INDIGO-Datacloud
Identity and Access Management Service

INDIGO - DataCloud

RIA-653549

Presented by Andrea Ceccanti (INFN)

andrea.ceccanti@cnaf.infn.it

WLCG AuthZ WG Meeting

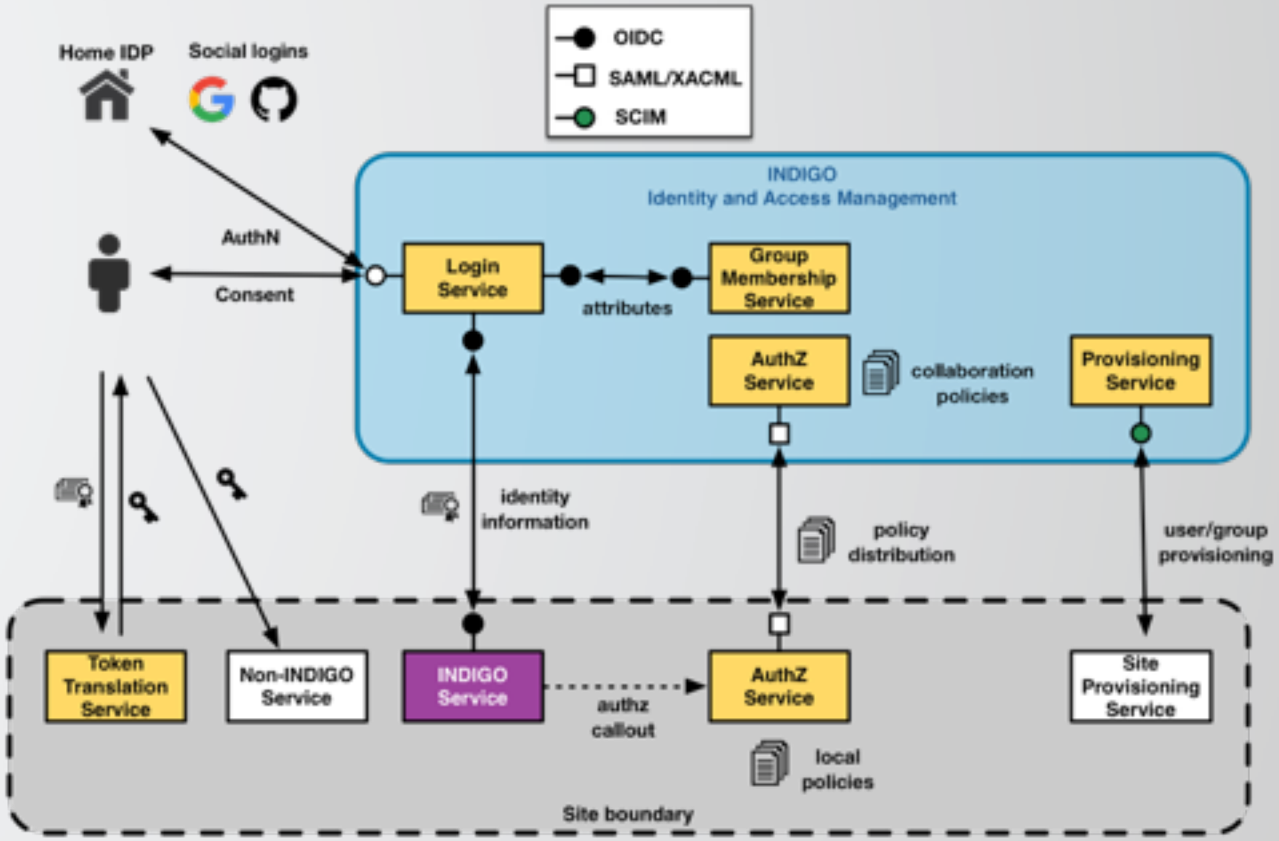
Dec, 14th 2017

INDIGO-DataCloud is co-founded by the
Horizon 2020Framework Programme

IAM overview

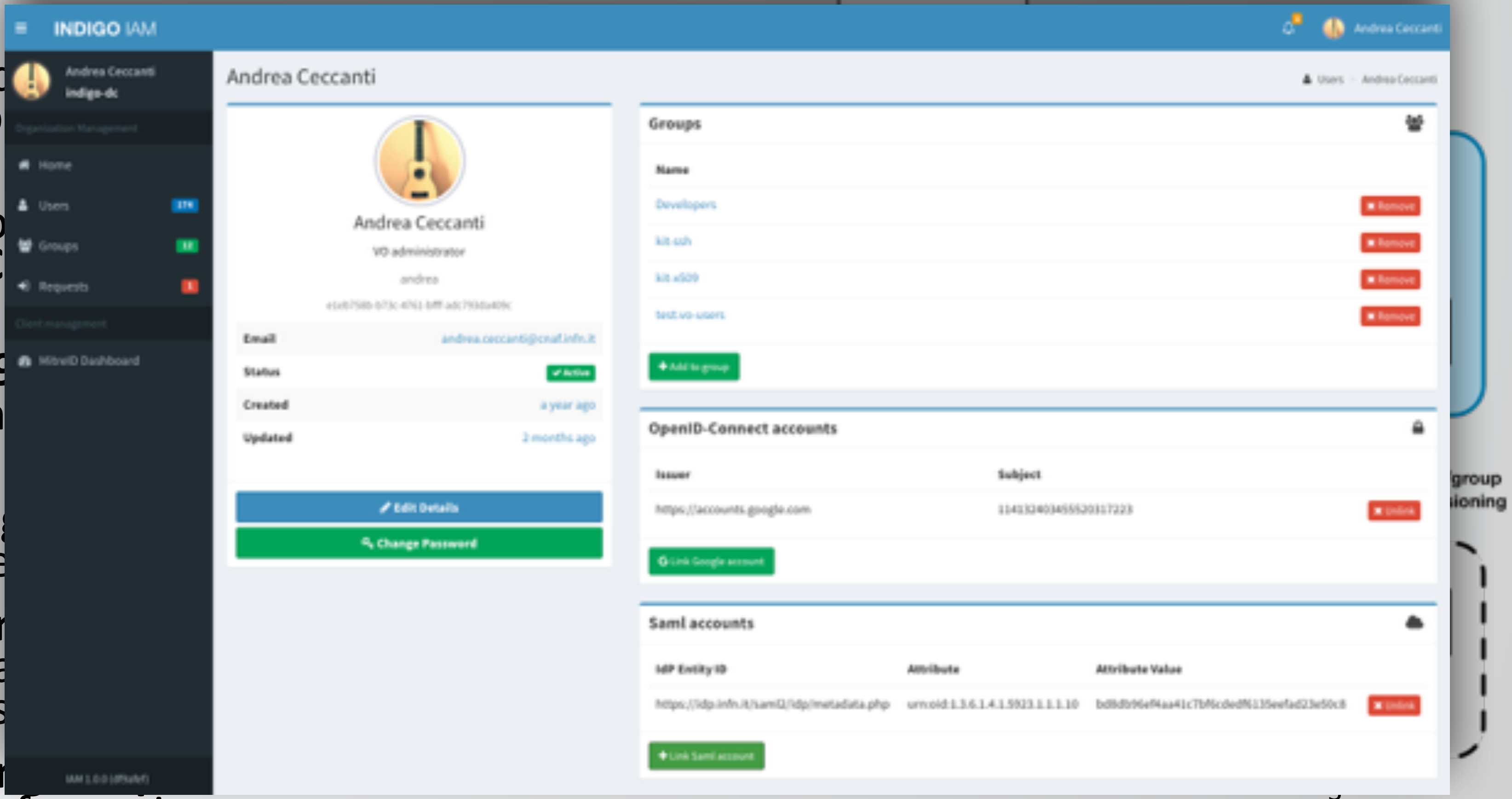
INDIGO IAM

- The **I**dentity and **A**ccess **M**anagement (**IAM**) service
  - Authenticates users with supported mechanisms (SAML, X.509, Google, username/password, …)
  - Provides a **persistent id** for the user and **other attributes** (e.g., group membership) to relying applications via standard **OpenID Connect/ OAuth2** interfaces
  - Provides the ability to link for **X.509** certificates, **SAML** and **OpenID Connect** accounts to the IAM account
  - Provides **group membership management** and **registration service** for the managed organization
  - Can be configured to support **automatic organization enrollment** for users authenticated by trusted **SAML** identity providers
  - Provides SCIM **standard provisioning endpoints** to expose organization membership information



