

# Identity and Access Management with the INDIGO IAM service

Andrea Ceccanti

[andrea.ceccanti@cnafe.infn.it](mailto:andrea.ceccanti@cnafe.infn.it)

FIM4R Mini Workshop

Femilab, Sept. 12th 2019



# INDIGO Identity and Access Management service

## Flexible authentication support

- (SAML, X.509, OpenID Connect, username/password, ...)

## Account linking

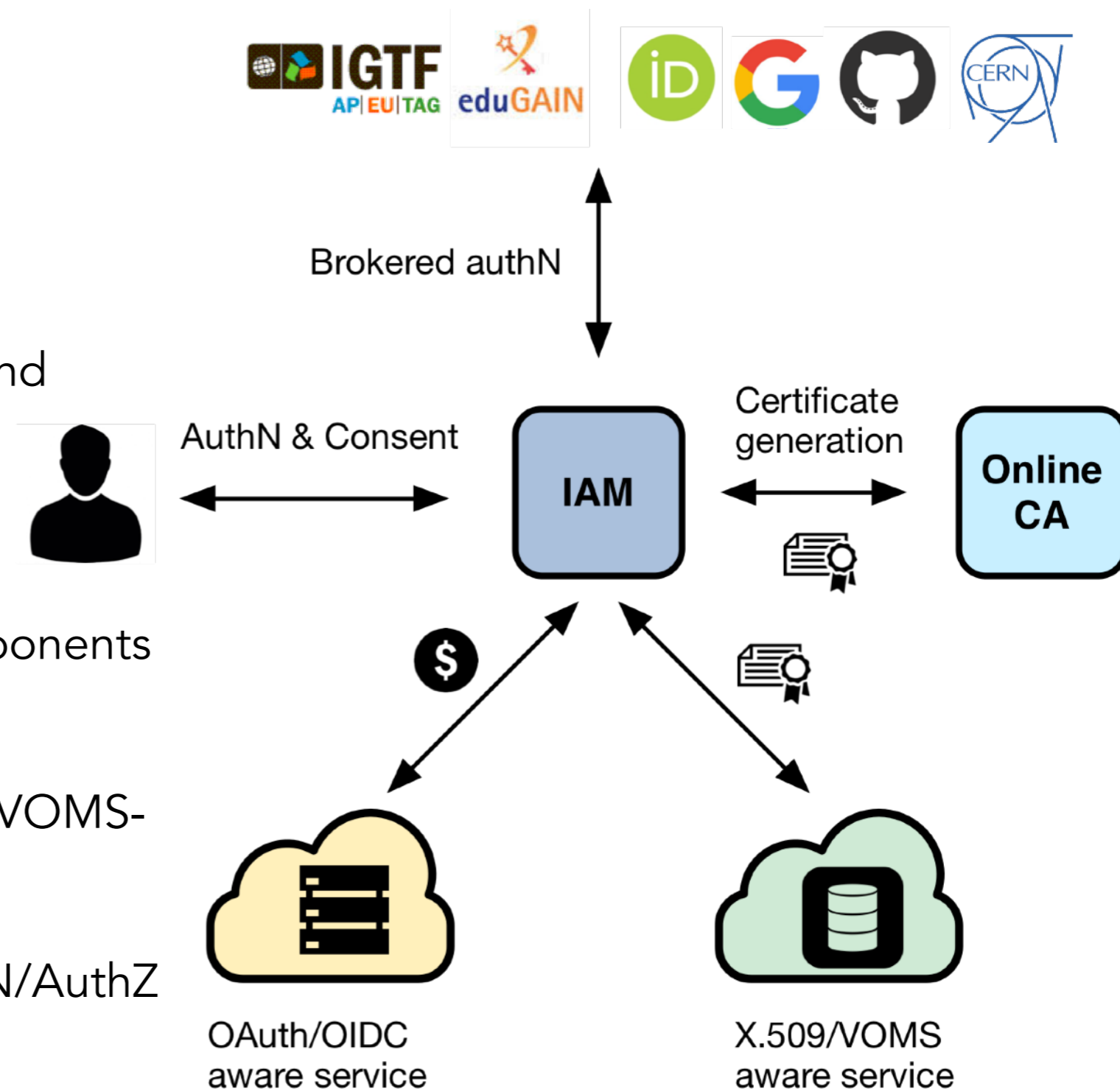
**Registration service** for moderated and automatic user enrollment

