INDIGO – DataCloud

INDIGO-AAI
an overview

Andrea Ceccanti
INFN
andrea.ceccanti@cnaf.infn.it

on behalf of the INDIGO AAI task force
The INDIGO consortium

- 26 partners from 11 countries
- The hexagon contains the partners involved in development activities
- 11 M€ of total funding by the EC
- 4 Big private companies

From the EC Evaluation summary report:

“The consortium is of exceptional quality, and complementary, and with good relevant experience and skills.”
Since the very beginning we identified key issues with both Grid and Cloud technologies that prevented scientific communities an easy and optimal exploitation of data and compute resources.

We therefore decided to propose the development of a software platform centered around two of the EINFRA-1-2014 pillars:

- Large scale virtualization of data/compute center resources. This became the focus of INDIGO WP4.

- Development and adoption of a standards-based computing platform (with an open software stack). This became the focus of INDIGO WP5.
INDIGO WP structure

Figure 4: Diagram showing the interrelation among the Work Packages
The INDIGO approach

- Based on Open Source solutions
  - widely supported by big communities

- whenever possible exploit general solutions instead of specific tools/services
  - or put effort in increasing the generality of tools developed in a given community
  - this will be important for sustainability of the architecture

- ensure that the framework offered to final users, as well as to developers, will have a low learning curve
  - existing software suites like ROOT, OCTAVE/MATLAB, MATHEMATICA or R-STUDIO, will be supported and offered in a transparent way
The AAI problem

- Heterogeneous infrastructures use heterogeneous authentication/authorization mechanisms
  - Hard to integrate resources from distributed infrastructures without common AAI ground

- Even where a single authentication technology is used, managing user and privileges on distributed resources in a **dynamic** and secure way is complex

- DCIs are not yet easily and securely accessible from common users
  - Federated identity support lacking or very limited
How can we have common authN and authZ primitives that “just work” across several distributed infrastructures?

Which tools should we provide to our users so that they have complete control on how authN and authZ is configured and performed on the resources (assembled from distributed providers) they will use for their research?

How do we avoid reinventing the wheel? How do we exploit what is already available, leverage existing standards and ensure that what we develop is sustainable?
AAI concepts recap
Authentication & Authorization

Slide courtesy of Paul Millar
AuthZ without AuthN

Photo by Alan Cleaver (CC-BY)

Slide courtesy of Paul Millar
Delegation
INDIGO AAI challenges

Identity layer

- Support multiple AuthN mechanisms
- Harmonise Identity
  - One INDIGO identity for multiple authN mechanisms
  - Provide a persistent INDIGO identifier to services
- Support group membership and attributes
- Reduce integration complexity
Authorization

- Support controlled delegation of privileges by design
- Provide tools to define, propagate, compose and enforce authorization policies based on identity attributes at various levels of the INDIGO stack
- Uniform and consistent authZ over resources assembled from multiple, heterogeneous providers
Identity in INDIGO

- The INDIGO identity layer speaks OpenID-connect
- The INDIGO Login Service is an OIDC provider
  - Authenticates users with supported AuthN mechanism
    - SAML, X.509, OIDC
  - Provides access to identity information through standard OIDC interfaces
- Can be seen as a first credential translation step
Why OpenID connect

- Standard and widely adopted in industry
  - Don’t reinvent the wheel
- Lots of things we need are covered and standardized
  - Discovery
  - Dynamic Registration
  - Distributed/Aggregated claims
  - Session management
  - Token revocation
- Friendly for mobile apps
- Reduced client integration complexity
INDIGO AuthN flow

Marcus wants to access some service at INDIGO service

Marcus wants to access some service at INDIGO service

Home IdP

Indigo IAM
INDIGO AuthN flow

INDIGO Services sees that Marcus is not authenticated, and redirects him to INDIGO IAM for authentication.
INDIGO AuthN flow

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.

Indigo IAM

Home IdP
INDIGO AuthN flow

Indigo IAM

INDIGO Service

Marcus

Home IdP

redirect to home IdP for AuthN

Indigo IAM
INDIGO Service

Home IdP authenticates Marcus and sends back an AuthN assertion

INDIGO AuthN flow
INDIGO AuthN flow

IAM validates assertion. Marcus is now authenticated at IAM.
INDIGO AuthN flow

Marcus

INDIGO Service

send back to IS
OIDC authz code

Home IdP

Indigo IAM
INDIGO AuthN flow

Home IdP

Indigo IAM

INDIGO Service

Marcus

INDIGO - DataCloud

exchange
authZ code
for OIDC ID-token
access token
INDIGO AuthN flow

IS validates ID-Token. Marcus is now authenticated at IS.
INDIGO AuthN flow

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

Indigo IAM

Home IdP

INDIGO Service

$
Authorization in INDIGO

- OAuth 2.0
  - Decouples authentication from authorization
  - Designed for delegated authorization, but **not** limited to it

Diagram:

- (A) Authorization Request
  - (B) Authorization Grant
  - (C) Authorization Grant
  - (D) Access Token
  - (E) Access Token
  - (F) Protected Resource
INDIGO services are modeled as APIs that trust an OAuth Authorization Service.

In order to access resources, a client needs an access token.

OAuth scopes used to:
- Target the token to specific APIs
- Provide hints for local AuthZ

Identity layer provides other attributes as base for AuthZ decisions.
Delegation in INDIGO

- OAuth is **all** about delegating authority to a service to act on resources the user owns at another service
  - Scopes enable fine-grained controlled delegation of privileges
  - refresh tokens enable offline delegated access

- We plan to make this delegation model more flexible and secure for longer delegation chains by leveraging **macaroons** as OAuth tokens
  - macaroons are bearer tokens that can be further constrained along the delegation chain to limit their authority and the context of their applicability
The IAM service

- Provides the tools needed to enable a secure composition of services from multiple providers in support of scientific applications
- Provides a unified view on identities and privileges on resources assembled from various providers
- Supports and integrates existing fed authN mechanisms
- Provides tools to define and manage enrollment flows for research communities
How to integrate external services like S3?

INDIGO Token Translation Service

- maps INDIGO identity & attributes to external service credentials
- plugin-based architecture
Next steps

- Start development and integration according to the INDIGO workplan

- First official INDIGO release expected end of July, 2016
  - but we will start make available services as soon as they are ready enough to be tested
Thanks!

Questions?

indigo-aai-tf@lists.indigo-datacloud.eu