Token-based AAI: integration patterns for relying applications

Andrea Ceccanti
INFN CNAF

Ibergrid 2019
Santiago de Compostela, September 25 2019

Agenda

Token-based AAI: an introduction

OAuth & OpenID connect overview

IAM integration exercise

OIDC on the command line with OIDC agent

User provisioning with FEUDAL

Apply for an IAM account

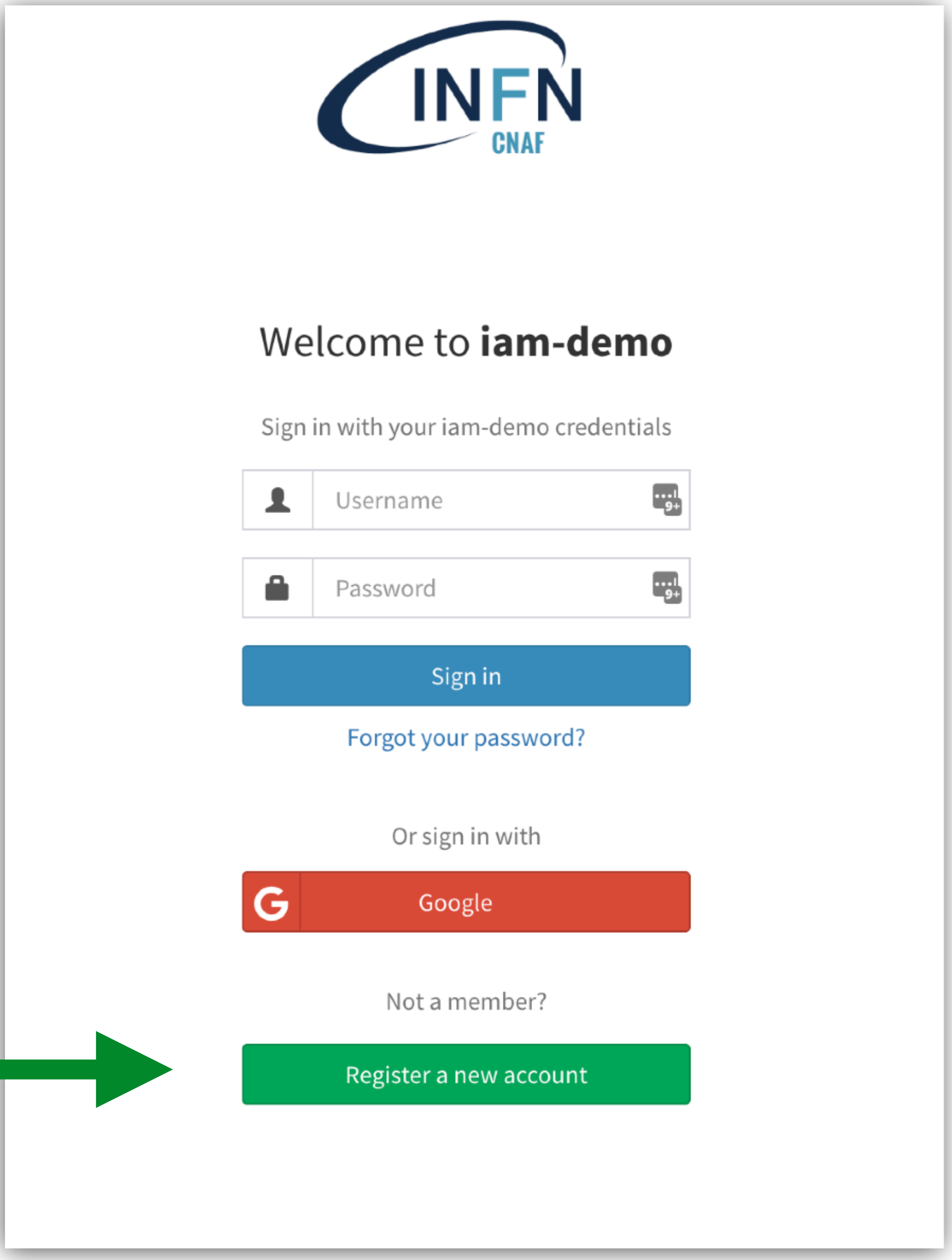
Please point your browser to:

- https://iam-demo.cloud.cnaf.infn.it

and apply for an account.

In the notes field put "Ibergrid 2019"

You will use that account later in the tutorial



Welcome to **iam-demo**

Sign in with your iam-demo credentials

IAM overview

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/de-provisioning of identities to services/relying resources

Token translation

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

INDIGO Identity and Access Management service

Flexible authentication support

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

Account linking

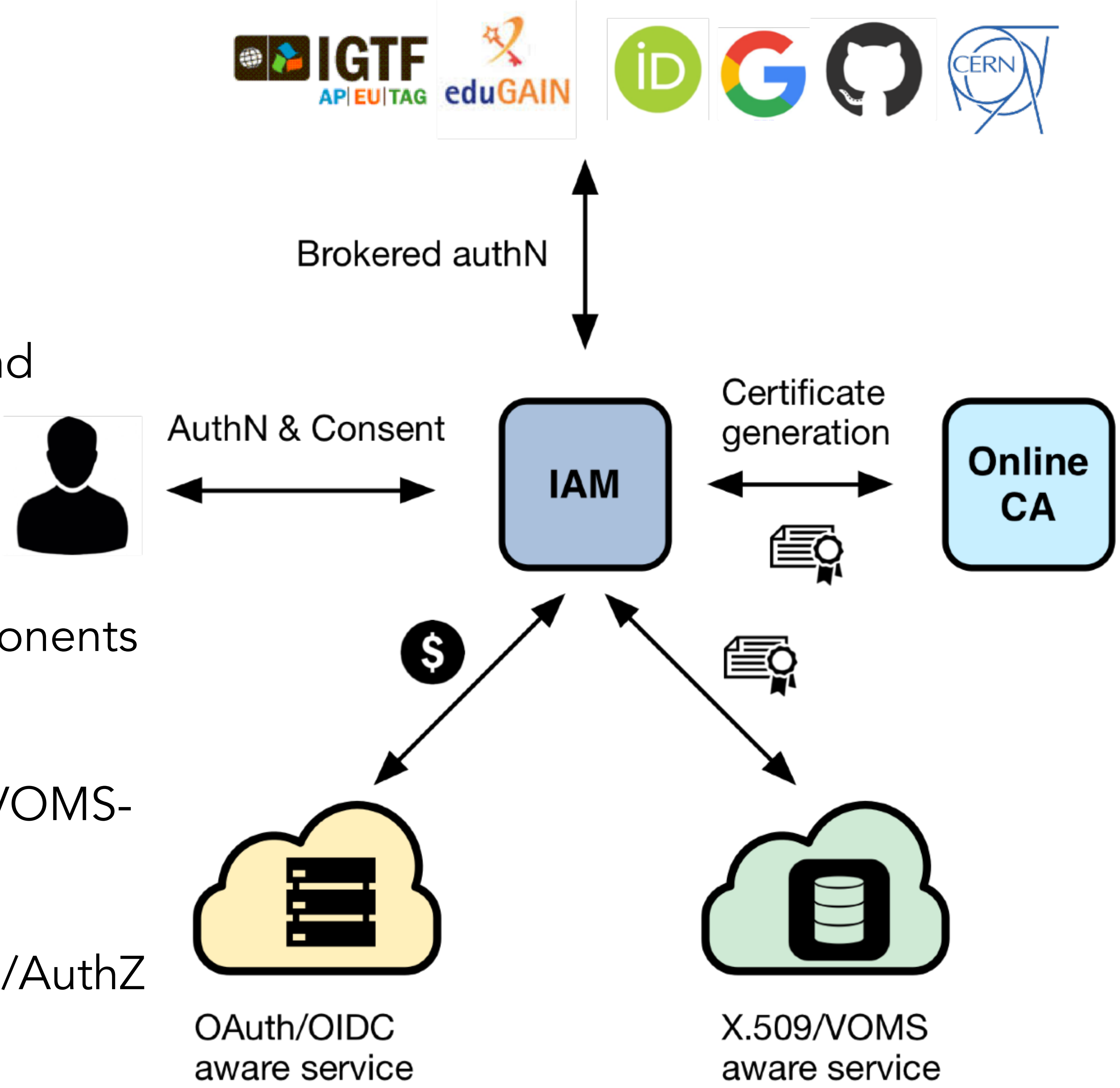
Registration service for moderated and automatic user enrollment

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



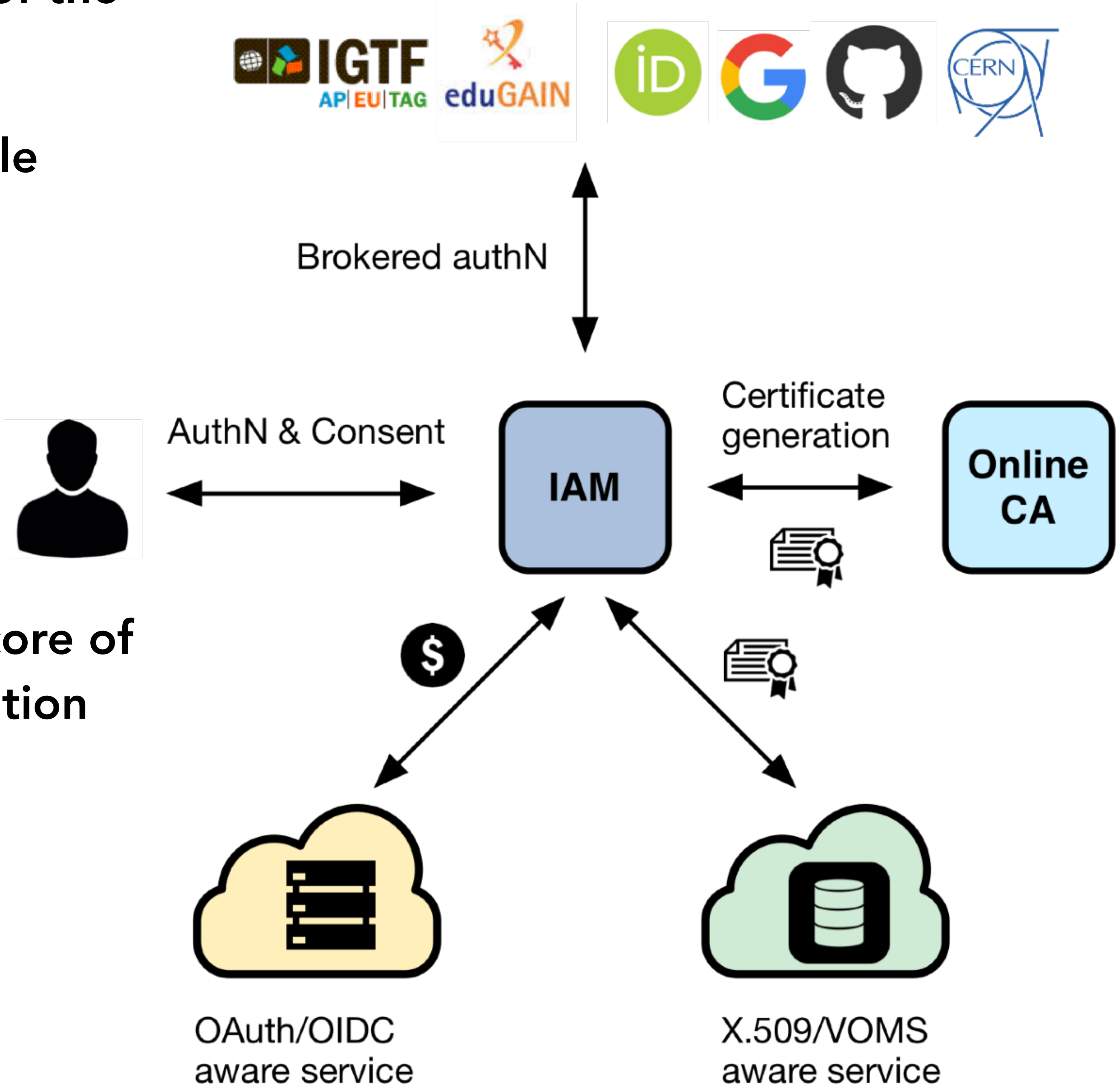
INDIGO Identity and Access Management service

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

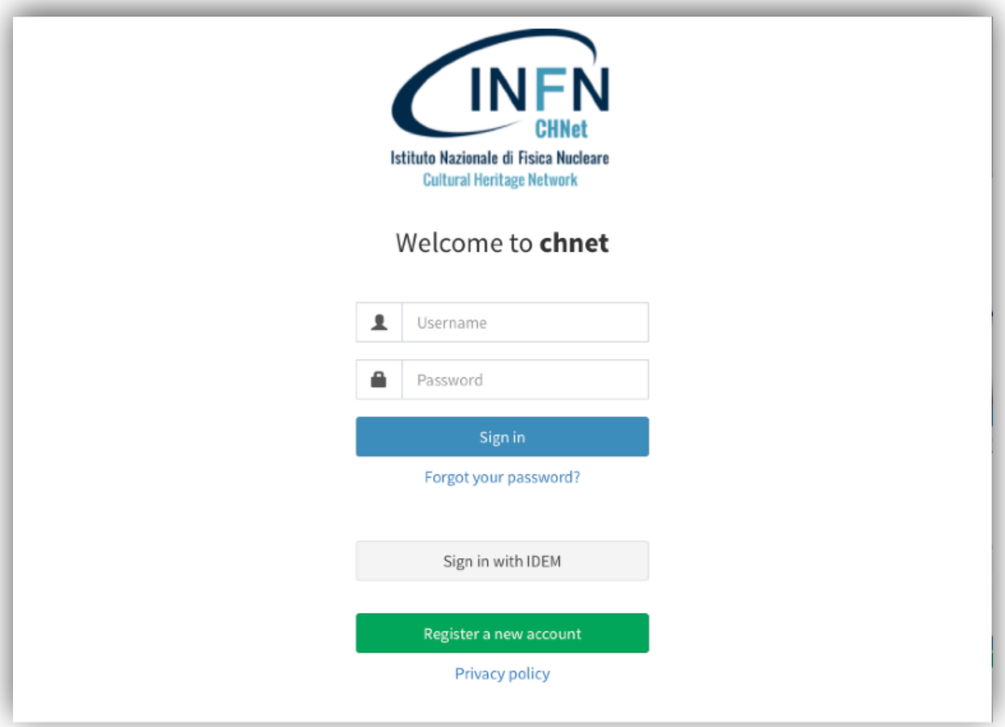


IAM deployment model

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** mechanisms.

The IAM Web appearance can be **customized** to include a **community logo**, **AUP** and **privacy policy** document.


INFN CHNet
Istituto Nazionale di Fisica Nucleare
Cultural Heritage Network

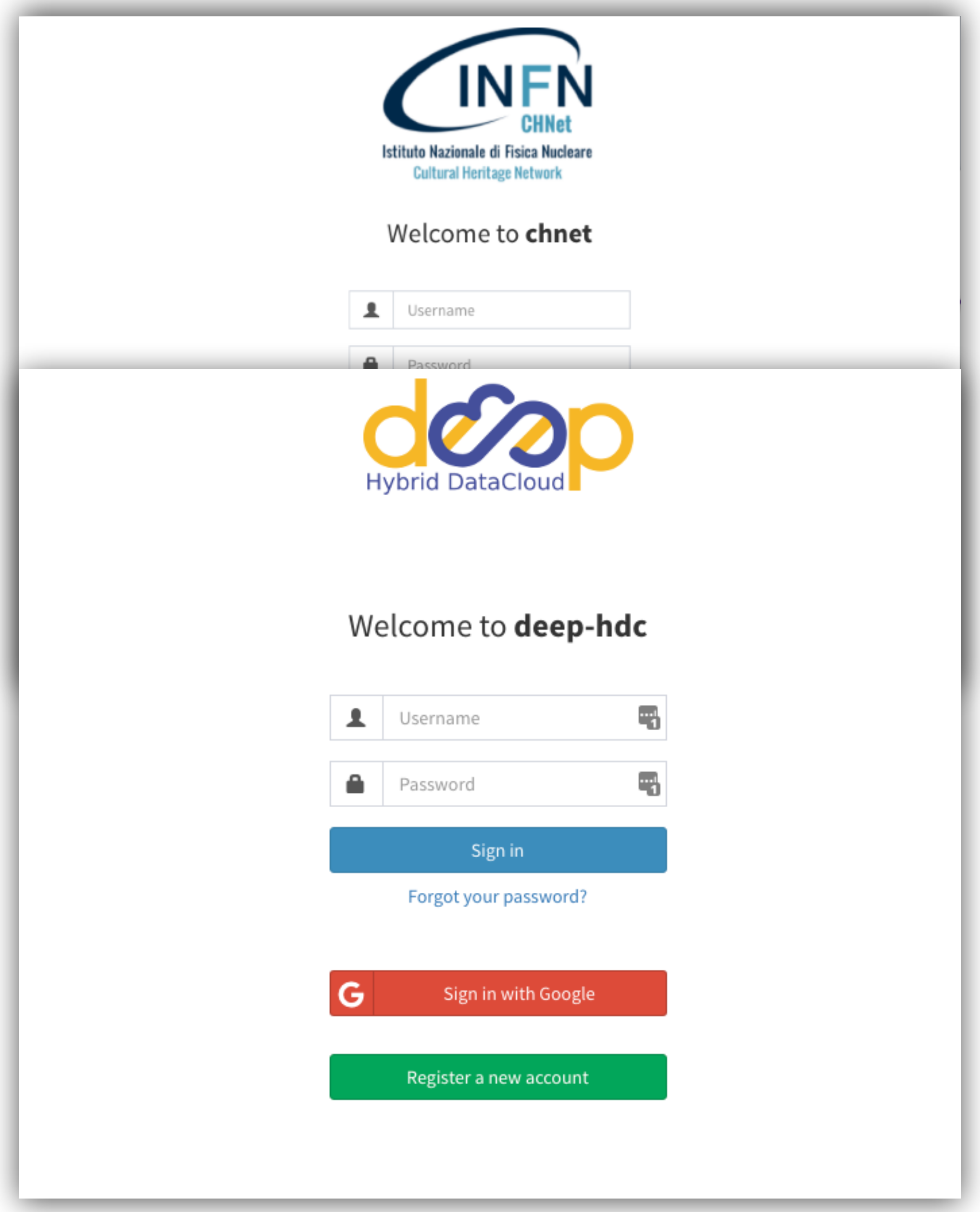
Welcome to **chnet**

IAM deployment model

An IAM instance is deployed for a **community** of users sharing resources, the good old **Virtual Organization (VO)** concept.

Client applications and services are integrated with this instance via **standard OAuth/OpenID Connect** mechanisms.

The IAM Web appearance can be **customized** to include a **community logo**, **AUP** and **privacy policy** document.



INFN
CHNet
Istituto Nazionale di Fisica Nucleare
Cultural Heritage Network

Welcome to **chnet**

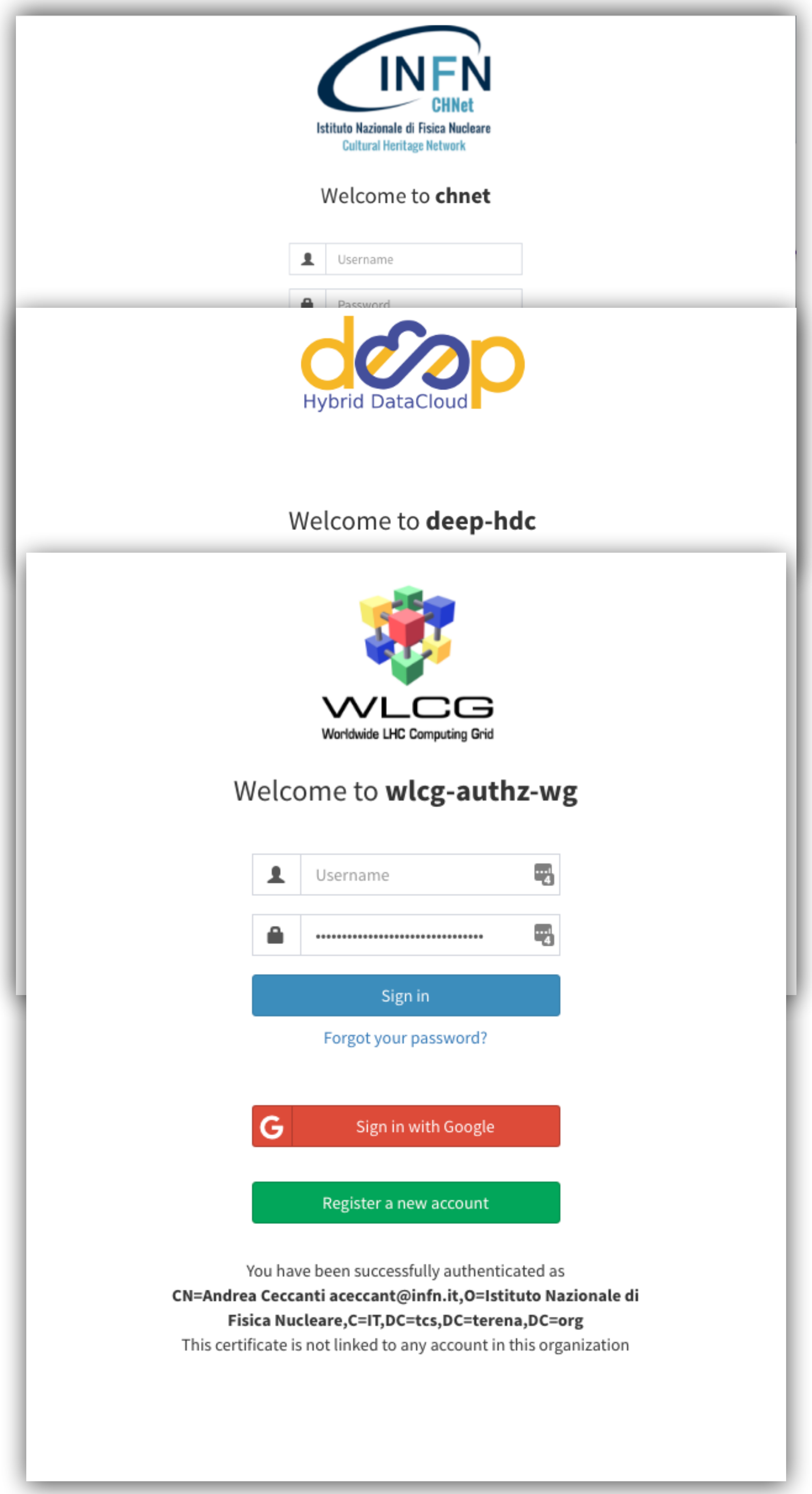
Welcome to **deep-hdc**

IAM deployment model

An IAM instance is deployed for a **community** of users sharing resources, the good old **Virtual Organization (VO)** concept.

