Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
ICSC Centro Nazionale di Ricerca in HPC, Big Data and Quantum Computing

Roadmap per l'integrazione delle piattaforme cloud Spoke8 e Spoke0 Gestione delle Identità e degli Accessi

Francesco Giacomini (INFN–CNAF)

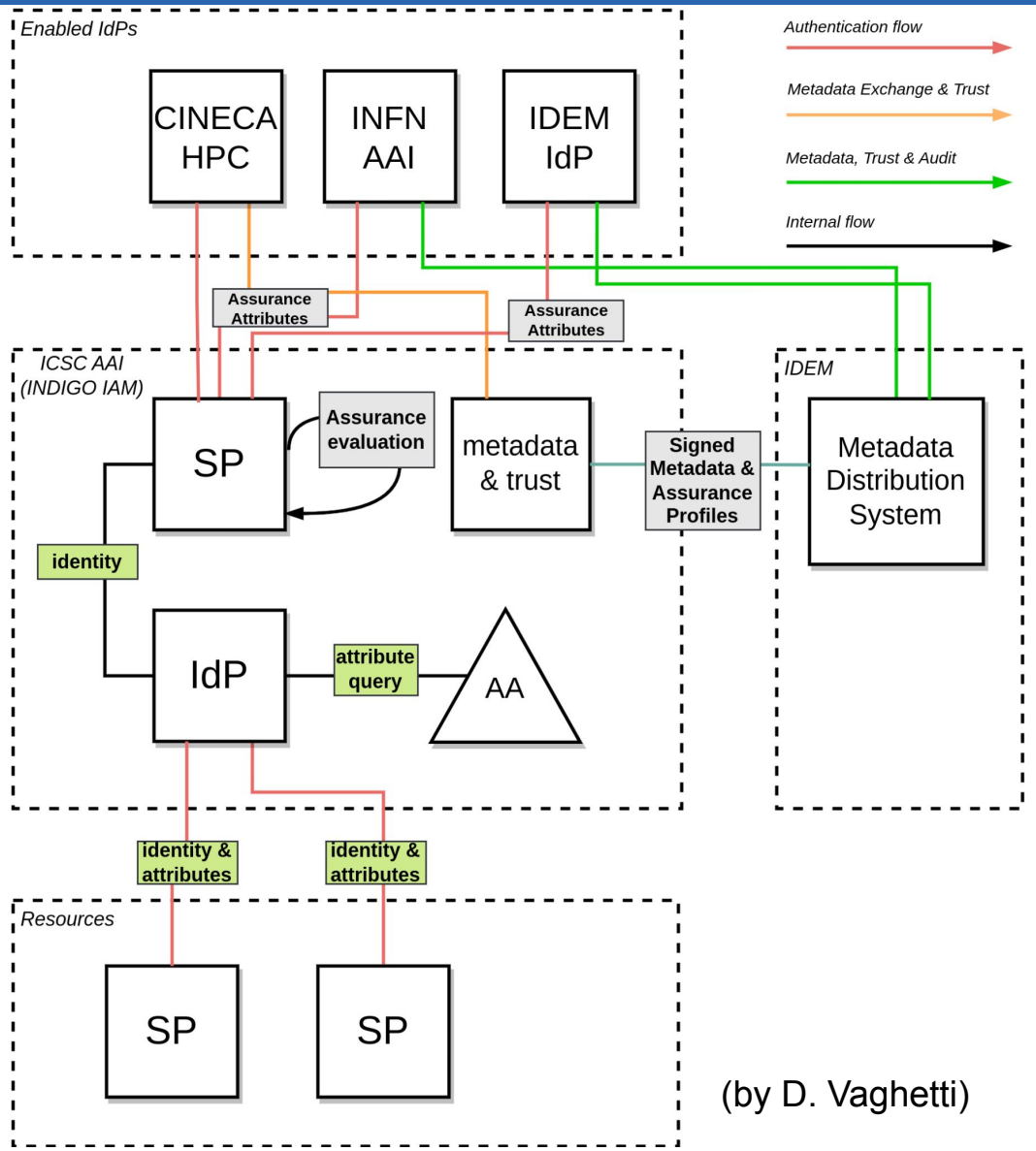
Incontro Plenario Spoke8, CINECA, 24-25 giugno 2024

