ESCAPE

European Science Cluster of Astronomy & Particle physics ESFRI research Infrastructures

ESCAPE AAI Webinar

Andrea Ceccanti - INFN

andrea.ceccanti@cnaf.infn.it

ESCAPE -The European Science Cluster of Astronomy & Particle Physics ESFRI Research Infrastructures has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement n°824064

Outline

- Introduction to the ESCAPE AAI
  - Basic AAI concepts: authentication & authorization
  - INDIGO IAM: key features
  - OAuth and OpenID Connect basics
  - Web application integration demonstration
  - AAI in the ESCAPE data lake demo
    - VOMS authn/z
    - Token-based authn/z

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Shared Google doc for feedback/questions

- A shared Google doc is linked to the agenda
  - Open in write access to anybody

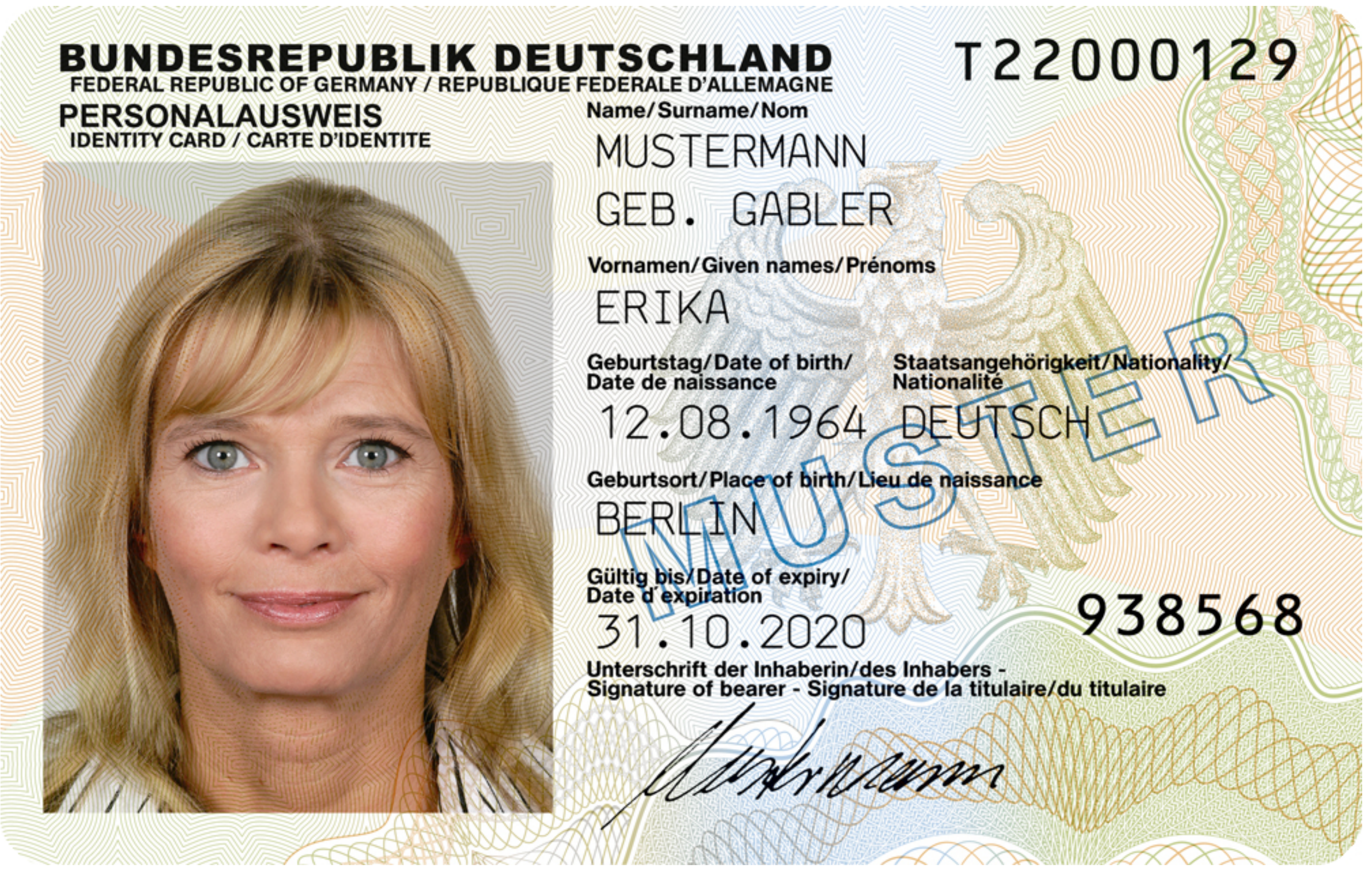
- https://docs.google.com/document/d/12pYn8FZDjYyWGzrOgnSJsyLEPa4TZhyXp_KSR-yDFNY/edit#

- Please use it to provide feedback/questions/comments on the Webinar

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Introduction to the ESCAPE AAI

Authentication, Identity



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

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

Mustermann

MUSTER

Slide courtesy of Paul Millar

Funded by the European Union's
Horizon 2020 - Grant N° 824064

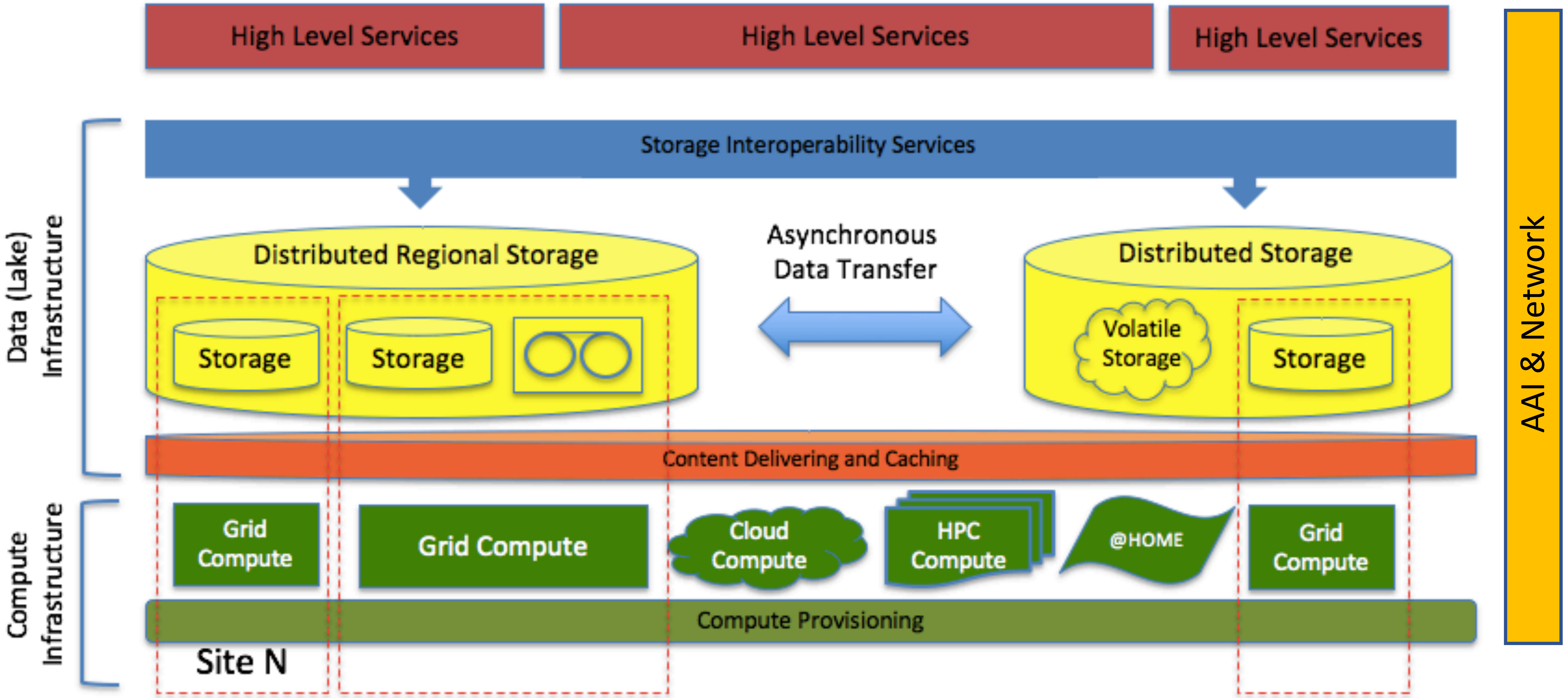
Authorization

Slide courtesy of Paul Millar

Funded by the European Union's
Horizon 2020 - Grant N° 824064

The ESCAPE data lake

Data Lake building blocks



Define, integrate and commission an ecosystem of tools and services to build a data lake

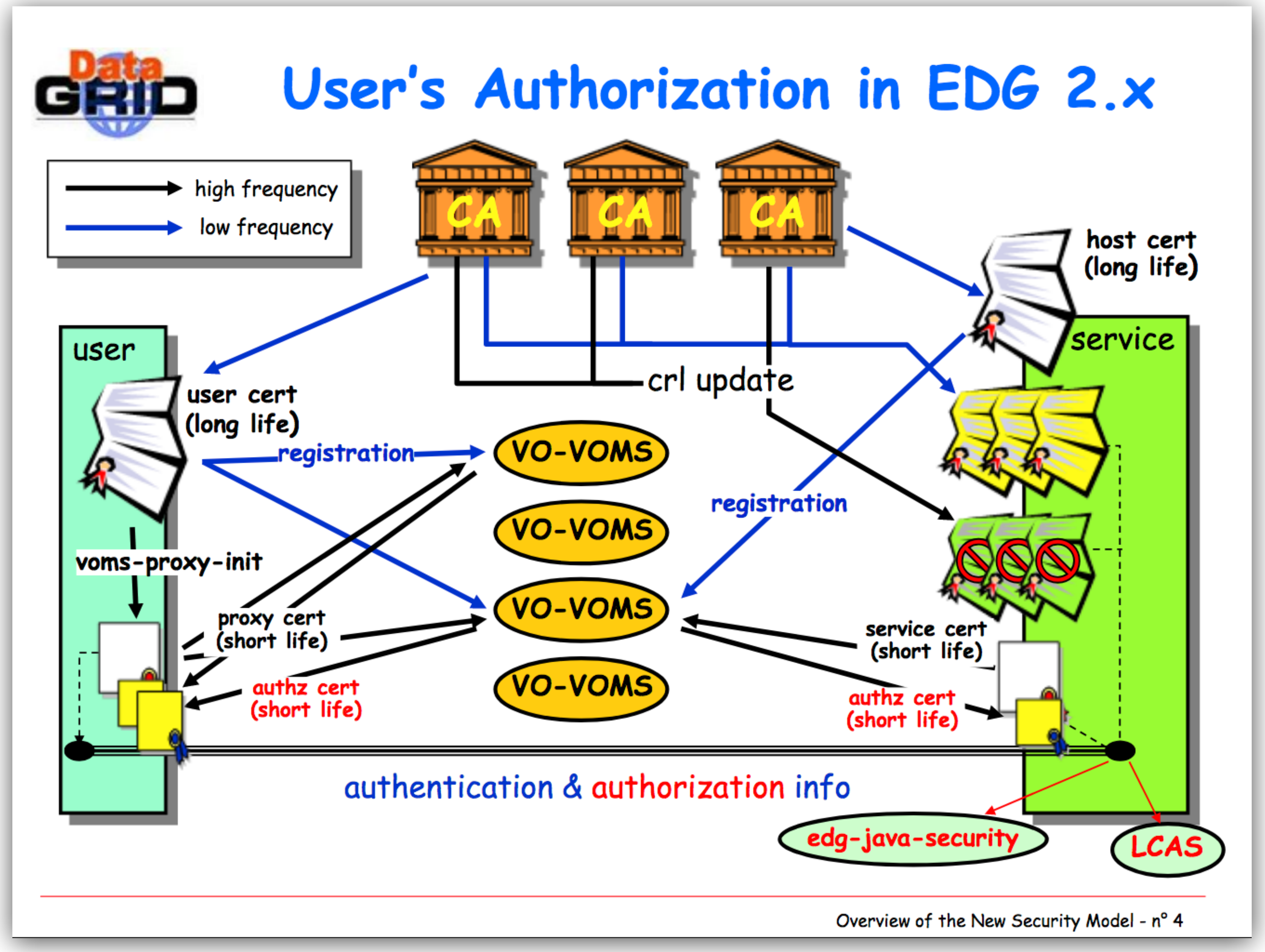
Leaves to the science projects the flexibility to choose the services and layout most suitable to their needs. Provides a reference implementation

Contributes to deliver Open Access and FAIR data services: relies on trustable data repositories; enables data management policies; hides the complexities of the underlying infrastructure providing a transparent data access layer

Funded by the European Union's
Horizon 2020 - Grant N° 824064

ESCAPE Data Lake AAI and WLCG

Current, X.509 based AAI

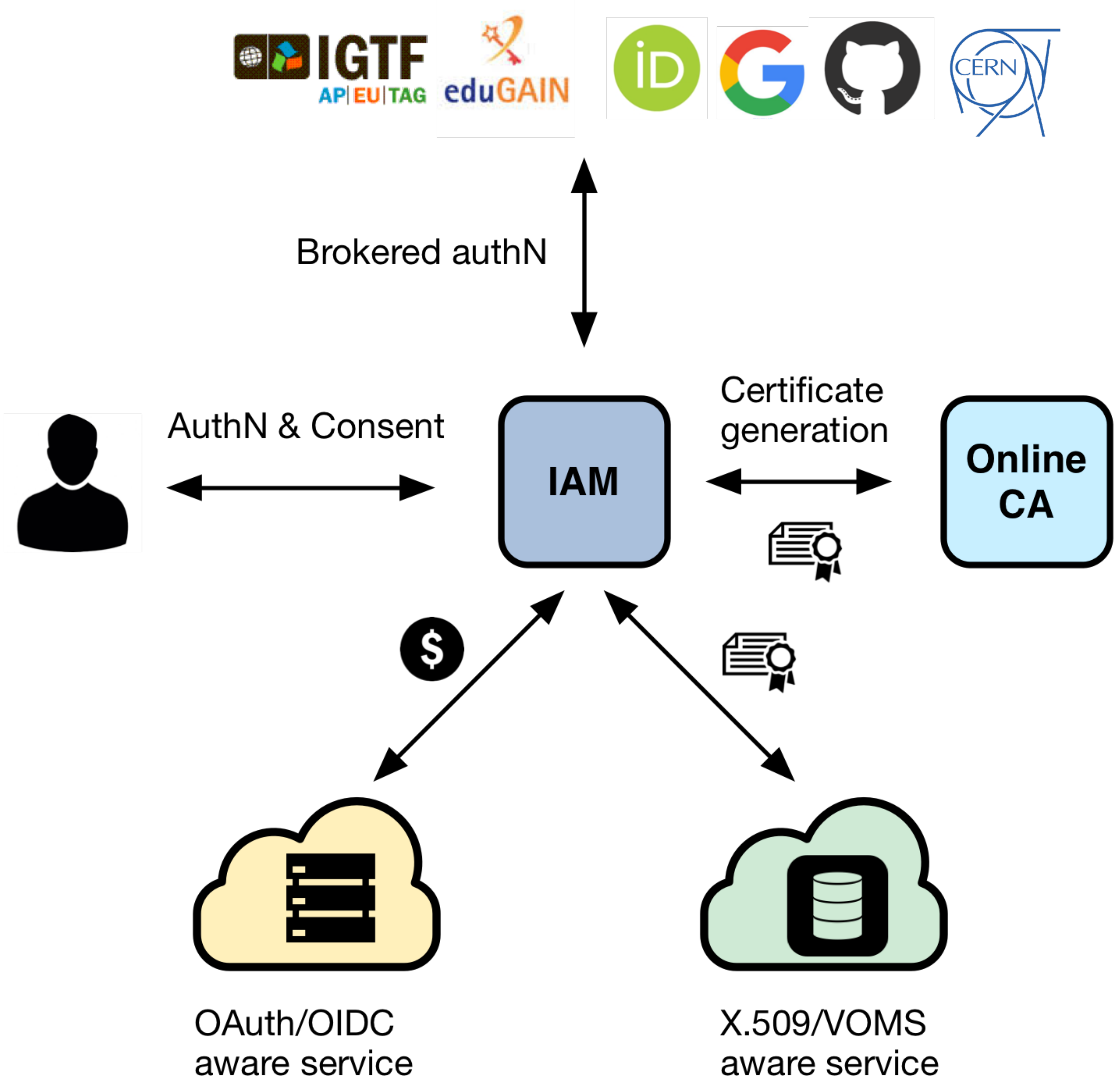


User's Authorization in EDG 2.x

Overview of the New Security Model - n° 4

Move beyond X.509

Future, token-based AAI



Brokered authN

AuthN & Consent

IAM

Certificate generation

Online CA

OAuth/OIDC aware service

X.509/VOMS aware service

Approach: leverage and build upon the WLCG experience

Moving beyond X.509: main challenges

- **Authentication**
  - **Flexible**, able to accomodate various authentication m
    - X.509, username
- **Identity harmo linking**
  - Harmonize mult single account,
- **Authorization**
  - **Orthogonal** to authentication, **attribute** or **capability-based**

- **Delegation**
  - Provide the ability for **services to act on behalf of**
  - **applications**
  - provisioning of ng resources
- **Token translation**
  - Enable **integration with legacy services through controlled credential translation**

Key challenge:

allow a gradual transition to the new AAI!