Client applications and services are integrated with this instance via **standard OAuth/OpenID Connect** mechanisms.

The IAM Web appearance can be **customized** to include a **community logo**, **AUP** and **privacy policy** document.


INFN
CHNet
Istituto Nazionale di Fisica Nucleare
Cultural Heritage Network

Welcome to **chnet**

Welcome to **deep-hdc**

Welcome to **wlcg-authz-wg**

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

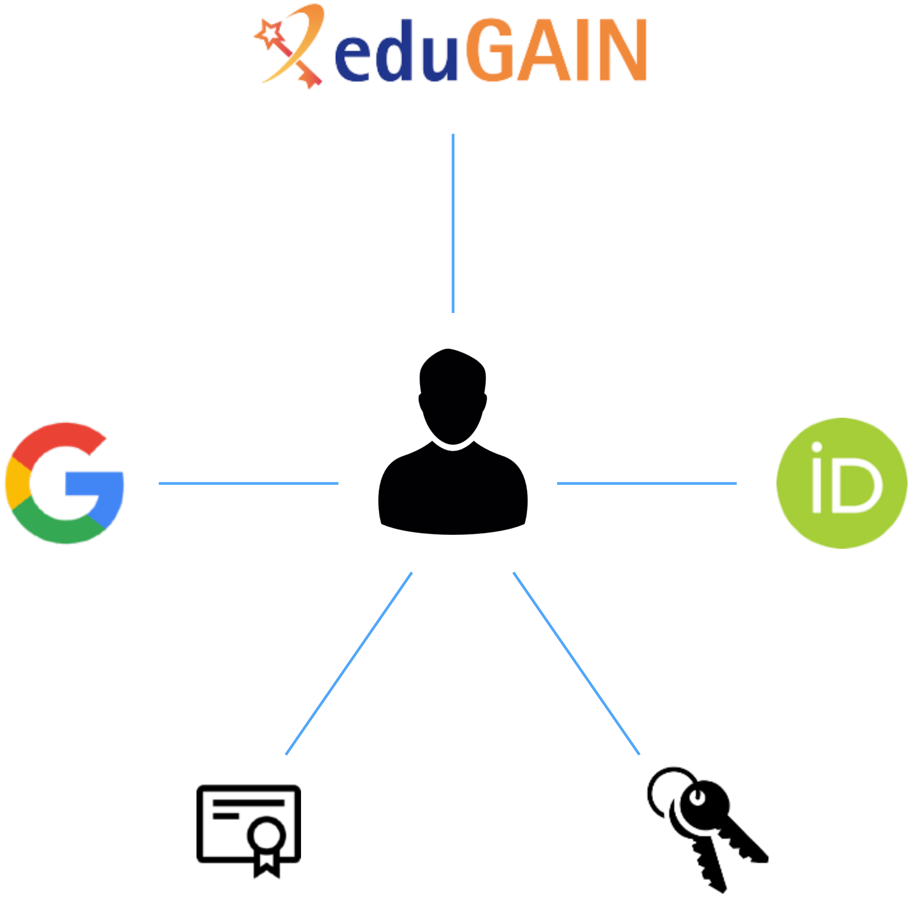
Flexible authentication & account linking

Authentication supported via

- **local username/password** credentials (created at registration time)
- **SAML** Home institution IdP (e.g., EduGAIN)
- **OpenID Connect** (Google, Microsoft, Paypal, ORCID)
- **X.509** certificates

Users can link any of the supported authentication credentials to their IAM account at registration time or later

To link an external credential/account, the user has to **prove** that he/she owns such account



User enrollment & registration service

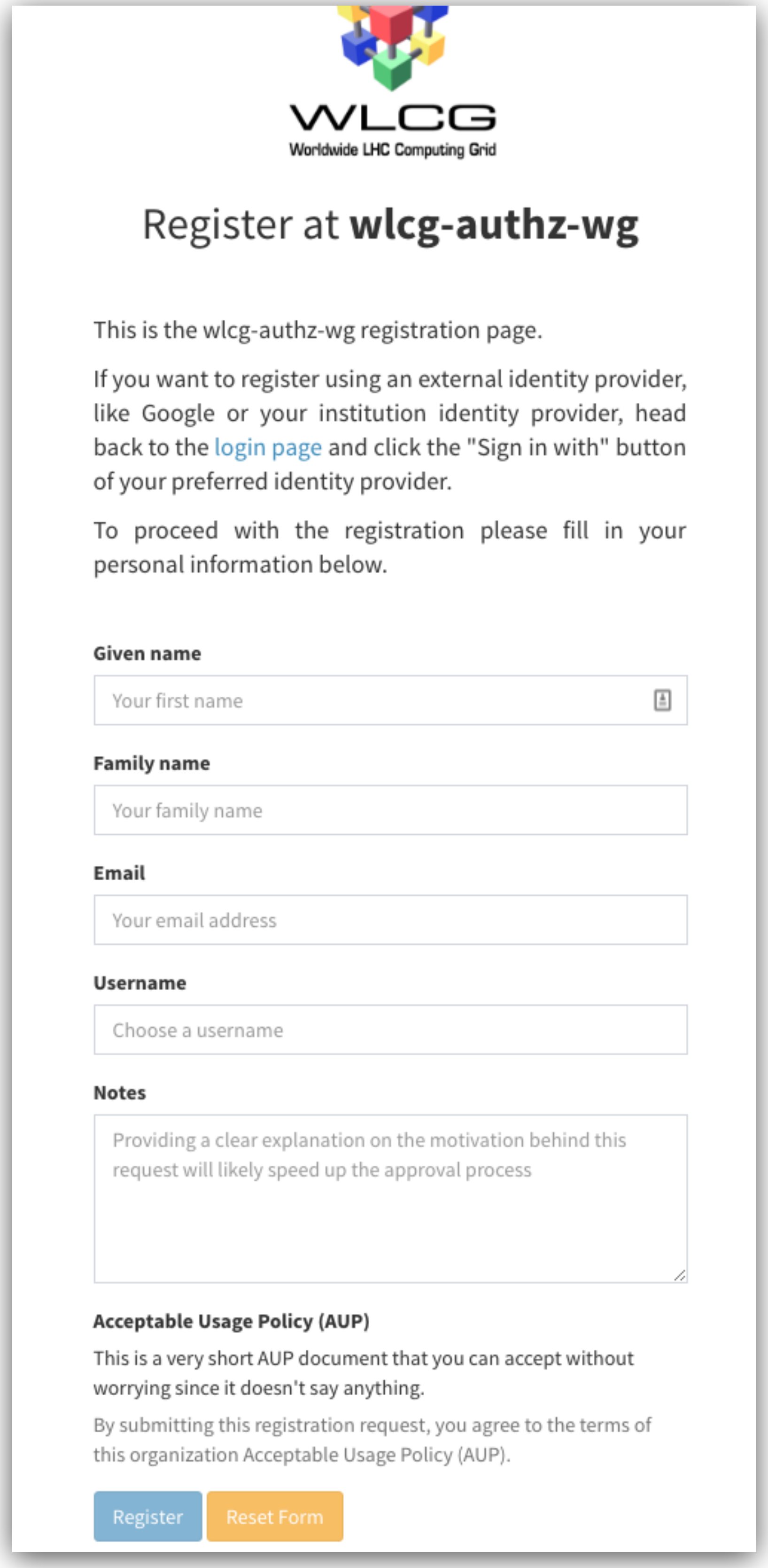
IAM supports two **enrollment flows:**

Admin-moderated flow

- The applicant fills basic registration information, accepts AUP, proves email ownership
- VO administrators are informed by email and can approve or reject incoming membership requests
- The applicant is informed via email of the administrator decision

Automatic-enrollment flow

- Users authenticated at **trusted**, **configurable** SAML IdPs are automatically on-boarded, without administrator approval



Register at **wlcg-authz-wg**

This is the wlcg-authz-wg registration page.

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

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

Given name

Your first name

Family name

Your family name

Email

Your email address

Username

Choose a username

Notes

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

Acceptable Usage Policy (AUP)

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

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

User enrollment & registration service

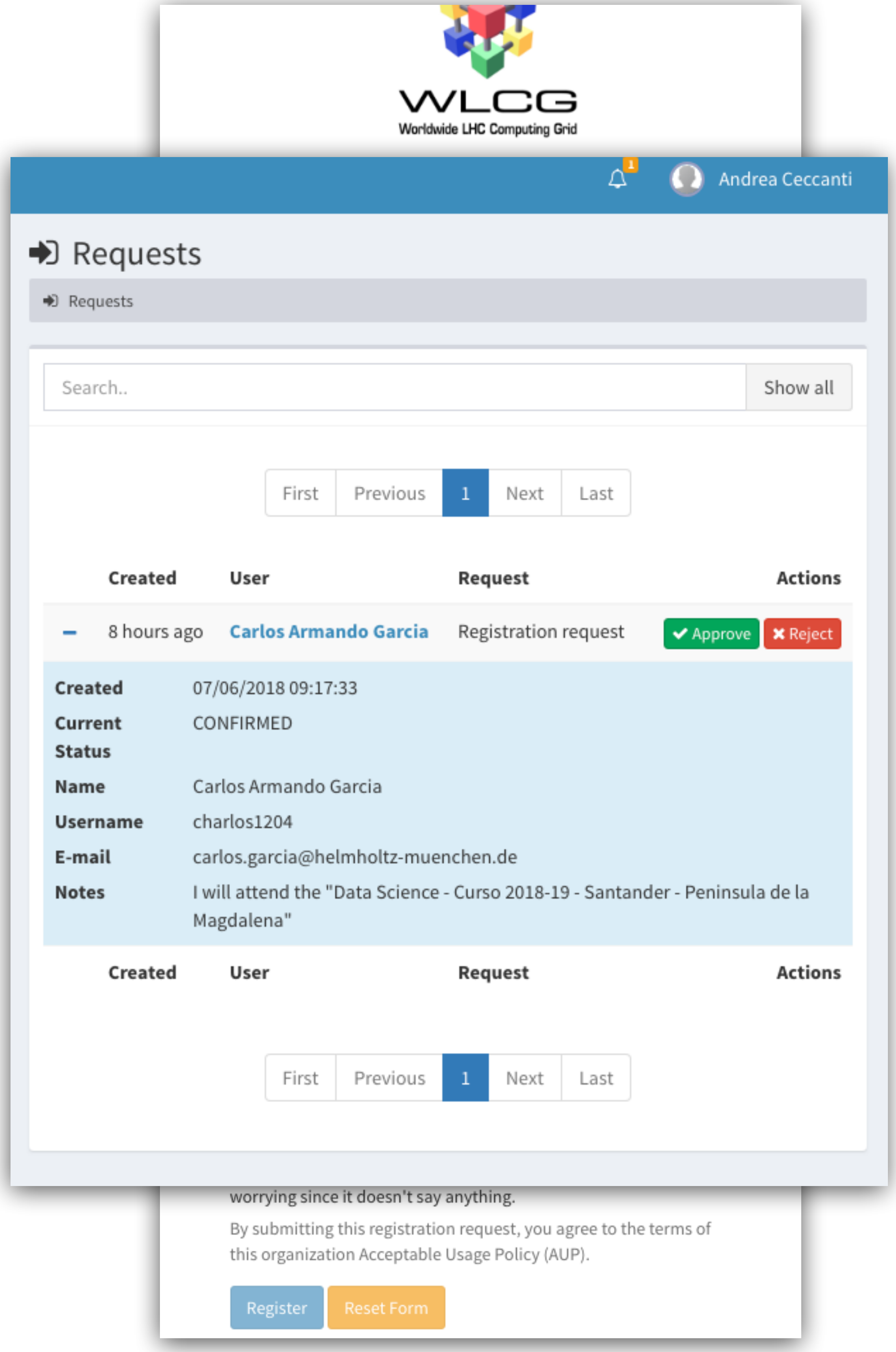
IAM supports two **enrollment flows:**

Admin-moderated flow

- The applicant fills basic registration information, accepts AUP, proves email ownership
- VO administrators are informed by email and can approve or reject incoming membership requests
- The applicant is informed via email of the administrator decision

Automatic-enrollment flow

- Users authenticated at **trusted**, **configurable** SAML IdPs are automatically on-boarded, without administrator approval



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.

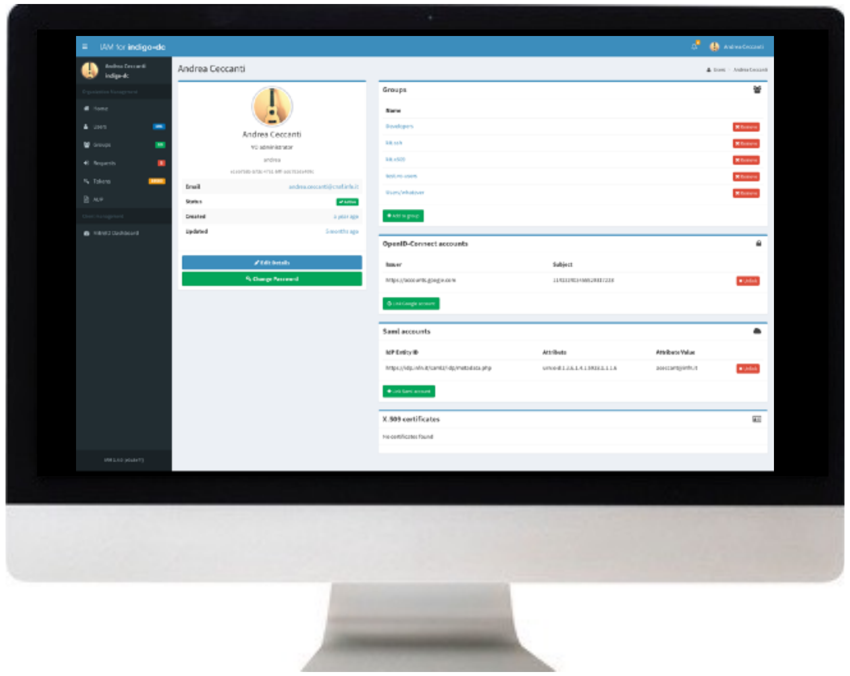
By submitting this registration request, you agree to the terms of this organization Acceptable Usage Policy (AUP).

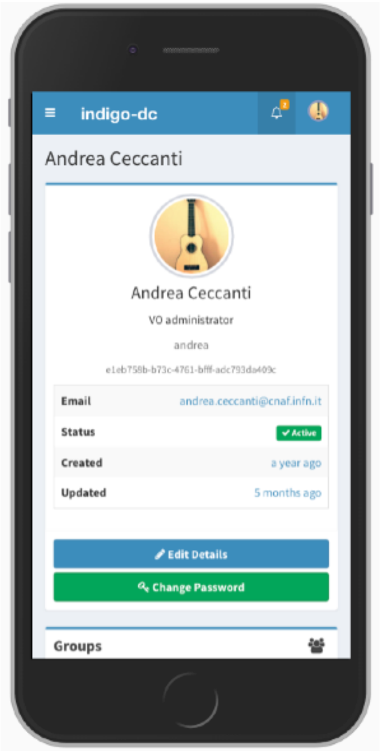
Management tools

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





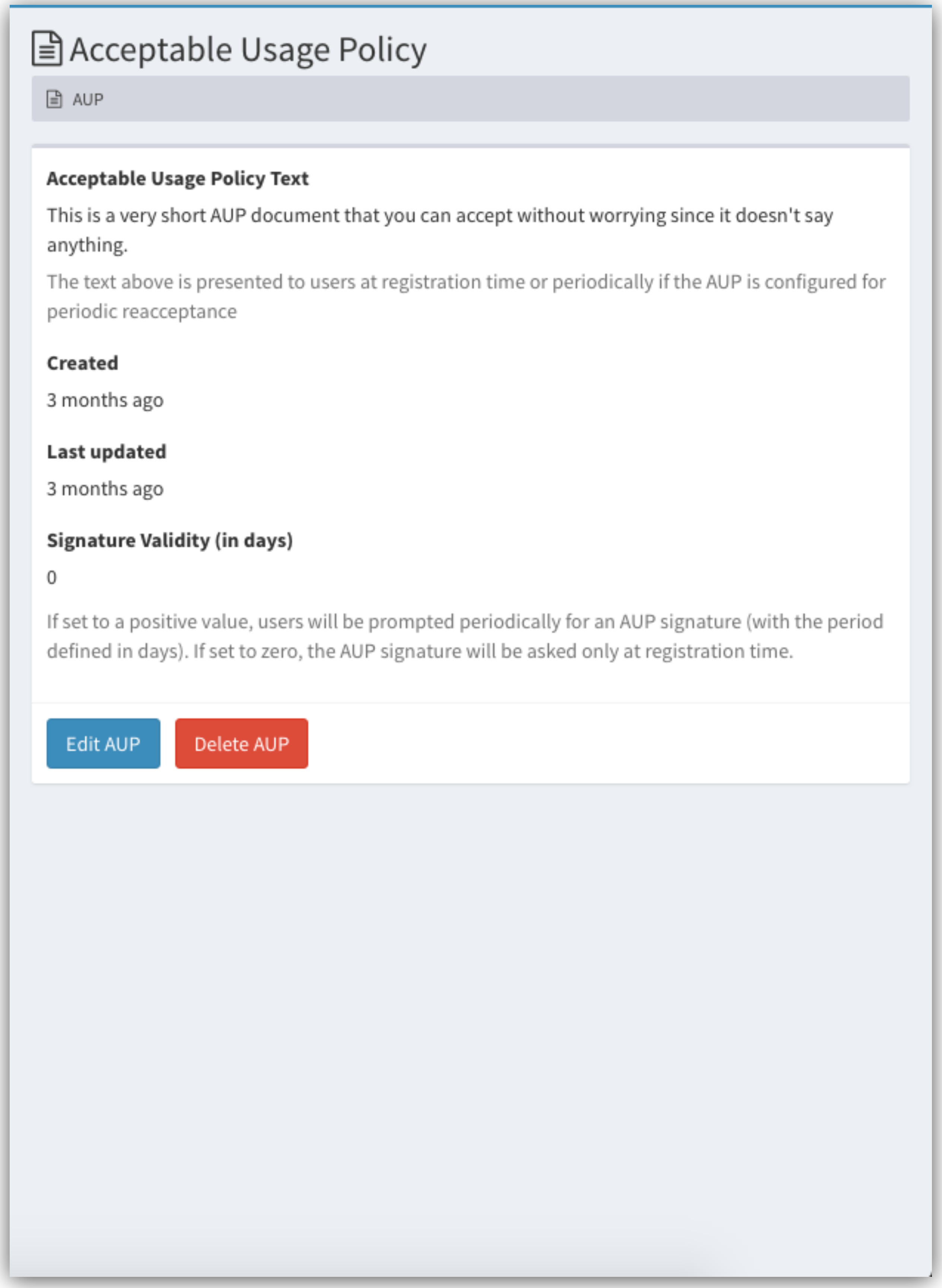
Email andrea.ceccanti@cnaf.infn.it
Status ✓ Active
Created a year ago
Updated 5 months ago

AUP enforcement support

AUP acceptance, if enabled, can be configured to be:

- requested once at user registration time
- periodically, with configurable period

