Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

terabit

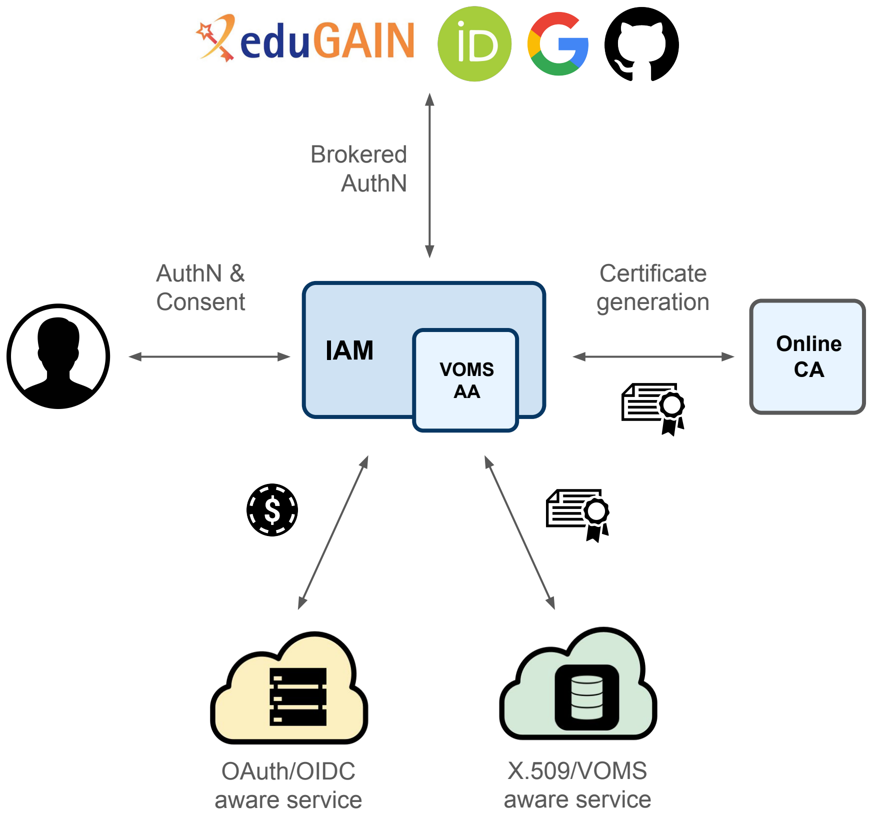
INDIGO IAM evolution: from MITREid to Spring Security, new dashboard and 2FA support

Roberta Miccoli - INFN CNAF

Workshop sul Calcolo nell'INFN - Palau (Sassari) | 20 - 24 maggio 2024

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, X.509, OpenID Connect, local users, etc.
- **Account linking**
- Moderated and automatic user enrollment
- Enforcement of **AUP acceptance**
- VO membership management
- Issuance of **JWT** tokens and VOMS attribute certificates with **identity** and **membership information**, **attributes** and **capabilities**
- Typically deployed as a **Docker container**



INDIGO IAM synergies with other projects

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

WLCG
Worldwide LHC Computing

- INFN commitment for the foreseeable future, with the current support of **several Italian and European projects**:

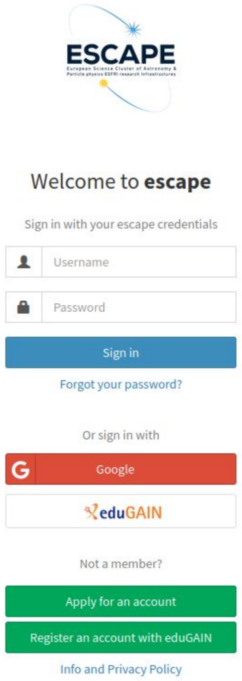
eosc | BEYOND

AARC

terabit

ICSC
Centro Nazionale di Ricerca in HPC, Big Data and Quantum Computing

IAM deployments


ESCAPE

Welcome to **escape**

Sign in with your escape credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

Google

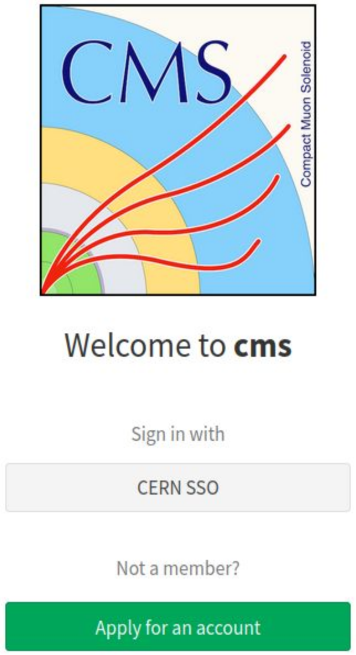
eduGAIN

Not a member?

