

INDIGO IAM: status and evolution plans

Andrea Ceccanti
INFN CNAF

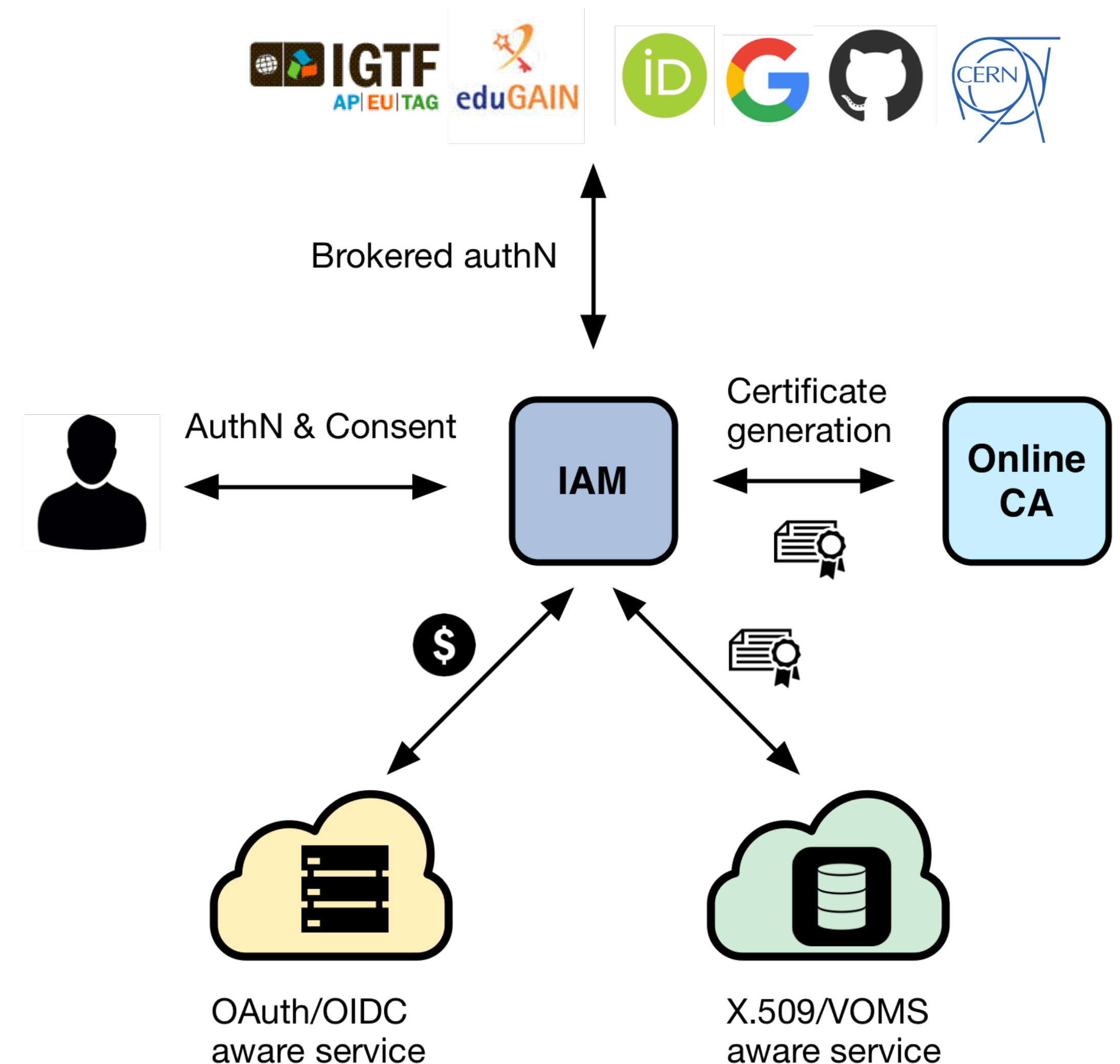
INDIGO IAM User's Workshop
November, 8th 2021



