Beyond X.509: Token-based Authentication and Authorization with the INDIGO Identity and Access Management Service

Andrea Ceccanti
andrea.ceccanti@cnaf.infn.it

Workshop CCR
Rimini, June 12th 2018

INDIGO IAM: main requirements

Provide a central **Identity and Authorization Service** to support scientific computing

- Based on **existing** and **popular** standards (**do not reinvent the wheel**)
- Providing **flexible authentication and authorization** to integrated services
- **Easy** to integrate ~~SAML~~
- Supporting **delegation** and long-running applications
- **Mobile-friendly**

IAM developed at INFN CNAF during the INDIGO DataCloud project with a **strong focus on code quality and testing**

INDIGO Identity and Access Management service

Flexible authentication support (SAML, X.509, OpenID Connect, username/password, …)

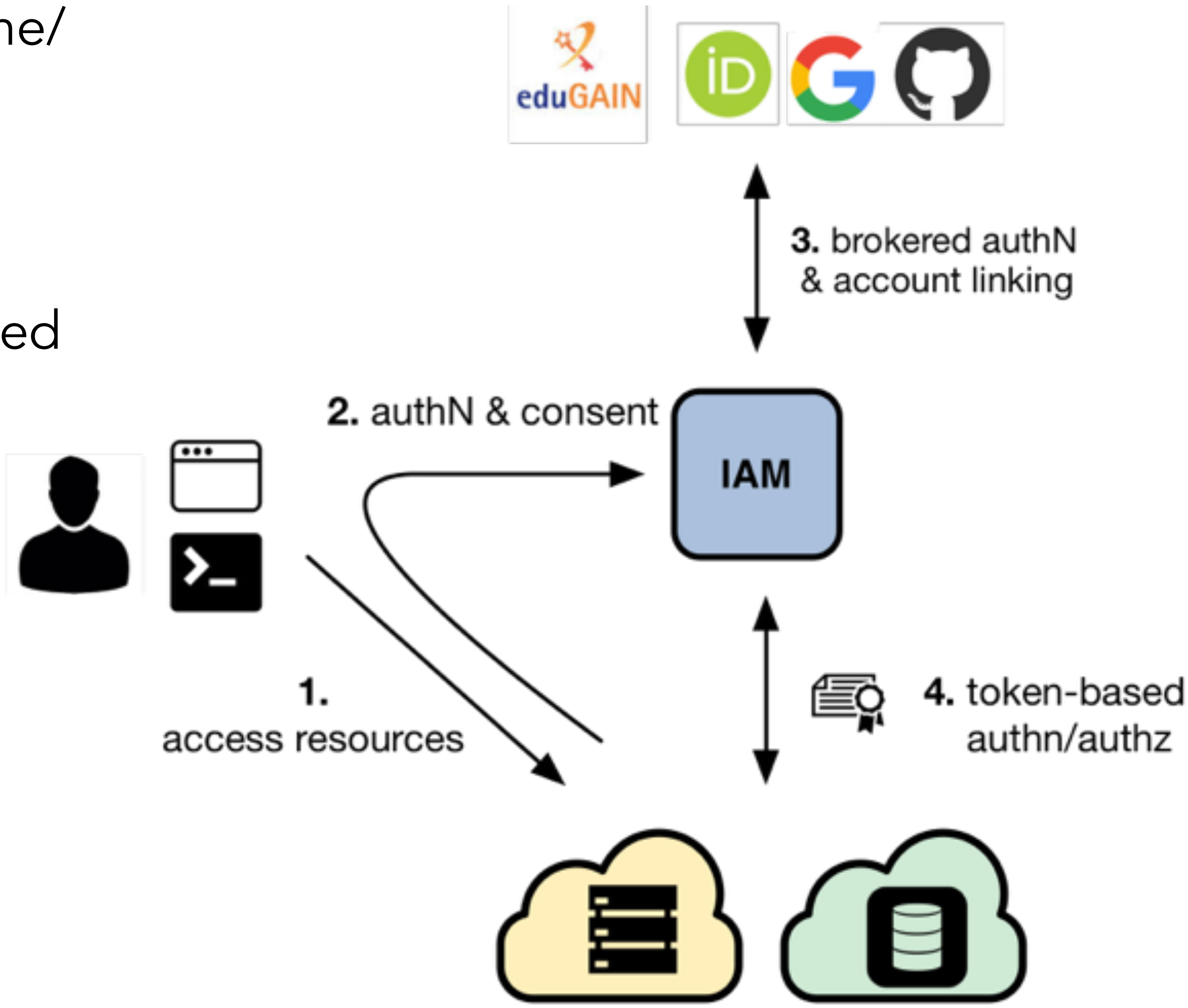
Account linking

Registration service for moderated and automatic user enrollment

AUP enforcement support

Mobile-friendly organization management tools

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

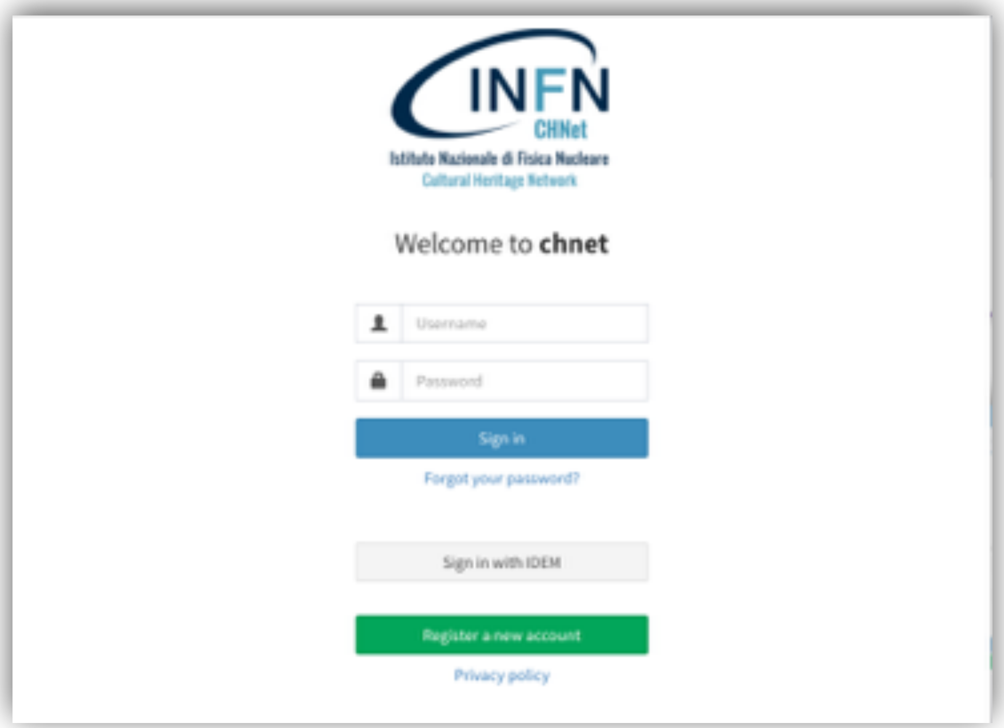

eduGAIN
3. brokered authN & account linking
2. authN & consent
IAM
1. access resources
4. token-based authn/authz

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.