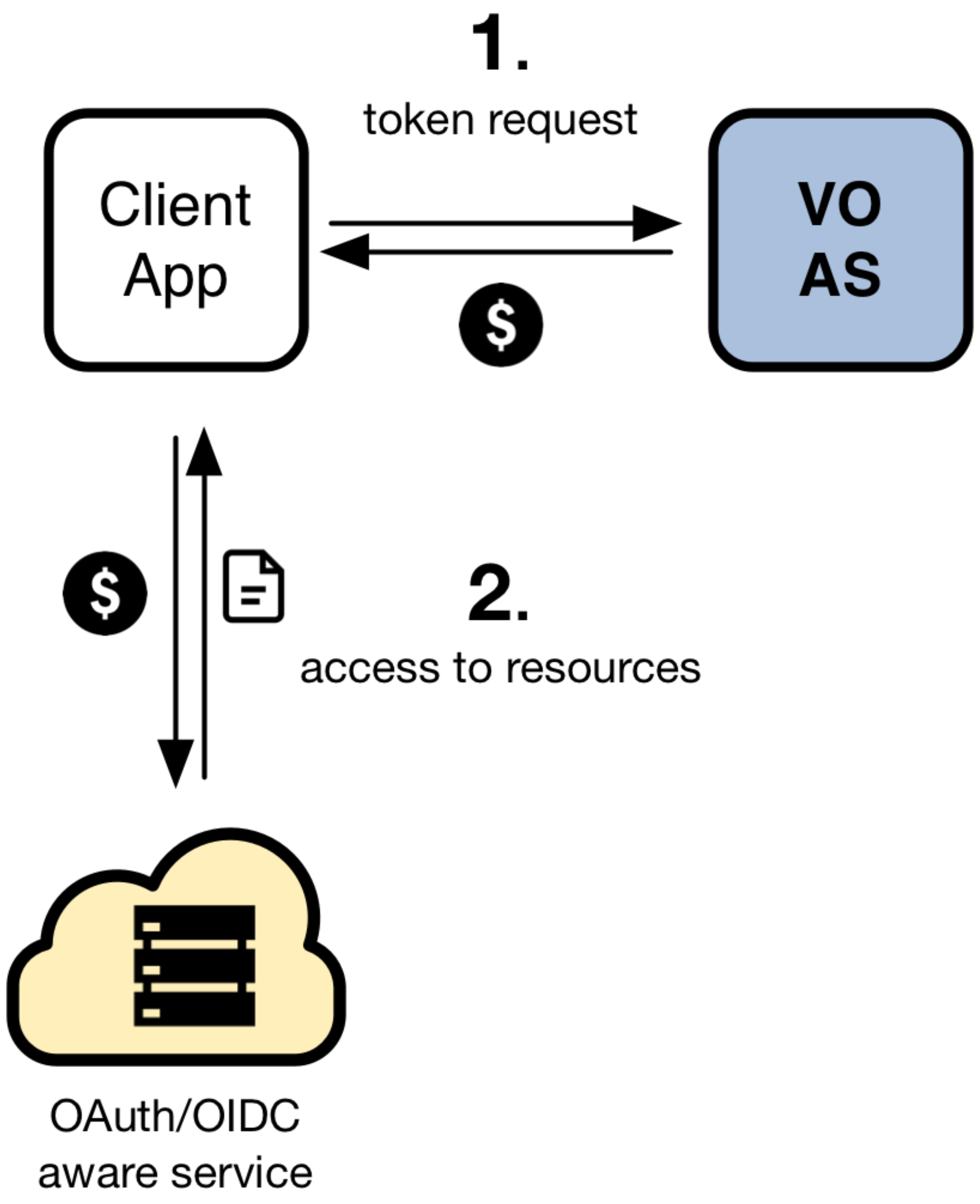
Funded by the European Union's Horizon 2020 - Grant N° 824064

Token-based AuthN/Z from 10000 mt

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

- The token is obtained from **a Virtual Organization** (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



Funded by the European Union's Horizon 2020 - Grant N° 824064

In practice…

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

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

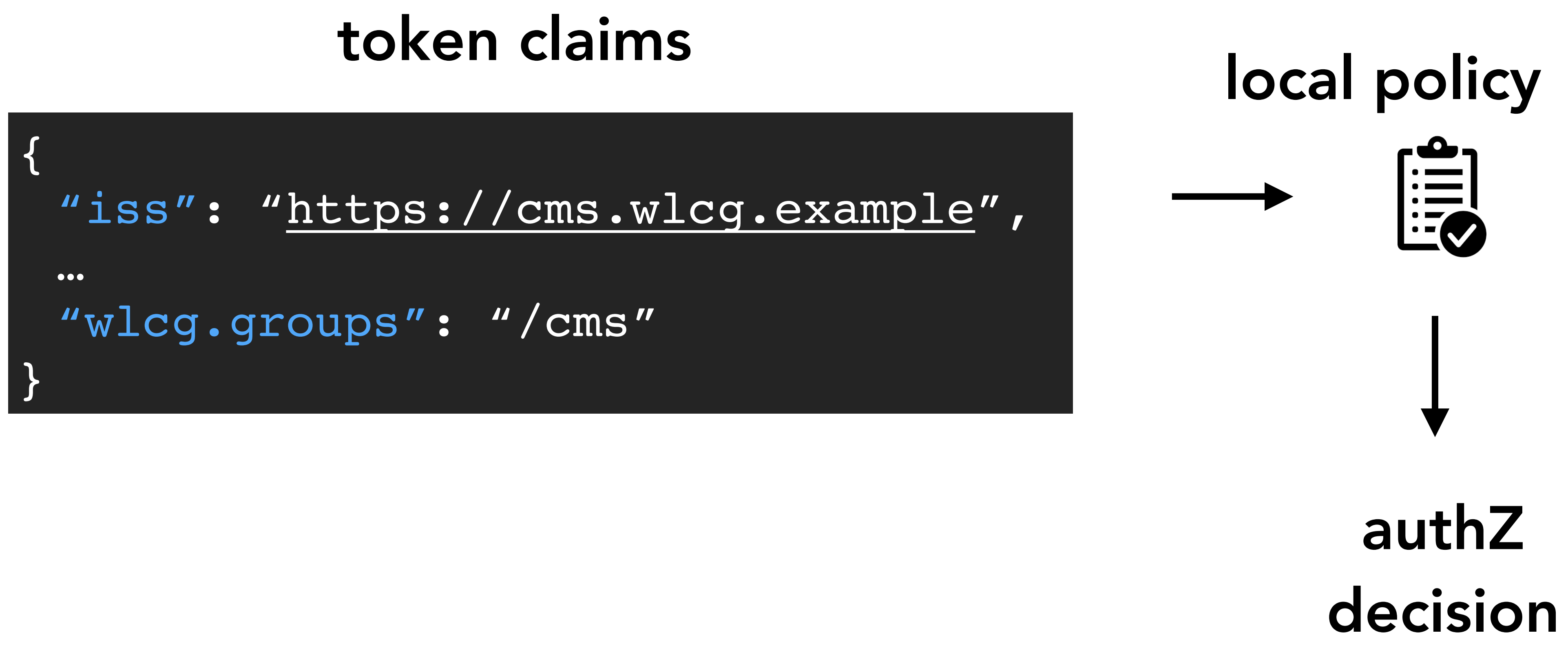
- This information is exposed to services via **signed JWT tokens** and **via OAuth/OpenID Connect protocol message exchanges** (aka flows)

- **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 **/lofar** namespace to anyone with the capability **storage.read:/lofar**

Funded by the European Union's
Horizon 2020 - Grant N° 824064

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



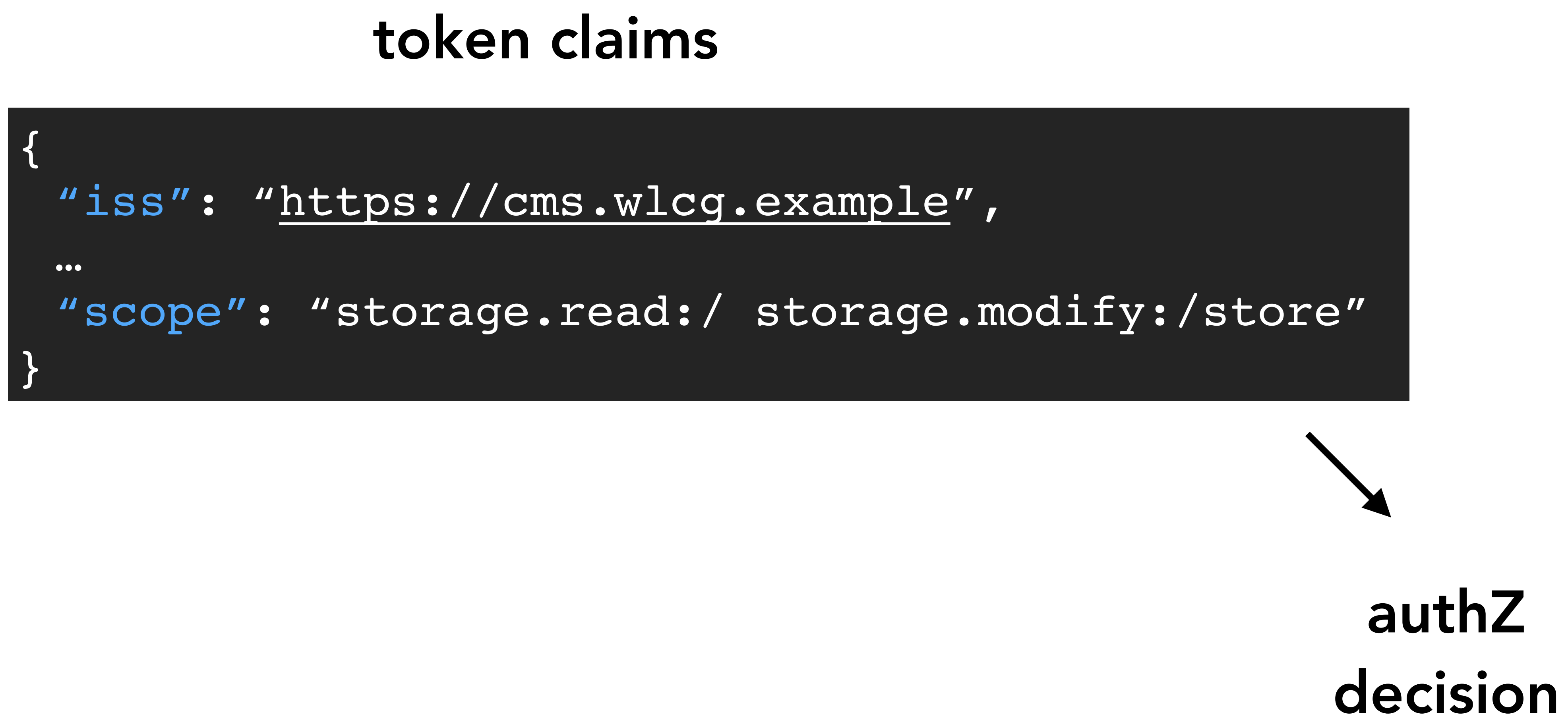
token claims

```
{
  "iss": "https://cms.wlcg.example",
  …
  "wlcg.groups": "/cms"
}
```

local policy

authZ decision

- **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



token claims

```
{
  "iss": "https://cms.wlcg.example",
  …
  "scope": "storage.read:/ storage.modify:/store"
}
```

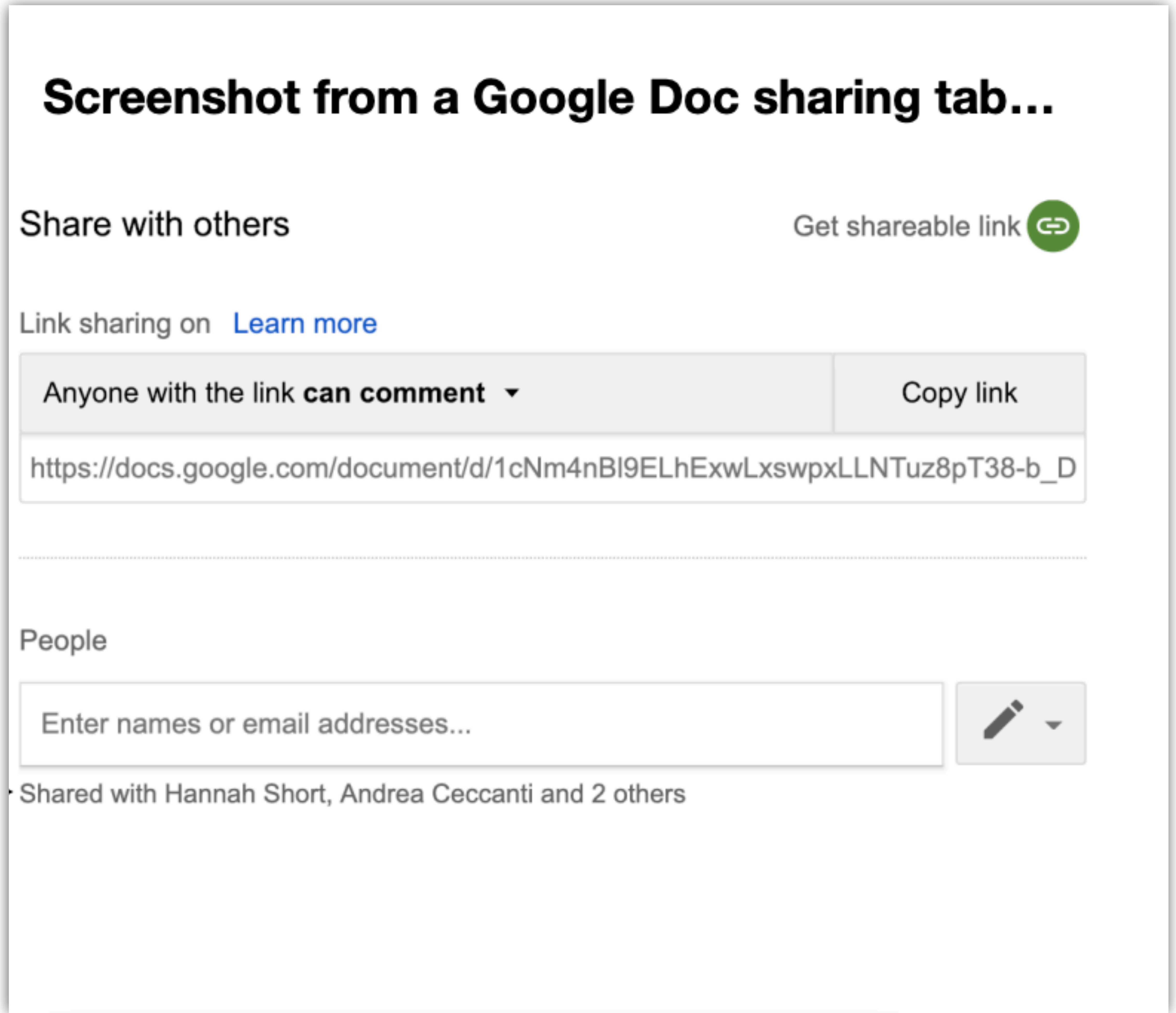
authZ decision

Identity-based vs Scope-based Authorization

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

scope-based authZ →

identity-based authZ →



Screenshot from a Google Doc sharing tab…

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/1cNm4nBI9ELhExwLxswpxLLNTuz8pT38-b_D

People

Enter names or email addresses...

Shared with Hannah Short, Andrea Ceccanti and 2 others

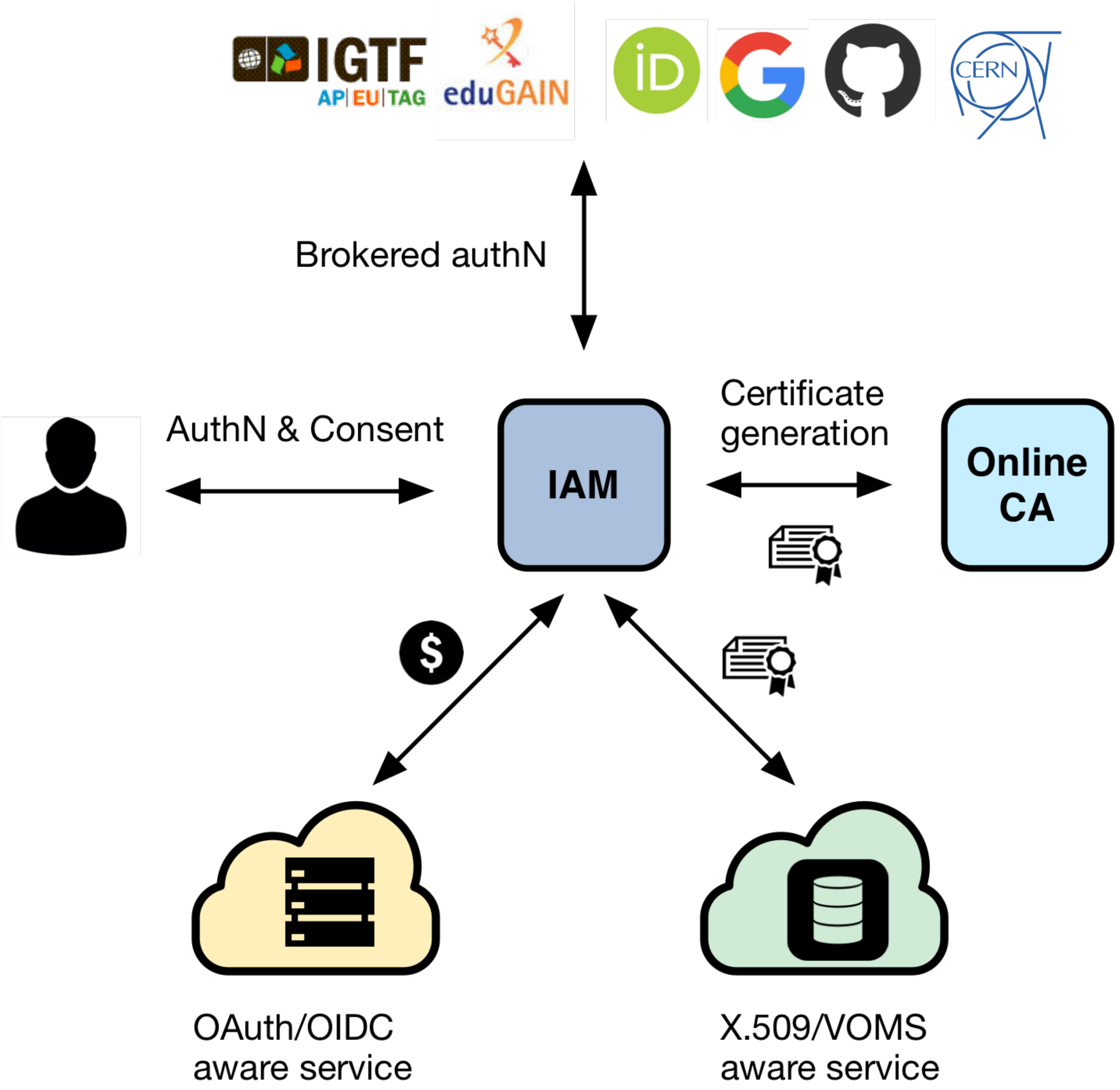
*** Slide courtesy of B. Bockelman**

Funded by the European Union's
Horizon 2020 - Grant N° 824064

INDIGO Identity and Access Management Service

- A **VO*-scoped** authentication and authorization service that
  - supports **multiple authentication mechanisms**
  - provides users with a **persistent, VO-scoped** identifier
  - exposes **identity information**, **attributes** and **capabilities** to services via **JWT** tokens and standard **OAuth & OpenID Connect** protocols
  - can integrate existing **VOMS**-aware services
  - supports **Web** and **non-Web access**, **delegation** and **token renewal**

*VO = Virtual Organization



Funded by the European Union's Horizon 2020 - Grant N° 824064

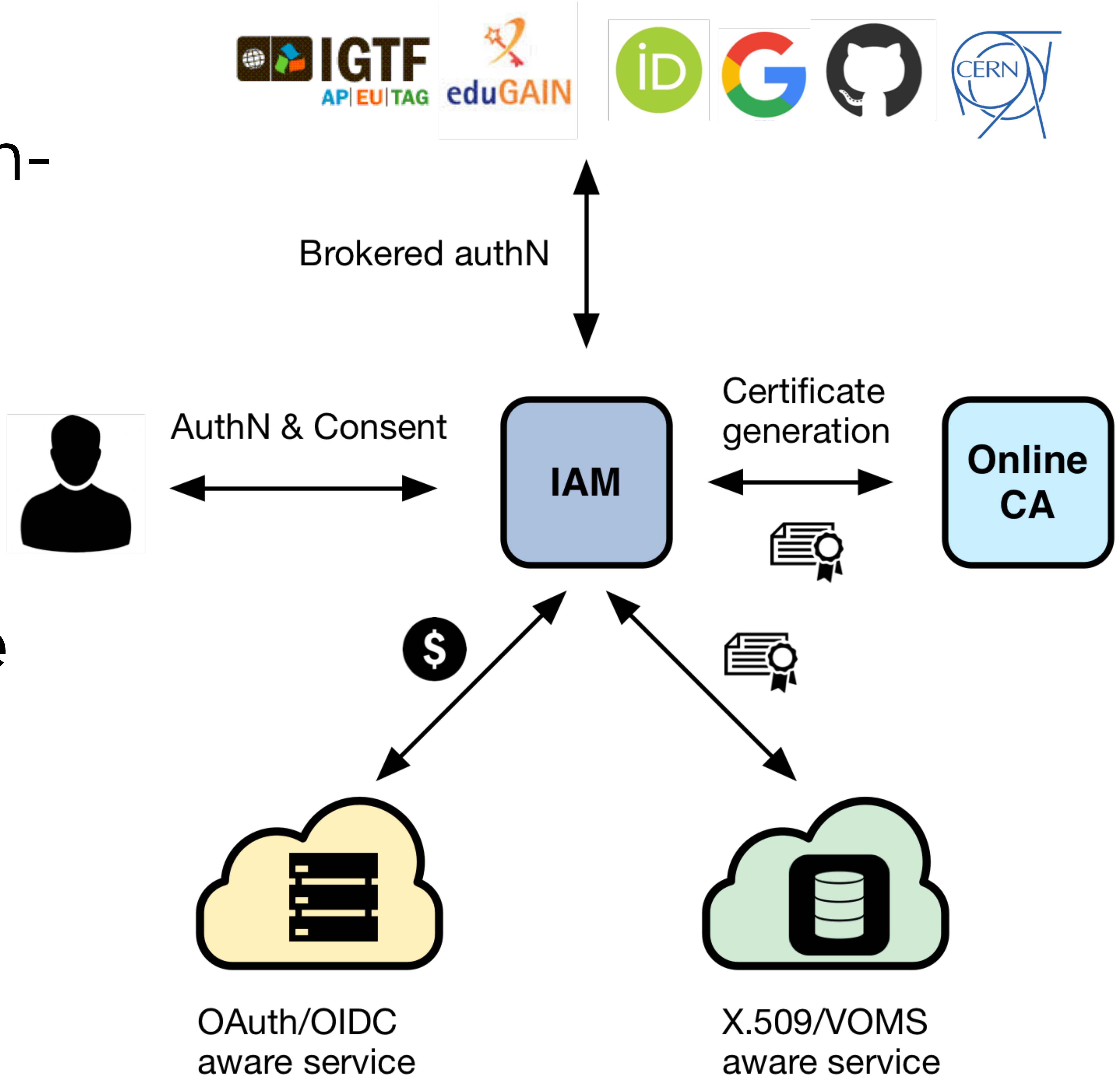
INDIGO Identity and Access Management Service

