



Status and prospects of WLCG transition to tokens

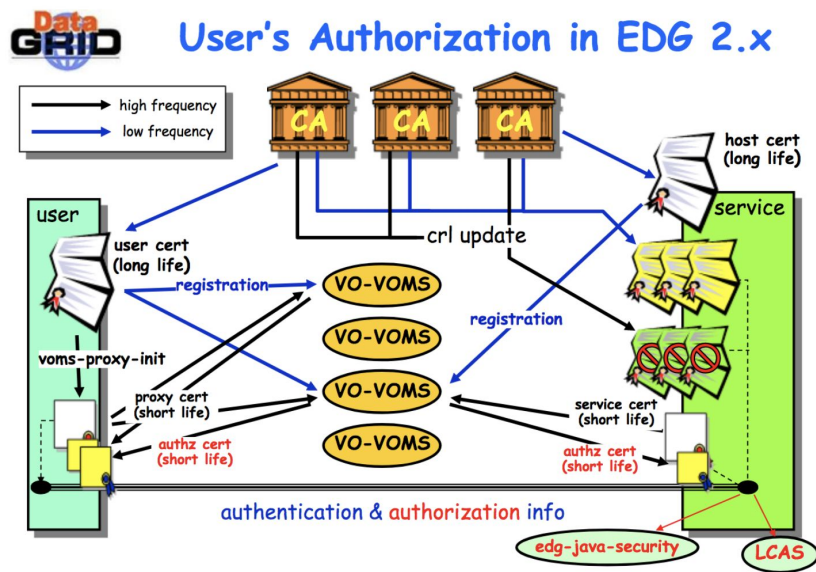
Evolution of the WLCG AAI beyond X.509

Enrico Vianello

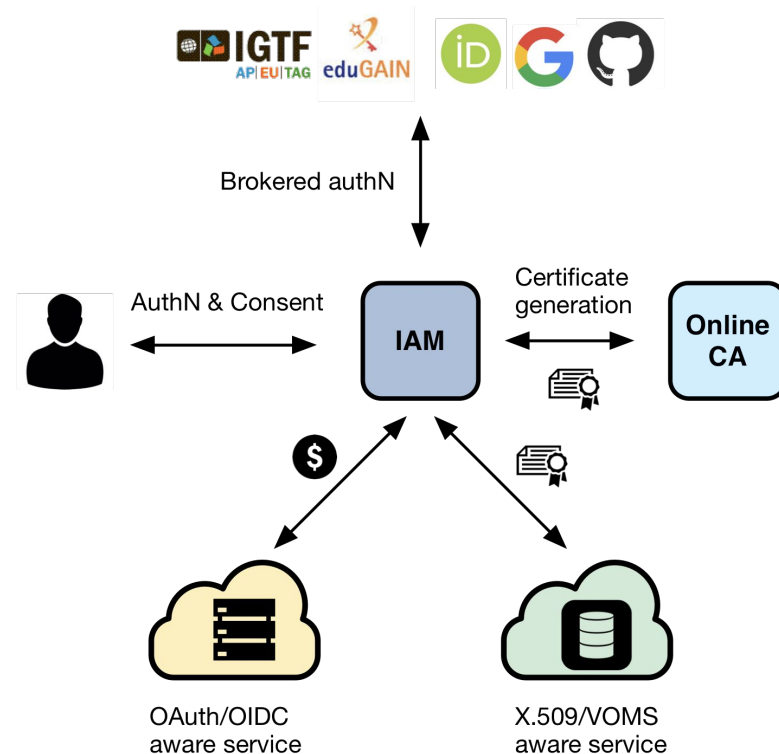
INFN-CNAF

Workshop sul Calcolo nell'I.N.F.N. @ Paestum 23 - 27 maggio 2022

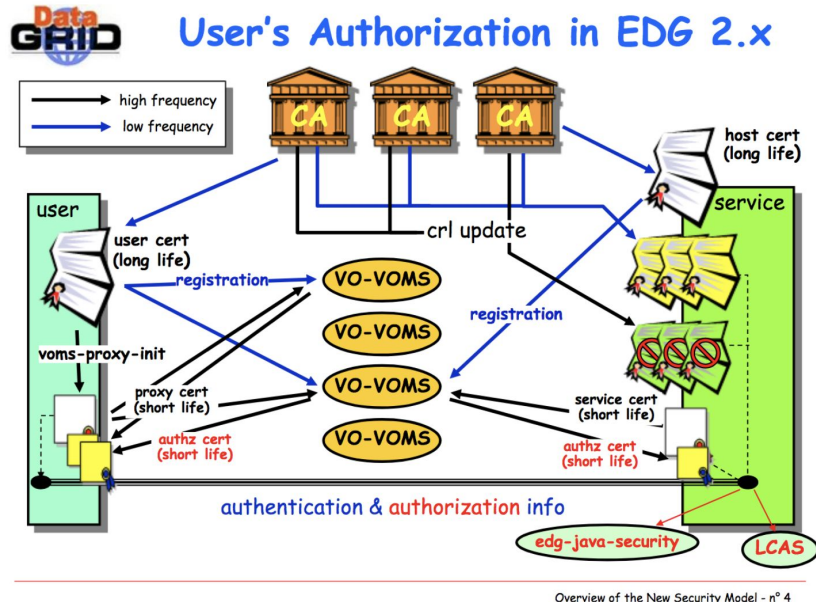
Evolution of the WLCG AAI beyond X.509



Overview of the New Security Model - n° 4



Evolution of the WLCG AAI beyond X.509



To access computing and storage resources in the WLCG community, users use a **VOMS proxy**