Apply for an account

Register an account with eduGAIN

Info and Privacy Policy



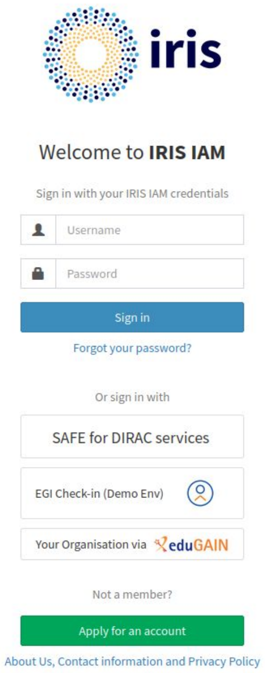
Welcome to **cms**

Sign in with

CERN SSO

Not a member?

Apply for an account


iris

Welcome to **IRIS IAM**

Sign in with your IRIS IAM credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

SAFE for DIRAC services

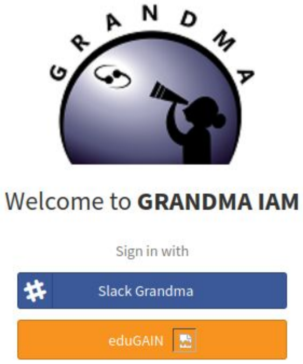
EGI Check-in (Demo Env)

Your Organisation via eduGAIN

Not a member?

Apply for an account

About Us, Contact information and Privacy Policy

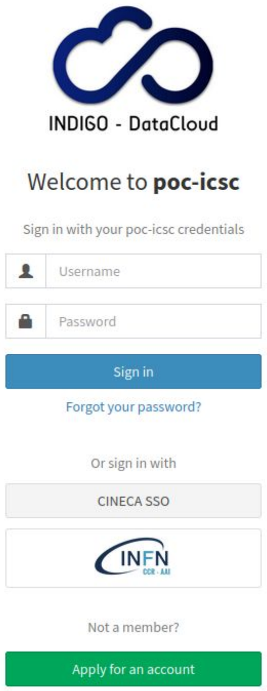

GRANDMA

Welcome to **GRANDMA IAM**

Sign in with

Slack Grandma

eduGAIN


INDIGO - DataCloud

Welcome to **poc-icsc**

Sign in with your poc-icsc credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

CINECA SSO

INFN CCR - AAI

Not a member?

Apply for an account

~ **20 instances inside CNAF** for internal purposes (INFN Cloud, CNAF Cloud, INFN T1 services, etc.) and support collaborations (ILDG, Belle-II, HERD, JUNO, etc.)

4 instance at CERN for LHCb, ATLAS, CMS and ALICE experiments and other instances for VOs management (e.g. dteam)