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**

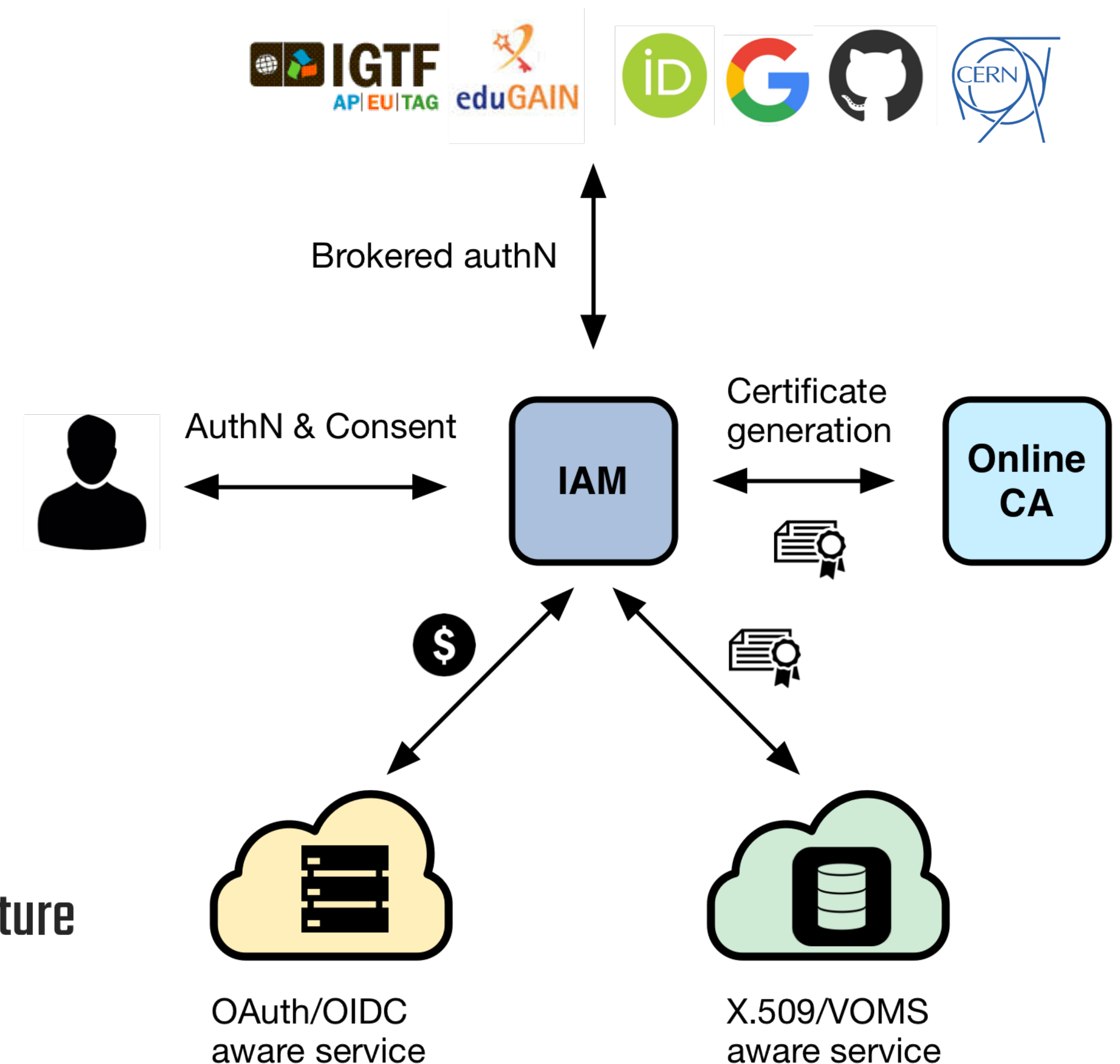
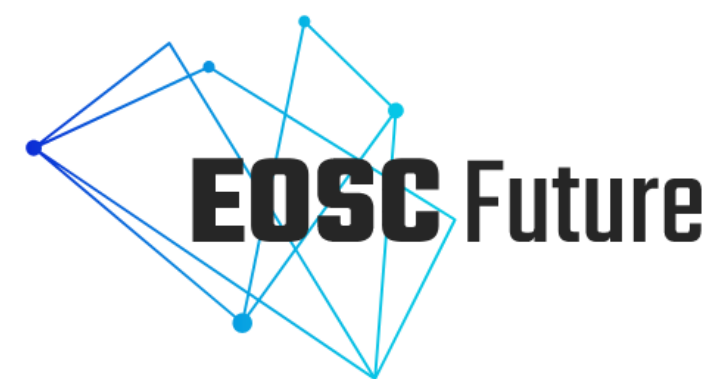


INDIGO Identity and Access Management Service

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:



INDIGO IAM: the development team

IAM is mainly developed by the **Software Development (SD)** group at INFN-CNAF.

We are currently 7 people, working on IAM, StoRM, VOMS, Argus maintenance and other activities

- Federica Agostini
- Andrea Ceccanti (Lead)
- Francesco Giacomini
- Roberta Miccoli
- Elisabetta Ronchieri
- Marcelo Soares
- Enrico Vianello

IAM: latest releases (v1.7.0 and v1.7.1)

New website, with restructured and improved documentation

Improved scalability on group membership persistence management, including **improved pagination on SCIM APIs**

Improved token-exchange flexibility, with 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 **via the userinfo endpoint**

The VOMS importer script, which allows to migrate users, group and role information from a VOMS installation to an IAM

Plus other **bug fixes** and **improvements**. For more details, see the v1.7.0 and v1.7.1 release notes.

Main IAM deployments

IAM deployment @ CNAF

~20 IAM instances in support of various projects

- WLCG, ESCAPE, DODAS, Deep Hybrid DataCloud, EOSC-Hub, HERD, IOTwins, EOSC-Pillar, EGO-VIRGO, T1-Computing, PLANET, MVM, CTA-LST, ...