User cannot login to the system (and as such be authenticated at authorized at services) unless the **AUP** has been accepted



Acceptable Usage Policy

AUP

Acceptable Usage Policy Text

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

The text above is presented to users at registration time or periodically if the AUP is configured for periodic reacceptance

Created

3 months ago

Last updated

3 months ago

Signature Validity (in days)

0

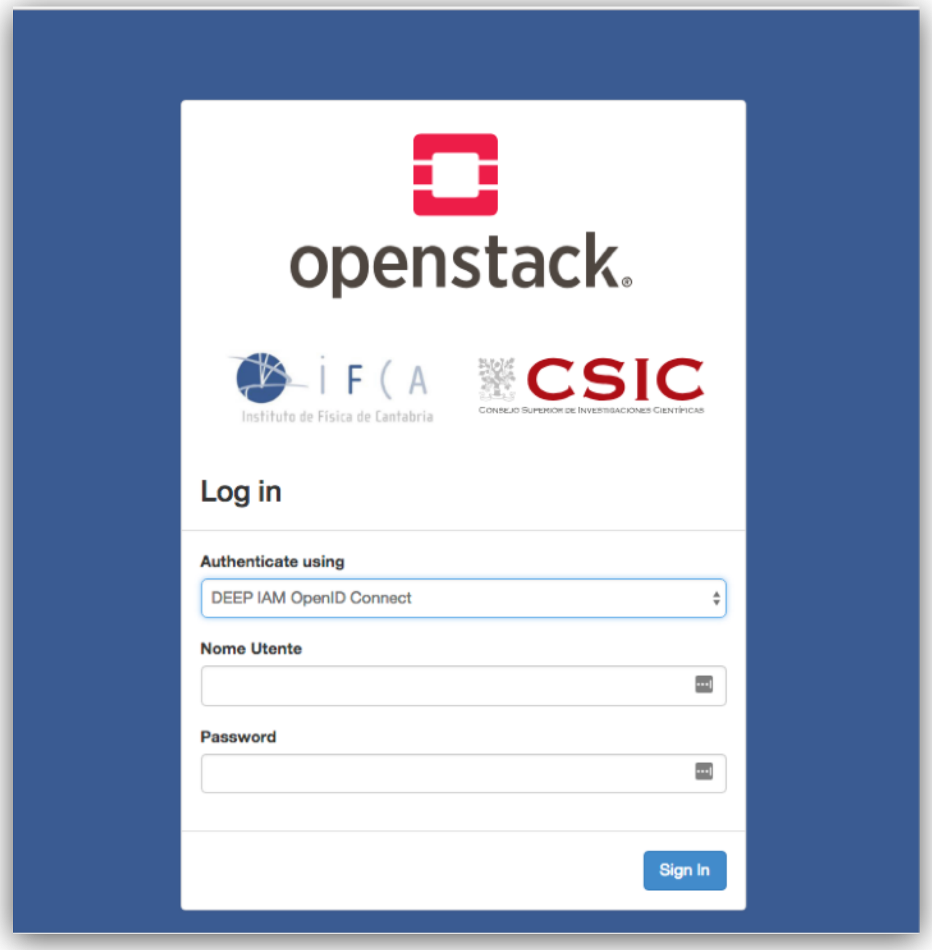
If set to a positive value, users will be prompted periodically for an AUP signature (with the period defined in days). If set to zero, the AUP signature will be asked only at registration time.

Easy integration with services

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

We have successfully integrated IAM with minimal effort with:

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


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

Log in

Authenticate using: DEEP IAM OpenID Connect

Nome Utente

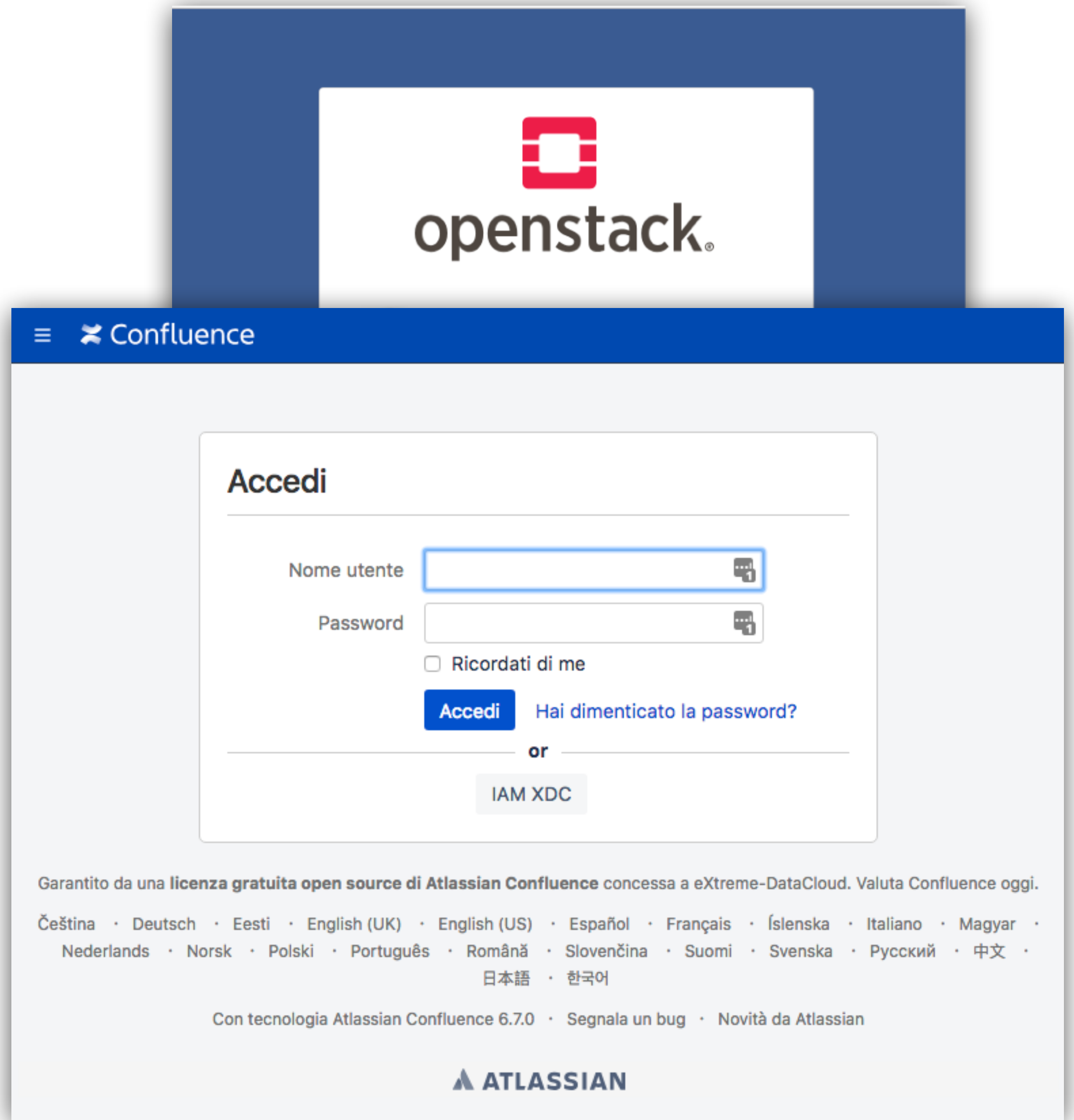
Password

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
- Kubernetes
- Moodle
- Rocketchat
- Grafana
- JupyterHub



Nome utente

Password

☐ Ricordati di me

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

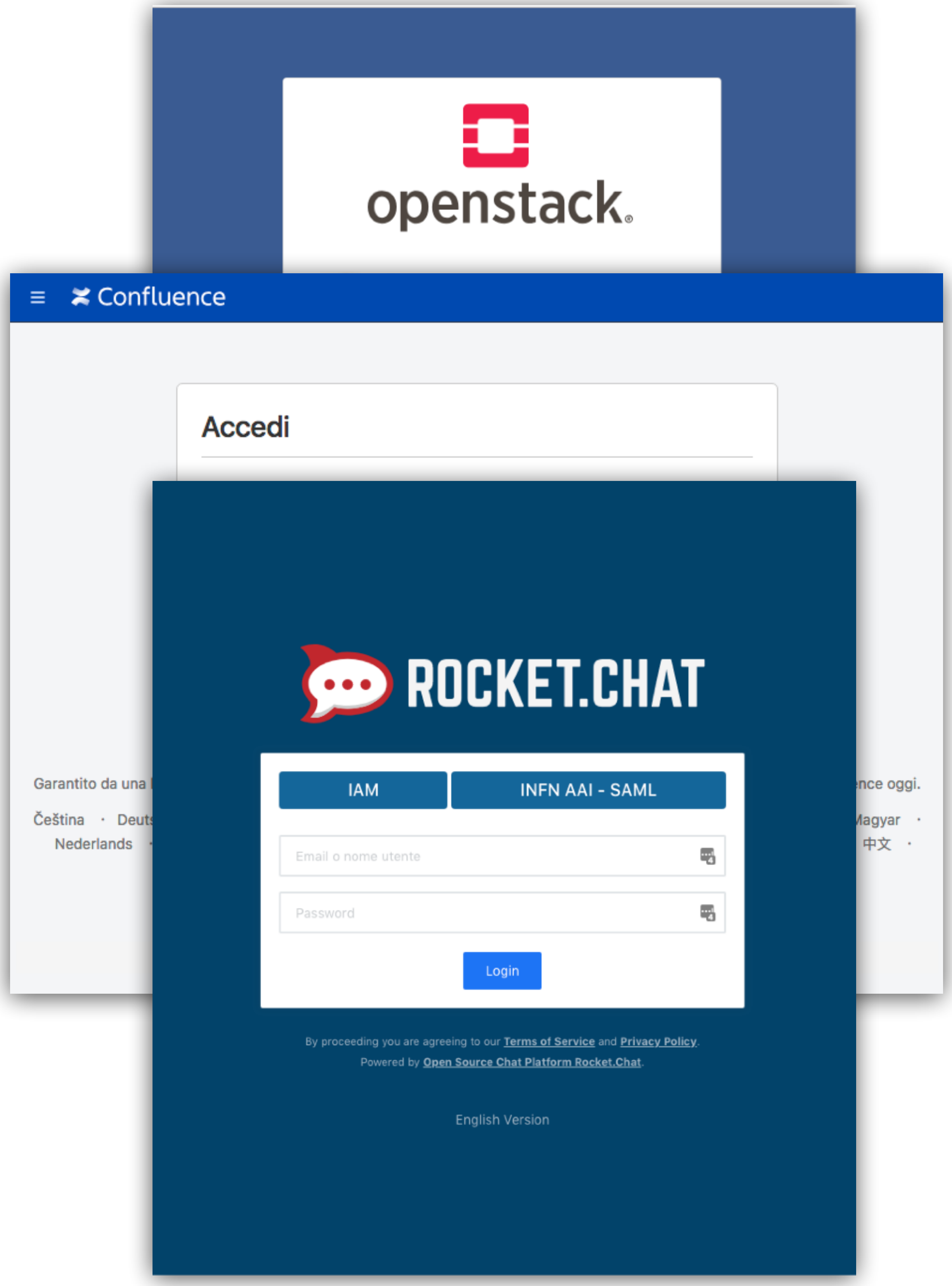
Con tecnologia Atlassian Confluence 6.7.0 · Segnala un bug · Novità da Atlassian

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
- Kubernetes
- Moodle
- Rocketchat
- Grafana
- JupyterHub



Garantito da una

Čeština · Deuts

Nederlands ·

nce oggi.

Magyar ·

中文 ·

By proceeding you are agreeing to our Terms of Service and Privacy Policy.

Powered by Open Source Chat Platform Rocket.Chat.

Enabling technologies

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"

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

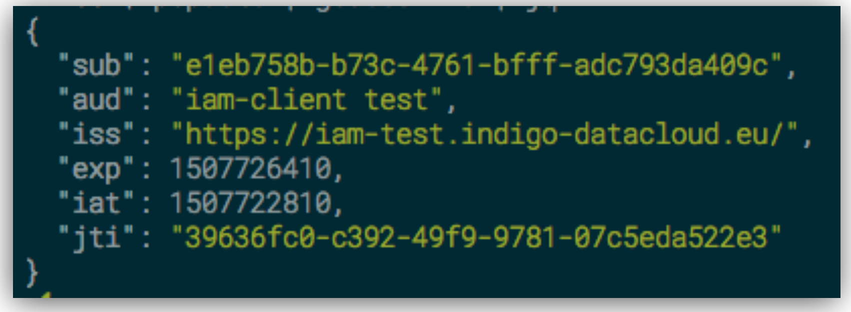
938568

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

MUSTER

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. API)

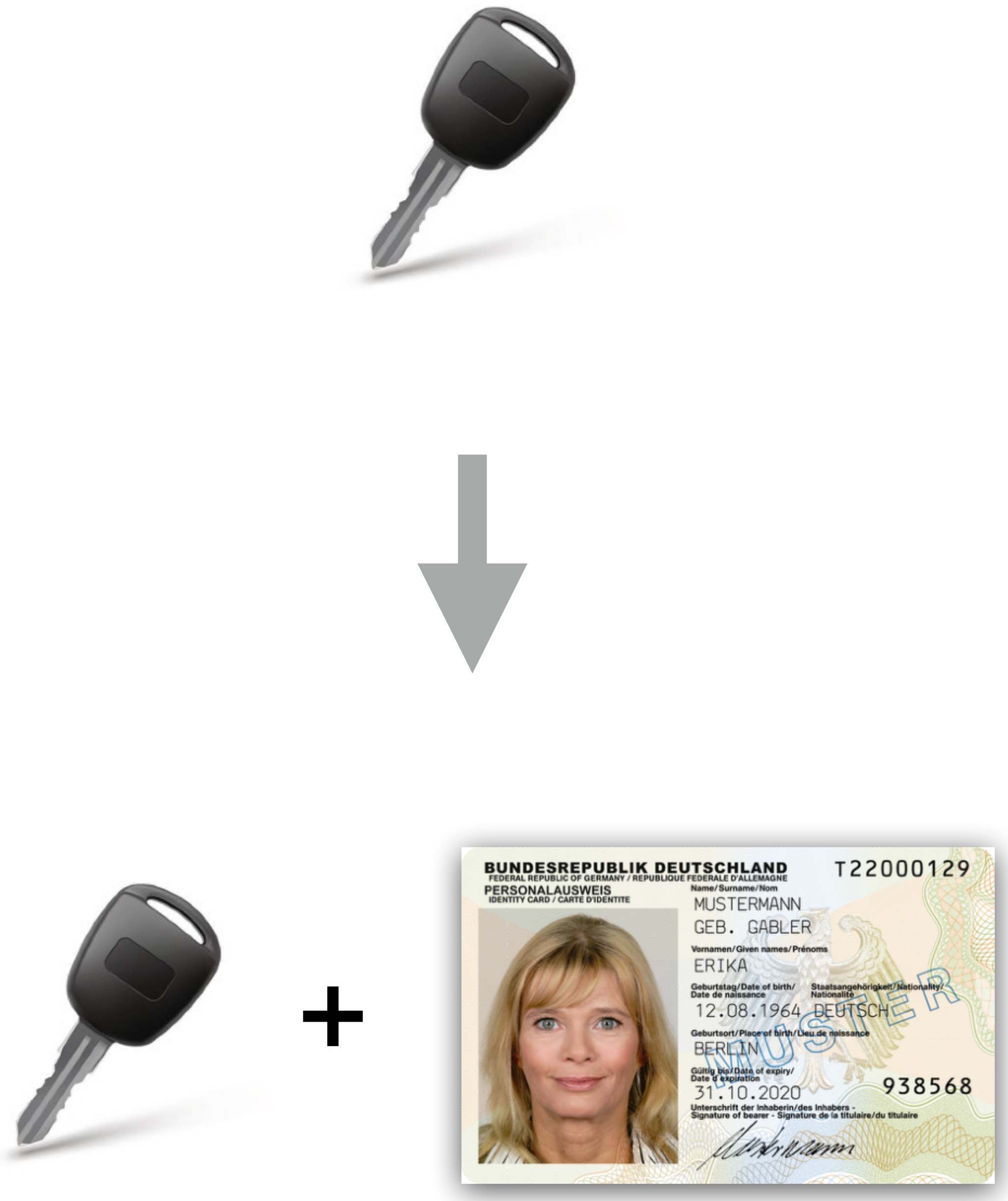
OpenID Connect: an identity layer for OAuth

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)

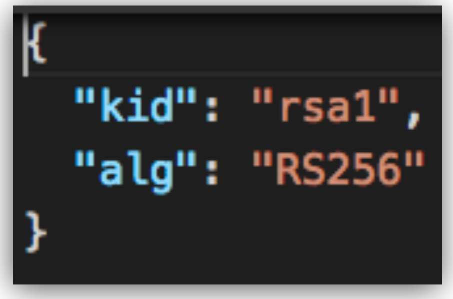

+
BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE
T22000129
Name/Surname/Nom
MUSTERMANN
GEB. GABLER
Vornamen/Given names/Prénoms
ERIKA
Geburtstag/Date of birth/ Date de naissance
12.08.1964
Staatsangehörigkeit/Nationality/ 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
MUSTER

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

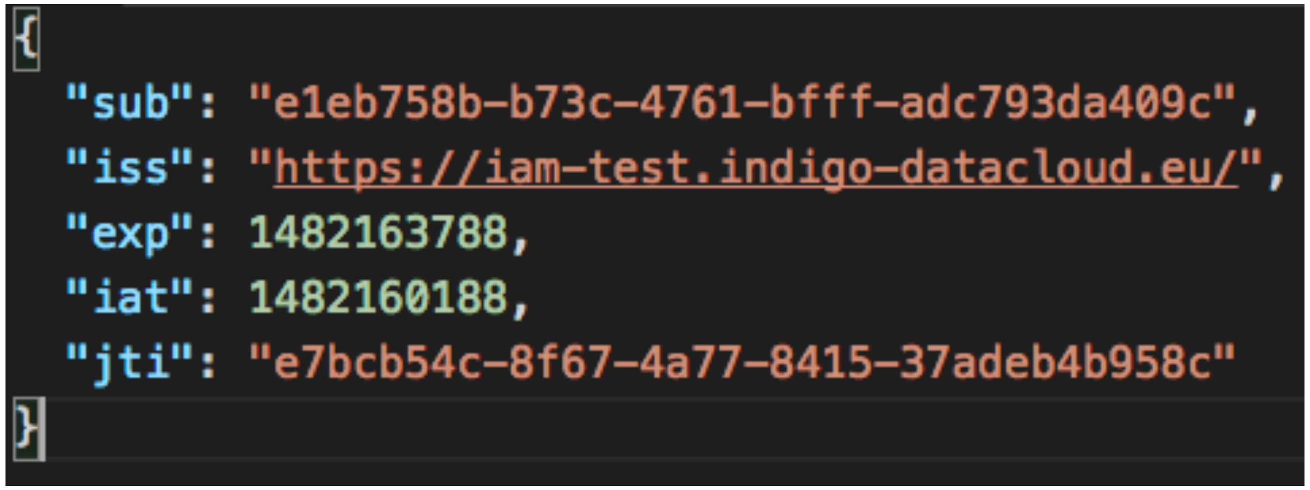
JWTs are typically **signed** and, if confidentiality is a requirement, can be **encrypted**.

Header **Body** **Signature**



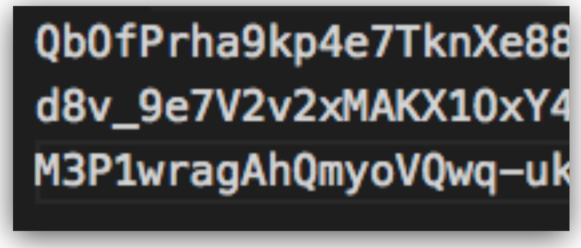
```
{
  "kid": "rsa1",
  "alg": "RS256"
}
```

.



