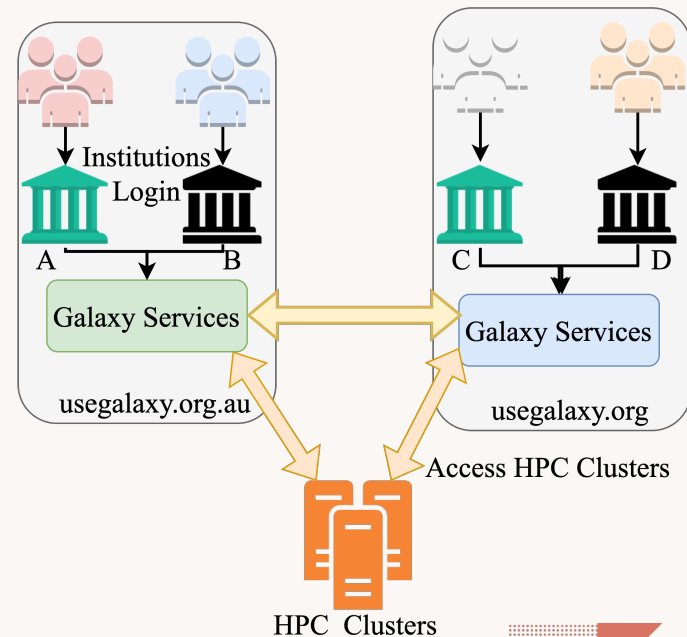
What is Custos?

- Open source security middleware for Science Gateways
  - Supports federated authentication via CILogon.
  - IAM solutions

- Deployed as a service on secured Indiana University network on behalf on Clients

Leveraging Custos: Galaxy

- Researchers from different institutions need to access Galaxy services through their institutional IDP
- Since there are vast number of institutions supporting all IDPs from Galaxy is not manageable.
- Custos provides CILogon based federation for Galaxy.
- Next step: Galaxy can use Custos to manage user-provided secrets, like API keys
- Big picture: Multiple Galaxy deployments can federate user accounts and permissions with Custos.
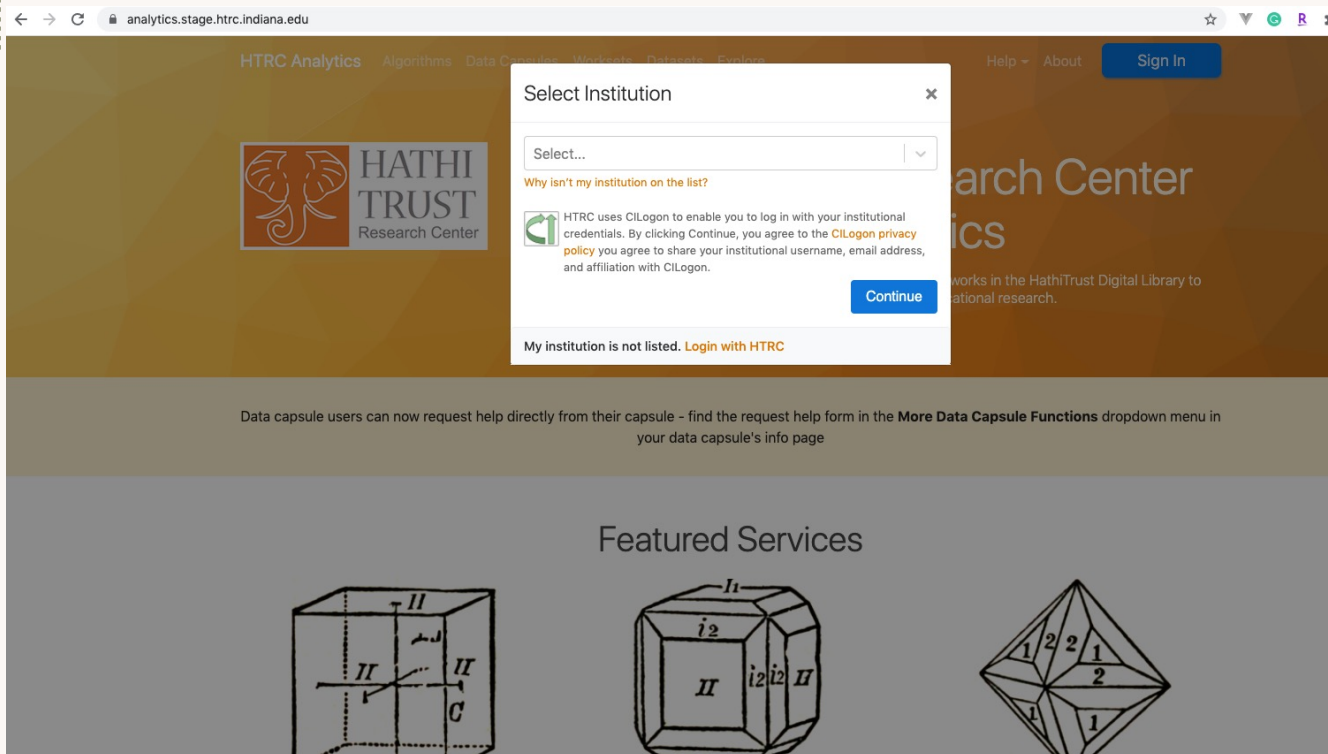
Galaxy using Custos