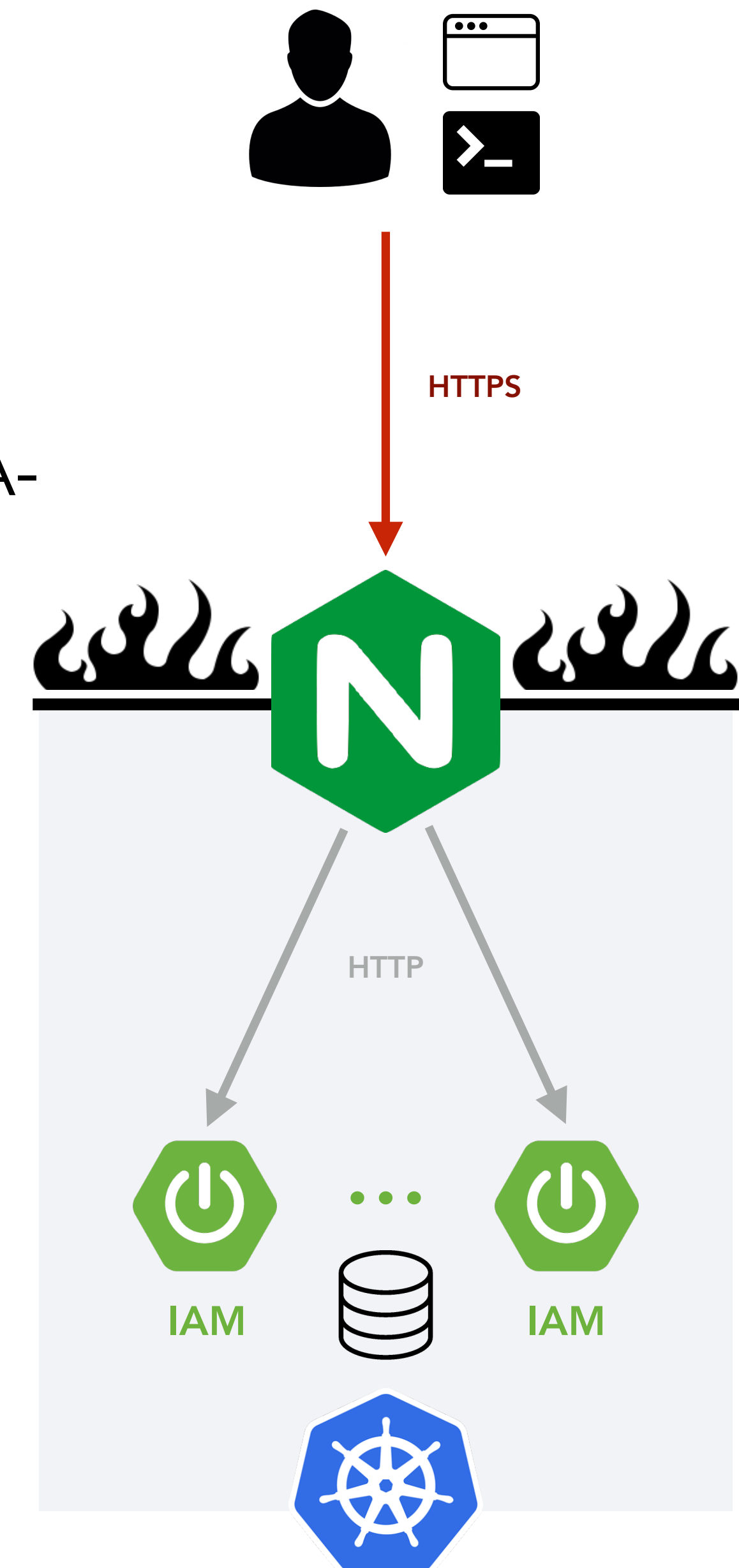
Deployed on a Kubernetes cluster

- Each projects gets a dedicated K8S namespace


Data stored on HA Percona MySQL cluster

Kubernetes advantages

- rolling updates
- consistent management



INDIGO IAM for cta-1st @ INFN



Welcome to cta-1st @ INFN-CNAF

Sign in with

Your X.509 certificate


CTA-LST SSO

Not a member?

Apply for an account

You have been successfully authenticated as
CN=Andrea Ceccanti,CN=657221,CN=aceccant,OU=Users,OU=Organic Units,DC=cern,DC=ch

INDIGO IAM for iotwins-Log in



Welcome to iotwins

Sign in with your iotwins credentials

Username

Password

Sign in

Forgot your password?


Or sign in with

INFN AAI

Not a member?

Apply for an account

INDIGO IAM for wlcg-Log in



Welcome to wlcg

Sign in with your wlcg credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

Your X.509 certificate


CERN SSO

Not a member?

Apply for an account

You have been successfully authenticated as
CN=Andrea Ceccanti,CN=657221,CN=aceccant,OU=Users,OU=Organic Units,DC=cern,DC=ch

INDIGO IAM for virgo-Log in



Welcome to virgo


Sign in with

LIGO

Not a member?

Apply for an account

INDIGO IAM for t1-computing-Log in



Welcome to t1-computing

Sign in with your t1-computing credentials

Username

Password

Sign in

Forgot your password?

Or sign in with


INFN AAI

Not a member?

Apply for an account

https://iam-t1-computing.cloud.cnaf.infn.it

INDIGO IAM for super-Log in



Welcome to super

Sign in with your super credentials

Username

Password

Sign in

Forgot your password?


Or sign in with

eduGAIN

Not a member?

Apply for an account

INDIGO IAM for herd-Log in



Welcome to herd

Sign in with your herd credentials

Username

Password

Sign in

Forgot your password?

Or sign in with


Google

INFN AAI

Not a member?

Apply for an account

INDIGO IAM for eossc-hub-Log in



Welcome to eossc-hub

Sign in with your eossc-hub credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

Google

B2ACCESS


eduGAIN

ESI

Not a member?

Apply for an account

INDIGO IAM for indigo-dc-Log in



Welcome to indigo-dc

Sign in with your indigo-dc credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

Google


ESI

eduGAIN

Not a member?

Apply for an account

INDIGO IAM for escape-Log in



Welcome to escape

Sign in with your escape credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