**Enforcement of AUP acceptance**

**Easy integration** in off-the-shelf components thanks to **OpenID Connect/OAuth**

**VOMS support**, to integrate existing VOMS-aware services

**Self-contained**, comprehensive AuthN/AuthZ solution



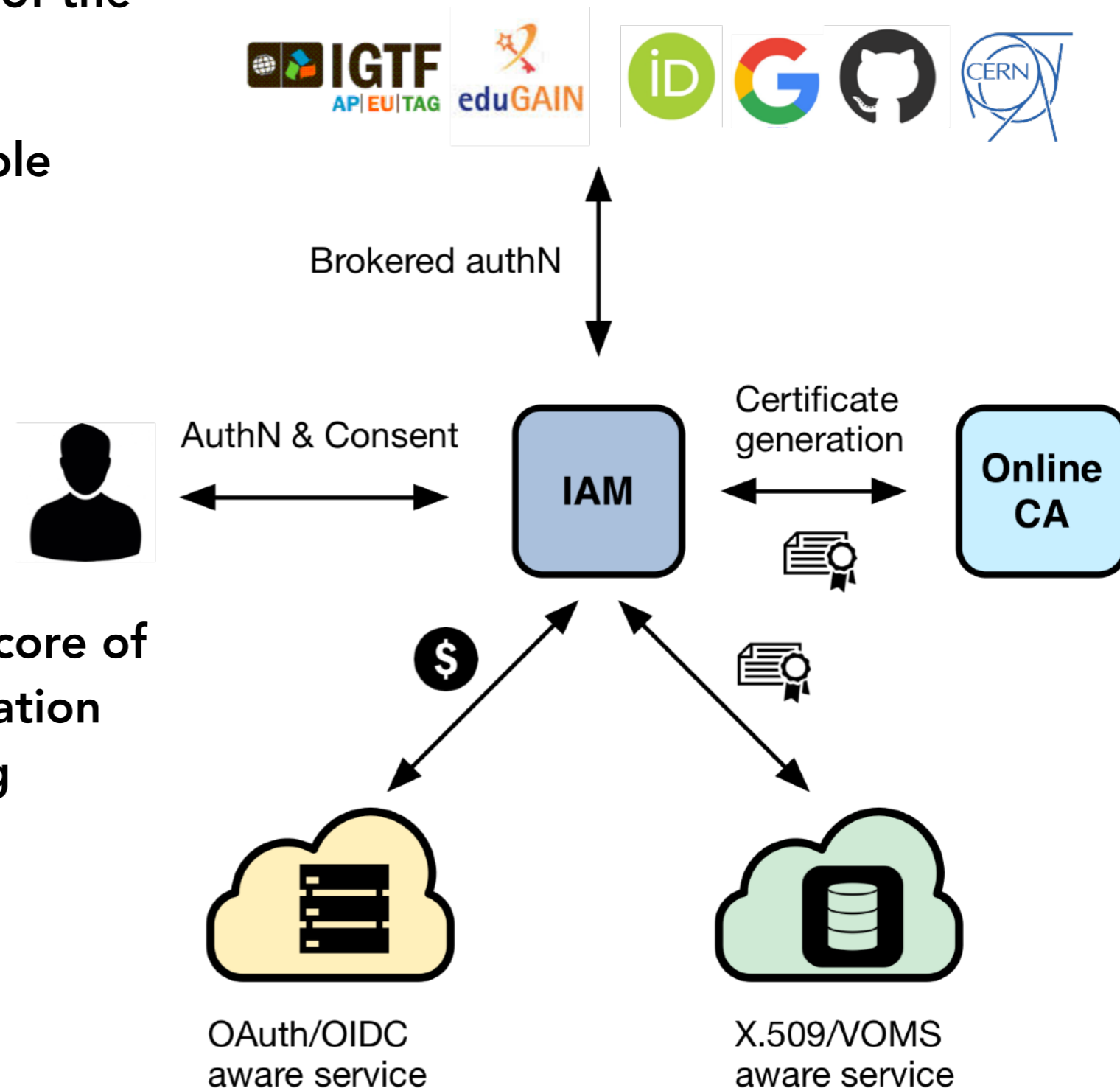
# INDIGO Identity and Access Management service