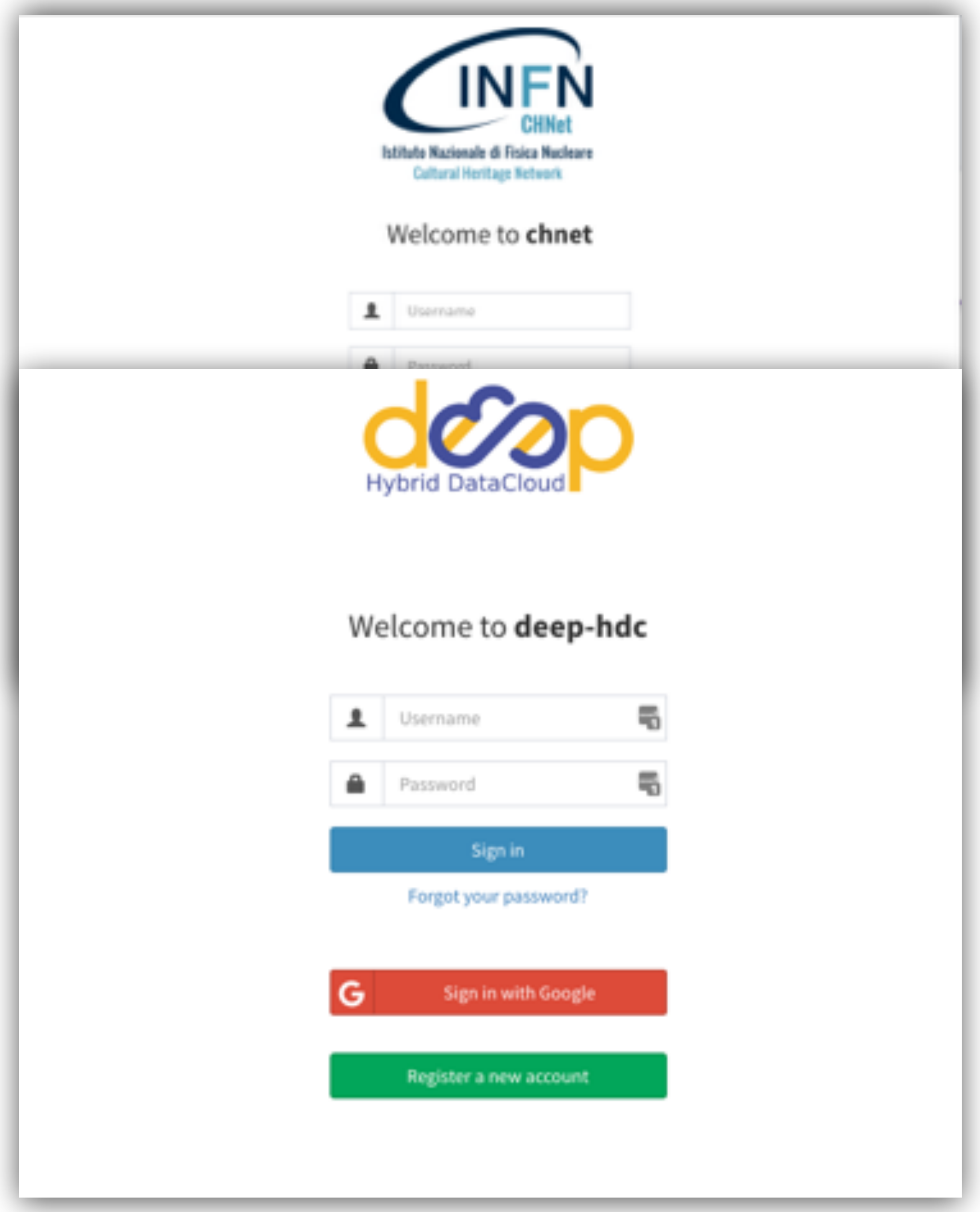
Welcome to **chnet**

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.

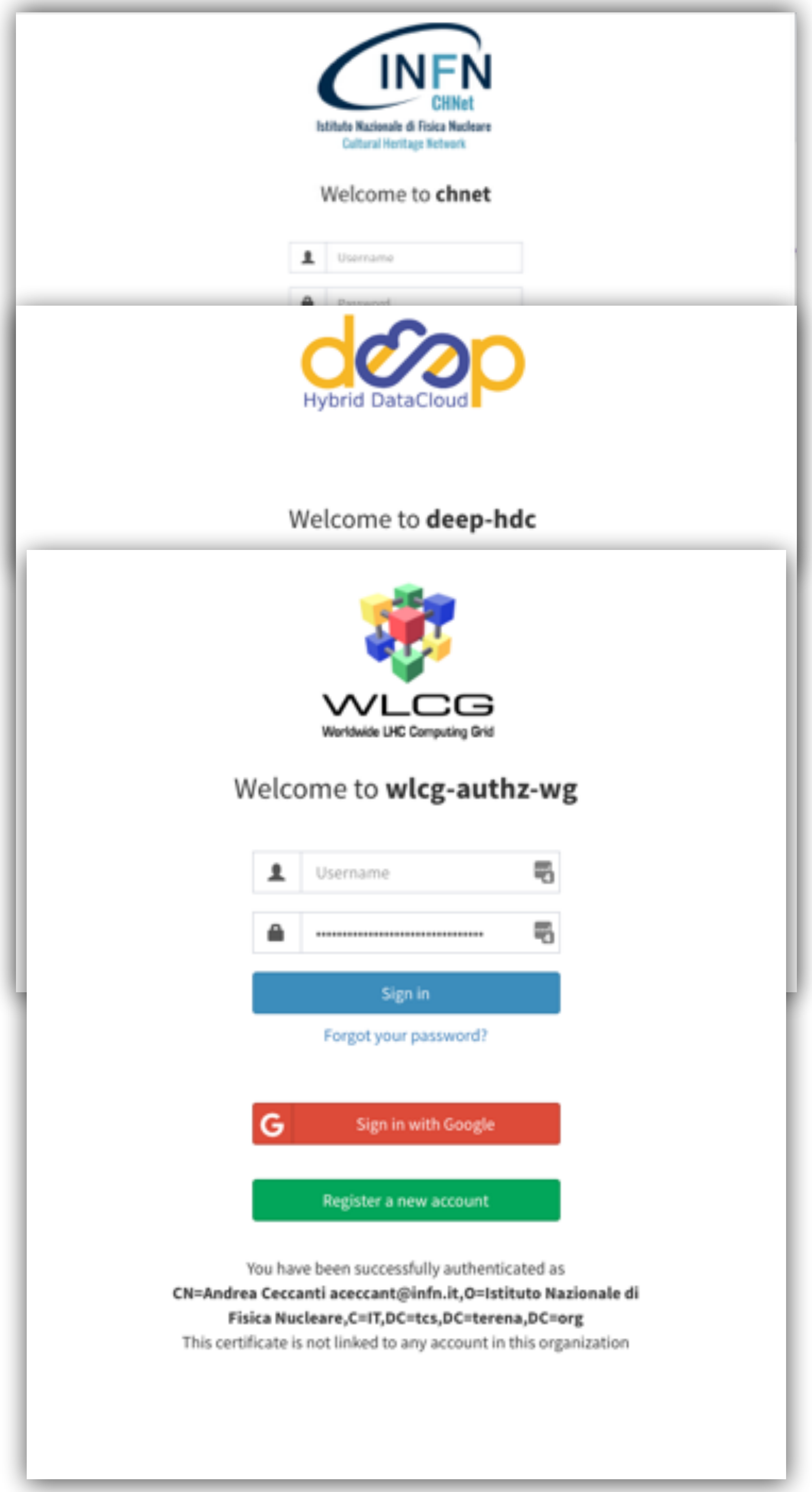


IAM deployment model

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.