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

.



```
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

A brief introduction to OAuth and OpenID Connect

OAuth roles

Resource owner

- A user that owns resources hosted at a service

Client

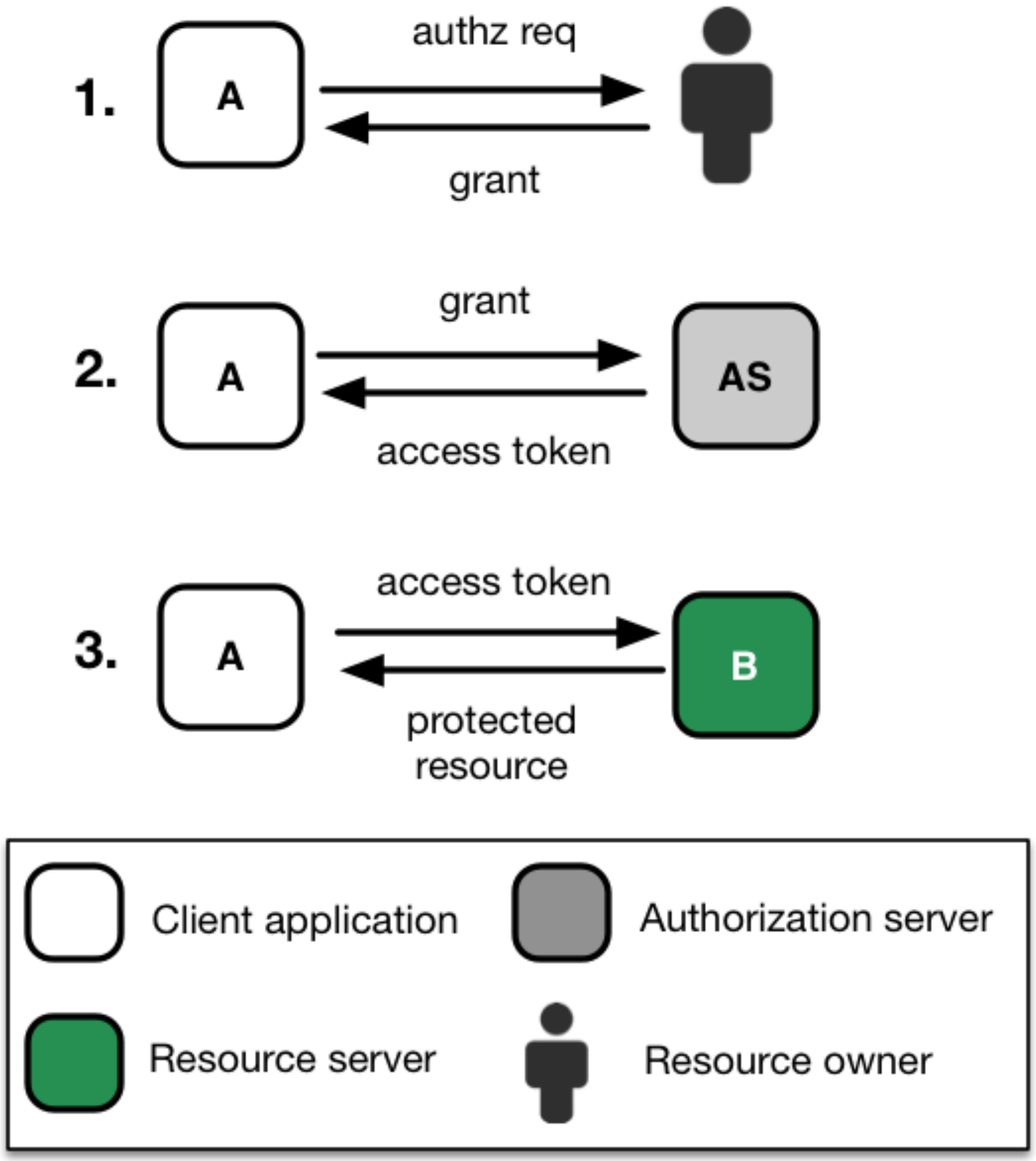
- An application that wants to have access to user resources

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



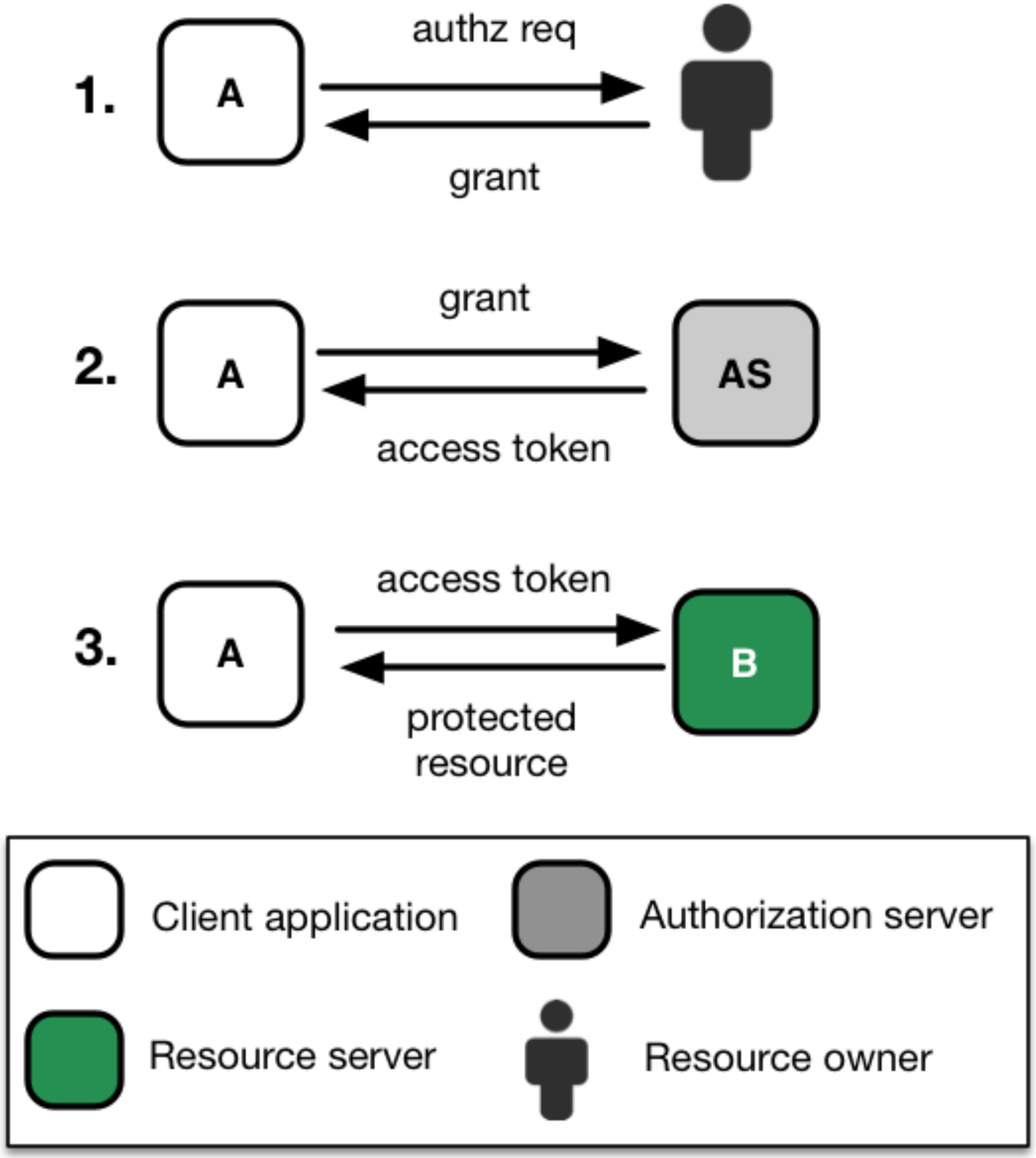
OAuth client registration

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

- https://tools.ietf.org/html/rfc6819#section-5.3

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 provider metadata

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://dodas-iam.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**

OAuth/OpenID Connect provider metadata

```
{
  "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"
  ], ...
```

OAuth/OpenID Connect provider metadata

```
...
  "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"
  ],
...
```

OAuth/OpenID Connect provider metadata

```
{
  "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",
```

OAuth/OpenID Connect provider metadata

```
   "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-OAEP-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",
```

OAuth/OpenID Connect provider metadata

```
  "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",
```

OAuth/OpenID Connect provider metadata

```
"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",
 ...,
```

OAuth/OpenID Connect provider metadata