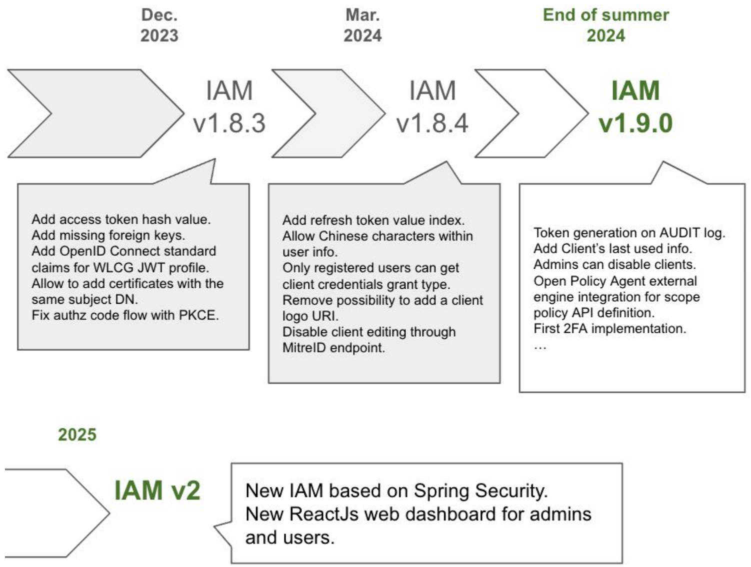
1 instance at STFC for IRIS project

3 instances at IN2P3 for MesoNET, EURO-LABS, GRANDMA projects

Development roadmap

- **Security**
  - Add Multi-Factor Authentication (MFA)
- **Superseded obsolete dependencies**
  - MITREid → Spring Authorization Server
  - AngularJS → React JS
- **Interoperability** focus
  - Support OIDC Federations
  - Improve conformance with AARC BluePrint Architecture and its guidelines
- **Scalability and performance** improvements
  - Access tokens not stored on database
  - Dedicated garbage collector service
  - Fine grained AuthZ with Open Policy Agent
- **Auditing** improvements

Latest release IAM v1.8.4 - released on **2024-03-25**



Dec. 2023

IAM v1.8.3

Add access token hash value.
Add missing foreign keys.
Add OpenID Connect standard claims for WLCG JWT profile.
Allow to add certificates with the same subject DN.
Fix authz code flow with PKCE.

Mar. 2024

IAM v1.8.4

Add refresh token value index.
Allow Chinese characters within user info.
Only registered users can get client credentials grant type.
Remove possibility to add a client logo URI.
Disable client editing through MitreID endpoint.

End of summer 2024

IAM v1.9.0

Token generation on AUDIT log.
Add Client's last used info.
Admins can disable clients.
Open Policy Agent external engine integration for scope policy API definition.
First 2FA implementation.
...

2025

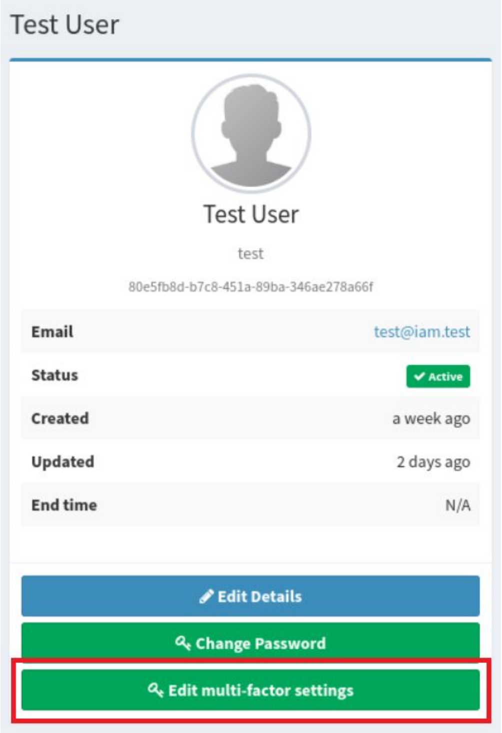
IAM v2

New IAM based on Spring Security.
New ReactJs web dashboard for admins and users.

The core of the development team is mainly at CNAF, with significant contributions from other people at INFN and STFC