INFN
CHNet
Istituto Nazionale di Fisica Nucleare
Cultural Heritage Network

Welcome to **chnet**

Welcome to **deep-hdc**

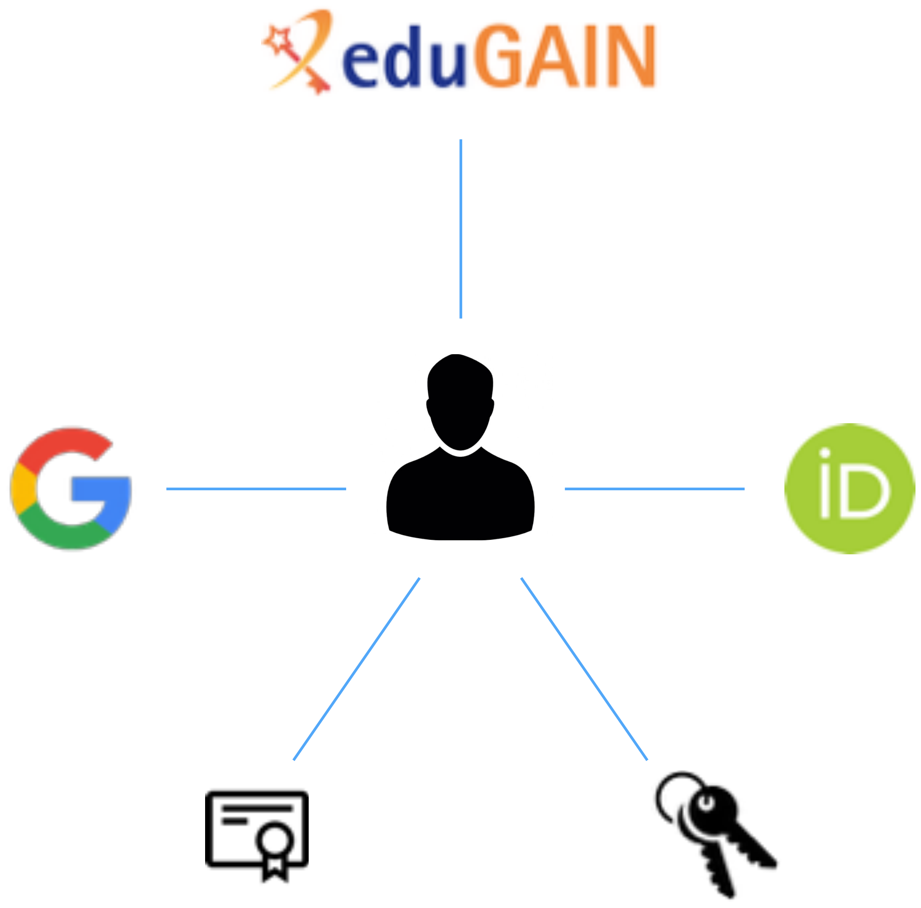
Welcome to **wlcg-authz-wg**

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

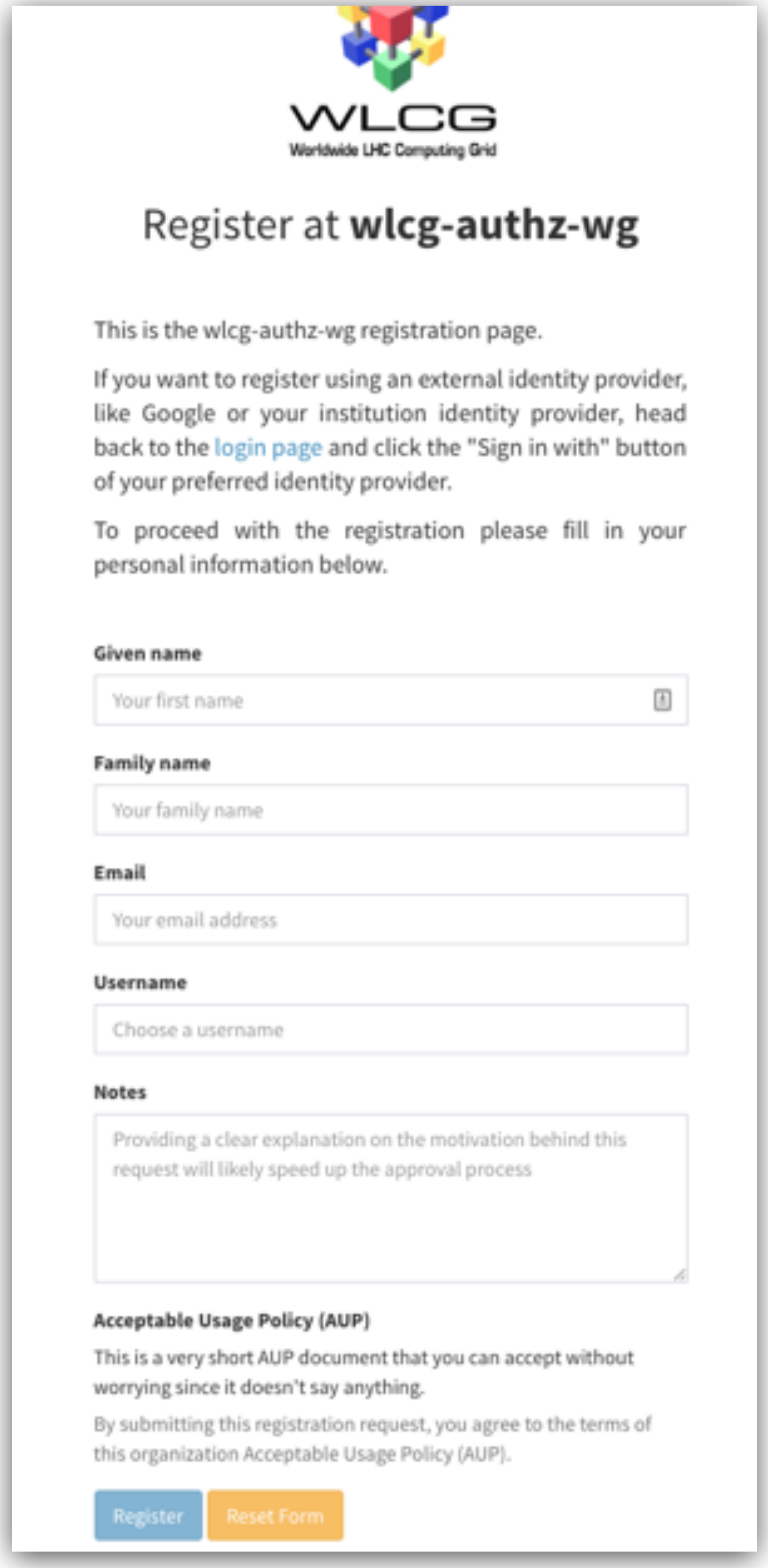
IAM supports two **enrollment flows:**

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



Register at **wlcg-authz-wg**

This is the wlcg-authz-wg registration page.

If you want to register using an external identity provider, like Google or your institution identity provider, head back to the login page and click the "Sign in with" button of your preferred identity provider.

To proceed with the registration please fill in your personal information below.

Given name

Your first name

Family name

Your family name

Email

Your email address

Username

Choose a username

Notes

Providing a clear explanation on the motivation behind this request will likely speed up the approval process

Acceptable Usage Policy (AUP)

This is a very short AUP document that you can accept without worrying since it doesn't say anything.

By submitting this registration request, you agree to the terms of this organization Acceptable Usage Policy (AUP).

User enrollment & registration service

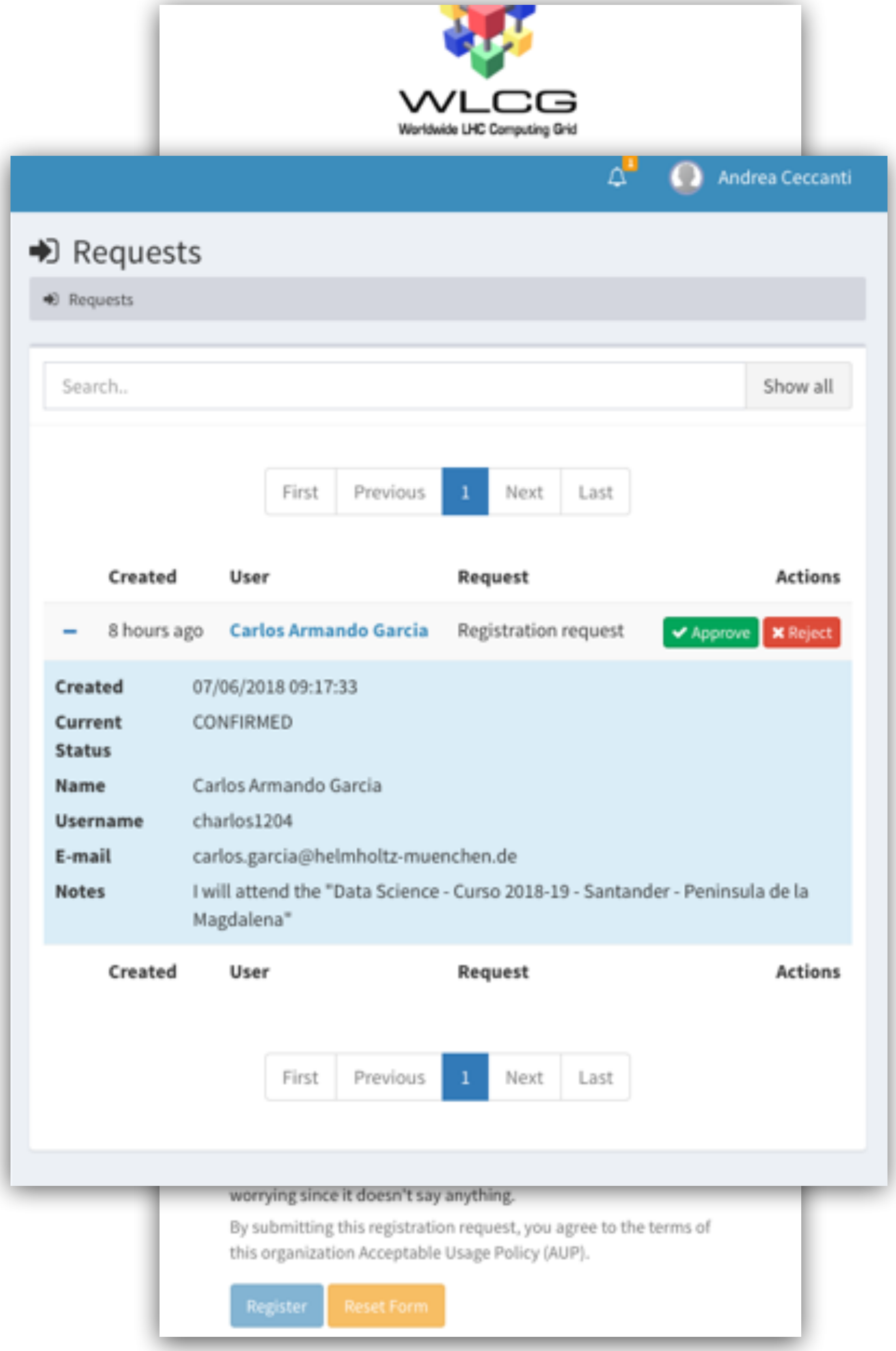
IAM supports two **enrollment flows:**

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



Requests

Requests

Search.. Show all

First Previous 1 Next Last

	Created	User	Request	Actions
–	8 hours ago	Carlos Armando Garcia	Registration request	✓ Approve ✖ Reject

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

Created	User	Request	Actions

First Previous 1 Next Last

worrying since it doesn't say anything.