Originally developed in the context of the INDIGO DataCloud project

Sustained by INFN for the foreseeable future with support from:

- EOSC-Hub
- ESCAPE

Selected by WLCG to be at the core of the next-generation WLCG authorization service in support of LHC computing



# IAM deployment model

An IAM instance is deployed for a **community** of users sharing resources, the good old **Virtual Organization (VO)** concept.

Client applications and services are integrated with this instance via **standard OAuth/OpenID Connect** mechanisms.

The IAM Web appearance can be **customized** to include a **community logo**, **AUP** and **privacy policy** document.

The image displays three screenshots of IAM web interfaces, stacked vertically. The top screenshot shows the INFN CHNet login page, featuring the INFN logo and the text 'Istituto Nazionale di Fisica Nucleare Cultural Heritage Network'. Below the logo is a 'Welcome to chnet' message and a login form with 'Username' and 'Password' fields. The middle screenshot shows the deep Hybrid DataCloud login page, featuring the 'deep' logo and the text 'Hybrid DataCloud'. Below the logo is a 'Welcome to deep-hdc' message. The bottom screenshot shows the WLCG Worldwide LHC Computing Grid login page, featuring the WLCG logo and the text 'Worldwide LHC Computing Grid'. Below the logo is a 'Welcome to wlcg-authz-wg' message and a login form with 'Username' and 'Password' fields. Below the login form are three buttons: 'Sign in' (blue), 'Sign in with Google' (red), and 'Register a new account' (green). At the bottom of the page, there is a message: 'You have been successfully authenticated as CN=Andrea Ceccanti aceccant@infn.it,O=Istituto Nazionale di Fisica Nucleare,C=IT,DC=tcs,DC=terena,DC=org This certificate is not linked to any account in this organization'.

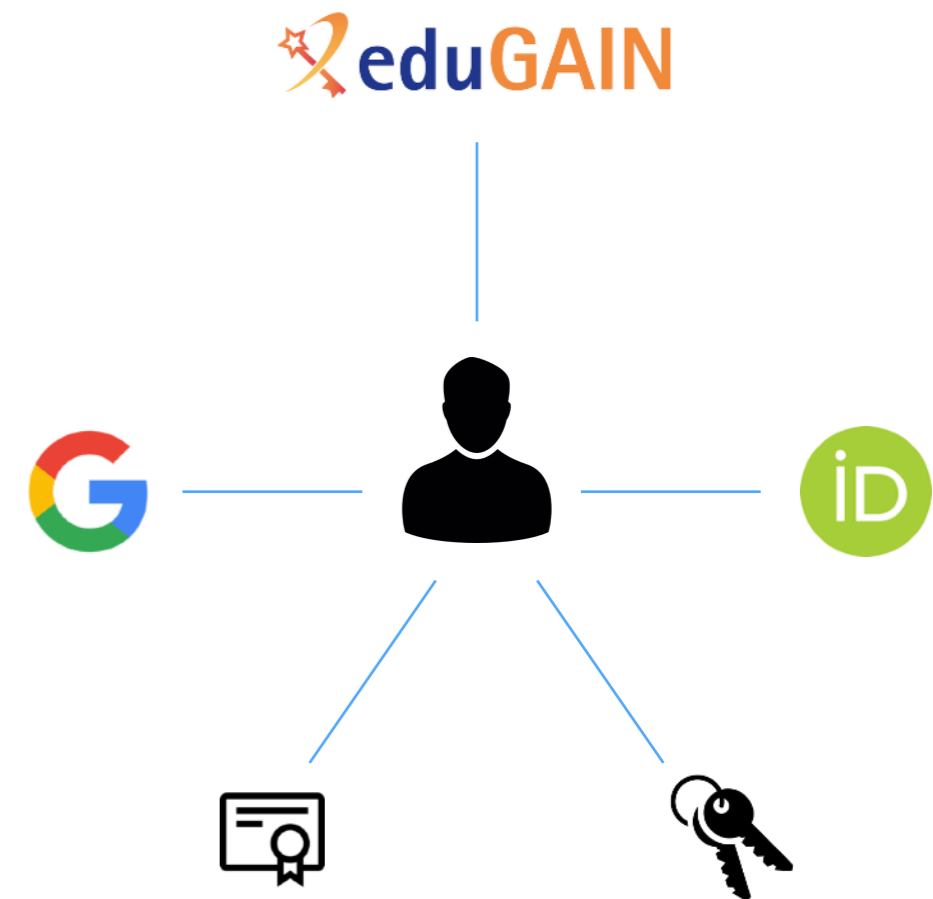
# Flexible authentication & account linking