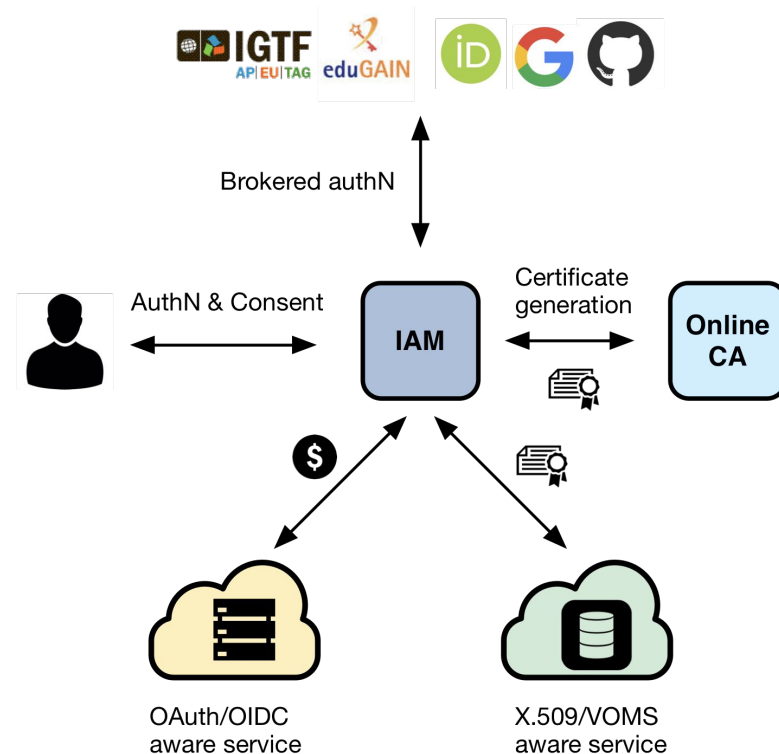
A VOMS proxy provides information about who you are, for which Virtual Organization (VO) you're acting and what you can do on the infrastructure (i.e., VOMS groups and roles)

Evolution of the WLCG AAI beyond X.509

In the near future we will use **tokens**, which will provide more or less the same information.

Tokens are obtained from a VO token issuer (e.g., INDIGO IAM) using **OAuth/OpenID Connect**.

Tokens are sent to services/resources following **OAuth** recommendations.



Core technologies

OAuth 2.0

- a standard framework for **delegated authorization**
- widely adopted in industry



OpenID Connect

- an **identity layer** built on top of OAuth 2
- “OAuth-based authentication done right”



JSON Web Tokens (JWTs)

- a **compact, URL-safe** means of representing **claims** to be transferred between two (or more) parties

```
{
  "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"
}
```

OAuth 2.0 features that matter



OAuth **doesn't share password data** but instead uses **authorization tokens to prove an identity** between consumers and service providers.

It allows you to **read data of a user from another application**.

- e.g. import all your google contacts within a social

login with social credentials on several applications

It supplies the authorization workflow for web, desktop applications, and mobile devices



To continue, log in to Spotify.



CONTINUE WITH FACEBOOK



CONTINUE WITH APPLE



CONTINUE WITH GOOGLE

CONTINUE WITH PHONE NUMBER

OR

Email address or username

Password

[Forgot your password?](#)



Remember me

LOG IN

OAuth 2.0 features that matter



It **relies on SSL** (Secure Sockets Layer)

It is **easy to implement** and **provides strong authentication**. In addition to the two-factor authentication, **tokens can be revoked** if necessary (i.e., suspicious activity).

Uses **single sign on**

Tokens are **self-contained**, i.e. their **integrity and validity** can be verified locally with **no callback to the token issuer**.

Gives users more control over their data → they can **selectively grant access** to various functionalities for applications they want to use



Example

Github since Nov. 2020 has dropped support for HTTP basic authentication. Only personal tokens are supported.

- tokens don't share your account password
- tokens have an expiration date

Expiration

7 days



The token will expire on Friday, Feb 8 2008

- tokens can have restricted permissions

Source: docs.github.com

<input checked="" type="checkbox"/> repo	Full control of private repositories
<input type="checkbox"/> repo:status	Access commit status
<input type="checkbox"/> repo_deployment	Access deployment status
<input type="checkbox"/> public_repo	Access public repositories
<input type="checkbox"/> admin:org	Full control of orgs and teams
<input type="checkbox"/> write:org	Read and write org and team membership
<input type="checkbox"/> read:org	Read org and team membership
<input type="checkbox"/> admin:public_key	Full control of user public keys
<input type="checkbox"/> write:public_key	Write user public keys
<input type="checkbox"/> read:public_key	Read user public keys
<input type="checkbox"/> admin:repo_hook	Full control of repository hooks
<input type="checkbox"/> write:repo_hook	Write repository hooks
<input type="checkbox"/> read:repo_hook	Read repository hooks
<input type="checkbox"/> admin:org_hook	Full control of organization hooks
<input type="checkbox"/> gist	Create gists
<input type="checkbox"/> notifications	Access notifications

What happens to X.509/VOMS?

It will take years before we have migrated the whole infrastructure away from user-managed X.509 credentials.

The transition will be gradual.

During the transition we will have a **mixed authN/Z model**:

X.509/VOMS + tokens.

Services at various level of the infrastructure will have to understand both.

WLCG JWT profile

https://zenodo.org/record/3460258#.Yos_qJNBwq0

“This document describes how WLCG users may use the available geographically distributed resources **without X.509 credentials**.”

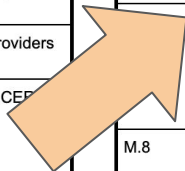
“In this model, **clients are issued with bearer tokens**; these tokens are subsequently used to interact with resources. **The tokens may contain authorization groups and/or capabilities, according to the preference of the Virtual Organisation (VO), applications and relying parties**.”

“Three major technologies are identified as providing the basis for this system: **OAuth2** (RFC 6749 & RFC 6750), **OpenID Connect** and **JSON Web Tokens** (RFC 7519).”

“**This document provides a profile for OAuth2 Access Tokens and OIDC ID Tokens**.”

The WLCG transition strategy and timeline

Milestone ID	Date	Description	Dependencies	Teams
M.0	Feb 2021	Produce document with list of use cases for CMS VOMS-Admin API.	None	WLCG Ops
M.1	May 2021	WLCG baseline services include HTTP-TPC endpoints. Mind: tape services come later.	None	WLCG Ops, Storage providers
M.2	June 2021	WLCG hosts "CE and pilot factory hackathon"	None	Pilot framework providers
M.3	July 2021	Production IAM Instance(s) Available for at least 1 LHC experiment, likely CMS and possibly ATLAS March 2022: - IAM is in production for CMS and ATLAS since autumn 2021.	None	WLCG Ops, IAM, CERN IT
M.4	Oct 2021	Pilot job submissions <u>may</u> be performed with tokens. March 2022: - Works on OSG for ATLAS, CMS and SAM ETF. - Very few CEs on EGI support tokens.	M.3	Experiments, pilot framework providers, OSG/EGI, sites, Monitoring
M.5	Dec 2021	VOMS-Admin shutoff for CMS. IAM is the sole authz provider for those (including for VOMS server). March 2022: - Postponed until spring or later.		WLCG Ops, CERN IT
M.6	Feb 2022	OSG ends support for the Grid Community Toolkit. March 2022: - (Postponed until May 1st?)	M.1, M.4	OSG



