Authentication & Authorisation Infrastructure

Paul Millar

paul.millar@desy.de

on behalf of Andrea Ceccanti, Bas Wegh and Marcus Hardt.

(with many slides taken from Andrea's earlier talks)
Architecture: a quick reminder

Marcus wants to access some service at INDIGO service.
Architecture: a quick reminder

INDIGO Services sees that Marcus is not authenticated, and redirects him to INDIGO IAM for authentication.
Architecture: a quick reminder

Marcus

INDIGO Service

redirect to IAM for AuthN

Home IdP

Indigo IAM
IAM lets Marcus choose how he wants to authenticate

Marcus chooses his Home IdP

redirect to IAM for AuthN

IAM lets Marcus choose how he wants to authenticate

Marcus chooses his Home IdP
Architecture: a quick reminder

Marcus

INDIGO Service

redirect to home IdP for AuthN

Home IdP

Indigo IAM
Architecture: a quick reminder

Home IdP authenticates Marcus and sends back an AuthN assertion.
Architecture: a quick reminder

IAM validates assertion. Marcus is now authenticated at IAM.
Architecture: a quick reminder

Marcus

INDIGO Service

send back to IS
OIDC authz code

Home IdP

Indigo IAM
Architecture: a quick reminder

Marcus

INDIGO Service

exchange authZ code
for OIDC ID-token
access token

Home IdP

Indigo IAM
Architecture: a quick reminder

IS validates ID-Token. Marcus is now authenticated at IS.
Architecture: a quick reminder

IS requests additional profile information about Marcus from IAM user info endpoint.
Group membership

- Once logged in, a user can add 3rd party group membership information.
  
  (group membership not asserted by IdP/OIDC/...)
- IAM can act as a group service.
- User is redirected to the group server, authenticates (any IAM supported mechanism), and is asked which groups they wish to assert membership:
  - Support selective assertions (e.g., admin role),
  - IAM will support “hosting” multiple organisations (like VOMS supports multiple VOs),
  - IAM will support contacting multiple group-membership services.
Delegation: acting on behalf ...

- Delegation is some third-party acts on behalf on the user.
- For example:
  - web-portal acting on behalf of the user,
  - running image acting on behalf of the web-portal,
  - Storage system (3rd party transfer) staging in data on behalf of running image
- Plan to use Macaroons as OAuth access token
  Allows easy and safe delegation
- Additionally:
  - Supporting long-lived activity via refresh tokens,
  - Broadening of access-token, if use-cases require it.
Course-grain authorisation
Reminder: IAM
IAM: status and future work

• Work at CNAF and CESNET
  - CESNET implements SCIM notification; CNAF implements IAM.

• Coding of IAM starting in January; targets are:
  - Support for SAML & OIDC authentication,
  - Basic user registration and management,
  - Basic user provisioning,
  - Basic support for delegation.

• Will deploy a test IdP (for developers)
• C.I./C.D. instance to allow integration tests
• Allow creation of users from GitHub/Google accounts, once OIDC is supported
• Currently only 1 of 2 posts filled at CNAF; discussion under on how to minimise the impact.
Reminder: TTS
TTS: status and future work

• Work focused at KIT
• Currently: writing low-level requirements.
  – Targeting both web service and RESTful interface.
• Initially will support:
  – ssh key-pair,
  – S3 key (locally hosted S3 app, NOT Amazon),
  – X.509 + VOMS (local use-case).
• Anticipate code ready at beginning of March
  – Test instance available for integration tests
Idea: provide AAI support to IaaS

- LIP and Padova both provide IaaS testbed services for WP4
- Good opportunity to test AAI infrastructure
  
  “Eat your own dog-food”

- OpenStack / KeyStone already has OIDC support
  - Need to evaluate it, and how we can leverage it to integrate with INDIGO AAI

- Open question about Open Nebula:
  
  Account creation may use "autocreate" feature in OpenNebula, or use provisioning to create new accounts.

- Good opportunity to try out IAM CI/CD instance.
DEMO-1: AAI Questions

- Where is authentication needed?
- Where is delegation needed?
- Where is authorisation needed?
- Where is user information provisioning needed, and with which granularity?
- Which different user roles are required?
- Do we need to showcase registration functionalities?

These are questions specifically for the functionality we want to demo.
Backup slides