Authentication supported via

- **local username/password** credentials (created at registration time)
- **SAML** Home institution IdP (e.g., EduGAIN)
- **OpenID Connect** (Google, Microsoft, Paypal, ORCID)
- **X.509** certificates

Users can link any of the supported authentication credentials to their IAM account at registration time or later

To link an external credential/account, the user has to **prove** that he/she owns such account



# User enrollment & registration service

IAM supports two **enrollment flows**:

## Admin-moderated flow

- The applicant fills basic registration information, accepts AUP, proves email ownership
- VO administrators are informed by email and can approve or reject incoming membership requests
- The applicant is informed via email of the administrator decision

## Automatic-enrollment flow

- Users authenticated at **trusted**, **configurable** SAML IdPs are automatically on-boarded, without administrator approval

The screenshot displays the WLCG registration service interface. At the top, the WLCG logo and 'Worldwide LHC Computing Grid' are visible. The user 'Andrea Ceccanti' is logged in. The main section is titled 'Requests' and contains a search bar and pagination controls. A table lists a single request:

Created	User	Request	Actions
8 hours ago	Carlos Armando Garcia	Registration request	<a href="#">Approve</a> <a href="#">Reject</a>

Below the table, a detailed view of the request is shown:

<b>Created</b>	07/06/2018 09:17:33
<b>Current Status</b>	CONFIRMED
<b>Name</b>	Carlos Armando Garcia
<b>Username</b>	charlos1204
<b>E-mail</b>	carlos.garcia@helmholtz-muenchen.de
<b>Notes</b>	I will attend the "Data Science - Curso 2018-19 - Santander - Peninsula de la Magdalena"

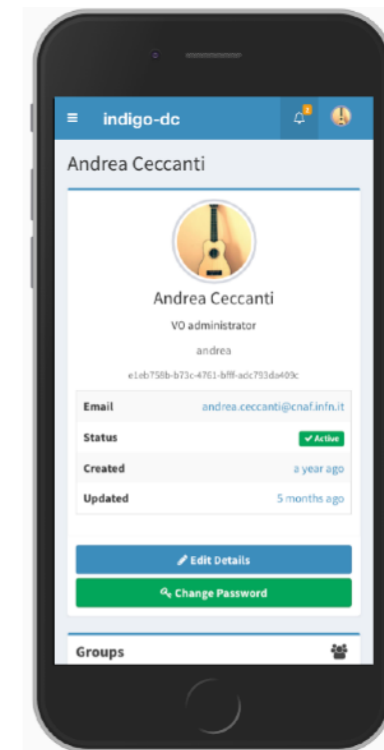
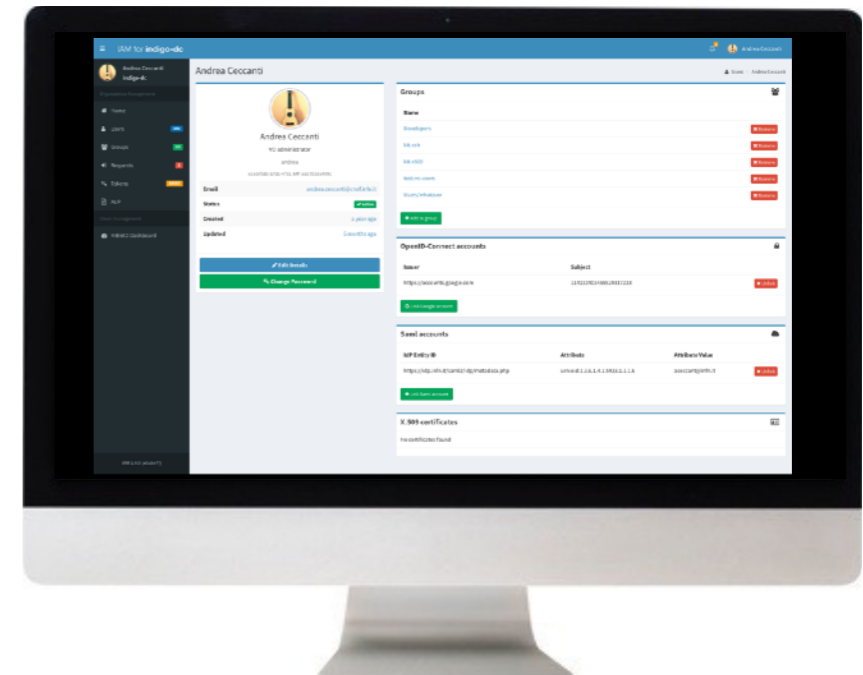
At the bottom, a registration form is partially visible, including a warning about the Acceptable Usage Policy (AUP) and buttons for 'Register' and 'Reset Form'.

