Authentication and Authorization with INDIGO IAM

Enrico Vianello, Andrea Ceccanti INFN CNAF

Corso Nazionale CCR Big Data Analytics Bologna, 9 Dicembre 2019





AAI challenges

OAuth & OpenID connect overview

IAM overview

A token-based AAI - in practice

Beyond X.509: migrating from X.509/VOMS to tokens

Hands on



Please point your browser to:

• <u>https://iam-demo.cloud.cnaf.infn.it</u>

and apply for an account.

Welcome to iam-de	mo
Sign in with your iam-demo creder	ntials
L Username	•••1 9•
Password	•••1 9+
Sign in	
Forgot your password?	
Or sign in with	
G Google	
Not a member?	
Register a new account	



You will use that account later in the tutorial

Check your e-mails and click on confirmation link:

iam-demo@cloud-vm195.cloud.cnaf.infn.it

Confirm your iam-demo registration request

A: Enrico Vianello

Dear Enrico Vianello,

you have requested to be a member of iam-demo.

In order for the registration to proceed, please confirm this request by going to the following URL:

https://iam-demo.cloud.cnaf.infn.it/registration/verify/e222995d-fb38-4855-a60

The iam-demo registration service

The following user has submitted a membership request:

Name: Enrico Vianello Username: test Email: <u>en.vianello@gmail.com</u>

Notes: test

You can approve or reject this request by following the link below:

https://iam-demo.cloud.cnaf.infn.it/dashboard#/requests

The iam-demo registration service



Request confirmed successfully

Your registration request has been confirmed successfully, and is now waiting for administrator approval. As soon as your request is approved you will receive a confirmation email.



Wait for admins approval

n-demo		<u> </u>
lo	Approve registration request?	
	 Do you confirm the approval of the registration request from the following user? Enrico Vianello, submitted 5 minutes ago. 	
51	Approve request Cancel	Dec 9, 2019 9:3
1		
132		

Check your e-mails again and click on password-reset link:

iam-demo@cloud-vm195.cloud.cnaf.infn.it Your iam-demo account is now active A: Enrico Vianello		CINER
Dear Enrico Vianello, your registration request has been approved. You can set your password by following this link: https://iam-demo.cloud.cnaf.infn.it/iam/password-reset/token/17f26a14-5deb-4d38-av	•••••	Set your password
The iam-demo registration service	Save	<image/>



A novel AAI: main challenges

A novel AAI: main challenges

Authentication

- Flexible, able to accomodate various authentication mechanisms
 - X.509, username & password,
 EduGAIN, social logins (Google,
 GItHub), ORCID, ...

Identity harmonization & account linking

• Harmonize multiple identities & credentials in a single account, providing a **persistent identifier**

Authorization

• Orthogonal to authentication, attribute or capability-based

Delegation

- Provide the ability for services to act on behalf of users
- Support for long-running applications

Provisioning

 Support provisioning/deprovisioning of identities to services/relying resources

Token translation

 Enable integration with legacy services through controlled credential translation

12

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 VOMSaware services

Self-contained, comprehensive AuthN/AuthZ solution



A brief introduction to OAuth and OpenID Connect

IAM enabling technologies in one slide

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

14





{		
	"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: a delegated authorization framework

OAuth defines how **controlled delegation of privileges** can happen among collaborating services

Provides answers to questions like:

- How can an application request access to protected resources?
 - How can I obtain **an access token**?
- How is authorization information exchanged across parties?
 - How is the access token presented to protected resources? (i.e. API)



OpenID Connect: an identity layer for OAuth

OAuth is a **delegated authorization** protocol

 an access token states the authorization rights of the client application presenting the token to access some resources

OpenID Connect extends OAuth to provide a standard **identity layer**

- i.e. information about who the user is and how it was authenticated via an additional ID token (JWT) and a dedicated user information query endpoint at the OpenID Connect Identity provider
- provides ability to establish login sessions (SSO)





JSON Web Tokens (JWT)

JSON Web Token (JWT) is an <u>open standard</u> that defines a compact, self-contained way of securely transmitting information between parties as a JSON object

JWTs are typically **signed** and, if confidentiality is a requirement, can be **encrypted**.



Why OAuth, OpenID Connect and JWT?