Your X.509 certificate

Google

eduGAIN

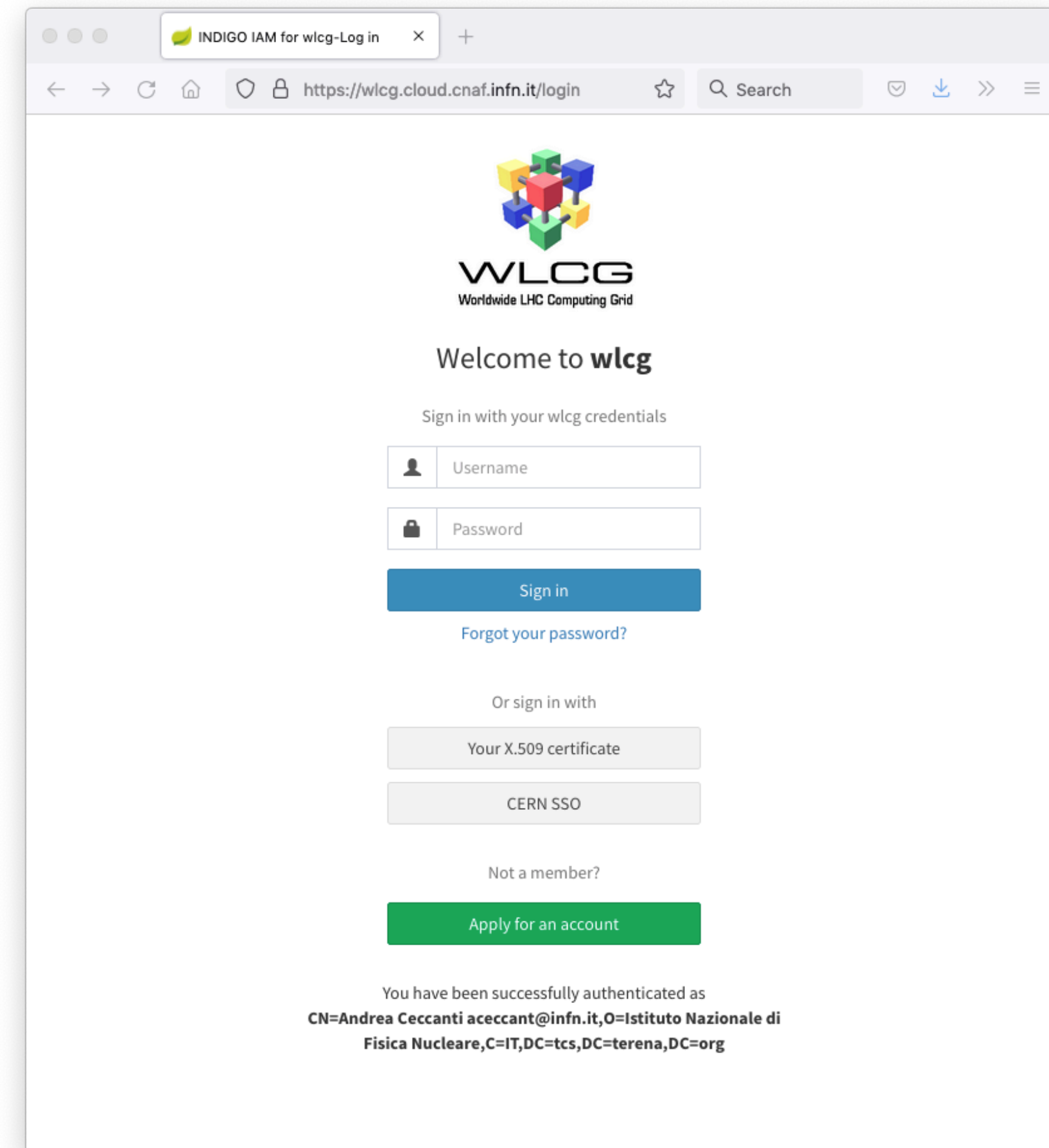