# Management tools

IAM provides a **mobile-friendly** dashboard for:

- User management
- Group management
- Membership request management
- Account linking and personal details editing
- Token management

All management functionality is also exposed by REST APIs

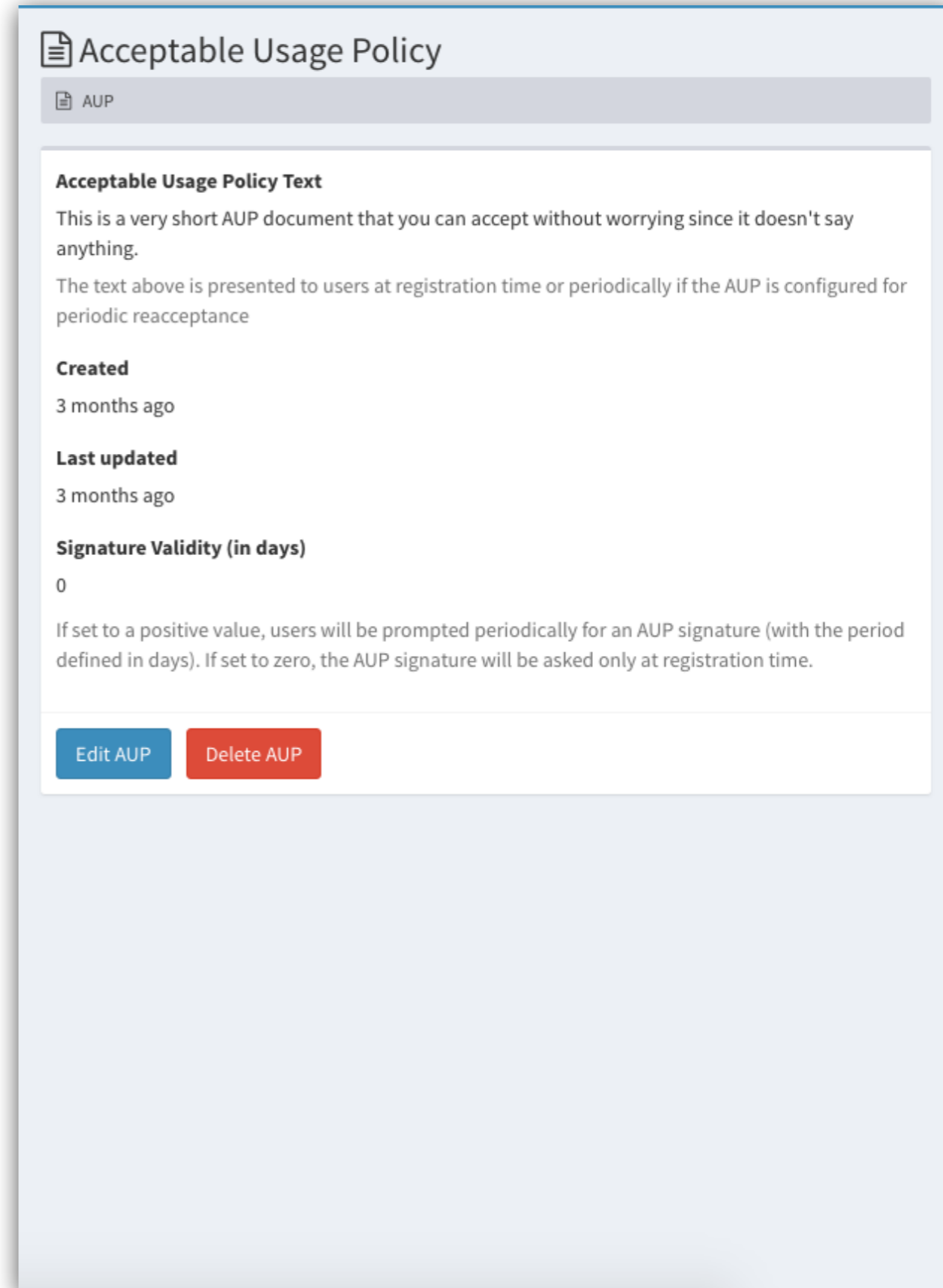


# AUP enforcement support

**AUP acceptance**, if enabled, can be configured to be:

- requested once at user registration time
- periodically, with configurable period

User cannot login to the system (and as such be authenticated at authorized at services) unless the **AUP** has been accepted



The screenshot shows a web interface for configuring an Acceptable Usage Policy (AUP). The title is "Acceptable Usage Policy" with a document icon. Below the title is a tab labeled "AUP". The main content area is titled "Acceptable Usage Policy Text" and contains the following text: "This is a very short AUP document that you can accept without worrying since it doesn't say anything. The text above is presented to users at registration time or periodically if the AUP is configured for periodic reacceptance". Below the text are two fields: "Created" (3 months ago) and "Last updated" (3 months ago). There is also a field for "Signature Validity (in days)" set to 0, with a note: "If set to a positive value, users will be prompted periodically for an AUP signature (with the period defined in days). If set to zero, the AUP signature will be asked only at registration time." At the bottom of the configuration area are two buttons: "Edit AUP" (blue) and "Delete AUP" (red).



# Easy integration with services

**Standard OAuth/OpenID Connect** enable **easy integration** with off-the-shelf services and libraries.

IAM has been successfully integrated with

- Openstack, Atlassian JIRA & Confluence, Moodle, Rocketchat, Grafana, Kubernetes, JupyterHub
- dCache, StoRM, FTS, RUCIO (in progress)