Two-Factor Authentication (2FA) draft

Enabling 2FA for local credentials



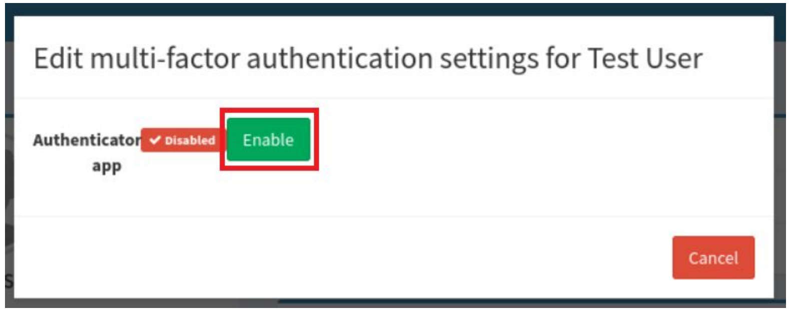
Test User

Test User

test

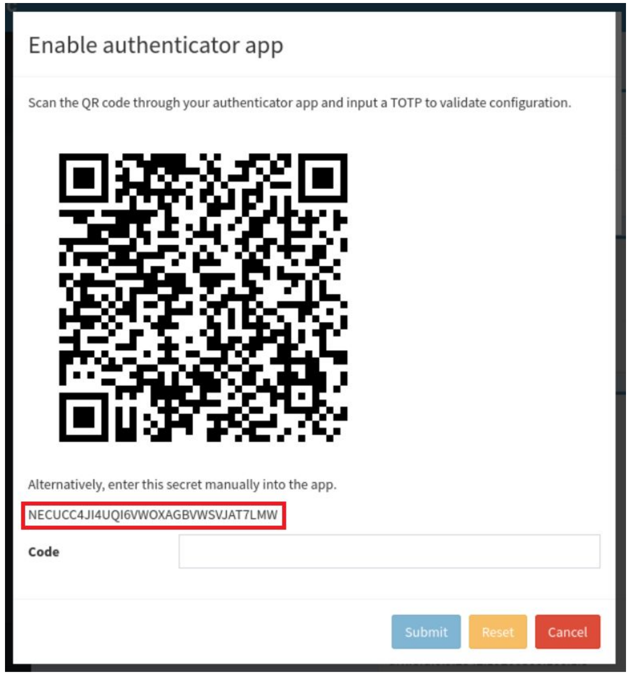
80e5fb8d-b7c8-451a-89ba-346ae278a66f

Email	test@iam.test
Status	✓ Active
Created	a week ago
Updated	2 days ago
End time	N/A



Edit multi-factor authentication settings for Test User

Authenticator app ✓ Disabled



Enable authenticator app

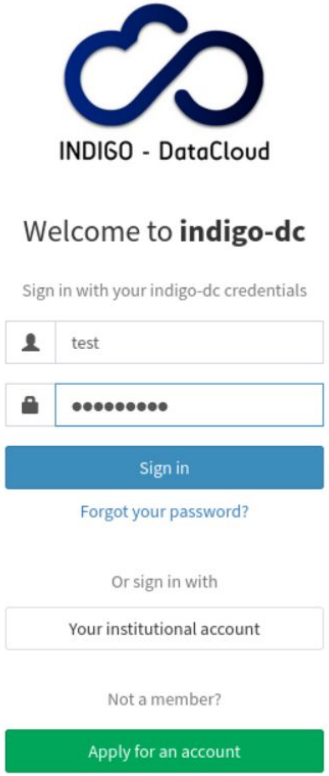
Scan the QR code through your authenticator app and input a TOTP to validate configuration.

Alternatively, enter this secret manually into the app.

NECUCC4JI4UQI6VWOXAGBVWSVJAT7LMW

Code

Signing in and verification



INDIGO - DataCloud

Welcome to **indigo-dc**

Sign in with your indigo-dc credentials

test

•••••••••

Sign in

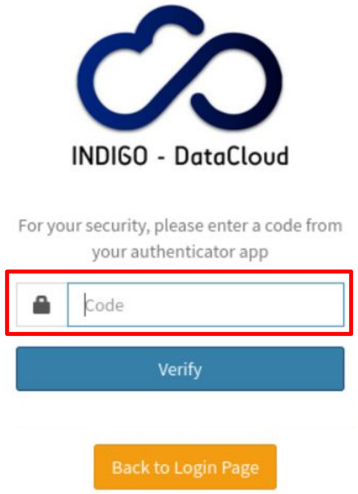
Forgot your password?

Or sign in with

Your institutional account

Not a member?