INDIGO IAM

- The **I**dentity and **A**ccess **M**anagement (**IAM**) service
    - Authenticates users with supportec (SAML, X.509, Google, username/p
    - Provides a **persistent id** for the use **attributes** (e.g., group membership applications via standard **OpenID C** **OAuth2** interfaces
    - Provides the ability to link for **X.509** **SAML** and **OpenID Connect** accoun account
    - Provides **group membership mana** **registration service** for the manage
    - Can be configured to support **autor** **organization enrollment** for users a by trusted **SAML** identity providers
    - Provides SCIM **standard provisionin** expose organization membership information



Andrea Ceccanti

Andrea Ceccanti

VO administrator

andrea

e1e07586-073c-4761-bfff-adc7930a409c

Email	andrea.ceccanti@cnaf.infn.it
Status	✓ Active
Created	a year ago
Updated	2 months ago

Edit Details

Change Password

Groups

Name	
Developers	Remove
kit-ssh	Remove
kit-x509	Remove
test.vo-users	Remove

+ Add to group

OpenID-Connect accounts

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

Link Google account

Saml accounts

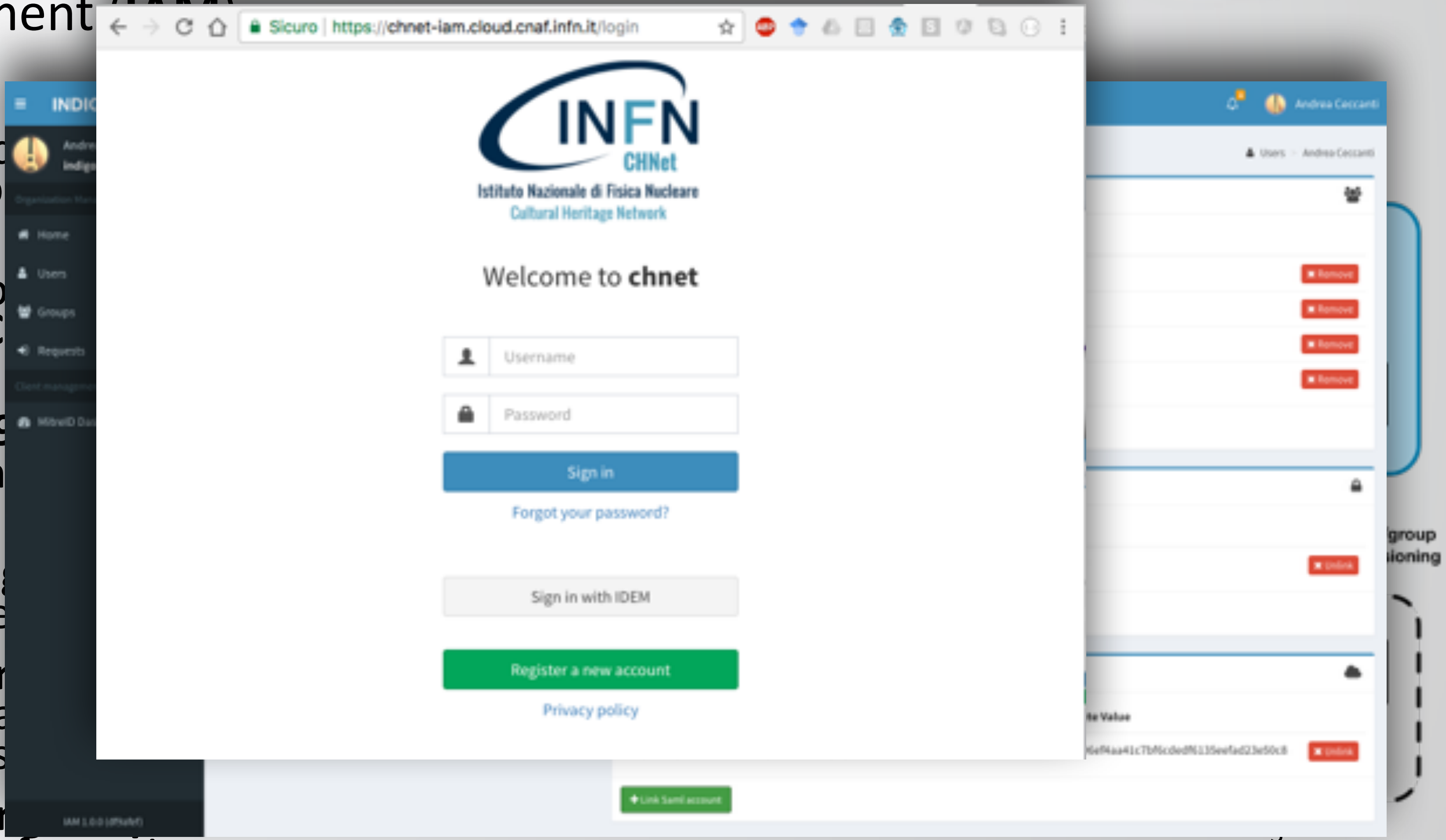
IdP Entity ID	Attribute	Attribute Value	
https://idp.infn.it/saml2/idp/metadata.php	urn:oid:1.3.6.1.4.1.5923.1.1.1.10	bd8db96ef4aa41c7bf6cded f6135eefad23e50c8	Unlink