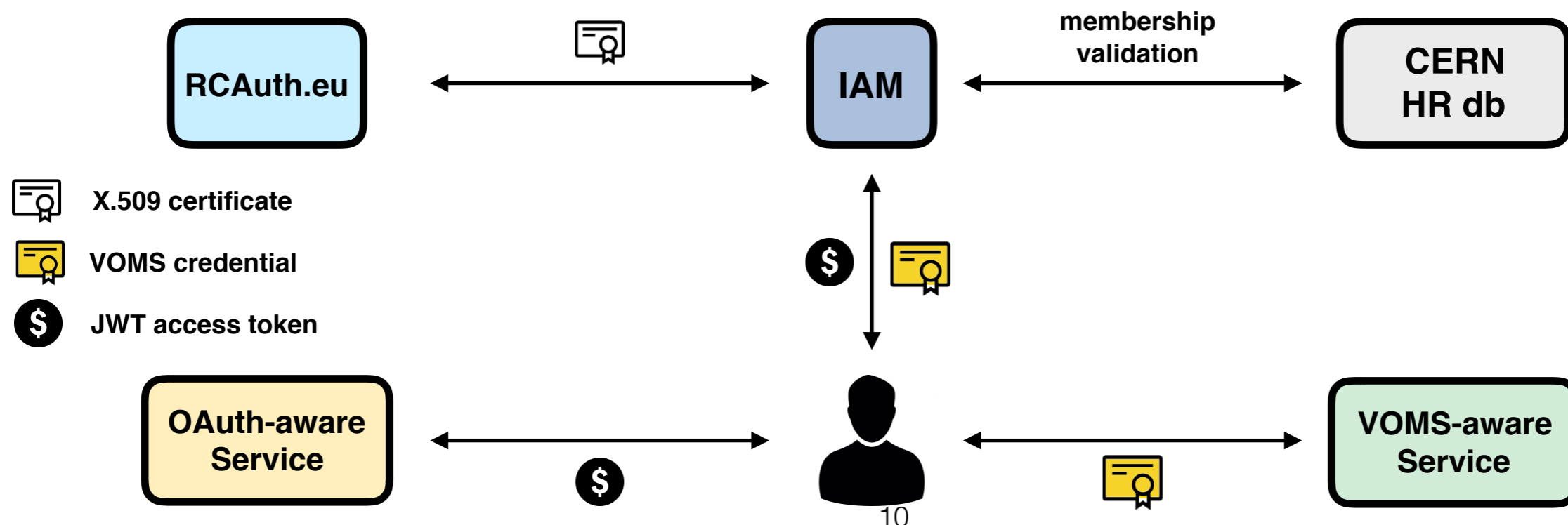


# Migrating from X.509/VOMS to tokens

IAM implements **VOMS provisioning** to expose authentication and authorization information in the form of a **VOMS attribute certificate**, **compatible** with existing VOMS clients

IAM integrates with **RCAuth.eu** online CA to generate X.509 certificates on-demand and link them to IAM user memberships

A **gradual transition** towards token-based authn/authz is thus possible



# IAM and SciTokens

IAM can issue tokens compatible with SciTokens profile

**Successful integration** with coarse grained capabilities already demonstrated for DOMA TPC activities

Yesterday, after some tweaks on both IAM and the scitokens client library, Brian managed to submit a job to HTCondor using a token issued by IAM

IAM can implement privileged access to certain scopes, so that only specific users are entitled to request them

- e.g. in the IAM ESCAPE VO, only users in the /escape/xfers group can request Scitokens data access scopes

# Software Quality

Aim to have ~90% unit test coverage on all code:

- now 29k LoC, 85% branch coverage, >1K tests

Open, test-driven development process

Static analysis tools

- [SonarCube IAM page](#)

Multiple test suites

- Unit tests
- Frontend test suite (based on Selenium and Robot framework)
- Deployment tests (in CI)

The screenshot displays a GitHub pull request interface. At the top, there are three summary cards: 'Coverage' showing 85.6% (818 Unit Tests) and 'Coverage on New Code' (—); 'Duplications' showing 3.8% (72 Duplicated Blocks) and '+0.0%' Duplications; and 'Size' (partially visible). Below these is the pull request title 'Add support to multiple OIDC providers #249' and a green 'Open' button. The pull request details include 'Conversation 1', 'Commits 2', 'Checks 0', and 'Files changed 35'. A comment from 'marcocaberletti' states 'This PR resolve issue #229.' Below this is a commit history showing 'Add support to multiple OIDC providers' (checked), 'requested review from andreaceccanti and enricovianello 14 days ago', and 'added this to PRs ready for review in IAM next release 14 days ago'. A 'New changes since you last viewed' section shows 'Restore Link button' (checked). A SonarQube bot comment reports '1 issue' with a note that issues are summarized because they were on non-modified lines. The issue is: '1. OidcConfiguration.java#L97: Method has 10 parameters, which is greater than 7 authorized.' At the bottom, a green 'Review requested' banner indicates that a review is needed for the pull request.

# IAM deployment strategies

IAM is a **Spring Boot** application

- currently based on the MitreID Connect libraries
- typically deployed behind an **NGINX**
- stores data in a **MariaDB/ MySQL** database