Standard, widely adopted in industry

 Do not reinvent the wheel, reuse existing knowledge and tools, extend when needed

Reduced integration complexity at relying services

• Off-the-shelf libraries and components

Authentication-mechanism agnostic

• The AAI is not bound to a specific authentication mechanism

Distributed verification of access and identity tokens

• It scales

OAuth roles

Resource owner

• A user that owns resources hosted at a service

Client

An application that wants to have access to user resources

Authorization server

• A service that authenticates users and client applications and issues access tokens according to some policy

Resource server

• A service that holds protected resources and grants access based on access tokens issued by the authorization server 19



OAuth client registration

In OAuth clients that interact with an Authorization Server (AS) need to be **registered**

When a client is registered, it typically receives the client **credentials**

- **client_id:** the client "username"
- **client_secret:** the client "password"

Credentials are required in some OAuth flows or to access specific endpoints, where different privileges may be assigned to different clients



OAuth client types

https://tools.ietf.org/html/rfc6749#section-2.1

confidential: Clients capable of maintaining the confidentiality of their credentials (e.g., client implemented on a secure server with restricted access to the client credentials), or capable of secure client authentication using other means

public: Clients incapable of maintaining the confidentiality of their credentials (e.g., clients executing on the device used by the resource owner, such as an installed native application or a web browser-based application), and incapable of secure client authentication via any other means.

Handling client credentials

Client credentials must be maintained confidential

- **not** stored in Docker images or source code
 - use ENV variables or other secret management mechanisms to pass down these secrets to your application

Follow recommendations in the client app security section of the OAuth security recommendations

• <u>https://tools.ietf.org/html/rfc6819#section-5.3</u>

OAuth/OpenID Connect grant types

Authorization grant types

Authorization Flows

=

Ways for an application to get tokens

OAuth/OpenID Connect grant types

Grant Type	Context	Client type
Authorization code	Server-side apps	Confidential
Implicit	Client-side, Javascript apps	Public
Device code	Limited-input devices, CLIs	Confidential
Resource owner password credentials	Trusted apps, CLIs	Confidential
Client credentials	Server-side apps	Confidential
Refresh token	Server-side apps	Confidential
Token exchange	Server-side apps	Confidential

OAuth & OpenID Connect provide a standard way to expose the authorization server/OpenID provider configuration to clients

Information is published at **a well-known endpoint** for the server, e.g.:

• https://iam-demo.cloud.cnaf.infn.it/.well-known/openid-configuration

Clients can use this information to know about

- supported grant types/authorization flows
- endpoint locations
- supported claims
- ...

and implement automatic client configuration

```
{
  "request_parameter_supported": true,
  "claims_parameter_supported": false,
  "introspection_endpoint": "https://dodas-iam.cloud.cnaf.infn.it/introspect",
  "scopes_supported": [
    "openid",
    "profile",
    "email",
   "address",
    "phone",
    "offline_access"
  ],
  "issuer": "https://dodas-iam.cloud.cnaf.infn.it/",
  "userinfo_encryption_enc_values_supported": [
    "A256CBC+HS512",
    "A256GCM",
   "A192GCM",
    "A128GCM",
    "A128CBC-HS256",
    "A192CBC-HS384".
    "A256CBC-HS512",
   "A128CBC+HS256"
 ], ...
```

```
"claims_supported": [
   "sub",
   "name",
   "preferred_username",
   "given_name",
   "family_name",
• • •
   "zoneinfo",
   "locale",
   "updated_at",
   "birthdate",
   "email",
   "email_verified",
   "phone_number",
   "phone_number_verified",
   "address",
   "organisation_name",
   "groups",
   "external_authn"
 ],
```