M.7	Mar 2022	All storage services provide support for tokens. March 2022: - Postponed until 2023 at the earliest. - Some storage services may be ready earlier.	M.1	WLCG Ops, Storage providers
	?	All VO's shut off VOMS-Admin		
	Sept 2022	End of HTCondor support for GSI Auth (link). March 2022: - Postponed until Nov 2022.		
M.8	Oct 2022	Rucio transfers performed with token auth in production March 2022: - May be possible for some storage services.	M.7	Rucio, Experiments
M.9	Mar 2023	Experiments stageout & data reads performed via tokens.	M.7	Experiments
M.10	Mar 2024	X.509 client auth becomes optional.	M.9, M.8, M.4	Experiments

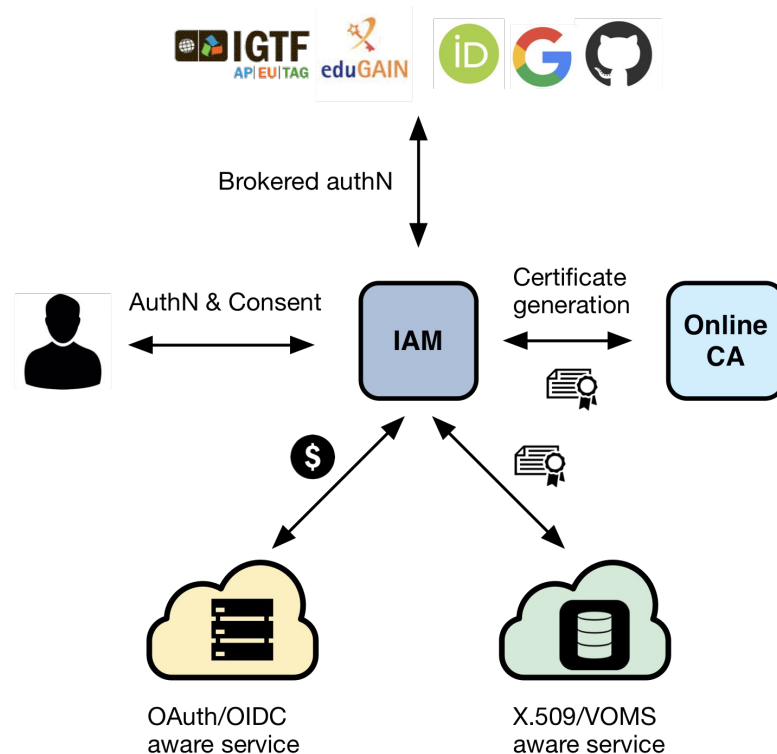
INDIGO IAM

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

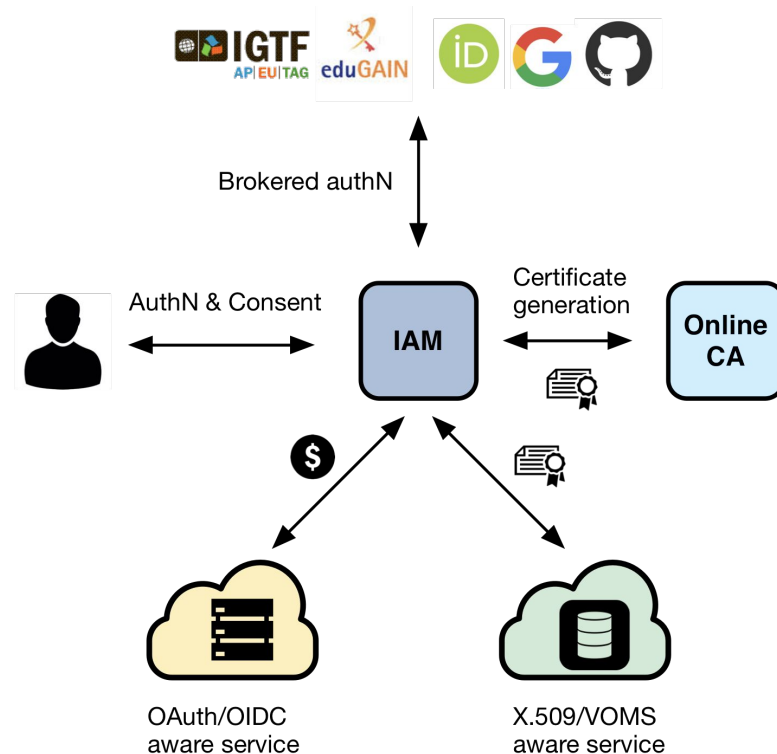
Sustained by INFN for the foreseeable future, with current support from:



INDIGO 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**



Easy integration with relying services

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

INDIGO IAM has been successfully integrated with:

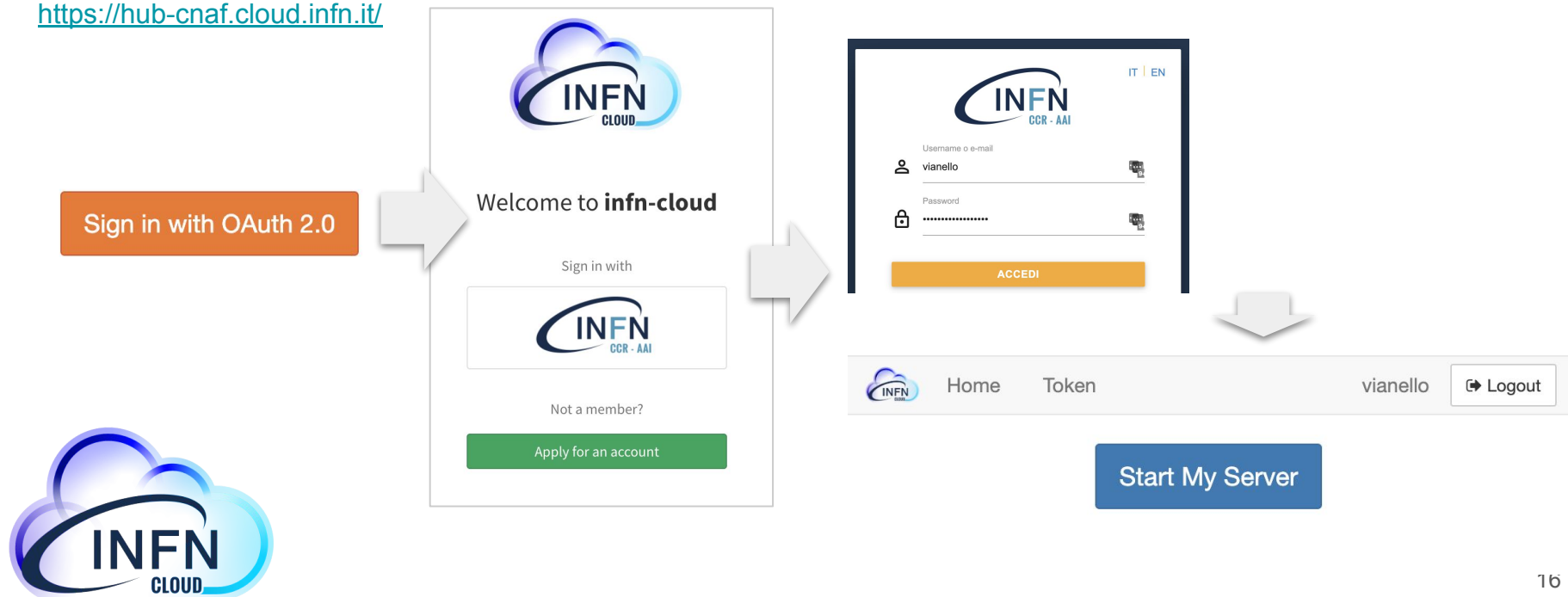
- Openstack, Atlassian JIRA & Confluence, Moodle, Rocketchat, Grafana, Kubernetes, JupyterHub, dCache, StoRM, XRootD (HTTP), FTS, RUCIO, HTCondor



Easy integration with relying services

Example: JupyterHub integration in the context of INFN-CLOUD

<https://hub-cnaf.cloud.infn.it/>



Easy integration with relying services

Example: StoRM WebDAV

xfer.cr.cnaf.infn.it

Please login with one of the configured providers:

ESCAPE IAM

WLCG IAM

[Go back to the storage area index page](#)

WLCG
Worldwide LHC Computing Grid

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

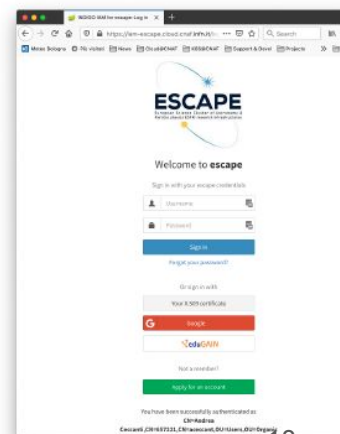
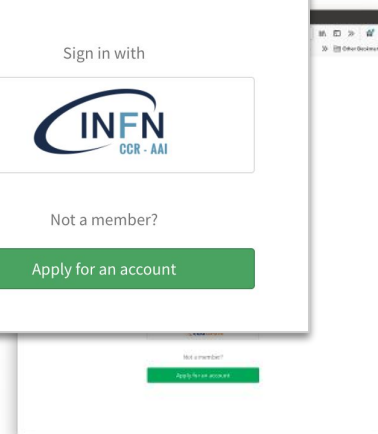
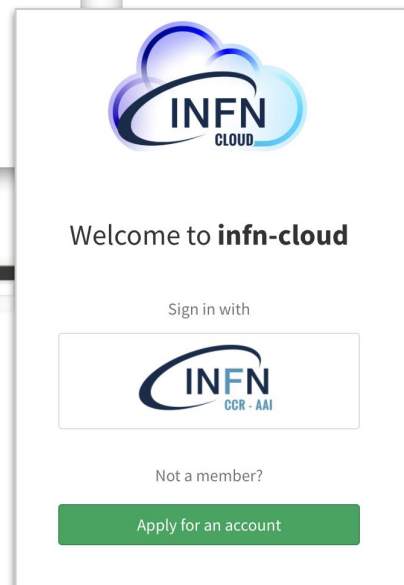
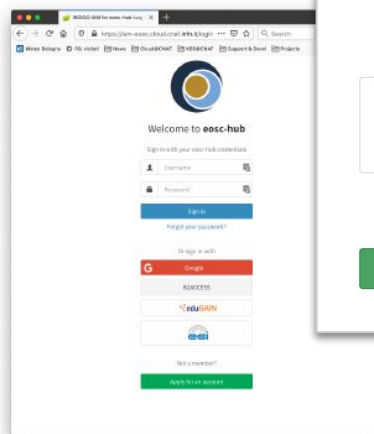
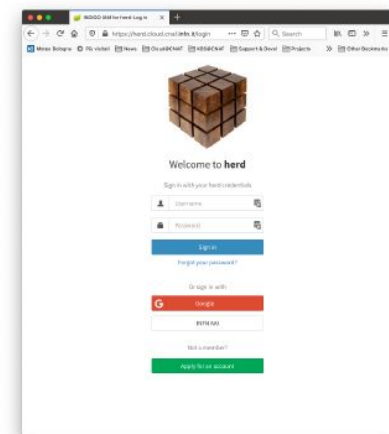
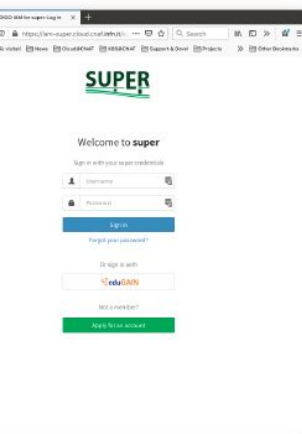
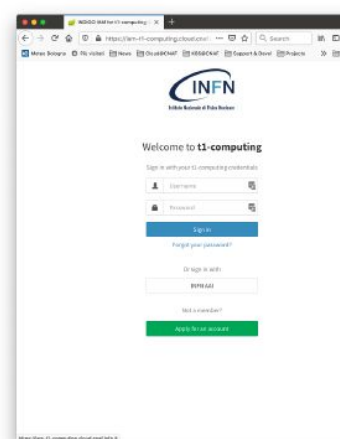
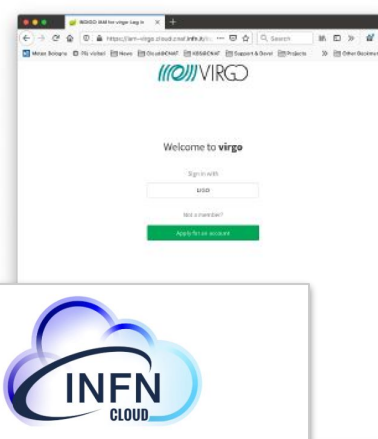
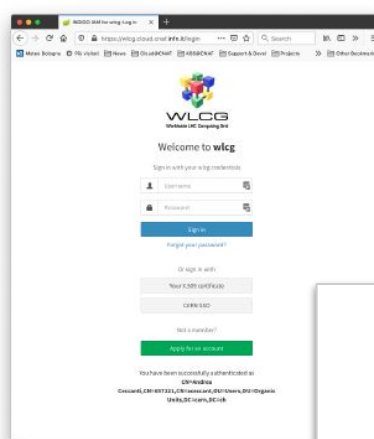
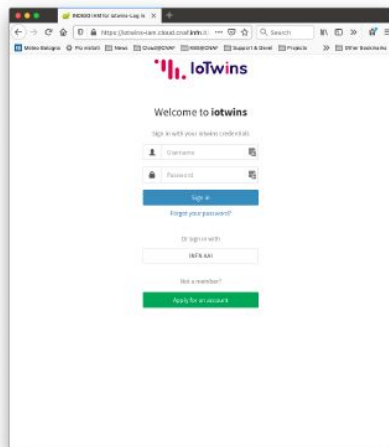
You have been successfully authenticated as
CN=Enrico Vianello vianello@infn.it,O=Istituto Nazionale di
Fisica Nucleare,C=IT,DC=tcs,DC=terena,DC=org