```
 "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 WebDAV

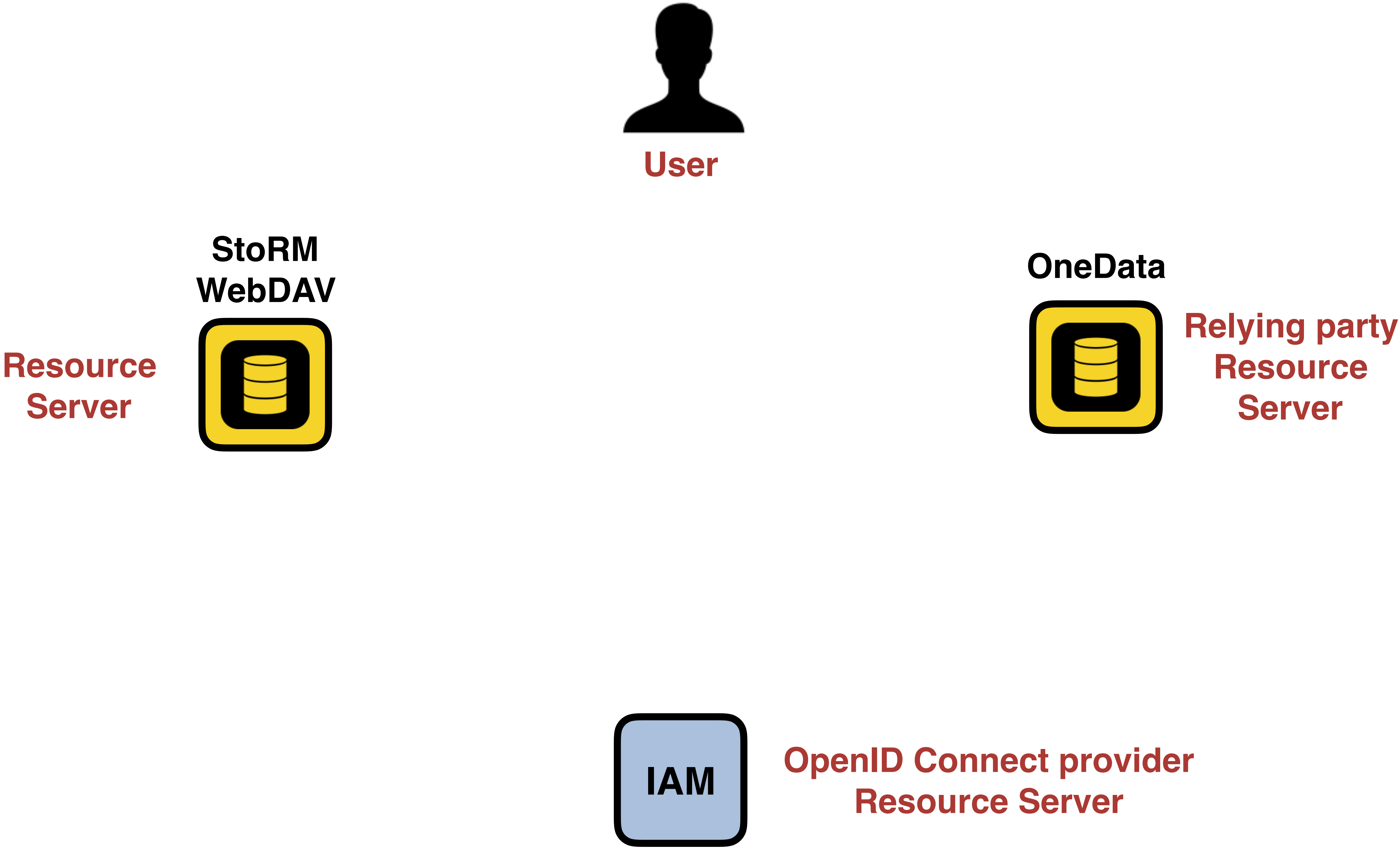
Resource Server

OneData

Client Resource Server

Authorization Server Resource Server

IAM, relying parties & OpenID Connect roles



User

StoRM WebDAV

Resource Server

OneData

Relying party
Resource
Server

IAM

OpenID Connect provider
Resource Server

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 eyJraWQiOiJy…rYI
User-Agent: curl/7.65.3
Accept: */*
```

OAuth bearer token usage

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

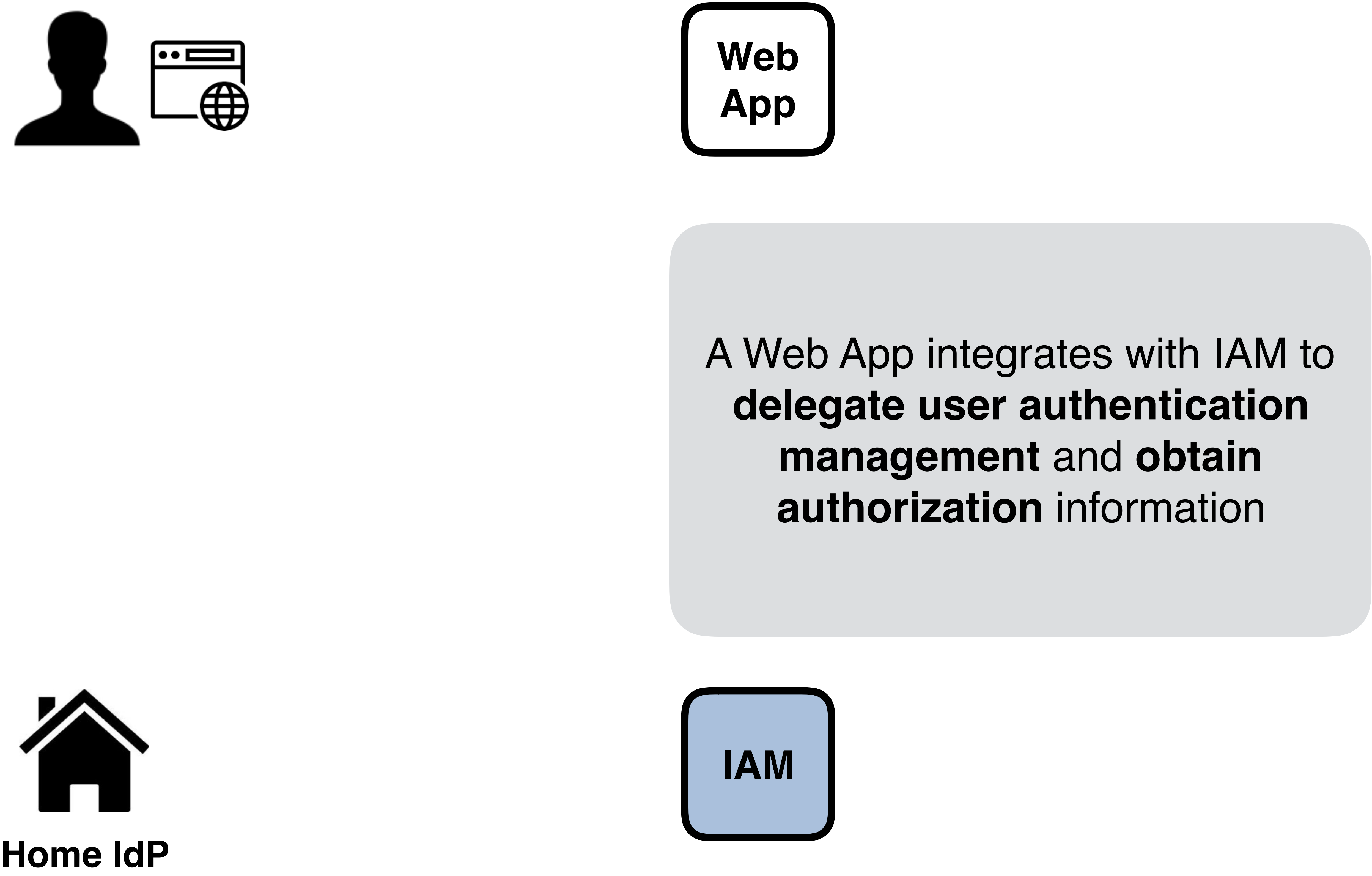
Typically, tokens are sent in the `Authorization` HTTP header, following the rules defined in RFC 6750, as in the following example HTTP request

The token!

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

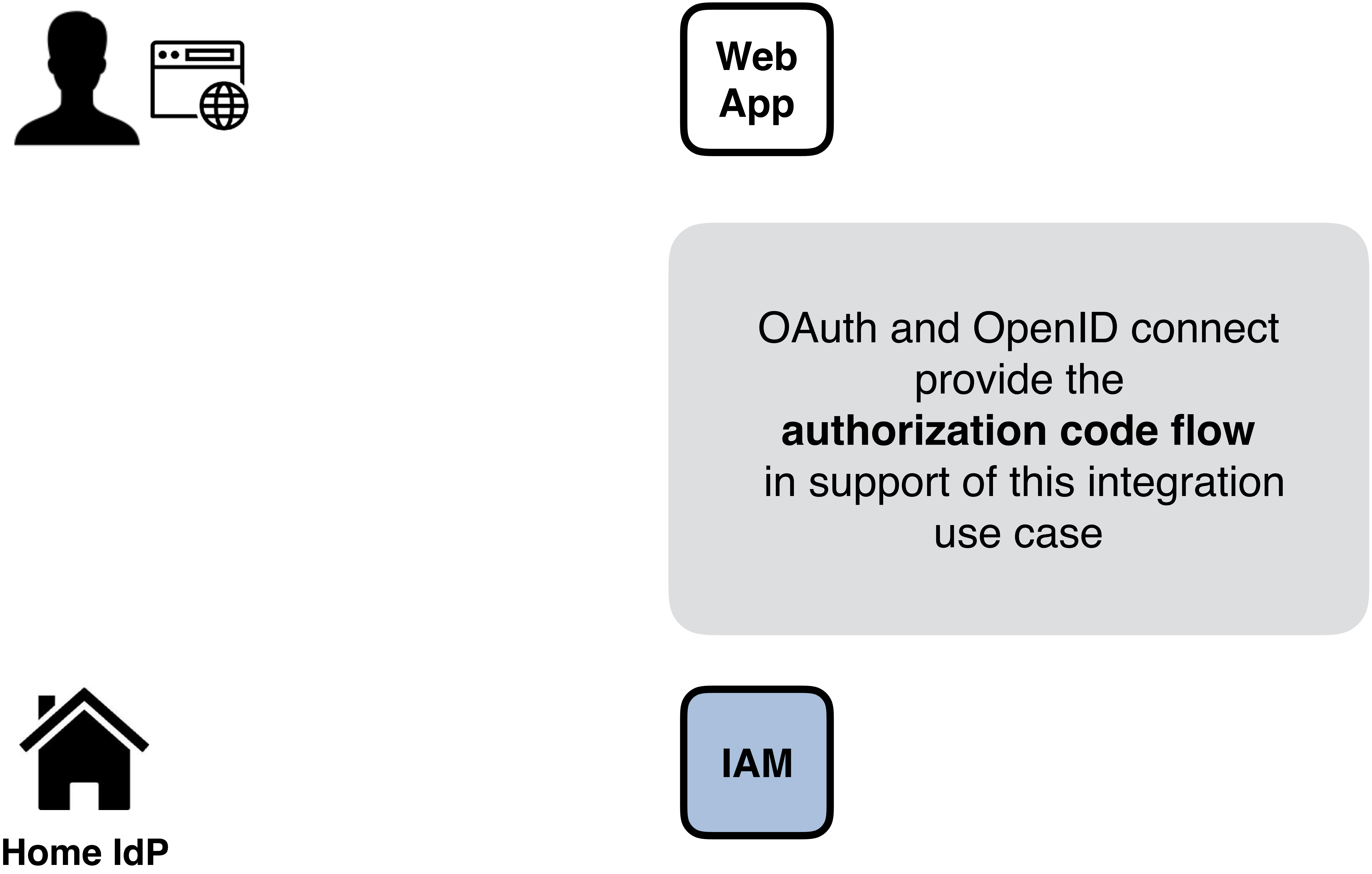
Web application integration scenario

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



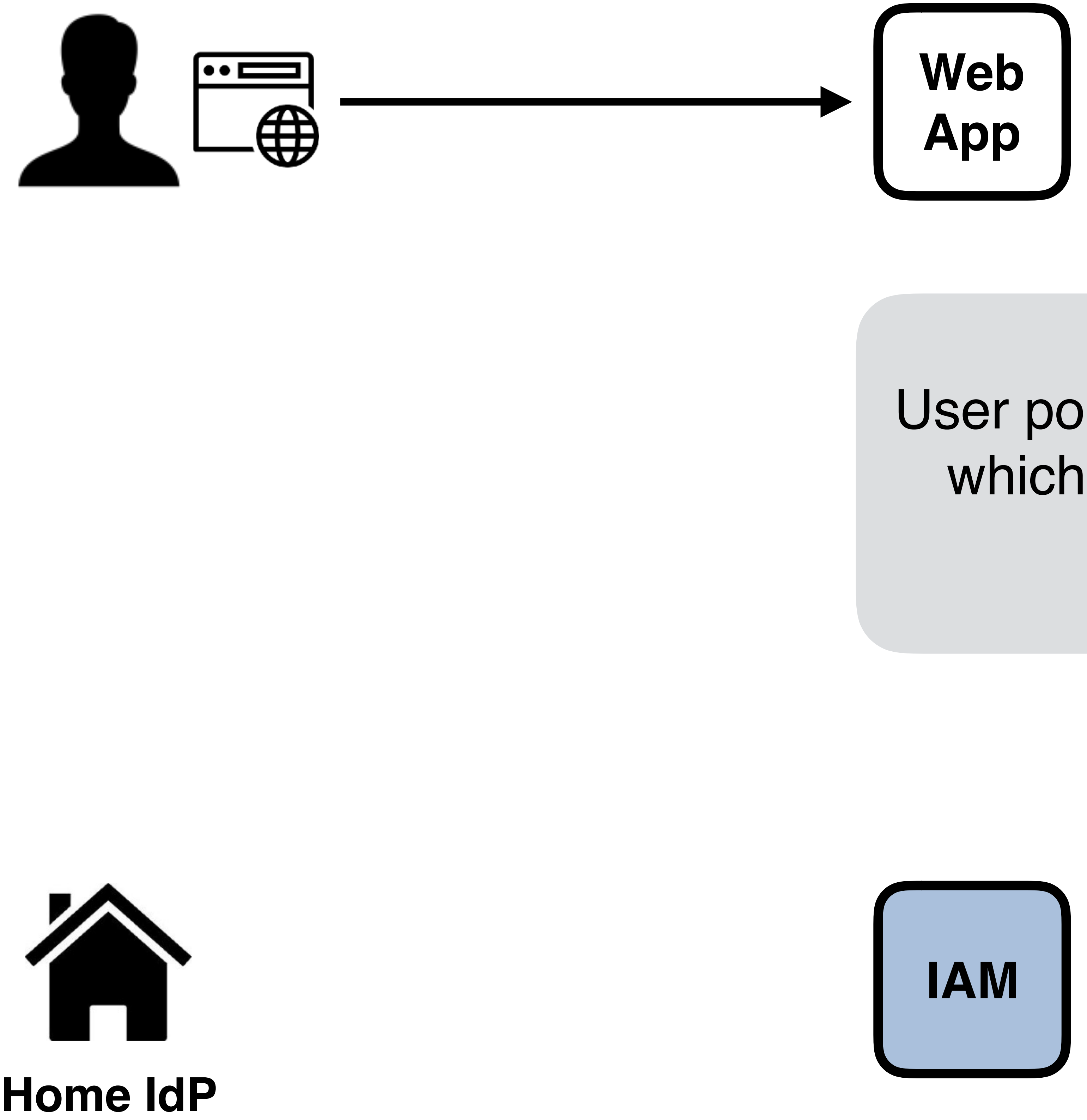
Web App

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

Home IdP

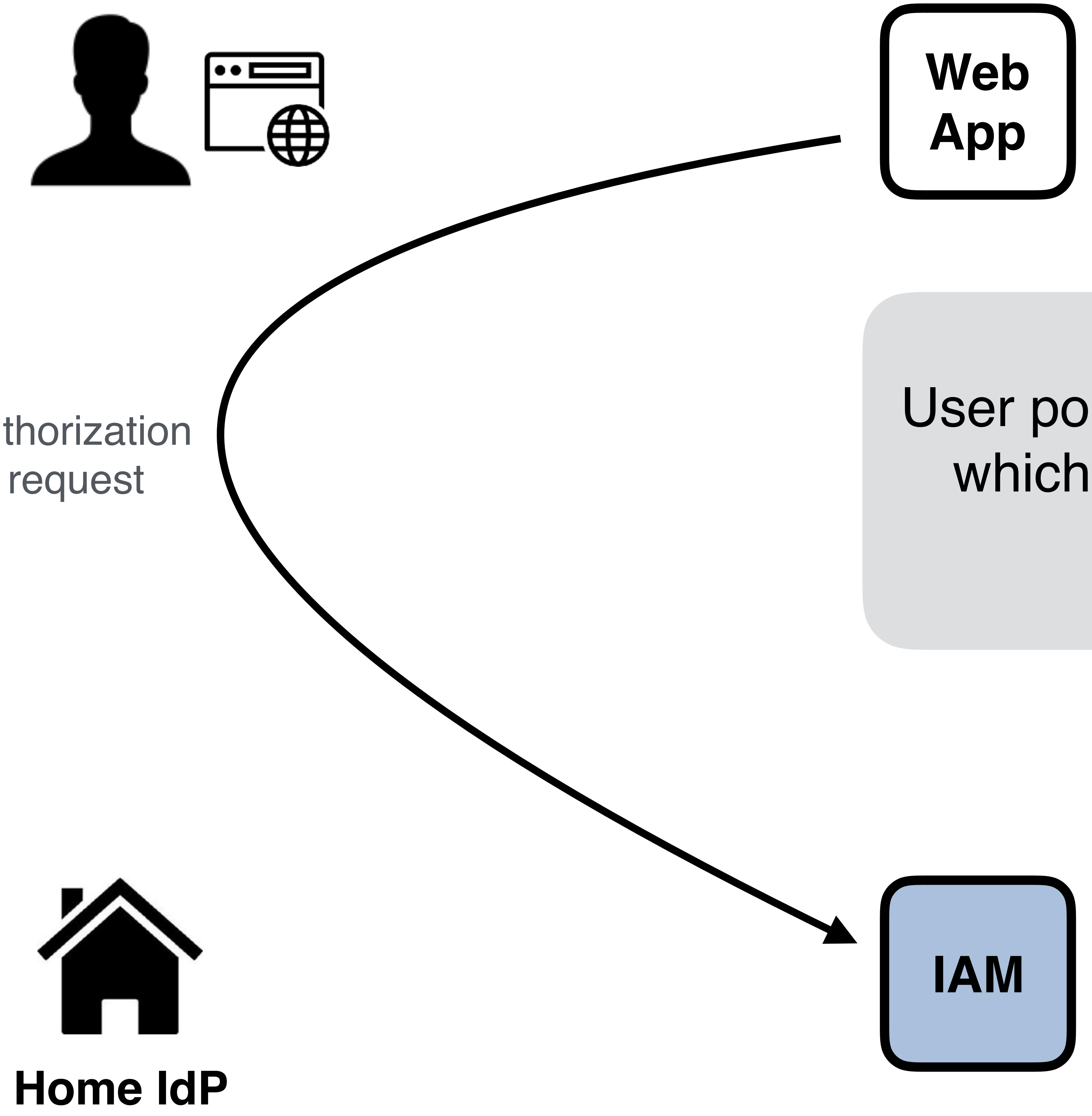
IAM

Authorization code flow



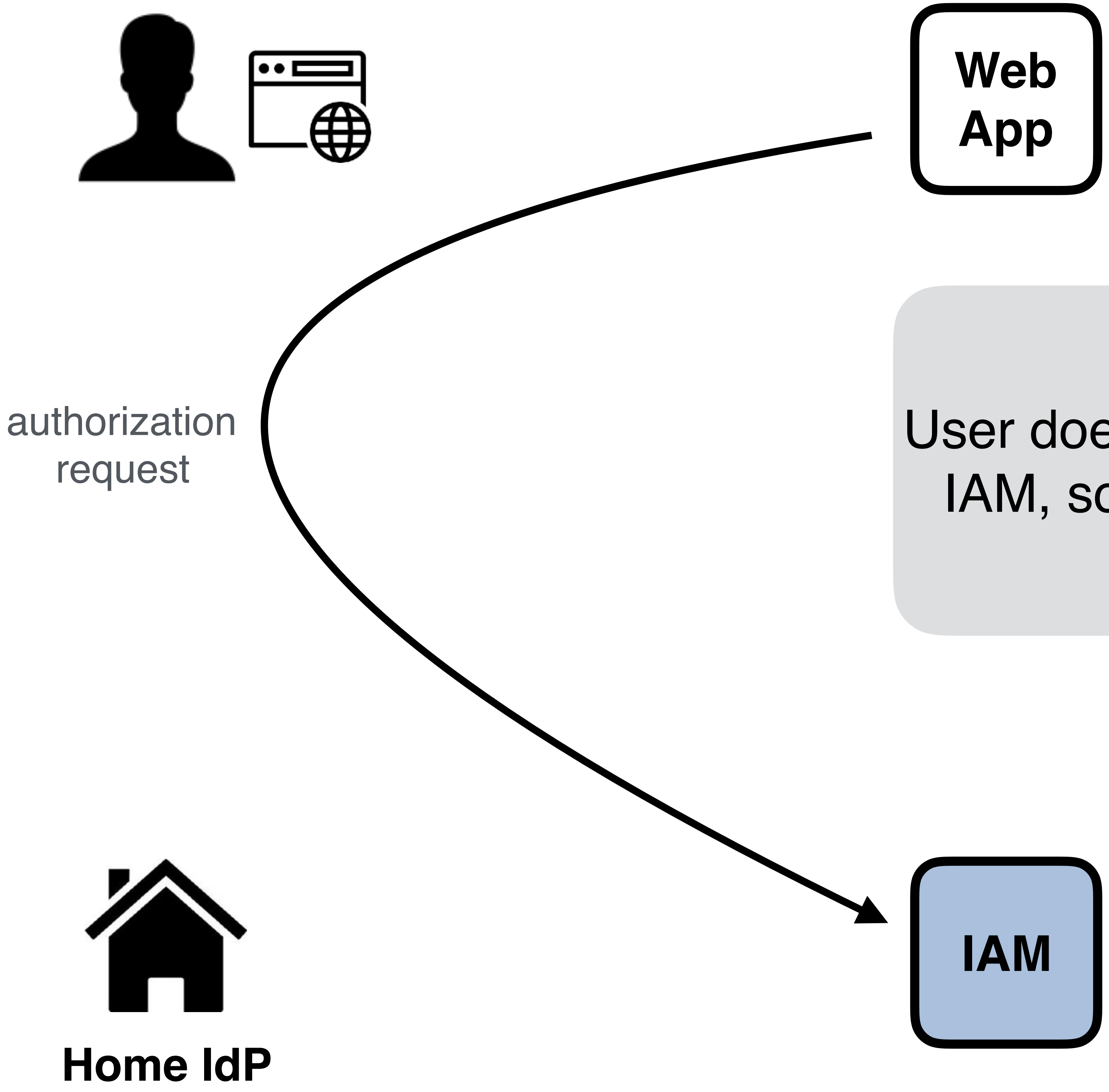
User points its browser to web app, which redirects back to IAM for authentication

Authorization code flow



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

Authorization code flow



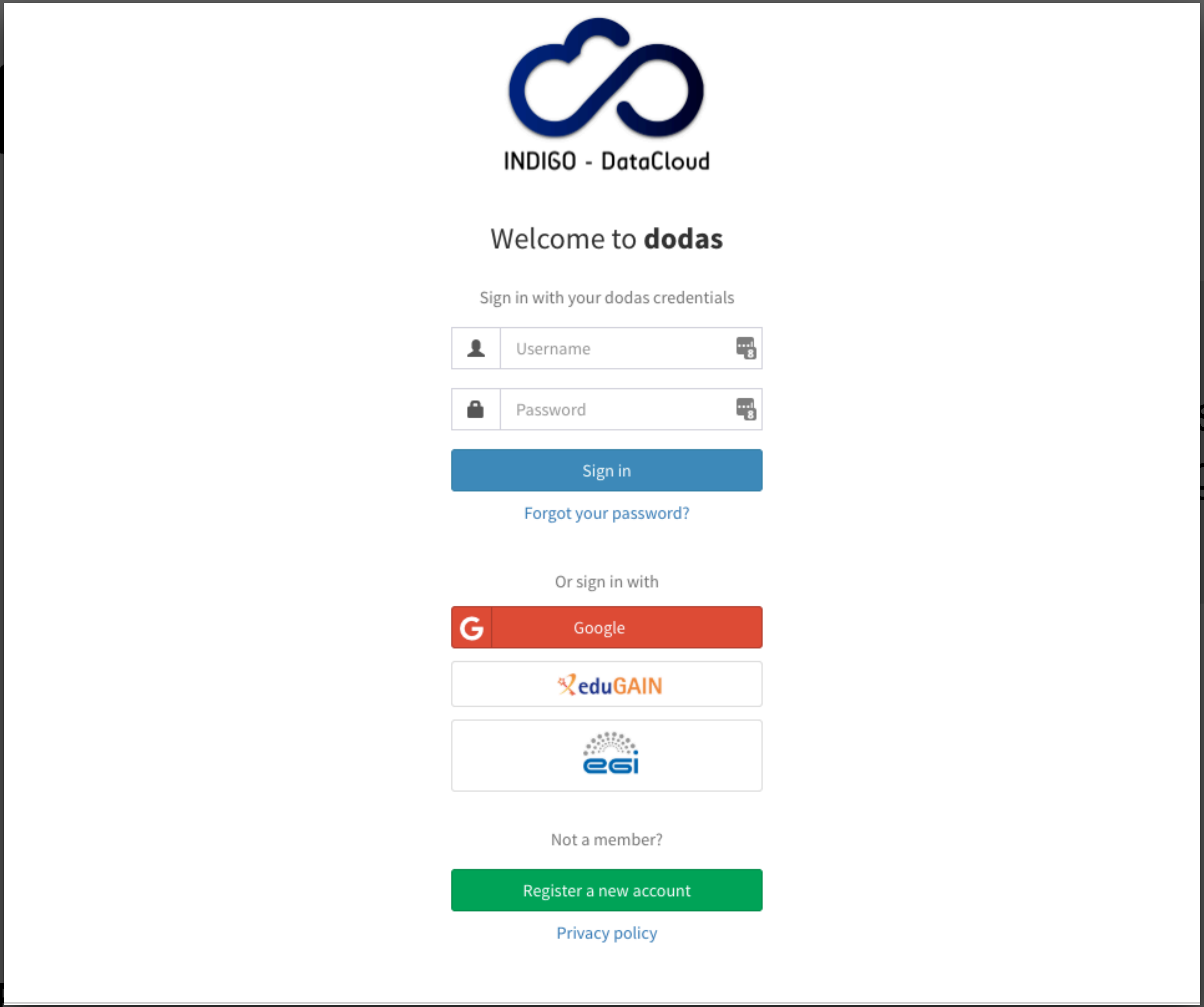
User does not have a valid session at IAM, so IAM shows the login page

