ESCAPE:
Authentication and Authorization

Andrea Ceccanti
INFN

ESCAPE WP2-WP5 workshop

July 2nd 2019

ESCAPE
European Science Cluster of Astronomy & Particle physics ESFRI research Infrastructures

INFN
CNAF

Objectives

Task 2.5 objectives (from the DoW)

“The ESCAPE project **will not build new authentication mechanisms** but **will leverage and build on existing work** to provide the secure composition of data and compute services needed **to enable the data-lake vision**. “

Task 2.5 objectives (from the DoW)

"Through **EGI** and **WLCG** there is a **15-year history of building global AAI**, and with the recent results of the **Indigo-DataCloud** project and the ongoing work in the **AARC** projects to move such AAI structures into the future, **the ESCAPE project will be well placed to integrate such work into the prototypes**."

Task 2.5 objectives (from the DoW)

We will adopt **standards-based** AAI solutions that:

- are flexible enough to support **heterogeneous authentication mechanisms** (federated identities, X.509 certificates, social logins);
- provide the abstraction of **collaboration/virtual organization**, and the tools to manage membership, entitlements and access policies that will regulate access to resources for that organization;
- can support **controlled delegation of privileges** across the distributed chain of services implementing the Data-Lake vision;
- **can be easily integrated** in existing data access and computing software leveraging standard, off-the-shelf libraries and components, in particular to map collaboration-level authentication and authorization attributes and capabilities to local access mechanisms.

Key AAI requirements

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/de-provisioning of identities to services/relying resources

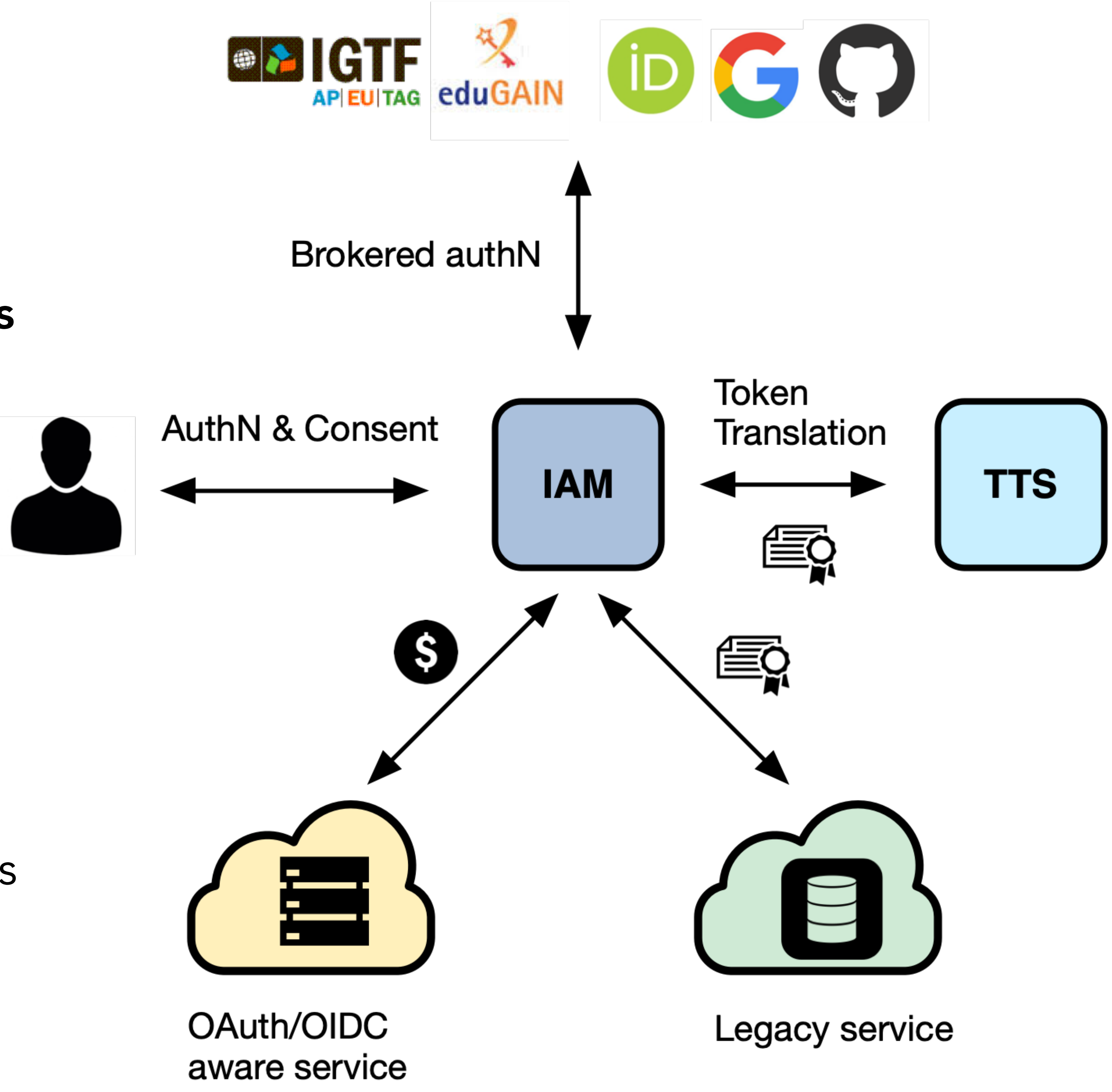
Token translation

- Enable **integration with legacy services through controlled credential translation**

High level AAI approach

Introduce a **central community-scoped authorization service** that

- deals with user authentication, supporting **multiple mechanisms**
- provides users with a **persistent, community-scoped** identifier
- exposes **identity information**, **attributes** and **capabilities** to services via **JWT** tokens and standard **OAuth & OpenID Connect** protocols
- can integrate with legacy services via token translation
- supports **Web** and **non-Web access**, **delegation** and **token renewal**

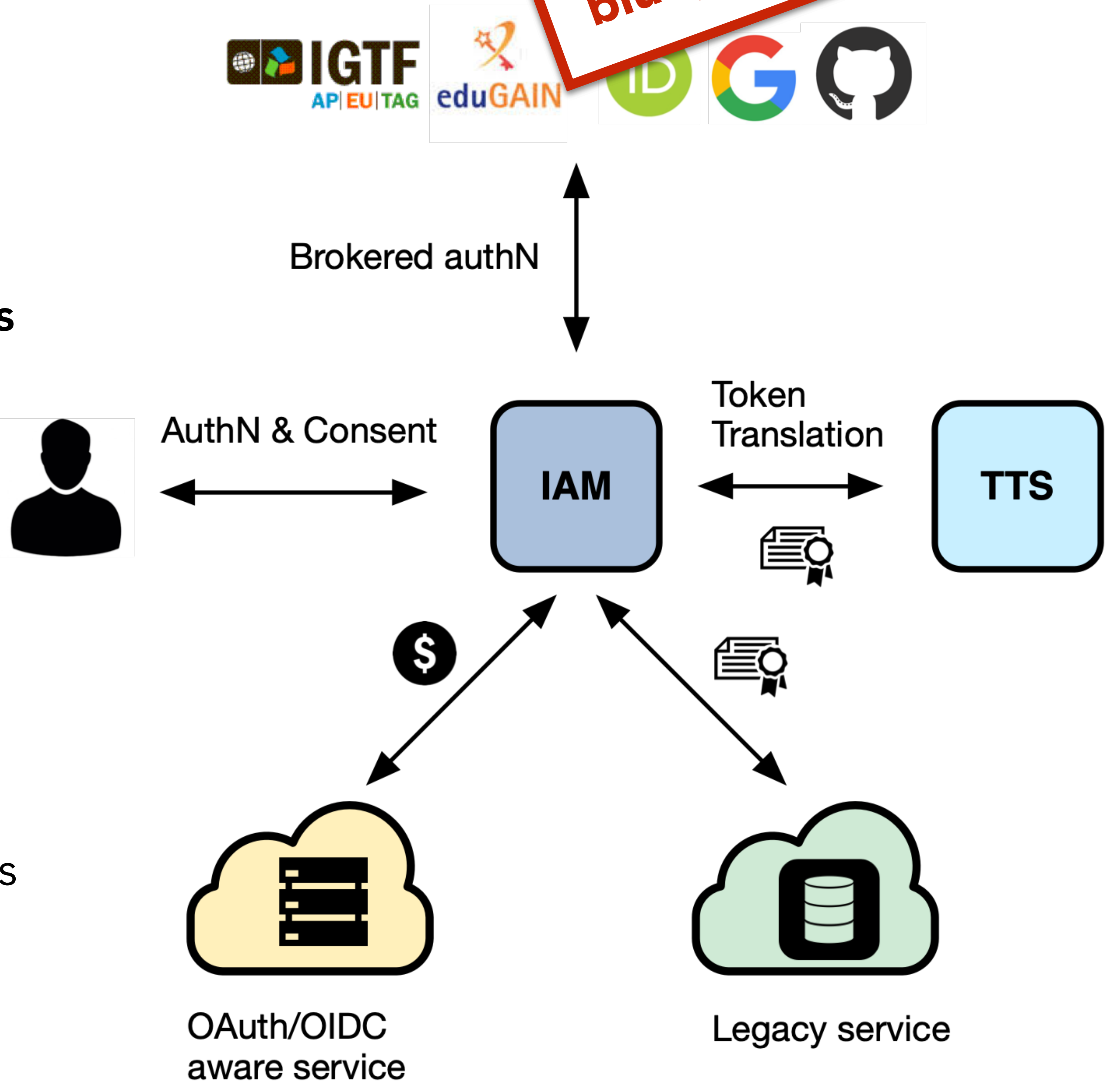


High level AAI approach

Introduce a **central community-scoped authorization service** that

- deals with user authentication, supporting **multiple mechanisms**
- provides users with a **persistent, community-scoped** identifier
- exposes **identity information**, **attributes** and **capabilities** to services via **JWT** tokens and standard **OAuth & OpenID Connect** protocols
- can integrate with legacy services via token translation
- supports **Web** and **non-Web access**, **delegation** and **token renewal**

Compliant with AARC blueprint architecture



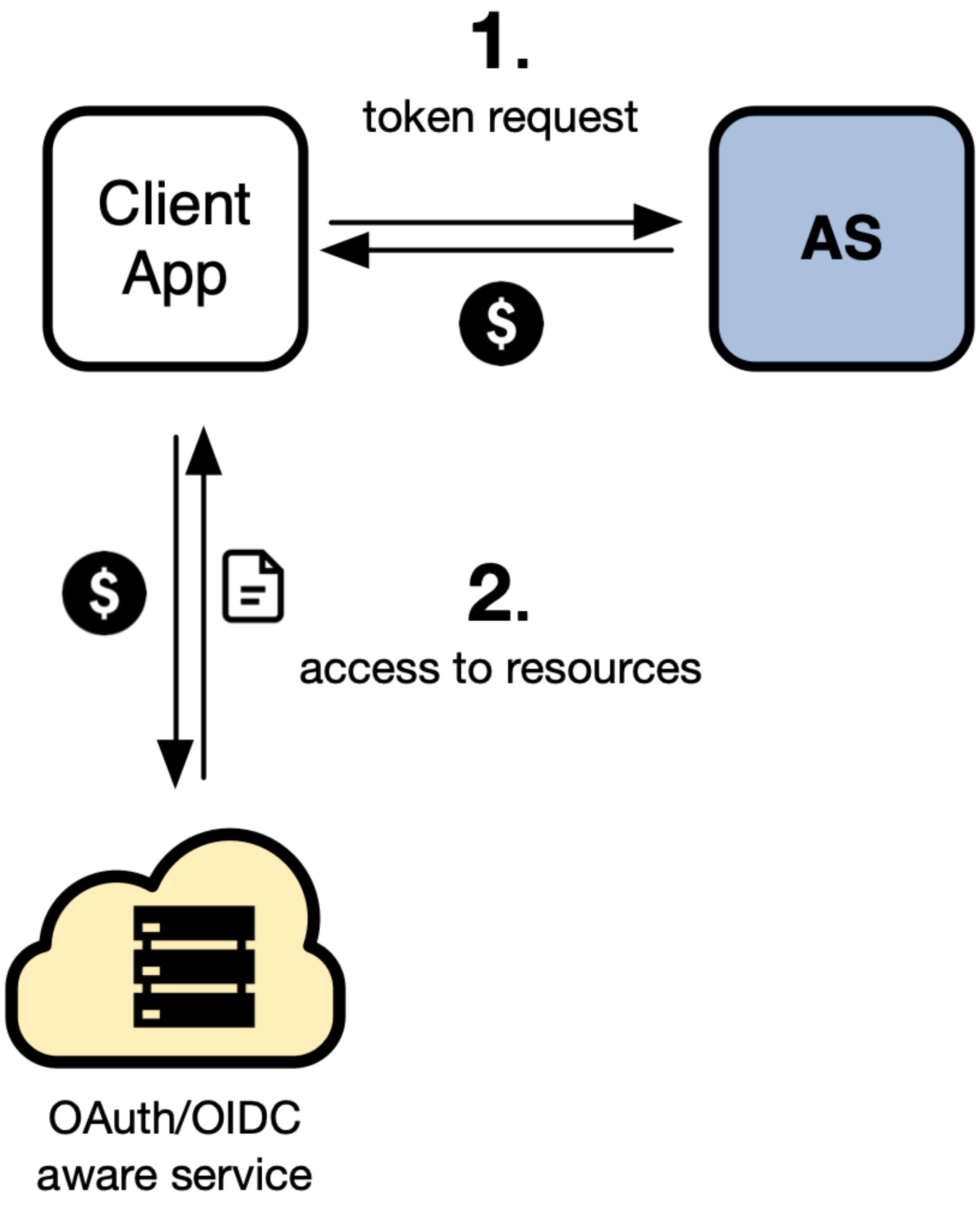
Token-based AAI

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

The token is obtained from **a community authorization server** using standard **OAuth/OpenID Connect** flows

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

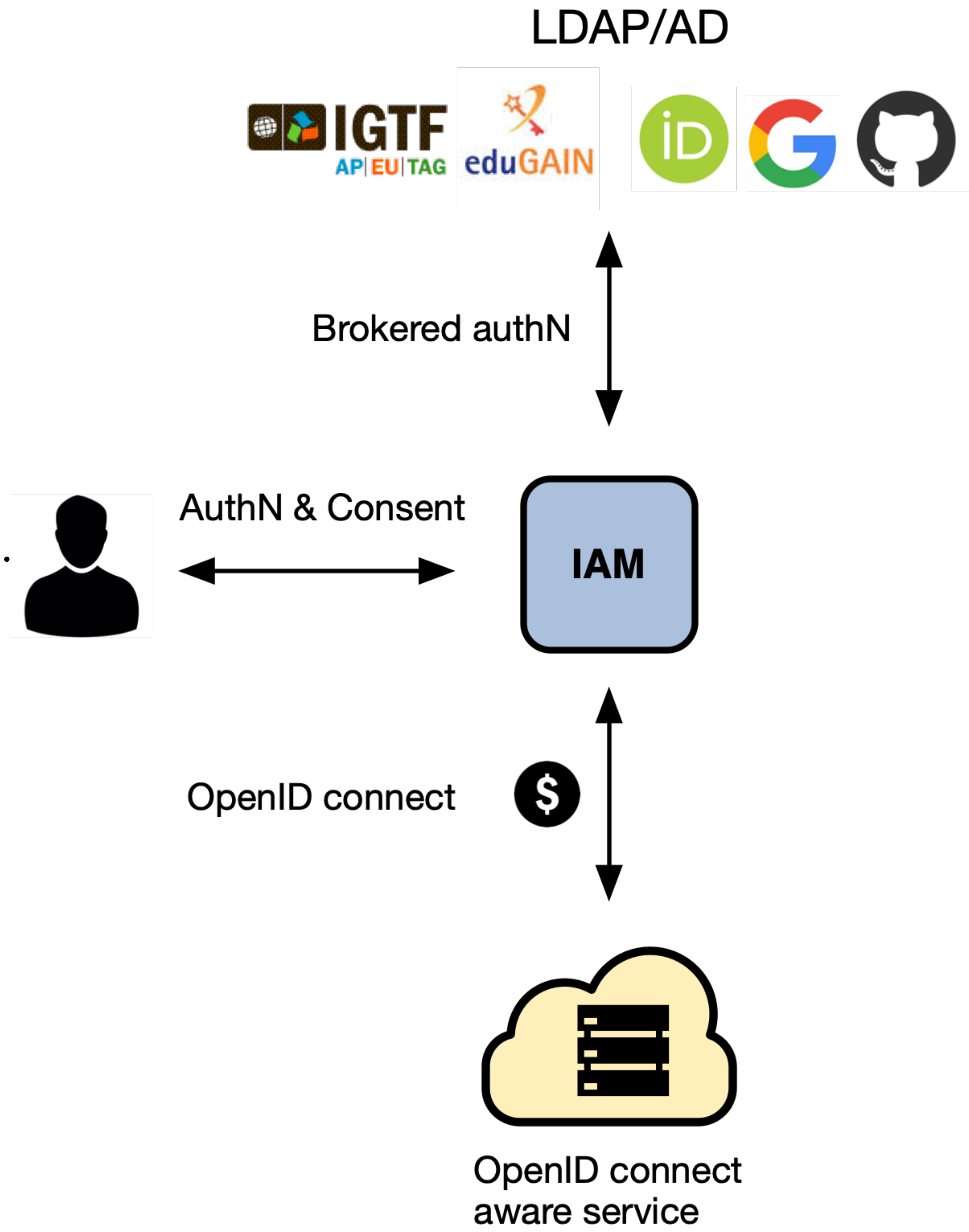
- **Identity attributes**: e.g., **groups**, roles, …
- **OAuth scopes**: capabilities linked to access tokens at token creation time



Centralized Authentication

Authentication is **delegated to the central community authorization server**, which can support **multiple authentication mechanisms**

- Identity federations (e.g., EduGAIN)
- Community accounts & credentials (e.g. a community-managed LDAP)
- Social logins (e.g., Google, ORCID)
- X.509 certificates



Authentication information is then **exposed to services/relying parties via the OpenID Connect protocol**

- low-friction integration at services

Authorization

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.: **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

Enabling technologies: an overview

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"

BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE

T22000129

Name/Surname/Nom
MUSTERMANN
GEB. GABLER

Vornamen/Given names/Prénoms
ERIKA

Geburtstag/Date of birth/
Date de naissance
12.08.1964

Staatsangehörigkeit/Nationality/
Nationalité
DEUTSCH

Geburtsort/Place of birth/Lieu de naissance
BERLIN

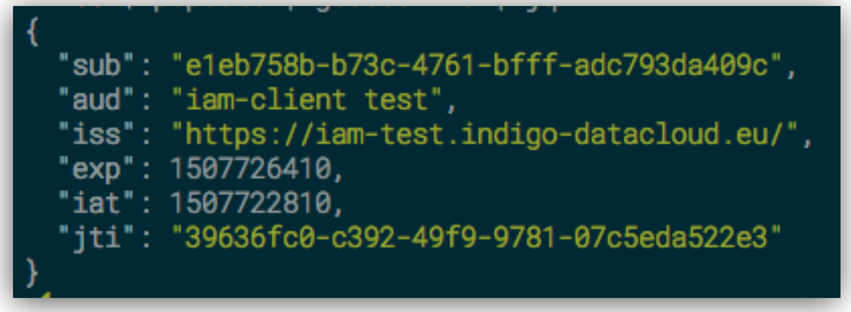
Gültig bis/Date of expiry/
Date d'expiration
31.10.2020

938568

Unterschrift der Inhaberin/des Inhabers -
Signature of bearer - Signature de la titulaire/du titulaire

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: 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. APIs)

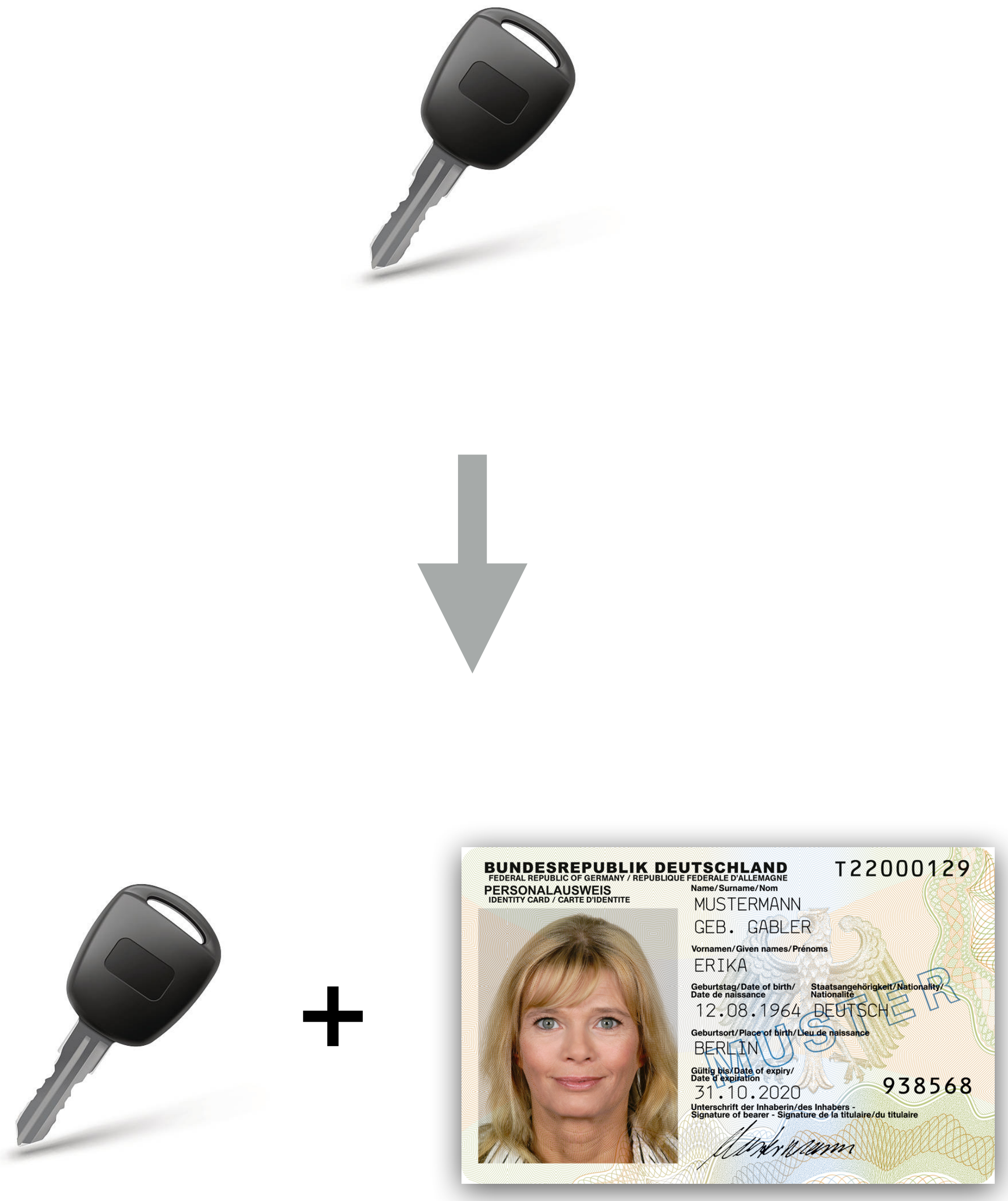
OpenID Connect: an identity layer for OAuth

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)



BUNDESREPUBLIK DEUTSCHLAND T22000129
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE

Name/Surname/Nom
MUSTERMANN
GEB. GABLER

Vornamen/Given names/Prénoms
ERIKA

Geburtstag/Date of birth/Date de naissance
12.08.1964

Staatsangehörigkeit/Nationality/Nationalité
DEUTSCH

Geburtsort/Place of birth/Lieu de naissance
BERLIN

Gültig bis/Date of expiry/Date d'expiration
31.10.2020

938568

MUSTER

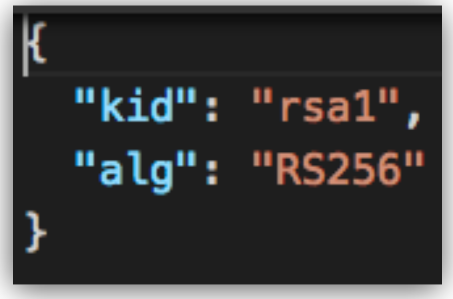
Unterschrift der Inhaberin/des Inhabers - Signature of bearer - Signature de la titulaire/du titulaire

JSON Web Tokens (JWT)

JSON Web Token (JWT) is an open standard 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**.