- **Selected by the WLCG Management Board** to be the core of the future, token-based WLCG AAI
  - while ensuring backward compatibility with the existing infrastructure

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

EOSC-hub

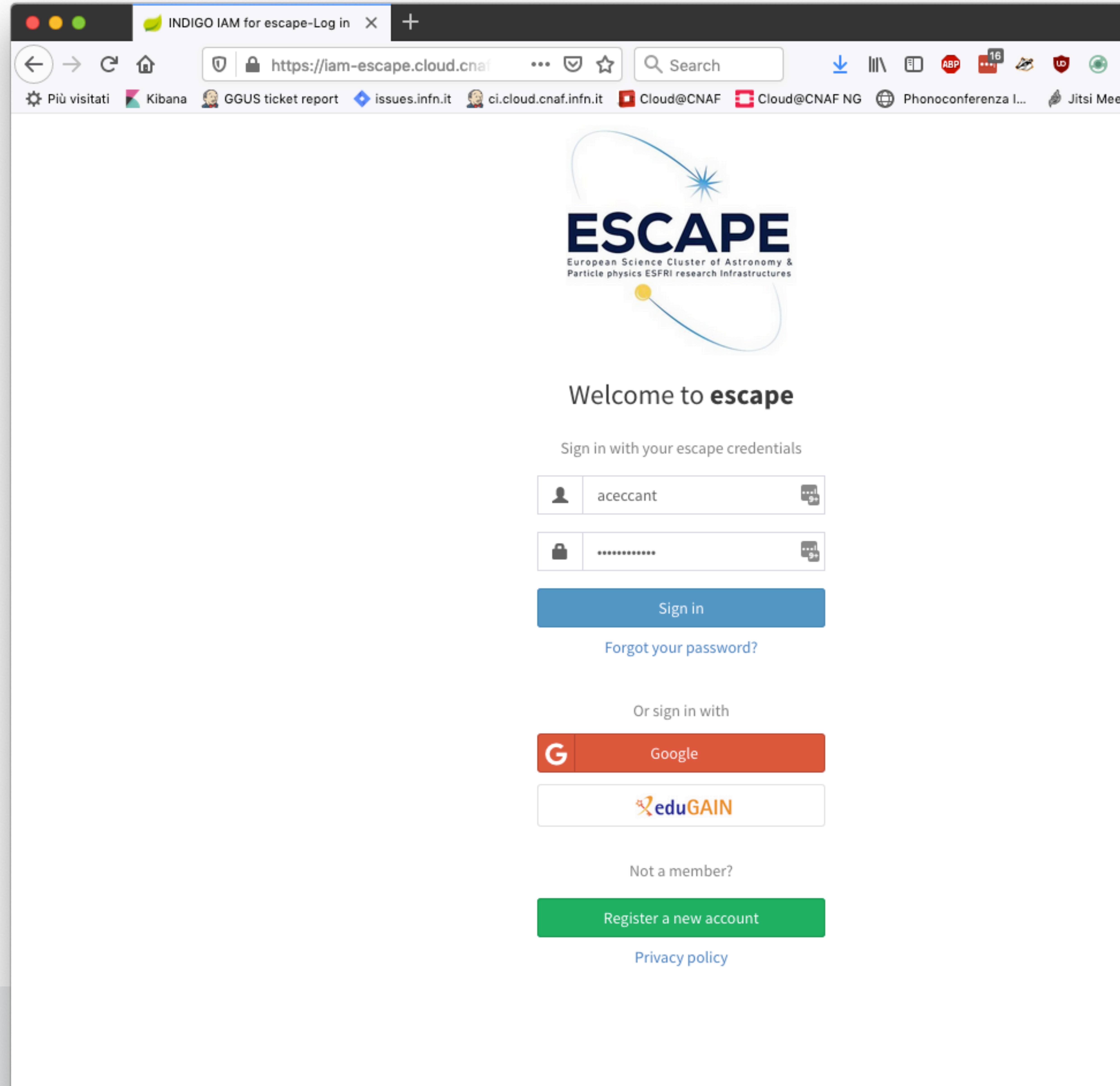
ESCAPE
European Science Cluster of Astronomy & Particle physics ESFRI research Infrastructures



Funded by the European Union's Horizon 2020 - Grant N° 824064

The ESCAPE IAM instance

- Escape IAM instance available
  - Root of trust for the ESCAPE Data Lake
  - 53 registered users
  - 9 groups
  - AuthN with EduGAIN, X.509 certificates, Google, username/password
  - VOMS endpoint available
  - Registration open
    - Administrator-vetted registration flow
  - Documentation available here


INDIGO IAM for escape-Log in
https://iam-escape.cloud.cna
Search
Più visitati
Kibana
GGUS ticket report
issues.infn.it
ci.cloud.cnaf.infn.it
Cloud@CNAF
Cloud@CNAF NG
Phonoconferenza I...
Jitsi Mee
ESCAPE
European Science Cluster of Astronomy & Particle physics ESFRI research Infrastructures

Welcome to **escape**

Sign in with your escape credentials

aceccant

••••••••••••

Key INDIGO IAM features

User enrolment & registration service

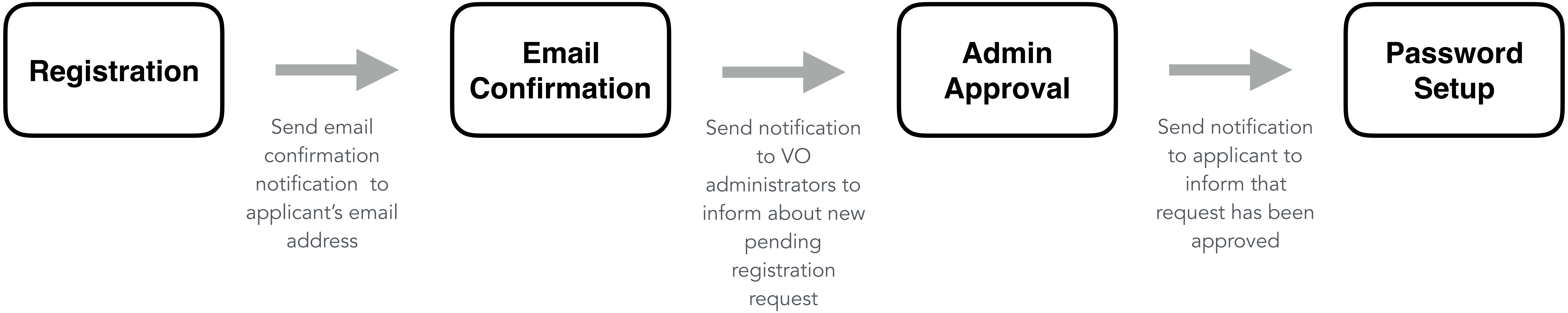
- IAM currently supports two **enrolment flows:**

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

Funded by the European Union's
Horizon 2020 - Grant N° 824064

IAM moderated enrolment flow



Registration

Send email confirmation notification to applicant's email address

Email Confirmation

Send notification to VO administrators to inform about new pending registration request

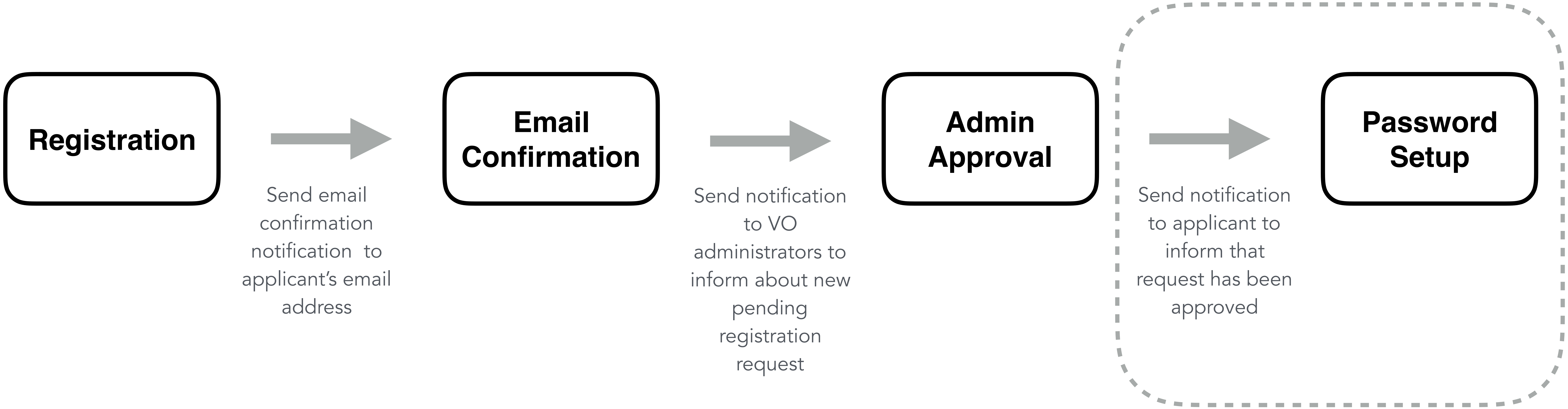
Admin Approval

Send notification to applicant to inform that request has been approved

Password Setup

IAM moderated enrolment flow

Optional step when users registers after having been authenticated using an external IdP



Registration

Send email confirmation notification to applicant's email address

Email Confirmation

Send notification to VO administrators to inform about new pending registration request

Admin Approval

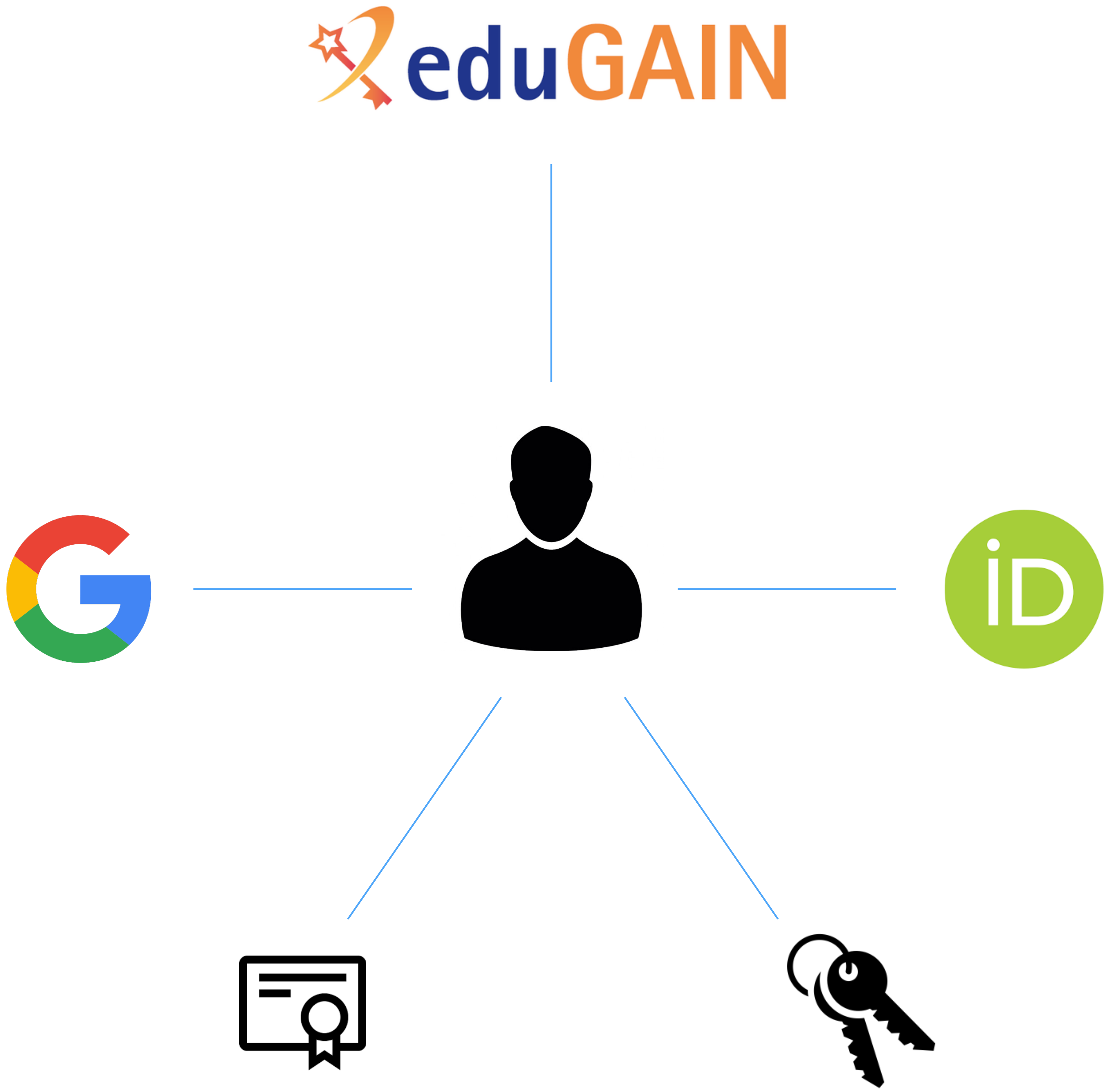
Send notification to applicant to inform that request has been approved

Password Setup

Funded by the European Union's Horizon 2020 - Grant N° 824064

Flexible authentication & account linking

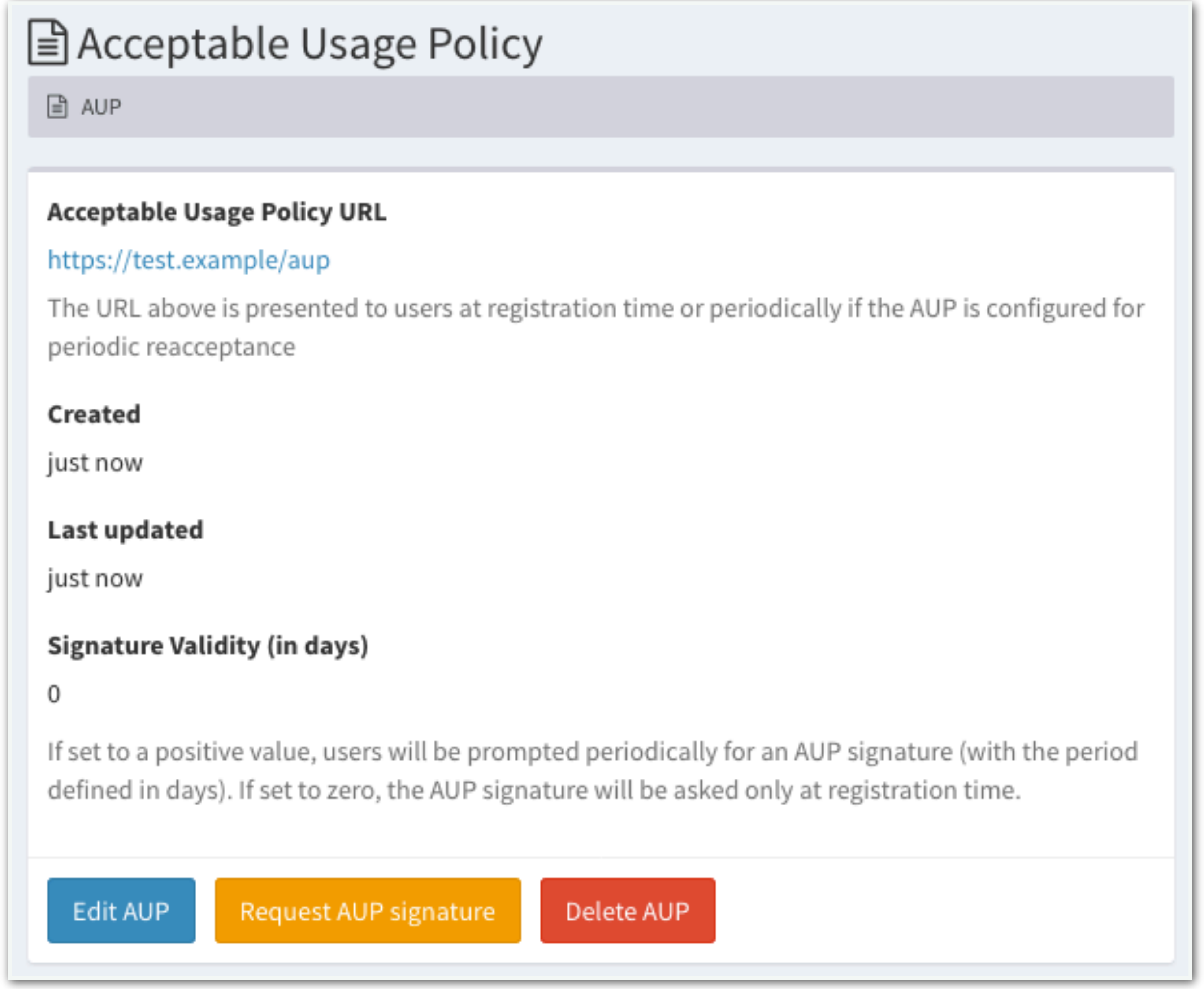
- Authentication supported via
  - **local username/password** credentials (created at registration time)
  - **SAML** Home institution IdP (e.g., EduGAIN)
  - **OpenID Connect** (Google, Microsoft, Paypal, ORCID)
  - **X.509** certificates
- Users can link any of the supported authentication credentials 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



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 URL

https://test.example/aup

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

Created

just now

Last updated

just now

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.

