INFN AAI-related activities in EGI ACE

Andrea Ceccanti

EGI ACE WP7.3 meeting

Sept 21st, 2021

INFN AAI-related activities

Evolve INDIGO IAM to support EOSC AAI standards and emerging community requirements (WLCG and others)

Work, in collaboration with GRNet, on the implementation of key features in Keycloak

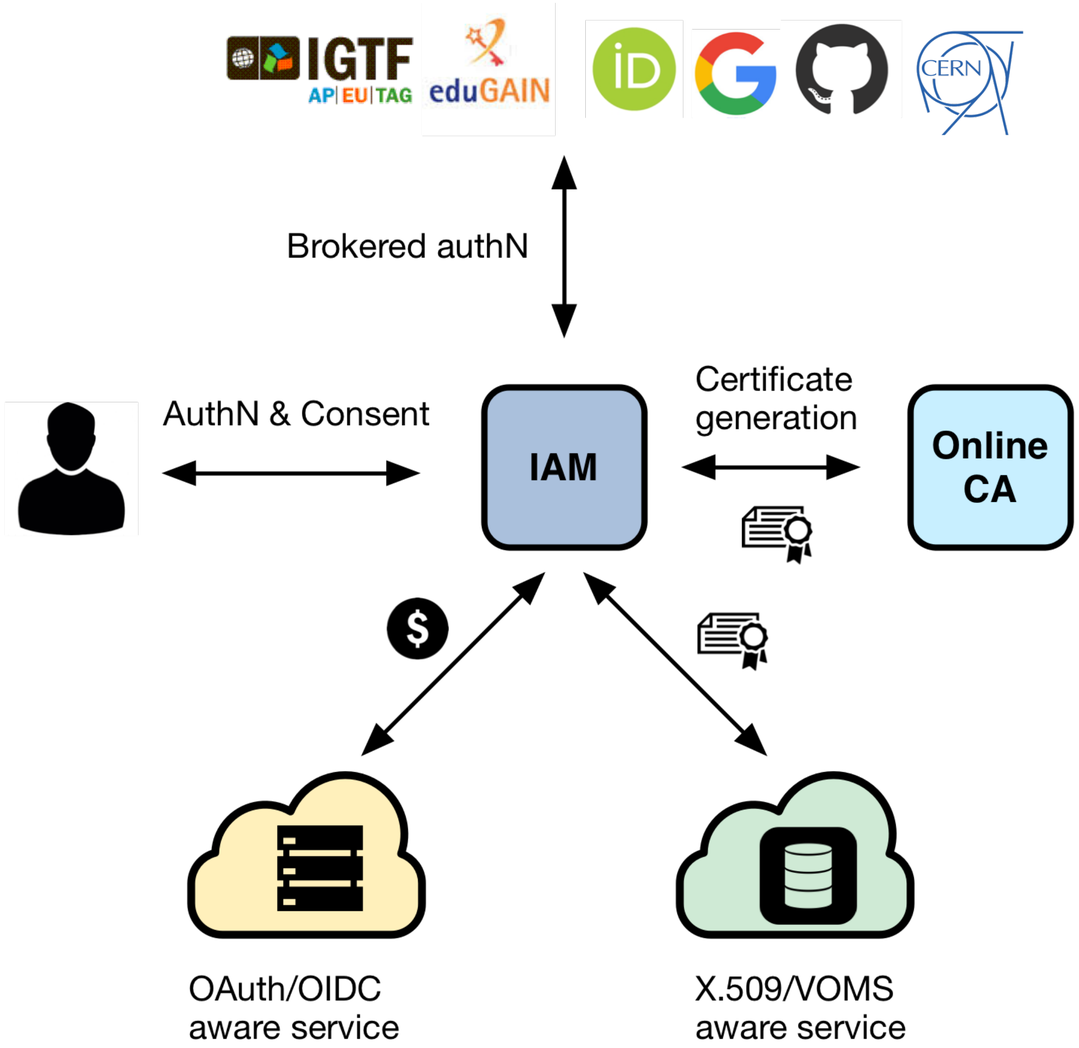
- e.g., integration with SAML identity federations

INDIGO IAM

INDIGO Identity and Access Management Service

An authentication and authorization service that

- supports **multiple authentication mechanisms**
- provides users with a **persistent, organization scoped** identifier
- exposes **identity information**, **attributes** and **capabilities** to services via **JWT** tokens and standard **OAuth & OpenID Connect** protocols
- can integrate existing **VOMS**-aware services
- supports **Web** and **non-Web access**, **delegation** and **token renewal**