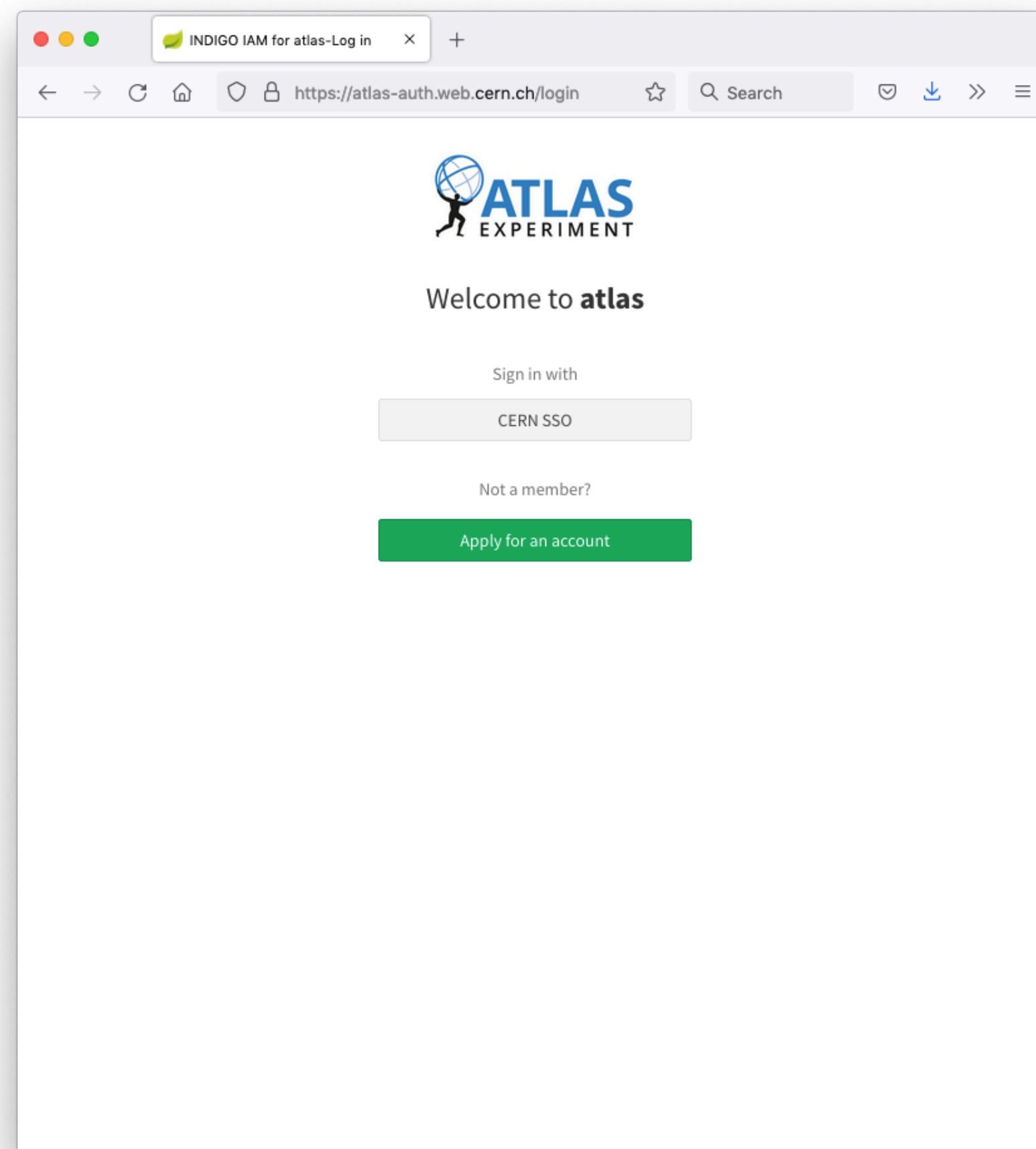
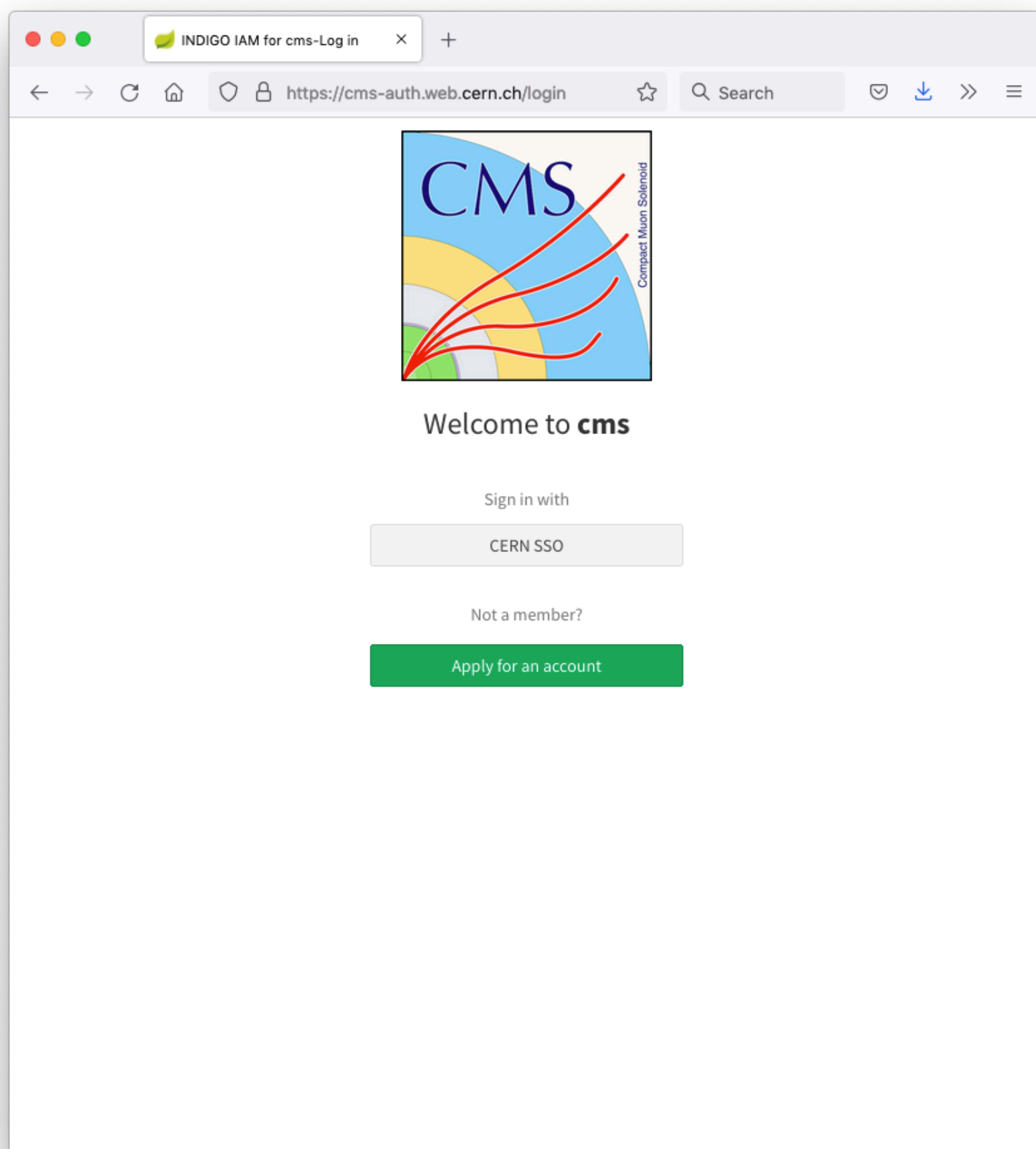
Not a member?