Funded by the European Union's
Horizon 2020 - Grant N° 824064

SCIM provisioning APIs

- IAM provides a RESTful API, based on the System for Cross-domain Identity Management (SCIM) standard, that can be used to access information in the IAM database
  - users, groups, group memberships, etc…

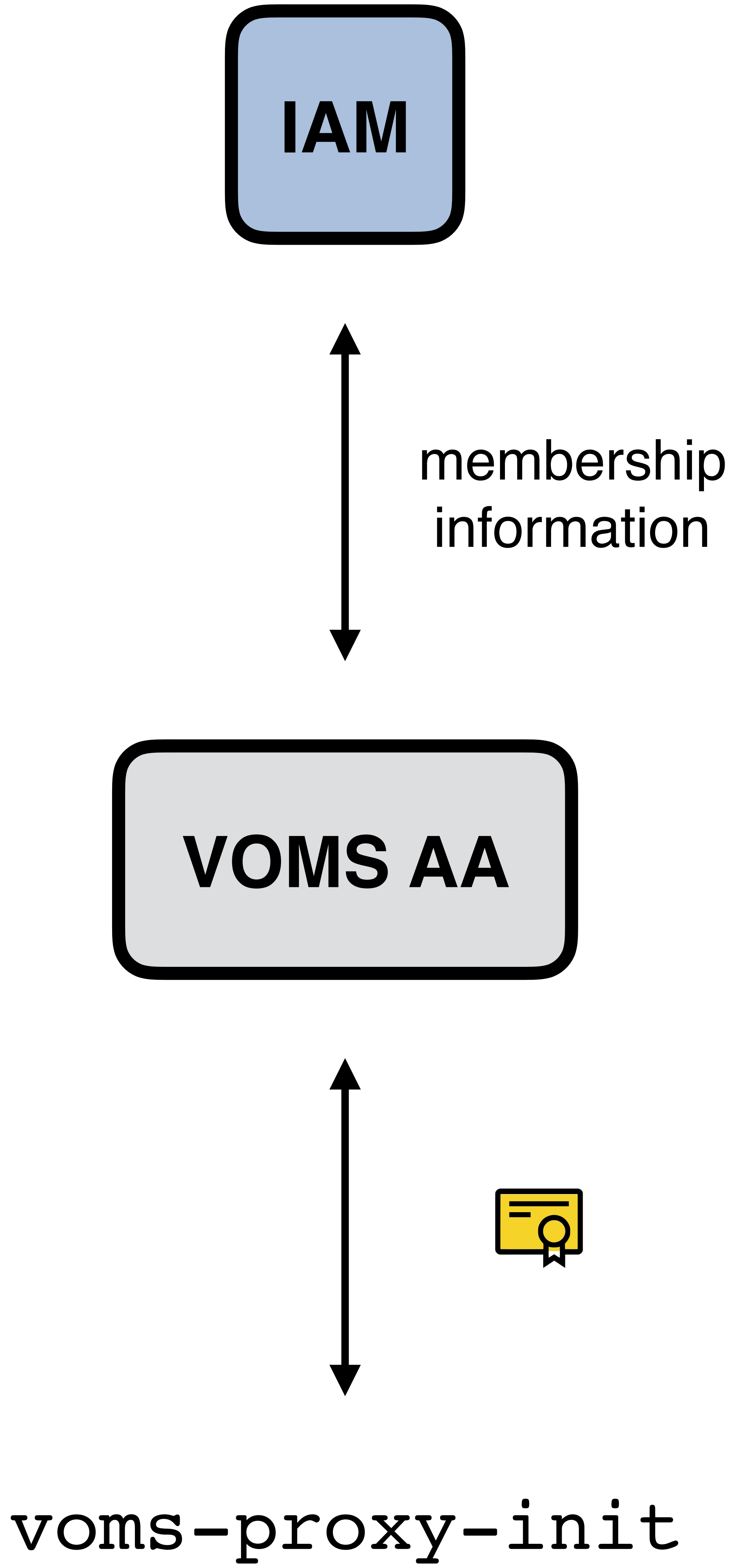
- The API can be used as an integration point towards external systems
  - Example:
    - The SCIM API is used in the integration with the HTCondor batch system to do account pre-provisioning based on IAM account information

Funded by the European Union's
Horizon 2020 - Grant N° 824064

VOMS provisioning

- IAM includes a VOMS attribute authority micro-service that can encode IAM membership information in a **standard VOMS Attribute Certificate**

- **Proven compatibility** with existing latest supported clients and Grid services
  - e.g., data transfers in the ESCAPE data lake testbed rely on this



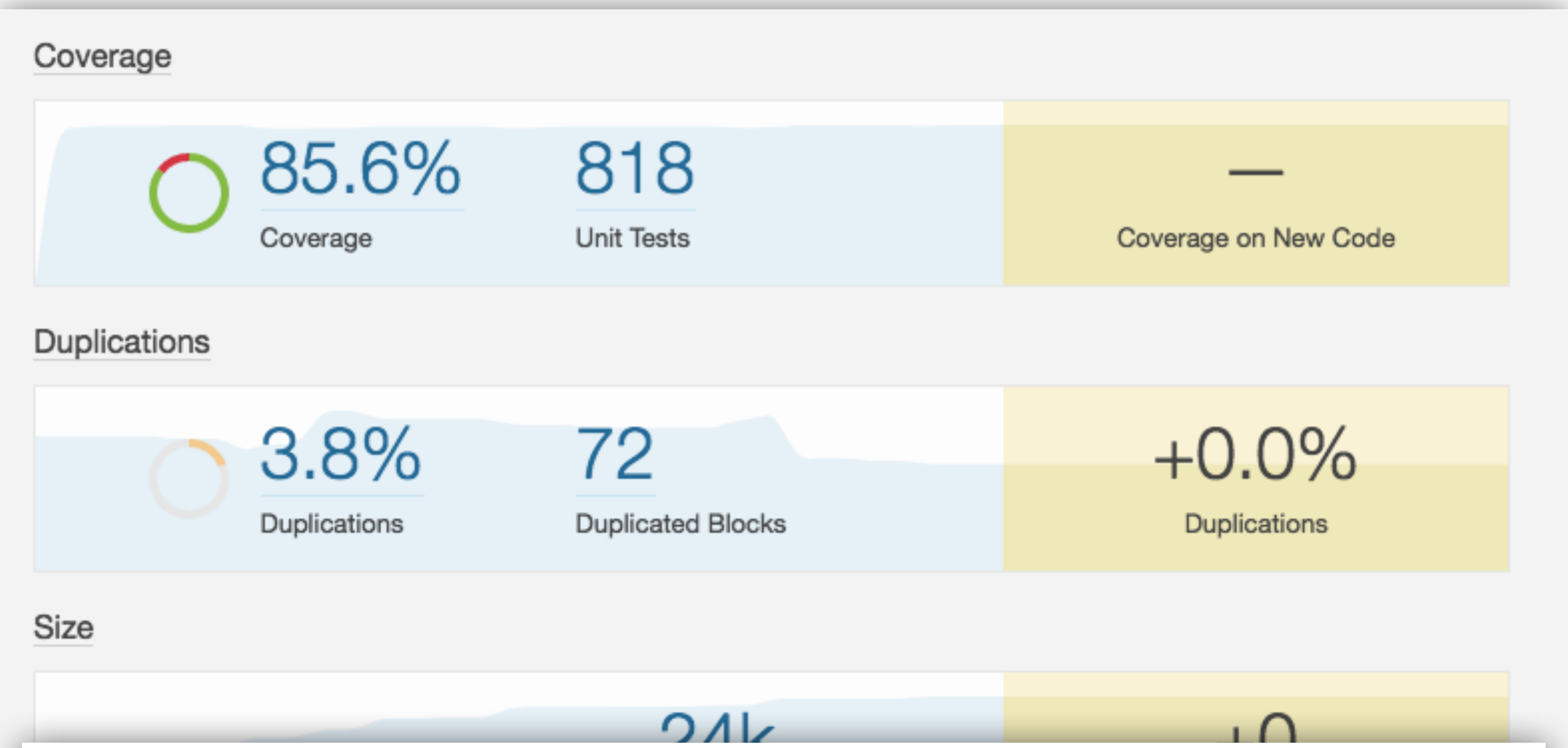
Easy integration with relying services

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

- IAM has been successfully integrated with
  - Openstack, Atlassian JIRA & Confluence, Moodle, Rocketchat, Grafana, Kubernetes, JupyterHub, **dCache, StoRM, XRootD (HTTP), FTS, RUCIO, HTCondor**

Software Quality in IAM

- Aim to have **~90% unit test coverage on all code**:
  - now 33K LoC, 86,4% branch coverage, >1.2K tests
- Open, **test-driven** development process
- **Static analysis** tools
  - SonarCloud IAM page
- **Multiple test suites**
  - **Unit tests**
  - **Frontend test suite** (based on Selenium and Robot framework)
  - **Deployment tests** (in CI)



Coverage

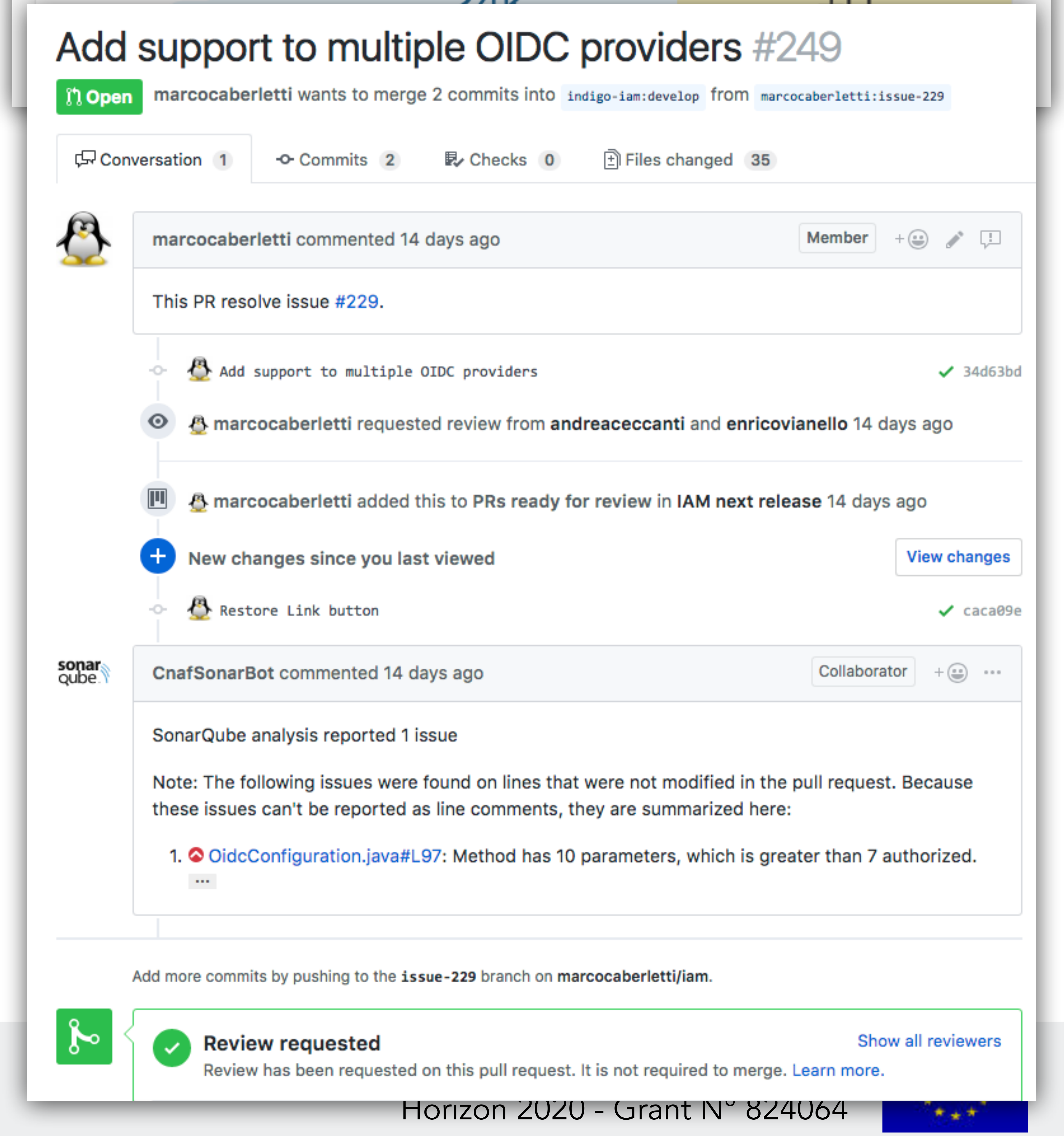
85.6% Coverage | 818 Unit Tests | — Coverage on New Code

Duplications

3.8% Duplications | 72 Duplicated Blocks | +0.0% Duplications

Size

24k | +0



Add support to multiple OIDC providers #249

Open marcocaberletti wants to merge 2 commits into `indigo-iam:develop` from `marcocaberletti:issue-229`

marcocaberletti commented 14 days ago — Member

This PR resolve issue #229.

`Add support to multiple OIDC providers` ✓ 34d63bd

marcocaberletti requested review from **andreaceccanti** and **enricovianello** 14 days ago

marcocaberletti added this to **PRs ready for review** in **IAM next release** 14 days ago

New changes since you last viewed — View changes

`Restore Link button` ✓ caca09e

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. OidcConfiguration.java#L97: Method has 10 parameters, which is greater than 7 authorized.

Add more commits by pushing to the **issue-229** branch on **marcocaberletti/iam**.

Review requested — Show all reviewers

Review has been requested on this pull request. It is not required to merge. Learn more.

Key IAM features demo

What will be demonstrated

- Registration at the ESCAPE Virtual Organization (VO)
- Account linking for institutional credentials and X.509 certificates
- AUP enforcement support
- SCIM API access
- VOMS provisioning

Funded by the European Union's
Horizon 2020 - Grant N° 824064

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

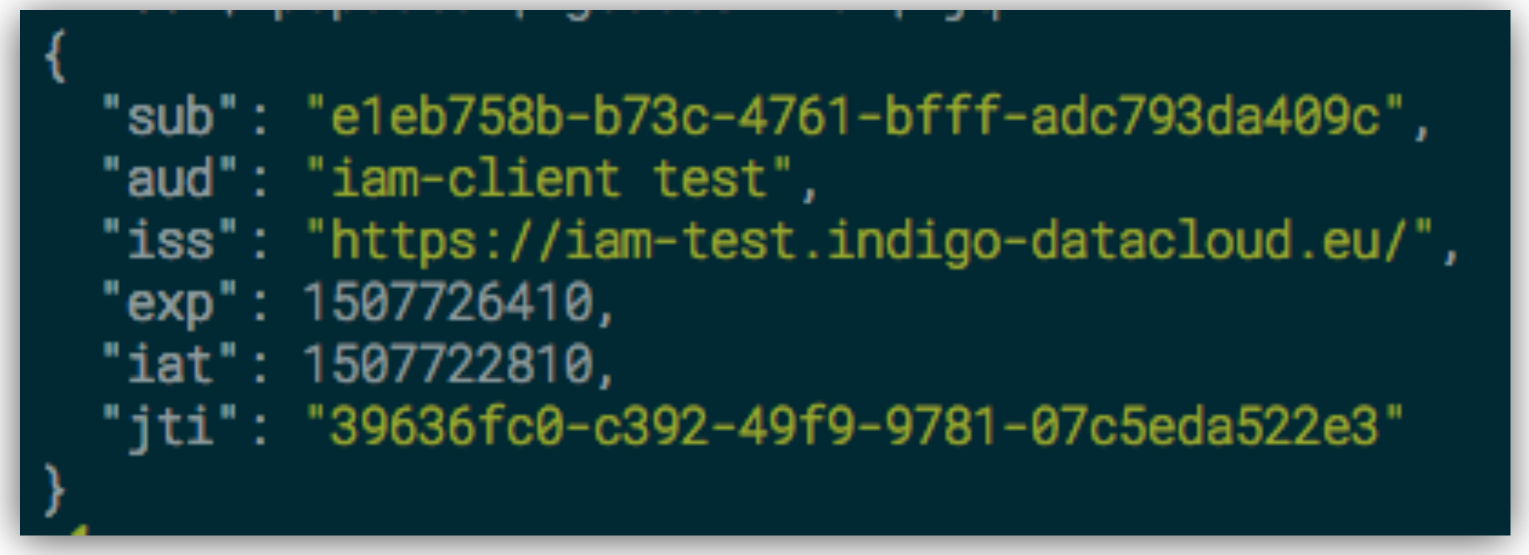
Gültig bis/Date of expiry/ Date d'expiration
31.10.2020