Leveraging Custos: HathiTrust Research Center

- Hathi Trust is the world largest nonprofit digital library in the world.
- Hathi Trust Digital Library and Hathi Trust Research Center are two separate entities
- Users from different Institutions need to access HTRC services and Digital Library Services through HTRC analytics gateway
- Custos provides federated authentication for HTRC analytics gateway and allows seamless access to services provided from both entities.
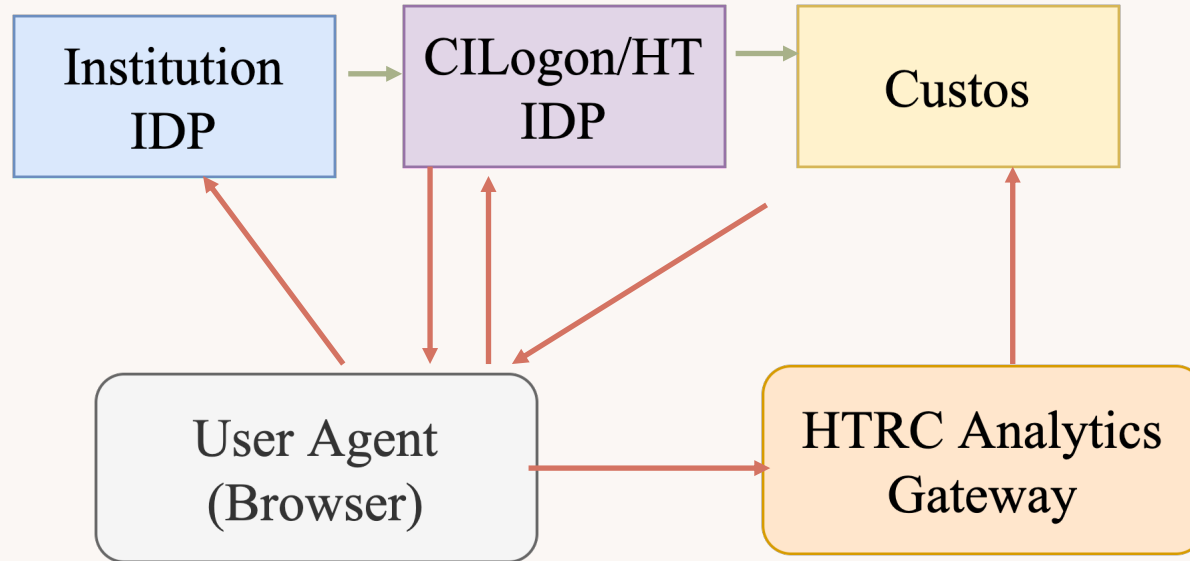
HTRC using Custos

User Identity Federation

Institution IDP → CILogon/HT IDP → Custos

User Agent (Browser) → HTRC Analytics Gateway

Beyond Identity Federation

- HTRC users need to analyze sensitive HT data

- HTRC does not allow to expose data to public.