Apply for an account

You have been successfully authenticated as
CN=Andrea Ceccanti,CN=657221,CN=aceccant,OU=Users,OU=Organic Units,DC=cern,DC=ch

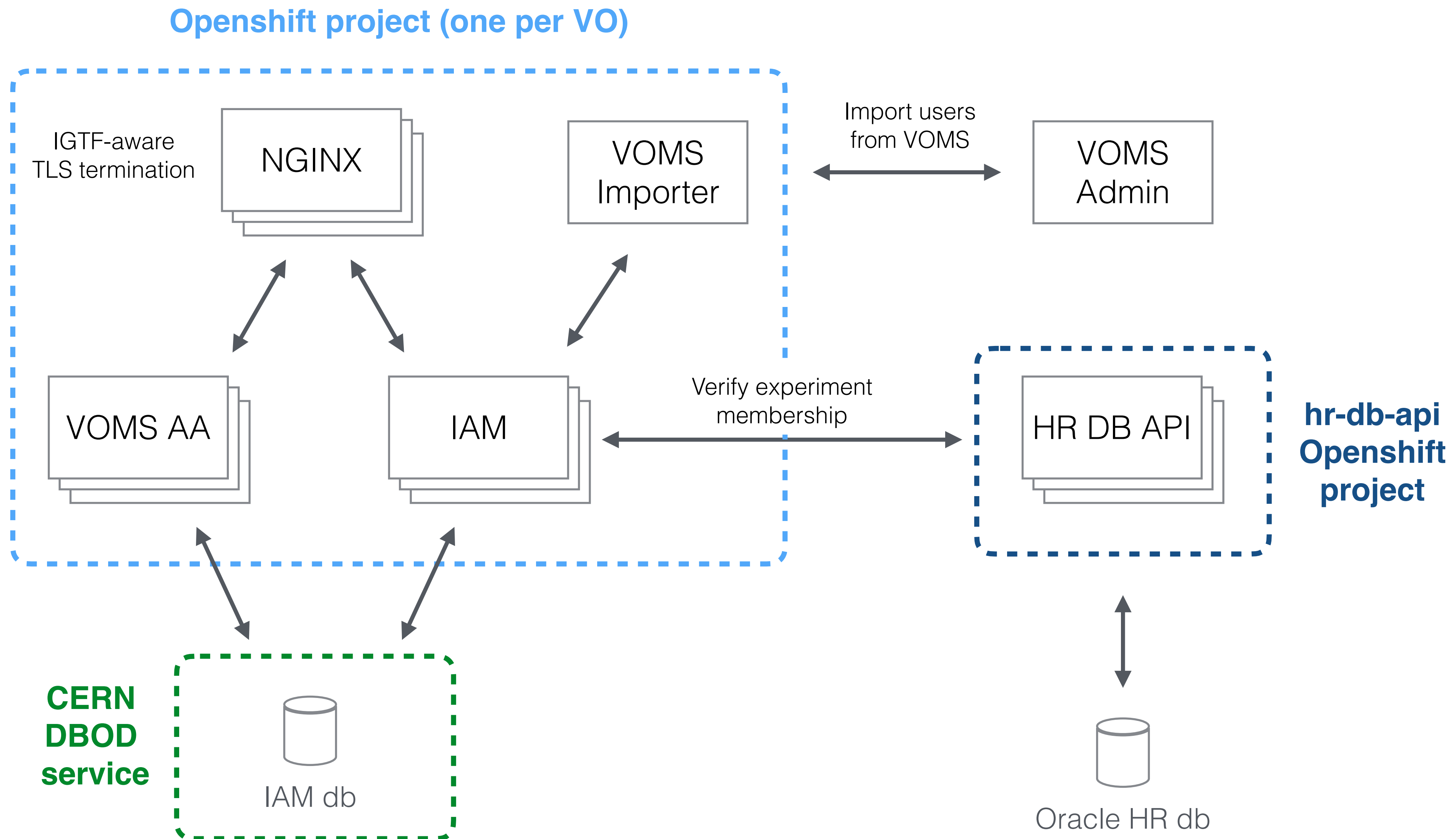
WLCG IAM deployments

Alice and LHCb coming soon



IAM deployment at CERN: overview

See Hannah's talk
later today



Main planned developments

IAM v1.8.0

Next release, ETA: December 2021

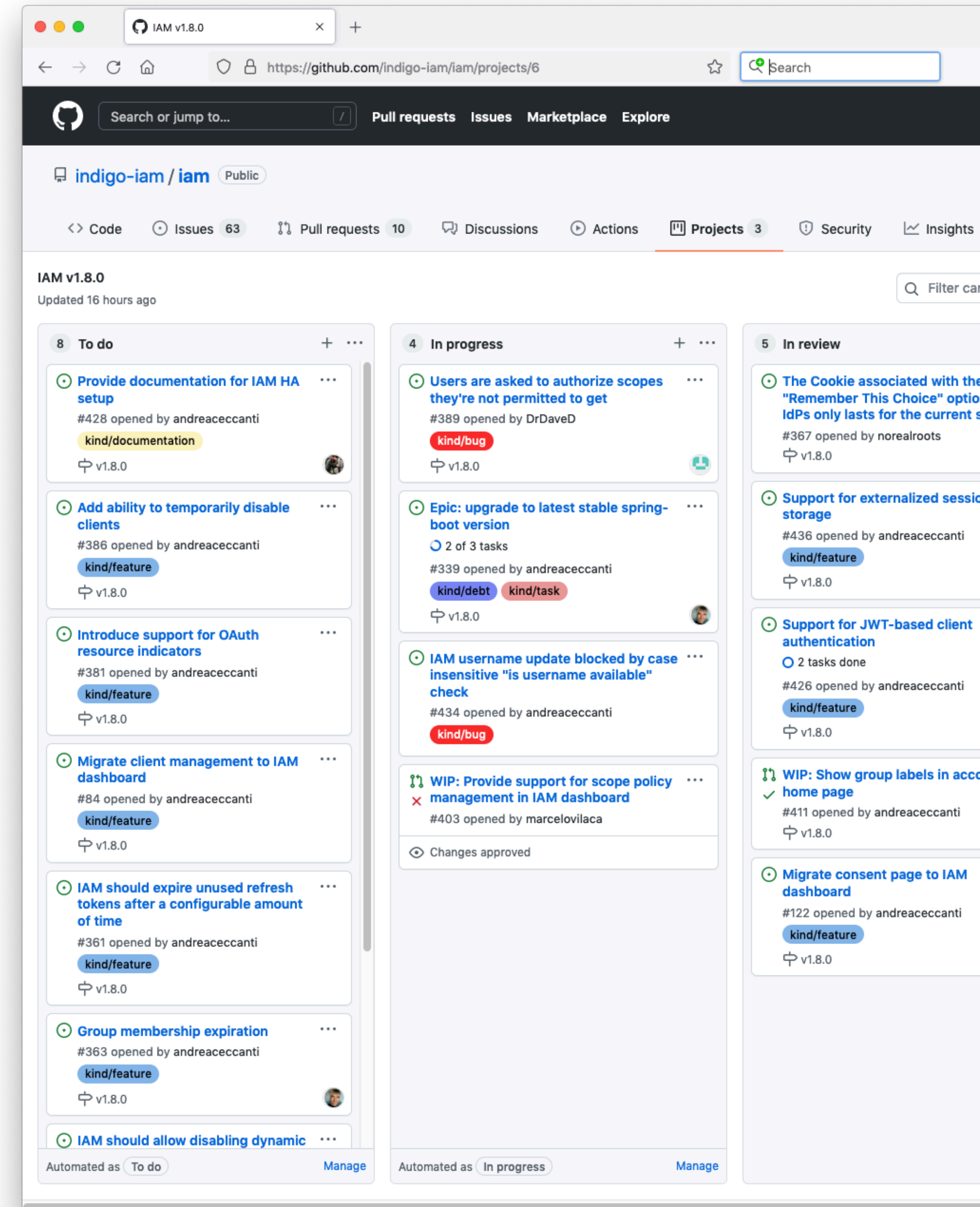
<https://github.com/indigo-iam/iam/milestone/11>

<https://github.com/indigo-iam/iam/projects/6>

Highlights:

- Spring dependencies upgrade
- Improved client management & registration
- Session externalization
- JWT-based client authentication

other minor improvements & bug fixes



Spring dependencies upgrade

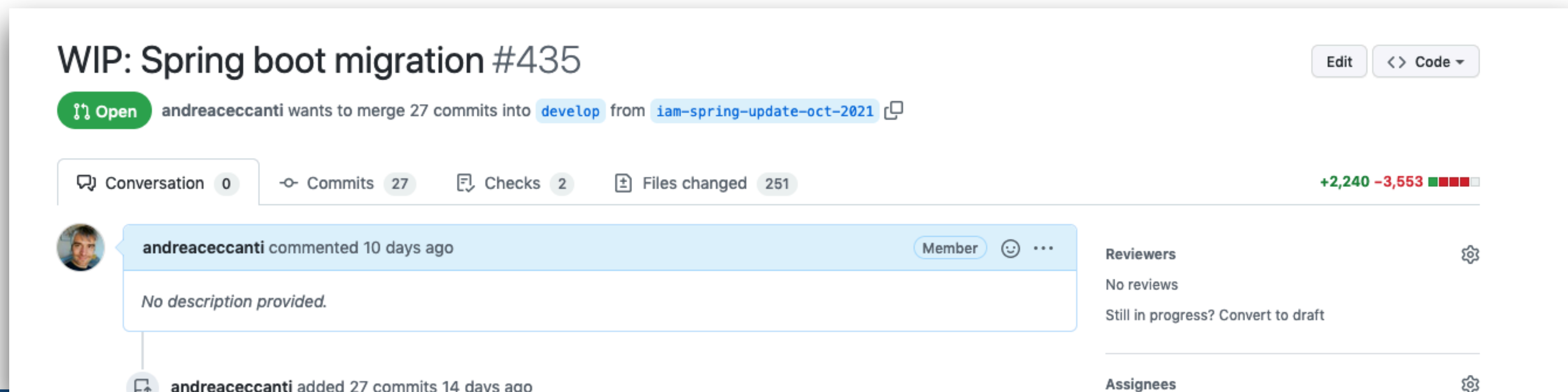
IAM is a Spring Boot application. IAM relies on **an old Spring Boot version** (1.3.8), which **has reached EOL** and needs to be upgraded ASAP.

The upgrade will also allow to **move to Java 11**.

<https://github.com/indigo-iam/iam/issues/339>

<https://github.com/indigo-iam/iam/pull/435>

<https://github.com/indigo-iam/iam/pull/439>



The screenshot shows a GitHub pull request interface. At the top, the title is "WIP: Spring boot migration #435". Below the title, it indicates that "andreaceccanti wants to merge 27 commits into develop from iam-spring-update-oct-2021". The interface includes a "Conversation" tab with 0 comments, "Commits" with 27, "Checks" with 2, and "Files changed" with 251. A green bar shows a change of +2,240 lines and -3,553 lines. A comment from "andreaceccanti" is visible, stating "No description provided." The right sidebar shows "Reviewers" (No reviews) and "Assignees" (empty).

Spring dependencies upgrade

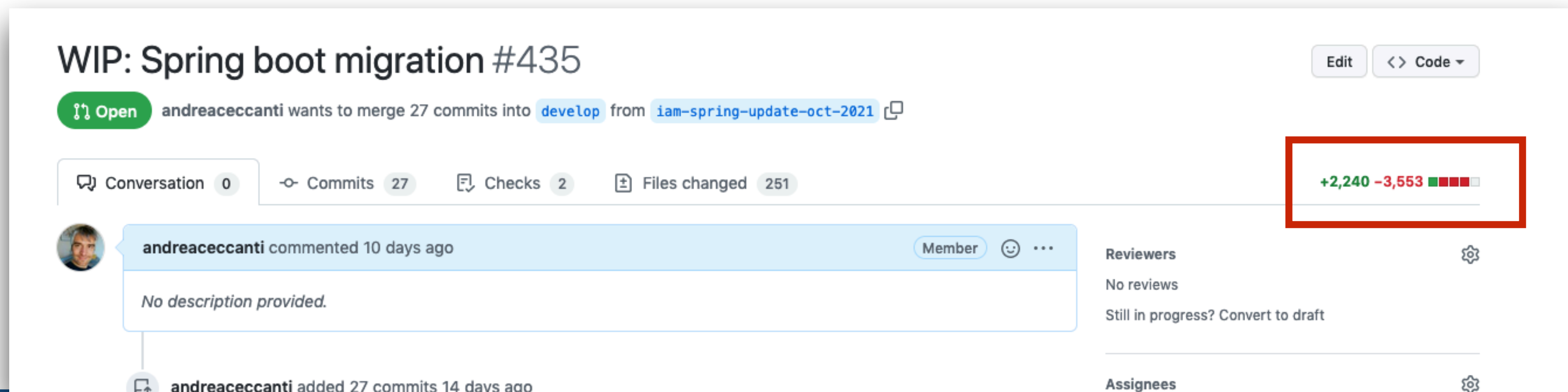
IAM is a Spring Boot application. IAM relies on **an old Spring Boot version** (1.3.8), which **has reached EOL** and needs to be upgraded ASAP.

The upgrade will also allow to **move to Java 11**.

<https://github.com/indigo-iam/iam/issues/339>

<https://github.com/indigo-iam/iam/pull/435>

<https://github.com/indigo-iam/iam/pull/439>



The screenshot shows a GitHub pull request interface. At the top, the title is "WIP: Spring boot migration #435". Below the title, it says "Open" and "andreaceccanti wants to merge 27 commits into develop from iam-spring-update-oct-2021". There are buttons for "Edit" and "Code". Below this, there are statistics: "Conversation 0", "Commits 27", "Checks 2", and "Files changed 251". A red box highlights the change statistics: "+2,240 -3,553". Below the statistics, there is a comment from "andreaceccanti" from 10 days ago, which says "No description provided." At the bottom, it says "andreaceccanti added 27 commits 14 days ago". On the right side, there are sections for "Reviewers" (No reviews) and "Assignees".