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"
}
```

Funded by the European Union's
Horizon 2020 - Grant N° 824064

OAuth: a delegated authorization framework

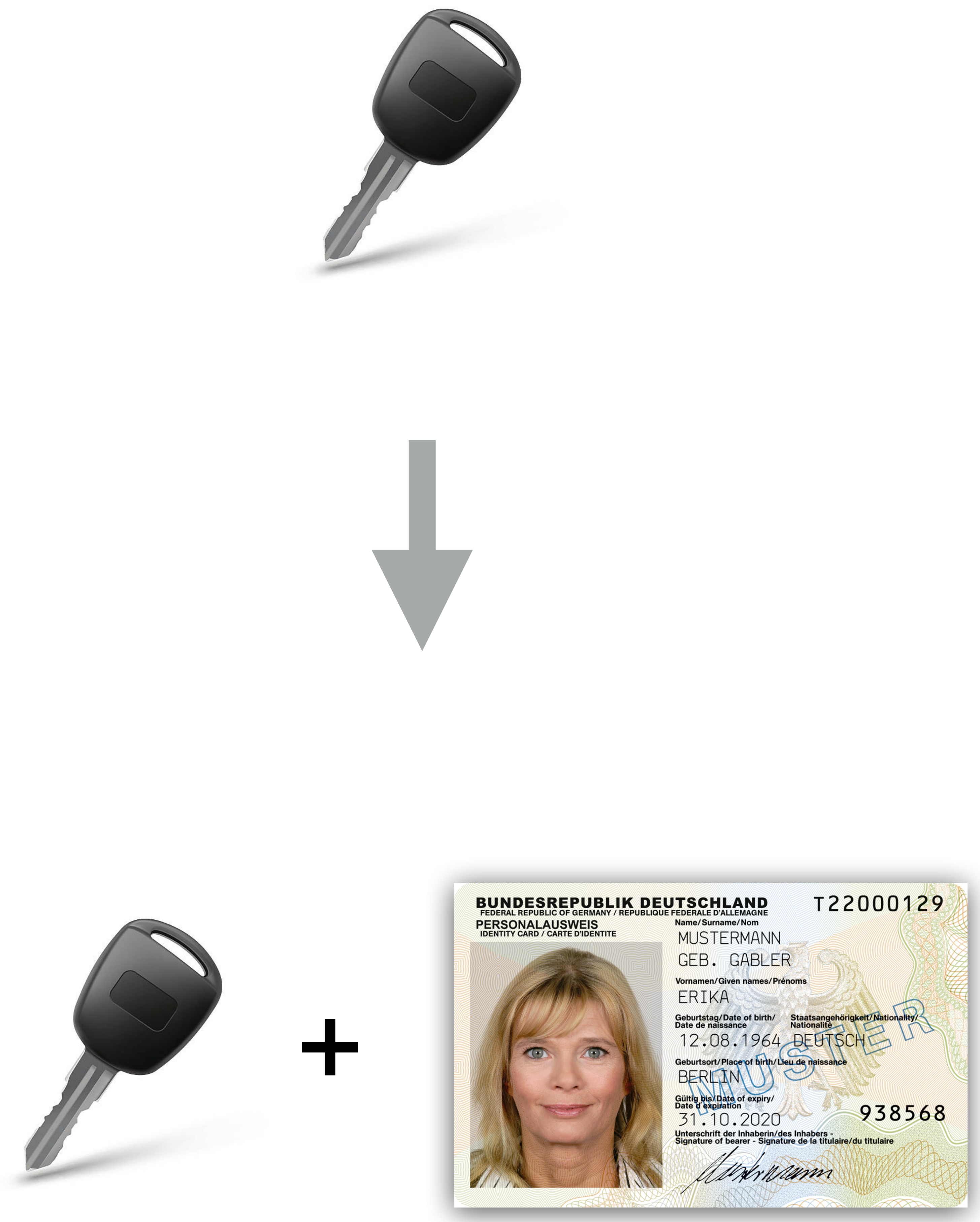
- OAuth defines how **controlled delegation of privileges** can happen among collaborating services

- 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 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**.

- JWTs integrity and signatures can be verified **independently** in a **distributed fashion** by relying parties

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Why OAuth, OpenID Connect and JWT?

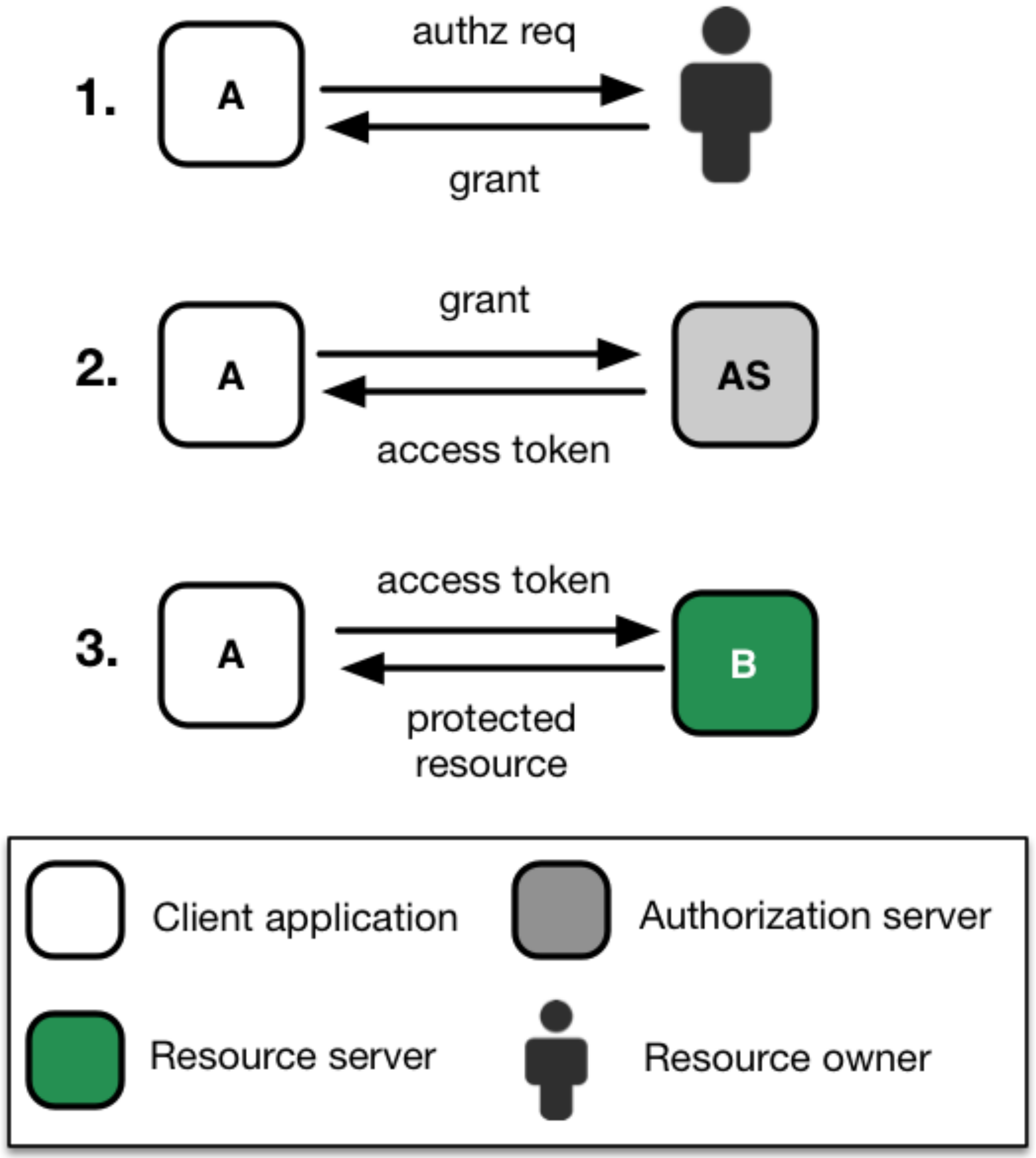
- Standard, widely adopted in industry
  - Do not reinvent the wheel, reuse existing knowledge and tools, extend when needed
- Reduced integration complexity at relying services
  - Off-the-shelf libraries and components
- Authentication-mechanism agnostic
  - The AAI is not bound to a specific authentication mechanism
- Distributed verification of access and identity tokens
  - It scales

Funded by the European Union's
Horizon 2020 - Grant N° 824064

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



Funded by the European Union's
Horizon 2020 - Grant N° 824064

OAuth/OpenID Connect actors and roles

Actor	Role	Example
Authorization Server (AS)	Asserting party	ESCAPE IAM instance
Resource Server (RS)	Relying party	The RUCIO REST API
Client	Relying party	The RUCIO Web Dashboard
Resource Owner	Subject	A registered IAM ESCAPE user

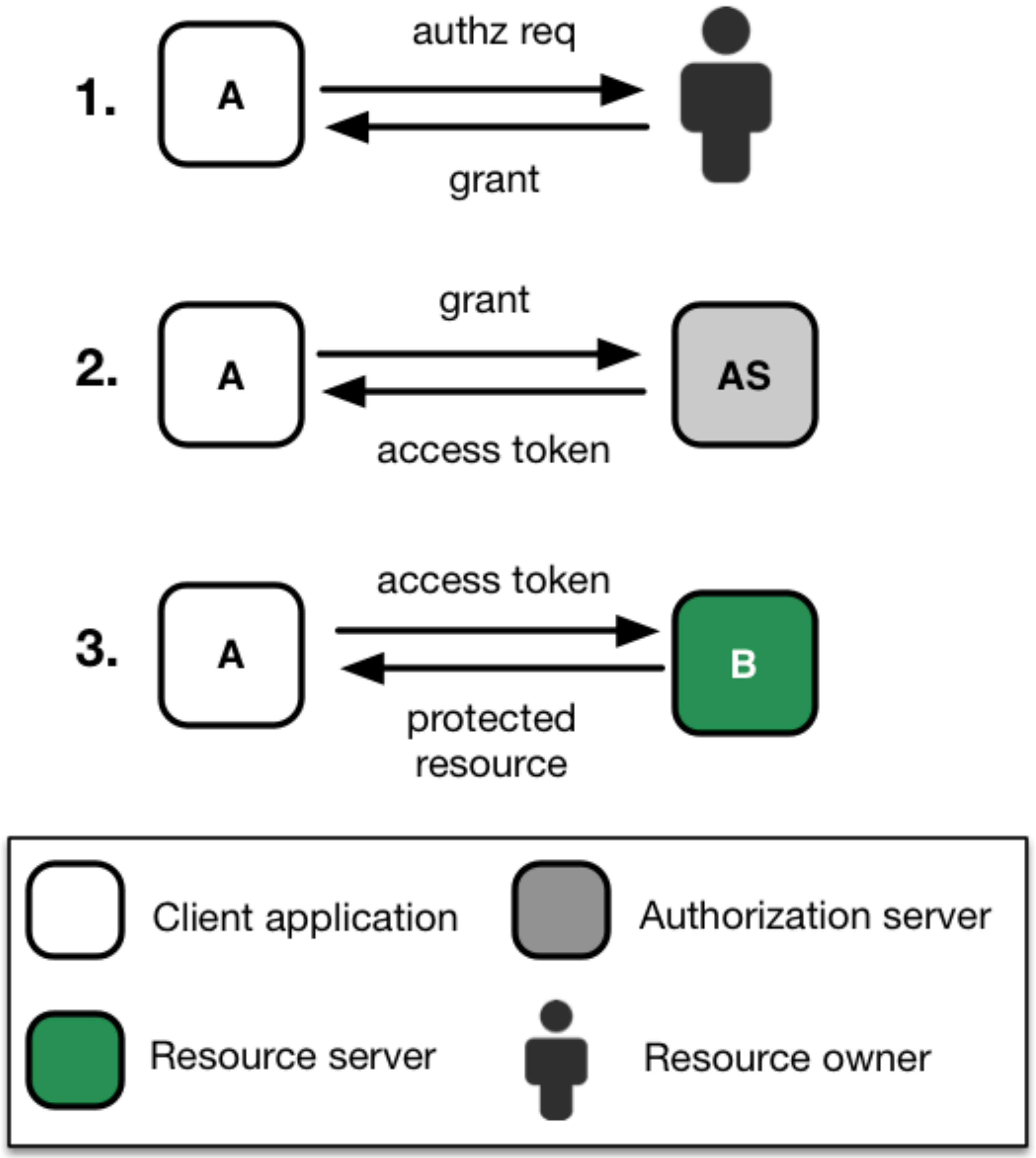
Funded by the European Union's
Horizon 2020 - Grant N° 824064

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/OpenID Connect flows or to access specific endpoints, where different privileges may be assigned to different clients



Funded by the European Union's
Horizon 2020 - Grant N° 824064

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.

Funded by the European Union's Horizon 2020 - Grant N° 824064

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 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