Horizontally scalable

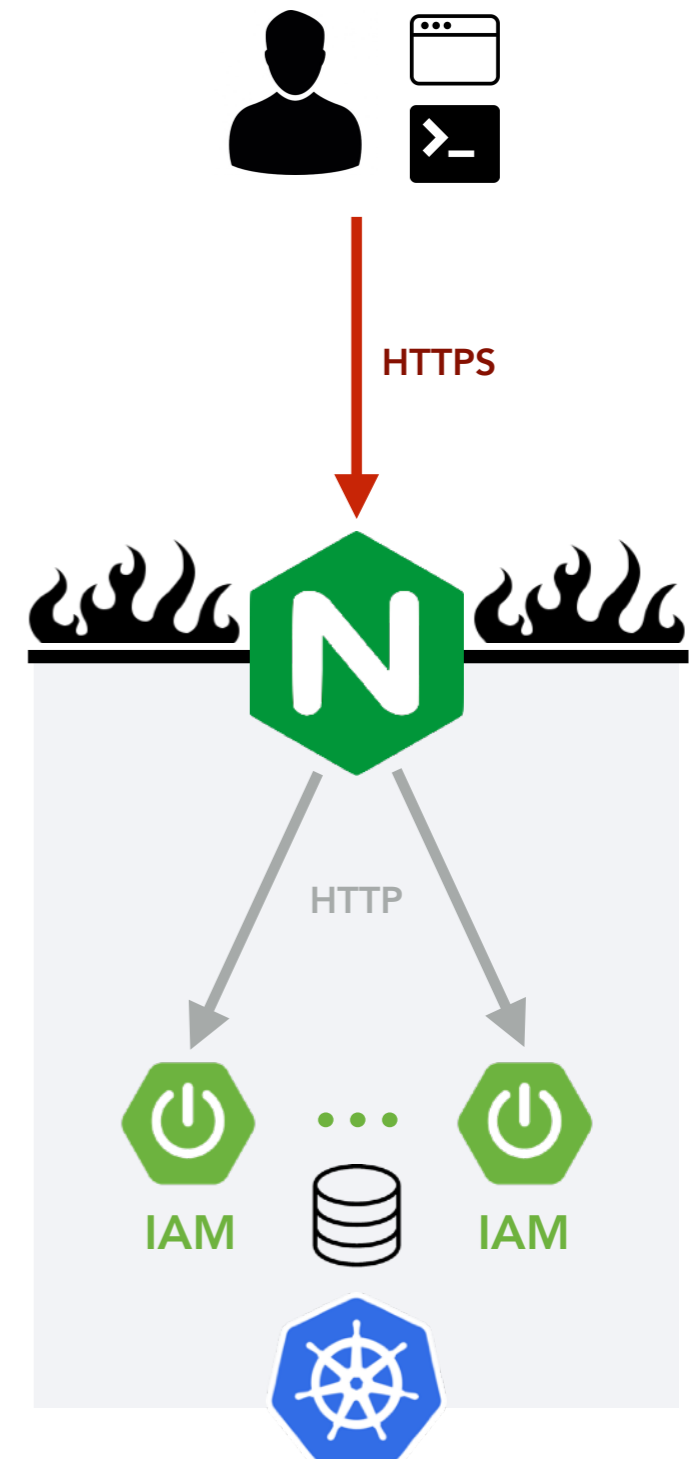
- all state persisted in the database

We deploy IAM as a **containerized** service on top of **Kubernetes**

- autoscaling, zero downtime rolling updates

And provide packages for

- CENTOS 7, UBUNTU 1604



# IAM evolution: porting to Keycloak

IAM 2 (currently in development) will be based on Keycloak

- Powerful RedHat SSO solution
- Vibrant community: > 250 GitHub contributors
- LDAP/Kerberos integration
- Multi-tenancy



IAM codebase will focus on what not already provided by Keycloak

- registration service and user/group management
- X.509 and VOMS authentication support



**Improved flexibility and sustainability**

# Useful references

IAM @ GitHub: <https://github.com/indigo-iam/iam>

IAM documentation: <https://indigo-iam.github.io/docs>

WLCG Authorization WG: <https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAuthorizationWG>

WLCG AuthZ WG Demos: <https://indico.cern.ch/event/791175/attachments/1806605/2948665/demos.mp4> (IAM starts at minute 46)

IAM in action video: <https://www.youtube.com/watch?v=1rZlvJADOnY>

## Contacts:

- [andrea.ceccanti@cnaa.infn.it](mailto:andrea.ceccanti@cnaa.infn.it)
- [indigo-iam.slack.com](https://indigo-iam.slack.com)

**Thanks!**  
**Questions?**