By submitting this registration request, you agree to the terms of this organization Acceptable Usage Policy (AUP).

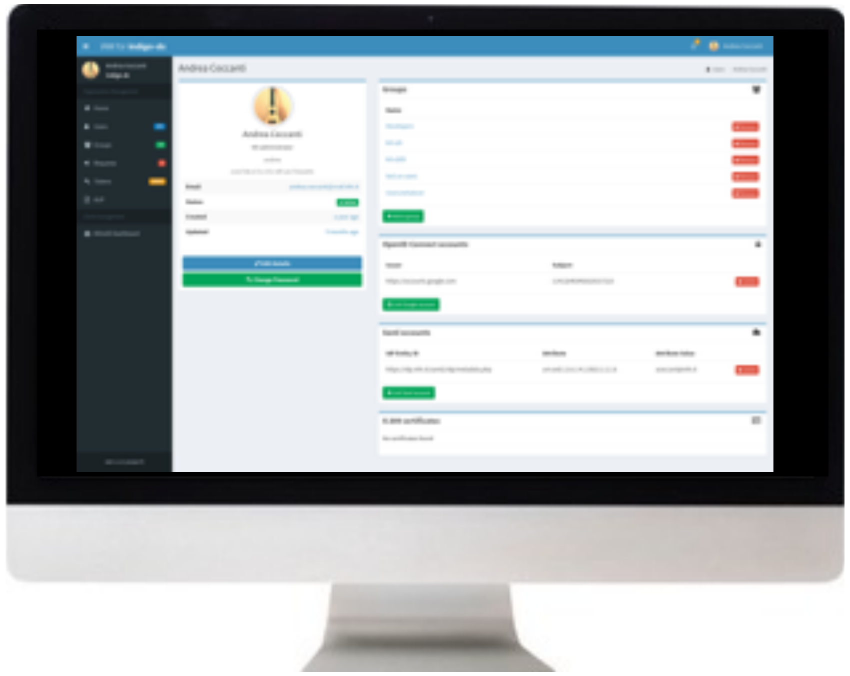
Register Reset Form

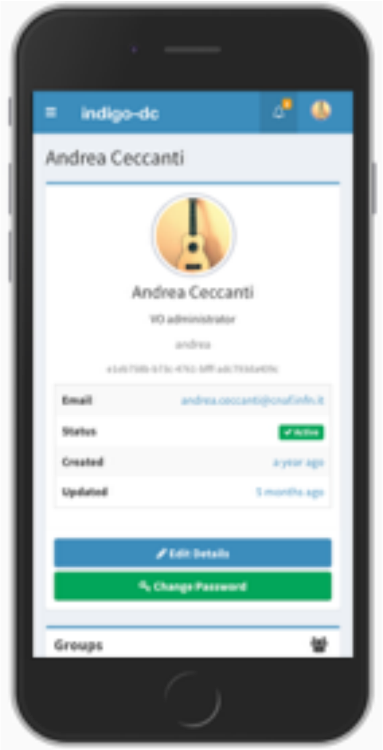
Management tools

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





Andrea Ceccanti

VO administrator

andrea

[illegible]

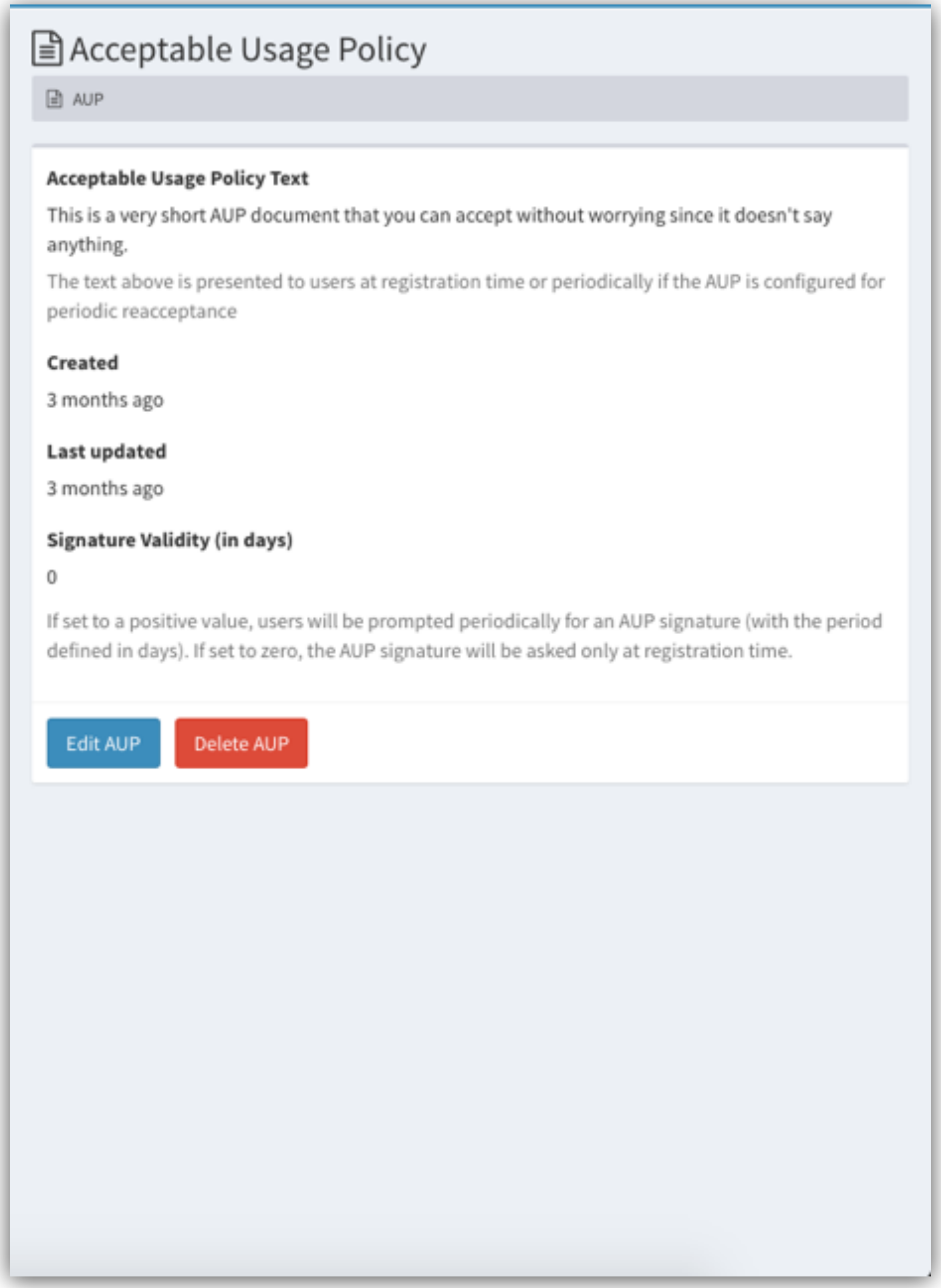
Email	andrea.ceccanti@cnaf.infn.it
Status	✓ Active
Created	a year ago
Updated	5 months ago

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



Acceptable Usage Policy

AUP

Acceptable Usage Policy 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

Created

3 months ago

Last updated

3 months ago

Signature Validity (in days)

0

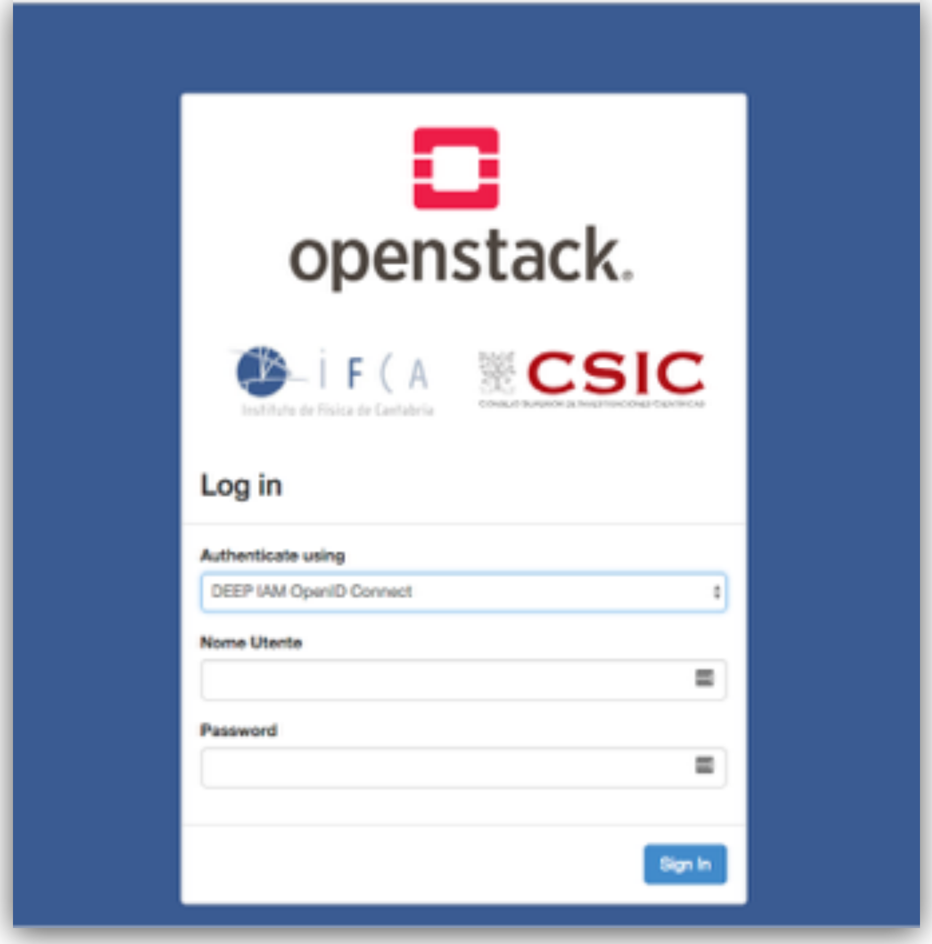
If set to a positive value, users will be prompted periodically for an AUP signature (with the period defined in days). If set to zero, the AUP signature will be asked only at registration time.