- HTRC came up with Data Capsules which provides secured environment to load and analyze data

HT Digital Library

Secret Data

Analyze Data

Download data
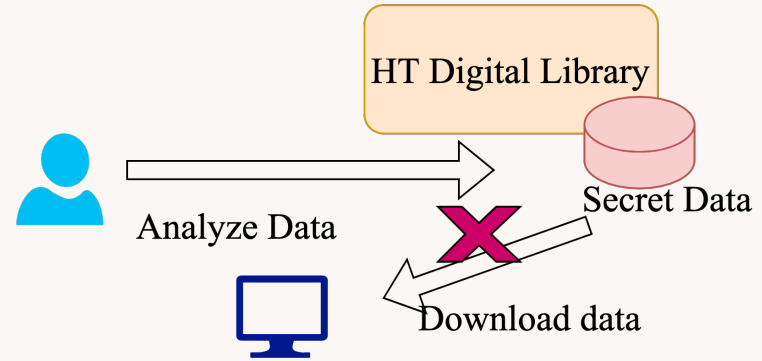
HTRC Data Capsule System
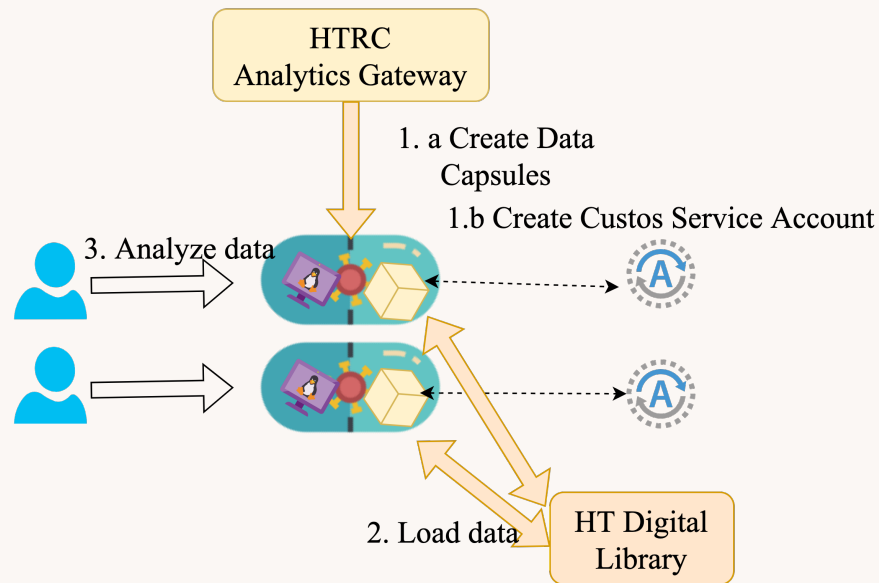
- Data capsules need to authenticate with HT data APIs to load data.
- Each data capsules needs to be audited and all operations carried out over data are logged.
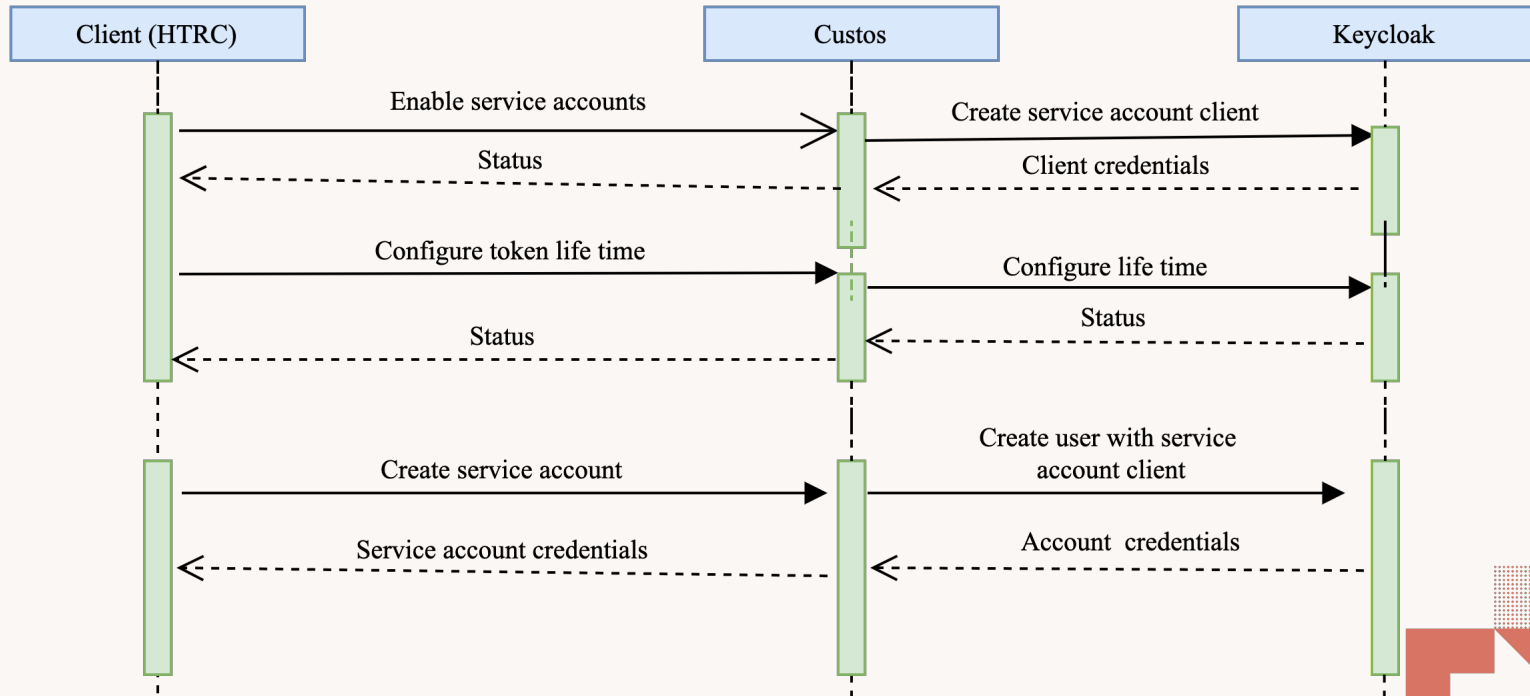- Custos provides service accounts-based authentication for Data capsules