. . .

```
{
  "authorization_endpoint": "https://dodas-iam.cloud.cnaf.infn.it/authorize",
  "claim_types_supported": [
    "normal"
  ],
  "claims_parameter_supported": false,
  "claims_supported": [
    "sub",
    "name",
    "preferred_username",
    "given_name",
    "family_name",
    "middle_name",
    . . . ,
  ],
  "code_challenge_methods_supported": [
    "plain",
    "S256"
  ],
  "grant_types_supported": [
    "authorization_code",
    "implicit",
    "refresh_token",
    "client_credentials",
    "password",
```

```
"password",
  "urn:ietf:params:oauth:grant-type:jwt-bearer",
  "urn:ietf:params:oauth:grant_type:redelegate",
  "urn:ietf:params:oauth:grant-type:token-exchange"
],
"id_token_encryption_alg_values_supported": [
  "RSA-OAEP",
  "RSA-0AEP-256",
  "RSA1 5"
],
"id_token_encryption_enc_values_supported": [
  "A256CBC+HS512".
 . . . ,
],
"id_token_signing_alg_values_supported": [
  "HS256",
  "HS384",
  . . . ,
],
"introspection_endpoint": "https://dodas-iam.cloud.cnaf.infn.it/introspect",
"issuer": "https://dodas-iam.cloud.cnaf.infn.it/",
"jwks_uri": "https://dodas-iam.cloud.cnaf.infn.it/jwk",
"op_policy_uri": "https://dodas-iam.cloud.cnaf.infn.it/about",
"op_tos_uri": "https://dodas-iam.cloud.cnaf.infn.it/about",
```

```
"registration_endpoint": "https://dodas-iam.cloud.cnaf.infn.it/register",
 "request_object_encryption_alg_values_supported": [
   "RSA-OAEP".
   . . . ,
],
 "request_object_encryption_enc_values_supported": [
  "A256CBC+HS512",
   . . . ,
],
 "request_object_signing_alg_values_supported": [
  "HS256",
   ••• ,
],
 "request_parameter_supported": true,
 "request_uri_parameter_supported": false,
 "require_request_uri_registration": false,
 "response_types_supported": [
   "code",
   "token"
 ],
 "revocation_endpoint": "https://dodas-iam.cloud.cnaf.infn.it/revoke",
 "scopes_supported": [
   "openid",
   "profile",
```

```
"scopes_supported": [
  "openid".
  "profile",
  "email",
  "address",
  "phone",
  "offline_access"
],
"service_documentation": "https://dodas-iam.cloud.cnaf.infn.it/about",
"subject_types_supported": [
  "public",
  "pairwise"
],
"token_endpoint": "https://dodas-iam.cloud.cnaf.infn.it/token",
"token_endpoint_auth_methods_supported": [
  "client_secret_post",
  "client_secret_basic",
  "none"
],
"token_endpoint_auth_signing_alg_values_supported": [
  "HS256",
 . . . ,
```

```
"userinfo_encryption_alg_values_supported": [
    "RSA-OAEP",
    ...,
],
"userinfo_encryption_enc_values_supported": [
    "A256CBC+HS512",
    ...,
],
"userinfo_endpoint": "https://dodas-iam.cloud.cnaf.infn.it/userinfo",
"userinfo_signing_alg_values_supported": [
    "HS256",
    ...,
]
```

}

IAM, relying parties & OAuth roles **Resource** owner **StoRM OneData WebDAV Resource** Server



Authorization Server Resource Server Client

Resource

Server

IAM, relying parties & OpenID Connect roles



Resource Server



StoRM

OneData



Relying party Resource Server



OpenID Connect provider Resource Server

IAM overview

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 the 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.



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



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

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.

Edit AUP

Delete AUP

Easy integration with services

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

We have successfully integrated IAM with minimal effort with:

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



IAM Software Quality

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

 now 24k lines of code, 86% branch coverage, >900 tests

Open, **test-driven** development process

Static analysis tools

• <u>SonarCube IAM page</u>

Multiple test suites

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

Covera	ge				
	0	86.0% Coverage	908 Unit Tests	Coverage on New Code	
Duplica	tions				
	0	3.7%	72	+0.2%	
Size	Ado nope	marcocaberletti wa	multiple OIDC provid nts to merge 2 commits into Indigo-Ian:devel mmits 2 R- Checks 0 Piles ch	ers #249 p from marcocaberletti:isswe-229 anged 35	
1	2	marcocaberletti commented 14 days ago Member + 😅 🥓 💷			
		 Add support to multiple OIDC providers Add S			
		 New changes s 	ince you last viewed	View changes	
	qube.	CnafSonarBot commented 14 days ago		Collaborator + 📖 ***	
		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. OldcConfiguration.java#L97: Method has 10 parameters, which is greater than 7 authorized.			
		Add more commits by pus	hing to the issue-229 branch on marcocaberletti/i	am.	
L	۶	Review requ	rested In requested on this pull request. It is not requir	Show all reviewers ed to merge. Learn more.	

IAM evolution: porting to Keycloak

IAM 2 (in development) will be based on <u>Keycloak</u>

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

We will focus on what not already provided by Keycloak

- flexible registration service
- X.509 and VOMS authentication support



Improved flexibility and sustainability



A token-based AAI - in practice

A token based AAI - WLCG model

In order to access resources/services, a **client application** needs an **access token**

The token is obtained from **a VO** (which acts as an OAuth Authorization Server) using standard **OAuth/OpenID Connect** flows

Authorization is then performed at the services leveraging info extracted from the token:

- Identity attributes: e.g., groups
- **OAuth scopes**: capabilities linked to access tokens at token creation time



In practice...

