Federated Authentication and Credential Translation in the EUDAT Collaborative Data Infrastructure

Ahmed Shiraz Memon (JSC - DE)
Jens Jensen (STFC eScience - UK)
Ales Cernivec (XLAB - SL)
Krzysztof Benedyczak (ICM - PL)
Morris Riedel (HI - IS)

Cloud Federation Management Workshop, Dec. 8th, 2014
Outline

• Background
• Motivation & Goals
• Components of the AAI
• Authentication Architecture
• Service Interaction
• Data Staging Use case
• Conclusion
Background: The EUDAT Project

- EC funded FP7 Project
- Scientific User Communities: VPH, ENES, EPOS, CLARIN, LifeWatch
- Aims at providing the Data e-Infrastructure
  - Services: Safe Replication, Dynamic replication, Research Data Store, PID, Data Sharing, AAI
  - Internal Services: Wiki, JIRA, SCM, Portal, etc…
Motivation

• User communities have their own established Federated Identity Management Systems
• Multiple authentication protocols (SAML, X.509, OpenID Connect, LDAP)
• Registration of User required at each service - lead to maintenance overhead, attributes management, synchronization, etc…
Goals

• Intuitive authentication method (SSO, Username-Password)
• Support for interactive (e.g. User-Service) and automated (e.g. Service-Service) authentication
• Support for Browser and non-Browser clients
• Delegated access of host and Web portal to data services
• Translation between authentication tokens
• Harmonisation of attributes from “multiple” attribute providers
Main Components of AAI

- Unity
- OAuth 2.0 Authorisation Server
- Online CA (SLCS)
- Web Portal / Certificate Client
- Identity Provider
- B2-<*> Services
Unity

• Complete Authentication and Identity Management solution
• Manage users, users attributes, and group membership
• Support multiple authentication protocols: X.509, OpenID-Connect (OIDC), SAML 2.0 (SOAP and WebSSO)
• Proxy IdP Pattern: simultaneous roles in AuthN flow i.e. SAML SP and SAML/OIDC IdP at the same time
• Advanced support for
  – designing user registration forms
  – Translation profiles
• Developed at ICM / University of Warsaw
• Increasing take-up: HBP, LSDMA, EUDAT, PL-Grid
Contrail OAuth 2.0 Framework

• Developed within FP7 Contrail Project
• A reference implementation of OAuth 2.0 Framework
• Authentication of users (Resource Owners) is based on SAML WebSSO, thus exposed as SAML Service Provide
• Supported “Grant” types: Authorization Code and Client Credentials
• Provision to manage tokens, clients, and users
Contrail Online CA

• Issues short-lived X.509 credentials to the portals (on user’s behalf)
• An “OAuth 2.0 Resource Server”
• X.509 Credentials are useful for authentication as well as authorisation
  – How? Embeds user’s attributes inside the certificate extensions
• Queries the user attributes from Unity via its SOAP query interface
Other components

• Community Web Portal / Certificate Client
  – A gateway to the EUDAT federation
  – An OAuth client
  – Asks for user consent, generate CSR, and post it to the online CA
  – Use certificate wher/n-ever necessary to perform operations on user’s behalf, e.g. GridFTP transfers

• Identity and/or Attribute Providers
  – Resides at home institutes
  – Authenticates users
  – Provides attributes to trusted SAML SPs

• B2-<*> Services
  – Data management services offered to the scientific user communities
AAI Architecture

Unity

OAuth2 AS

Online CA

Identity Provider

Community Portal/Certificate Client

B2SHARE

B2SAFE

B2FIND

B2STAGE

OAuth Resource Server

SAML

OAuth Client

SAML Authorization Server

SAML IdP

OAuth Authorisation Server

OAuth IdP

Query Attributes

Request Access token

Validate Access token

Request X.509 Cert.

Create, Share, Stage, Find Data
Authentication Flow
Credential Translation Flow

1. **Browser** requests an X509 certificate.
2. **Community** creates a CSR.
3. **AuthZ Server** sends access token, username (or UUID) and CSR.
4. **CA** validates the access token.
5. **Validation confirmation + Token's meta information** is sent back.
6. **CA** embeds user attributes inside the certificate.
7. **Certificate** is issued.
8. **Unity** uses the certificate for access.
Use case: Data Staging with Federated Identities

• Goal: Moving data between EUDAT and PRACE infrastructures using “Federated Identities”

• Different authentication protocols
  – EUDAT: Username/Password
  – PRACE: X.509

• Options
  – PRACE trusts EUDAT online CA and map/link DNs
  – PRACE issues new credentials to the EUDAT users and DCAU to establish an authentication session between the endpoints + establish a trust relationship
  – Not relying on the user credentials; instead an automated client that has a robot certificate and performs the transfer
AAI as a Framework

- Powerful framework sufficiently enough to address EUDAT Communities’ requirements and based on loosely coupled components that can be replaced and used independently
- Technically interoperable while adopting standards
- Also, a need to understand semantic interoperability, i.e. different understanding of attributes and policies – harmonisation
- EUDAT carefully follows FIM4R (RDA FIM) and eduGAIN to understand the implementation of policies
- Address “federated” authorisation challenges
Conclusion

• Federated AAI evolved from Contrail and Unity projects
• Combined diverse technologies: SAML, OpenID, OpenID-Connect (OAuth) and X.509, to address integration requirements
• It offers both Web and command line authentication
• Supports delegation
  – Coarse grained via OAuth
  – Fine grained with SAML push attributes
• Learn from other e-Infrastructure projects (e.g. XSEDE, HBP, ESFRIs)
Thanks!!!

Questions???