HTRC Analytics Gateway

1. a Create Data Capsules

1.b Create Custos Service Account

3. Analyze data

2. Load data

HT Digital Library

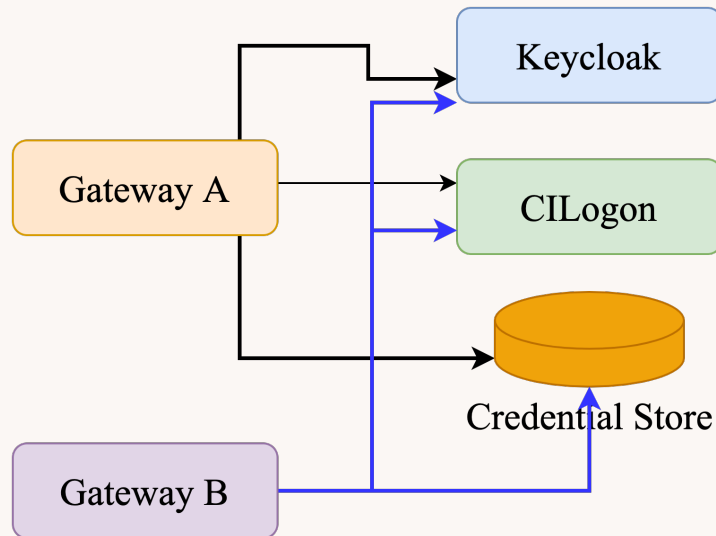# Ubuntu VM with preconfigured tools