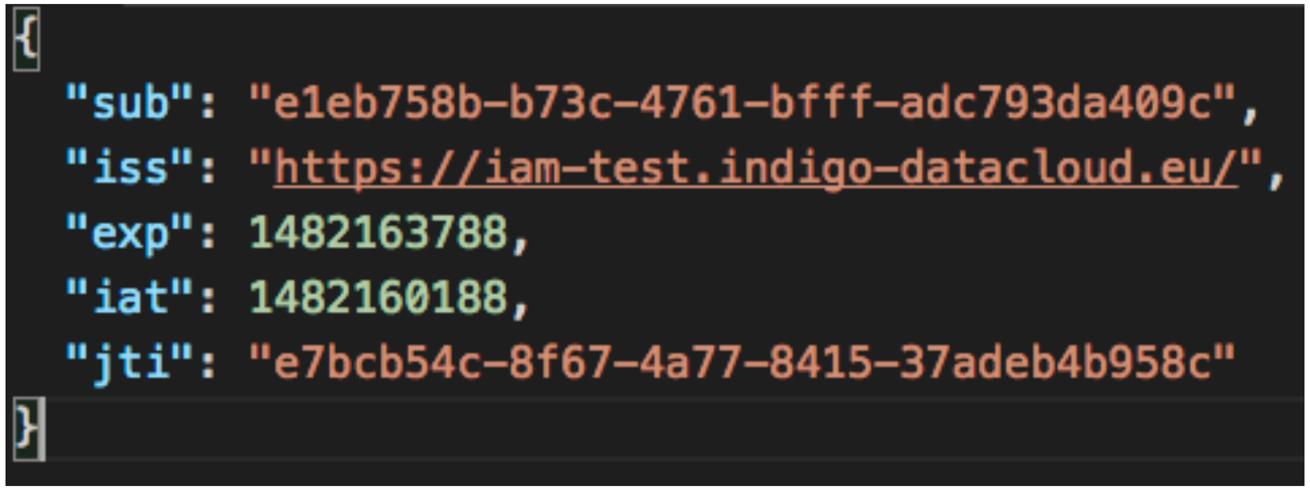
Header



```
{
  "kid": "rsa1",
  "alg": "RS256"
}
```

.

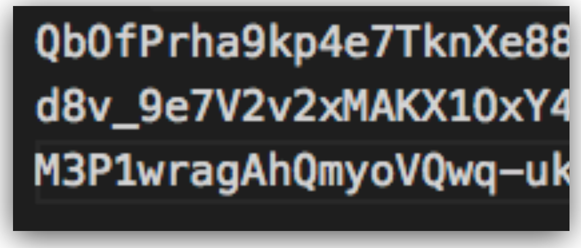
Body



```
{
  "sub": "e1eb758b-b73c-4761-bfff-adc793da409c",
  "iss": "https://iam-test.indigo-datacloud.eu/",
  "exp": 1482163788,
  "iat": 1482160188,
  "jti": "e7bcb54c-8f67-4a77-8415-37adeb4b958c"
}
```

.

Signature



```
Qb0fPrha9kp4e7TknXe88
d8v_9e7V2v2xMAKX10xY4
M3P1wragAhQmyoVQwq-uk
```

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

The INDIGO IAM service

INDIGO Identity and Access Management service

Flexible authentication support

- (SAML, X.509, OpenID Connect, username/password, …)

Account linking

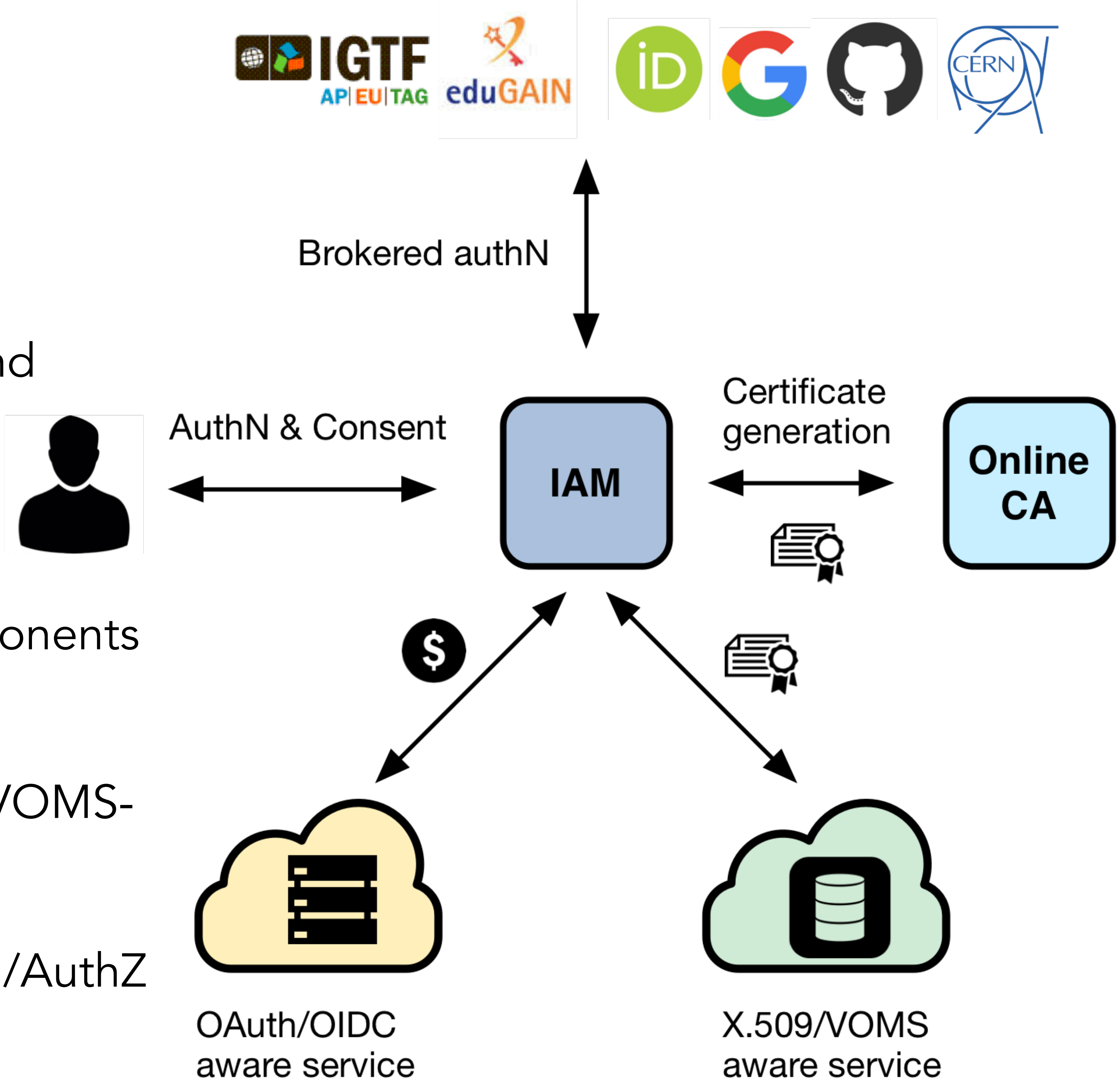
Registration service for moderated and automatic user enrollment

Enforcement of AUP acceptance

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

VOMS support, to integrate existing VOMS-aware services

Self-contained, comprehensive AuthN/AuthZ solution



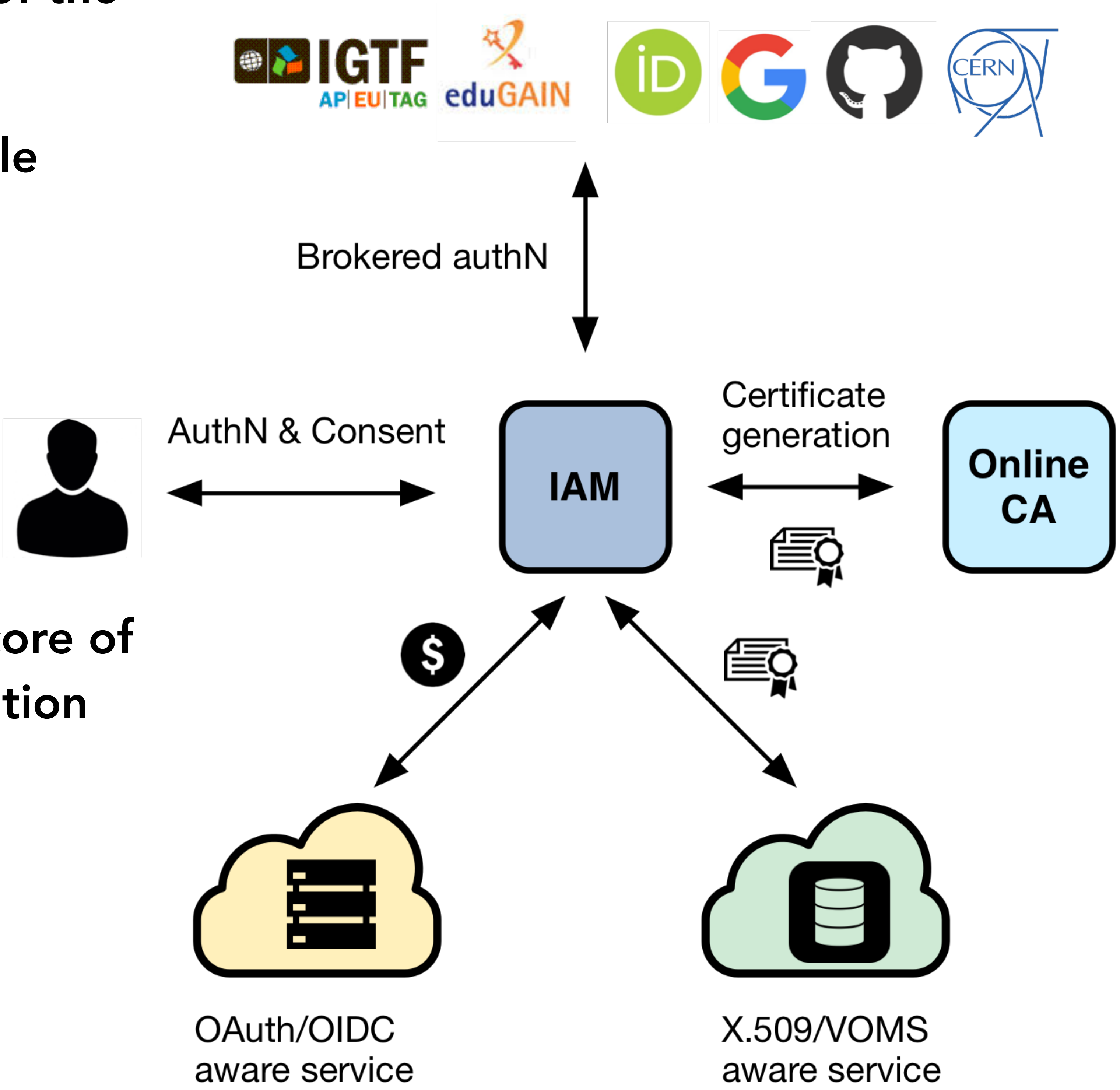
INDIGO Identity and Access Management service

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

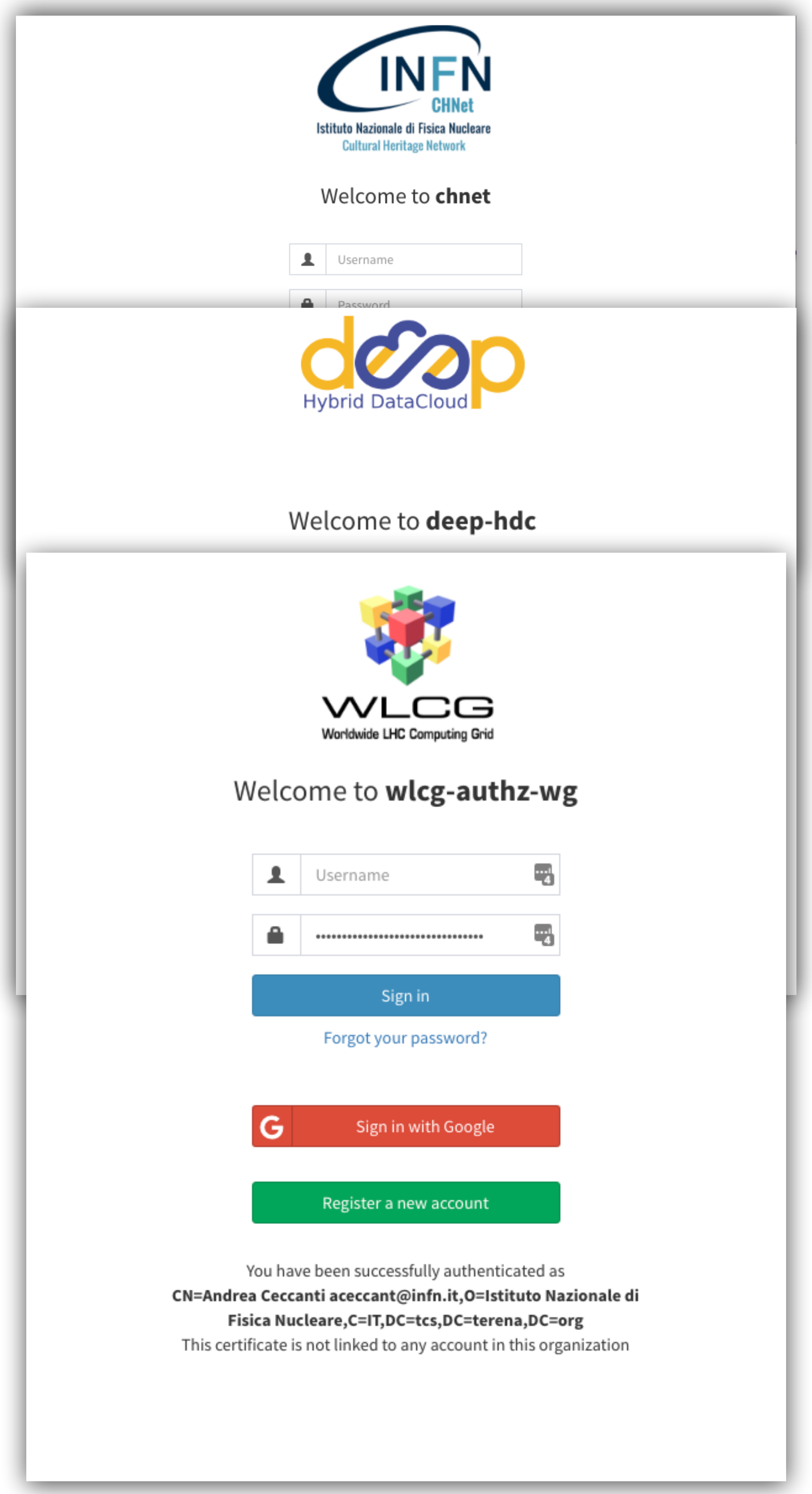


IAM deployment model

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**

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**

Username
Password

deep Hybrid DataCloud

Welcome to **deep-hdc**

WLCG
Worldwide LHC Computing Grid

Welcome to **wlcg-authz-wg**

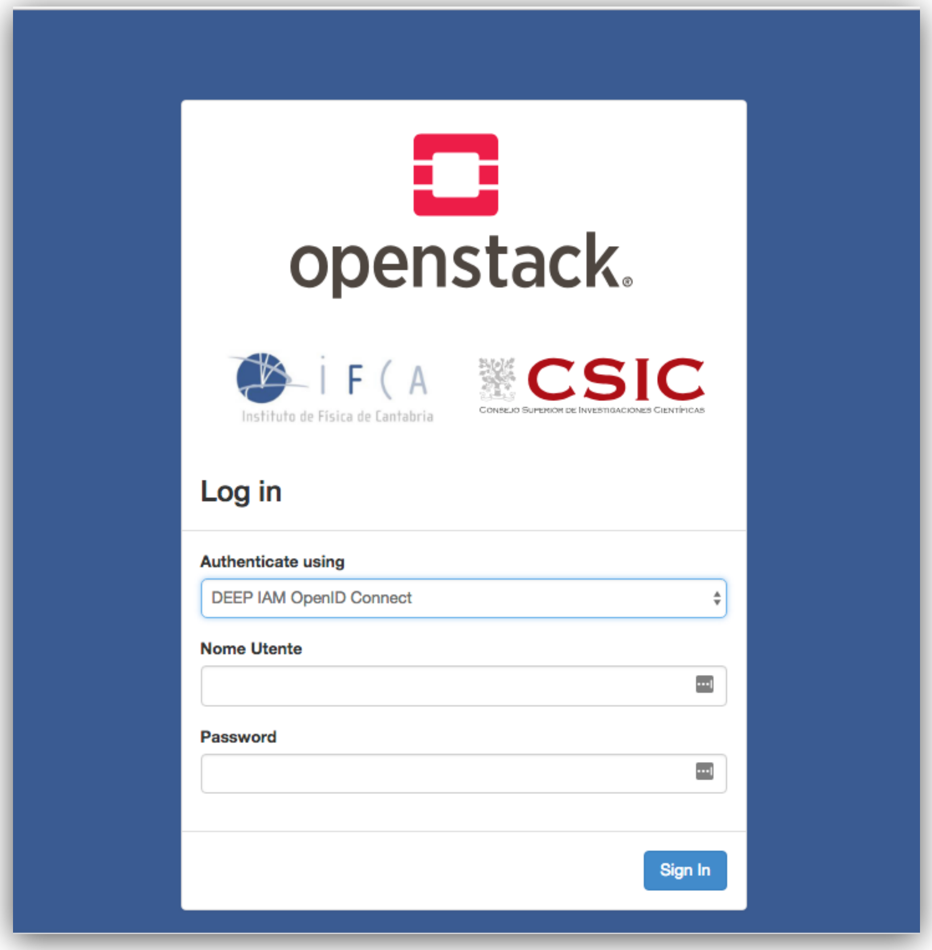
You have been successfully authenticated as
CN=Andrea Ceccanti aceccant@infn.it,O=Istituto Nazionale di Fisica Nucleare,C=IT,DC=tcs,DC=terena,DC=org
This certificate is not linked to any account in this organization

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



openstack.
IFCA Instituto de Física de Cantabria
CSIC Consejo Superior de Investigaciones Científicas

Log in

Authenticate using: DEEP IAM OpenID Connect

Nome Utente

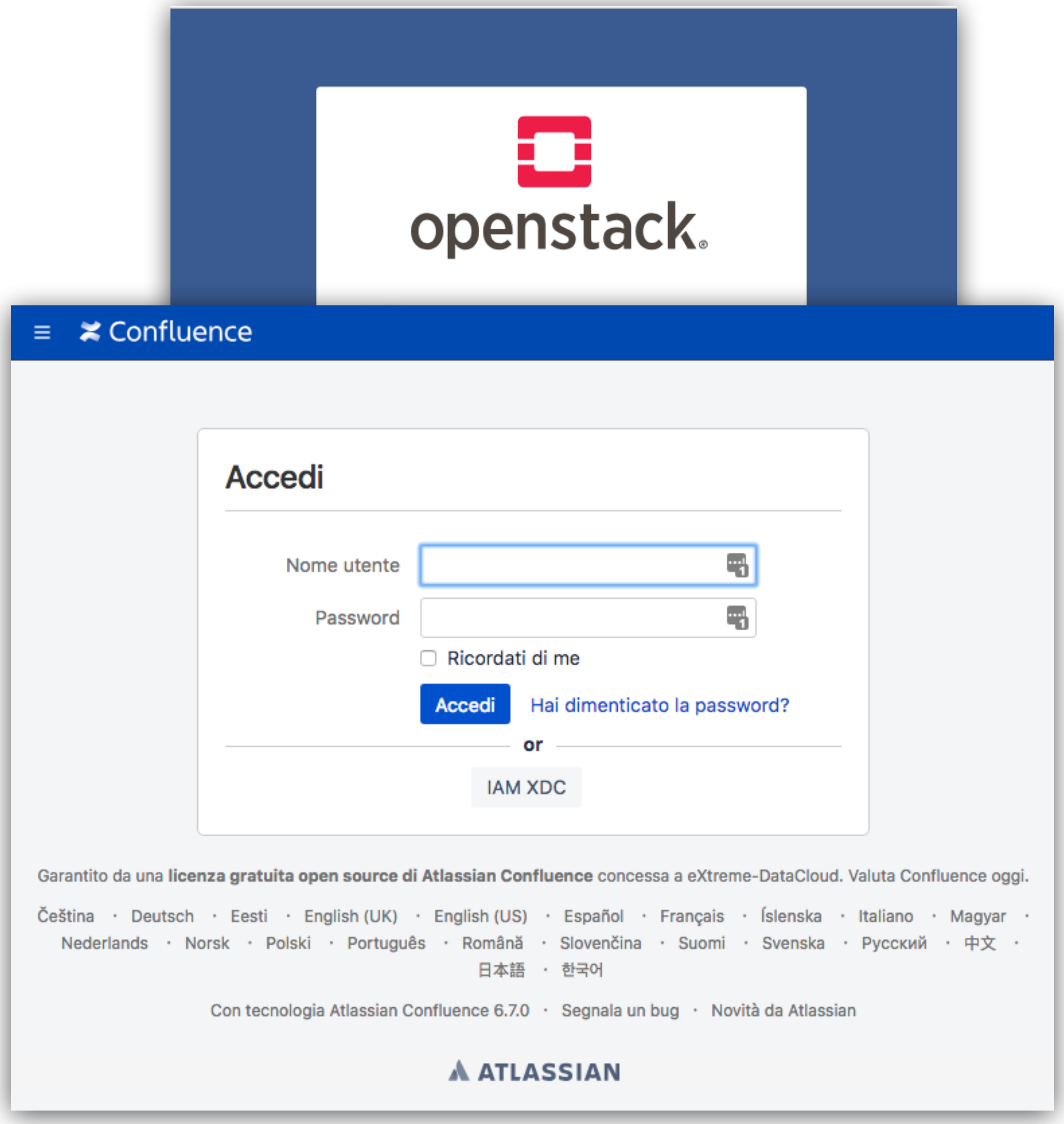
Password

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



Accedi

Nome utente

Password

☐ Ricordati di me

Accedi Hai dimenticato la password?

or

IAM XDC

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

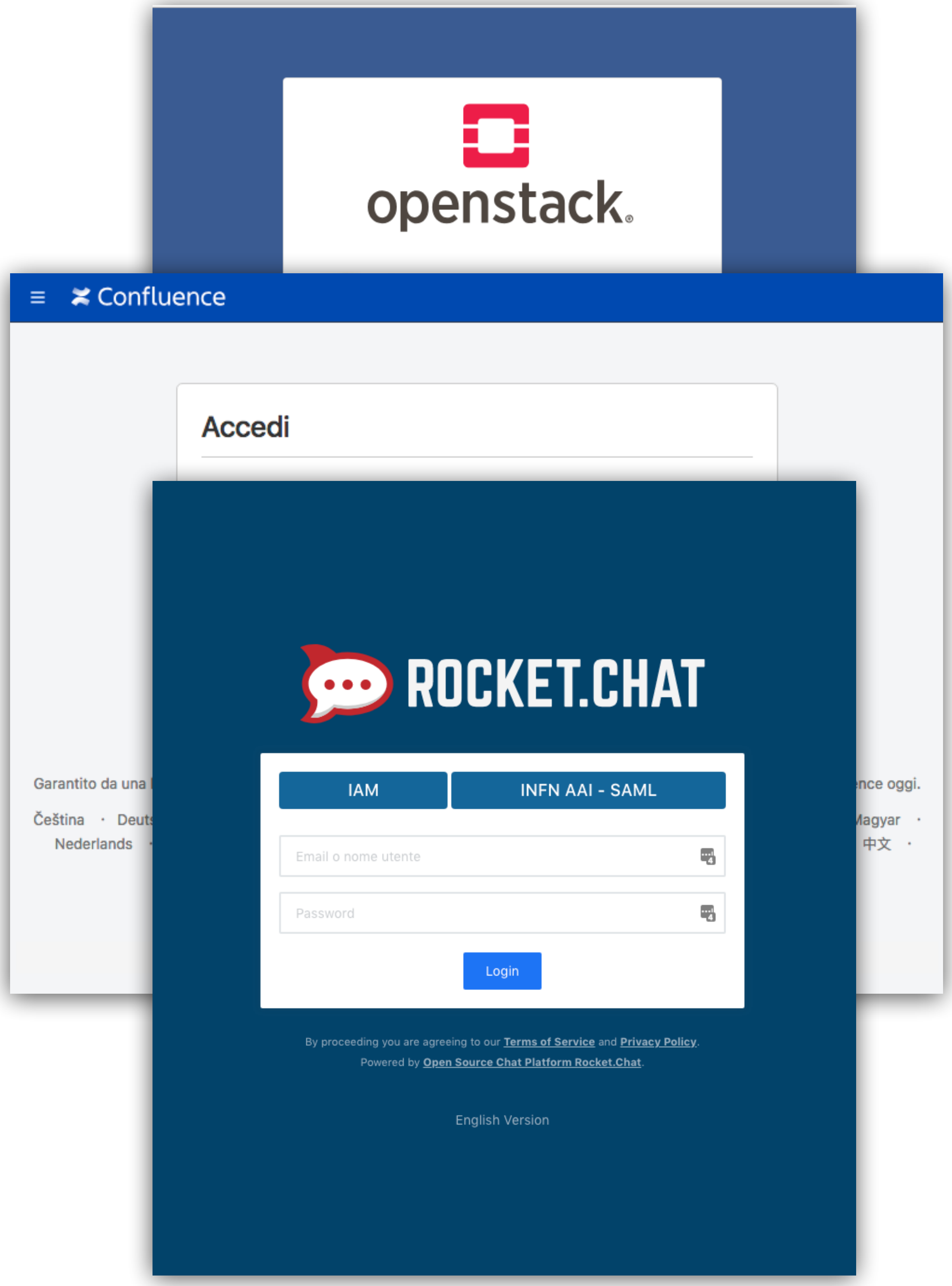
Con tecnologia Atlassian Confluence 6.7.0 · Segnala un bug · Novità da Atlassian

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



By proceeding you are agreeing to our Terms of Service and Privacy Policy.
Powered by Open Source Chat Platform Rocket.Chat.