+ Link Saml account

/group
ioning

INDIGO IAM

- The **I**dentity and **A**ccess **M**anagement (IAM) service
  - Authenticates users with supported (SAML, X.509, Google, username/p
  - Provides a **persistent id** for the use **attributes** (e.g., group membership applications via standard **OpenID C OAuth2** interfaces
  - Provides the ability to link for **X.509 SAML** and **OpenID Connect** accoun account
  - Provides **group membership mana registration service** for the manage
  - Can be configured to support **auton organization enrollment** for users a by trusted **SAML** identity providers
  - Provides [SCIM](#) **standard provisionin** expose organization membership information



Sicuro https://chnet-iam.cloud.cnaf.infn.it/login

INFN CHNet

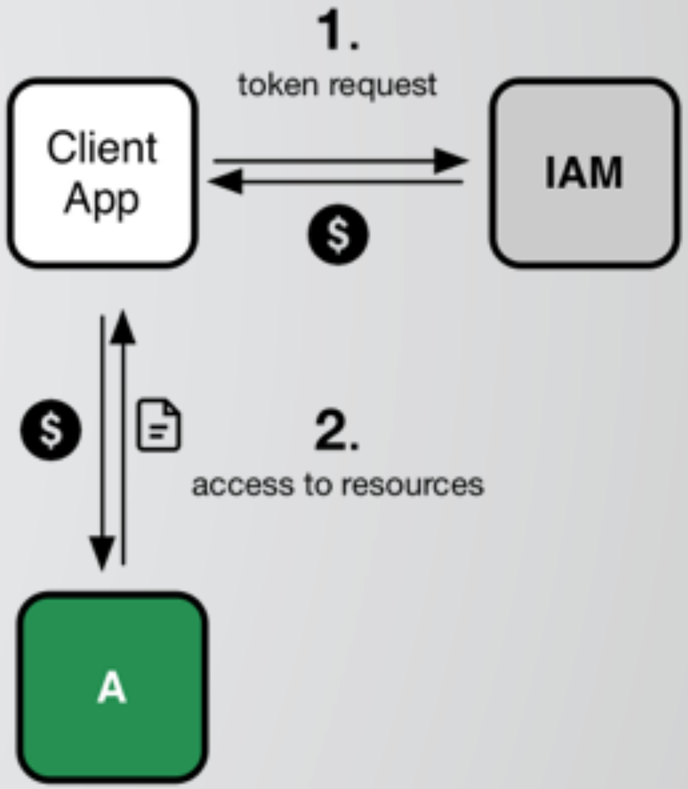
Istituto Nazionale di Fisica Nucleare

Cultural Heritage Network

Welcome to **chnet**

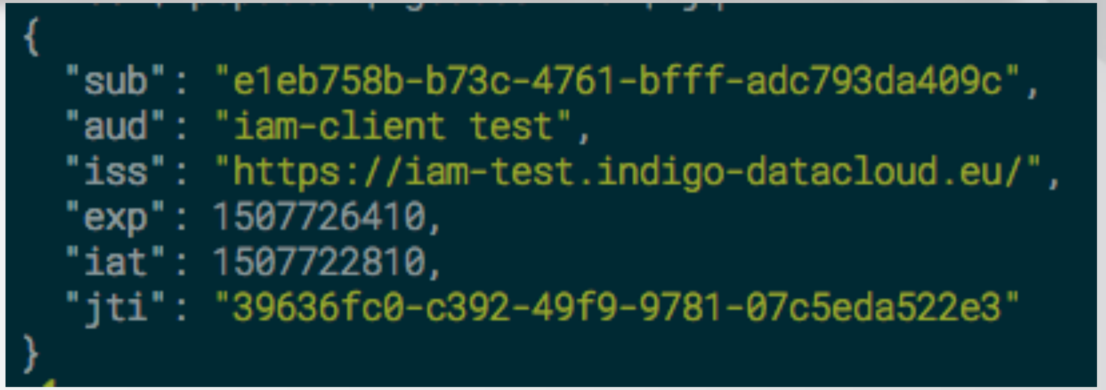
Authorization in INDIGO: **OAuth**

- In order to access resources, a client needs an OAuth **access token**
- The token is obtained from the **INDIGO IAM** using standard OAuth/OpenID Connect flows
- Authorization can then be performed @ the services leveraging:
  - **OAuth scopes:** authorization labels that can be linked to access tokens at token creation time
  - **Identity attributes:** e.g. VO name, group membership attributes, username