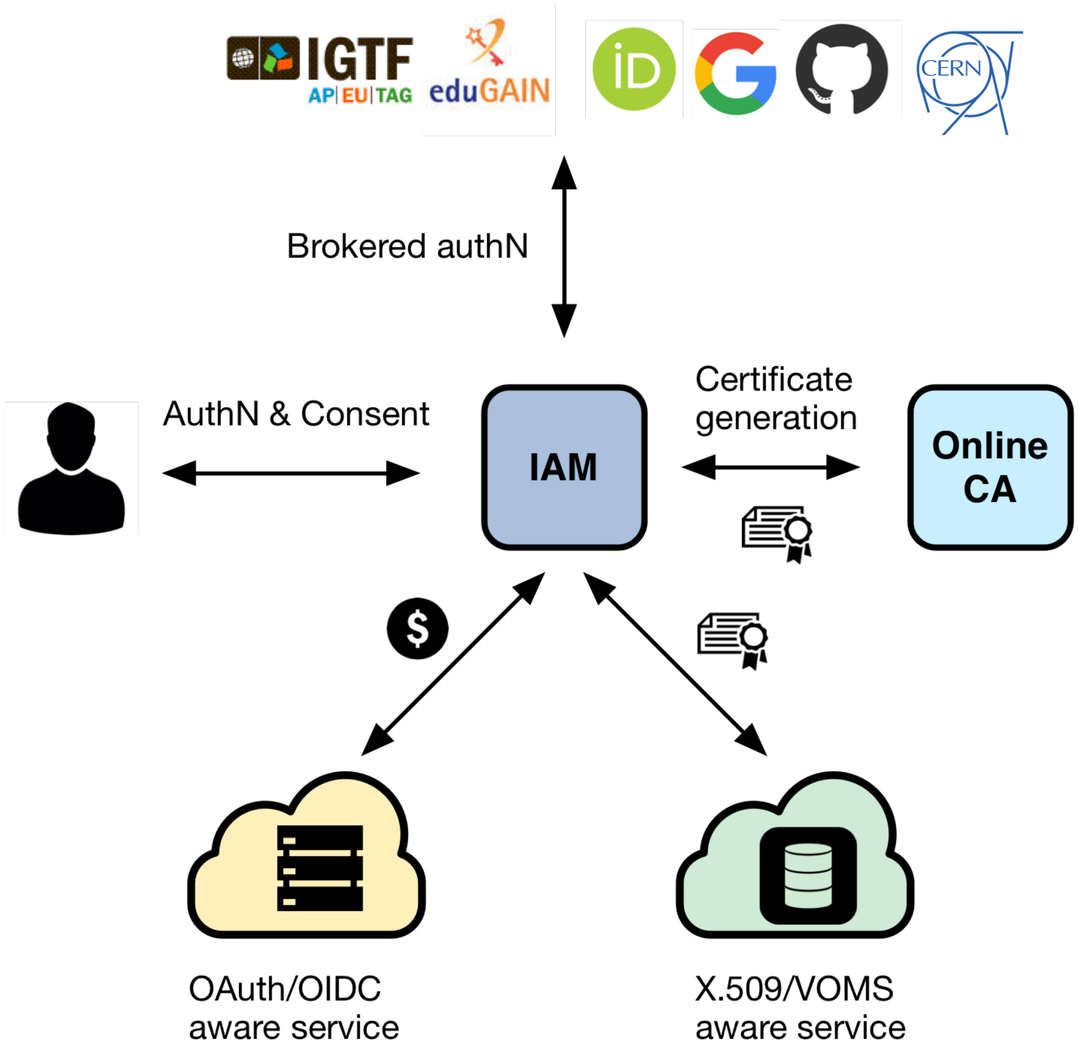
INDIGO Identity and Access Management Service

First developed in the context of the **H2020 INDIGO DataCloud** project

Selected by the WLCG management board to be the core of the future, token-based WLCG AAI

Sustained by INFN for the foreseeable future, with current support from several EU projects:

- ESCAPE, EOSC Pillar, EOSC-Future, EGI-ACE



Main recent developments

New IAM website

- with restructured and improved documentation

Improved token-exchange flexibility

- support for scope policies and token exchange policies

Support for linking SSH keys to IAM accounts

- keys are then exposed to relying apps via SCIM provisioning APIs or accessible presenting a token

More details in release notes

- https://github.com/indigo-iam/iam/releases/tag/v1.7.0
- https://github.com/indigo-iam/iam/releases/tag/v1.7.1

Main planned developments

Improved handling of client applications

- Fix scalability issues in MitreId client-management APIs
- Add ability to disable and expire clients

Support for the OAuth resource indicators standard

- TLDR: a standardised way for clients to request that issued tokens are limited to a specific audience

Group membership expiration

Keycloak

Keycloak and SAML identity federations

Keycloak SAML support works fine with single IdPs, but does not handle large identity federations nicely

Most people using Keycloak delegate EduGAIN integration to an external proxy

We’re working on implementing native support for large-scale identity federations in Keycloak in collaboration with GRNet

https://github.com/eosc-kc/keycloak/issues

Thank you.
Questions?