The central authorization servers provides **attributes** that can be used for authorization at services, e.g.:

- groups/roles, e.g.: cms, production-manager
- capabilities, e.g.: storage.read:/cms, submit-job

This information is exposed to services via **signed JWT tokens** and **via OAuth/OpenID Connect protocol message exchanges** (aka flows)

Services can then **grant or deny access** to functionality based on this information. Examples:

- allow read access on the /cms to all members of the cms group
- allow read access on the /atlas namespace to anyone with the capability read:/atlas

Identity-based vs Scope-based Authorization

Identity-based authorization: the token brings information about attribute ownership (e.g., groups/ role membership), the service maps these attributes to a local authorization policy

Scope-based authorization: the token brings information about which actions should be authorized at a service, the service needs to understand these capabilities and honor them. The authorization policy is managed at the VO level





Identity-based vs Scope-based Authorization

The two models can coexist, even in the context of the same application!

The two models can co-exist:

scope-based authZ



identity-based authZ



Share with others	Get shareable link
Link sharing on Learn more	
Anyone with the link can comment -	Copy link
https://docs.google.com/document/d/1cNm4n	1BI9ELhExwLxswpxLLNTuz8pT38-b
People	
Enter names or email addresses	
Shared with Hannah Short, Andrea Ceccanti and	2 others

OAuth bearer token usage

There's a standard that defines how to send tokens to resource servers

Typically, tokens are sent in the Authorization HTTP header, following the rules defined in RFC 6750, as in the following example HTTP request

GET /shared-oauth HTTP/1.1
Host: apache.test.example
Authorization: Bearer eyJraWQi0iJy...rYI
User-Agent: curl/7.65.3
Accept: */*

OAuth Refresh Tokens

Refresh tokens are the credentials that can be used to acquire new access tokens.



The **lifetime** of a refresh token is much **longer** compared to the lifetime of an access token. Refresh tokens can also expire.



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 <u>**RCAuth.eu</u>** online CA to generate X.509 certificates ondemand and link them to IAM user memberships</u>

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



Migrating from X.509/VOMS to tokens

Beyond X.509: Token-based Authentication and Authorization for HEP (CHEP 2018)

https://indico.cern.ch/event/587955/contributions/3012583/ attachments/1685421/2709996/CHEP-2018-Beyond-X.509-AC.pdf

WLCG AuthZ Working Group Demos: <u>https://indico.cern.ch/event/</u> <u>791175/attachments/1806605/2948665/demos.mp4</u> (IAM starts at minute 46) Web application integration scenario

Web application: authorization code flow





A Web App integrates with IAM to delegate user authentication management and obtain authorization information





Web application: authorization code flow





OAuth and OpenID connect provide the **authorization code flow** in support of this integration use case







User points its browser to web app, which redirects back to IAM for authentication













Welcome to **dodas**

Sign in with your dodas credentials



session at gin page



Welcome to **dodas**

Sign in with your dodas credentials

User selects EduGAIN, and chooses his home **IDP** for authentication

auth

Home Idl



session at gin page

authorization request

••



Sign in with your IdP

You will be redirected for authentication to:

INFN - Istituto Nazionale di Fisica Nucleare

Proceed?

Sign in with IdP

Remember this choice on this computer

Search again Back to login page l session at ogin page

Home IdP





Username ...I 8 Password LOGIN nome IDP ion Come ottenere un accesso ad INFN-AAI Cambio o Rigenerazione Password - Recupero Username X.509 Certificate Accesso tramite certificato. ACCEDI Kerberos5 GSS-API Accesso tramite Kerberos 5.

IT EN

65

Check





Home IDP authenticates user and sends back an authentication assertion, via redirection and possibly other interactions between IAM and the IDP



IAM





IAM validates the assertion, the user is a registered one, so IAM shows a "Give consent" page













The Web App exchanges the **authorization code** with a couple of tokens: an **access token** and an **id token**







In the IAM implementation, both tokens are **JWT tokens**.





The **access token** provides (mainly) authorization information


The **id token** provides (mainly) authentication information

Home IdP



Both tokens are validated following to the OpenID Connect guidelines, checking temporal validity, token signature, audience, etc...