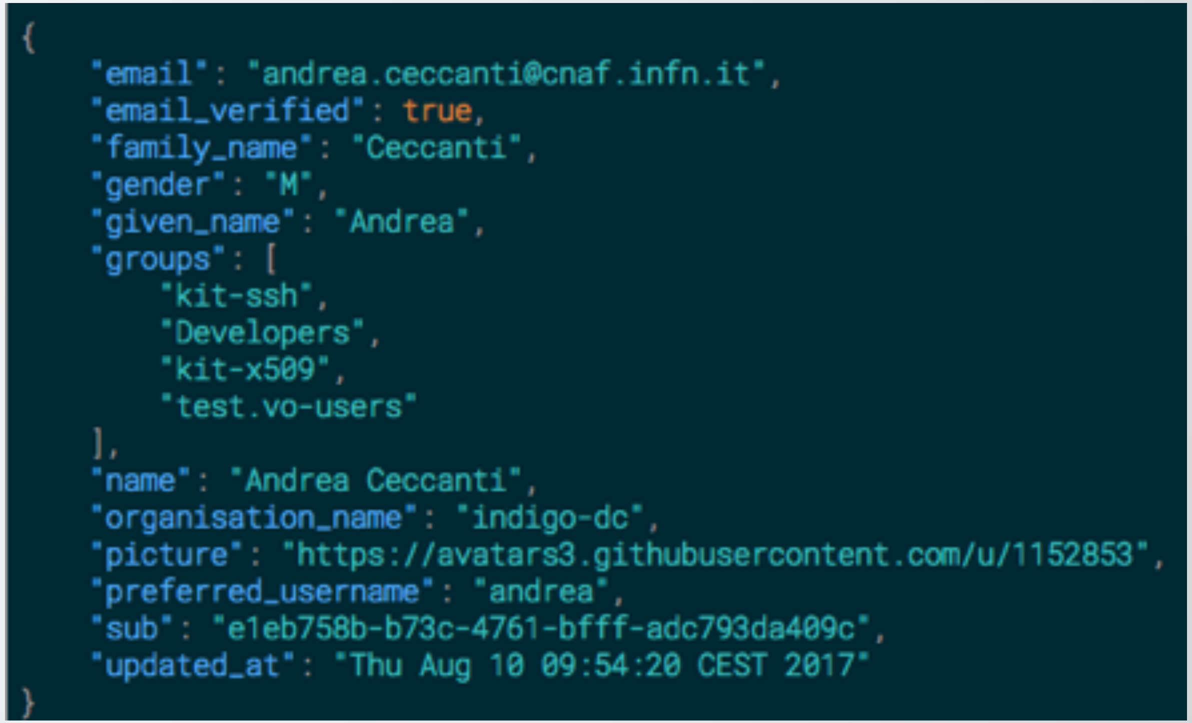


Tokens in INDIGO: **Json Web Tokens (JWT)**

- We use signed JWTs for our Access Tokens
- Access tokens contain basic authz information
- More authn/authz 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"
}
```

IAM demo

Registration/Enrollment flow

- “Traditional”, VOMS-Admin inspired administrator approved enrollment flow, augmented with support for EduGAIN/Google authN
  1. Applicant fills basic registration information (which includes AUP acceptance)
  2. Applicant Email ownership verification step (via a verification token sent to to the address
  3. Organization admins informed via email of incoming membership request
  4. Applicant informed of administrators decision

Automatic enrollment

- IAM can also be configured to supports automatic enrollment, without administrator approval, for user authenticating via a trusted SAML IdP

Authentication and account linking

- Users can authenticate to the IAM with
  - IAM username/password credentials (created at registration time)
  - their SAML Home Institution IdP (if SAML AuthN enabled by configuration)