Funded by the European Union's
Horizon 2020 - Grant N° 824064

OAuth/OpenID Connect grant types

Authorization grant types

=

Authorization Flows

=

Ways for an application to get tokens

Funded by the European Union's
Horizon 2020 - Grant N° 824064

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

Funded by the European Union's
Horizon 2020 - Grant N° 824064

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

Example metadata document:

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

Funded by the European Union's
Horizon 2020 - Grant N° 824064

OAuth bearer token usage

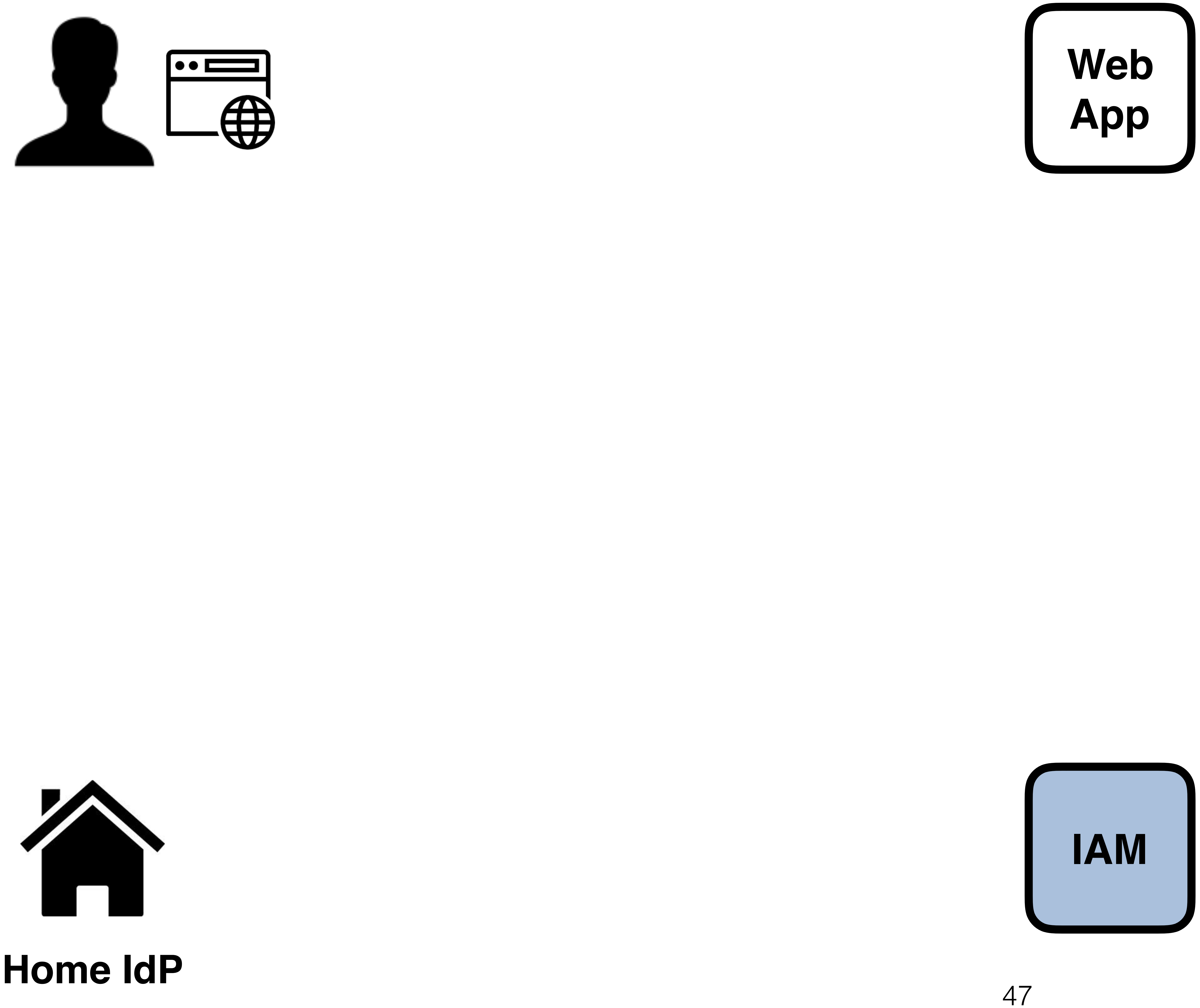
- There's a standard that defines how to send tokens to resource servers
- Typically, tokens are sent in the **Authorization** HTTP header, following the rules defined in RFC 6750, as in the following example HTTP request

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

The token!

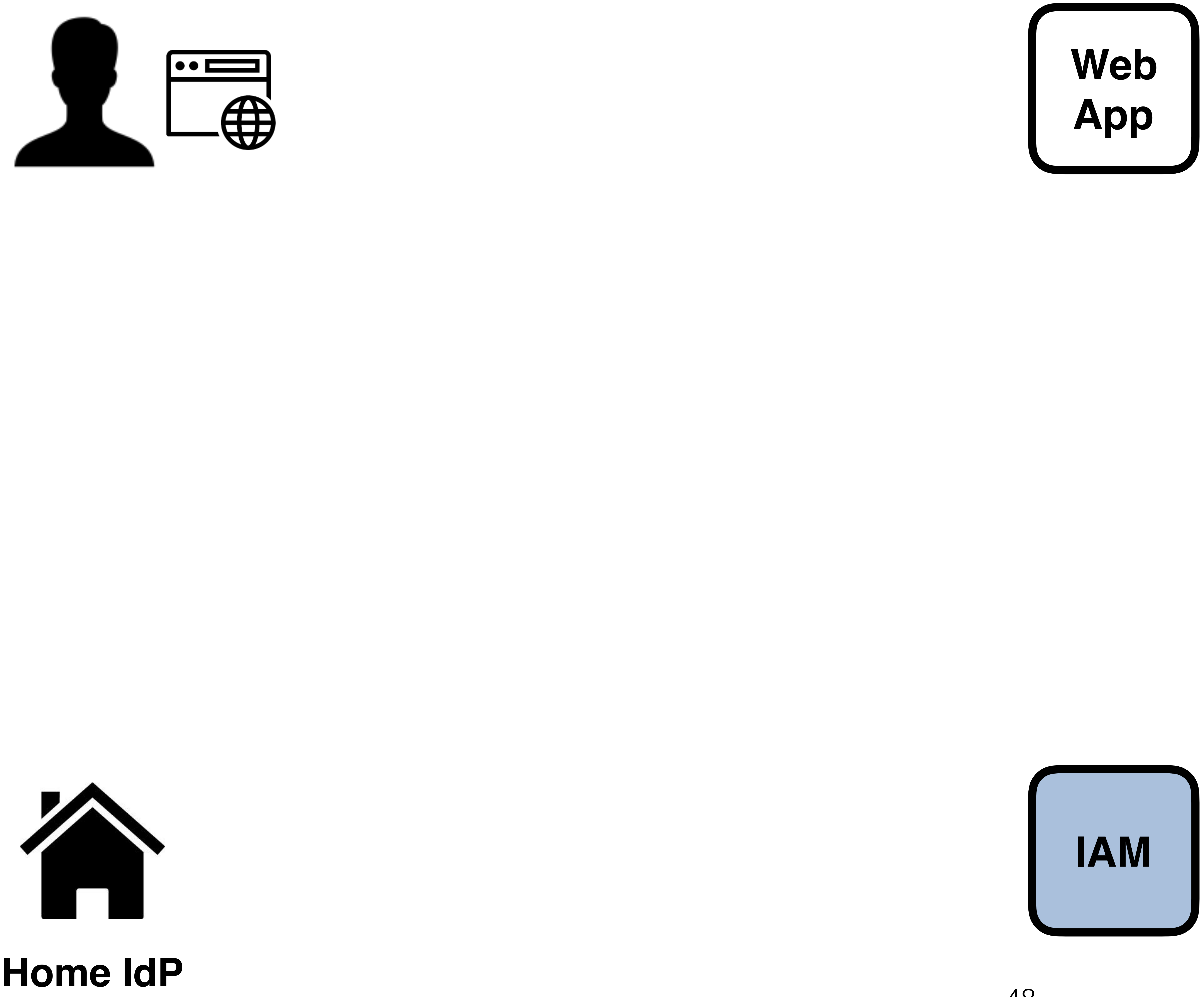
Web application integration scenario

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



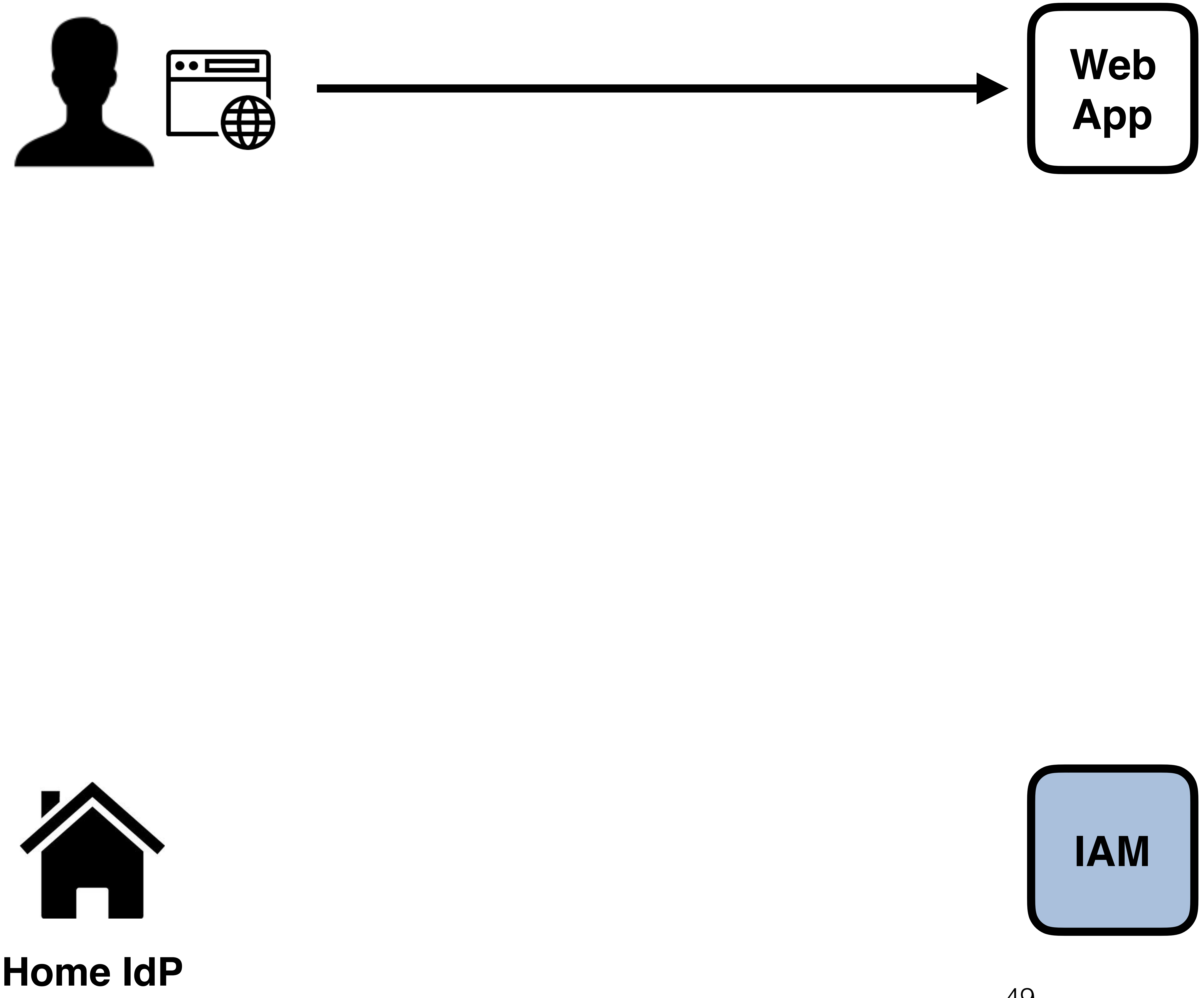
Web App

IAM

Home IdP

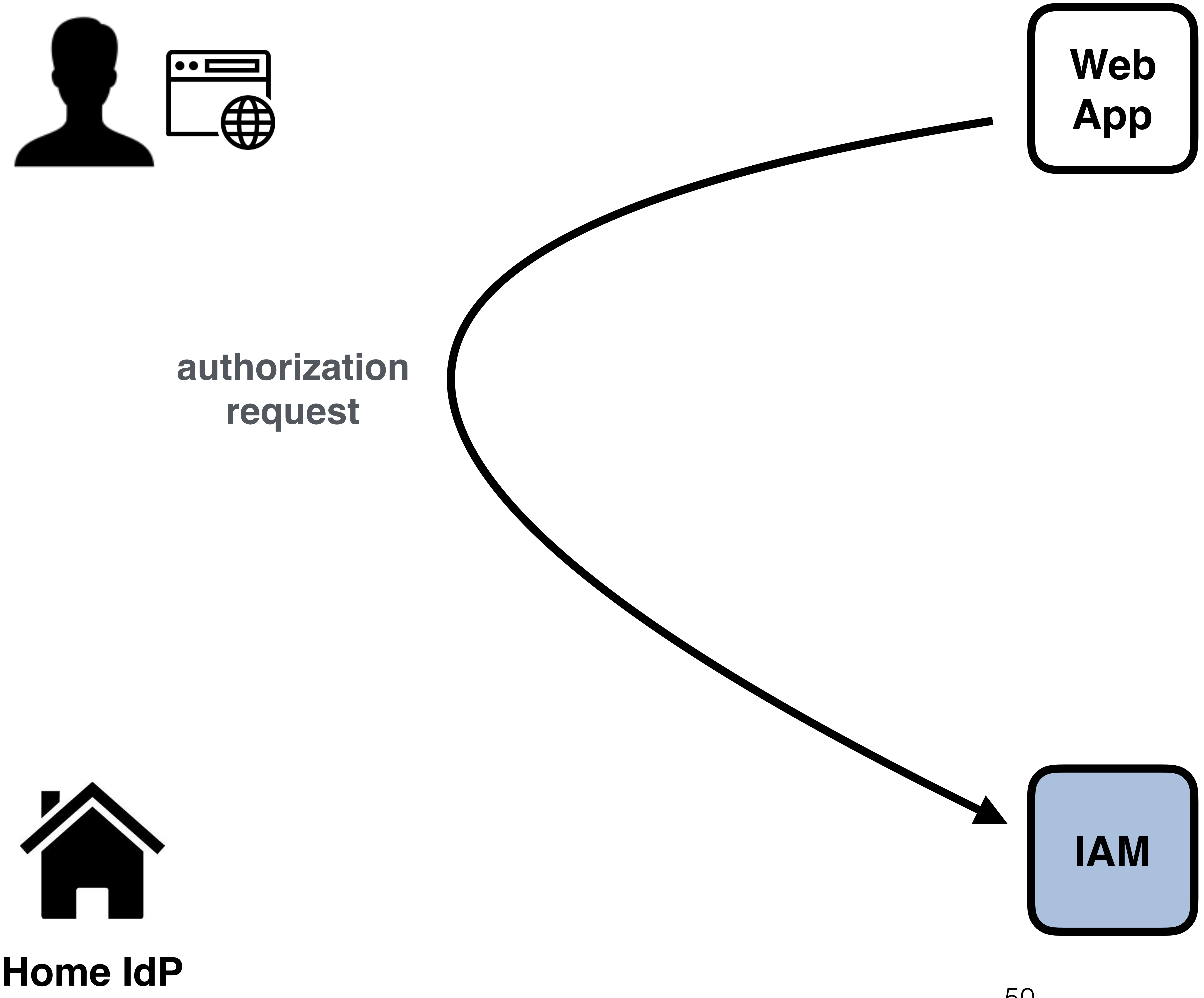
OAuth and OpenID connect provide the **authorization code flow** in support of this integration use case

Web application: authorization code flow



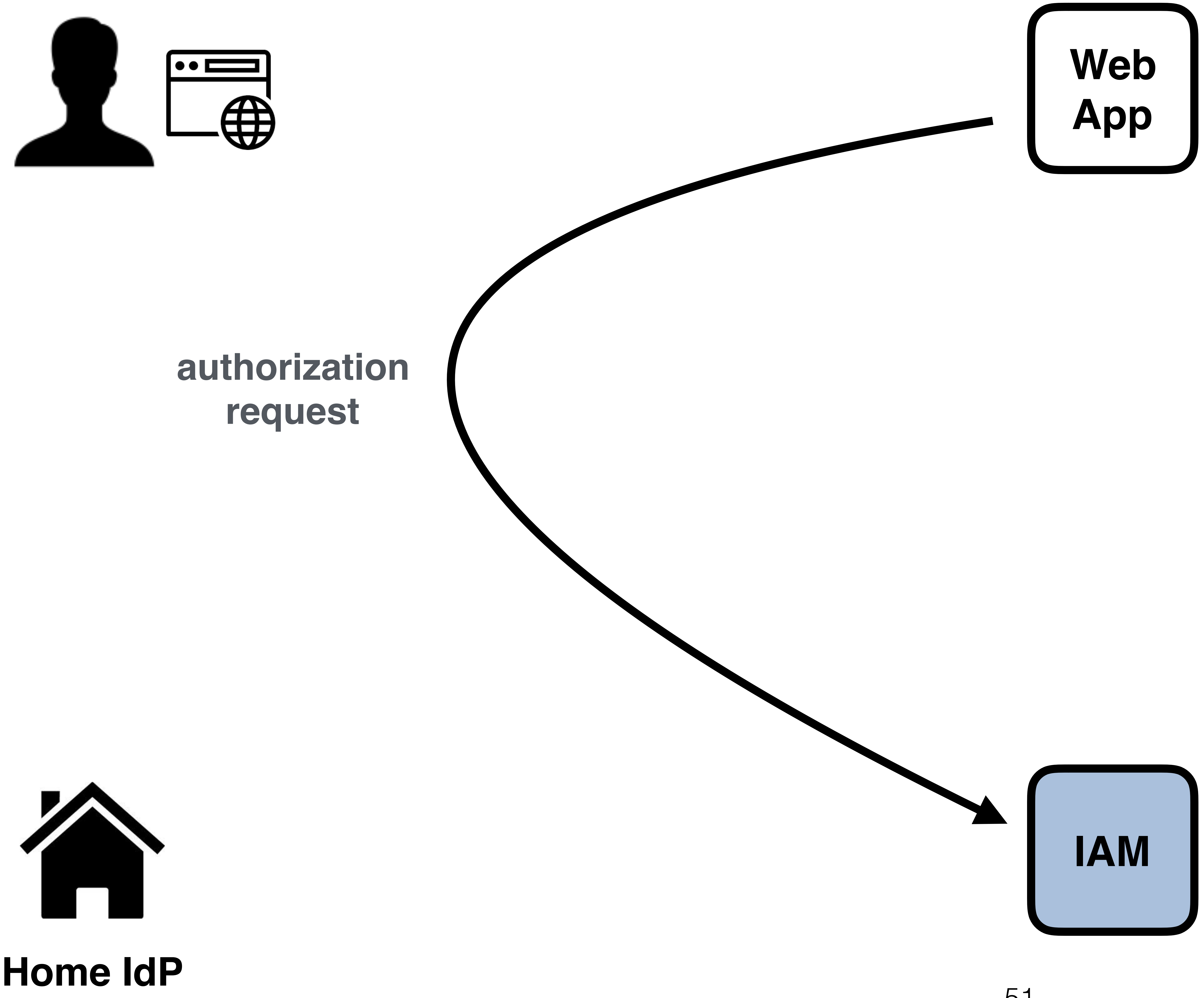
User points its browser to web app, which redirects back to IAM for authentication

Web application: authorization code flow



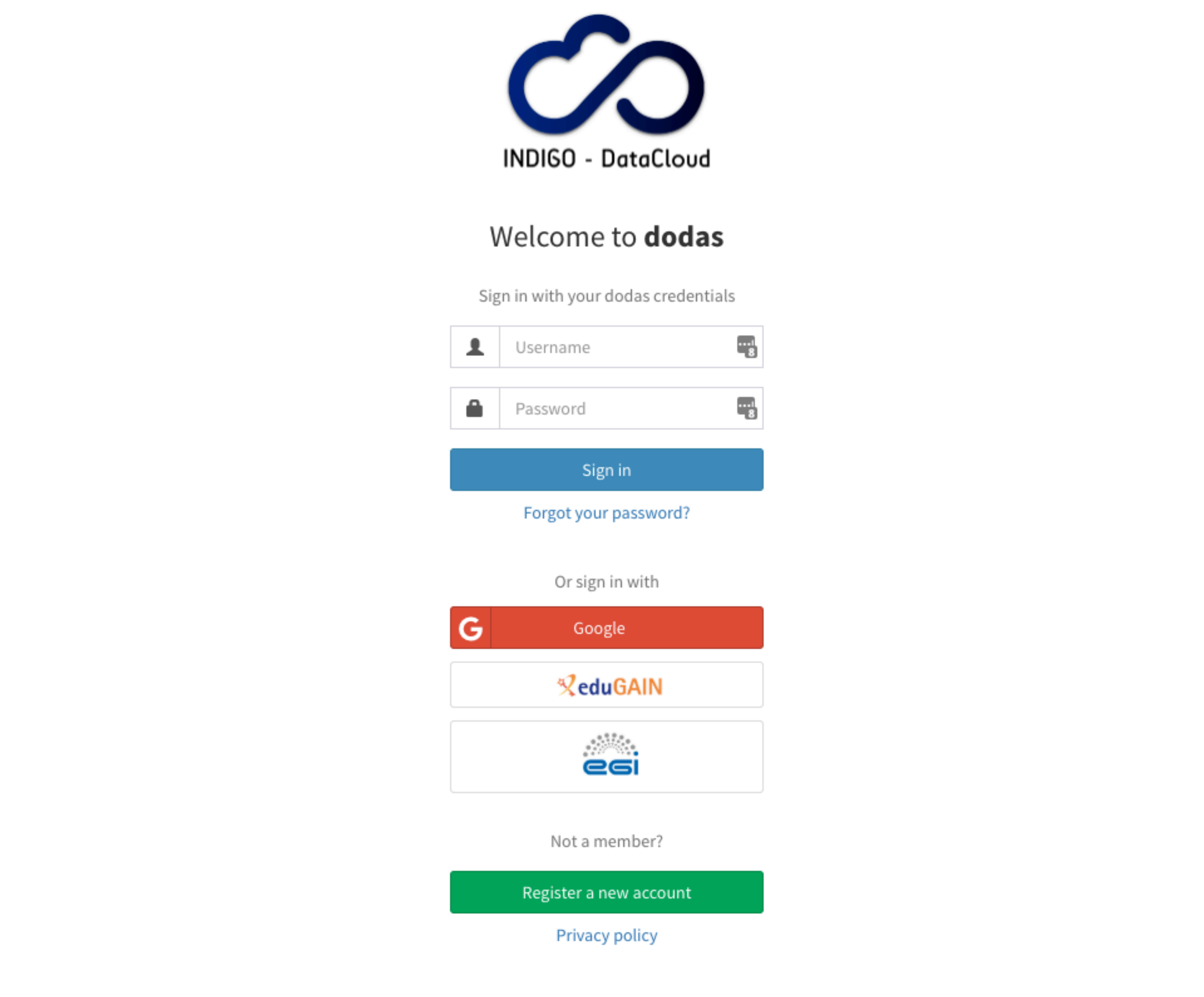
User points its browser to web app, which redirects back to IAM for authentication

Web application: authorization code flow



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

Web application: authorization code flow



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

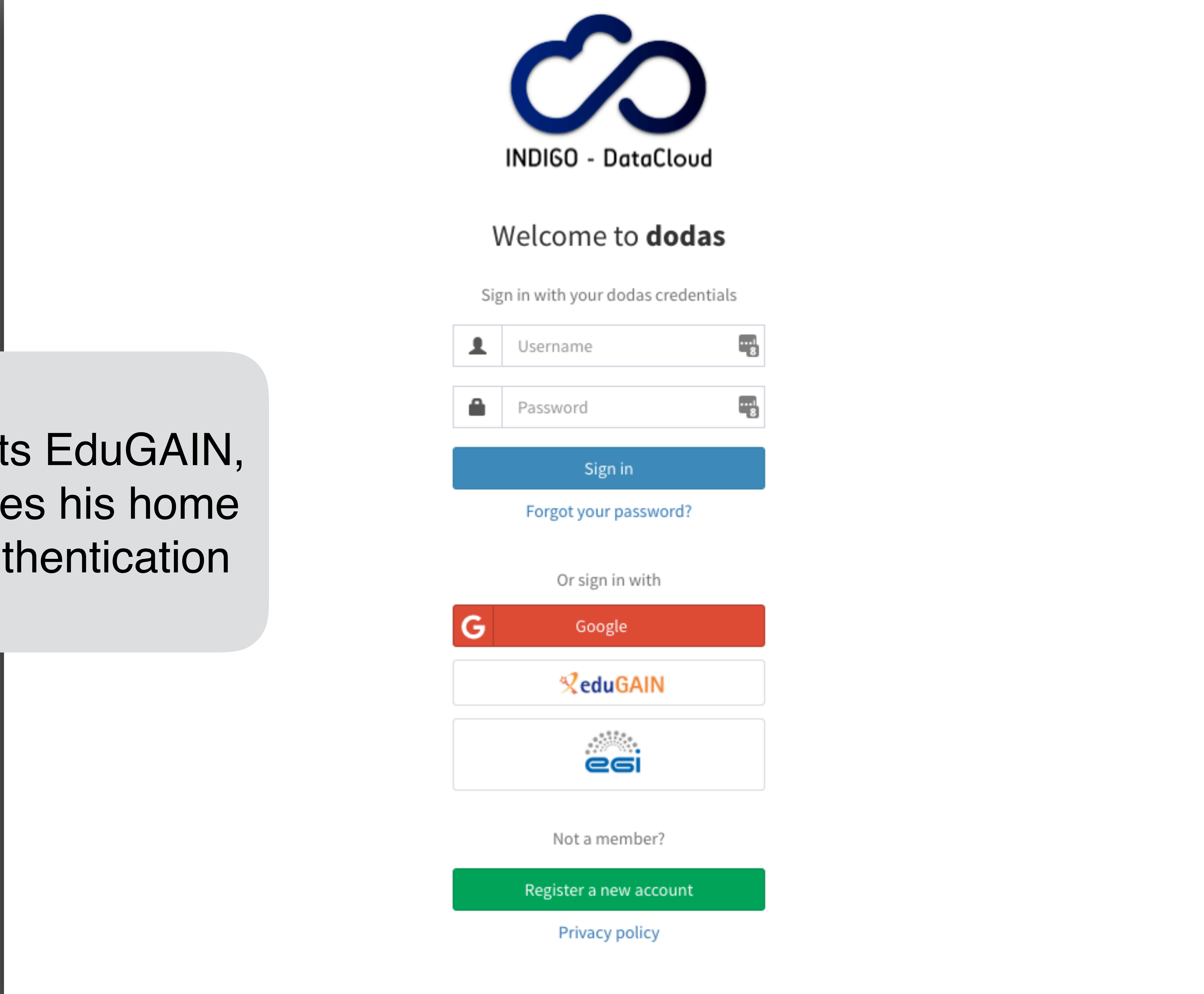
Privacy policy

authorizatio
request

ve a valid session at
ows the login page

Home IdP

Web application: authorization code flow