Additional information about the user can be requested by querying the **/userinfo** endpoint and providing the just obtained **access token** for authentication/ authorization purposes





The returned JSON object contains authentication information that can overlap with the contents of the **id token**, depending on the IAM configuration

Authorization code flow in practice

In practice, decent OAuth/OpenID Connect client libraries implement all the above **behind the scenes.**

As an example, <u>Apache mod_auth_openidc</u> requires the following information to enable a working OpenID Connect integration

- The OpenID Connect provider discovery/metadata URL
- Client credentials

The library then takes care of exchanging messages with the OpenID provider, implementing verification checks, and provides the obtained authentication/authorization information to the protected web application

• typically via env variables or HTTP headers

Demo setup



demo.cloud.cnaf.infn.it



HTTPD is an Apache server configured with mod_auth_openidc

The **/shared** directory is only accessible to users authenticated by **iam-demo**

IAM iam-demo.cloud.cnaf.infn.it

Demo setup



demo.cloud.cnaf.infn.it



HTTPD is an Apache server configured with mod_auth_openidc

The **/ibergrid** directory is only accessible to users authenticated by **iam-demo** in the **ibergrid** group

IAM

iam-demo.cloud.cnaf.infn.it

Apache mod_auth_openidc configuration

ServerName demo.cloud.cnaf.infn.it

```
<VirtualHost _default_:80>
```

```
OIDCProviderMetadataURL https://iam-demo.cloud.cnaf.infn.it/.well-known/openid-
configuration
OIDCClientID demo_client
OIDCClientSecret ****
OIDCScope "openid email profile"
OIDCRedirectURI https://demo.cloud.cnaf.infn.it/oidc/redirect_uri
OIDCCryptoPassphrase ****
```

```
<Location /shared>
```

```
...
AuthType openid-connect
Require valid-user
LogLevel debug
</Location>
```

</VirtualHost>

IAM client configuration



Note that the redirect uri above matches with the one in the Apache configuration



Point your browser to: https://demo.cloud.cnaf.infn.it



IAM demo

/shared /ibergrid

The **/shared** directory is accessible to all authenticated users. The **/ibergrid** directory is accessible only users in the **ibergrid** group.

Click on /shared protected path



Use your IAM credentials at https://iam-demo.cloud.cnaf.infn.it/login

Welcome to **iam-demo**

Sign in with your iam-demo credentials

1	Username	•••I 9+
	Password	••••I 9+
	Sign in	
	Forgot your password?	
	Or sign in with	
G	Google	
	Not a member?	
	Register a new account	



Hi Enrico Vianello

This is the /shared section of this demo website.

You're now logged in as: vianello

This application has received the following information:

EOSC-hub

• access_token (JWT):

}

eyJraWQiOiJyc2ExliwiYWxnljoiUlMyNTYifQ.eyJzdWliOiJlMzM3MzU0My05NDM2LTQ1MGUtOTFiZi00MzlmM2VhMTg2MjliLCJpc3MiOiJodHRwczpcL1wvaWFtLWRlk

• access_token (decoded):
{
 "sub": "e3373543-9436-450e-91bf-439f3ea18622",
 "iss": "https://iam-demo.cloud.cnaf.infn.it/",
 "name": "Enrico Vianello",
 "groups": [
 "ibergrid",
 "demo",
 "ibergrid/feudal"
}
\$ export ACCESS_TOKEN=[paste your copied token]

"email": "enrico.vianello@cnaf.infn.it"

Istituto Nazionale di Fisica Nucleare

Copy your access token

Access to /userinfo endpoint

Get more user info from /userinfo endpoint:

\$ curl https://iam-demo.cloud.cnaf.infn.it/userinfo -H
"Authorization: Bearer \${ACCESS_TOKEN}" | jq `.'

```
"sub": "e3373543-9436-450e-91bf-439f3ea18622",
"name": "Enrico Vianello",
"preferred_username": "vianello",
"given_name": "Enrico",
"family_name": "Vianello",
"picture": "https://cdn.iconscout.com/icon/premium/png-512-thumb/rocket-man-833478.png",
"updated_at": 1575733577,
"email": "enrico.vianello@cnaf.infn.it",
"email_verified": true,
"groups": [
    "ibergrid",
    "demo",
    "ibergrid/feudal"
],
    "organisation_name": "iam-demo"
```

Client registration

Follow IAM documentation and create your client:

https://indigo-iam.github.io/docs/v/current/user-guide/clientregistration.html

client name convention: **demo_<surname>**

Get info from introspection endpoint

Get more user info from **/introspect** endpoint:

\$ export CLIENT_ID=[paste your client id]
\$ export CLIENT SECRET=[paste your client secret]

\$ curl -H "Content-Type: application/x-www-form-urlencoded"
-u \${CLIENT_ID}:\${CLIENT_SECRET} -d "token=\${ACCESS_TOKEN}"
https://iam-demo.cloud.cnaf.infn.it/introspect | jq `.'