  - their Google account (if Google AuthN enabled by configuration)
  - their X.509 certificate (if X.509 AuthN enabled by configuration)
- Users can link/unlink any of these credentials to the their IAM account
- Account linking can happen
  - at registration time
  - later, linking via the IAM dashboard

SAML authentication and linking

- IAM favours a **persistent** id attribute from the IdP to enable linking
- The attribute used is configurable, with the default being (in order)
    - EduPersonUniqueID, EduPersonTargetedID, EduPersonPrincipalName
- IAM allows to restrict which IdPs to trust by
    - IdP EntityId whitelisting
    - IdP SIRTFI compliance or R&S compliance

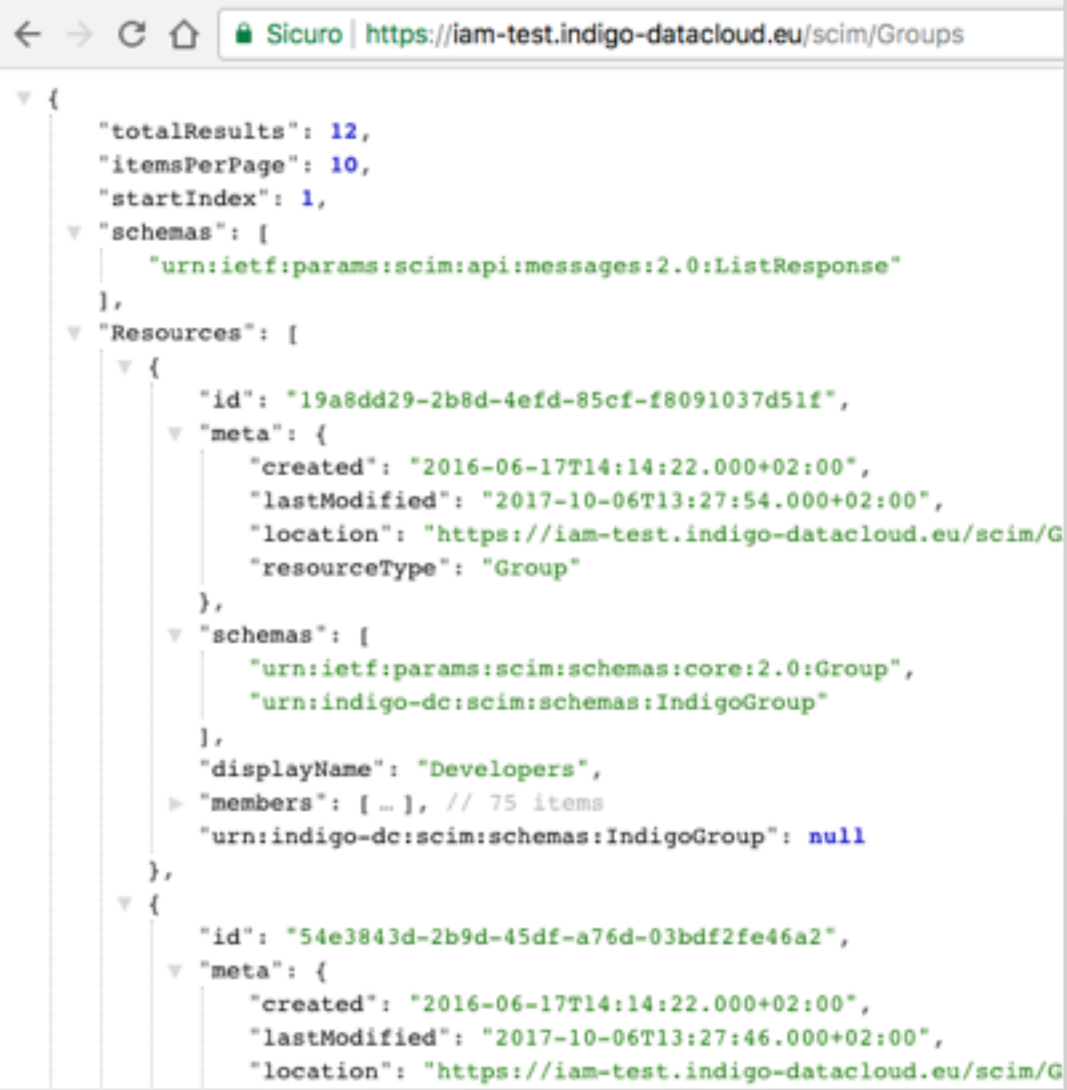
Group management

- IAM provides Group management functionality via
  - the dashboard
  - SCIM provisioning APIs
- Groups can be organized hierarchically

Provisioning in INDIGO: **SCIM**

- SCIM is a IETF standard defining
  - an (extensible) schema to represent users and groups in an organization
  - the REST API used for querying and managing this information

- **IAM** implements SCIM endpoints for user and groups management