How does it look like for users?

Joining a community/virtual organization

User enrollment & registration service

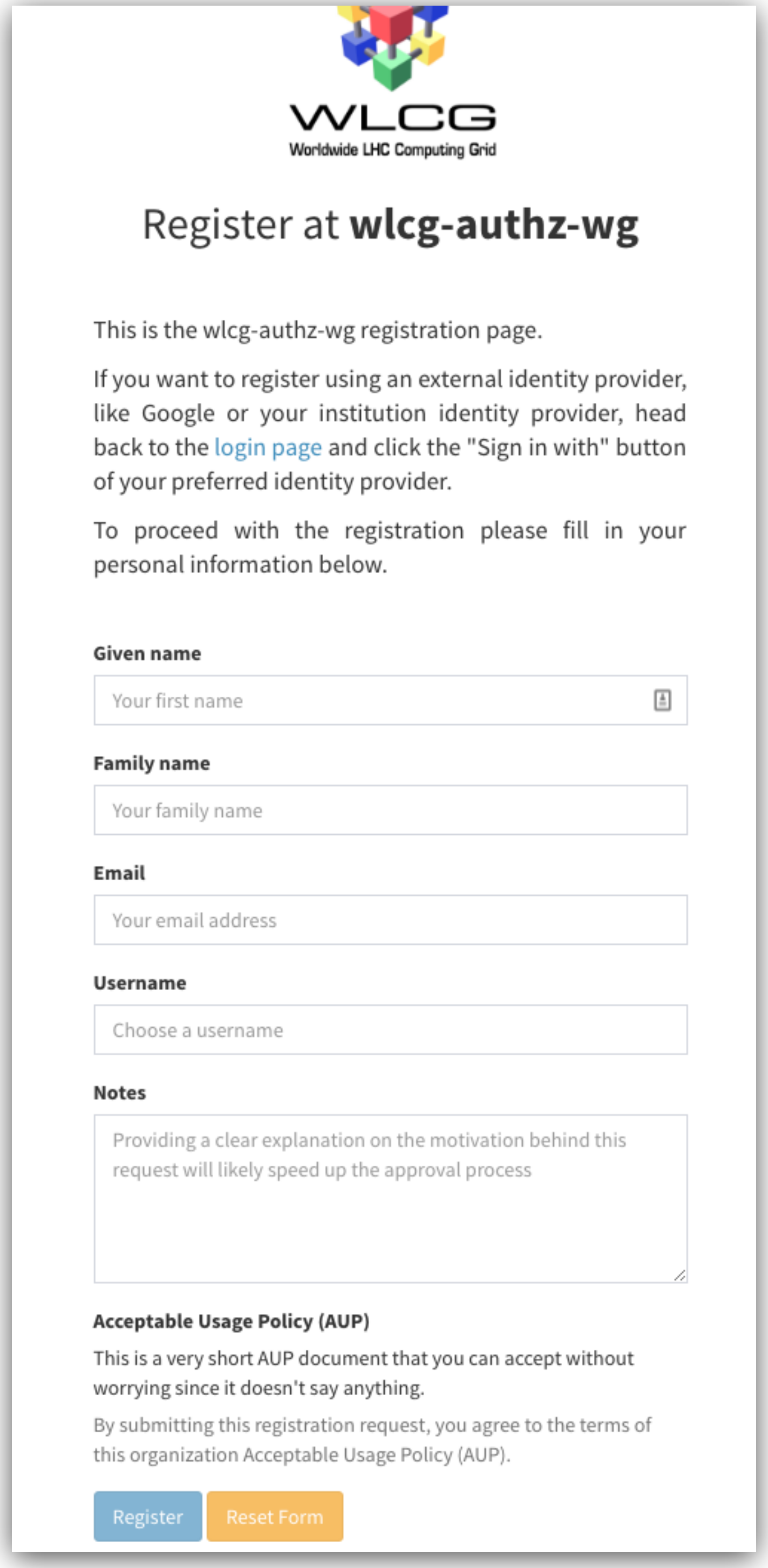
IAM supports two **enrollment flows:**

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

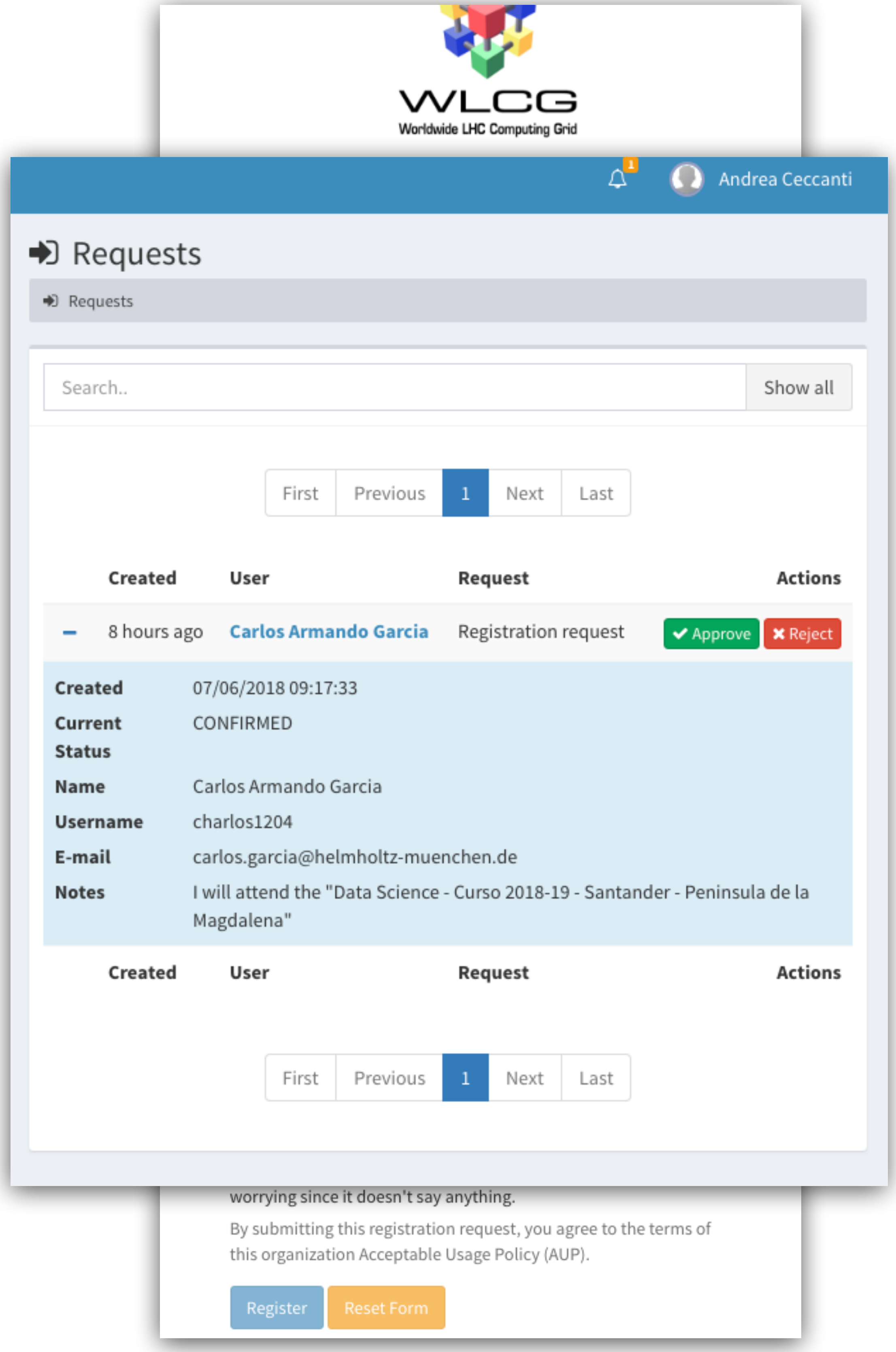
IAM supports two **enrollment flows:**

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



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"

worrying since it doesn't say anything.

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

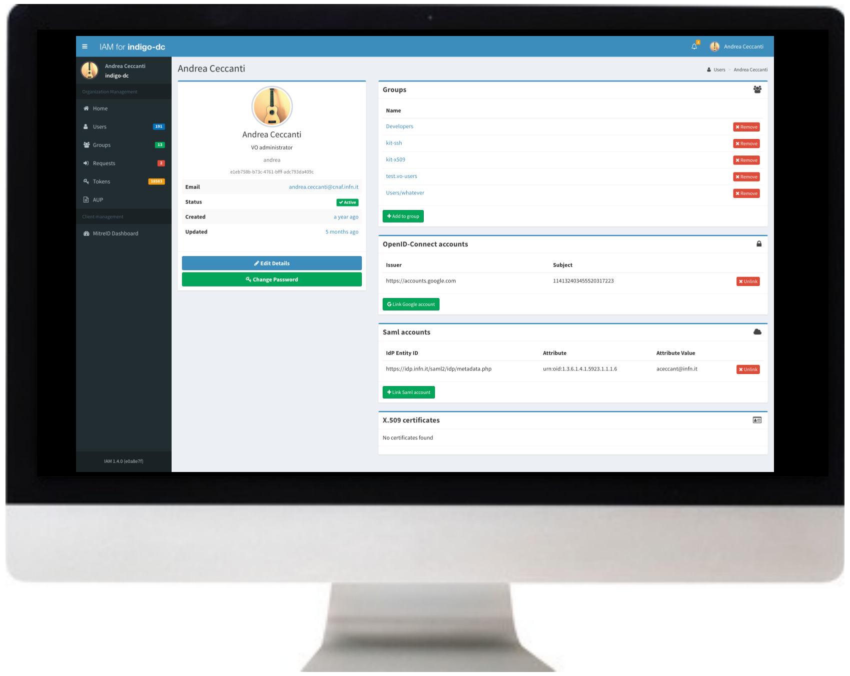
Managing a community/virtual organization

Management tools

IAM provides a **mobile-friendly** dashboard for:

- User management
- Group management
- Membership request management
- Account linking
- Token management

All management functionality is also exposed by REST APIs



Andrea Ceccanti

Andrea Ceccanti
VO administrator
andrea
e1eb758b-b73c-4761-bfff-adc793da409c

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

Groups

Name
Developers
kit-ssh
kit-x509
test.vo-users
Users/whatever

OpenID-Connect accounts

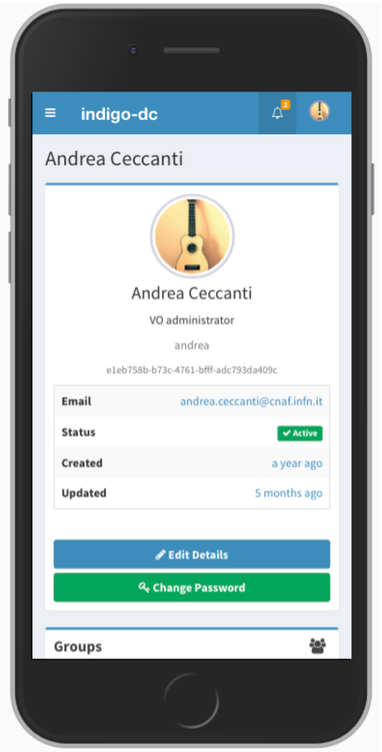
Issuer	Subject
https://accounts.google.com	114132403455520317223

Saml accounts

IdP Entity ID	Attribute	Attribute Value
https://idp.infn.it/saml2/idp/metadata.php	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	aceccant@infn.it

X.509 certificates

No certificates found



Andrea Ceccanti

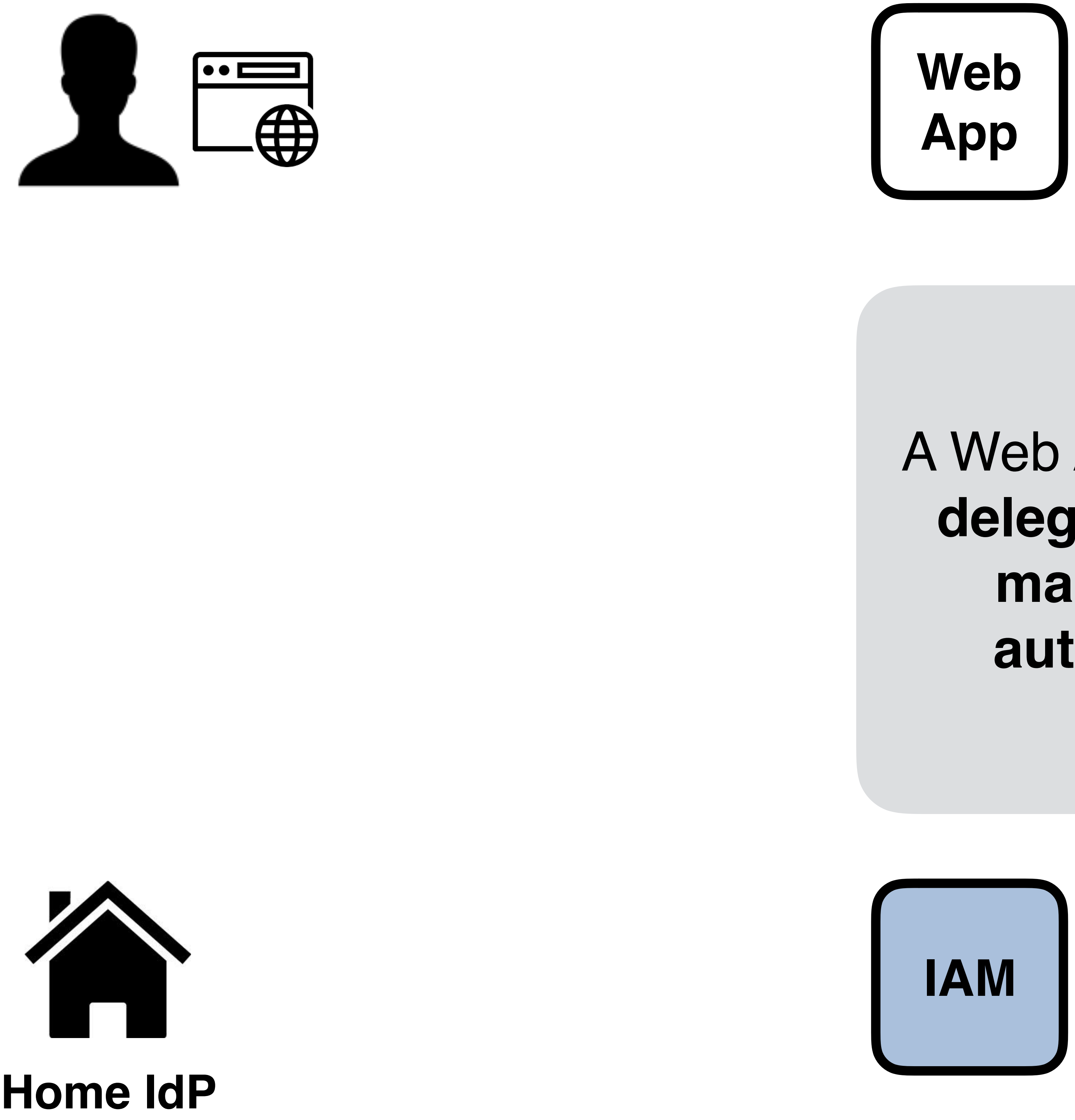
Andrea Ceccanti
VO administrator
andrea
e1eb758b-b73c-4761-bfff-adc793da409c

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

Groups

Web-based authentication flows

Web application: authorization code flow



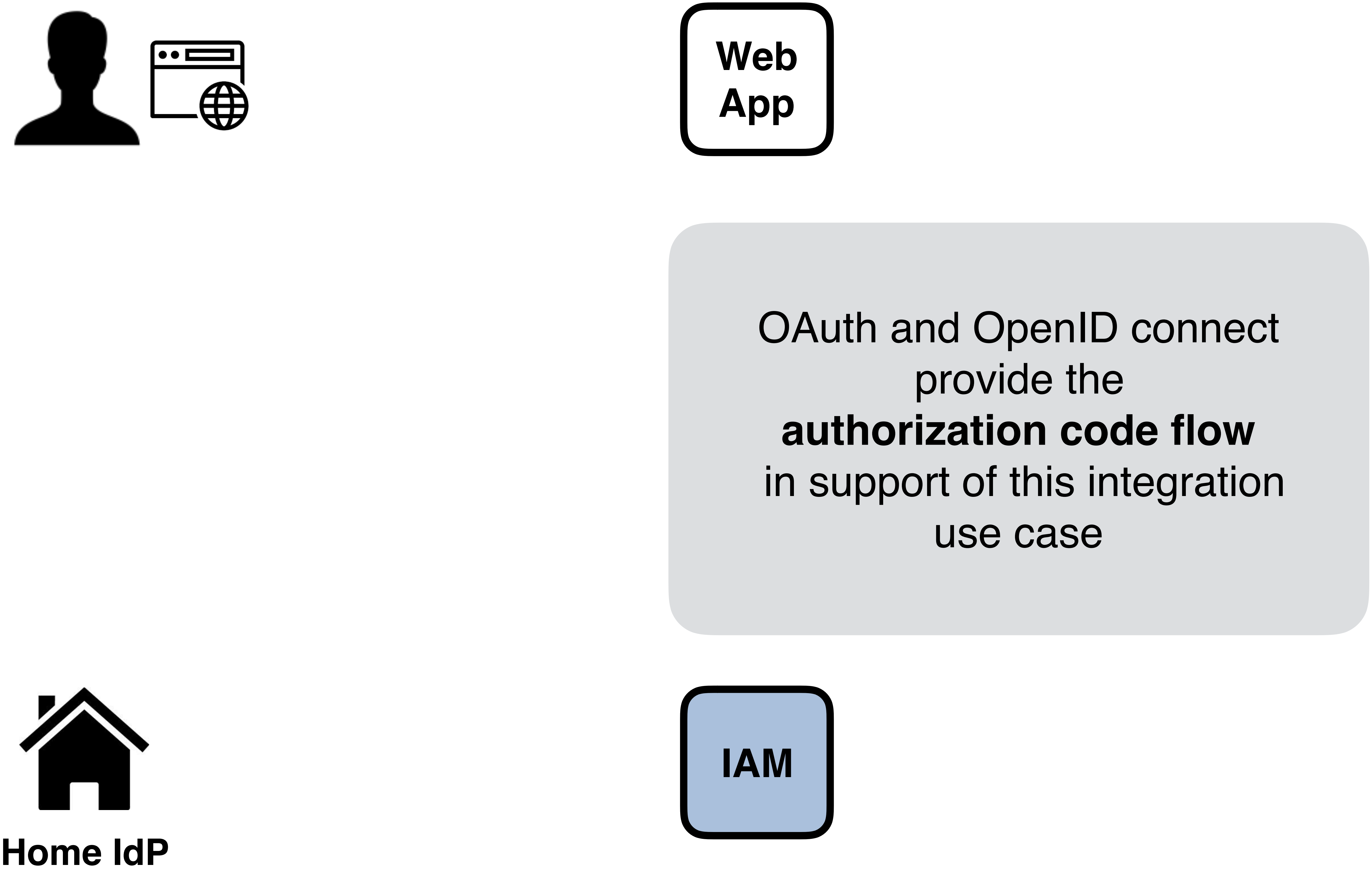
Web App

IAM

Home IdP

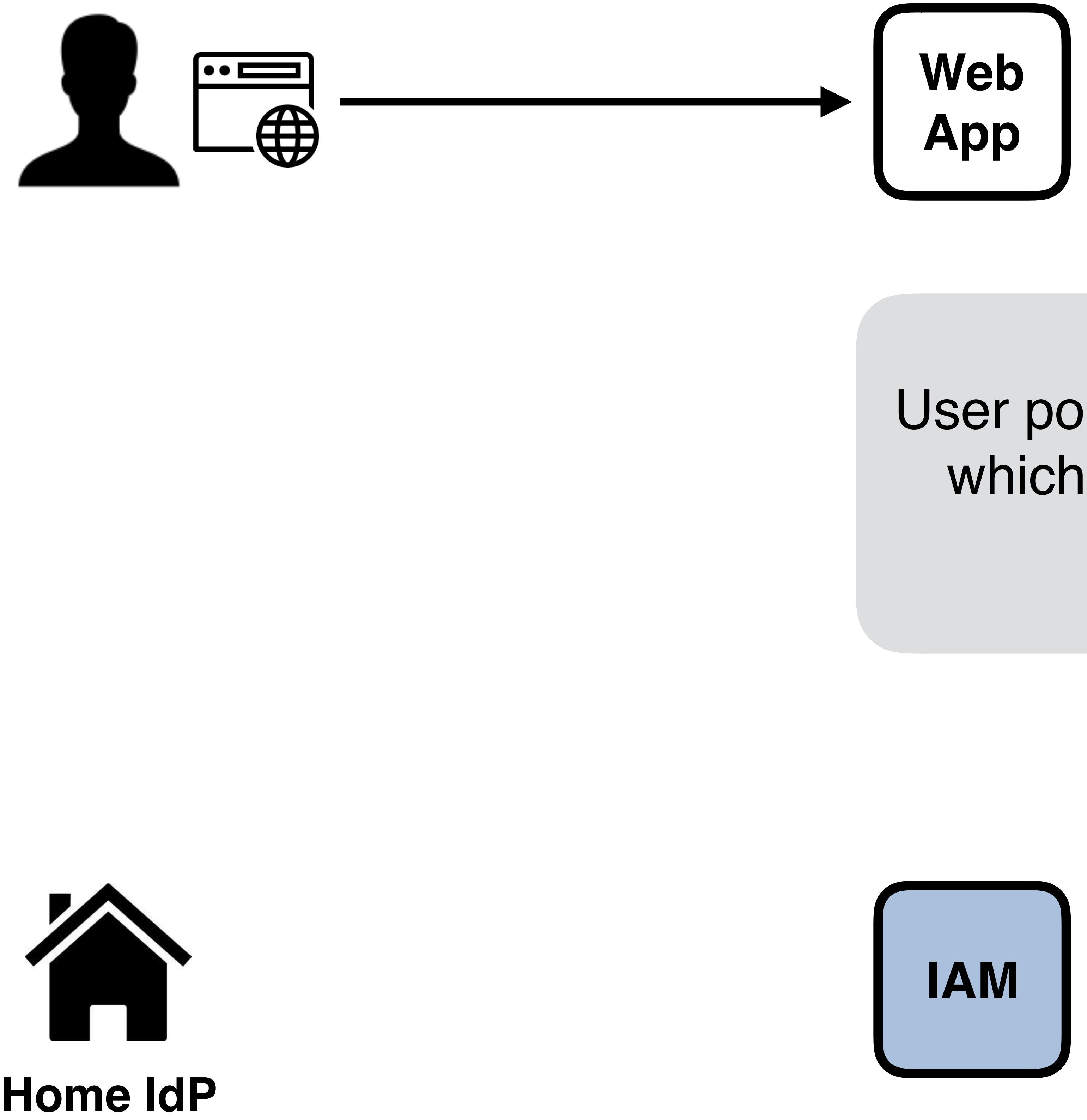
A Web App integrates with IAM to **delegate user authentication management** and **obtain authorization** information