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

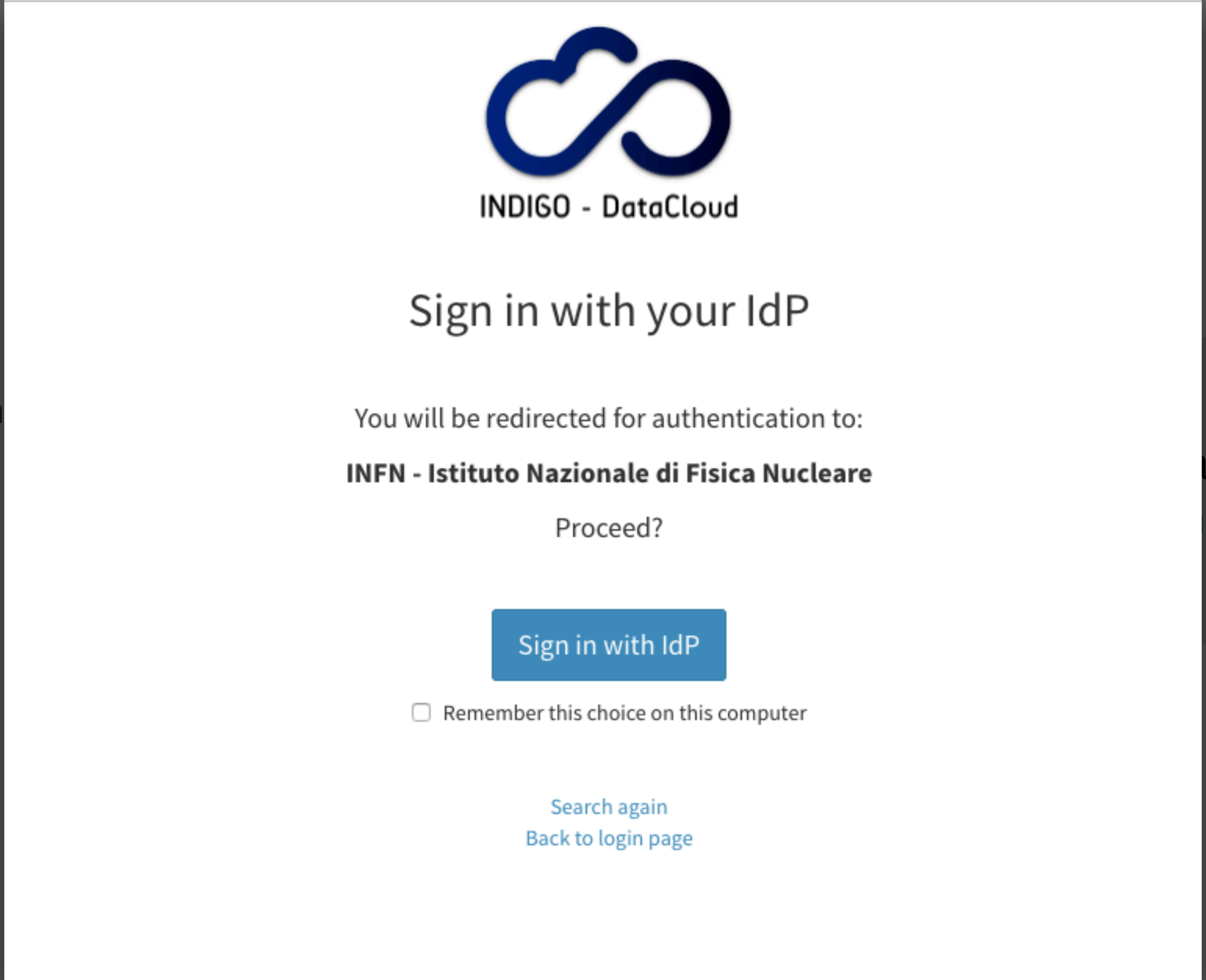
User selects EduGAIN, and chooses his home IDP for authentication

ve a valid session at
ows the login page

Home IdP

Web application: authorization code flow

authorization request



INDIGO - DataCloud

Sign in with your IdP

You will be redirected for authentication to:

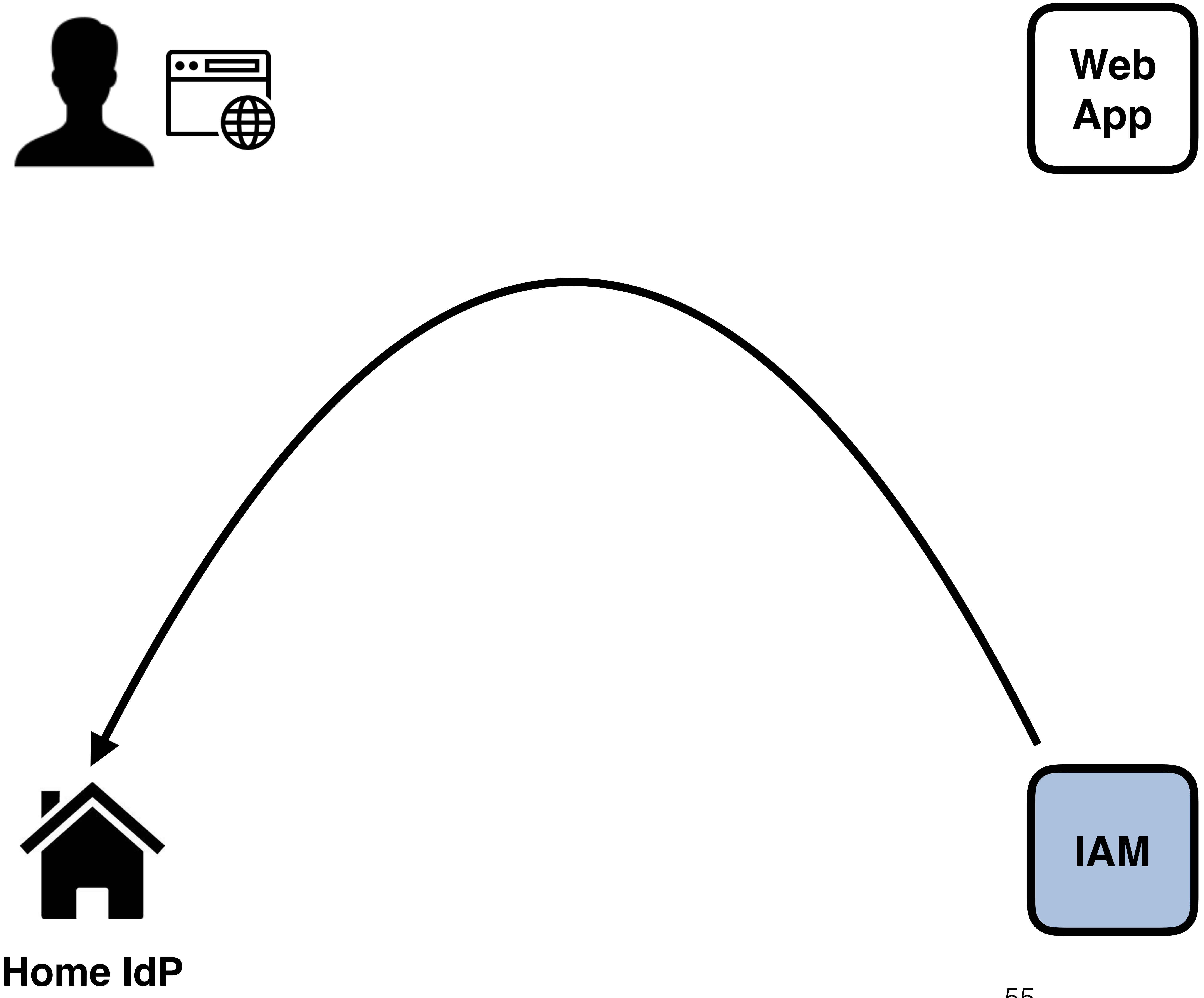
INFN - Istituto Nazionale di Fisica Nucleare

Proceed?

ave a valid session at
ows the login page

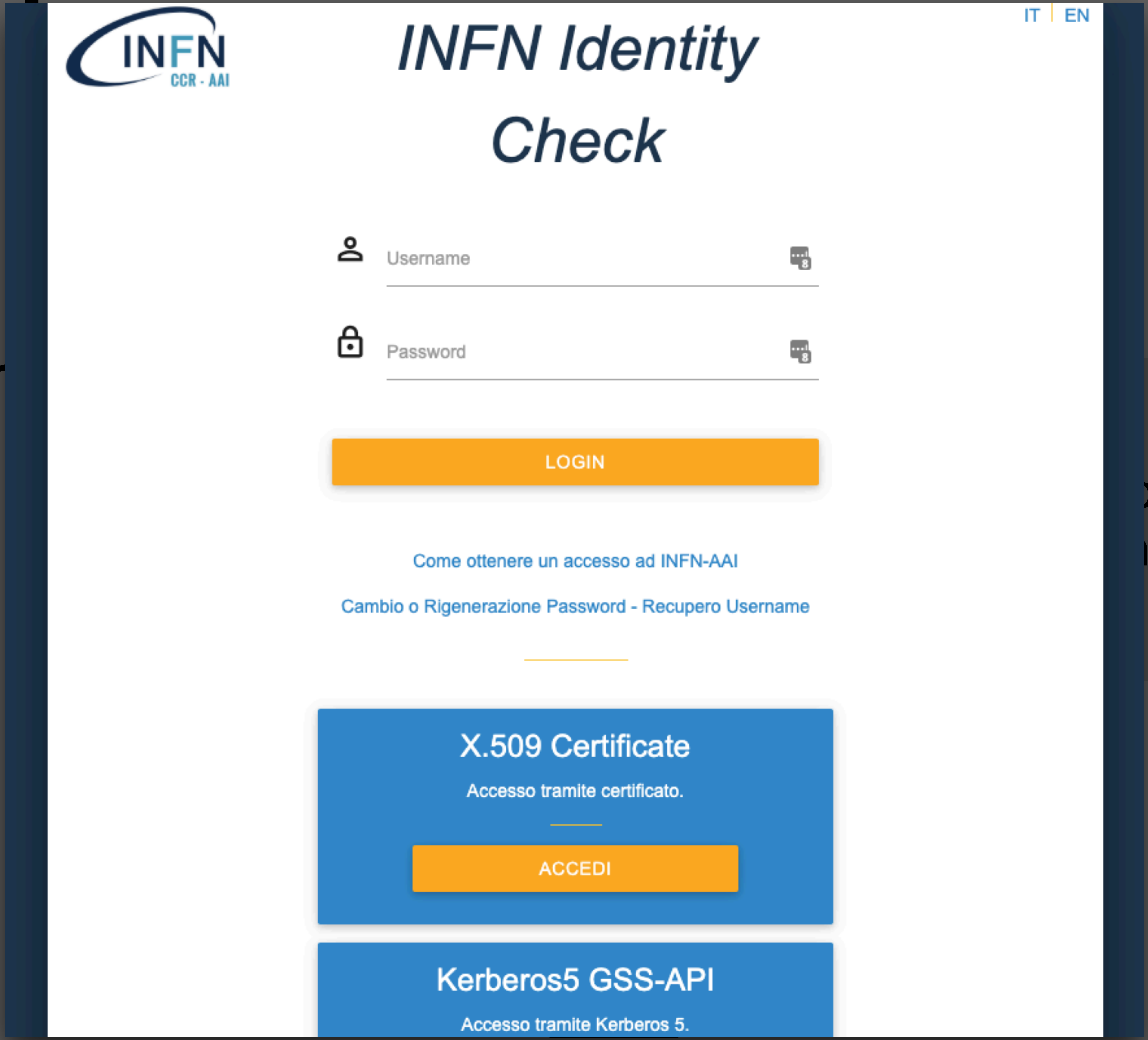
Home IdP

Web application: authorization code flow



User is redirected to home IDP for authentication

Web application: authorization code flow



IT | EN

INFN CCR - AAI

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

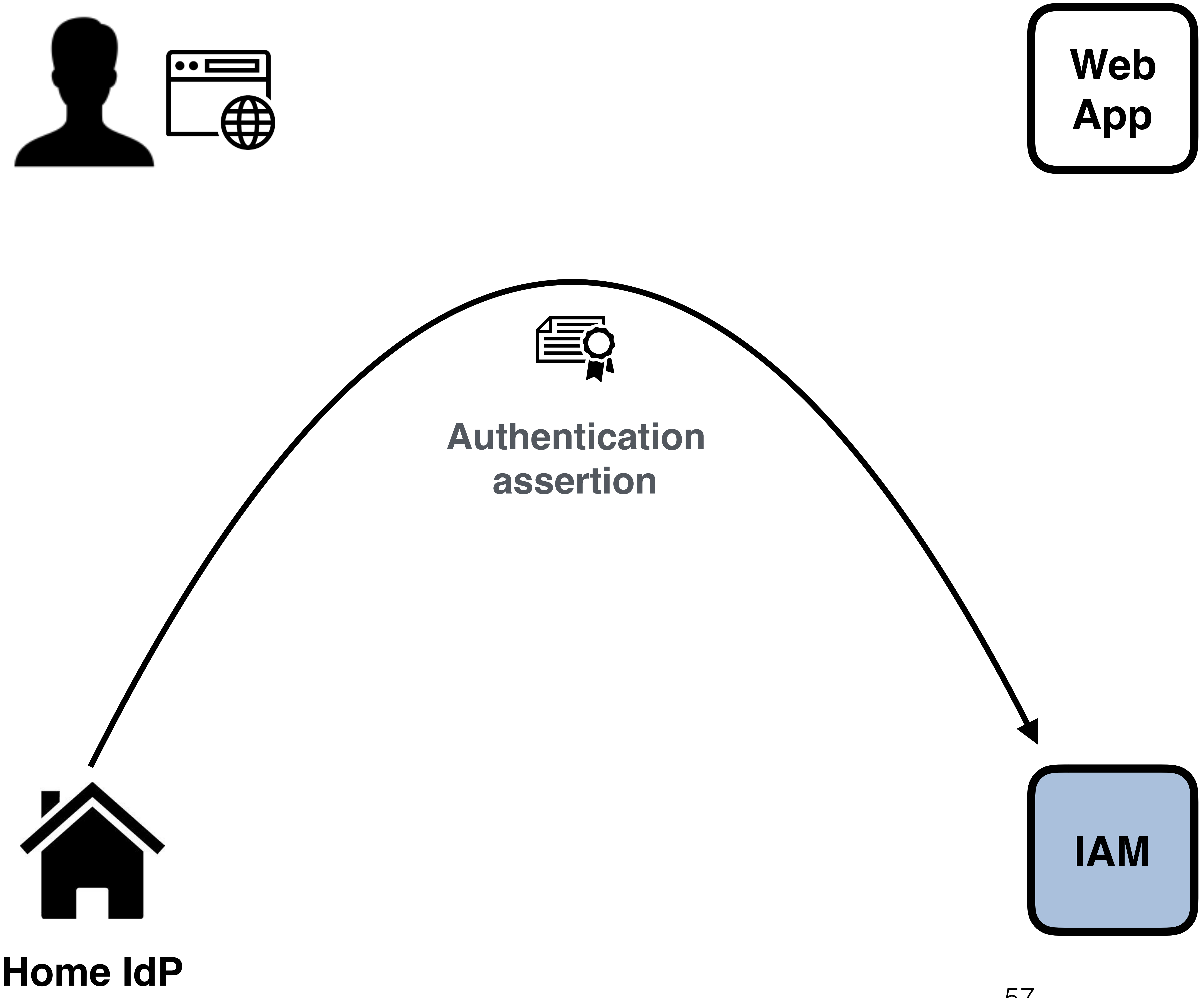
Kerberos5 GSS-API

Accesso tramite Kerberos 5.

cted to home IDP
entication

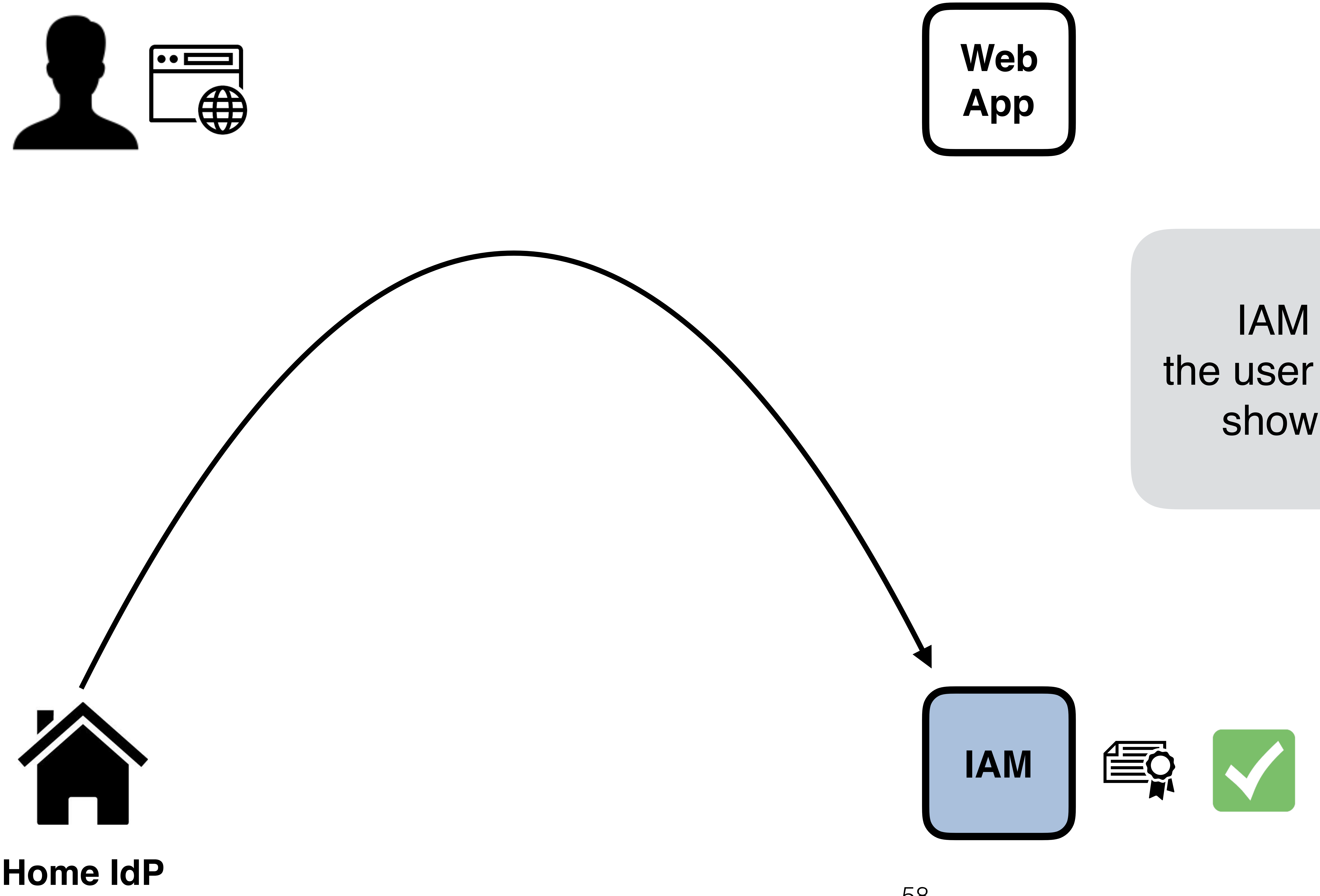
Home IdP

Web application: authorization code flow



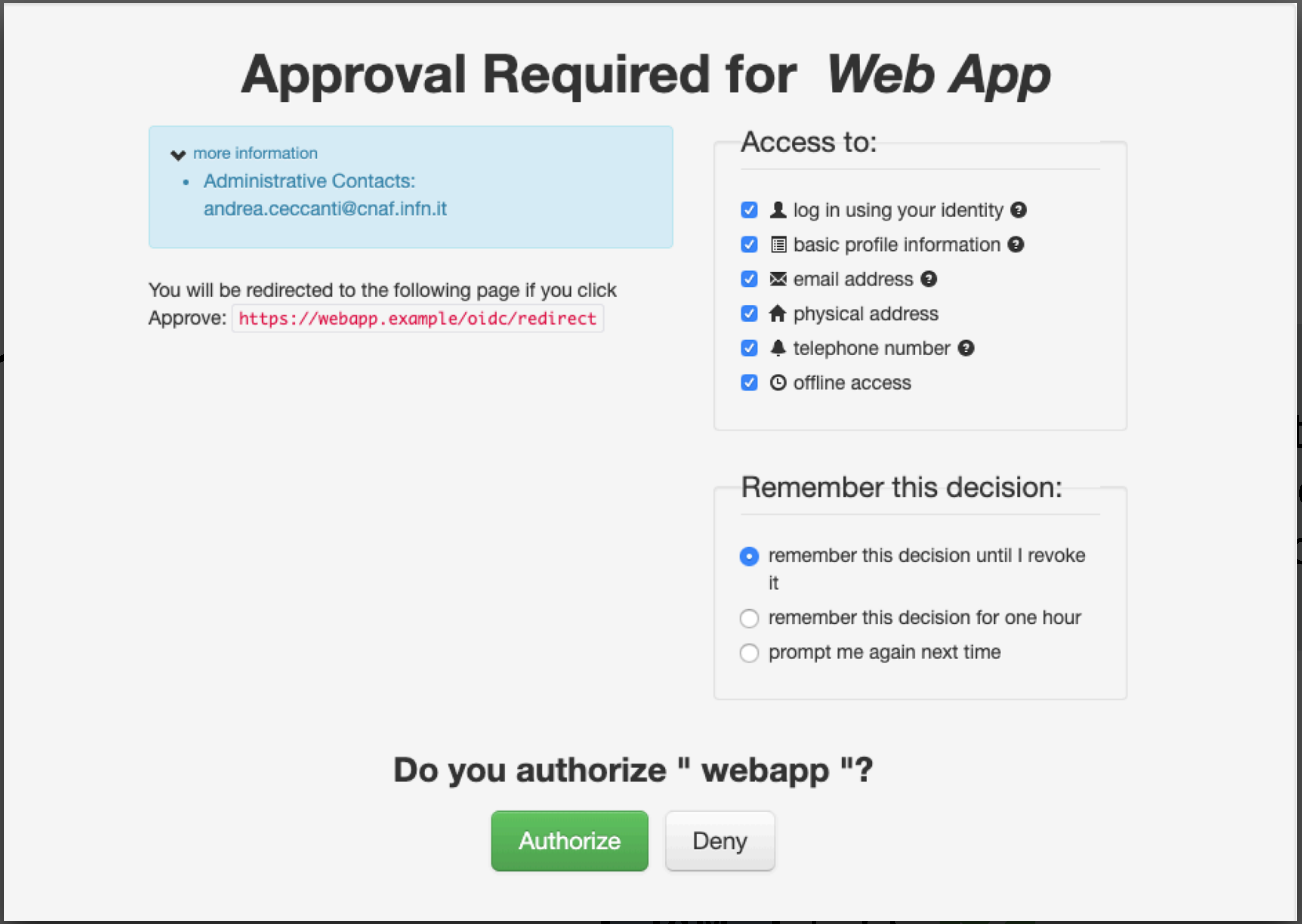
Home IDP authenticates user and sends back an authentication assertion, via redirection and possibly other interactions between IAM and the IDP

Web application: authorization code flow



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

Web application: 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

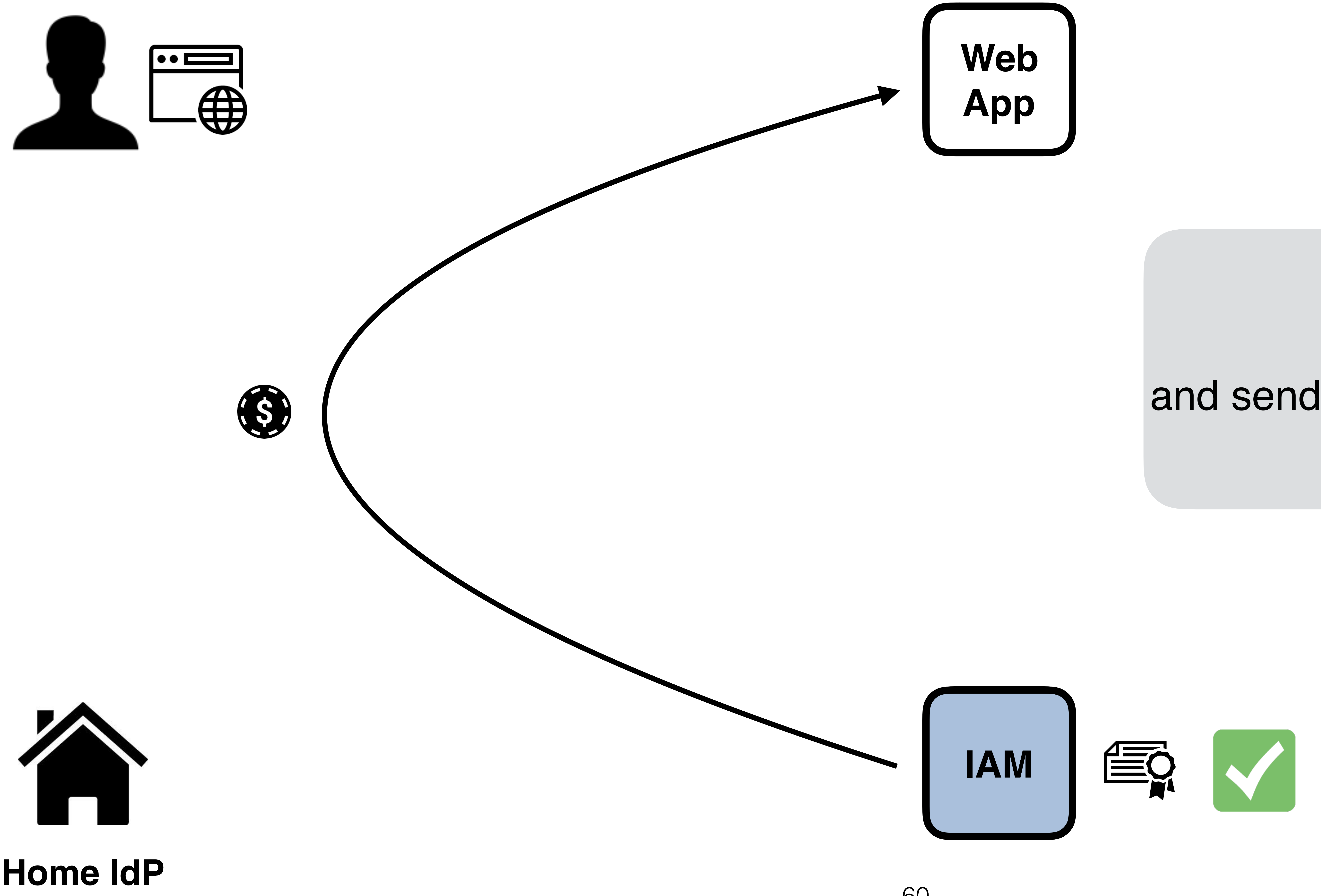
Do you authorize " webapp "?

the assertion,
ered one, so IAM
consent" page

IAM

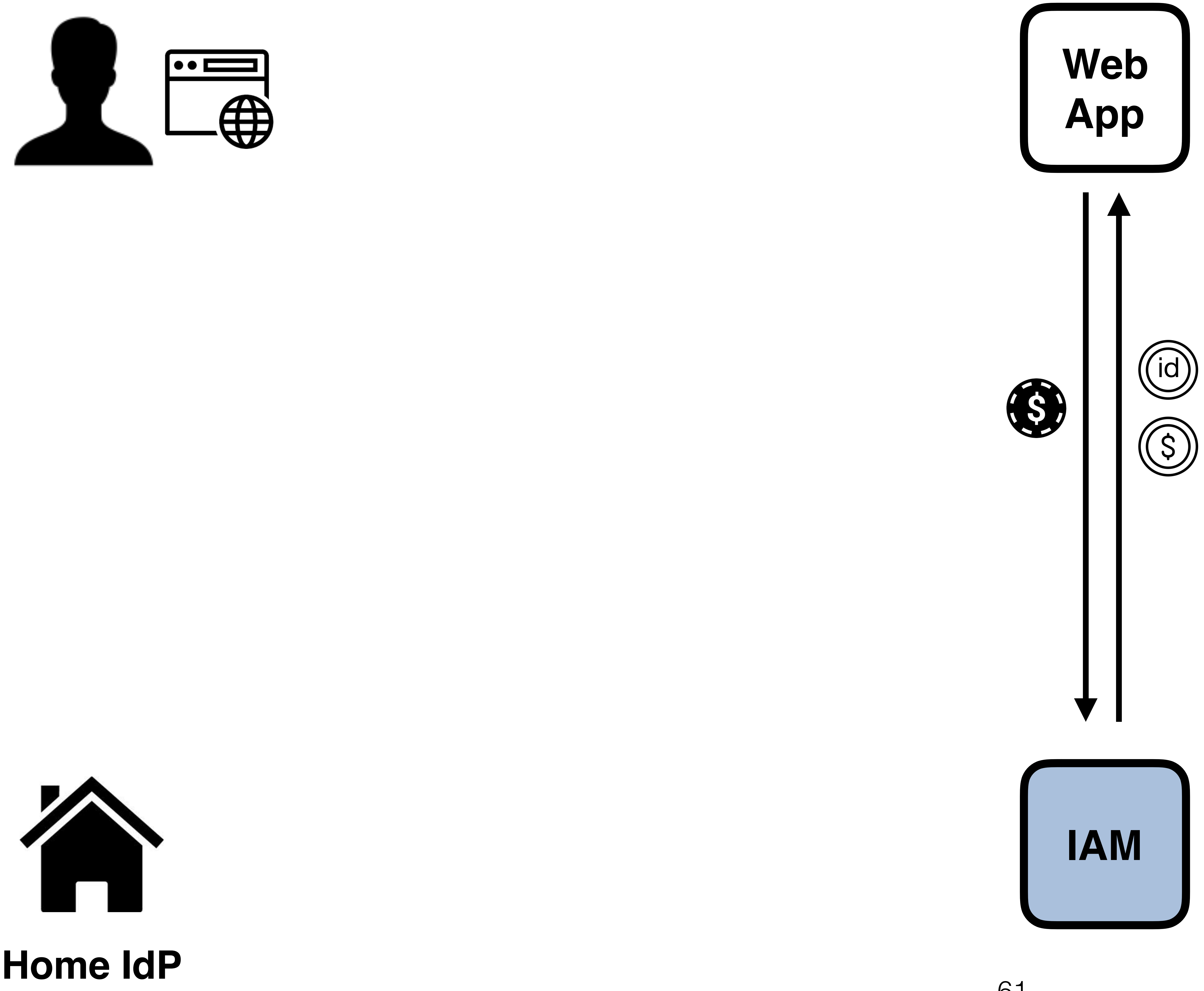
Home IdP

Web application: authorization code flow



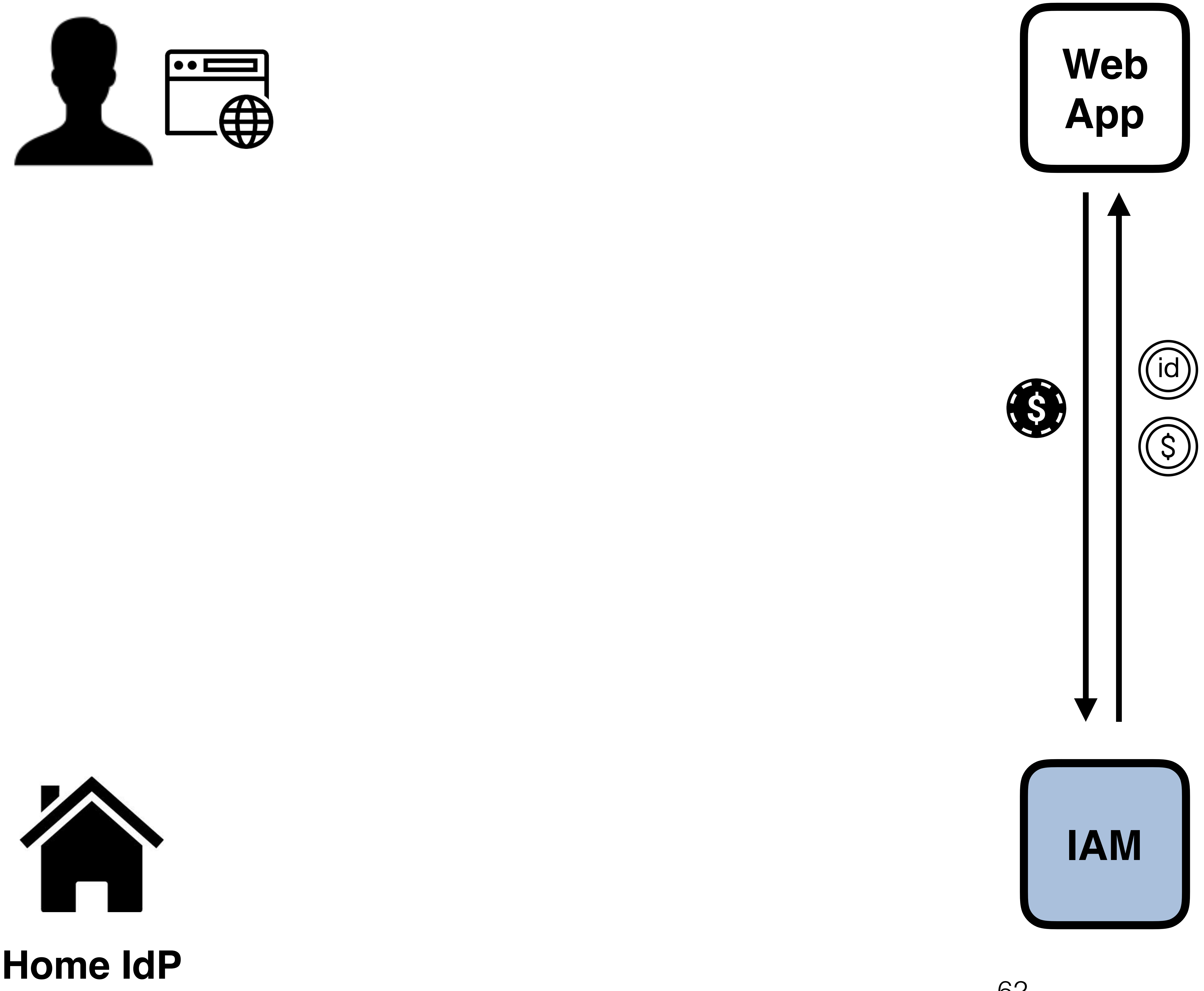
IAM generates an
authorization code
and sends it back to web app using an
HTTP redirect

Web application: authorization code flow



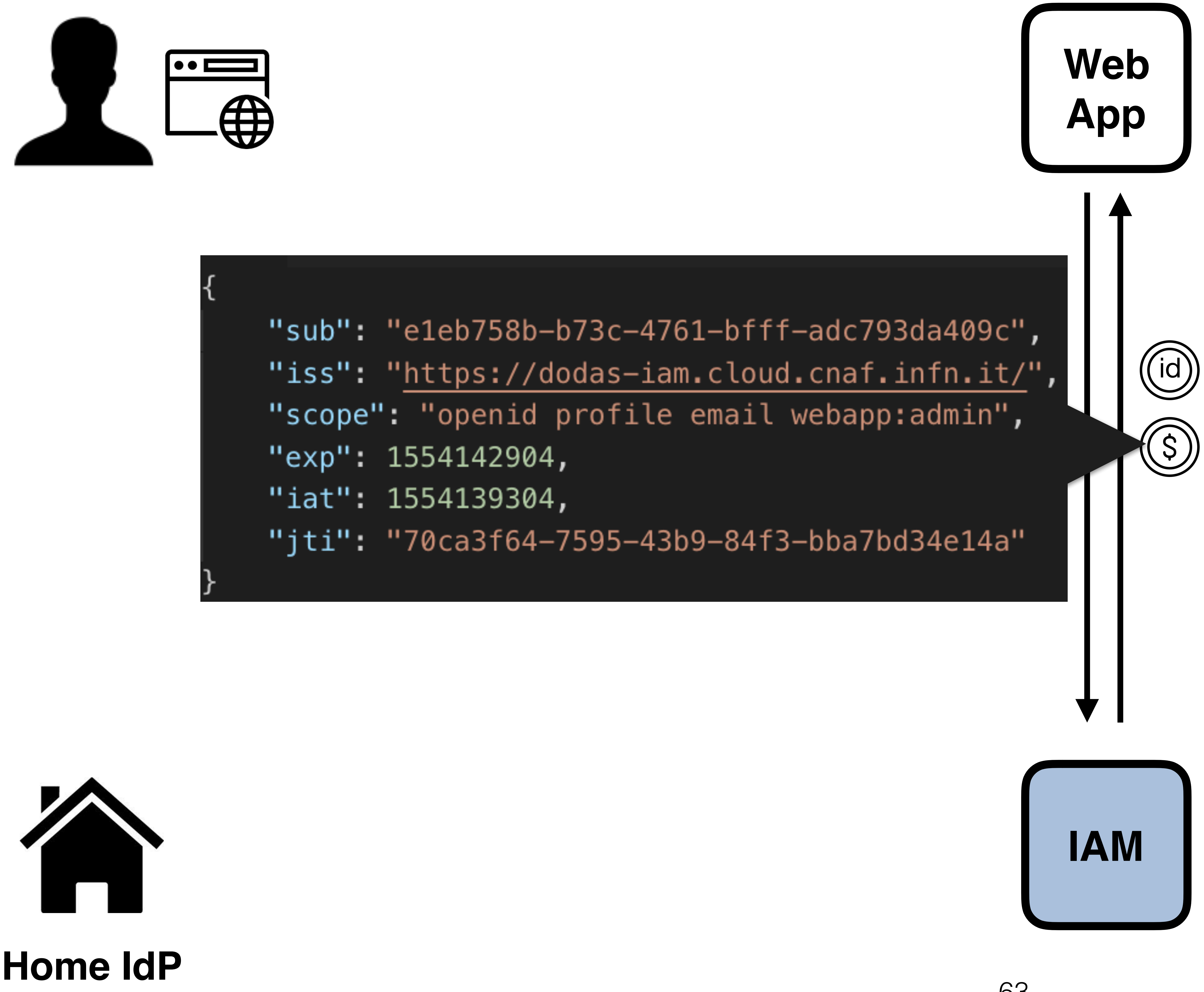
The Web App exchanges the **authorization code** with a couple of tokens: an **access token** and an **id token**

Web application: authorization code flow



In IAM,
both tokens are
JWT tokens.

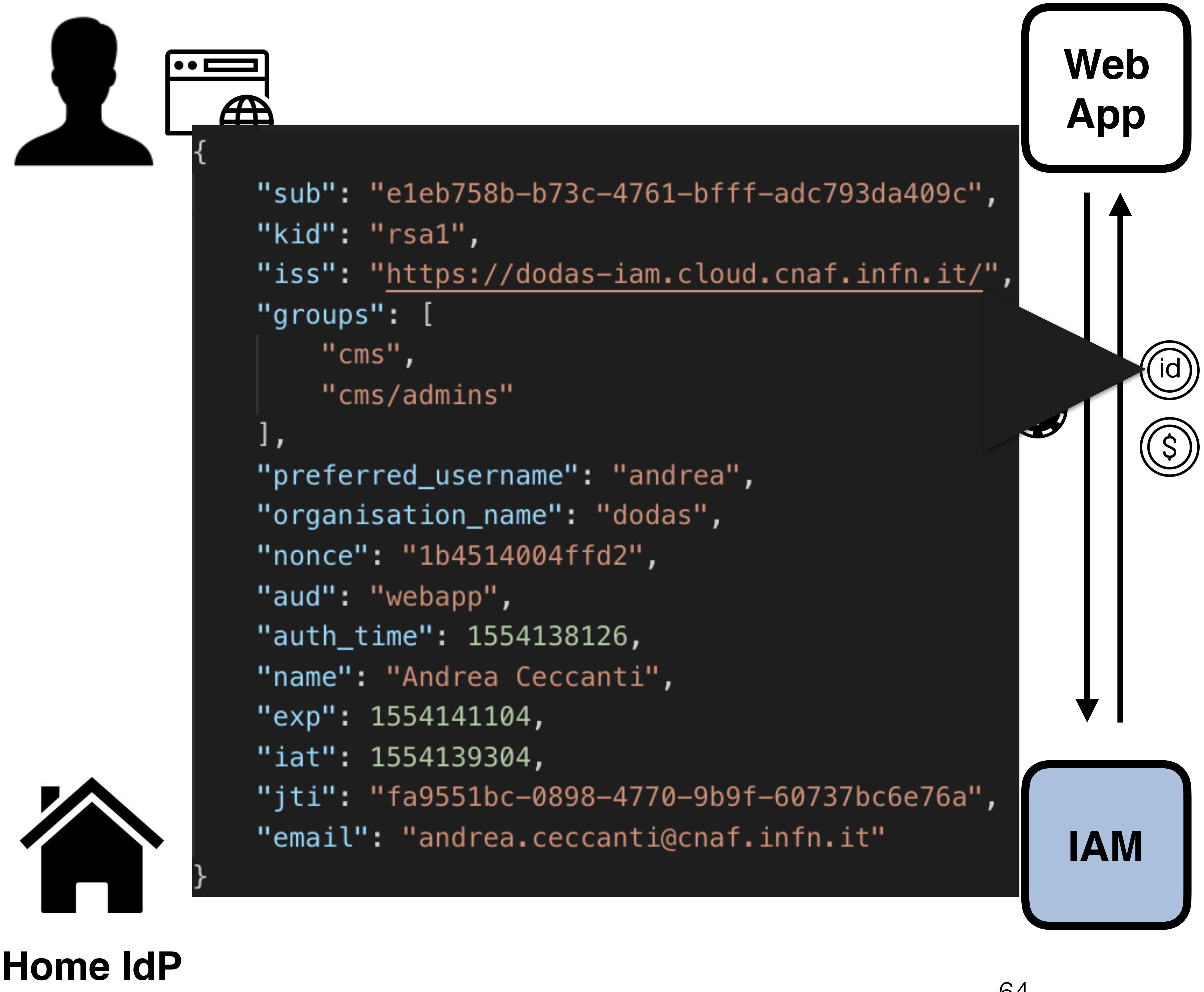
Web application: authorization code flow