```
{
    "totalResults": 12,
    "itemsPerPage": 10,
    "startIndex": 1,
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
    "Resources": [
        {
            "id": "19a8dd29-2b8d-4efd-85cf-f8091037d51f",
            "meta": {
                "created": "2016-06-17T14:14:22.000+02:00",
                "lastModified": "2017-10-06T13:27:54.000+02:00",
                "location": "https://iam-test.indigo-datacloud.eu/scim/G
                "resourceType": "Group"
            },
            "schemas": [
                "urn:ietf:params:scim:schemas:core:2.0:Group",
                "urn:indigo-dc:scim:schemas:IndigoGroup"
            ],
            "displayName": "Developers",
            "members": [ … ], // 75 items
            "urn:indigo-dc:scim:schemas:IndigoGroup": null
        },
        {
            "id": "54e3843d-2b9d-45df-a76d-03bdf2fe46a2",
            "meta": {
                "created": "2016-06-17T14:14:22.000+02:00",
                "lastModified": "2017-10-06T13:27:46.000+02:00",
                "location": "https://iam-test.indigo-datacloud.eu/scim/G
```

CLI support: getting a token out of IAM

- OAuth password flow
  - User credentials exposed to the device, cannot leverage SAML/ Google authentication

- OAuth device code flow (**recommended**)
  - User credentials **not** exposed to the device, can leverage any authentication flow supported by IAM

IAM OAuth scope policies

- MitreID does not support limiting the access to certain OAuth scopes to specific users or groups

- IAM implements the Scope Policy API that allow administrators to restrict which users/groups are entitled to request OAuth scopes

Argus Authorization Service & INDIGO AAI

Objective:

- Integrate INDIGO AAI in Argus to provide consistent and centralized authorization for services that accept OAuth tokens

- Plan:
  - Write an Argus PIP to extract authN and authZ information from the OAuth token
  - Write a profile that defines how the attributes can be used to write and enforce policies
- ETA
  - **Done** (PR under review)

IAM resources

- IAM @ Github: https://github.com/indigo-iam/iam
- IAM docs @ Gitbook : https://iam-docs.gitbooks.io/iam-documentation/content/v/develop/
- INDIGO IAM test instance: https://iam-test.indigo-datacloud.eu

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

Thank you

https://www.indigo-datacloud.eu

Better Software for Better Science

INDIGO - DataCloud

INFN Istituto Nazionale di Fisica Nucleare

Universiteit Utrecht

CESNET

CSIC Consejo Superior de Investigaciones Científicas

PSNC

cea energie atomique • energies alternatives

cmcc Centro Euro-Mediterraneo sui Cambiamenti Climatici

AGH AGH University of Science and Technology

Reply

ICCU

DESY

CERM Firenze

egi

KIT Karlsruher Institut für Technologie

Science & Technology Facilities Council

RB

cnrs dépasser les frontières

LIP Laboratório de Instrumentação e Física Experimental de Partículas

T-Systems

CERN

Consiglio Nazionale delle Ricerche

Universitat Politècnica de València

indra

AtoS

Istituto Nazionale di Geofisica e Vulcanologia

INAF Istituto Nazionale di Astrofisica National Institute for Astrophysics

@indigodatacloud

www.indigo-datacloud.eu

https://www.facebook.com/indigodatacloud/