Web application: authorization code flow



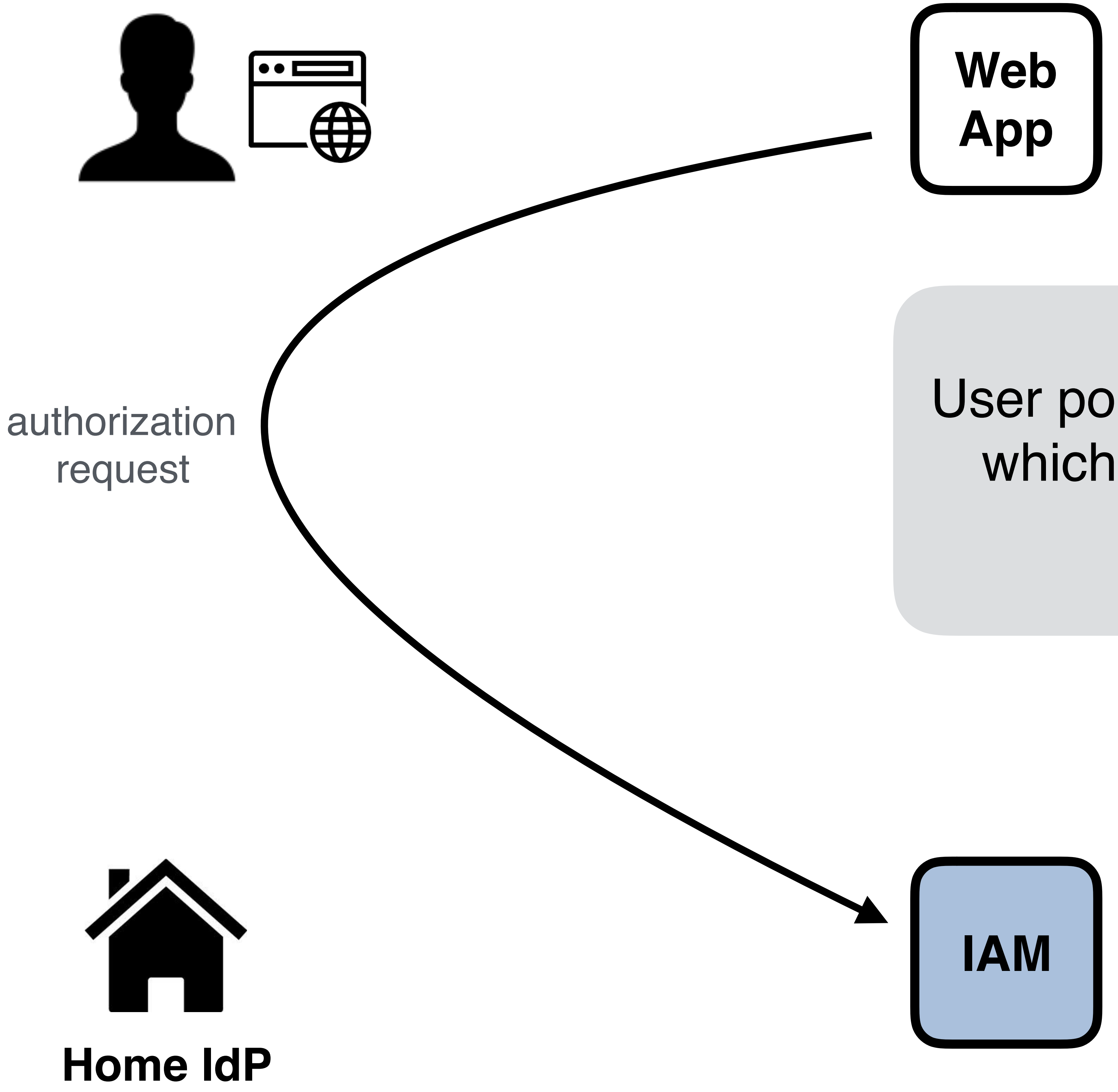
OAuth and OpenID connect provide the **authorization code flow** in support of this integration use case

Authorization code flow



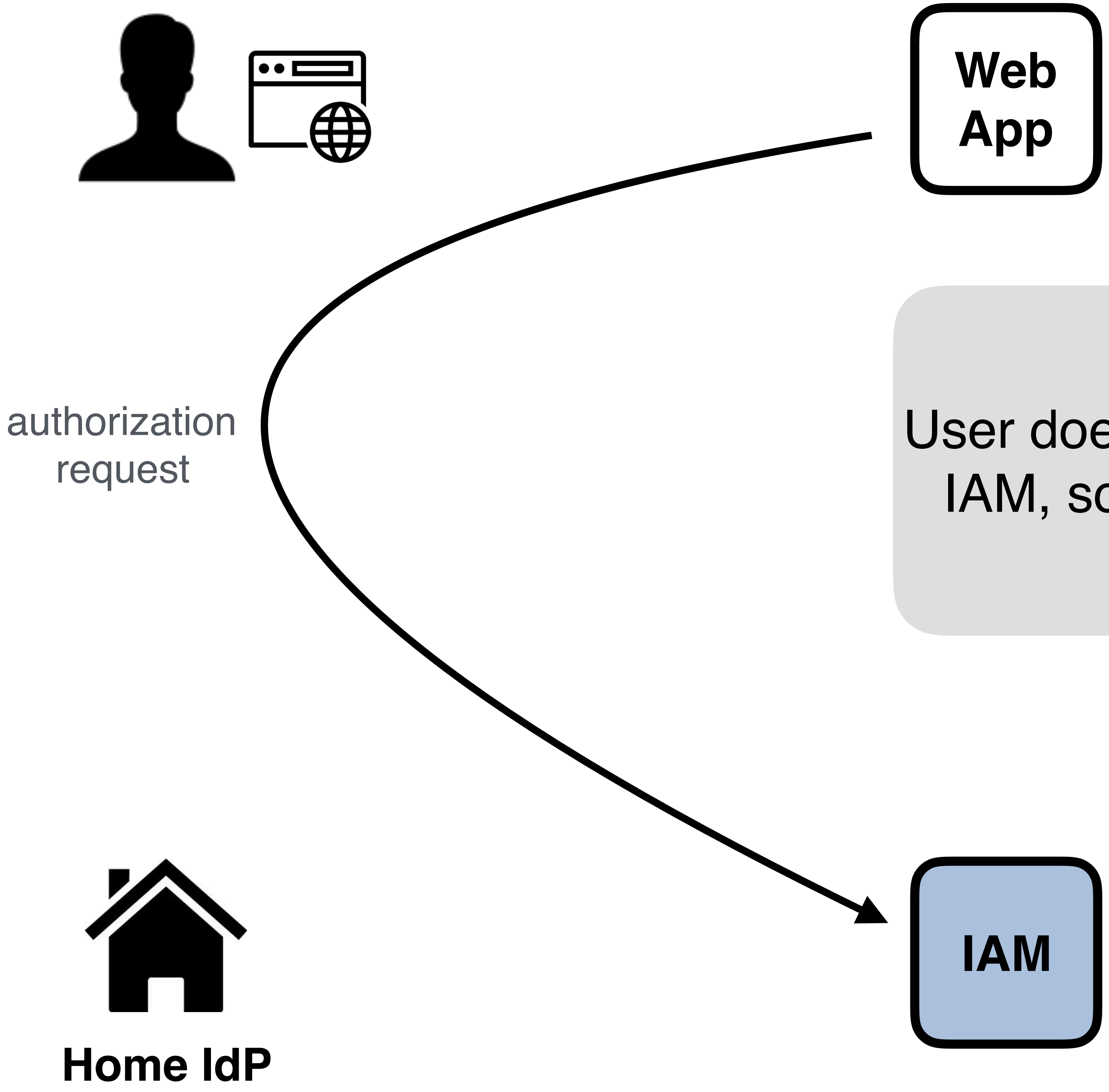
User points its browser to web app, which redirects back to IAM for authentication

Authorization code flow



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

Authorization code flow



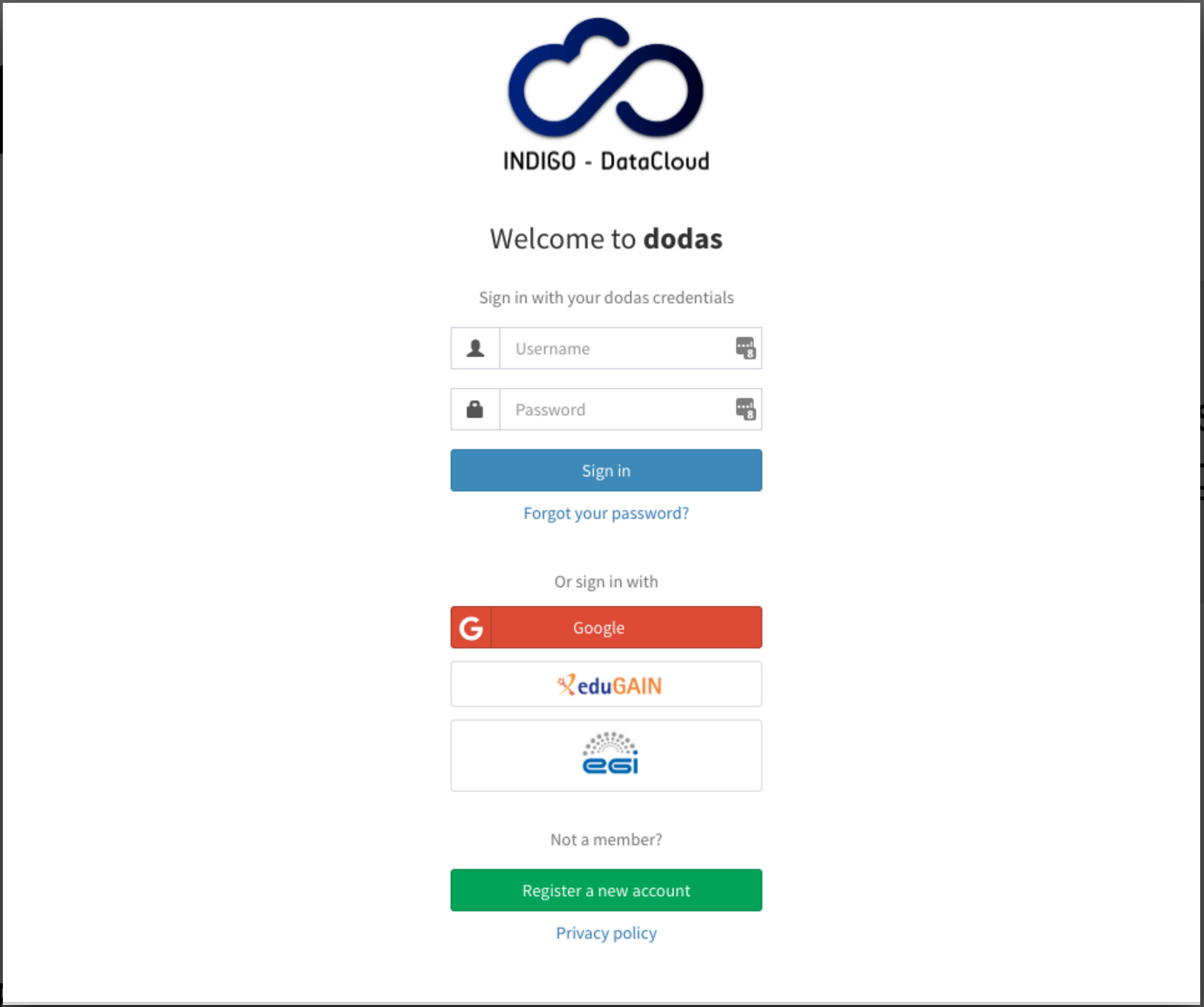
User does not have a valid session at IAM, so IAM shows the login page

Authorization code flow

authorization request

session at
gin page

Home IdP



INDIGO - DataCloud

Welcome to **dodas**

Sign in with your dodas credentials

Username

Password

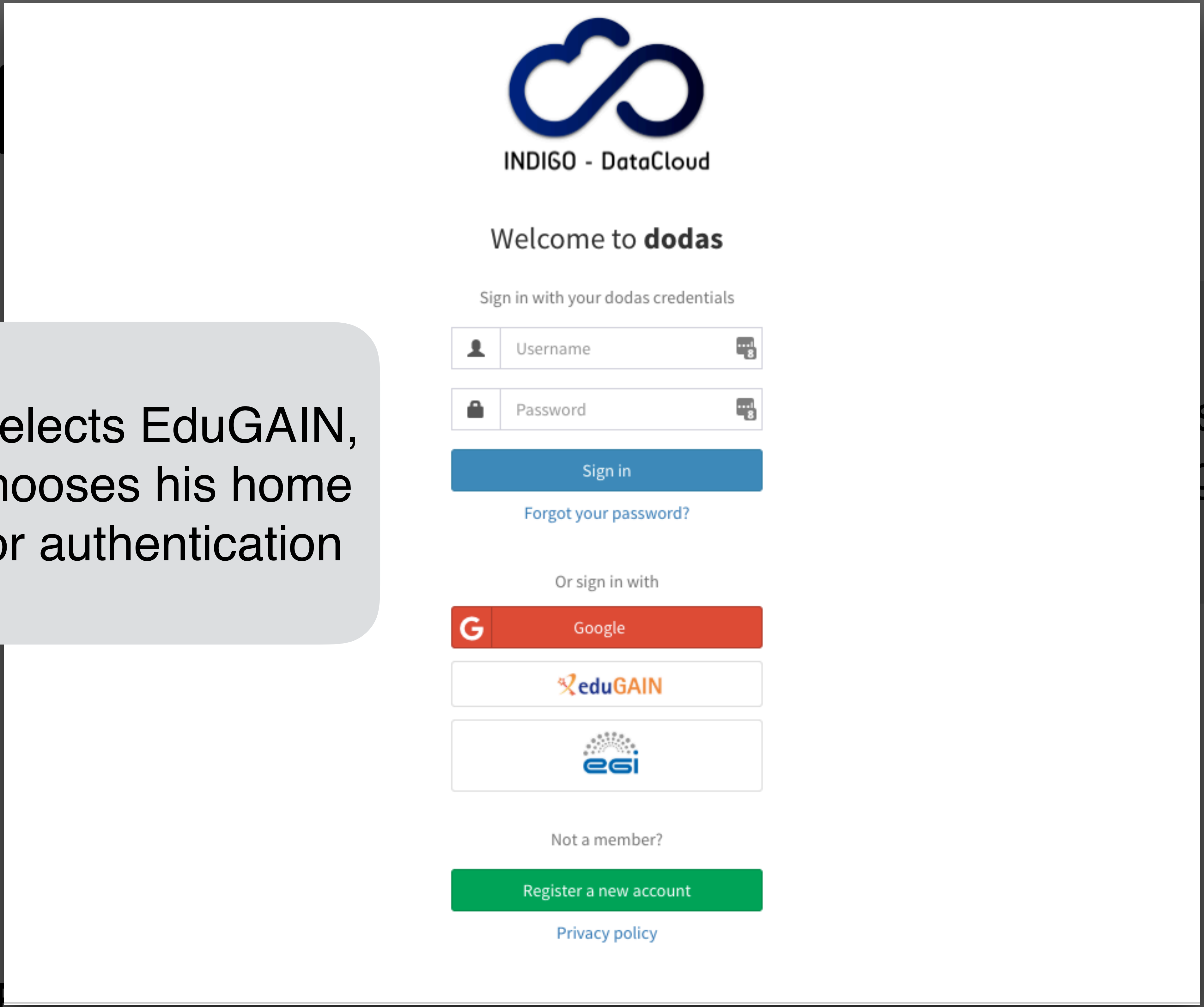
Not a member?

Authorization code flow

auth

r

User selects EduGAIN, and chooses his home IDP for authentication



INDIGO - DataCloud

Welcome to **dodas**

Sign in with your dodas credentials

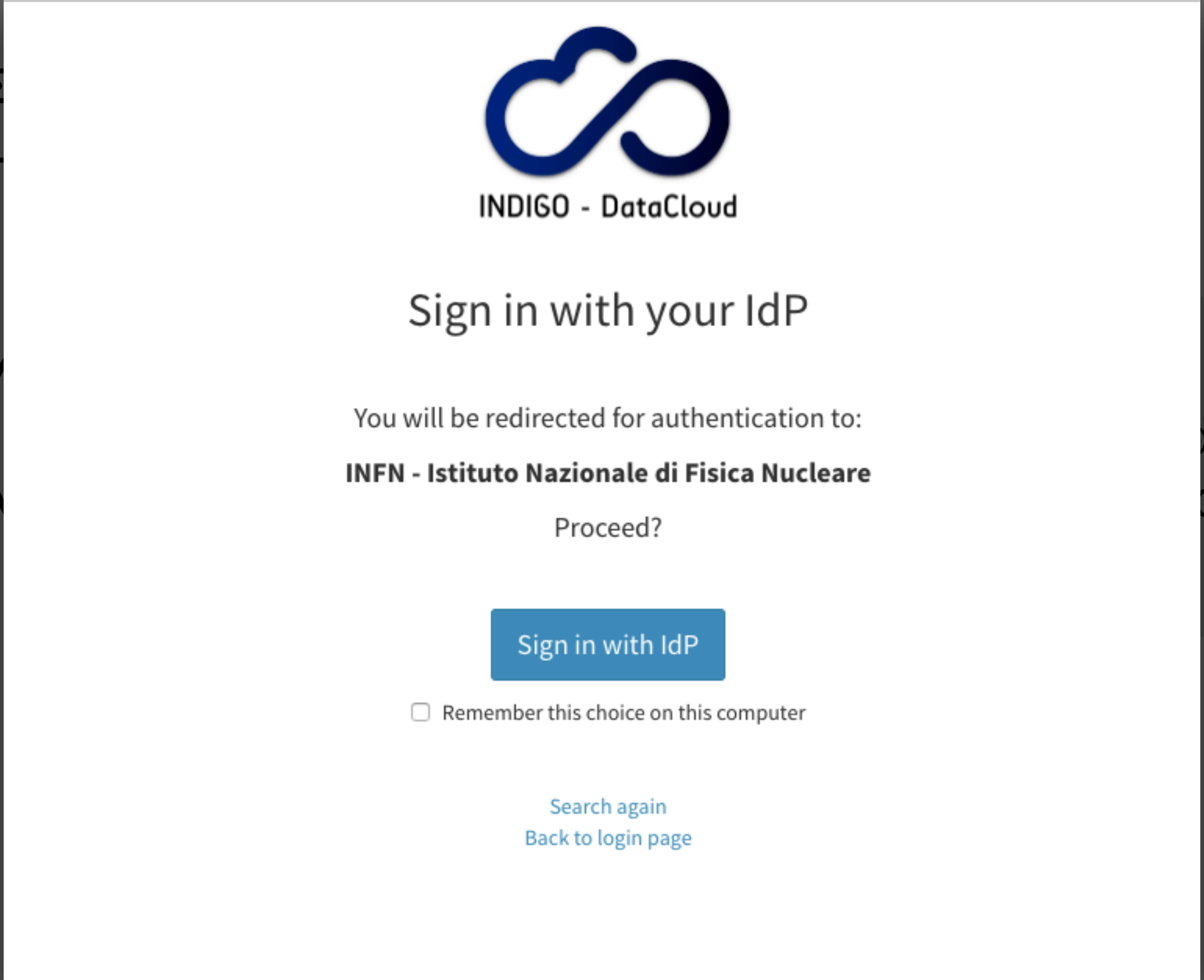
session at

gin page

Home Idl

Authorization code flow

authorization
request



INDIGO - DataCloud

Sign in with your IdP

You will be redirected for authentication to:

INFN - Istituto Nazionale di Fisica Nucleare

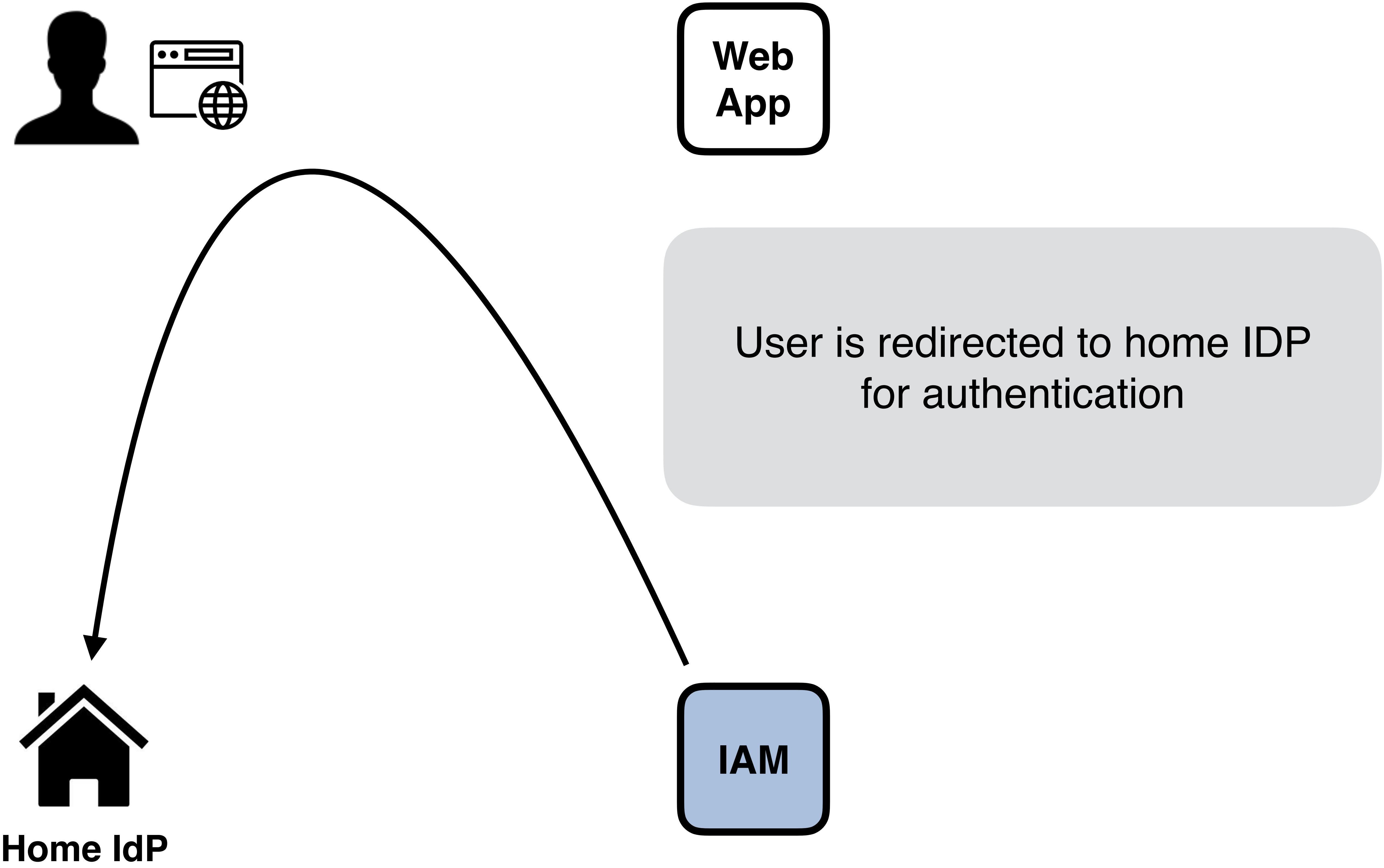
Proceed?