Authorization code flow

authorization request

session at
gin page

Home Id



Welcome to **dodas**

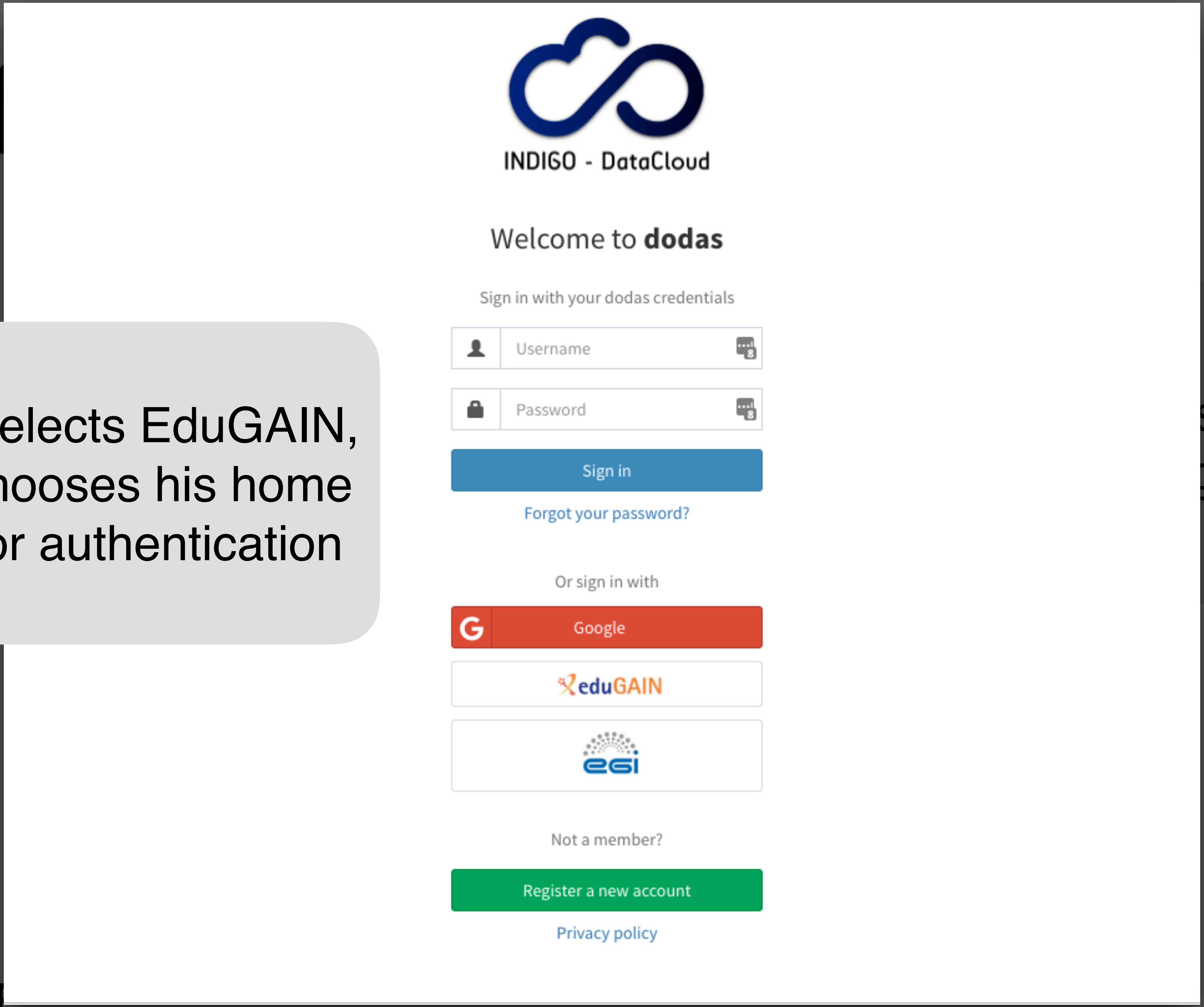
Sign in with your dodas credentials

Or sign in with

Not a member?

Authorization code flow

auth
r



INDIGO - DataCloud

Welcome to **dodas**

Sign in with your dodas credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

Google

eduGAIN

egi

Not a member?

Register a new account

Privacy policy

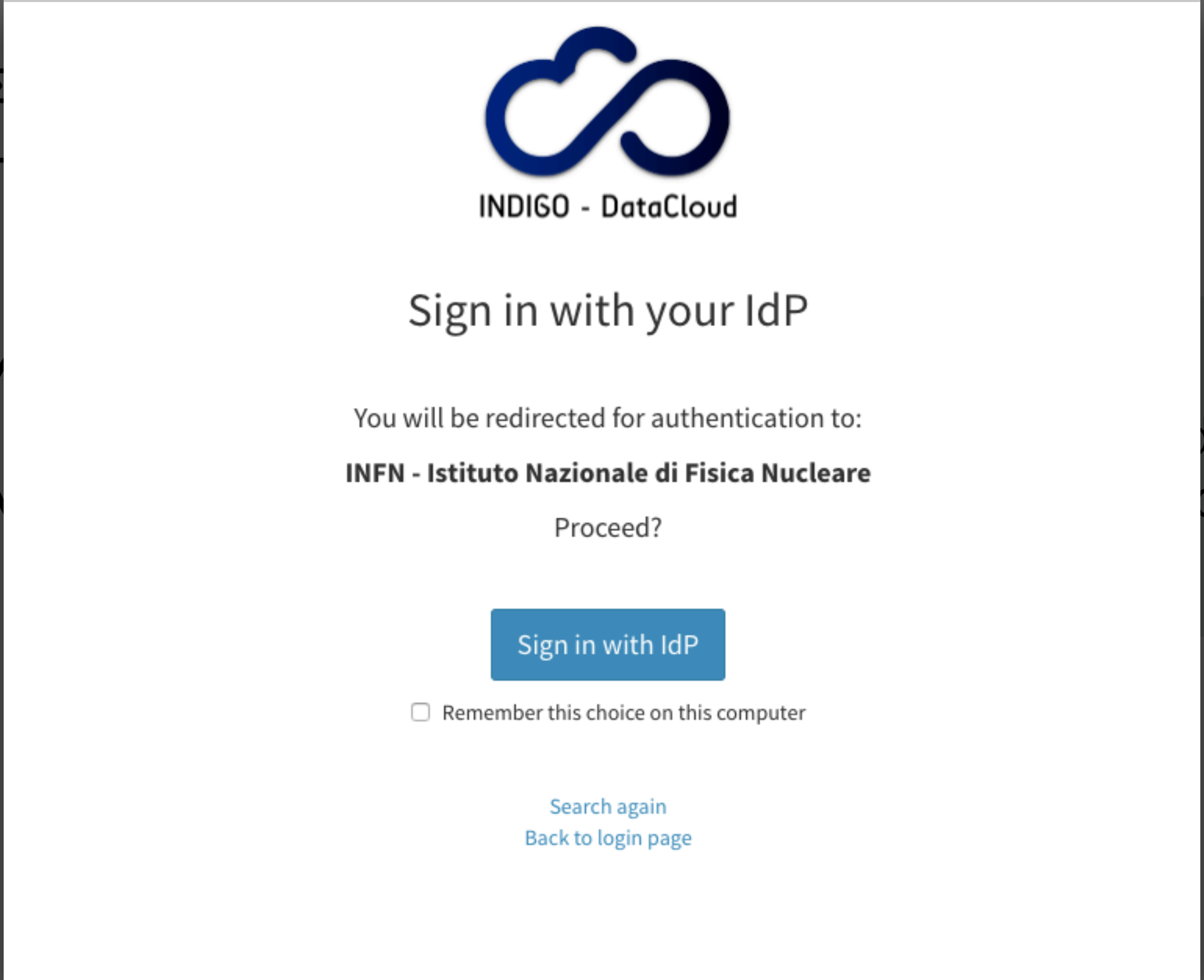
User selects EduGAIN, and chooses his home IDP for authentication

session at
gin page

Home IdI

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?

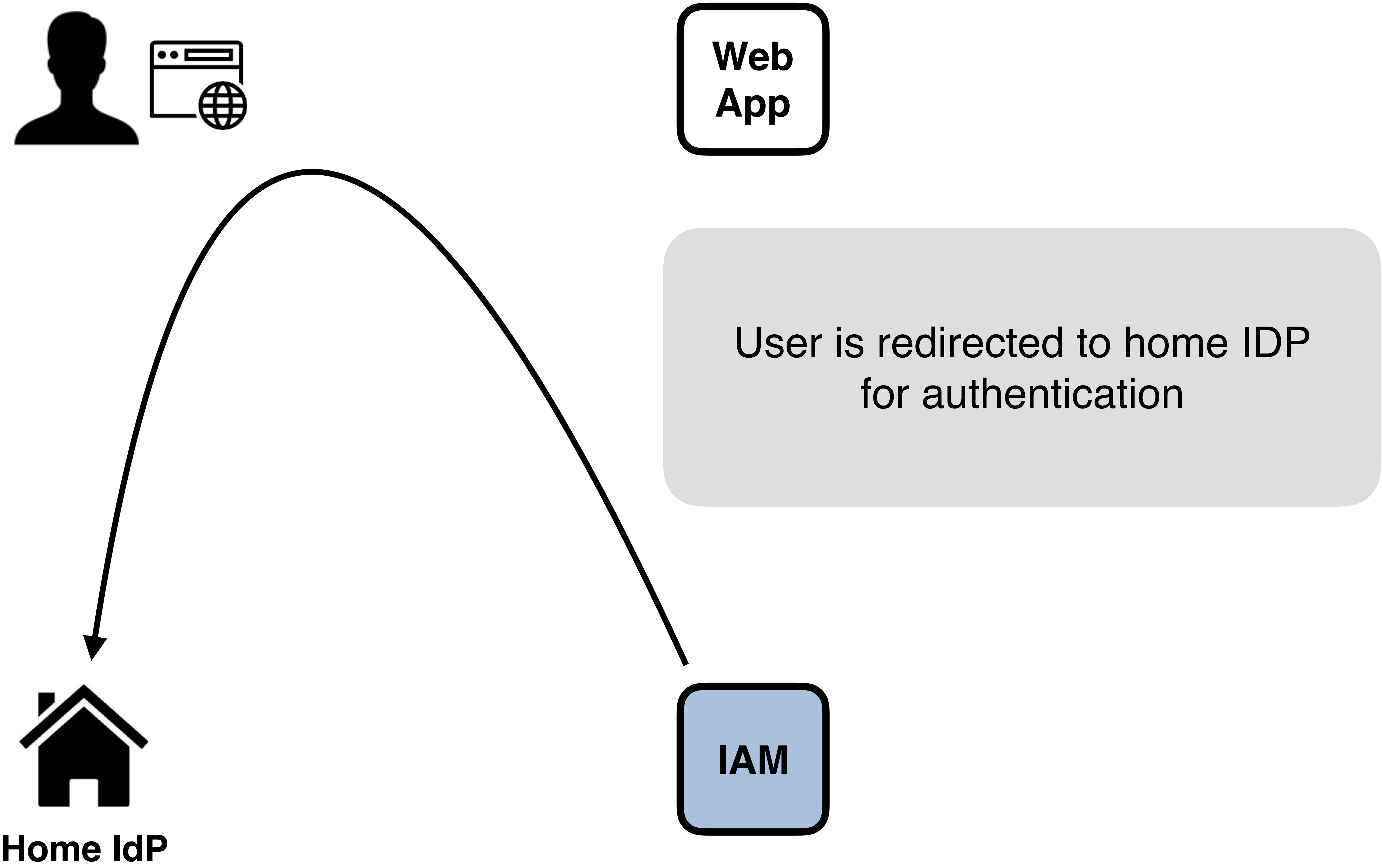
□ Remember this choice on this computer

session at

ogin page

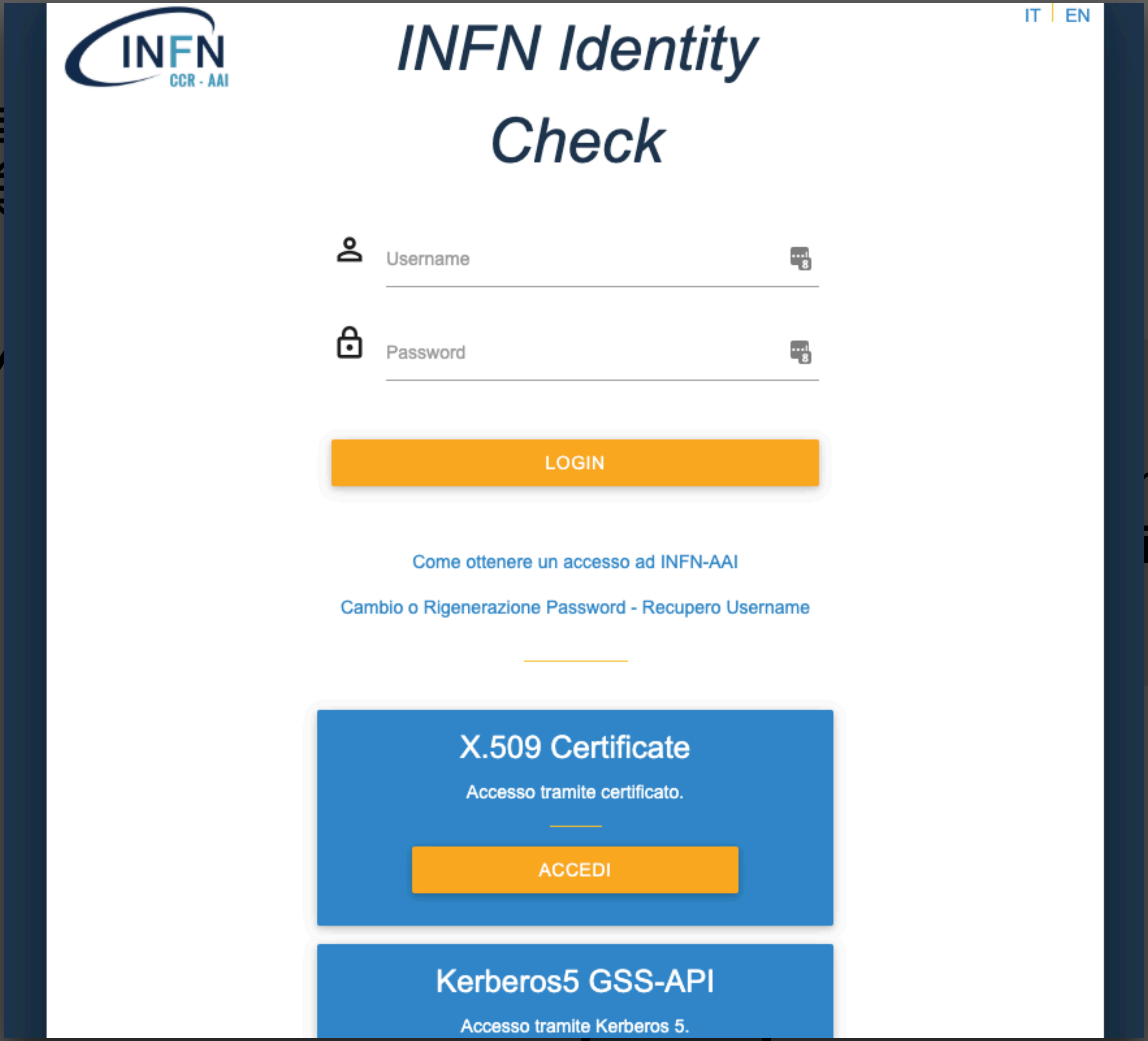
Home IdP

Authorization code flow



User is redirected to home IDP for authentication

Authorization code flow



INFN Identity Check

Username

Password

LOGIN

Come ottenere un accesso ad INFN-AAI

Cambio o Rigenerazione Password - Recupero Username

X.509 Certificate

Accesso tramite certificato.

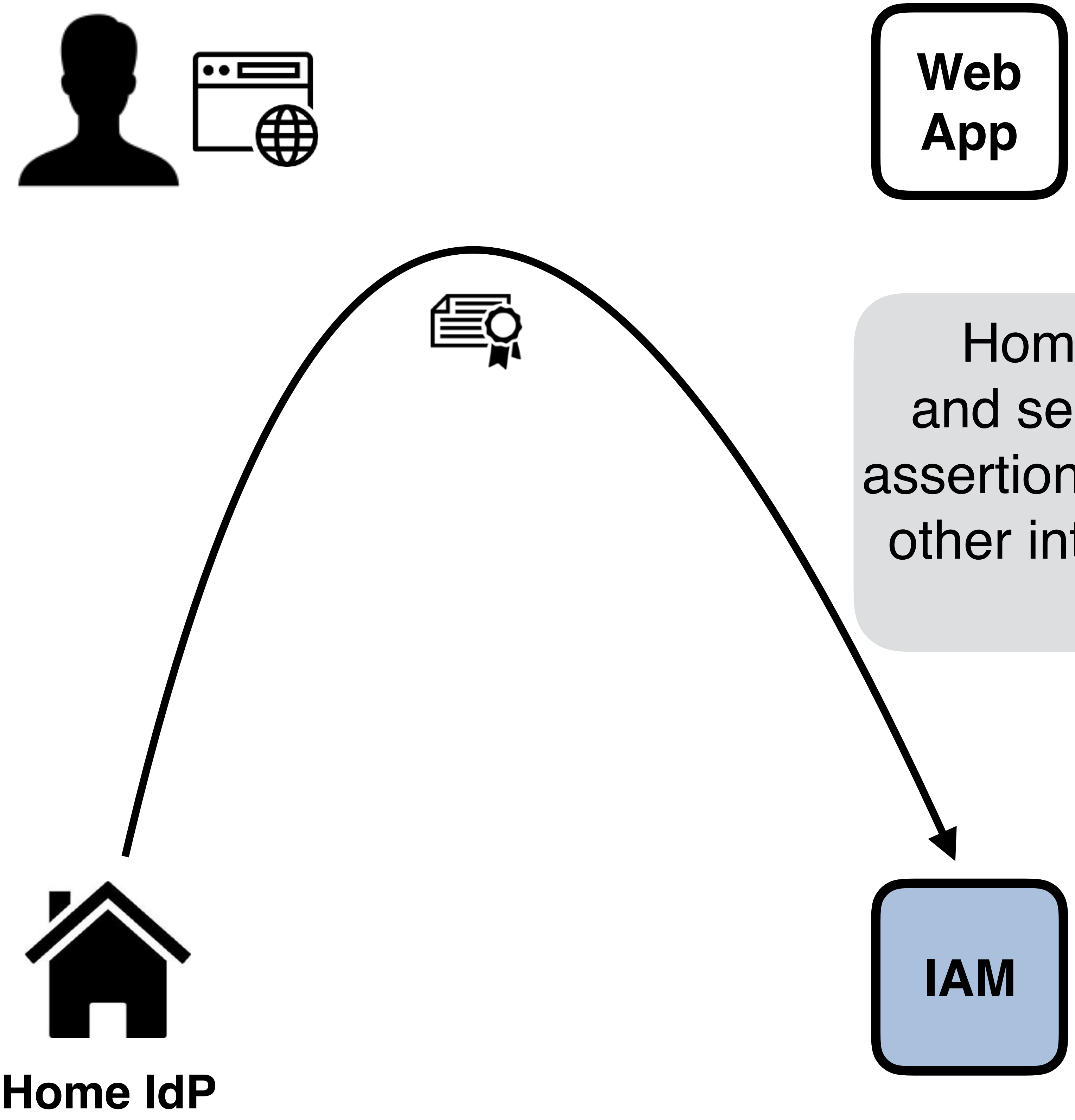
ACCEDI

Kerberos5 GSS-API

Accesso tramite Kerberos 5.

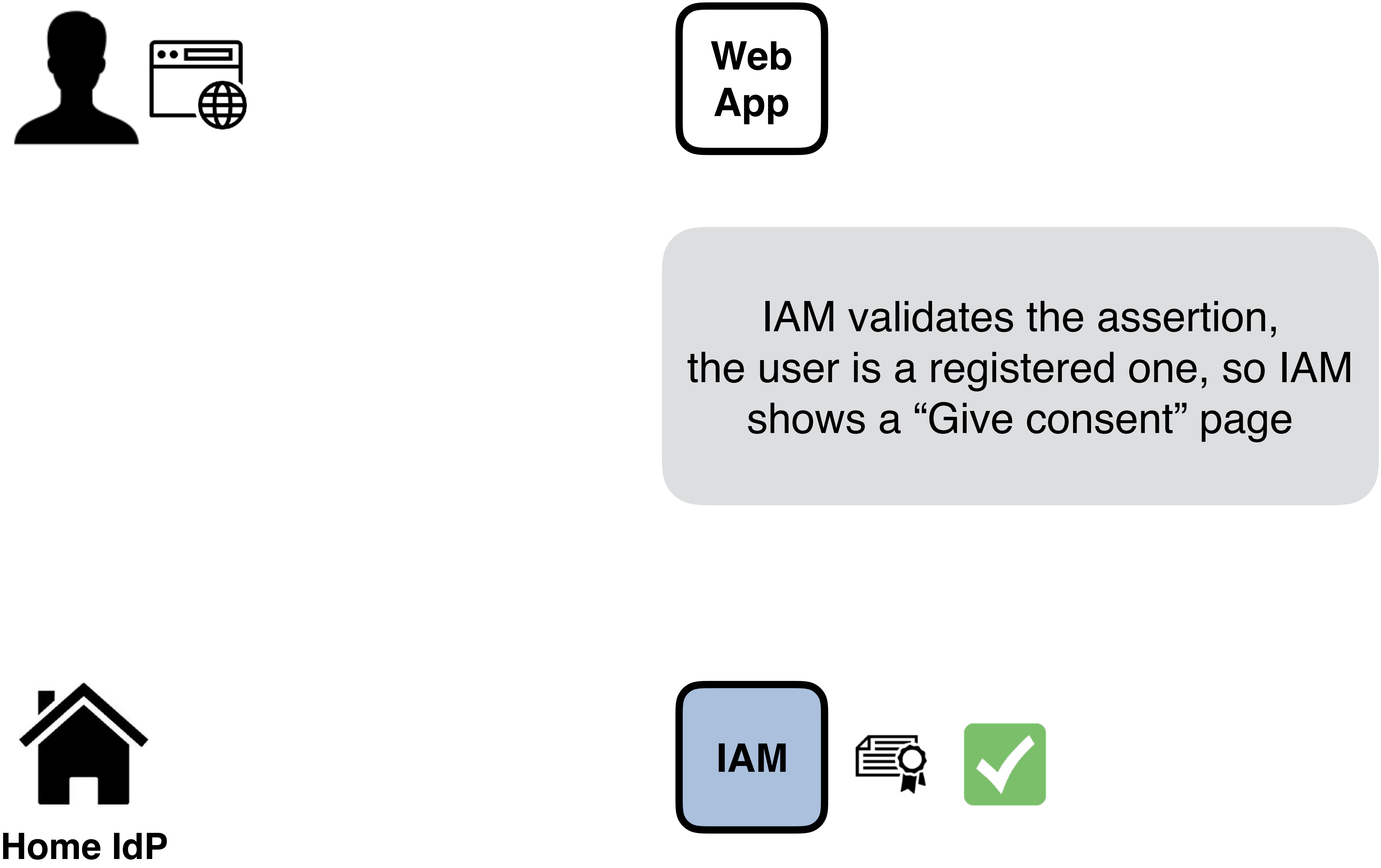
ome IDP
ion

Authorization code flow



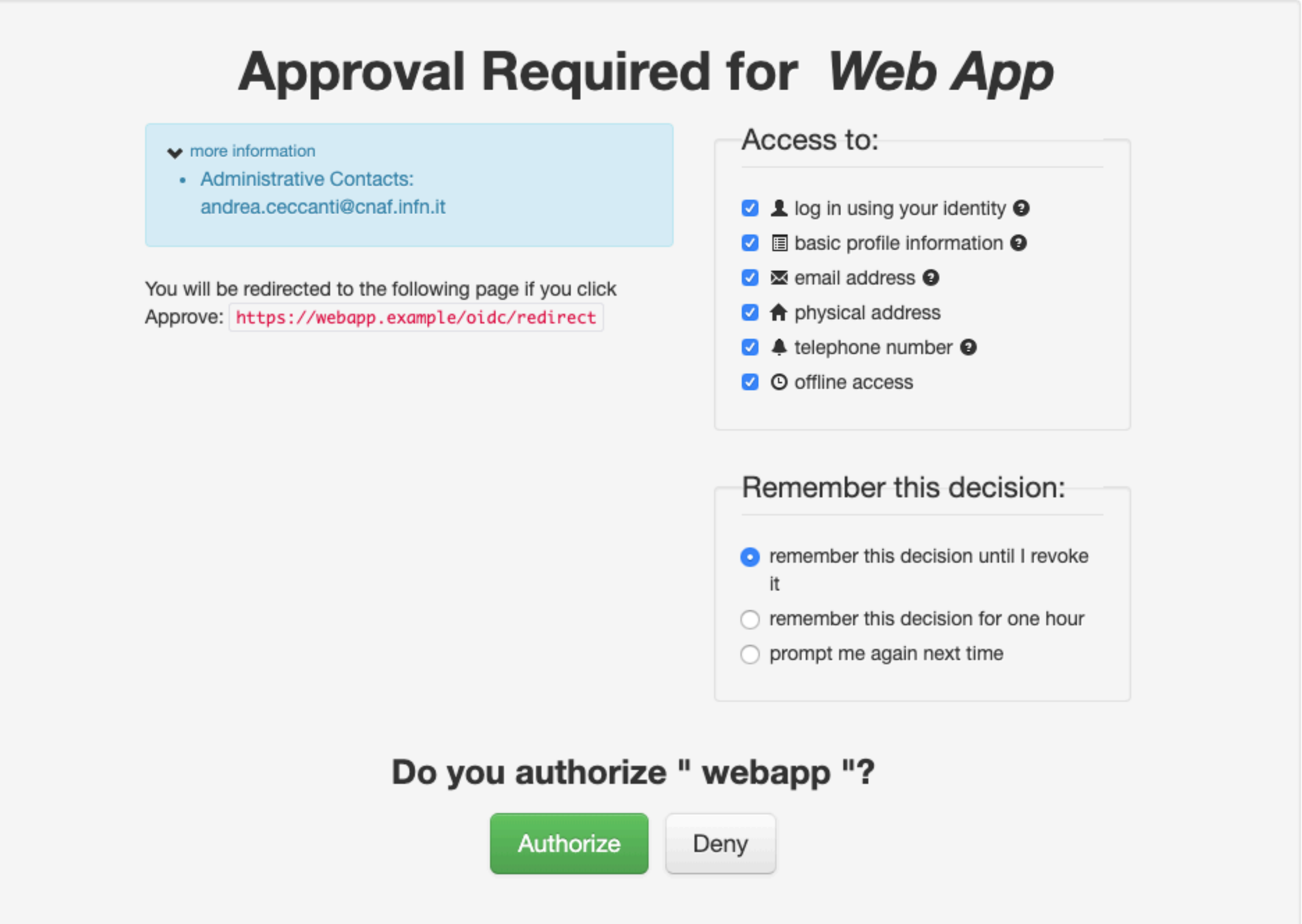
Home IDP authenticates user and sends back an authentication assertion, via redirection and possibly other interactions between IAM and the IDP