Outline

1. Where we want to go
2. Where we are
3. Brief intro to INDIGO-IAM
4. How to grant access to a resource

Where we want to go

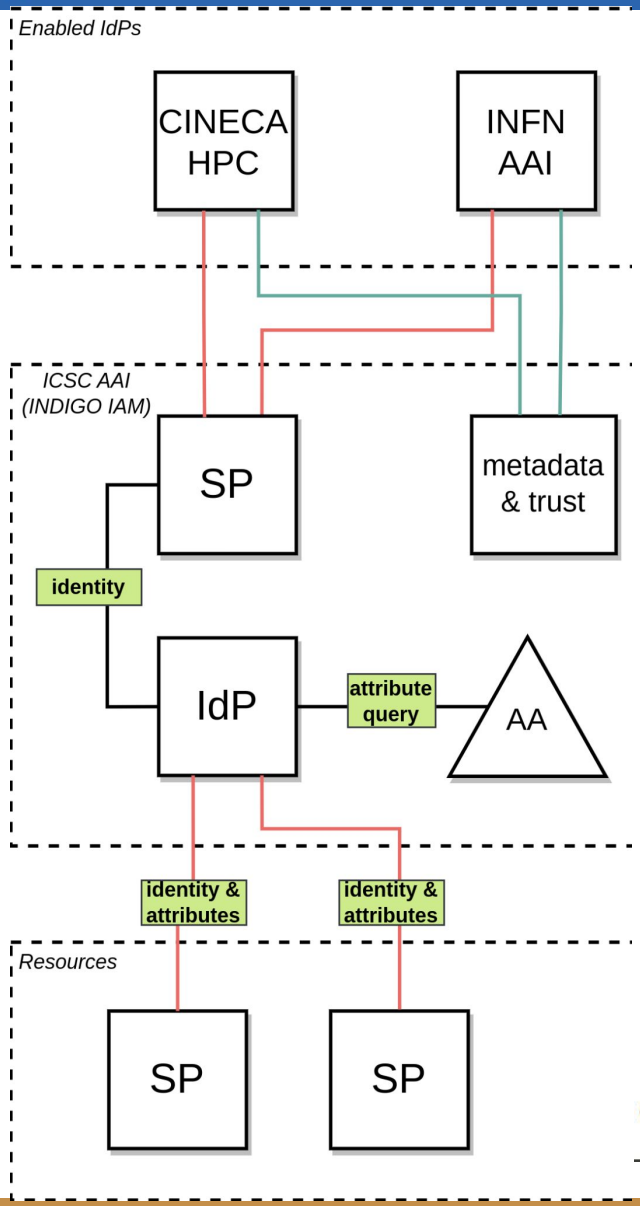
- Authentication via a home institute identity provider
  - possibly in a federation (SAML or OIDC)
- High levels of identity assurance
  - including multi-factor authentication
- Support for management of organization and project membership
- Access to resources is granted based on authorization tokens issued by the ICSC AAI
  - ideally no need to have local personal accounts

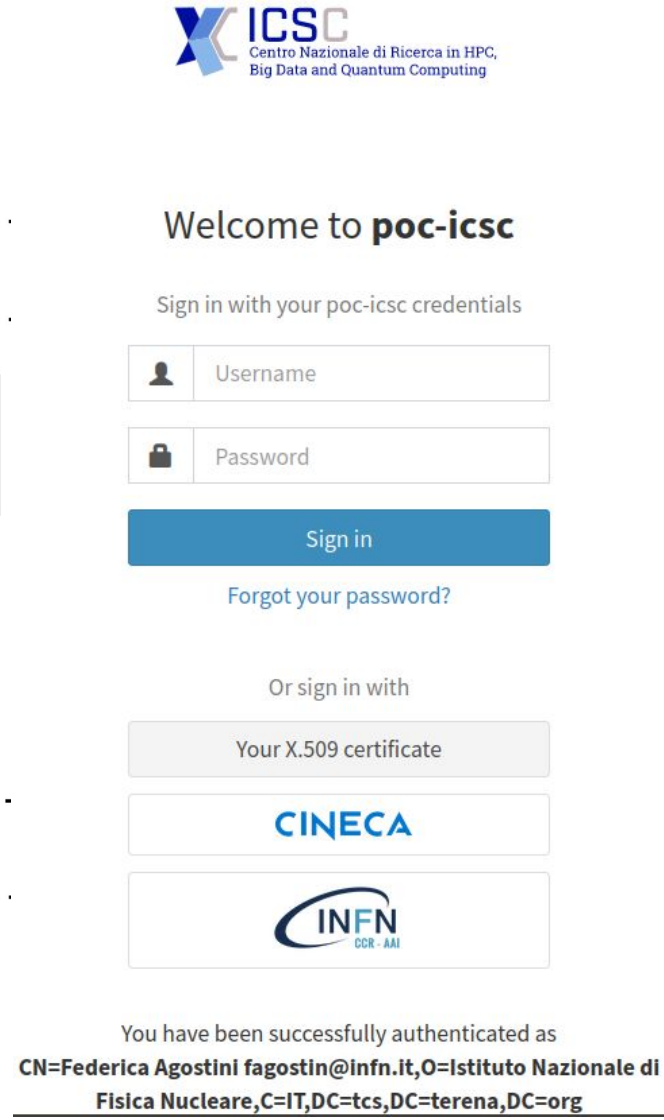


(by D. Vaghetti)