Apply for an account



INDIGO - DataCloud

For your security, please enter a code from your authenticator app

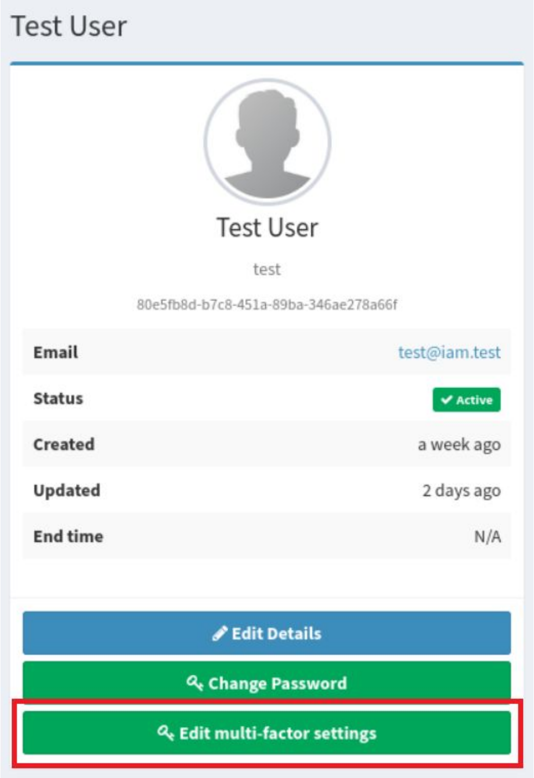
Code

Verify

Back to Login Page

Authenticated!

Disabling 2FA



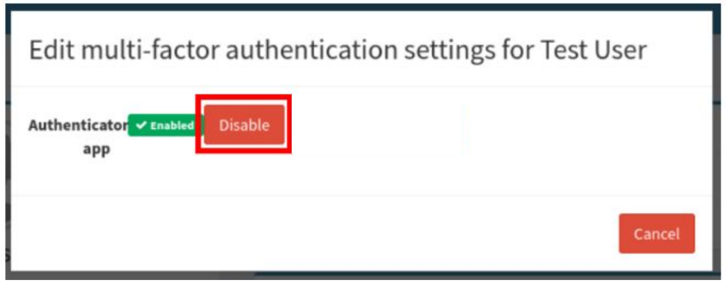
Test User

Test User

test

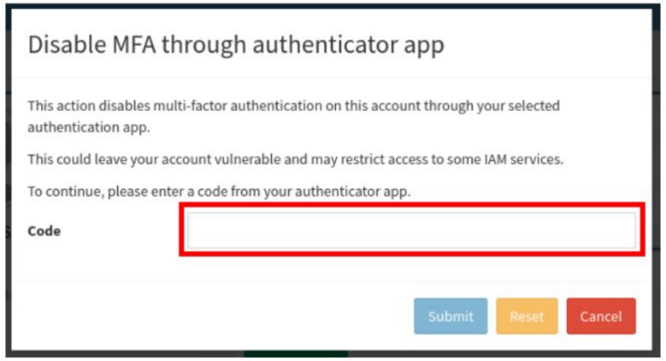
80e5fb8d-b7c8-451a-89ba-346ae278a66f

Email	test@iam.test
Status	✓ Active
Created	a week ago
Updated	2 days ago
End time	N/A



Edit multi-factor authentication settings for Test User

Authenticator app ✓ Enabled



Disable MFA through authenticator app

This action disables multi-factor authentication on this account through your selected authentication app.

This could leave your account vulnerable and may restrict access to some IAM services.

To continue, please enter a code from your authenticator app.

Code

Current 2FA implementation status

Done

- Authenticator app working for local IAM authentication
- Multi-factor settings menu on dashboard
- 2FA enabled by configuration

In progress

- Encryption and decryption of MFA secrets

To Do

- Integrate 2FA when login with external identity providers in case they do not support it
- Allow the IAM administrator to disable 2FA per user

Migration to Spring Authorization Server

Spring Authorization Server

Spring Authorization Server is a framework, built on top of **Spring Security**, that provides a secure, lightweight and customizable foundation for building an **OAuth 2.1** and **OpenID Connect 1.0** Authorization Server implementation.

Why

- We still rely on a forked and self-maintained version of MITREid Connect library which has no substantial support/evolution since few years (apart from our forked repository)
- It is a natural evolution of the current architecture Java/Spring-based
- Long-term support and easier maintainability
- Better OIDC/OAuth standards compliance
- Compliance with OAuth 2.1 standard