□ Remember this choice on this computer

d session at
ogin page

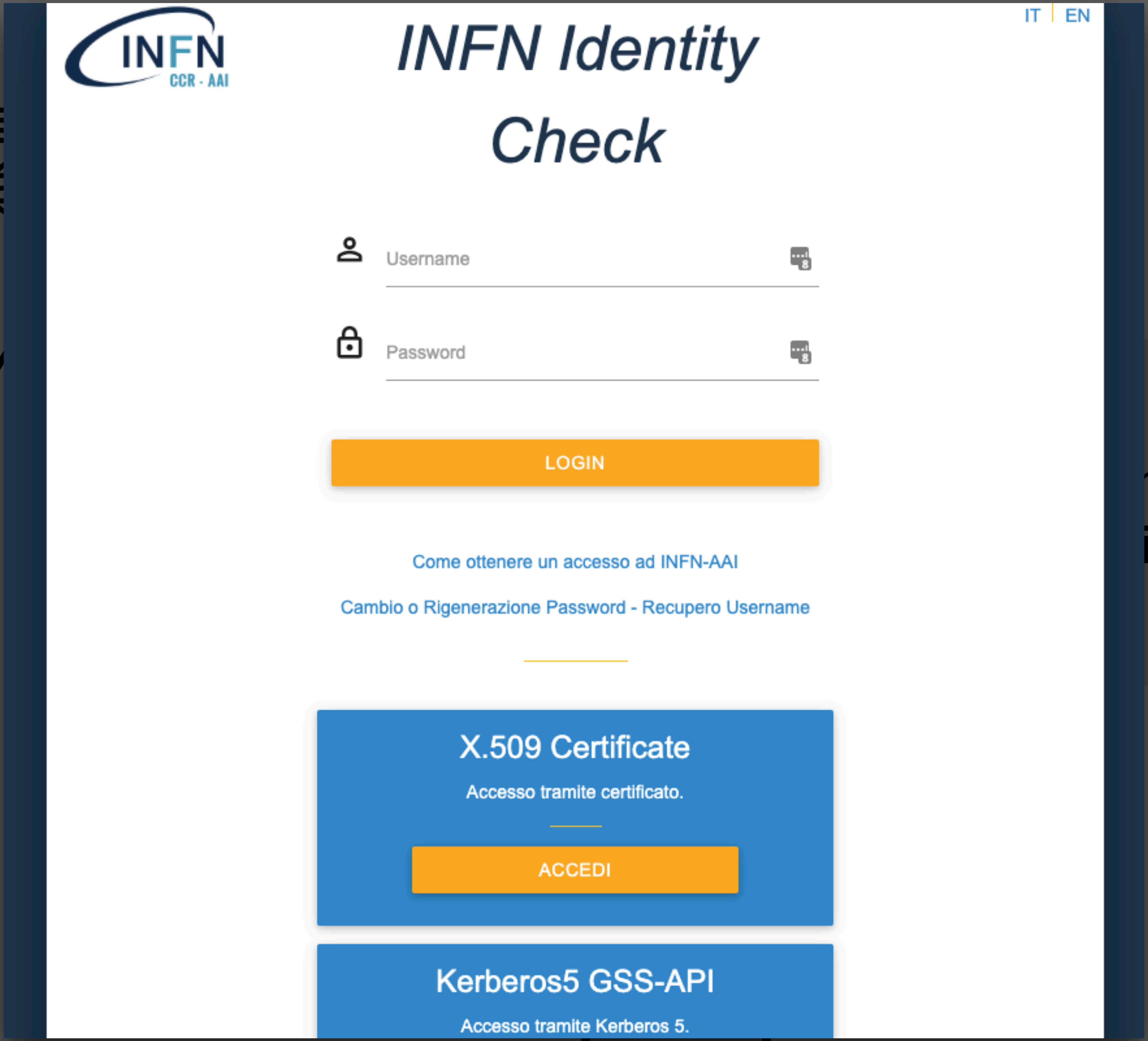
Home IdP

Authorization code flow



User is redirected to home IDP for authentication

Authorization code flow



INFN Identity Check

Come ottenere un accesso ad INFN-AAI

Cambio o Rigenerazione Password - Recupero Username

X.509 Certificate

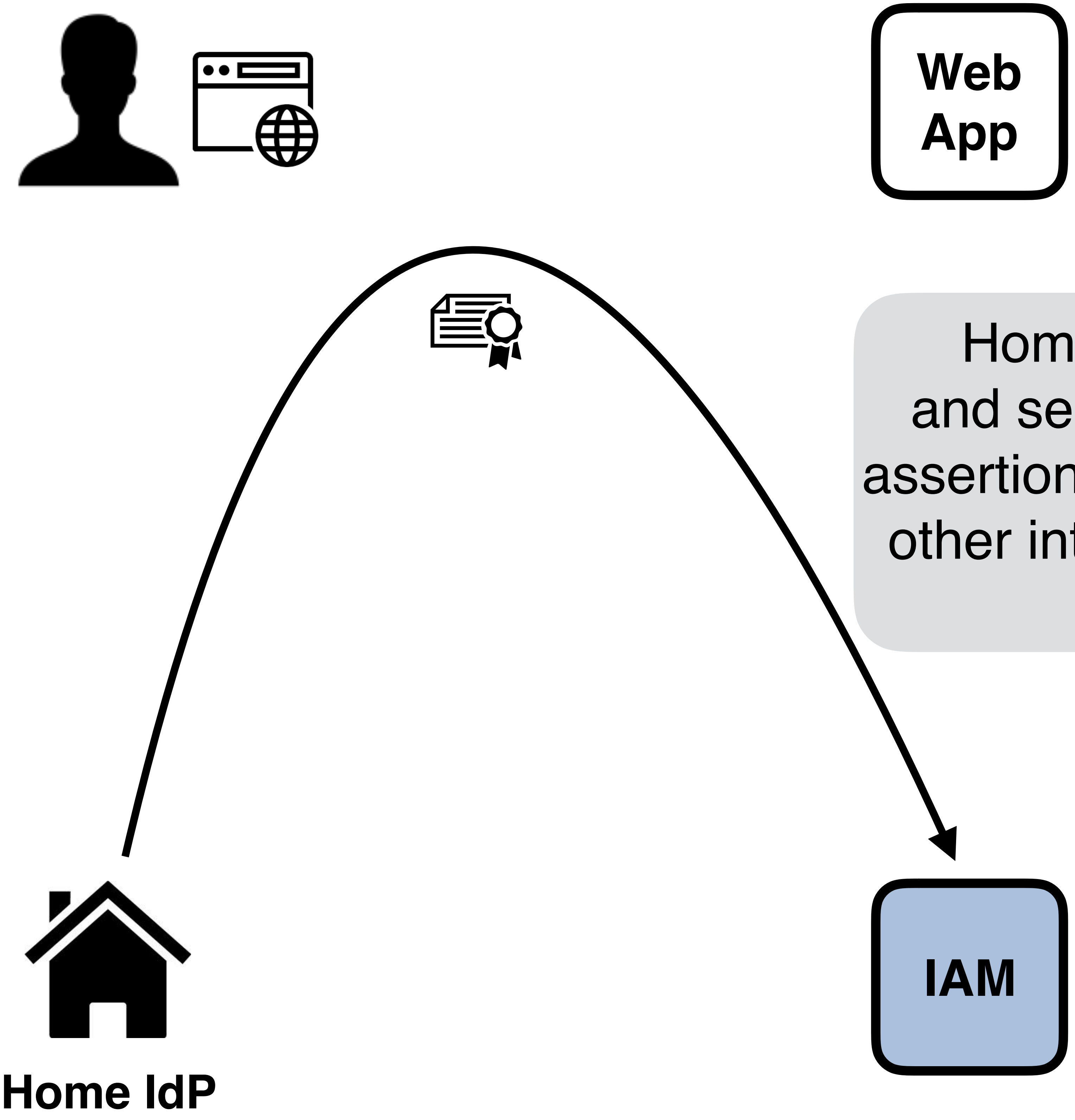
Accesso tramite certificato.

Kerberos5 GSS-API

Accesso tramite Kerberos 5.

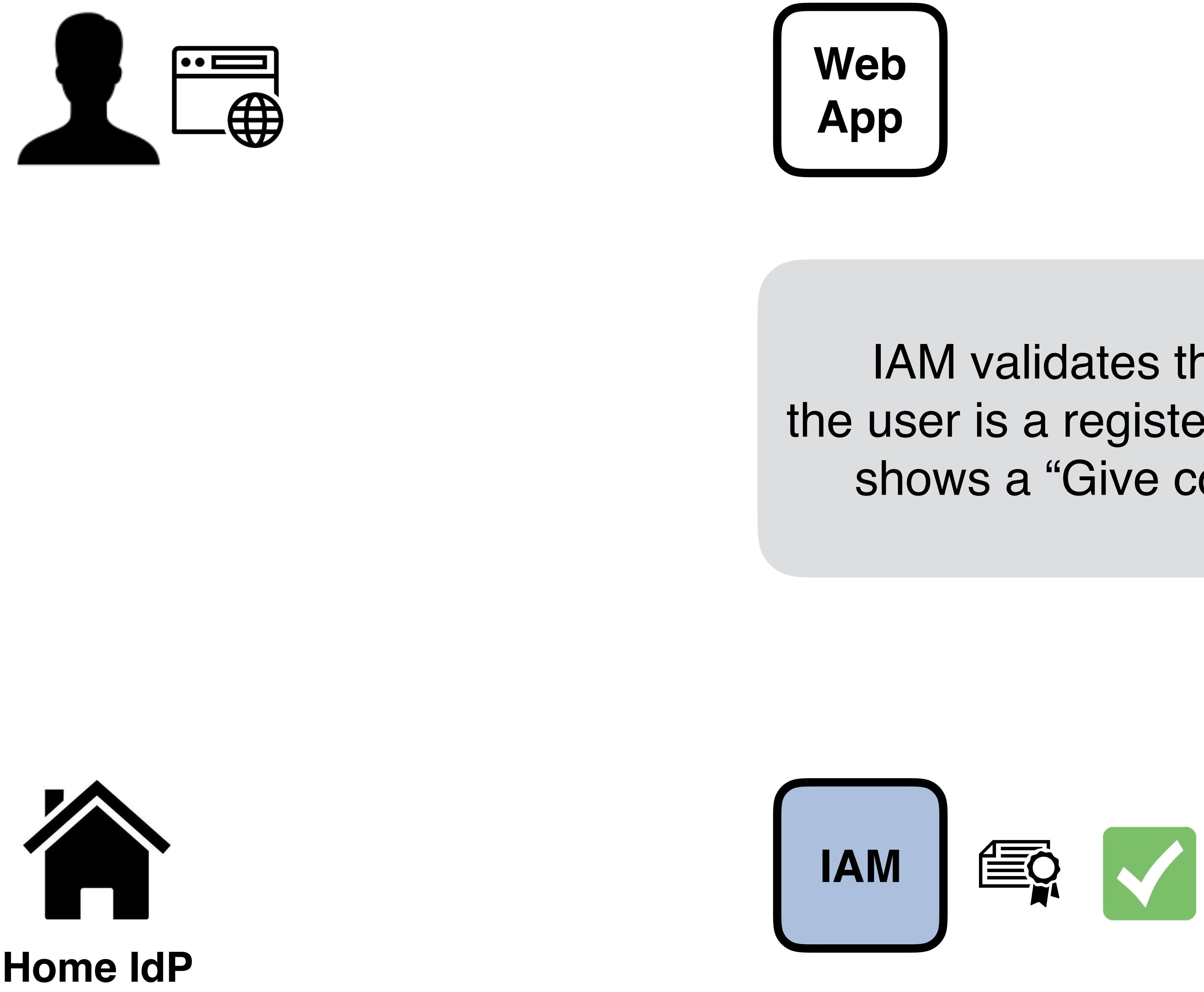
home IDP
ion

Authorization code flow



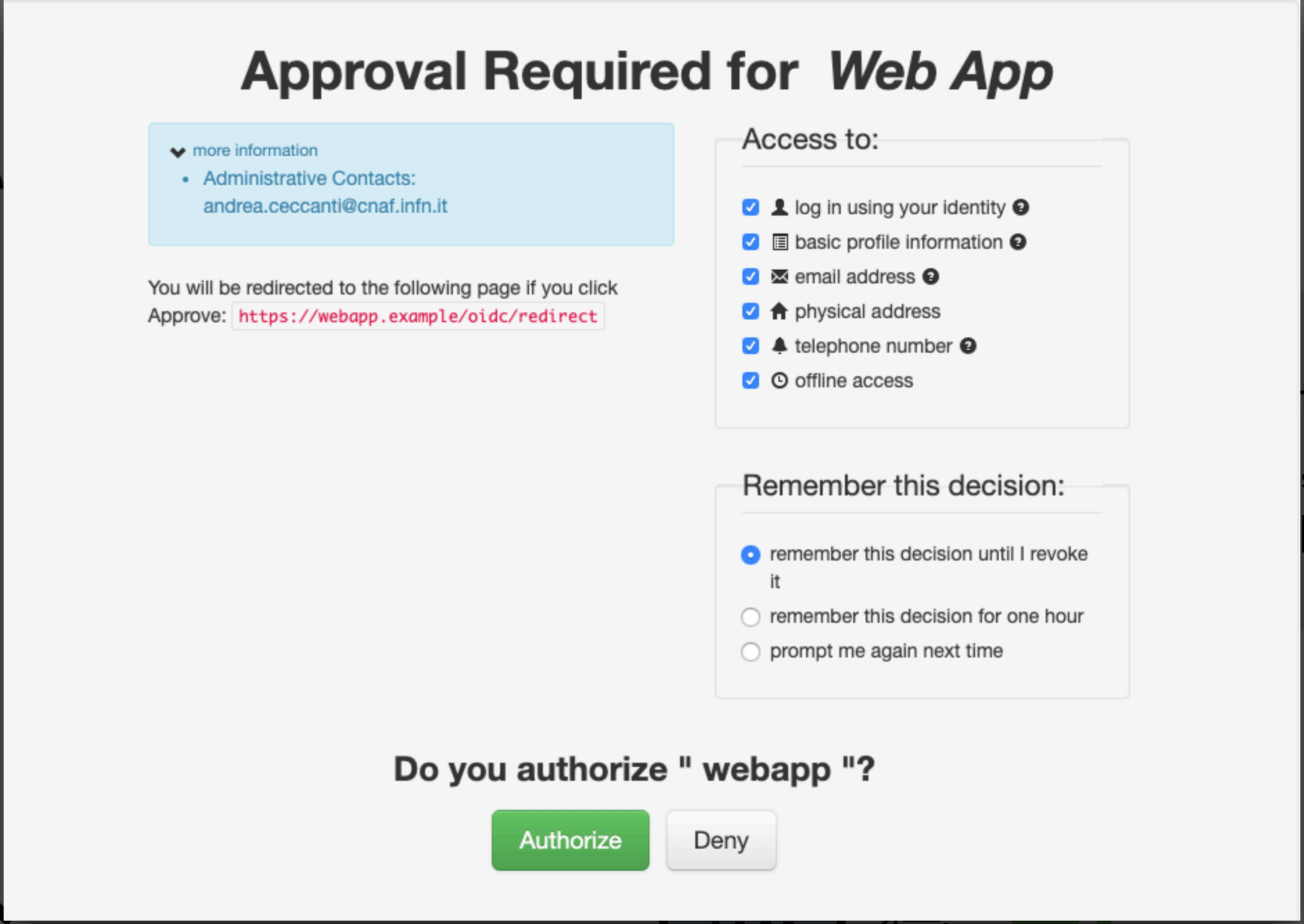
Home IDP authenticates user and sends back an authentication assertion, via redirection and possibly other interactions between IAM and the IDP

Authorization code flow



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

Authorization code flow



Approval Required for *Web App*

- more information
  - Administrative Contacts: andrea.ceccanti@cnaf.infn.it

You will be redirected to the following page if you click Approve: `https://webapp.example/oidc/redirect`

Access to:

- ☑ log in using your identity
- ☑ basic profile information
- ☑ email address
- ☑ physical address
- ☑ telephone number
- ☑ offline access

Remember this decision:

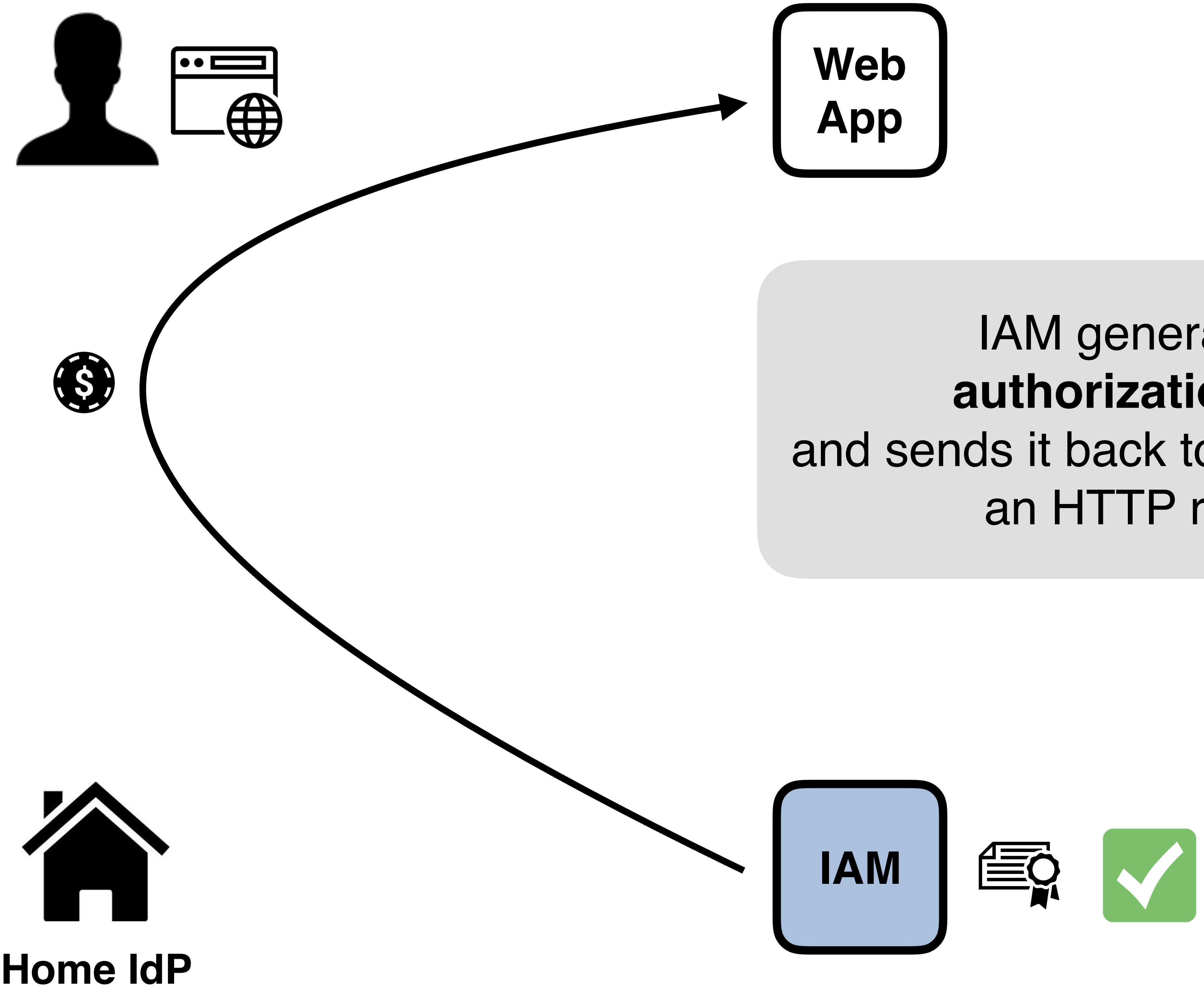
- ● remember this decision until I revoke it
- ○ remember this decision for one hour
- ○ prompt me again next time

Do you authorize " webapp "?