Easy integration with services

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

We have successfully integrated IAM with minimal effort with:

- Openstack
- Atlassian JIRA & Confluence
- Moodle
- Rocketchat
- Grafana
- Kubernetes
- JupyterHub



Log in

Authenticate using

DEEP IAM OpenID Connect

Nome Utente

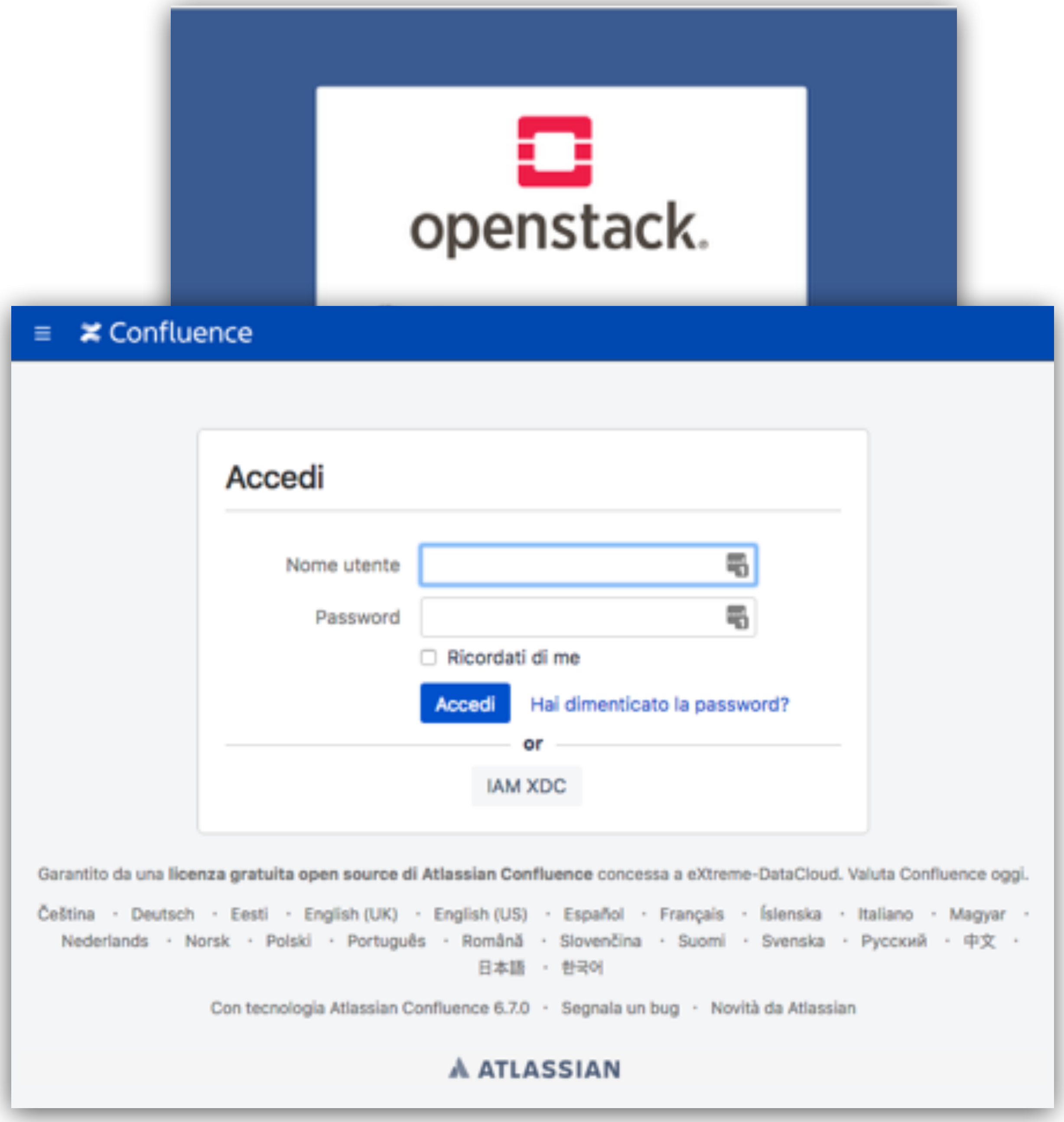
Password

Easy integration with services

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

We have successfully integrated IAM with minimal effort with:

- Openstack
- Atlassian JIRA & Confluence
- Moodle
- Rocketchat
- Grafana
- Kubernetes
- JupyterHub



Garantito da una **licenza gratuita open source di Atlassian Confluence** concessa a eXtreme-DataCloud. Valuta Confluence oggi.

Čeština · Deutsch · Eesti · English (UK) · English (US) · Español · Français · Íslenska · Italiano · Magyar · Nederlands · Norsk · Polski · Português · Română · Slovenčina · Suomi · Svenska · Русский · 中文 · 日本語 · 한국어

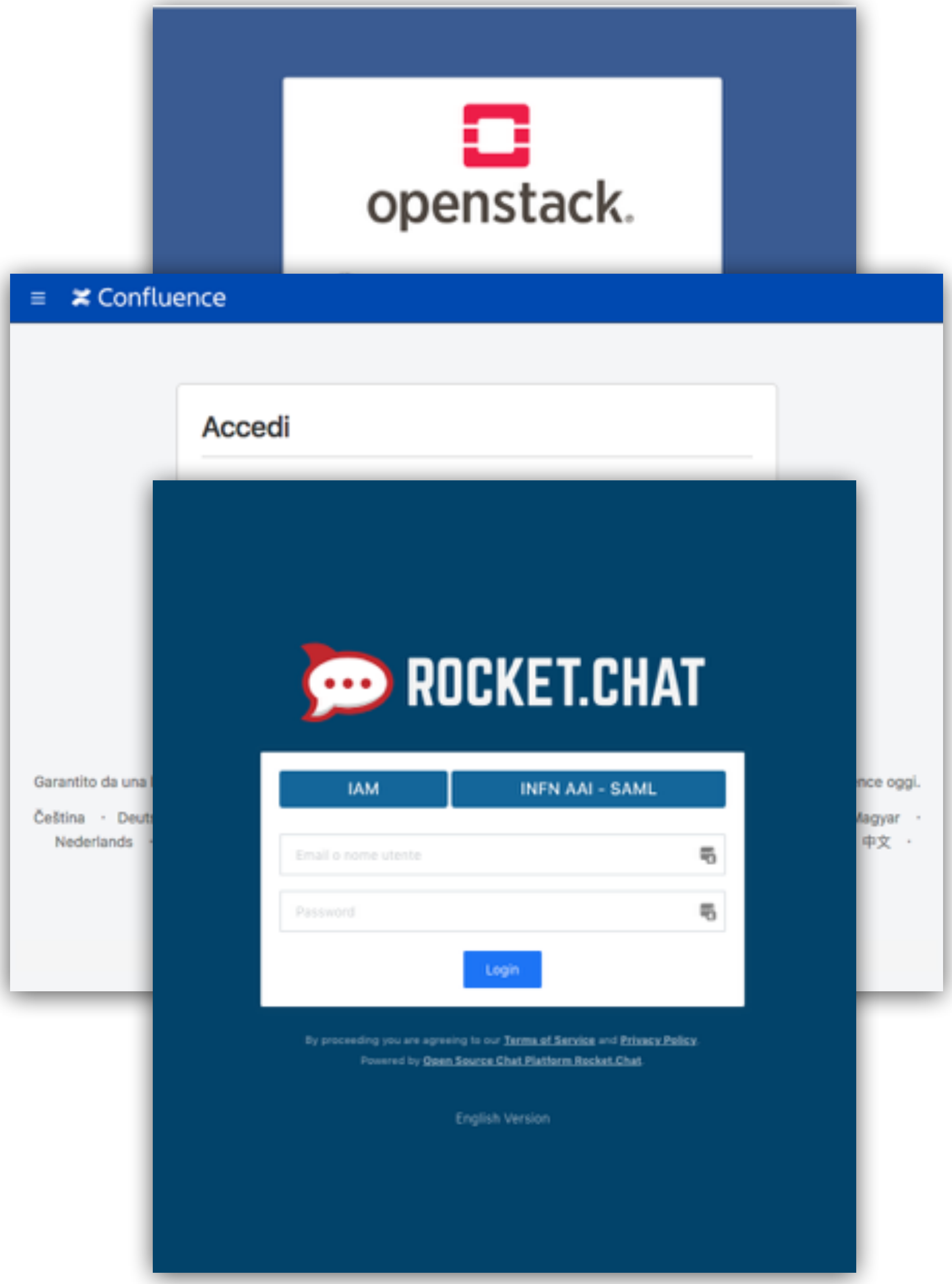
Con tecnologia Atlassian Confluence 6.7.0 · Segnala un bug · Novità da Atlassian