Custos Service Accounts
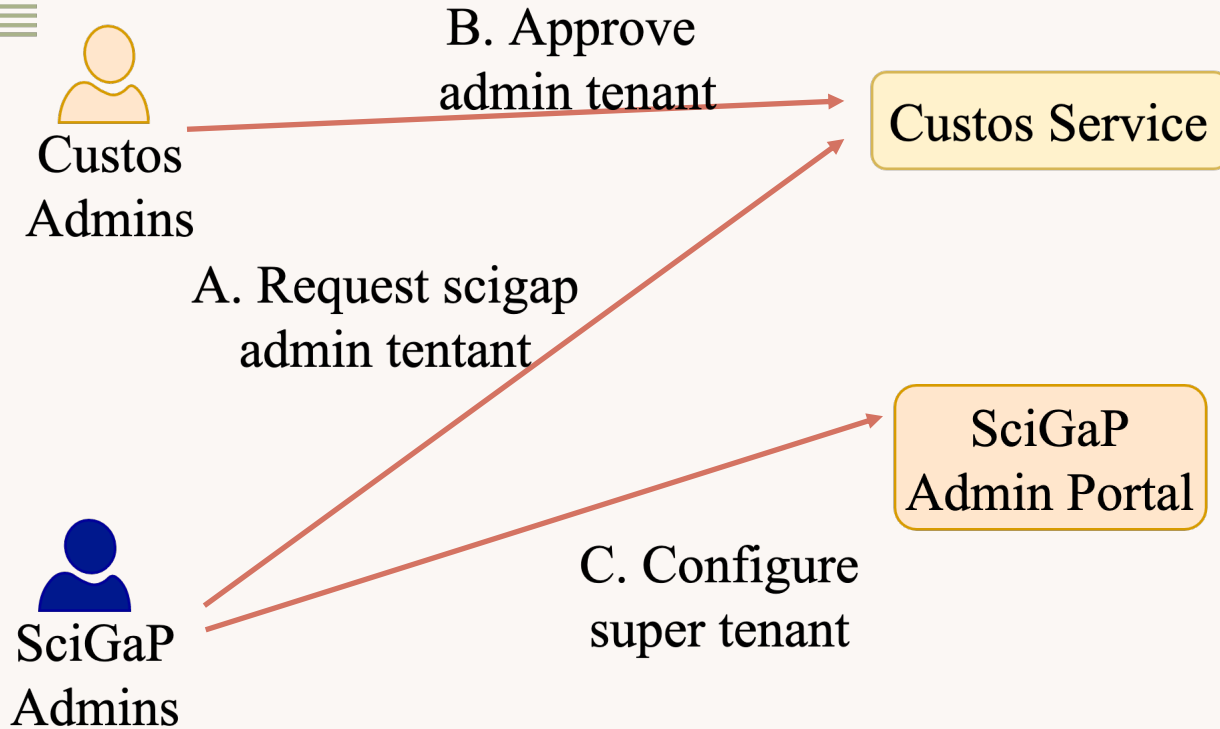
- Service Account Creation Process
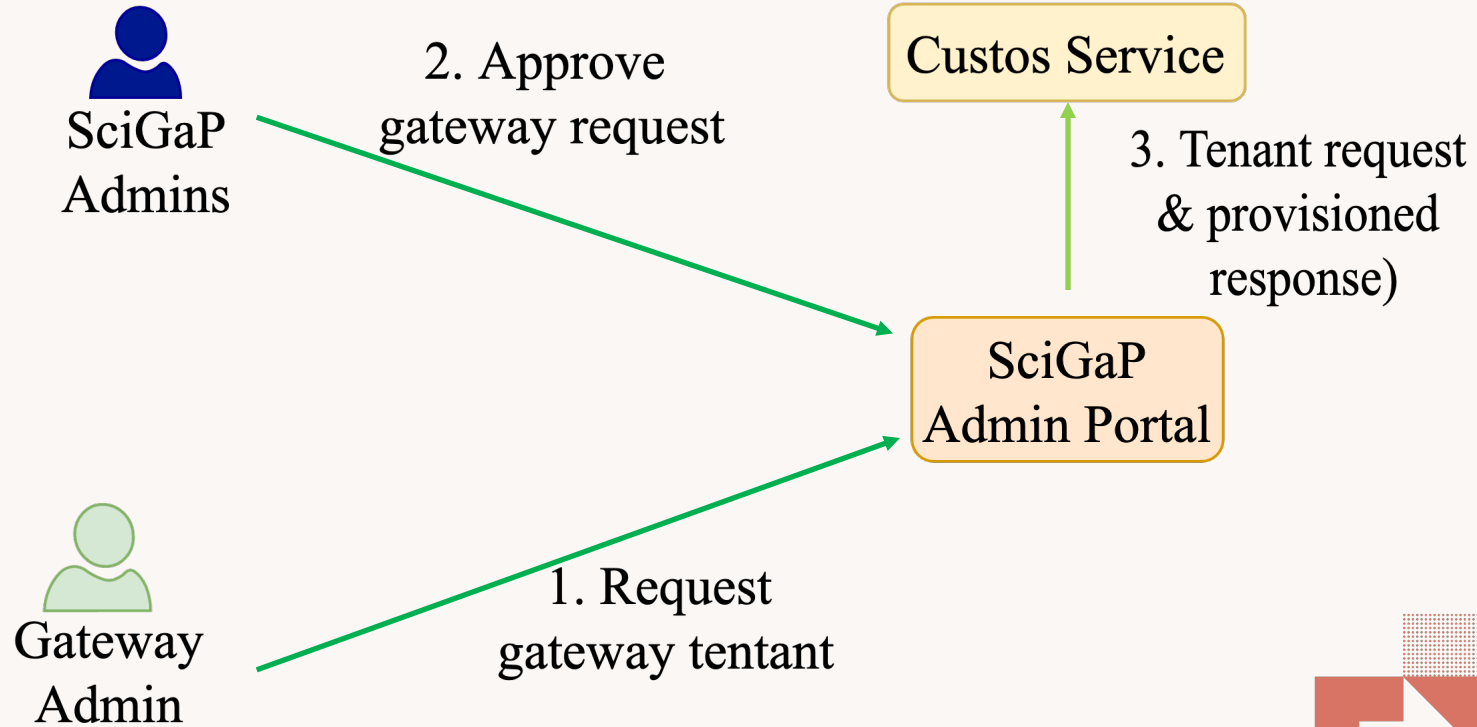
Apache Airavata Platform Integration