tion,
, so IAM
page

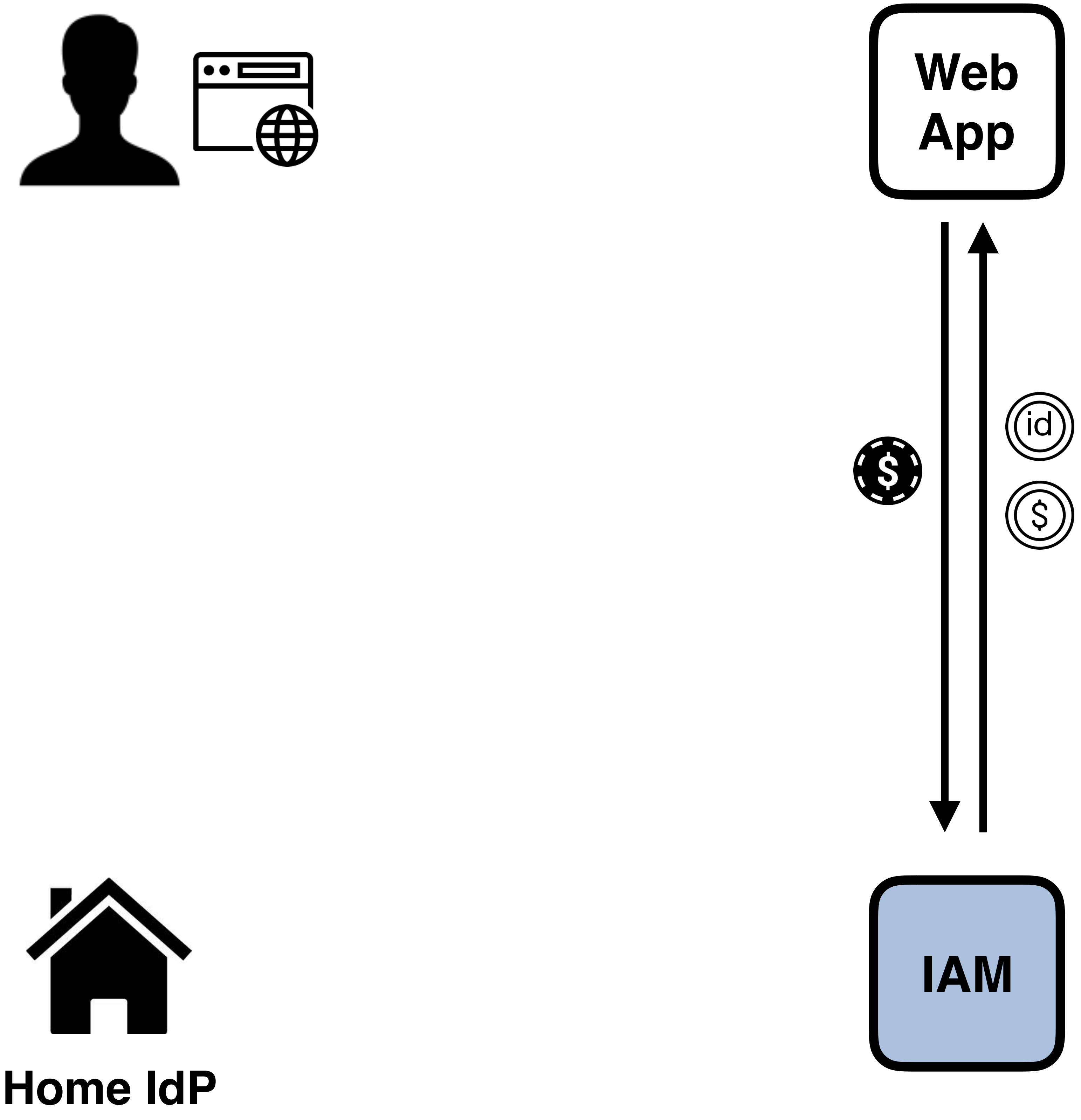
Home IdP

Authorization code flow



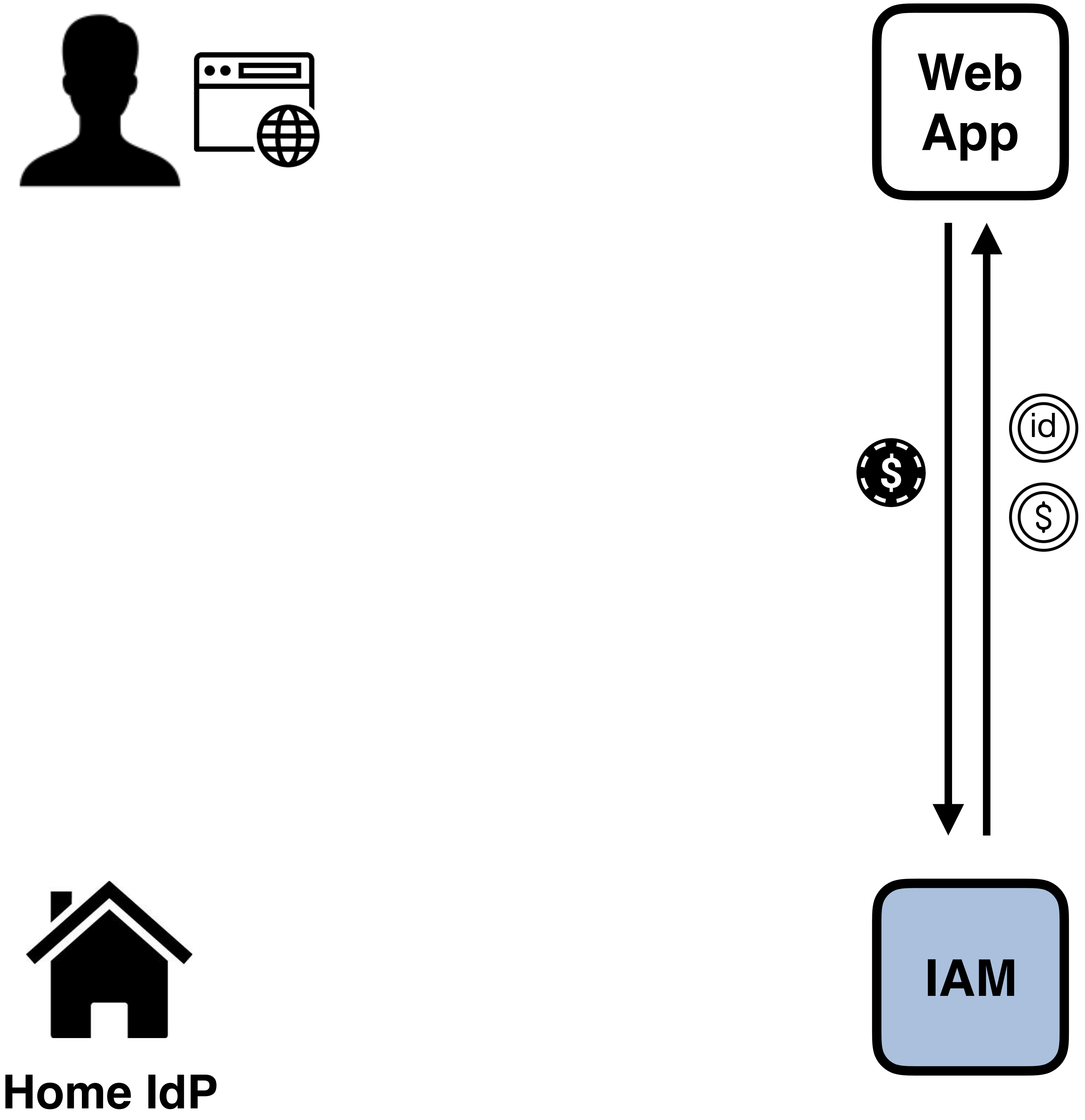
IAM generates an
authorization code
and sends it back to web app using
an HTTP redirect

Authorization code flow



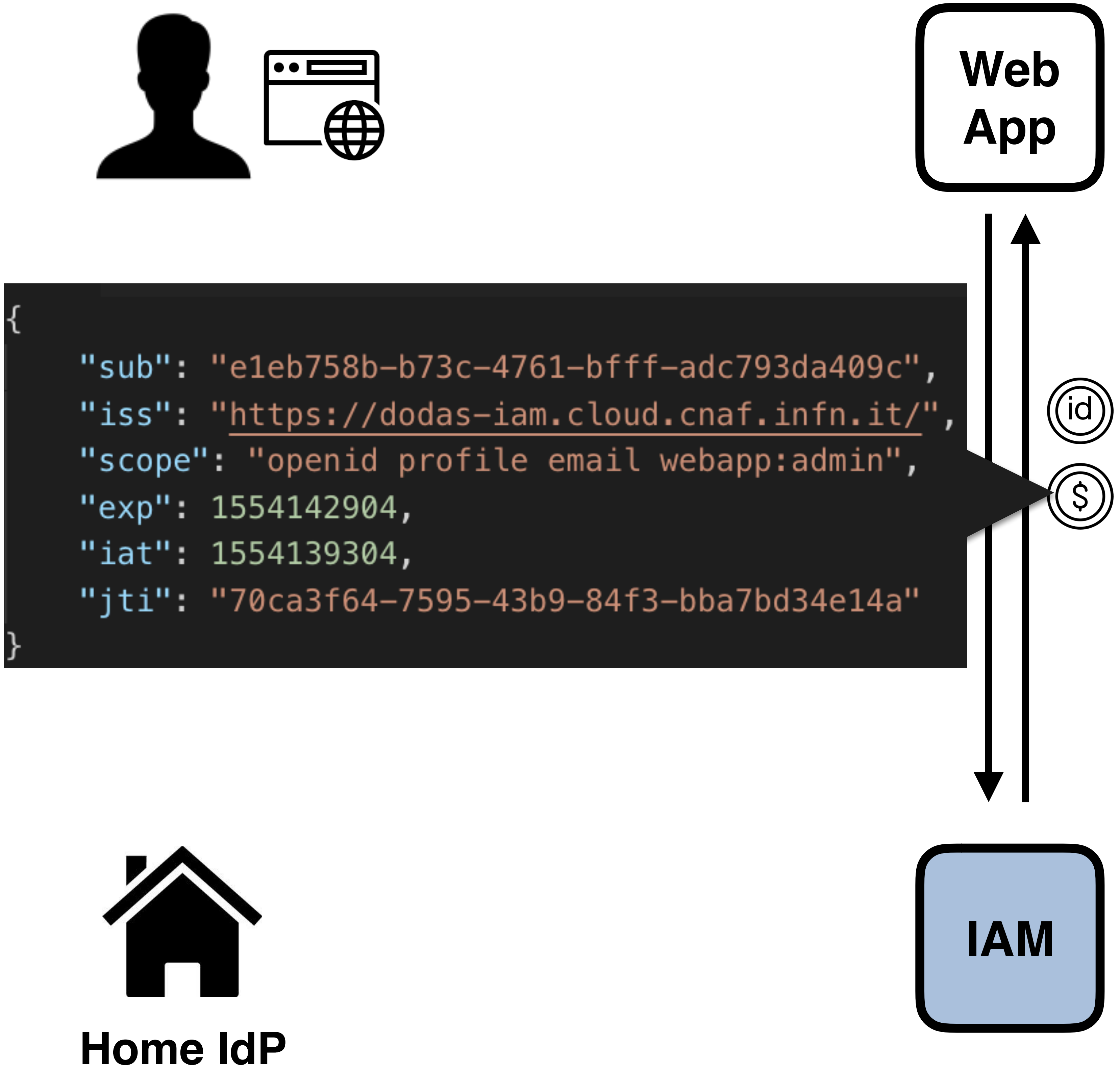
The Web App exchanges the **authorization code** with a couple of tokens:
an **access token** and an **id token**

Authorization code flow



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

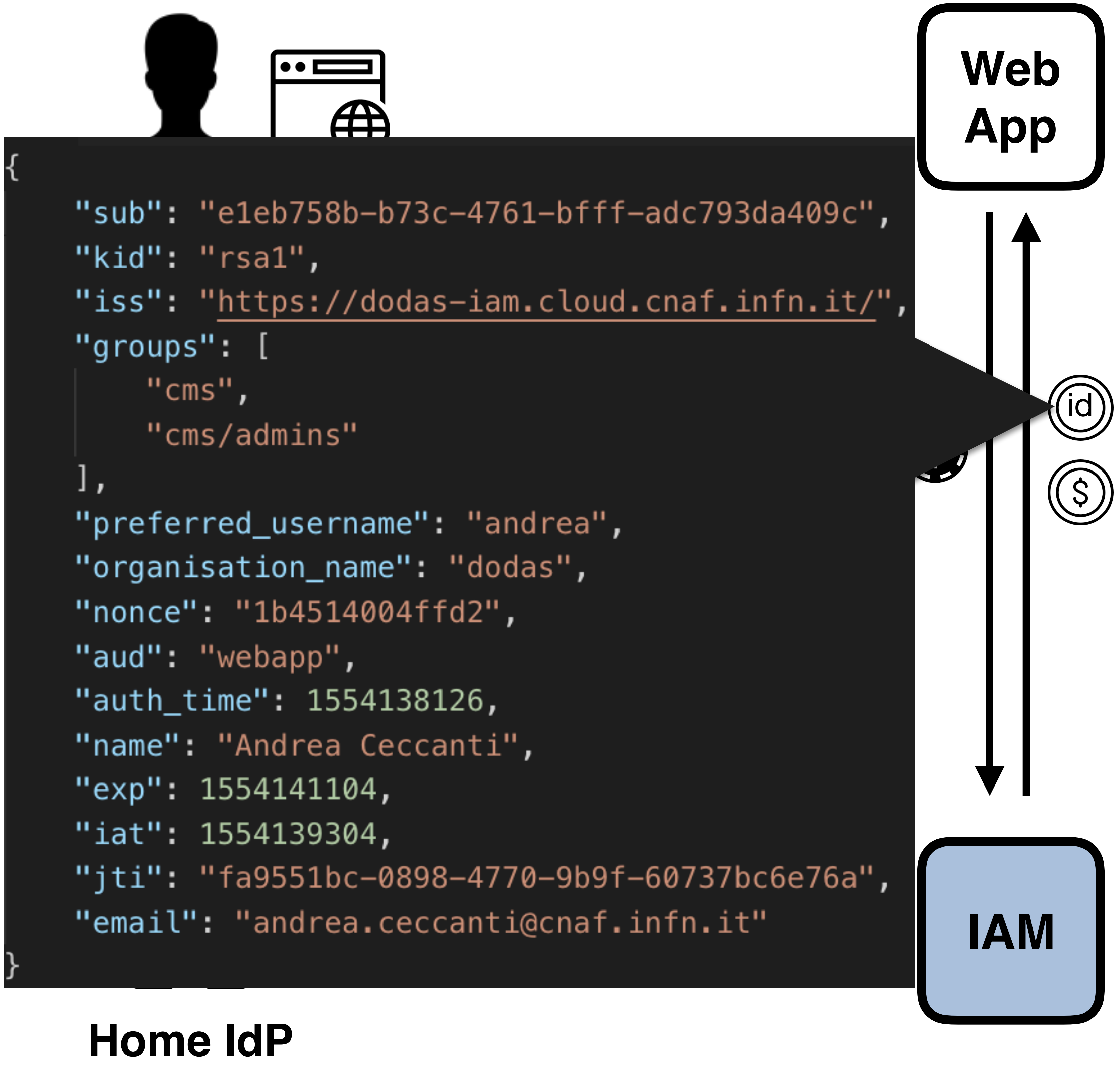
Authorization code flow



```
{
    "sub": "e1eb758b-b73c-4761-bfff-adc793da409c",
    "iss": "https://dodas-iam.cloud.cnaf.infn.it/",
    "scope": "openid profile email webapp:admin",
    "exp": 1554142904,
    "iat": 1554139304,
    "jti": "70ca3f64-7595-43b9-84f3-bba7bd34e14a"
}
```

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

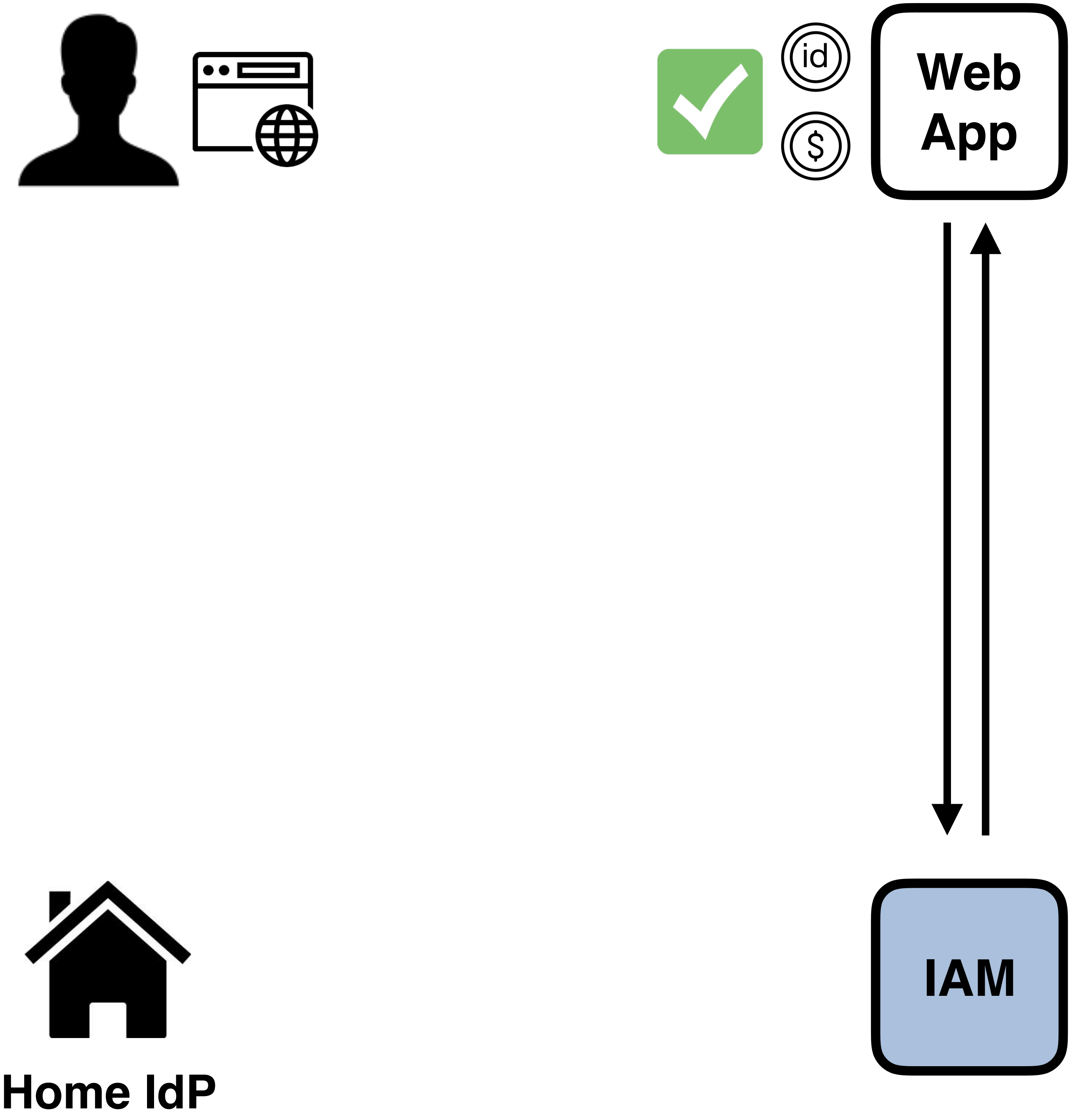
Authorization code flow



```
{
    "sub": "e1eb758b-b73c-4761-bfff-adc793da409c",
    "kid": "rsa1",
    "iss": "https://dodas-iam.cloud.cnaf.infn.it/",
    "groups": [
        "cms",
        "cms/admins"
    ],
    "preferred_username": "andrea",
    "organisation_name": "dodas",
    "nonce": "1b4514004ffd2",
    "aud": "webapp",
    "auth_time": 1554138126,
    "name": "Andrea Ceccanti",
    "exp": 1554141104,
    "iat": 1554139304,
    "jti": "fa9551bc-0898-4770-9b9f-60737bc6e76a",
    "email": "andrea.ceccanti@cnaf.infn.it"
}
```

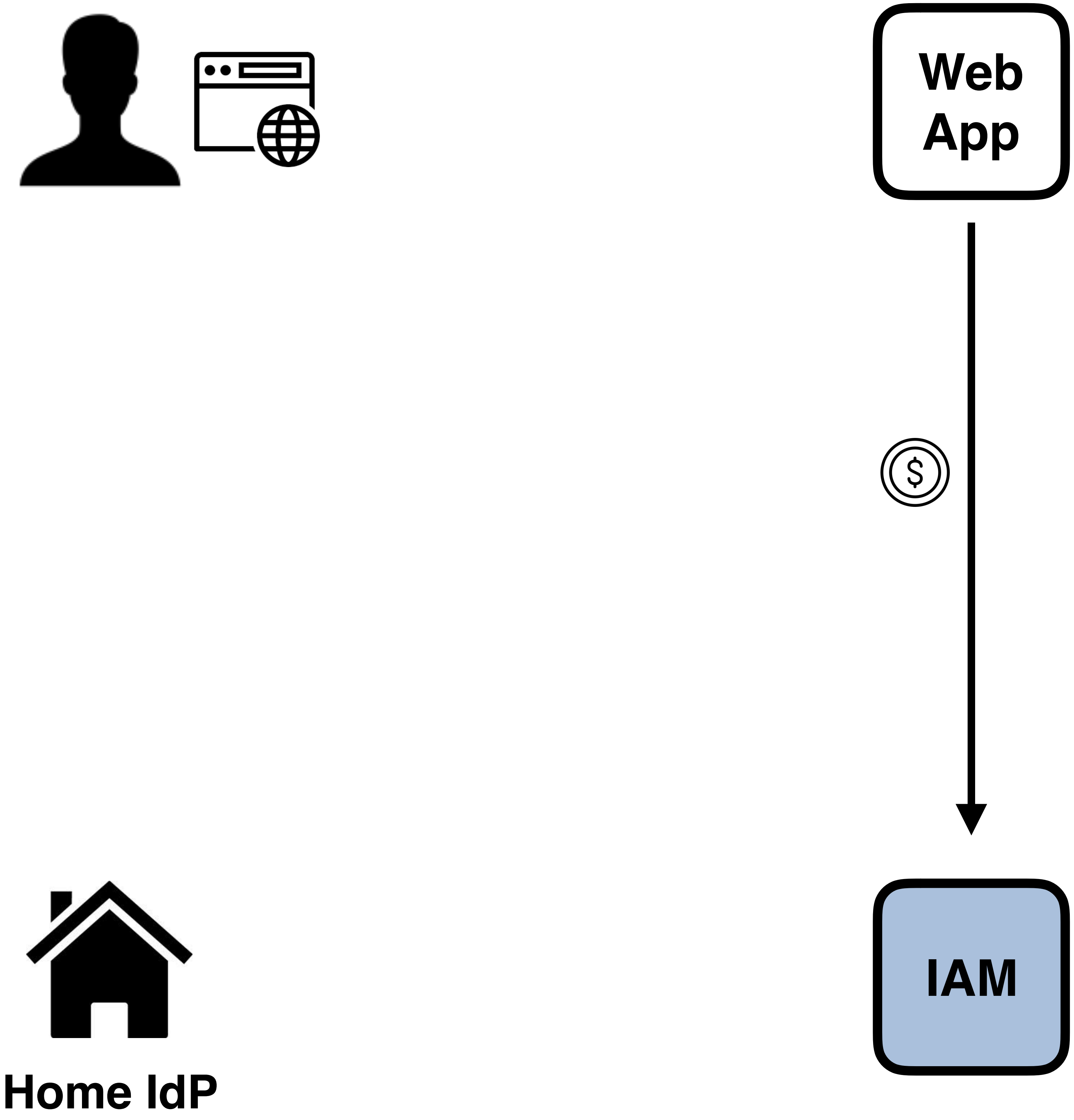
The **id token** provides (mainly) authentication information