Get info from introspection endpoint

Get more user info from */introspect* endpoint:

{

```
"active": true,
"scope": "openid profile email",
"expires_at": "2019-12-08T20:25:36+0100",
"exp": 1575833136,
"sub": "e3373543-9436-450e-91bf-439f3ea18622",
"user_id": "vianello",
"client_id": "demo.cloud.cnaf.infn.it",
"token_type": "Bearer",
"iss": "https://iam-demo.cloud.cnaf.infn.it/",
"groups":
  "ibergrid",
  "demo",
  "ibergrid/feudal"
],
"name": "Enrico Vianello",
"preferred_username": "vianello",
"organisation_name": "iam-demo",
"email": "enrico.vianello@cnaf.infn.it"
```

Identity based Authz

Point again your browser to: https://demo.cloud.cnaf.infn.it



IAM demo

/shared The /shared directory is accessible to all authenticated users./ibergrid The /ibergrid directory is accessible only users in the ibergrid group.

Click on /ibergrid protected path

Identity based Authz

Approval Required for *demo.cloud.cnaf.infn.it*

> more information

You will be redirected to the following page if you click Approve: https://demo.cloud.cnaf.infn.it/oidc/redirect_uri

Access to:

- log in using your identity
 basic profile information
- email address

Remember this decision:

- remember this decision until I revoke it
- remember this decision for one hour
- prompt me again next time

Do you authorize " demo.cloud.cnaf.infn.it "?

Authorize Deny

401 Unauthorized

You are not authorized to access the requested resources

Back to index

Apache mod_auth_openidc configuration

ServerName demo.cloud.cnaf.infn.it

<VirtualHost _default_:80>

OIDCProviderMetadataURL https://iam-demo.cloud.cnaf.infn.it/.well-known/openidconfiguration OIDCClientID demo_client OIDCClientSecret ***** OIDCScope "openid email profile" OIDCRedirectURI https://demo.cloud.cnaf.infn.it/oidc/redirect_uri OIDCCryptoPassphrase ****

```
<Location /ibergrid>
```

AuthType openid-connect Require claim groups:ibergrid LogLevel debug </Location>

</VirtualHost>

. . .

Ask for Group Membership

Go to https://iam-demo.cloud.cnaf.infn.it/dashboard#/home

torione dense
Join group(s)?
Select one or more groups
ibergrid × ibergrid/feudal ×
Provide a motivation for your request(s) This motivation will be show to the administrators that will manage your request
corso big data
created To minutes ago

Identity based Authz

Open a new Anonymous Navigation window on your browser in order to avoid using your previous session

Point again your browser to: https://demo.cloud.cnaf.infn.it



IAM demo

/shared The /shared directory is accessible to all authenticated users./ibergrid The /ibergrid directory is accessible only users in the ibergrid group.

Click on /ibergrid protected path

Identity based Authz

index / iam-test-web

Hi Enrico Vianello

This is the /ibergrid section of this demo website.

You're now logged in as: vianello

This application has received the following information:

access_token (JWT):

eyJraWQiOiJyc2ExliwiYWxnljoiUIMyNTYifQ.eyJzdWliOiJIMzM3MzU0My05NDM2LTQ1MGUtOTFi.

ረት

access_token (decoded):

```
{
    "sub": "e3373543-9436-450e-91bf-439f3ea18622",
    "iss": "https://iam-demo.cloud.cnaf.infn.it/",
    "name": "Enrico Vianello",
    "groups": [
        "ibergrid",
        "demo",
        "ibergrid/feudal"
],
    "preferred_username": "vianello",
```

Thanks for your attention. Questions?

Useful references

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

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

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

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

Contacts:

- <u>andrea.ceccanti@cnaf.infn.it</u>
- <u>enrico.vianello@cnaf.infn.it</u>
- <u>indigo-aai.slack.com</u>