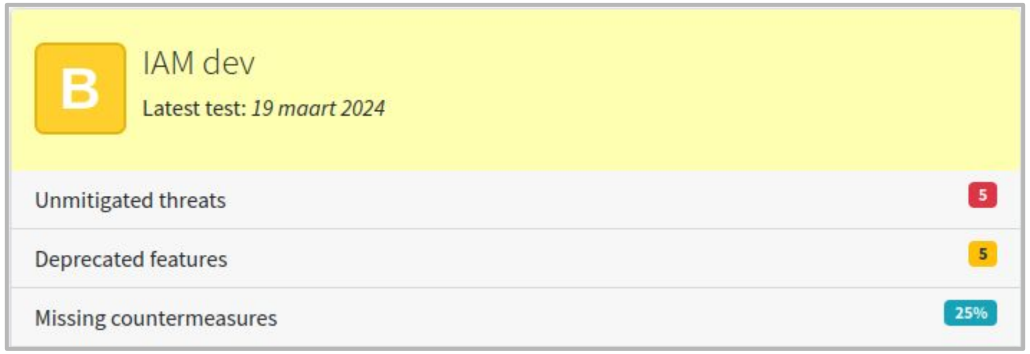
Why not

- Moving to Spring Security is definitely a priority, but we need to carefully assess whether it would be more cost-effective to enhance the current IAM code rather than depending on the SAS framework

OIDC/OAuth standards compliance

Tested with OAuch.io

Where we are…



B

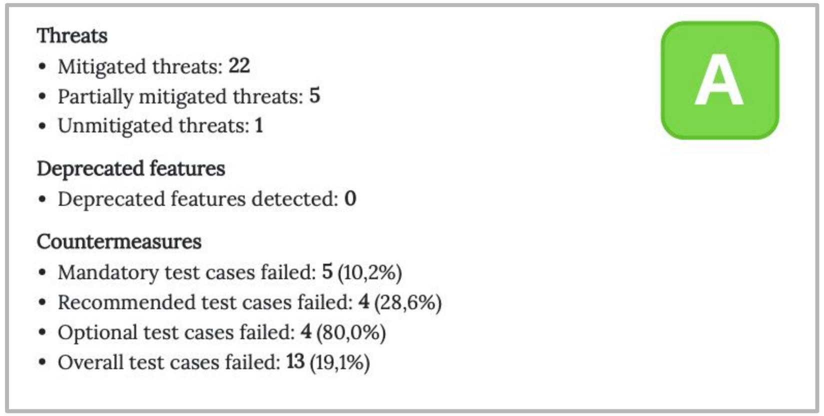
IAM dev

Latest test: *19 maart 2024*

Unmitigated threats	5
Deprecated features	5
Missing countermeasures	25%

- Based on MitreID Connect library and OAuth 2.0 standard
- OAuth 2.1 tests excluded because not supported

First tests done with a rough application built on top of Spring Authorization Server



Threats

- Mitigated threats: **22**
- Partially mitigated threats: **5**
- Unmitigated threats: **1**

Deprecated features

- Deprecated features detected: **0**

Countermeasures

- Mandatory test cases failed: **5** (10,2%)
- Recommended test cases failed: **4** (28,6%)
- Optional test cases failed: **4** (80,0%)
- Overall test cases failed: **13** (19,1%)

A

- Already supports many OAuth standard grants
- Many OIDC/OAuth endpoints are supported by default
- Tests in progress