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

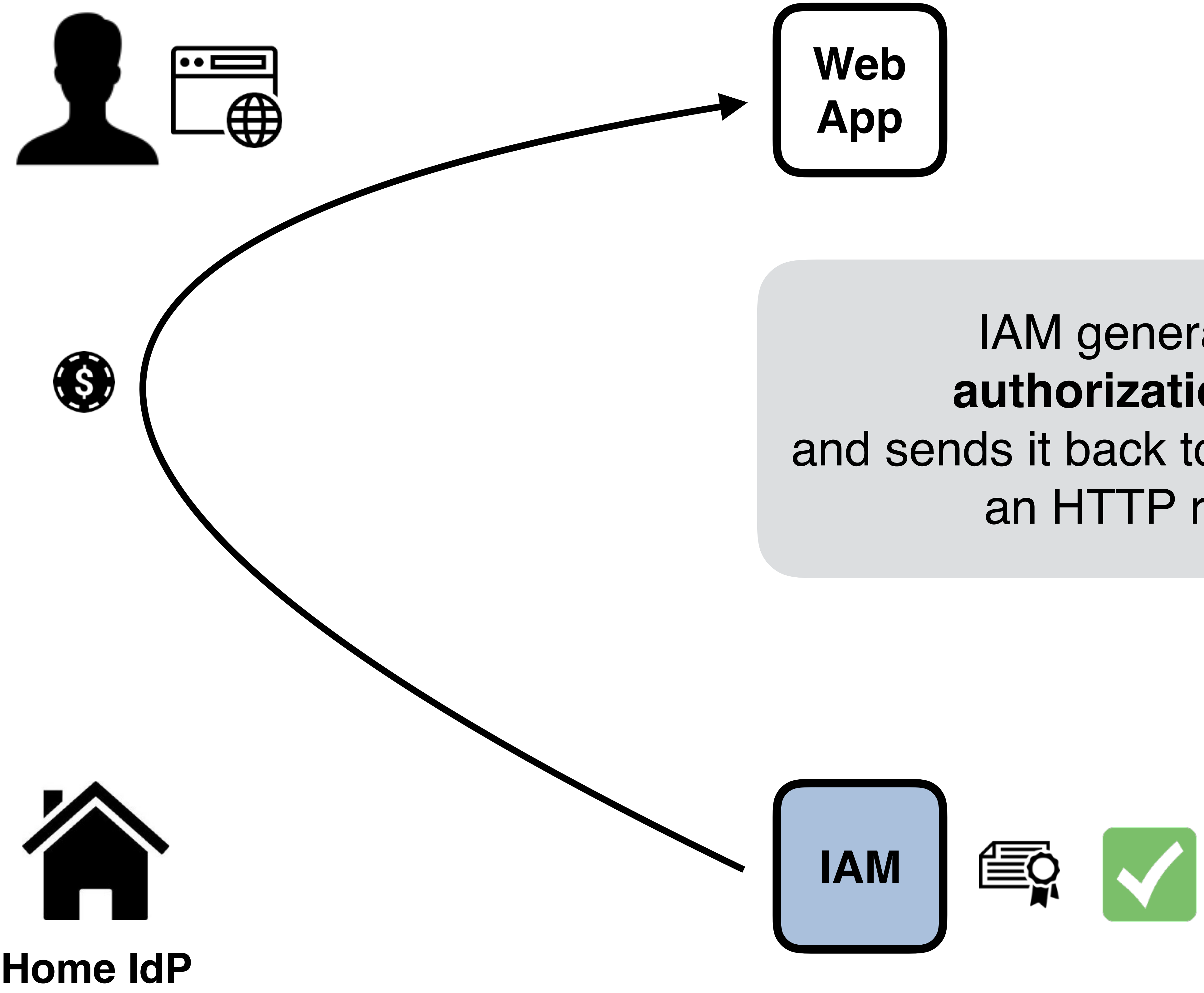
Do you authorize " webapp "?

tion,
, so IAM
page

IAM

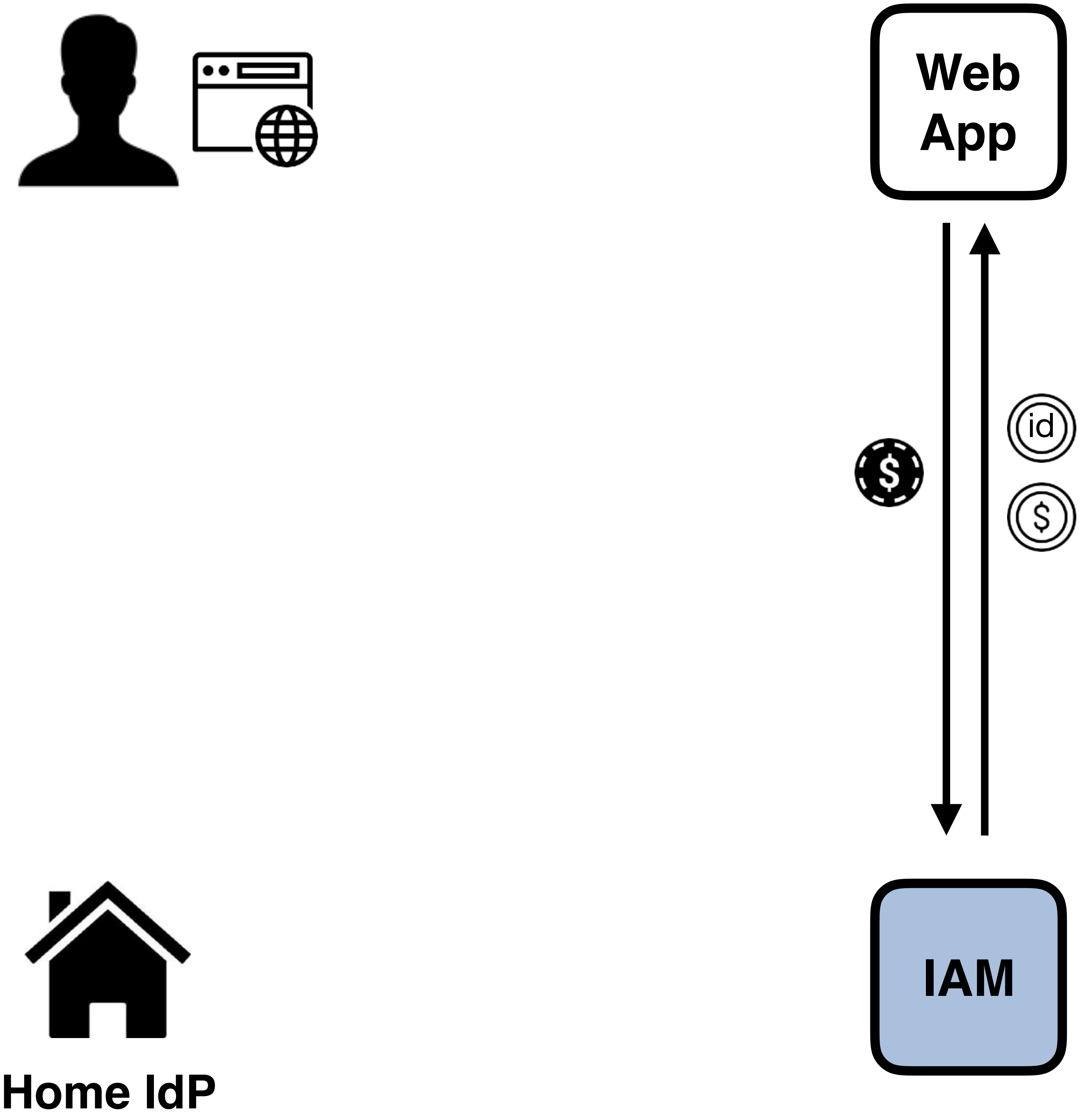
Home IdP

Authorization code flow



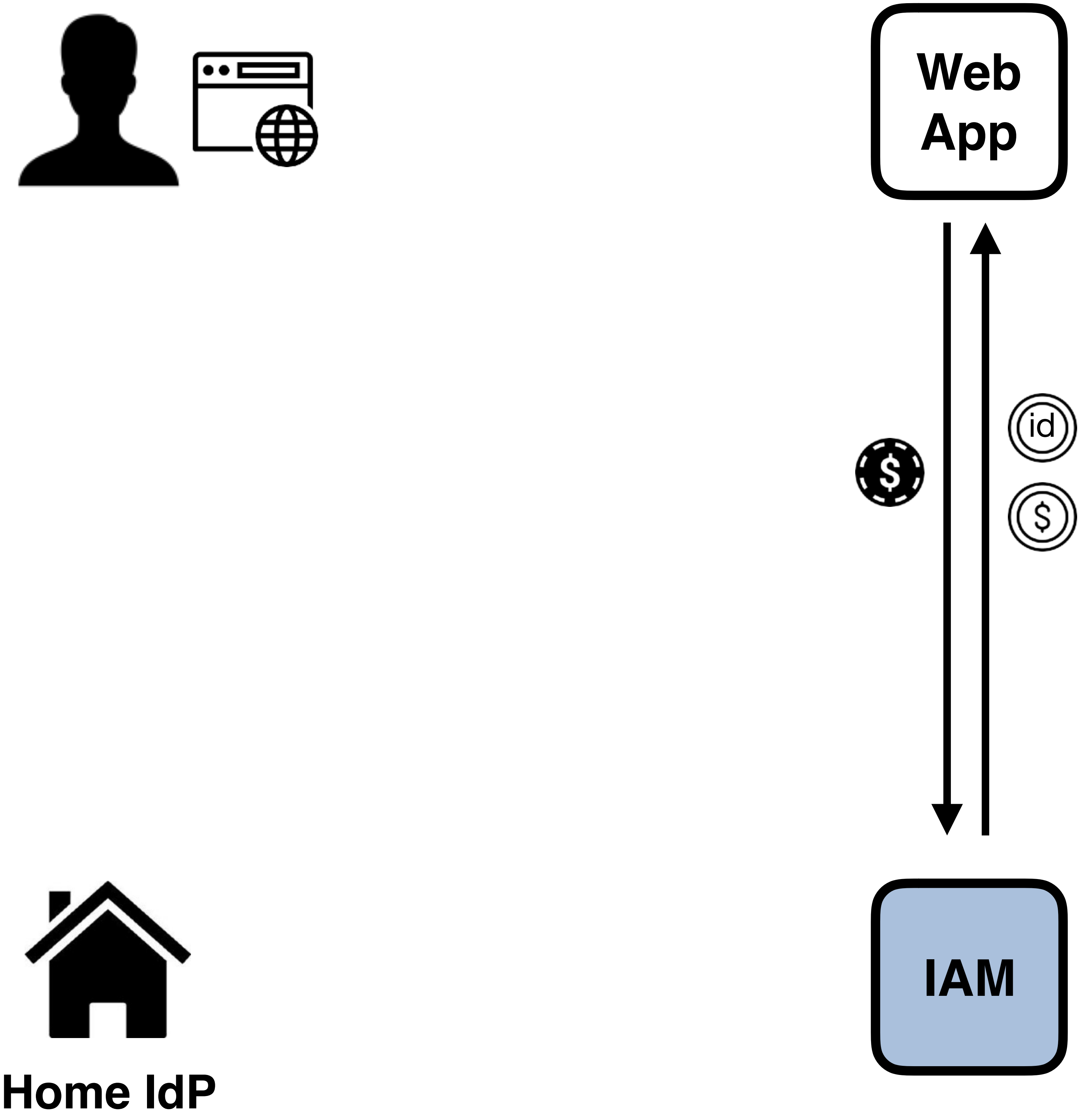
IAM generates an
authorization code
and sends it back to web app using
an HTTP redirect

Authorization code flow



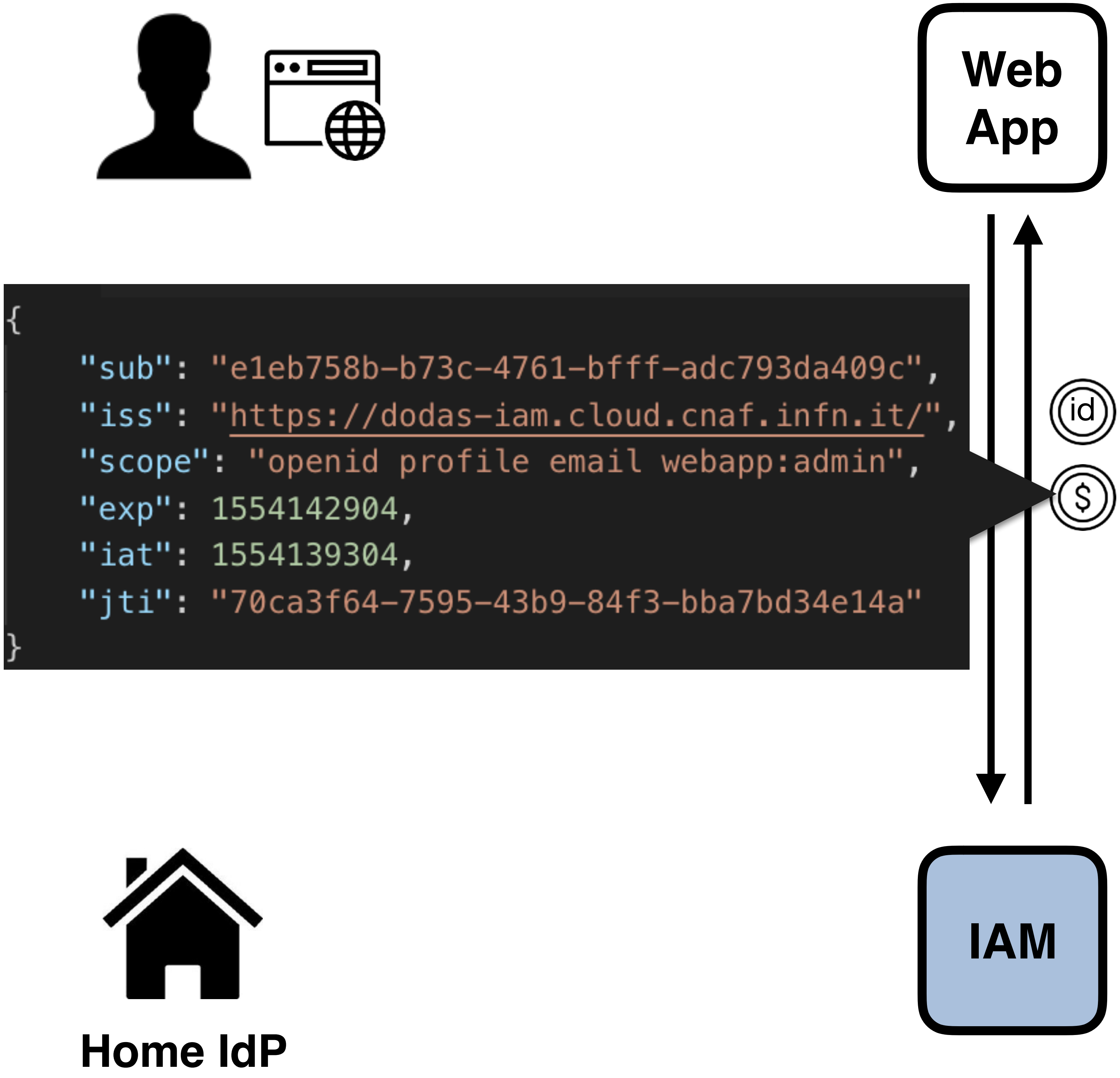
The Web App exchanges the **authorization code** with a couple of tokens: an **access token** and an **id token**

Authorization code flow



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

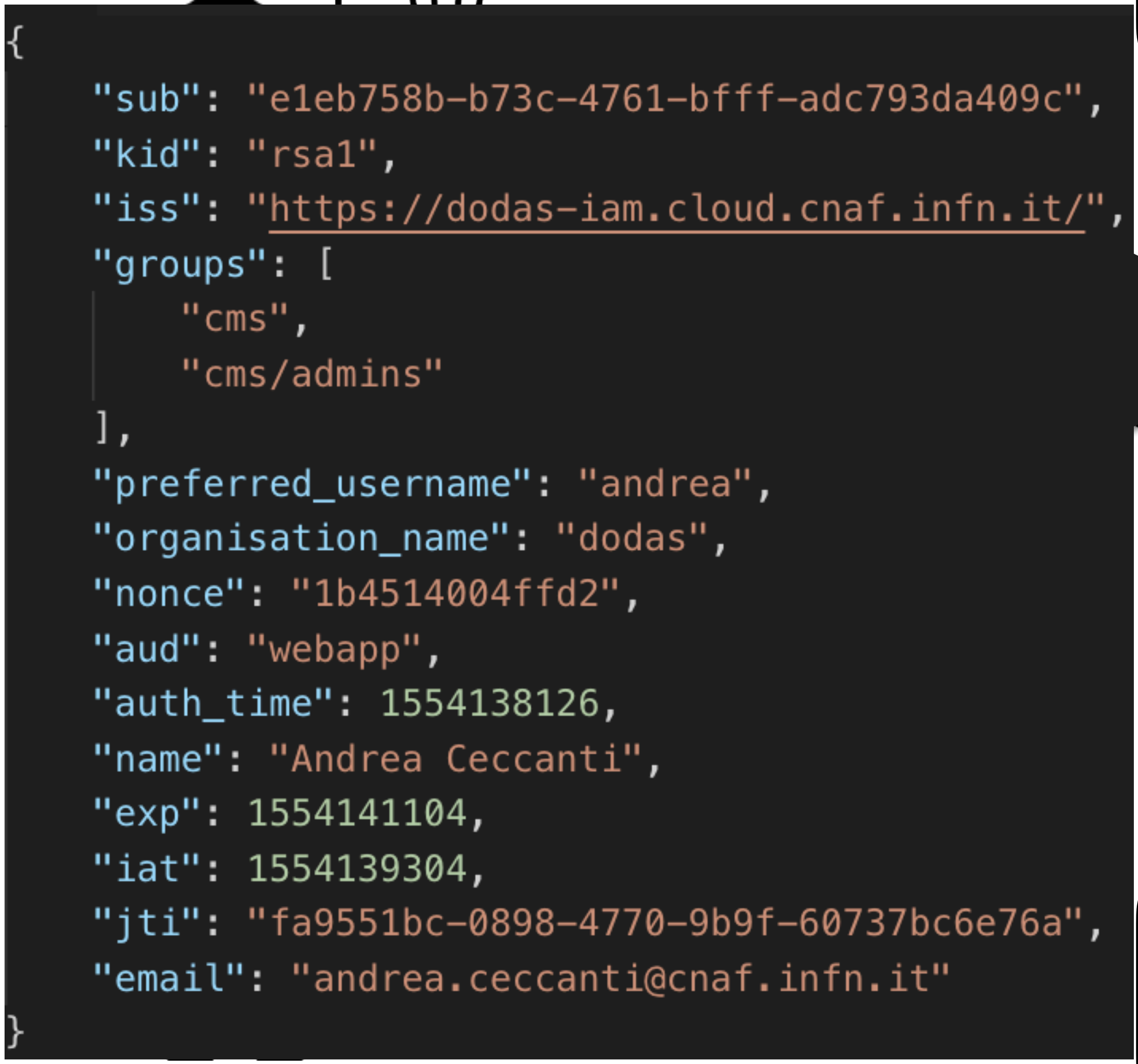
Authorization code flow



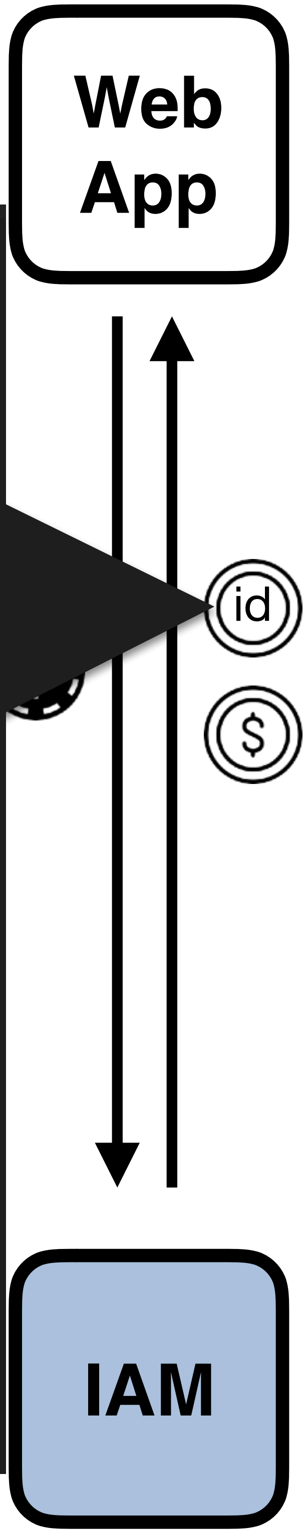
```
{
    "sub": "e1eb758b-b73c-4761-bfff-adc793da409c",
    "iss": "https://dodas-iam.cloud.cnaf.infn.it/",
    "scope": "openid profile email webapp:admin",
    "exp": 1554142904,
    "iat": 1554139304,
    "jti": "70ca3f64-7595-43b9-84f3-bba7bd34e14a"
}
```

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

Authorization code flow



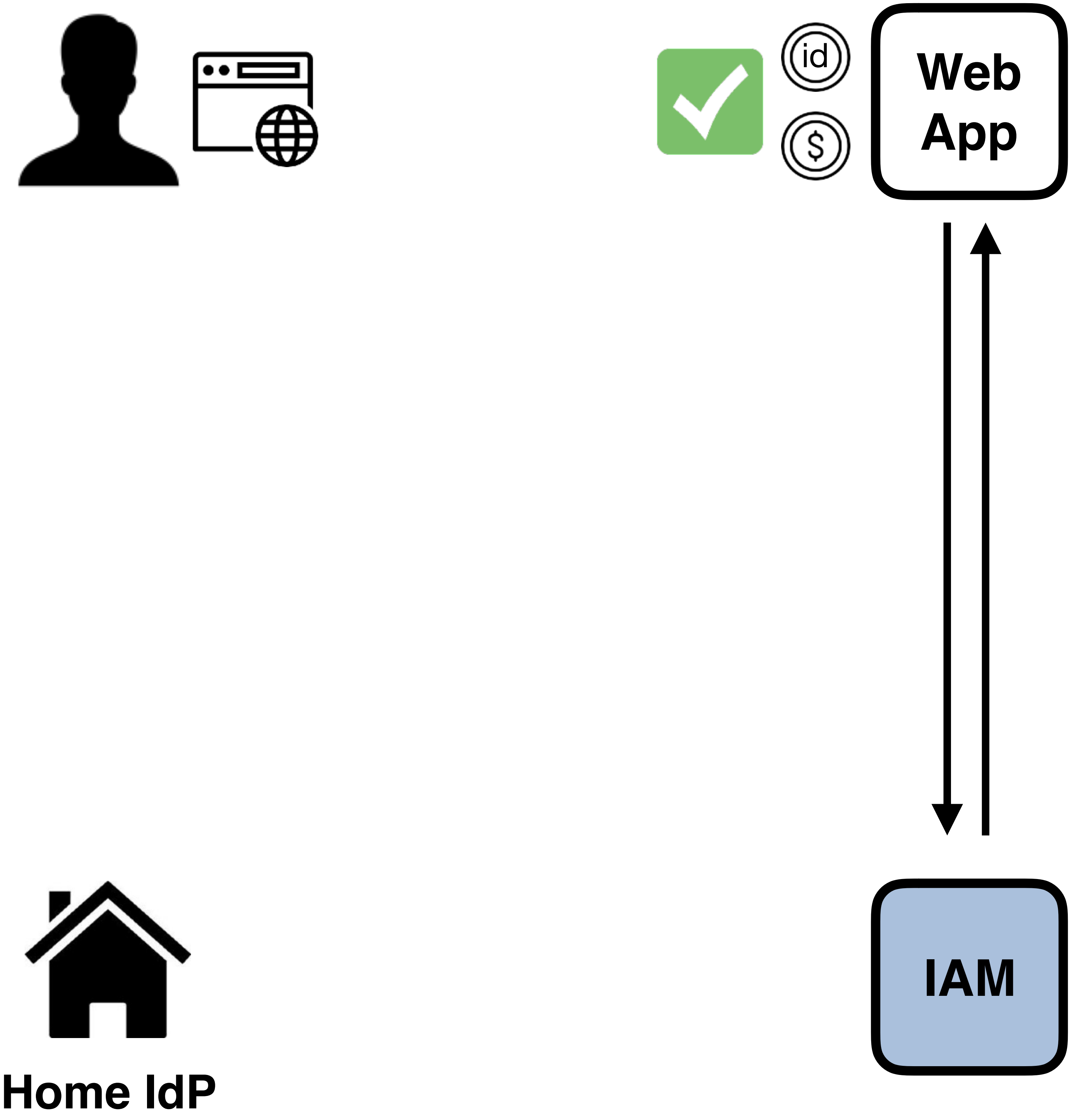
```
{
    "sub": "e1eb758b-b73c-4761-bfff-adc793da409c",
    "kid": "rsa1",
    "iss": "https://dodas-iam.cloud.cnaf.infn.it/",
    "groups": [
        "cms",
        "cms/admins"
    ],
    "preferred_username": "andrea",
    "organisation_name": "dodas",
    "nonce": "1b4514004ffd2",
    "aud": "webapp",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