xfer.cr.cnaf.infn.it

/wlcg/

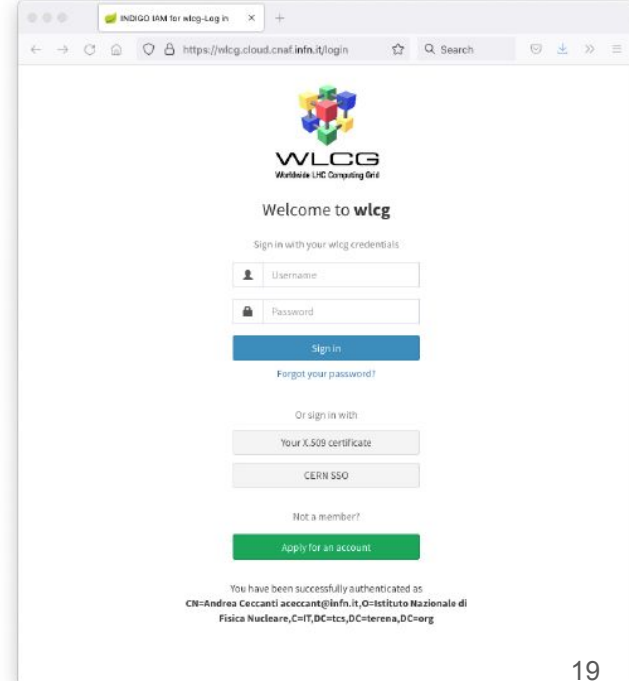
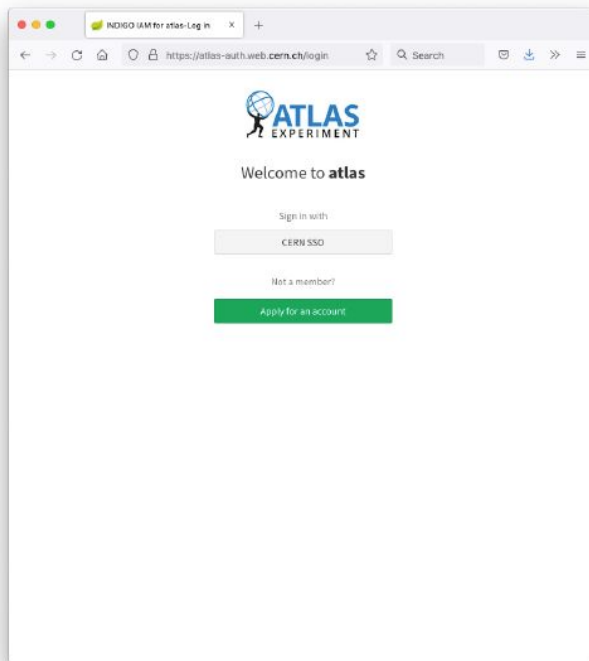
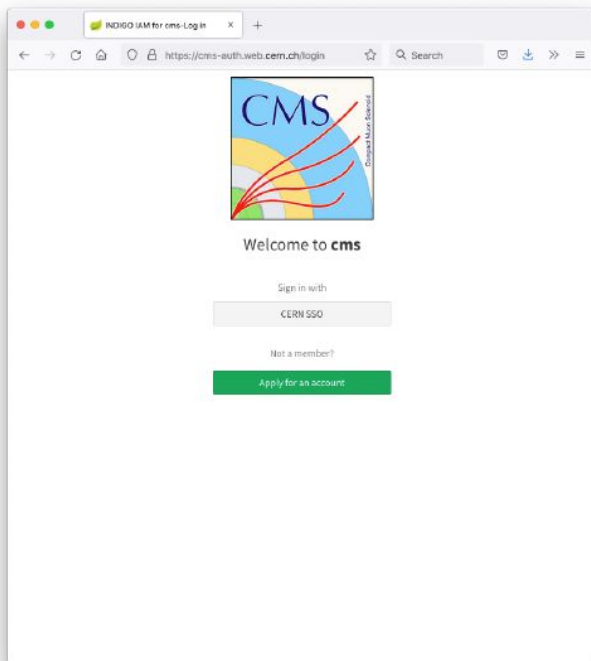
[Go to parent directory](#)

Name	Last modified	Size (in byte)
10MBfile	2021-03-10T16:15:23.908+01:00	10485760
1GBfile	2021-03-10T16:14:36.363+01:00	1073741824
1M	2020-07-06T09:50:57.522+02:00	1048576
4GBfile	2021-03-03T11:51:46.434+01:00	4244635648
4GBfile.copy	2021-03-25T14:43:41.358+01:00	4244635648
andrea/	2021-03-12T11:15:46.204+01:00	4096
https/	2020-04-08T14:56:56.209+02:00	4096
msoares/	2021-04-07T13:23:32.010+02:00	8192
protected/	2022-05-23T15:34:19.801+02:00	4096
robot-02FA9B44-CDF9-4E6D-8573-E9F2E87160C5/	2020-11-19T16:18:59.263+01:00	4096