Where we are

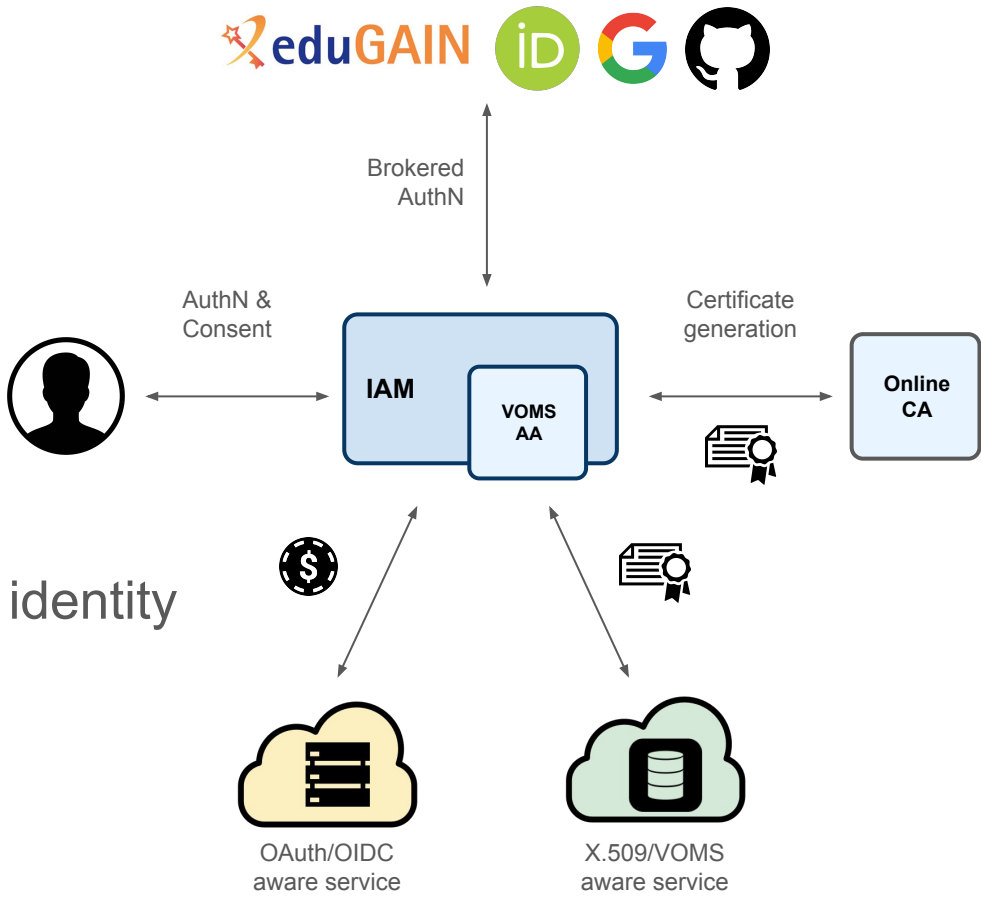
- Proof-of-concept Spoke0/TeRABIT
- Authentication via CINECA and INFN IdPs
  - OIDC and SAML respectively
- INDIGO-IAM as ICSC AAI
  - User enrollment
  - Groups, roles, attributes
  - Access Policies
- Tokens issued by IAM grant access to computing and storage resources
- Personal account still needed at CINECA





INDIGO-IAM in one slide

- Standard OAuth2 Authorization Service and OpenID Connect Provider
  - Easy integration with (web) applications
- Java application based on the Spring Boot framework
- Multiple authentication mechanisms
  - SAML, OpenID Connect, X.509, username/password
- Account linking
- Moderated and automatic user enrollment
- Enforcement of AUP acceptance
- Management of organization membership
- Issuance of JWT tokens and X.509 Attribute Certificates with identity and membership information, attributes and capabilities
- Typically deployed as a Docker container
- Design choices rely on 20+ years of experience on large geographically-distributed federated systems (Grid)



How to grant access to a resource?

- Two basic models
  - **identity-based**: the credentials presented at a resource contain identity information (subject, groups, roles, attributes) that are mapped to specific permissions at the resource
  - **capability-based**: the credentials presented at a resource already contain the permission to do something at the resource
- INDIGO-IAM supports both models
  - To support the capability-based model, IAM includes a *Policy Engine*
  - What model is good for ICSC and Spoke8 specifically?
  - WLCG (the Grid of High-Energy Physics experiments) is moving from the identity-based to the capability-based model