- SciGaP
  - Science Gateways Platform as a Service
    - Supports over 40 science gateways.
- Challenges
  - Manual creation of Keycloak Realm
  - Manually configure CILogon Client
  - Store credentials in local credential store
  - Repeat this procedure for all Gateways and
  - It's a time consuming process
- Solution: Replace Keycloak, CILogon and Credential Store with Custos Service
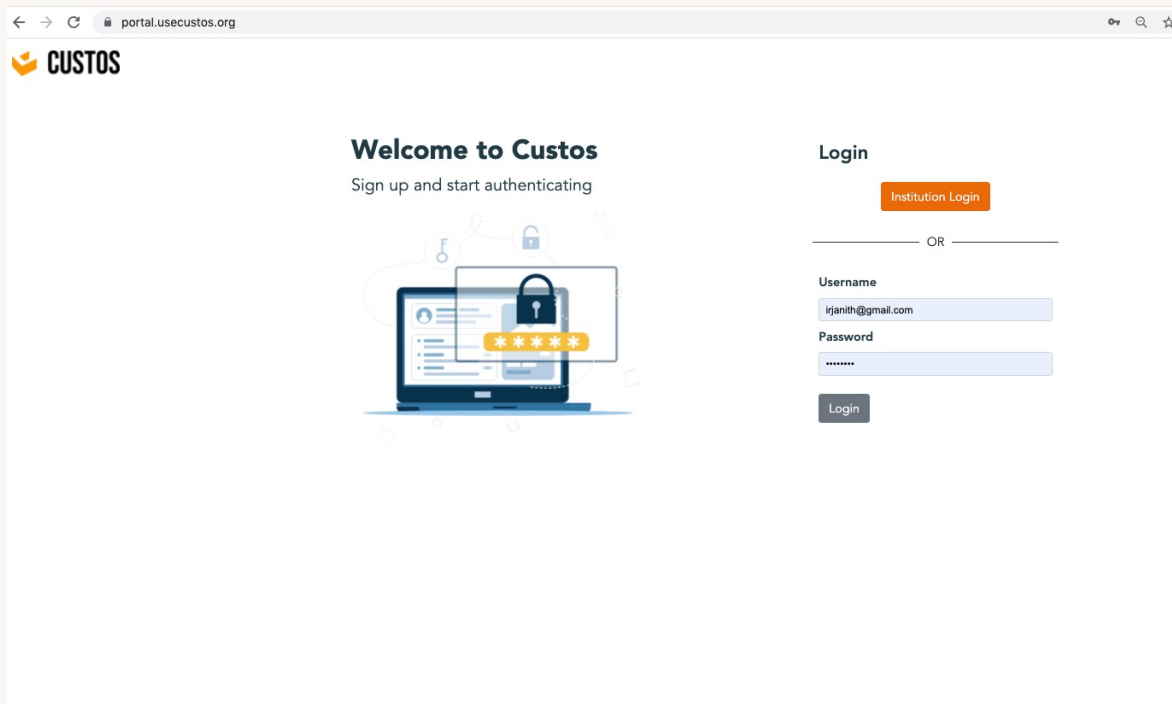
Custos supports automatic gateway provisioning

Custos
Admins

B. Approve
admin tenant

Custos Service

A. Request scigap
admin tentant

SciGaP
Admin Portal

C. Configure
super tenant

SciGaP
Admins

Cont...

SciGaP Admins

2. Approve gateway request

Custos Service

3. Tenant request & provisioned response)

SciGaP Admin Portal

Gateway Admin

1. Request gateway tentant

Custos Administrative Portal

- User interface for Custos operations

Tenant Dashboard

Conclusion

- Integration statistics
  - Federated authentication
    - Galaxy, HTRC, SciGaP
  - Secret management
    - Galaxy, SciGaP
  - Service Accounts
    - Galaxy, HTRC, Airavata MFT

- Subscribe Custos mailing list: custos-subscribe@airavata.apache.org

- Repository: https://github.com/apache/airavata-custos.git

Thank You