WLCG IAM deployments

- WLCG, ATLAS, CMS (ALICE and LHCb coming soon)



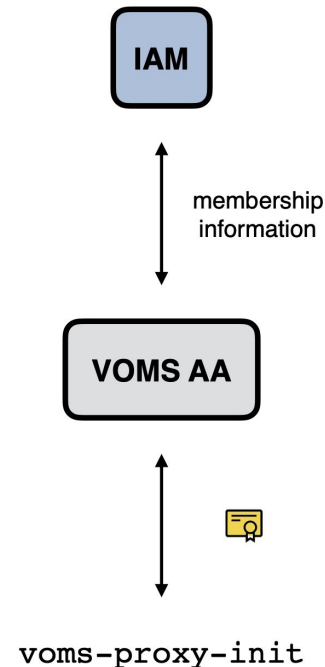
From VOMS to INDIGO IAM

VOMS → IAM

Knowing that the transition from X.509 to tokens will take time, INDIGO IAM was designed to be **backward-compatible** with our existing infrastructure

- INDIGO IAM **provides a VOMS attribute authority** micro-service that can encode IAM membership information in a standard VOMS Attribute Certificate → can issue VOMS credentials (voms-proxy-init) understood by existing clients

At some point **IAM will be the only authoritative VOMS server** for the infrastructure



What's in common?

Attribute handling

VOMS users can have assignable attributes → IAM has support for generic attributes as well

Group managers

In VOMS-Admin, VO managers may delegate the approval of some groups/roles for subgroups of people to other VO members → IAM supports for group managers, currently only to approve/reject group membership requests

What's in common?

AUP expiration

Within VOMS Admin, an expired AUP prevents to issue new VOMS X.509 proxies
→ an expired AUP signature forces the user to sign the AUP when the user tries to login into IAM and prevents the issuing of new tokens, the refresh of tokens or the issuing of VOMS attribute certificates

Roles

VOMS Admin roles → are replaced by some “tagged” groups. There's a plan to add a direct Role support in IAM

What's in common?

Primary group

Within VOMS Admin, exists the concept of a primary group → In WLCG JWT tokens the content of the wlcg.groups claim (the list of user's group memberships) is an ordered list of groups, and the profile defines how a particular group ordering can be requested.

Additional certificates

Within VOMS Admin users can add additional certificates → IAM allows to link multiple certificates to an account, in the same way VOMS does

Command line clients comparison

Storage testbed

- [IAM for WLCG](#) as Authorization Server
- StoRM deployment with **StoRM WebDAV** component enabled
- A **wlcg** storage area with a **/protected** path writable only by users that has VOMS **Role=test** or are members of the **wlcg.group /wlcg/test** (readable for other vo members)



Welcome to **wlcg**

Sign in with your wlcg credentials

	<input type="text" value="Username"/>	
--	---------------------------------------	--

	<input type="password" value="Password"/>	
--	---	--

Sign in

[Forgot your password?](#)

Or sign in with

Your X.509 certificate

CERN SSO

Not a member?

Apply for an account

StoRM WebDAV “xfer.cr.cnaf.infn.it” configuration

```
storm:
  authz:
    policies:
      - sa: wlcg
        description: Grant all access to /wlcg/protected to /wlcg/test members and users with VOMS role = test
        actions:
          - all
        paths:
          - /protected/**
        effect: permit
        principals:
          - type: fqan
            params:
              fqan: /wlcg/Role=test
          - type: jwt-group
            params:
              iss: https://wlcg.cloud.cnaf.infn.it/
              group: /wlcg/test
```

StoRM WebDAV “xfer.cr.cnaf.infn.it” configuration

- sa: **wlcg**

description: **Allow read access to /wlcg/protected area to wlcg members**

actions:

- **read**

- **list**

paths:

- **/protected/****

effect: **permit**

principals:

- type: **vo**

params:

vo: **wlcg**

- type: **jwt-group**

params:

iss: **<https://wlcg.cloud.cnaf.infn.it/>**

group: **/wlcg**

StoRM WebDAV “xfer.cr.cnaf.infn.it” configuration

- sa: **wlcg**

description: **Deny write access to /wlcg/protected area**

actions:

- **write**
- **delete**

paths:

- **/protected/****

effect: **deny**

principals:

- type: **anyone**

Current user experience with VOMS proxy

Preliminary phase:

- get your personal X.509
- .globus directory setup with personal user certificate and key

Common usage:

- create VOMS proxy
- read/transfer with common client tools

The expected user experience with tokens

Preliminary phase:

- generate an account configurations file for your Authorization Server with `oidc-agent (oidc-gen)`
- select oidc configuration file (`oidc-add`)

Common usage:

- generate token (`oidc-token`)
- read/transfer with common client tools

oidc-agent is a set of tools to manage OpenID Connect tokens and make them easily usable from the command line

Tests with oidc-agent

```
$ eval $(oidc-agent --no-autoload)
$ oidc-gen -w device wlcg
```

...

```
[16] https://wlcg.cloud.cnaf.infn.it/
Issuer [https://iam-test.indigo-datacloud.eu/]: 16
```

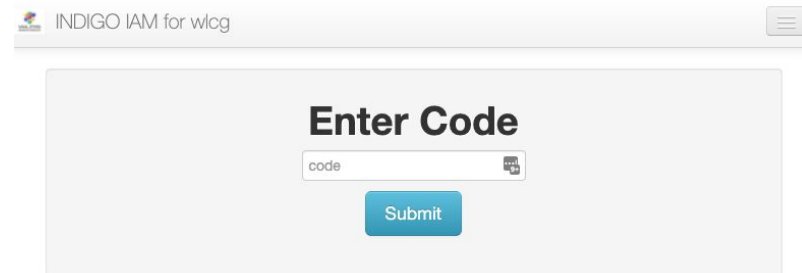
...

Scopes or 'max' (space separated) [openid profile offline_access]: max
Using a browser on any device, visit:

<https://wlcg.cloud.cnaf.infn.it/device>

And enter the code: 7RJZZ3

Enter encryption password for account configuration 'wlcg':
Confirm encryption Password:
Everything setup correctly!