Easy integration with services

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

We have successfully integrated IAM with minimal effort with:

- Openstack
- Atlassian JIRA & Confluence
- Moodle
- Rocketchat
- Grafana
- Kubernetes
- JupyterHub



Demo

Technical details

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

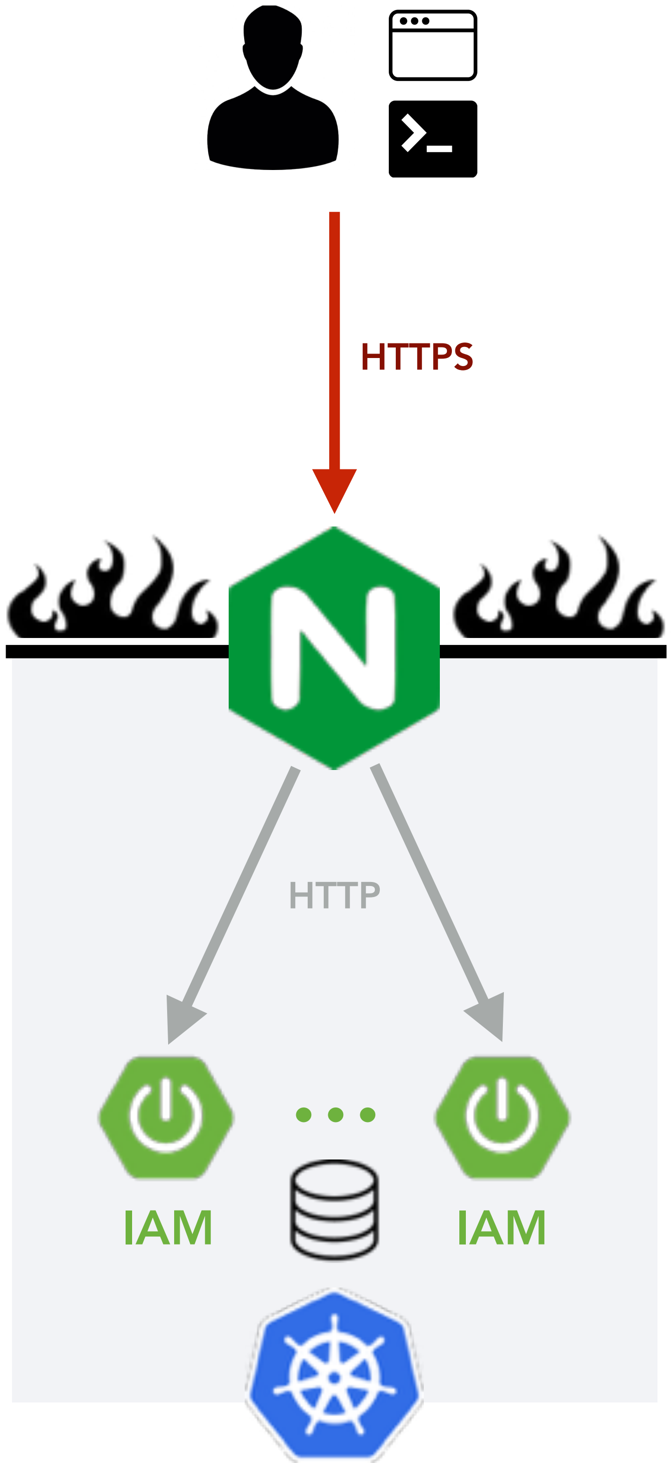
- all state persisted in the database

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

- autoscaling, zero downtime rolling updates

And provide packages for

- CENTOS 7, UBUNTU 1604



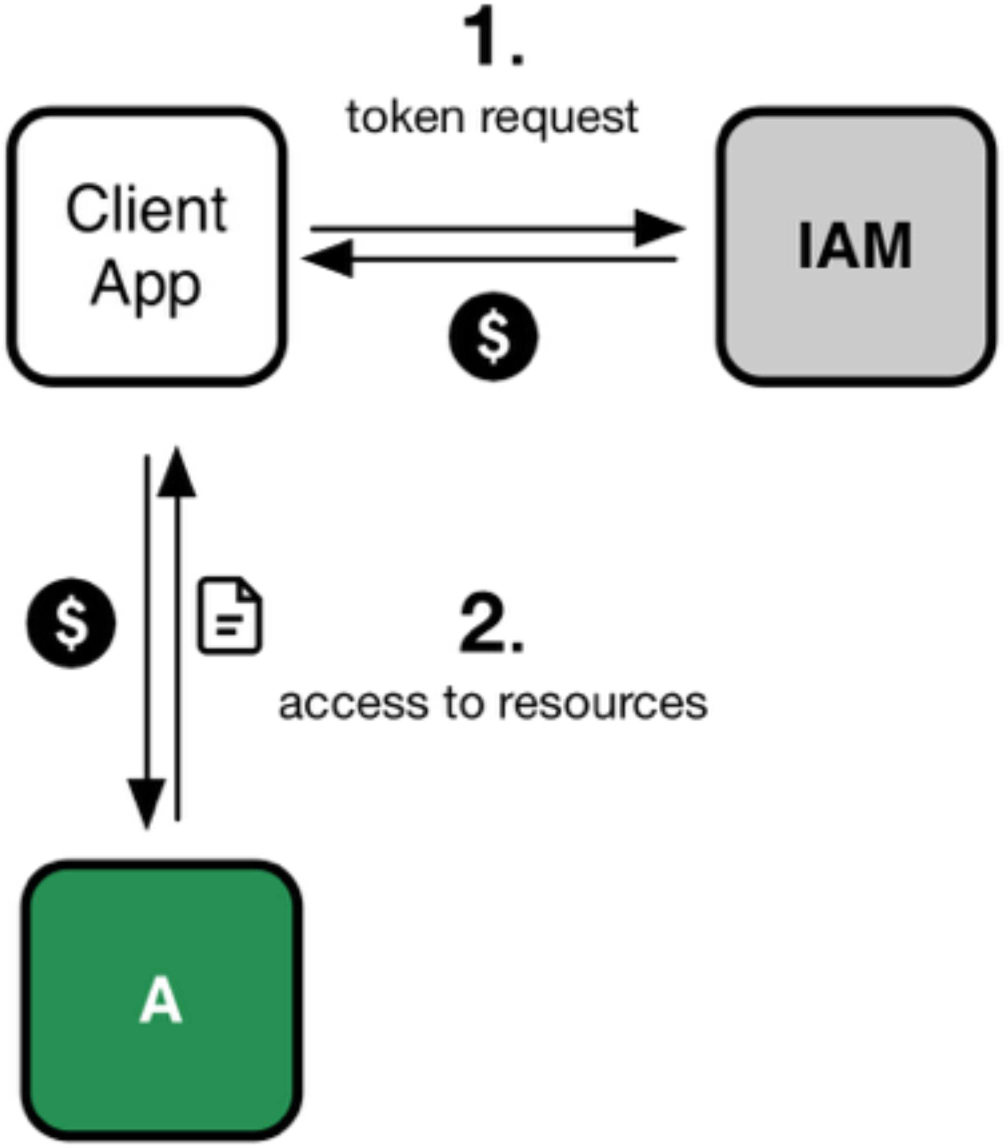
Token-based AuthN/AuthZ with OAuth/OIDC

In order to acces resources, a **client** needs an **access token**

The token is obtained from **IAM** using standard **OAuth/OpenID Connect** flows

Authorization is then performed @ the services leveraging:

- **OAuth scopes**: authorization lables that can be linked to access token at token creation time
- **Identity attributes**: e.g., Organization name,