Home IdP

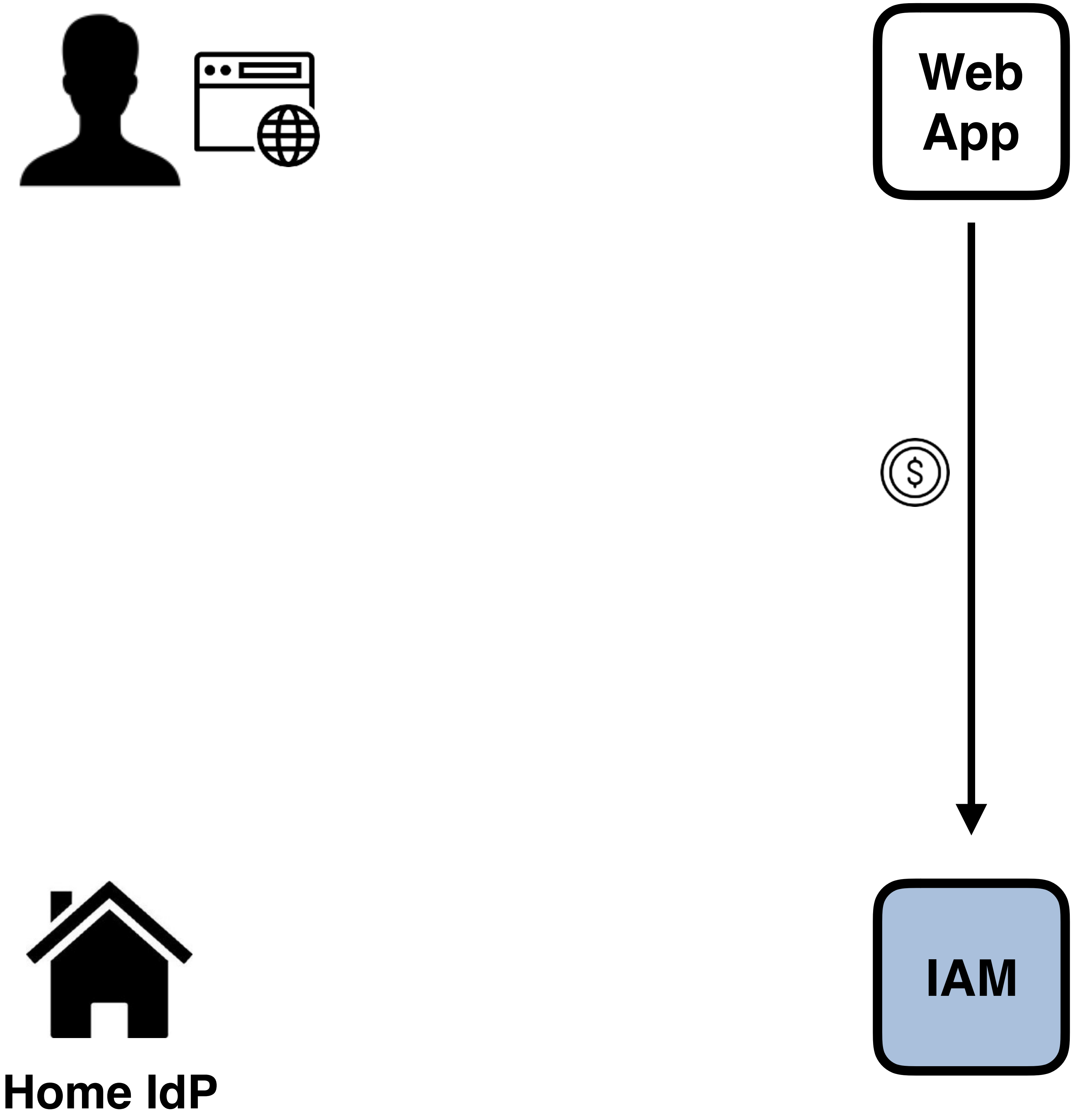
The **id token** provides (mainly) authentication information

Authorization code flow



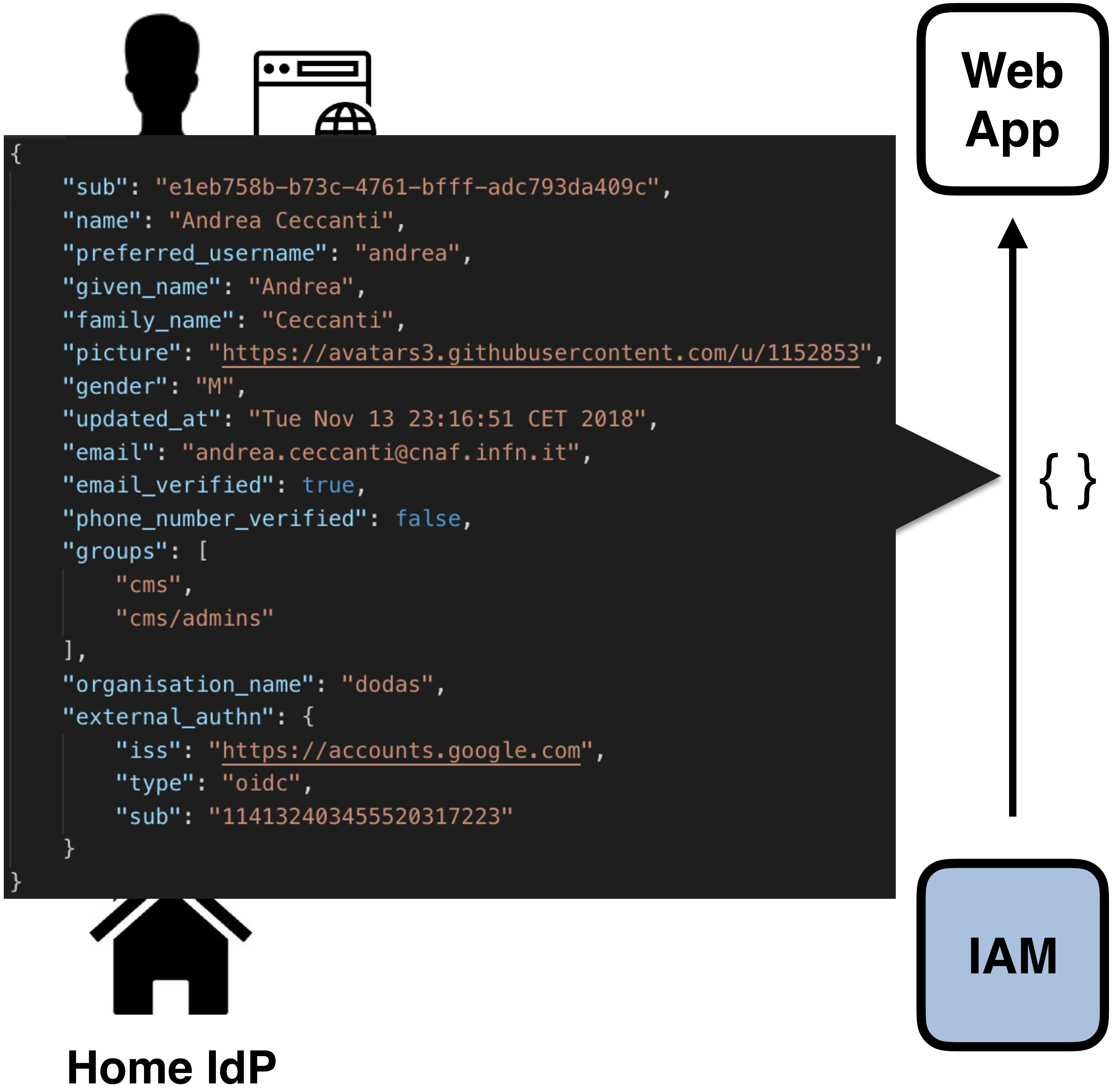
Both tokens are **validated** following to the OpenID Connect guidelines, checking **temporal validity**, **token signature**, **audience**, etc…

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



```json
{
    "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

Authorization code flow in practice

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

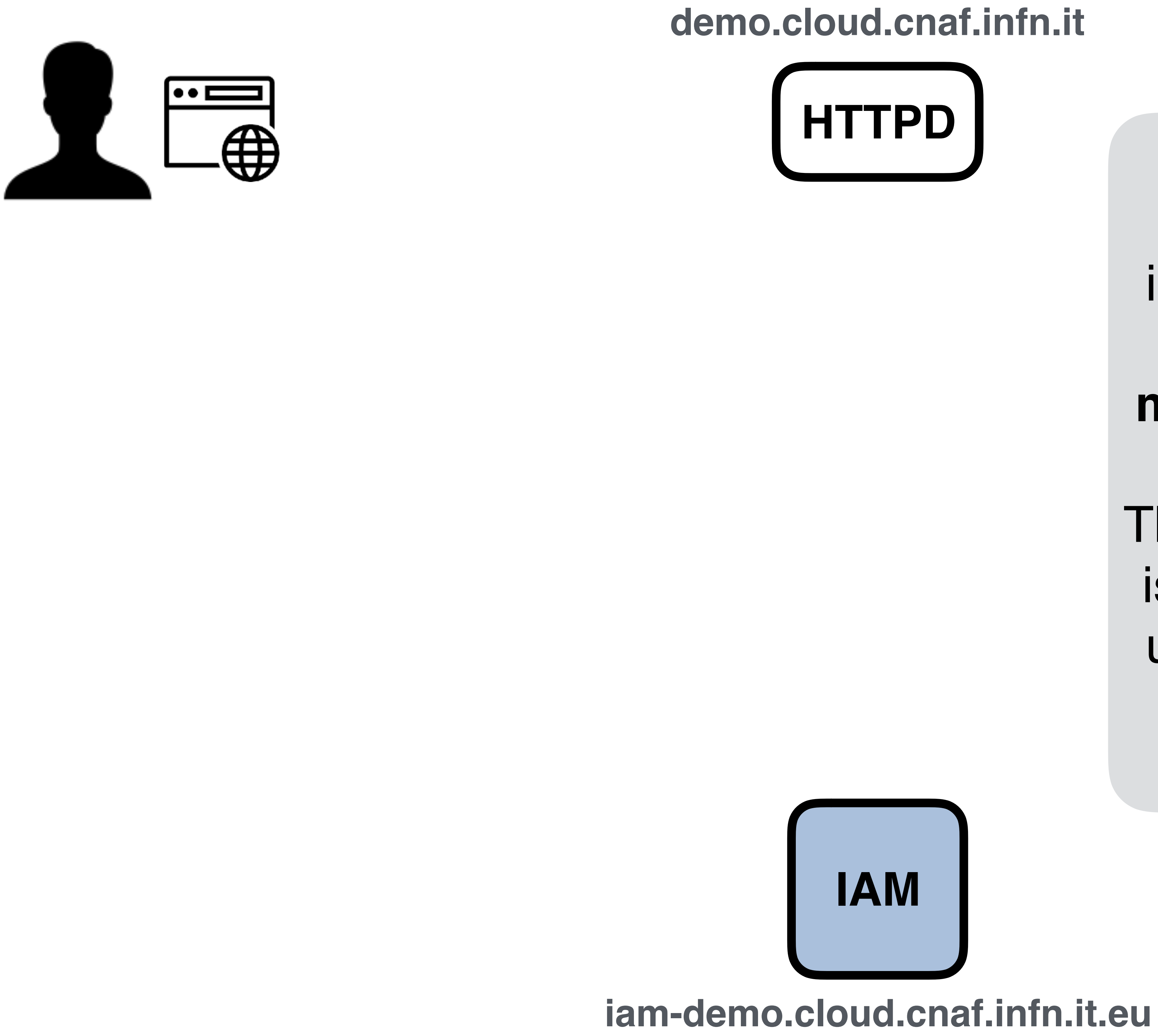
As an example, Apache mod_auth_openidc requires the following information to enable a working OpenID Connect integration

- 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

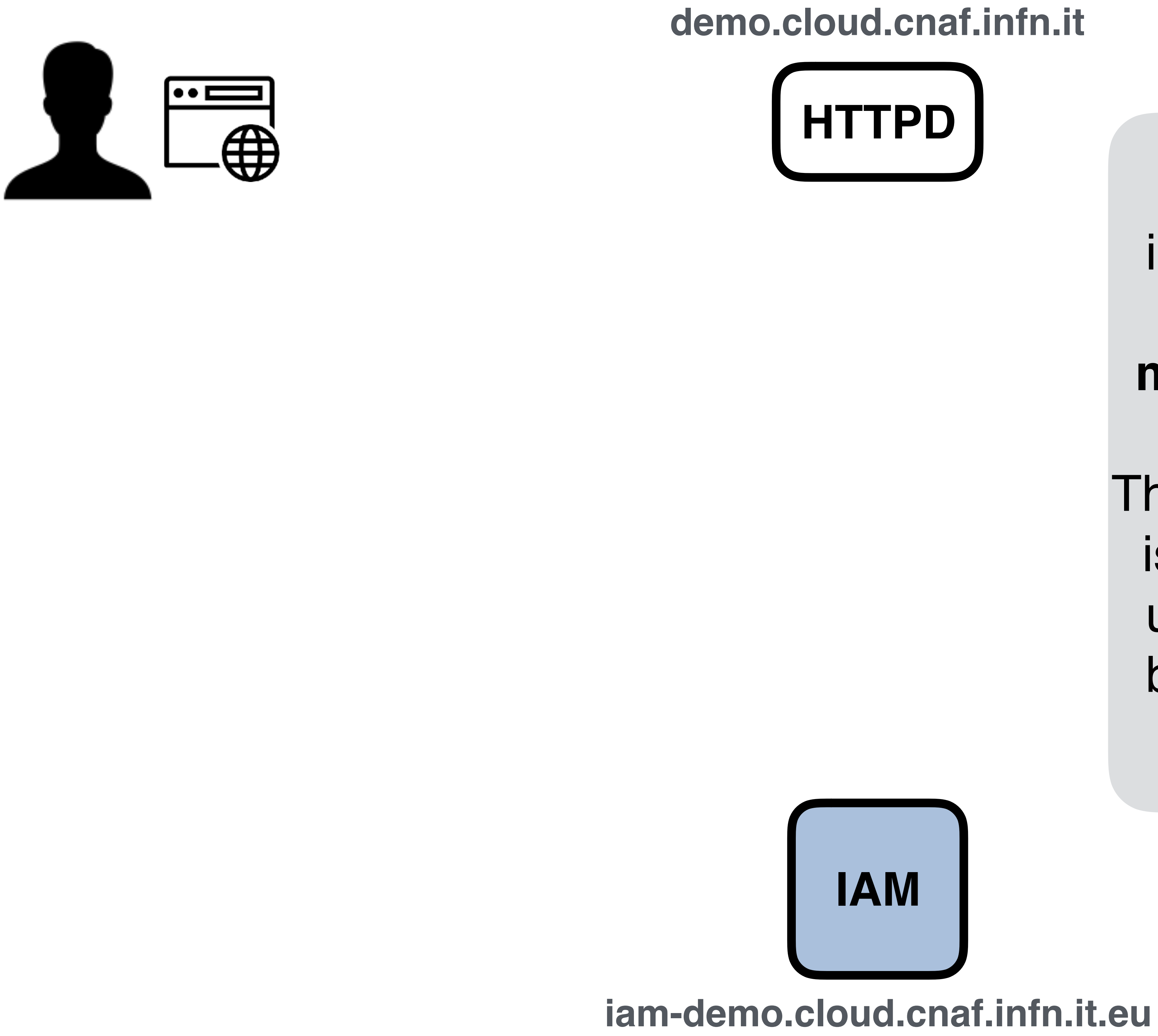
IAM

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

HTTPD
is an Apache server
configured with
mod_auth_openidc

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

Demo setup



demo.cloud.cnaf.infn.it

HTTPD

IAM

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

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

Apache mod_auth_openidc configuration

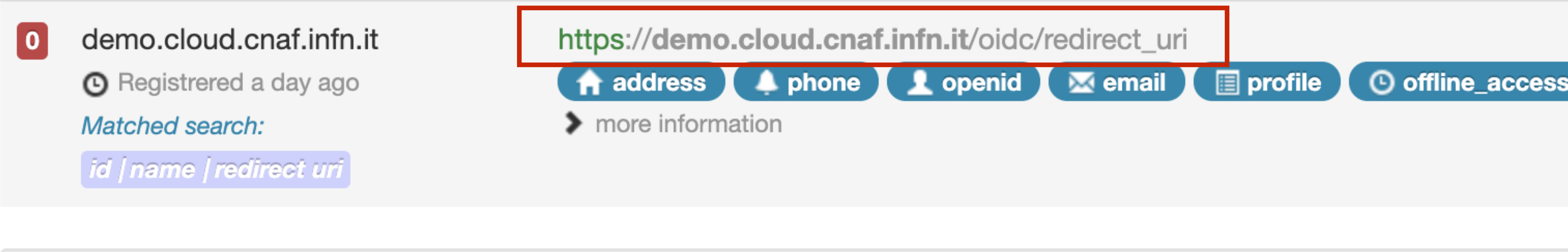
```
ServerName demo.cloud.cnaf.infn.it

<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



0 demo.cloud.cnaf.infn.it

Registrered a day ago

Matched search:

id | name | redirect uri

https://demo.cloud.cnaf.infn.it/oidc/redirect_uri

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

DEMO

Exercise

A docker-compose environment that replicates the one show in the demo has been setup at this repo

- https://github.com/andreaceccanti/iam-tutorial

You can replicate the integration exercise following the instructions in the README file:

- https://github.com/andreaceccanti/iam-tutorial/blob/master/apache-integration-demo/README.md

Thanks for your attention.

Questions?

Useful references

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

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

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
- enrico.vianello@cnaf.infn.it
- indigo-aai.slack.com