Authorization code flow



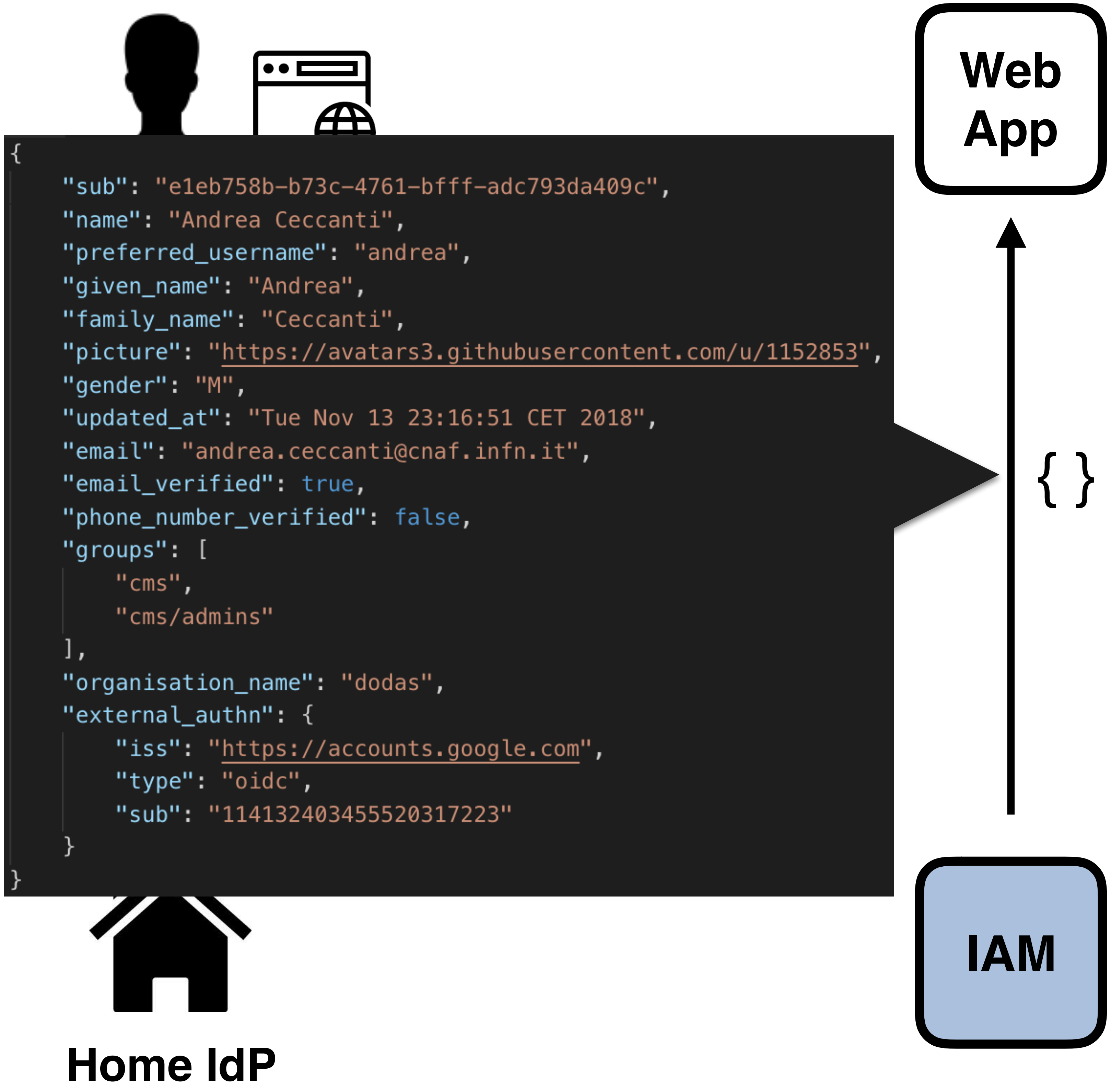
Both tokens are **validated** following to the OpenID Connect guidelines, checking **temporal validity**, **token signature**, **audience**, etc…

Authorization code flow



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

Authorization code flow



```
{
    "sub": "e1eb758b-b73c-4761-bfff-adc793da409c",
    "name": "Andrea Ceccanti",
    "preferred_username": "andrea",
    "given_name": "Andrea",
    "family_name": "Ceccanti",
    "picture": "https://avatars3.githubusercontent.com/u/1152853",
    "gender": "M",
    "updated_at": "Tue Nov 13 23:16:51 CET 2018",
    "email": "andrea.ceccanti@cnaf.infn.it",
    "email_verified": true,
    "phone_number_verified": false,
    "groups": [
        "cms",
        "cms/admins"
    ],
    "organisation_name": "dodas",
    "external_authn": {
        "iss": "https://accounts.google.com",
        "type": "oidc",
        "sub": "114132403455520317223"
    }
}
```

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

Command line authentication flow

Command-line integration scenario

Purpose:

- obtain an OAuth token from a **command-line interface (CLI)**
- use the token for authentication and authorization purposes at services

IAM supports this use case in two ways:

- via the **OAuth device code flow**
- via the **OAuth password flow**

Device code flow is the **recommended solution**

- but there are scenarios where the password flow could fit

The OAuth Device code flow

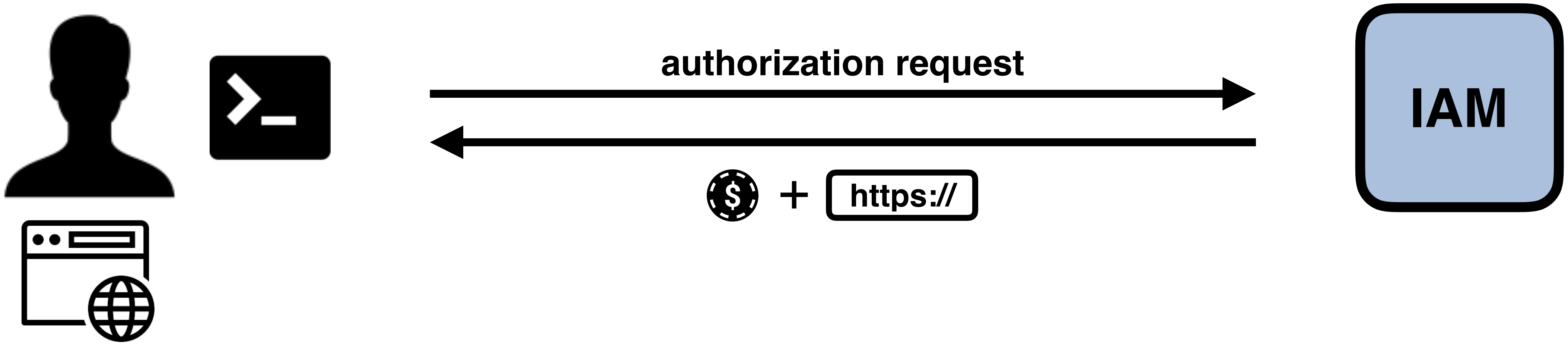
https://datatracker.ietf.org/doc/draft-ietf-oauth-device-flow/

The OAuth device code flow enables OAuth on devices that have internet connectivity but lack a browser or an easy way to enter text

In this flow, the device instructs the user to open a URL on a secondary device such as a smartphone or computer in order to complete the authorization. There is no communication channel required between the user’s two devices.

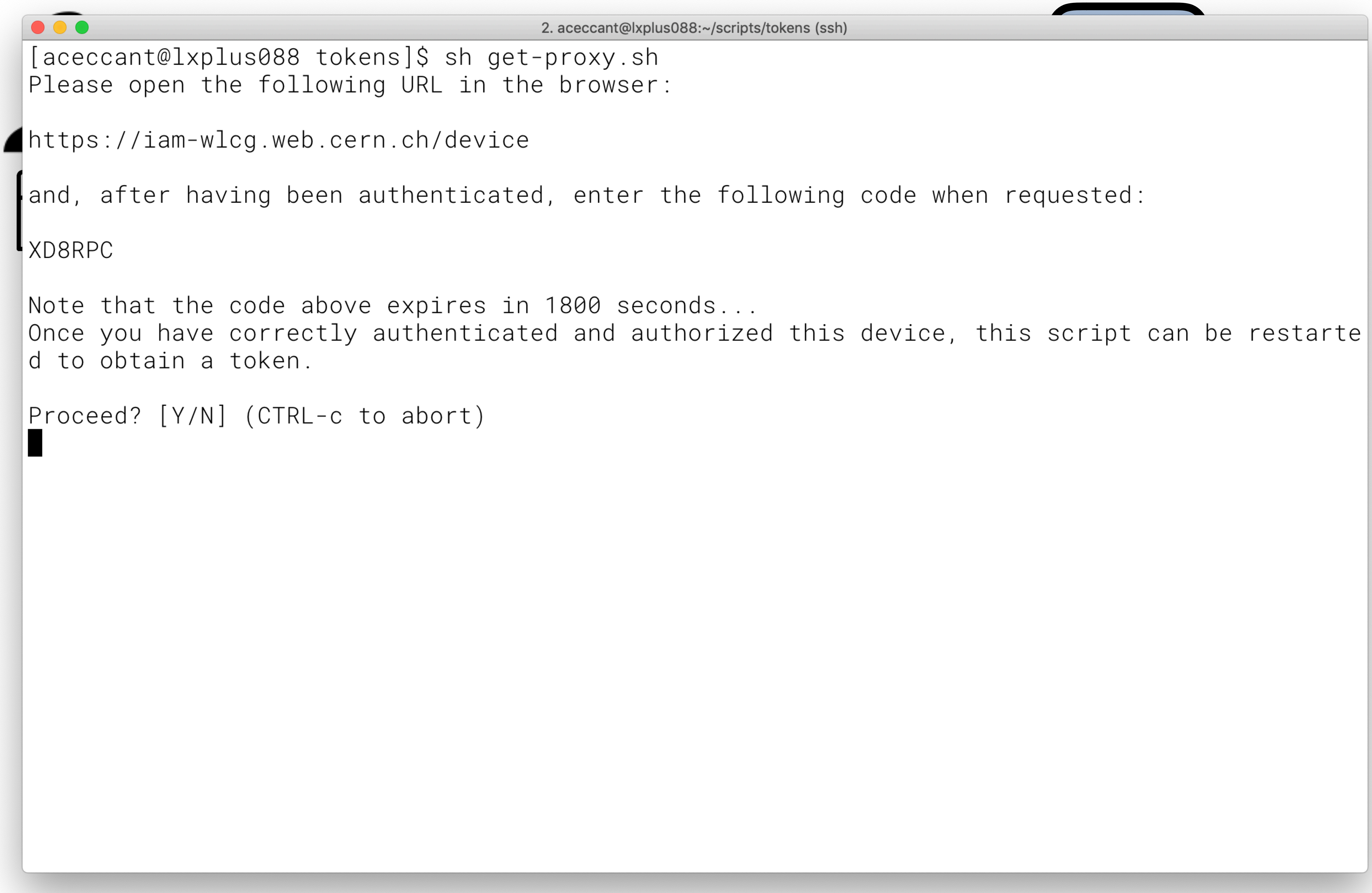
It is convenient of our CLI use cases since it enables federated authentication from a terminal (assuming the user has access to a browser, which is the case for most of our use cases)

The Device code flow



The command line client starts the flow and obtains a **URL** and a **code** from IAM

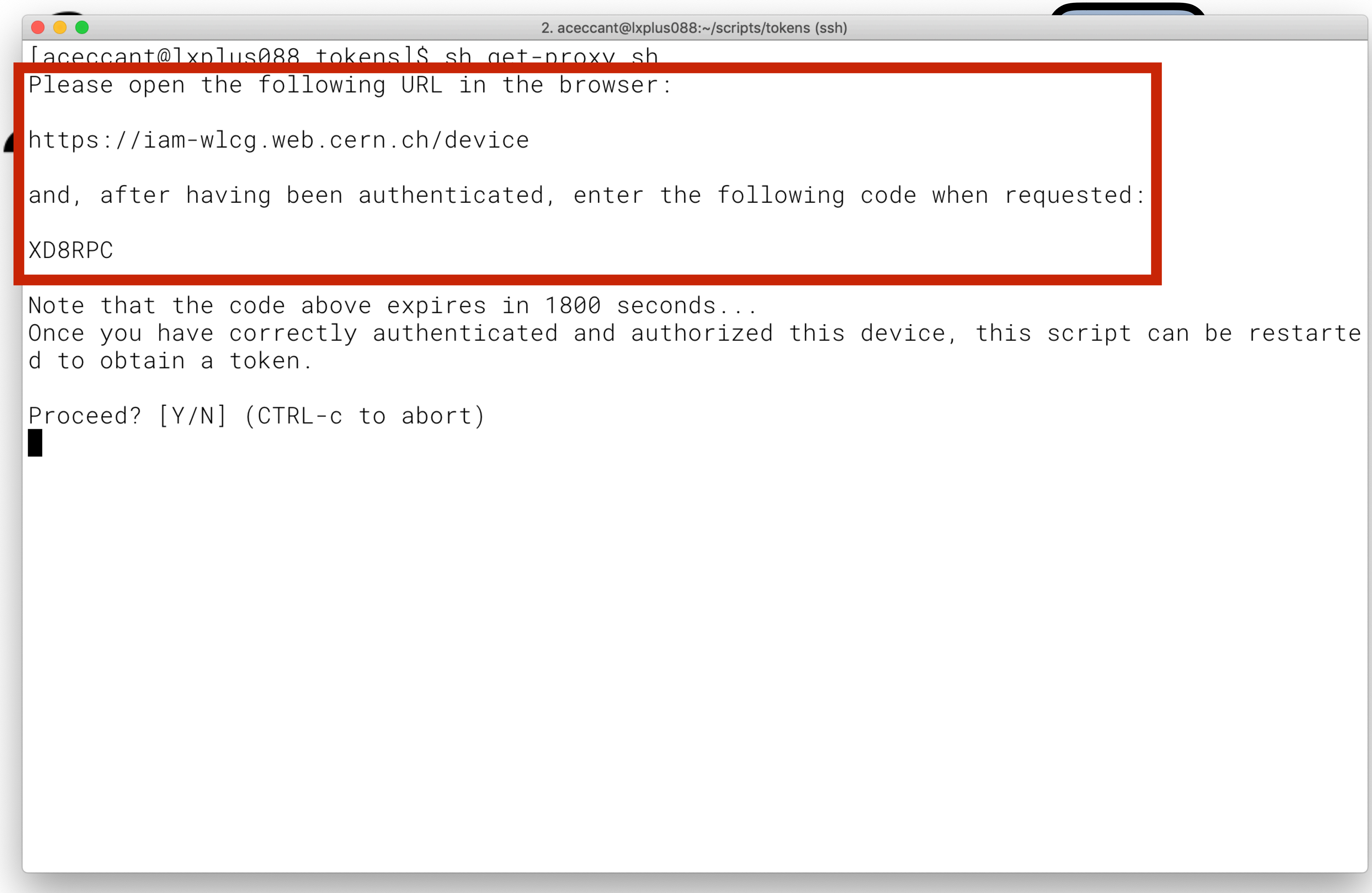
The Device code flow



2. aceccant@lxplus088:~/scripts/tokens (ssh)

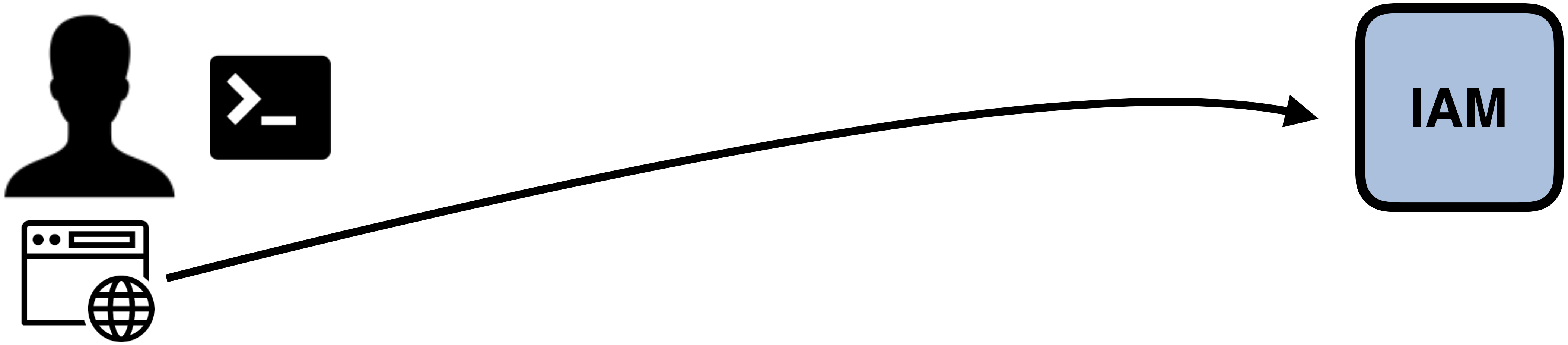
```
[aceccant@lxplus088 tokens]$ sh get-proxy.sh
Please open the following URL in the browser:

https://iam-wlcg.web.cern.ch/device

and, after having been authenticated, enter the following code when requested:

XD8RPC

Note that the code above expires in 1800 seconds...
Once you have correctly authenticated and authorized this device, this script can be restarte
d to obtain a token.

Proceed? [Y/N] (CTRL-c to abort)
```

The Device code flow



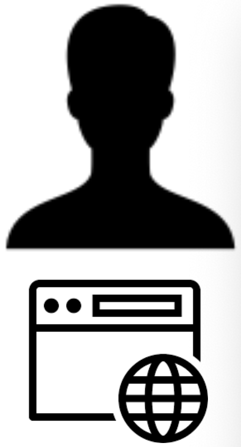
```
[aceccant@lxplus088 tokens]$ sh get-proxy.sh
Please open the following URL in the browser:

https://iam-wlcg.web.cern.ch/device

and, after having been authenticated, enter the following code when requested:

XD8RPC

Note that the code above expires in 1800 seconds...
Once you have correctly authenticated and authorized this device, this script can be restarte
d to obtain a token.

Proceed? [Y/N] (CTRL-c to abort)
█
```

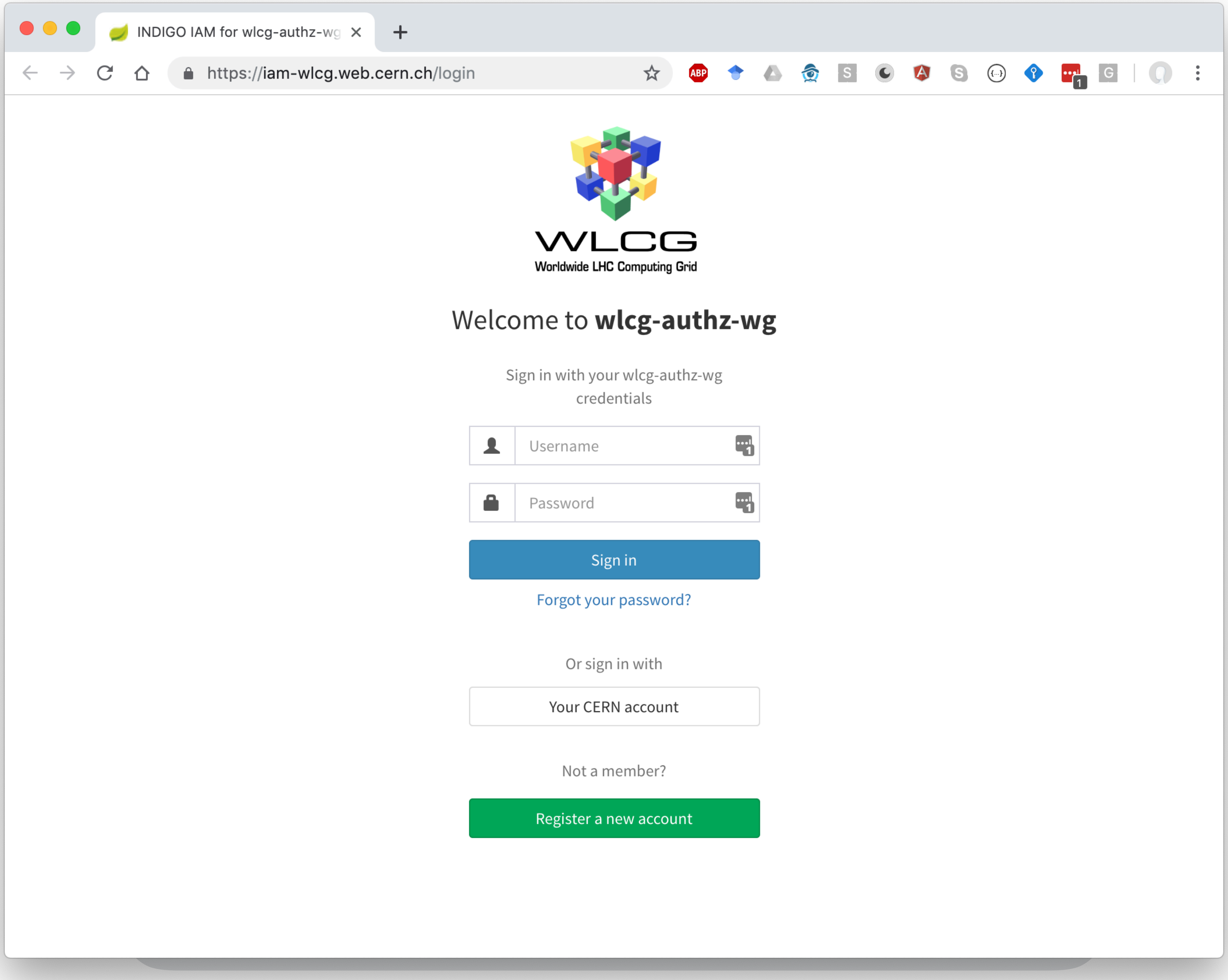
The Device code flow



The user opens the presented URL in a browser (which could run on a different device), authenticates as usual, and is later asked to enter the **code** obtained in the previous step

The Device code flow





INDIGO IAM for wlcg-authz-wg

https://iam-wlcg.web.cern.ch/login

WLCG

Worldwide LHC Computing Grid

Welcome to **wlcg-authz-wg**

Sign in with your wlcg-authz-wg credentials

Username

Password

Sign in

Forgot your password?

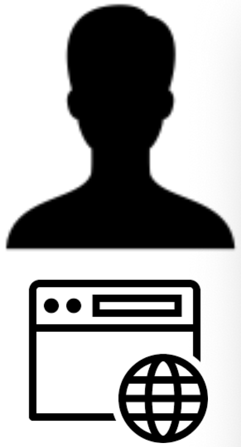
Or sign in with

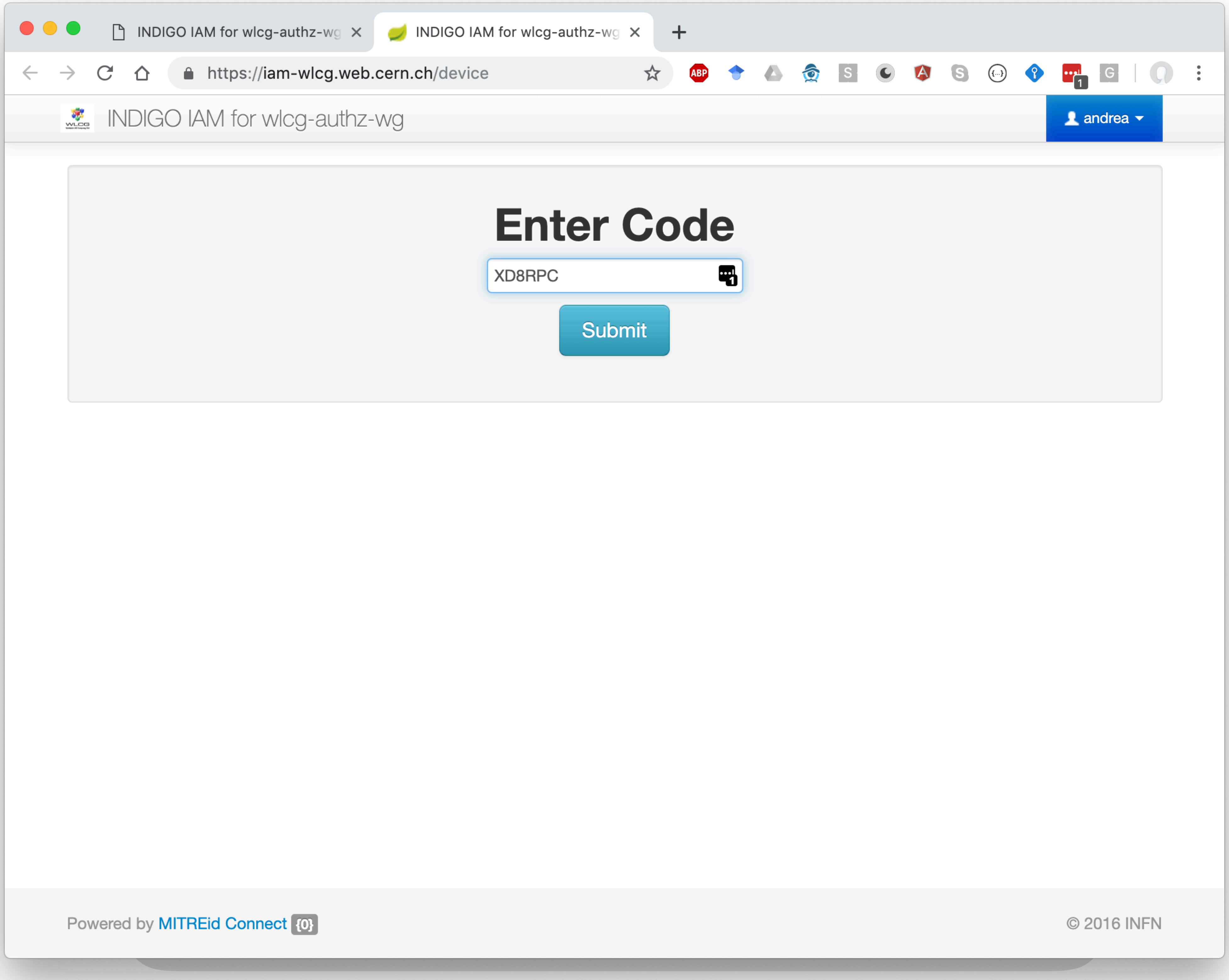
Your CERN account

Not a member?