INDIGO IAM tokens: signed JWTs

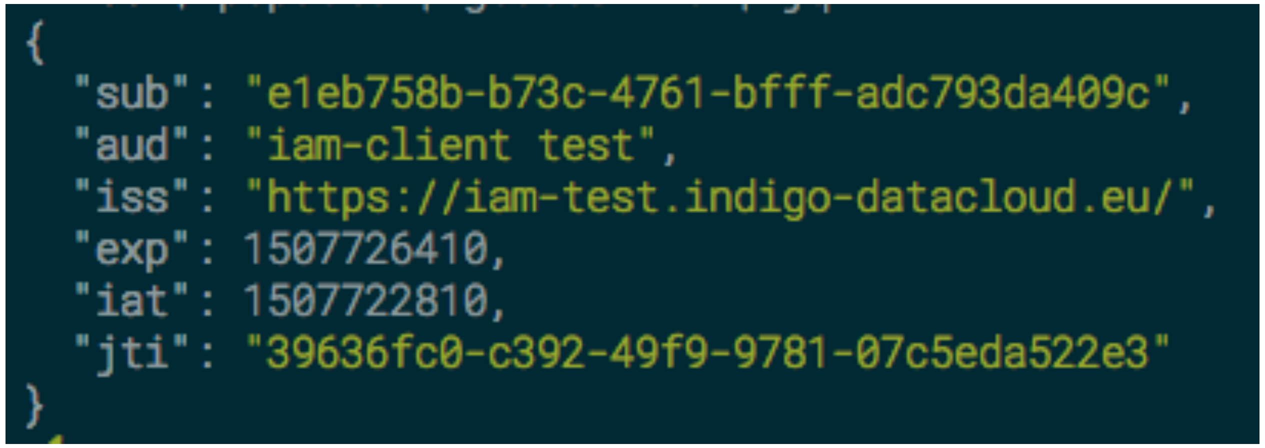
IAM uses **structured, self-contained access tokens**

- signed JSON Web Tokens (JWT)

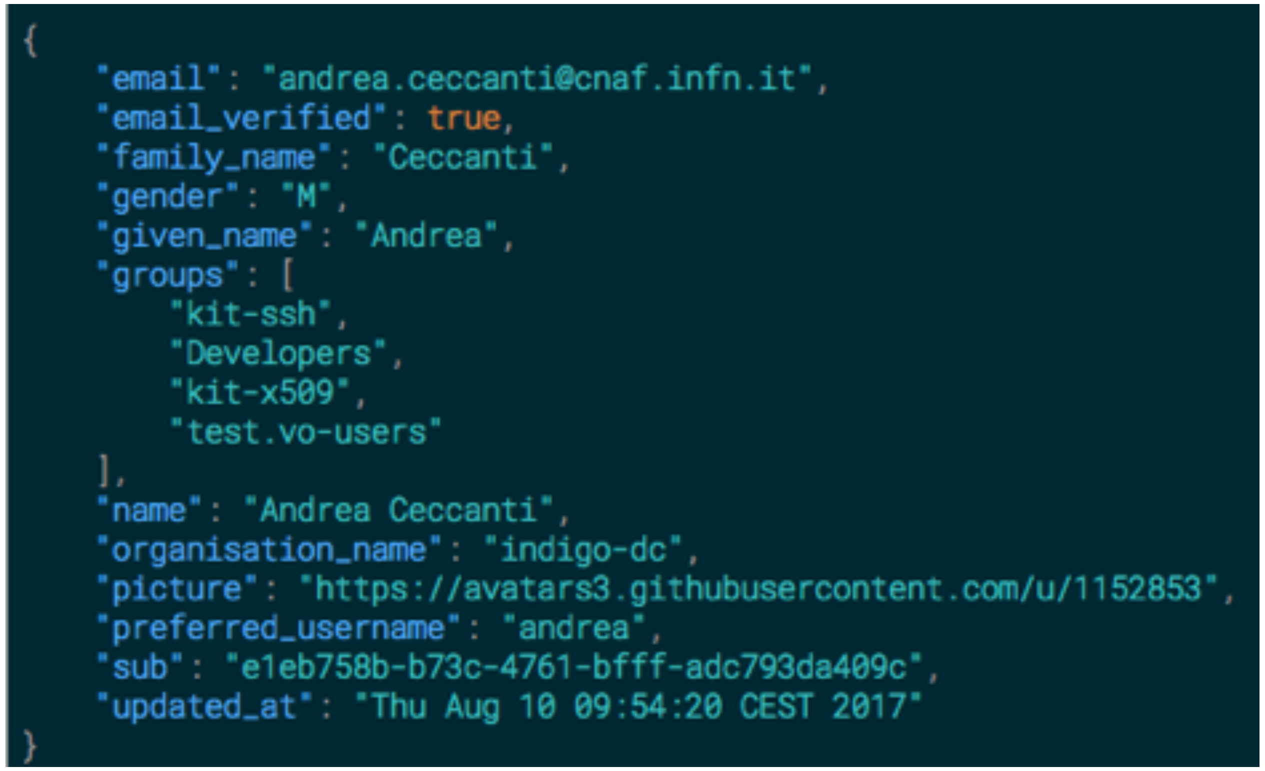
Access tokens provide to applications basic **authorization** information

- IAM can be configured to include selected AuthN info in access tokens

Authentication info about can be obtained via **OAuth token introspection & OpenID Connect userinfo** IAM endpoints

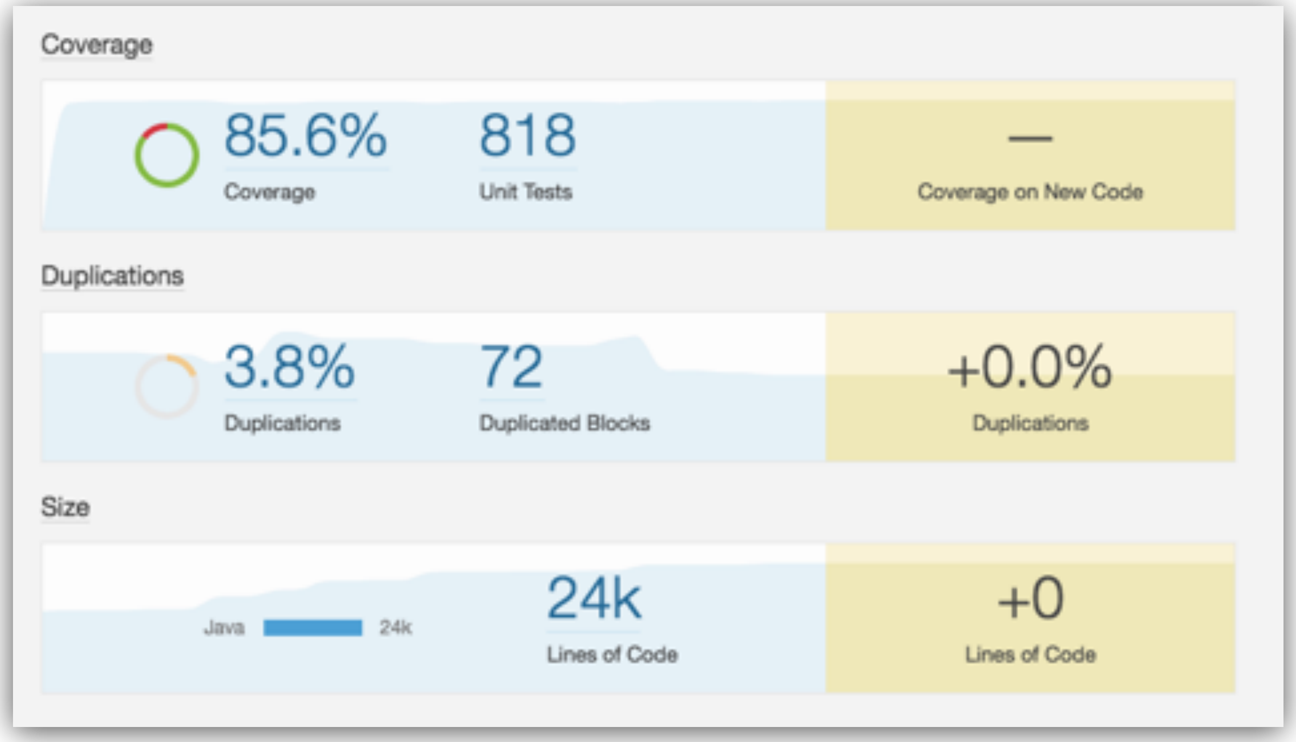


```
{
  "sub": "e1eb758b-b73c-4761-bfff-adc793da409c",
  "aud": "iam-client test",
  "iss": "https://iam-test.indigo-datacloud.eu/",
  "exp": 1507726410,
  "iat": 1507722810,
  "jti": "39636fc0-c392-49f9-9781-07c5eda522e3"
}
```



```
{
    "email": "andrea.ceccanti@cnaf.infn.it",
    "email_verified": true,
    "family_name": "Ceccanti",
    "gender": "M",
    "given_name": "Andrea",
    "groups": [
        "kit-ssh",
        "Developers",
        "kit-x509",
        "test.vo-users"
    ],
    "name": "Andrea Ceccanti",
    "organisation_name": "indigo-dc",
    "picture": "https://avatars3.githubusercontent.com/u/1152853",
    "preferred_username": "andrea",
    "sub": "e1eb758b-b73c-4761-bfff-adc793da409c",
    "updated_at": "Thu Aug 10 09:54:20 CEST 2017"
}
```