The screenshot shows a web browser window titled "INDIGO IAM for wlcg". The main content area is titled "Enter Code" and contains a text input field labeled "code" with a small QR code icon to its right. Below the input field is a blue "Submit" button.

Tests with oidc-agent

\$ oidc-add wlcg -p

Enter decryption password for account config 'wlcg':

```
{
  "name": "wlcg",
  "client_name": "oidc-agent:wlcg-a0fc22ea62eb",
  "issuer_url": "https://wlcg.cloud.cnaf.infn.it/",
  "device_authorization_endpoint": "https://wlcg.cloud.cnaf.infn.it/devicecode",
  "daeSetByUser": 0,
  "client_id": "095cd171-5fc6-4518-9b76-635ca79c4293",
  "client_secret": "XXXXXXXX",
  "refresh_token": "XXXXXX.YYYYYY.",
  "cert_path": "/etc/pki/tls/certs/ca-bundle.crt",
  "scope": "openid profile compute.create storage.read:/ compute.read
compute.modify wlcg eduperson_entitlement storage.create:/ offline_access compute.cancel
eduperson_scoped_affiliation storage.modify:/ email wlcg.groups",
  "audience": "",
  "redirect_uris": ["http://localhost:43825", "edu.kit.data.oidc-agent:/redirect",
"http://localhost:8080", "http://localhost:4242"],
  "username": "",
  "password": ""
}
```

Tests with oidc-agent

```
$ export BEARER_TOKEN=$(oidc-token wlcg)
```

```
$ gfal-mkdir davs://xfer.cr.cnaf.infn.it:8443/wlcg/protected/test-paestum
```

```
gfal-mkdir error: 1 (Operation not permitted) - HTTP 403 : Permission refused
```

```
$ export BEARER_TOKEN=$(oidc-token -s wlcg.groups:/wlcg/test wlcg)
```

```
$ gfal-mkdir davs://xfer.cr.cnaf.infn.it:8443/wlcg/protected/test-paestum
```

```
$ gfal-rm -r davs://xfer.cr.cnaf.infn.it:8443/wlcg/protected/test-paestum
```

```
davs://xfer.cr.cnaf.infn.it:8443/wlcg/protected/test-paestum RMDIR
```

Tests with oidc-agent

```
$ export BEARER_TOKEN=$(oidc-token wlcg)
```

```
$ printenv BEARER_TOKEN | jwt
```

PAYLOAD: DATA

```
{
  "wlcg.ver": "1.0",
  "sub": "9f89c4bb-0ae1-4026-8370-914db490446f",
  "aud": "https://wlcg.cern.ch/jwt/v1/any",
  "nbf": 1653062401,
  "scope": "openid compute.create profile compute.read
storage.read:/ compute.modify eduperson_entitlement
wlcg storage.create:/ offline_access compute.cancel
eduperson_scoped_affiliation storage.modify:/ email
wlcg.groups",
  "iss": "https://wlcg.cloud.cnaf.infn.it/",
  "exp": 1653066000,
  "iat": 1653062401,
  "jti": "0af0a62b-2331-4333-933f-326ace375bc9",
  "client_id": "466446bf-9307-4199-abd3-fa5185684fd9",
  "wlcg.groups": [
    "/wlcg",
    "/wlcg/pilots",
    "/wlcg/xfers"
  ]
}
```

Tests with oidc-agent

```
$ export BEARER_TOKEN=$(oidc-token -s wlcg.groups:/wlcg/test wlcg)
```

```
$ printenv BEARER_TOKEN | jwt
```

PAYLOAD: DATA

```
{
  "wlcg.ver": "1.0",
  "sub": "9f89c4bb-0ae1-4026-8370-914db490446f",
  "aud": "https://wlcg.cern.ch/jwt/v1/any",
  "nbf": 1652715664,
  "scope": "wlcg.groups:/wlcg/test",
  "iss": "https://wlcg.cloud.cnaif.infn.it/",
  "exp": 1652719264,
  "iat": 1652715664,
  "jti": "4b93eb1f-2ede-4f7f-973b-5e7ac3a9e0fe",
  "client_id": "095cd171-5fc6-4518-9b76-635ca79c4293",
  "wlcg_groups": [
    "/wlcg/test",
    "/wlcg",
    "/wlcg/pilots",
    "/wlcg/xfers"
  ]
}
```

Tests with VOMS-proxy

```
$ voms-proxy-init --voms wlcg
```

```
$ gfal-mkdir davs://xfer.cr.cnaf.infn.it:8443/wlcg/protected/test-paestum
```

```
gfal-mkdir error: 1 (Operation not permitted) - HTTP 403 : Permission refused
```

```
$ voms-proxy-init --voms wlcg:/wlcg/Role=test
```

```
$ gfal-mkdir davs://xfer.cr.cnaf.infn.it:8443/wlcg/protected/test-paestum
```

```
$ gfal-rm -r davs://xfer.cr.cnaf.infn.it:8443/wlcg/protected/test-paestum
```

```
davs://xfer.cr.cnaf.infn.it:8443/wlcg/protected/test-paestum RMDIR
```

Tests with VOMS-proxy

```
$ voms-proxy-init --voms wlcg
```

```
$ voms-proxy-info --all
```

```
...  
=== VO wlcg extension information ===  
VO      : wlcg  
...  
attribute : /wlcg  
attribute : /wlcg/pilots  
attribute : /wlcg/xfers  
...
```

```
$ voms-proxy-init --voms wlcg:/wlcg/Role=test
```

```
$ voms-proxy-info --all
```

```
...  
=== VO wlcg extension information ===  
VO      : wlcg  
...  
attribute : /wlcg/Role=test  
attribute : /wlcg  
attribute : /wlcg/pilots  
attribute : /wlcg/xfers  
...
```

INDIGO IAM - status and release plan

IAM: latest releases (v1.7.0, v1.7.1 and v1.7.2)

[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](#), [v1.7.1](#) and [v1.7.2](#) release notes.