Refactored client management & registration

<https://github.com/indigo-iam/iam/issues/386>

<https://github.com/indigo-iam/iam/issues/84>

Up to now IAM has relied on MitreID Connect client management APIs, which however have **scalability and usability limits**

- No pagination on client management APIs, this causes issues on the management dashboard with large number of clients
- Client management always require to use a registration access tokens, i.e. it's hard for users to have a clear view of their registered clients
- No client search API

Refactored client management & registration

The new client management & registration API will:

- implement **pagination**
- implement **server-side search functionalities**
- allow to **limit client registration only to registered VO members**
- add the ability to **temporarily disable clients**
- add the **ability to expire and remove from the database clients that are not used**
- allow users to **see and manage clients linked to their account from the IAM dashboard**

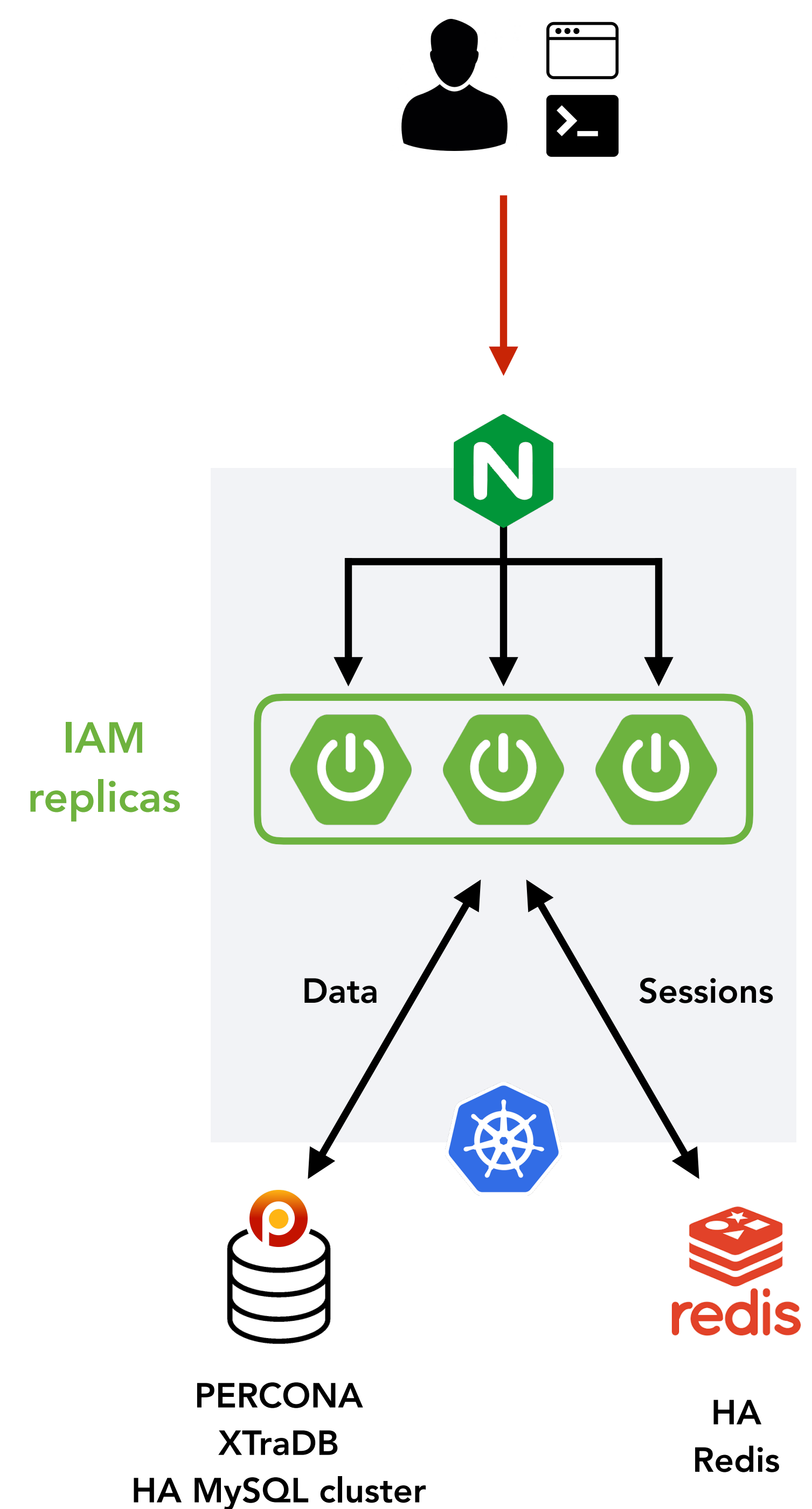
Session data externalization

<https://github.com/indigo-iam/iam/issues/436>

<https://github.com/indigo-iam/iam/pull/437>

With session externalization, IAM becomes a completely stateless application

This supports **replicated/HA IAM deployments**



JWT-based client authentication

The OAuth and OpenID Connect protocols support **JWT-based client-authentication**, which means that clients authenticate to the token issuer (e.g., IAM) sending a **signed JWT** instead of a (client_id, client_secret) credential.

The token issuer inspects the JWT, resolves the client_id and verifies the JWT using either a shared secret or a public key linked to the client configuration

Pros

- time-limited client credentials under the control of the client

Cons

- clients need to know how to generate and sign a JWT

JWT-based client authentication

<https://github.com/indigo-iam/iam/pull/427>

Introduces support in IAM for `client_secret_jwt` and `private_key_jwt` auth schemes.

Advantages:

- reduced risks of exposed client credentials
- support time-limited credential delegation

Other improvements in 1.8.0

Improved support for key rotation and token signature algorithm selection

- <https://github.com/indigo-iam/iam/issues/430>

Support for OAuth resource indicators

- <https://github.com/indigo-iam/iam/issues/381>
- ie., a standard way to request an audience for issued tokens

Improved Consent page

- <https://github.com/indigo-iam/iam/pull/417>

Longer-term planned developments

Support for Multi-factor authentication

- <https://github.com/indigo-iam/iam/issues/418>
- See Sam's talk

IAM API endpoints consolidation

- <https://github.com/indigo-iam/iam/issues/407>

Migrate IAM dashboard to the latest Angular

- <https://github.com/indigo-iam/iam/issues/87>

Evaluate migrating away from MitreID connect

- <https://github.com/indigo-iam/iam/issues/406>
- in favour of the new [Spring Authorization server](#) project

**Thanks for your attention.
Questions?**

References

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

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

Contacts:

- andrea.ceccanti@cnae.infn.it
- iam-support@lists.infn.it
- indigo-iam.slack.com