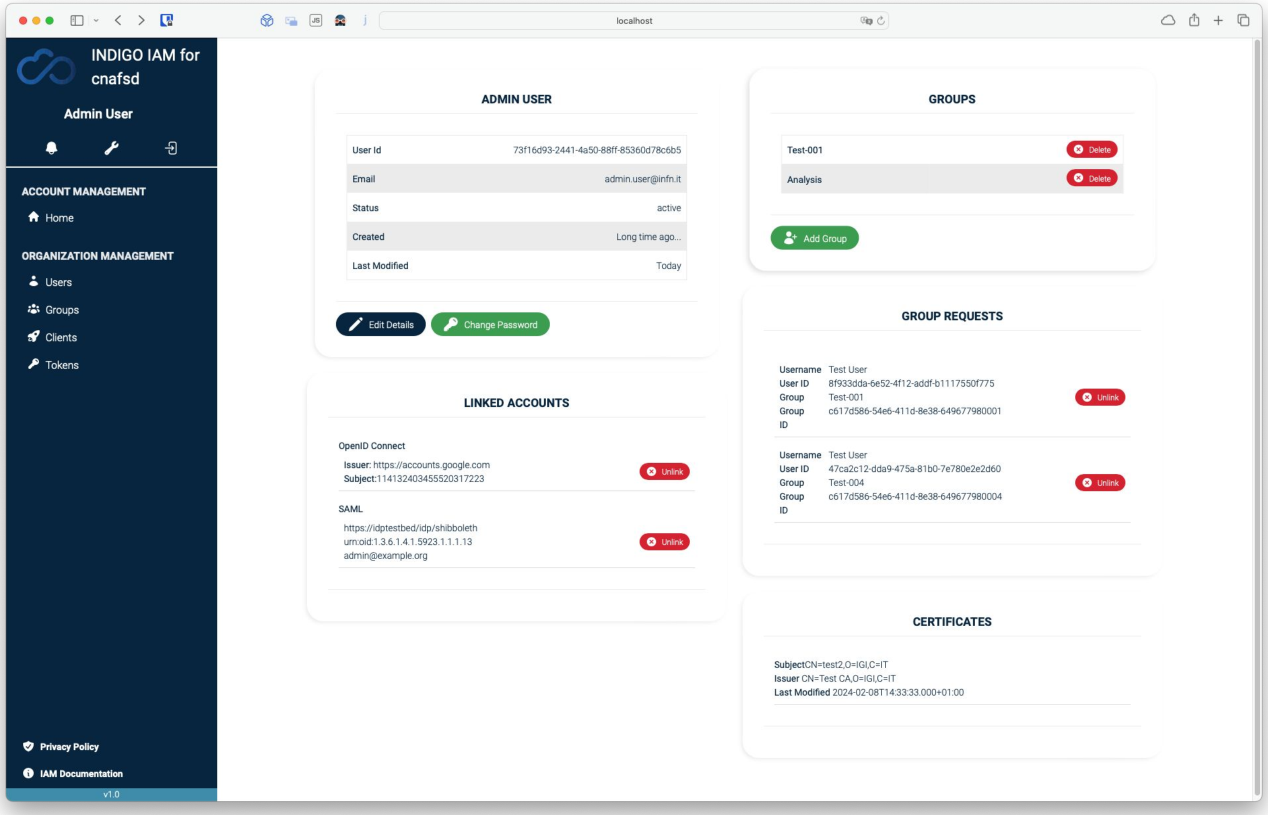
New Dashboard: a React based web application

Motivation

- Remove AngularJS (EOF) and JavaServer Pages (JSPs)
- Full support of modern **HTML5** / **TypeScript** / **CSS** development stack based
- **Decouple** the frontend code from the INDIGO IAM codebase
- Handle AuthN/AuthZ via **OpenID Connect** and **OAuth2** frameworks
- Modern and lightweight rendering framework (**React**)
- **Customizable** by different organizations
- Reuse of standard and custom web components
- **Styles harmonization** for all future INFN web applications

Proof of Concept

- Simple and lightweight
- Highly scalable
- Straightforward deployment as a Docker image
- Currently a demo version is deployed on our development Kubernetes cluster using Argo CD
- GitHub Source



ADMIN USER

User Id	73f16d93-2441-4a50-88ff-85360d78c6b5
Email	admin.user@infn.it
Status	active
Created	Long time ago...
Last Modified	Today

GROUPS

Test-001

Analysis

LINKED ACCOUNTS

OpenID Connect

Issuer: https://accounts.google.com
Subject:114132403455520317223

SAML

https://idptestbed/idp/shibboleth
urn:oid:1.3.6.1.4.1.5923.1.1.1.13
admin@example.org

GROUP REQUESTS

Username	Test User
User ID	8f933dda-6e52-4f12-addf-b1117550f775
Group	Test-001
Group ID	c617d586-54e6-411d-8e38-649677980001

Username	Test User
User ID	47ca2c12-dda9-475a-81b0-7e780e2e2d60
Group	Test-004
Group ID	c617d586-54e6-411d-8e38-649677980004

CERTIFICATES

SubjectCN=test2,O=IGI,C=IT
Issuer CN=Test CA,O=IGI,C=IT
Last Modified 2024-02-08T14:33:33.000+01:00