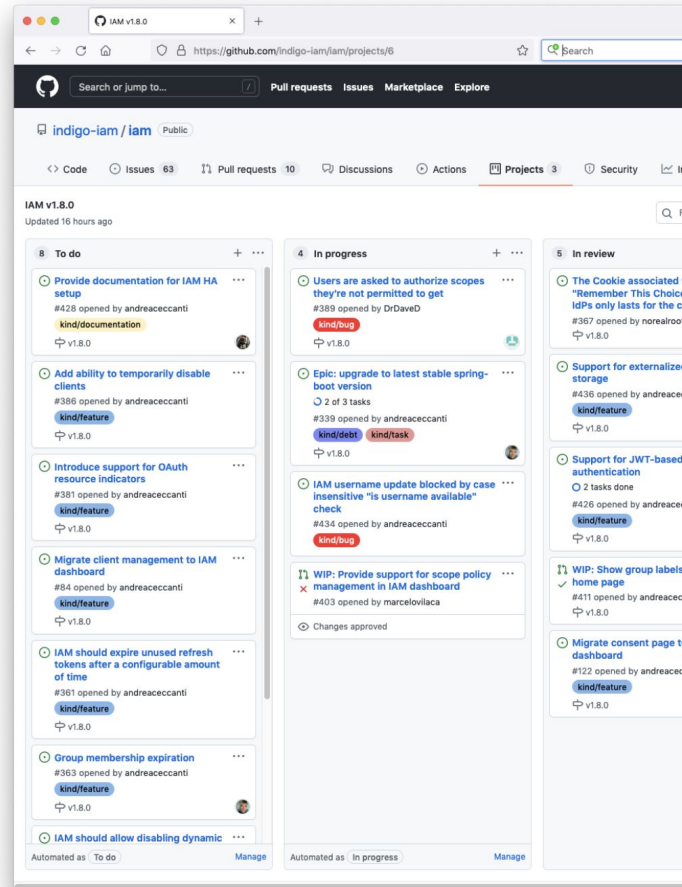
Planned releases: IAM v1.8.0

ETA: June 2022 [milestone](#) [project](#)

Highlights:

- **Spring dependencies upgrade**
 - avoid vulnerabilities
- **Improved client management & registration**
 - pagination, search, lifecycle
- **Session externalization**
 - stateless application
 - support for replicated/HA IAM deployments
- **JWT-based client authentication**

other minor **improvements & bug fixes**



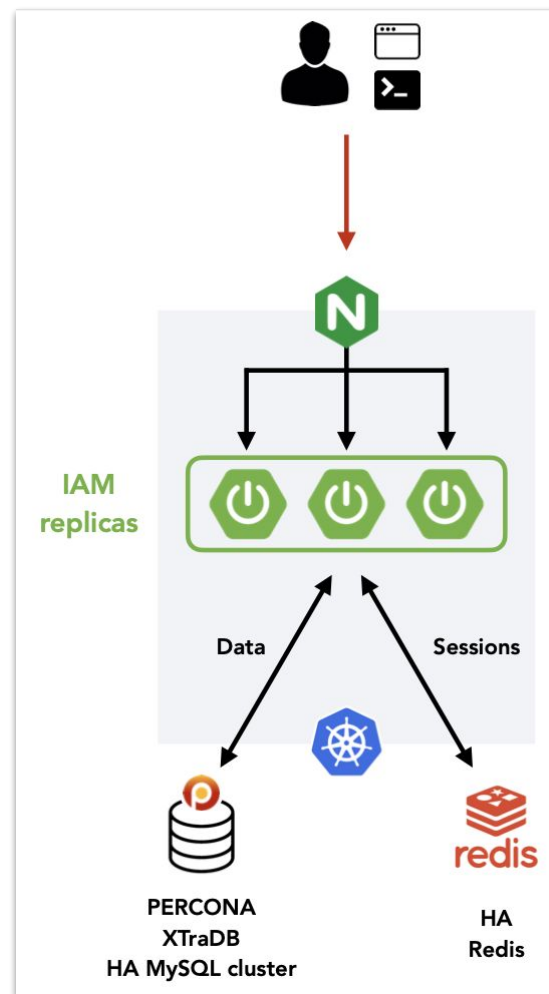
Planned releases: IAM v1.8.0

ETA: June 2022 [milestone](#) [project](#)

Highlights:

- **Spring dependencies upgrade**
 - avoid vulnerabilities
- **Improved client management & registration**
 - pagination, search, lifecycle
- **Session externalization**
 - stateless application
 - support for replicated/HA IAM deployments
- **JWT-based client authentication**

other minor **improvements & bug fixes**



Planned releases: IAM v1.8.1

ETA: September 2022

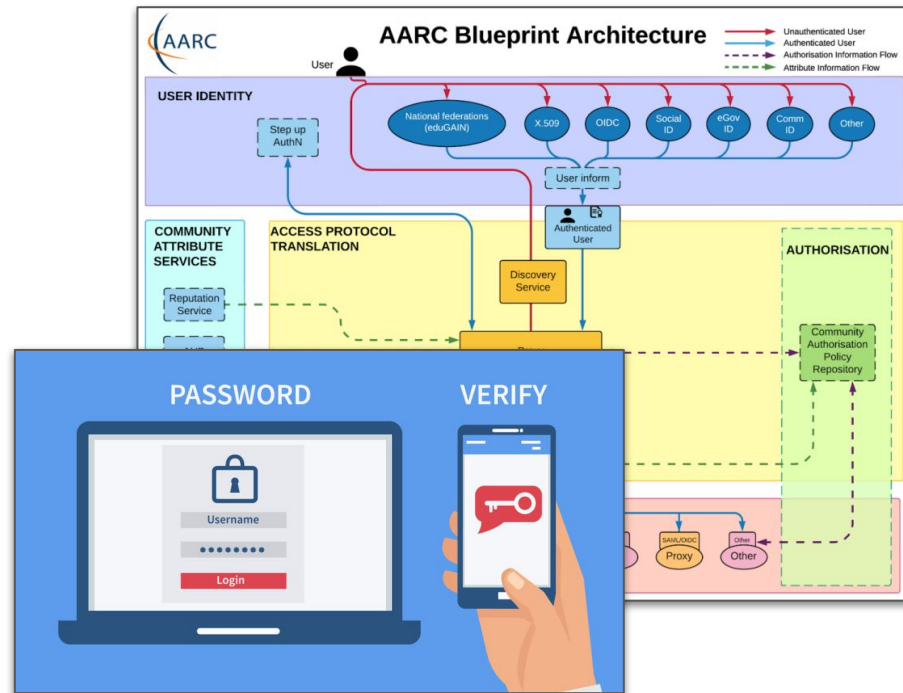
Highlights:

- Improve AARC guidelines support
- Improve Scope Policies web interface

other minor **improvements & bug fixes**

Also on development:

- Support for **Multi-factor authentication**



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

**“I don't need to worry about identity theft
because no one wants to be me.”**

Jay London