Register a new account

The Device code flow




INDIGO IAM for wlcg-authz-wg
INDIGO IAM for wlcg-authz-wg
https://iam-wlcg.web.cern.ch/device
INDIGO IAM for wlcg-authz-wg
andrea

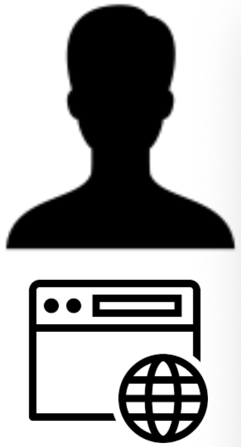
Enter Code

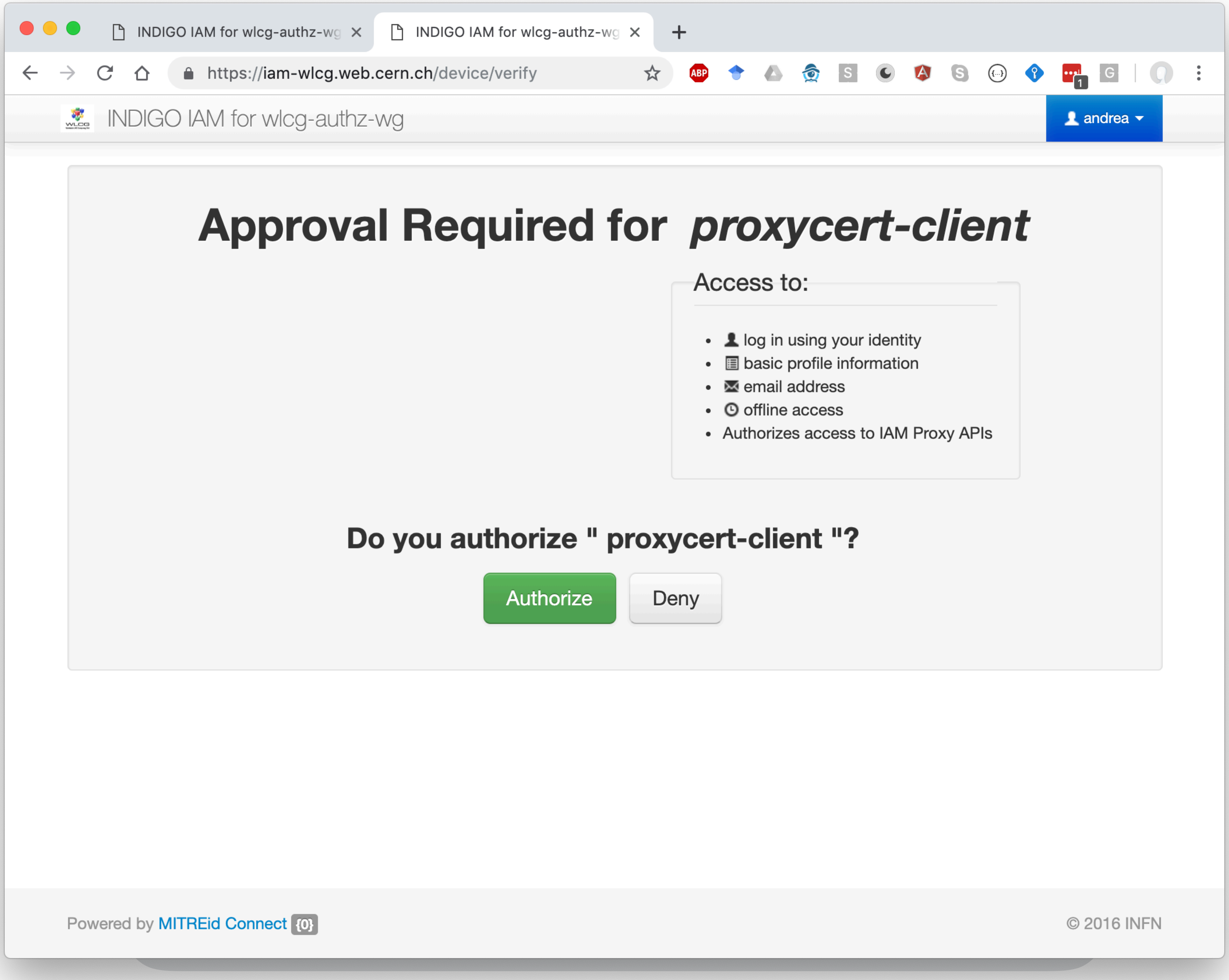
XD8RPC

Powered by MITREid Connect {0}

© 2016 INFN

The Device code flow





INDIGO IAM for wlcg-authz-wg
INDIGO IAM for wlcg-authz-wg
https://iam-wlcg.web.cern.ch/device/verify
INDIGO IAM for wlcg-authz-wg
andrea

Approval Required for *proxycert-client*

Access to:

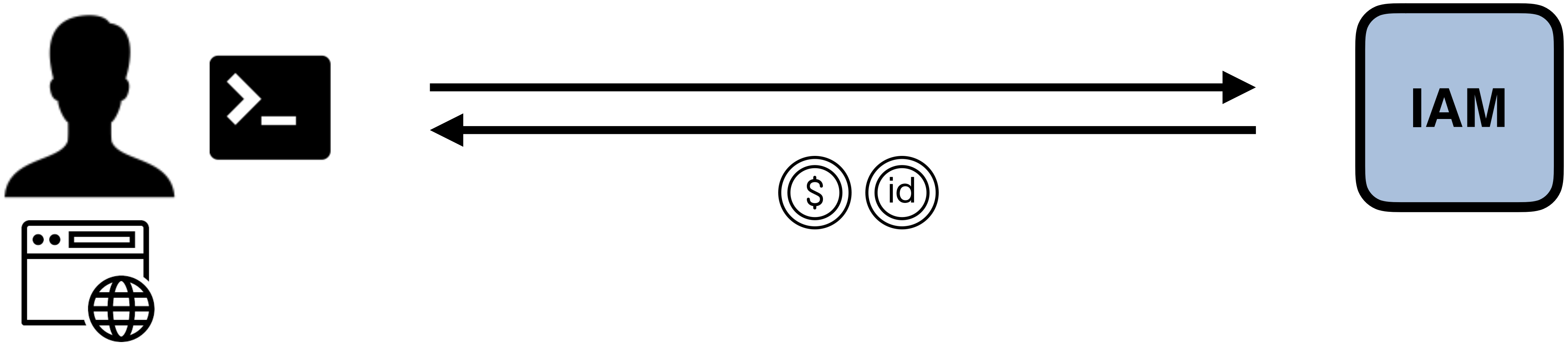
- log in using your identity
- basic profile information
- email address
- offline access
- Authorizes access to IAM Proxy APIs

Do you authorize " proxycert-client "?

Powered by MITREid Connect {0}

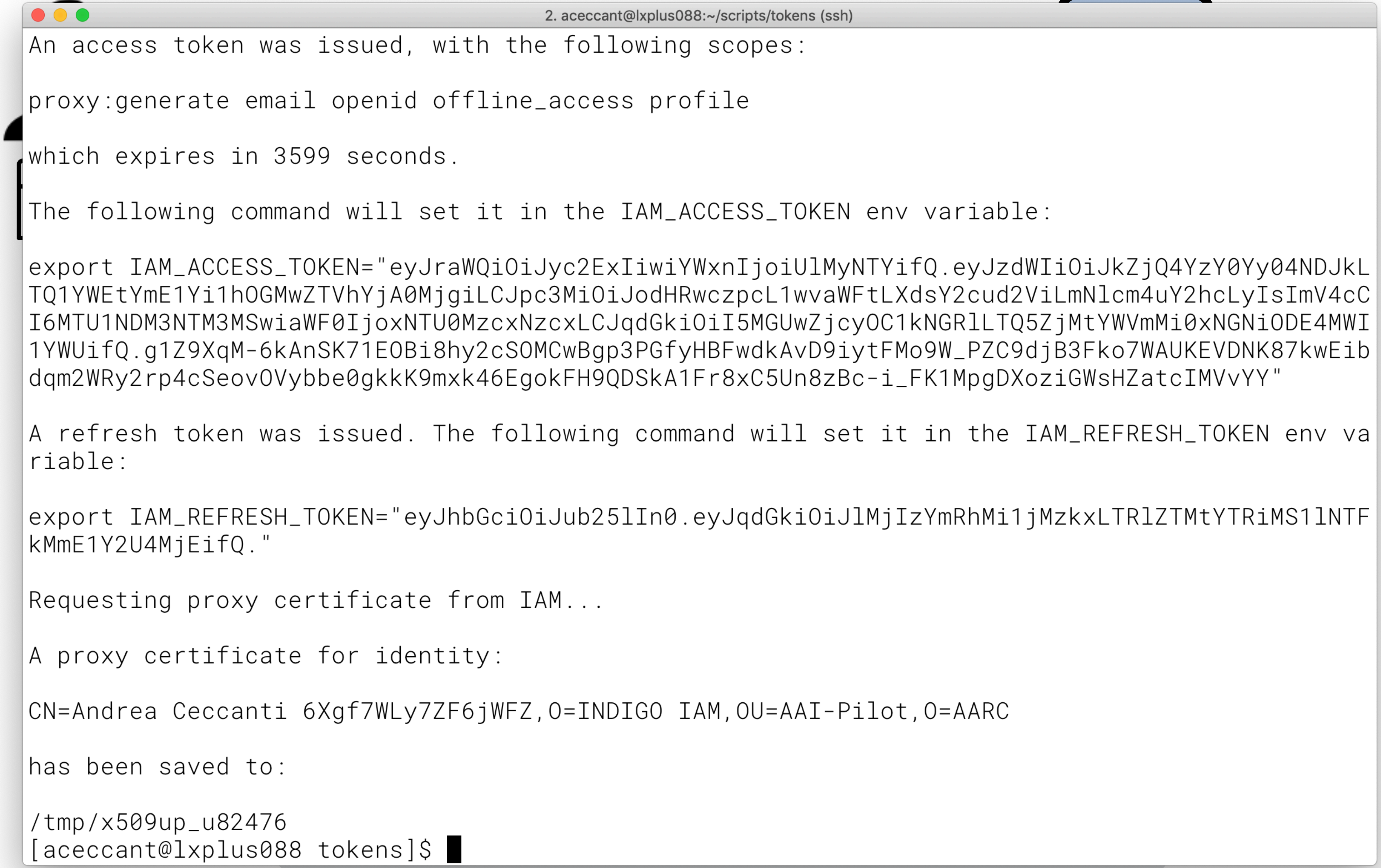
© 2016 INFN

The Device code flow



Once the user has given consent, the CLI can go back to IAM to fetch the tokens
The protocol also supports periodic polling from the client

The Device code flow



```
An access token was issued, with the following scopes:

proxy:generate email openid offline_access profile

which expires in 3599 seconds.

The following command will set it in the IAM_ACCESS_TOKEN env variable:

export IAM_ACCESS_TOKEN="eyJraWQiOiJyc2ExIiwiYWxnIjoiUlMyNTYifQ.eyJzdWIiOiJkZjQ4YzY0Yy04NDJkL
TQ1YWEtYmE1Yi1hOGMwZTVhYjA0MjgiLCJpc3MiOiJodHRwczpcL1wvaWFtLXdsY2cud2ViLmNlcm4uY2hcLyIsImV4cC
I6MTU1NDM3NTM3MSwiaWF0IjoxNTU0MzcxNzcxLCJqdGkiOiI5MGUwZjcyOC1kNGRlLTQ5ZjMtYWVmMi0xNGNiODE4MWI
1YWUifQ.g1Z9XqM-6kAnSK71EOBi8hy2cSOMCwBgp3PGfyHBFwdkAvD9iytFMo9W_PZC9djB3Fko7WAUKEVDNK87kwEib
dqm2WRy2rp4cSeovOVybbe0gkkK9mxk46EgokFH9QDSkA1Fr8xC5Un8zBc-i_FK1MpgDXoziGWsHZatcIMVvYY"

A refresh token was issued. The following command will set it in the IAM_REFRESH_TOKEN env va
riable:

export IAM_REFRESH_TOKEN="eyJhbGciOiJub25lIn0.eyJqdGkiOiJlMjIzYmRhMi1jMzkxLTRlZTMtYTRiMS1lNTF
kMmE1Y2U4MjEifQ."

Requesting proxy certificate from IAM...

A proxy certificate for identity:

CN=Andrea Ceccanti 6Xgf7WLy7ZF6jWFZ,O=INDIGO IAM,OU=AAI-Pilot,O=AARC

has been saved to:

/tmp/x509up_u82476
[aceccant@lxplus088 tokens]$ 
```

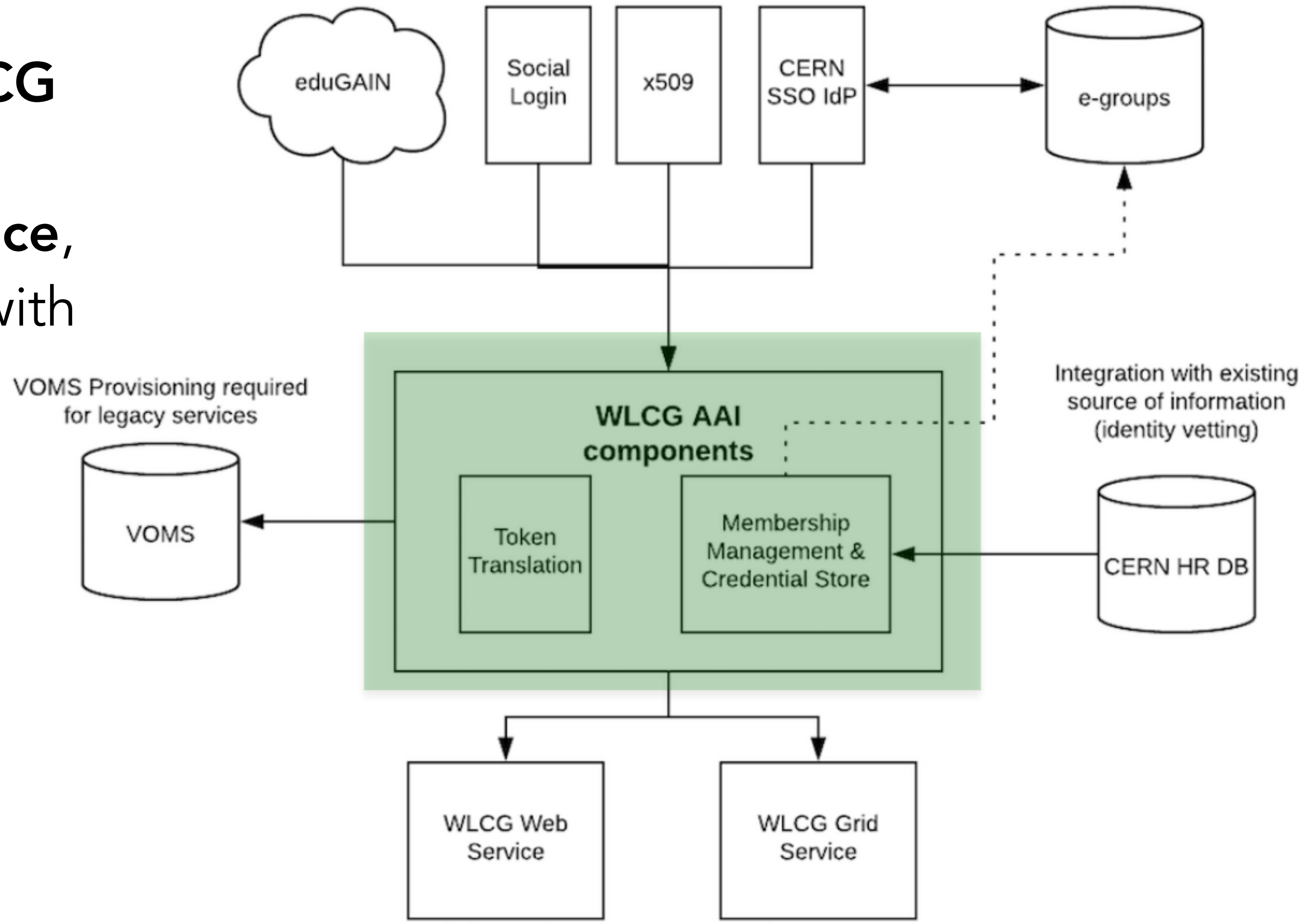
Standardization/Harmonization activities

The WLCG Authorization WG

https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAuthorizationWG

Main objectives:

- Design and testing of a **WLCG Membership Management and Token Translation service**, facilitated by pilot projects with the support of AARC
- Definition of a **token-based authentication and authorization profile for WLCG**

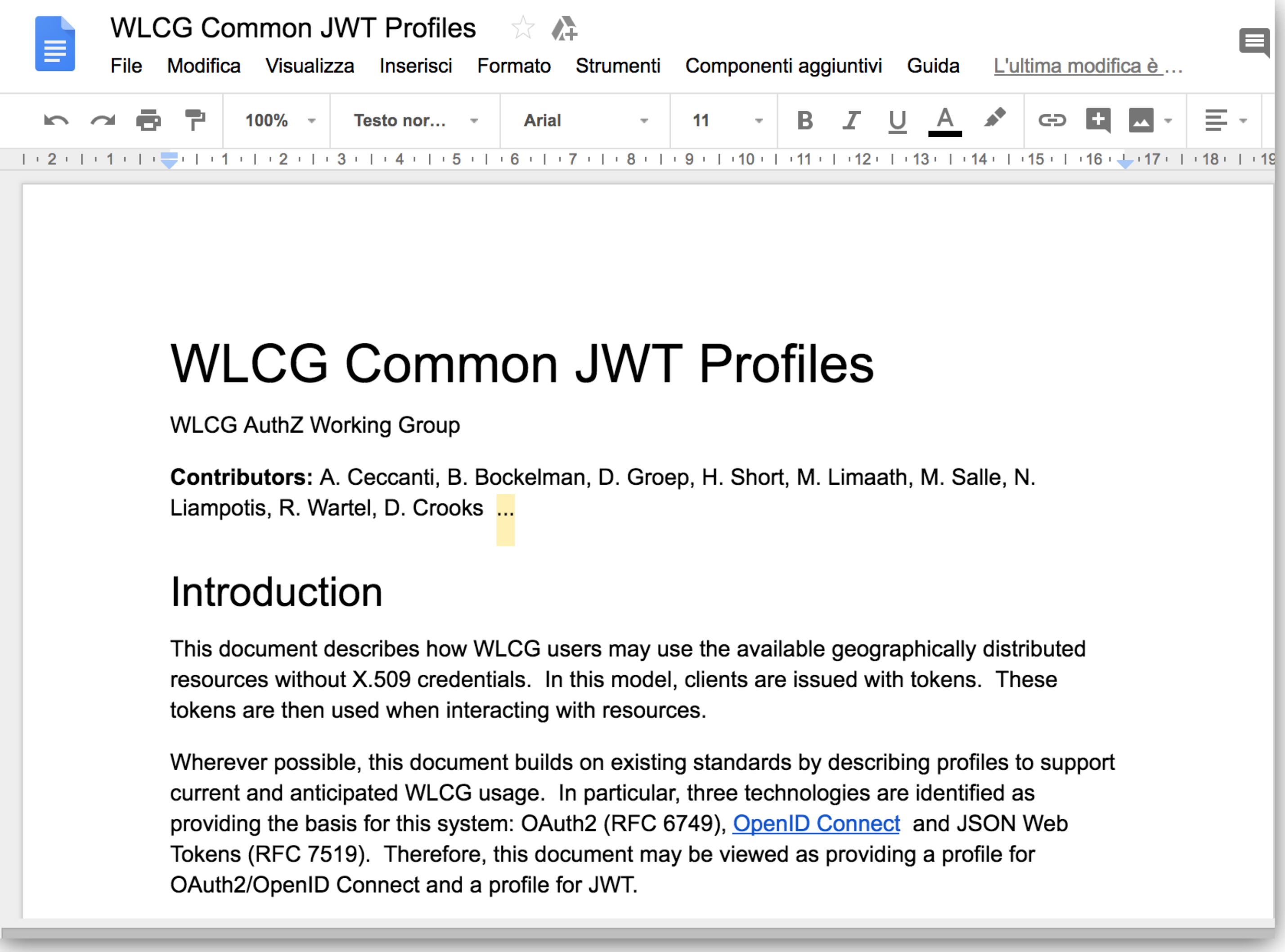

eduGAIN
Social Login
x509
CERN SSO IdP
e-groups
VOMS Provisioning required for legacy services
WLCG AAI components
Integration with existing source of information (identity vetting)
VOMS
Token Translation
Membership Management & Credential Store
CERN HR DB
WLCG Web Service
WLCG Grid Service

A common profile for Token-based AuthN/AuthZ

How is **authentication** and **authorization** information encoded in **identity** and **access tokens**?

How is **trust** established between parties exchanging tokens?

What's the recommended **token lifetime?**



WLCG Common JWT Profiles

WLCG AuthZ Working Group

Contributors: A. Ceccanti, B. Bockelman, D. Groep, H. Short, M. Limaath, M. Salle, N. Liampotis, R. Wartel, D. Crooks ...

Introduction

This document describes how WLCG users may use the available geographically distributed resources without X.509 credentials. In this model, clients are issued with tokens. These tokens are then used when interacting with resources.

Wherever possible, this document builds on existing standards by describing profiles to support current and anticipated WLCG usage. In particular, three technologies are identified as providing the basis for this system: OAuth2 (RFC 6749), OpenID Connect and JSON Web Tokens (RFC 7519). Therefore, this document may be viewed as providing a profile for OAuth2/OpenID Connect and a profile for JWT.

Approach:

rely on existing standards as much as possible, extend only when needed

Next steps

ESCAPE AAI: next steps

Collect and **understand key AAI requirements** across the ESCAPE cluster

- How are users and agents authenticated?
- What's the authorization model? What's the delegation model? How are authorization privileges and policies managed?
  - **Focus on data access**
- What are the legacy auhtn/authz mechanisms that must be supported?

Agree on **a common way to express Authn/Authz information** and expose this information to services

- Start from the WLCG experience and expand/adapt it as needed

Understand what are the **key software components** that needs to be integrated

- and whether the integration requires changes in the software

ESCAPE AAI: next steps

Understand how we make and assess progress

- Identify and bring together the "AAI experts" across the communities
  - People that know the experiment/community computing model and can answer nerdy AAI questions
- Do we need AAI-focused, cross-WP communication channels?
  - i.e., a dedicated mailing list or is the e-dios list enough?
- Setup collaborative tools to track requirements collection, integration activities, issues?
  - issue tracker, wiki, …
- Setup a testbed
  - the sooner we find issues, the sooner we start to solve them!

Thanks for your attention.

Questions?

Useful references

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

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

WLCG Authorization WG: https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAuthorizationWG

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

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

Contacts:

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