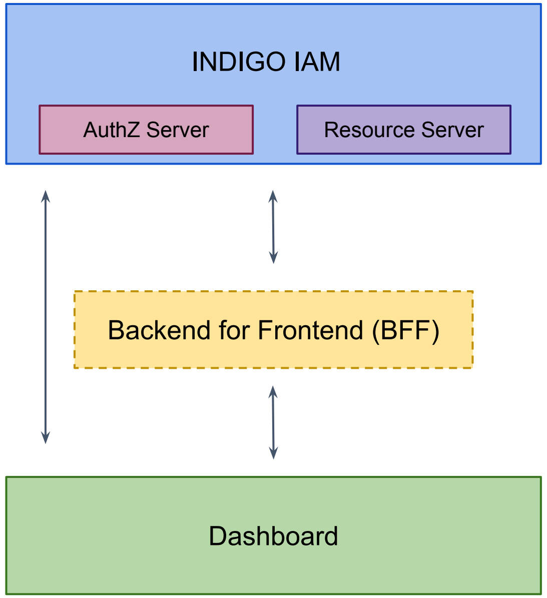
Homepage example

Application architecture pattern

We are following the **Backend For Frontend (BFF)** pattern for security reasons

- The BFF interacts with the authorization server as a confidential OAuth client
- The BFF manages OAuth tokens within a cookie-based session, keeping them secure from the JavaScript application
- The BFF forwards all requests to a resource server after adding the appropriate access token

We are using Next.js, an advanced web development framework, for server-side rendering



Source: https://datatracker.ietf.org/doc/draft-ietf-oauth-browser-based-apps/

Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

terabit

Thanks for your attention!

Useful references

IAM on GitHub: https://github.com/indigo-iam/iam

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

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

For general information:

- OAuth 2.0: https://oauth.net/2/ and OAuth 2.1: https://oauth.net/2.1/
- OpenID Connect: https://openid.net/connect/

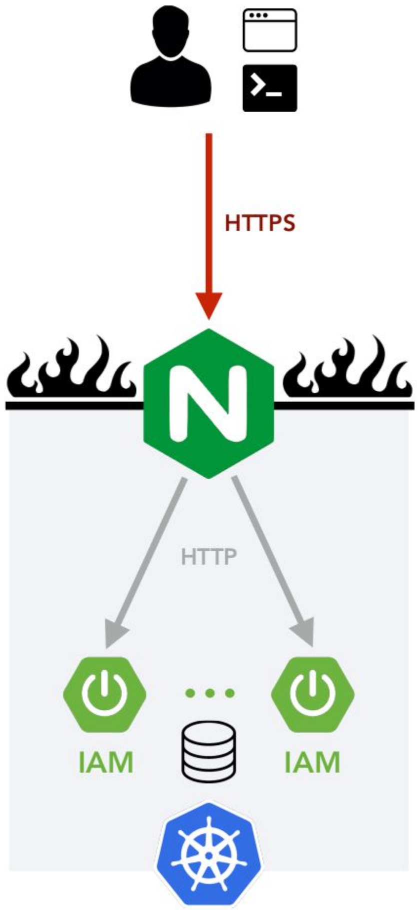
Contacts:

- iam-support@lists.infn.it

Backup slides

IAM core technologies

- **Java** application based on the **Spring Boot** framework
  - OIDC/OAuth 2.0 implementation currently based on the MITREid Connect
  - deployed behind an **NGINX**
  - stores data in a **MariaDB/MySQL** database
- Typically deployed as a **Docker container** in **Kubernetes**
- Horizontally scalable
  - sessions and external caching stored into Redis
- Deployment in HA is possible



(Some) Existing IAM deployments

- (CNAF) Several IAMs to control access to PaaS and SaaS services offered by **INFN Cloud**, to the OpenStack-based **CNAF Cloud** and, for small experiments, to some **INFN Tier-1 services**
- (CNAF) Several IAMs hosted for **other collaborations**: ILDG, Belle-II, HERD, JUNO, etc.
- (CERN) One IAM for each **LHC experiment**
- From T. Dack (STFC): *Since 2018, STFC has been operating a production instance of IAM as a multi-VO identity proxy, authorisation platform and IdP of last resort, to provide access to a broad range of services of IRIS, the coordinating body for STFC science activities*
- From M. Jouvin (IN2P3): *we are currently running three production instances. In every case, it was to provide a unified and pervasive, token-based, authN/Z service to new projects/communities where there was no pre-existing PKI-based (e.g. VOMS) federated AAI. The 3 projects are **MesoNET**, **EURO-LABS**, **GRANDMA***
- Under evaluation, at different stages, in CTA, SKA, ET, etc.