Software Quality



Coverage

85.6% Coverage

818 Unit Tests

— Coverage on New Code

Duplications

3.8% Duplications

72 Duplicated Blocks

+0.0% Duplications

Size

Java 24k

24k Lines of Code

+0 Lines of Code

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

- now 24k LoC, 85.6% branch coverage, >800 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)

Software Quality

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

- now 24k LoC, 85.6% branch coverage, >800 tests

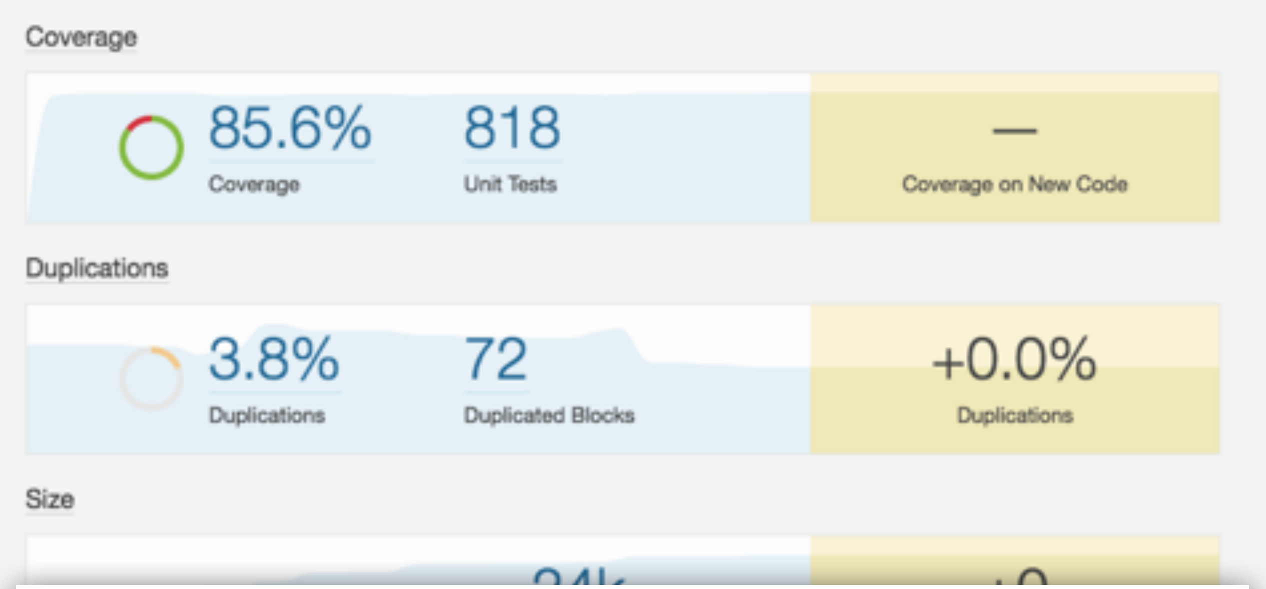
Open, **test-driven** development process

Static analysis tools

- SonarCube IAM page

Multiple test suites

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



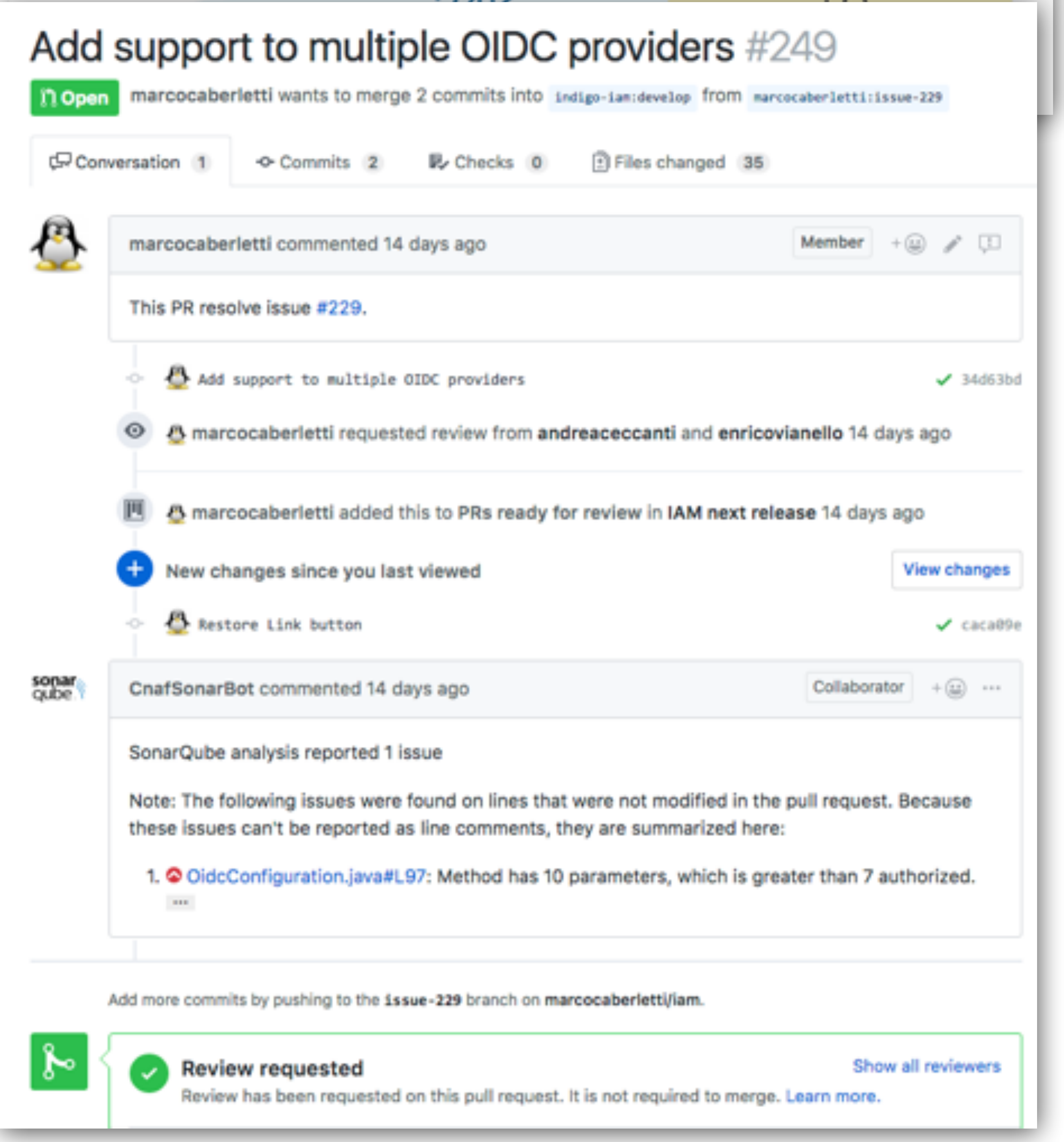
Coverage

85.6% Coverage | 818 Unit Tests | — Coverage on New Code

Duplications

3.8% Duplications | 72 Duplicated Blocks | +0.0% Duplications

Size



Add support to multiple OIDC providers #249

Open marcocaberletti wants to merge 2 commits into `indigo-iam:develop` from `marcocaberletti:issue-229`

marcocaberletti commented 14 days ago

This PR resolve issue #229.

`Add support to multiple OIDC providers` ✓ 34d63bd

marcocaberletti requested review from **andreaceccanti** and **enricovianello** 14 days ago

marcocaberletti added this to PRs ready for review in **IAM next release** 14 days ago

New changes since you last viewed

`Restore Link button` ✓ caca09e

CnafSonarBot commented 14 days ago

SonarQube analysis reported 1 issue

Note: The following issues were found on lines that were not modified in the pull request. Because these issues can't be reported as line comments, they are summarized here:

1. OidcConfiguration.java#L97: Method has 10 parameters, which is greater than 7 authorized.

Add more commits by pushing to the **issue-229** branch on **marcocaberletti/iam**.

Review requested
Review has been requested on this pull request. It is not required to merge. Learn more.

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
- 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

Contacts:

- andrea.ceccanti@cnaf.infn.it
- indigo-aai.slack.com

Thanks!

Questions?