```
{
    "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

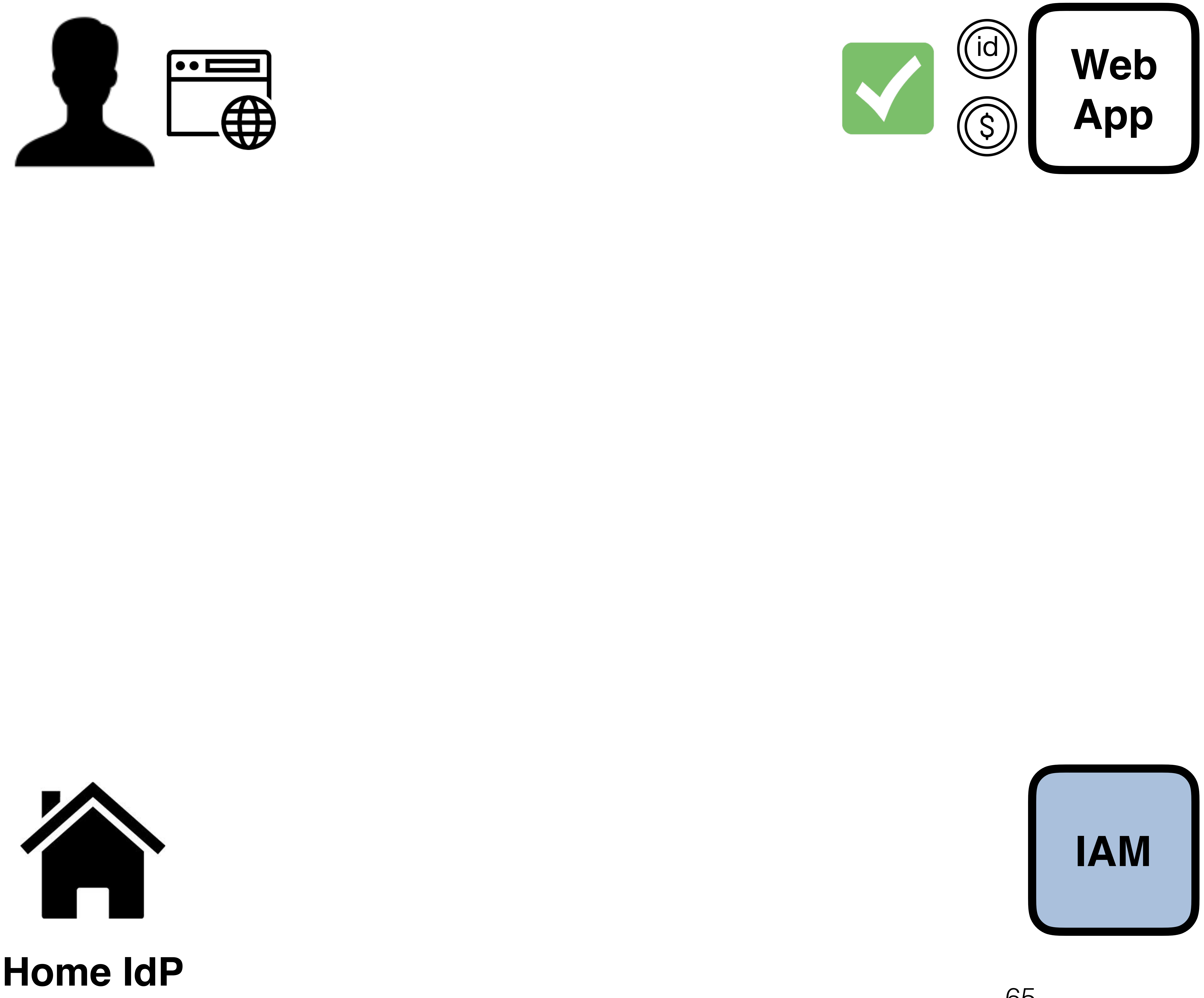
Web application: authorization code flow



```
{
    "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"
}
```

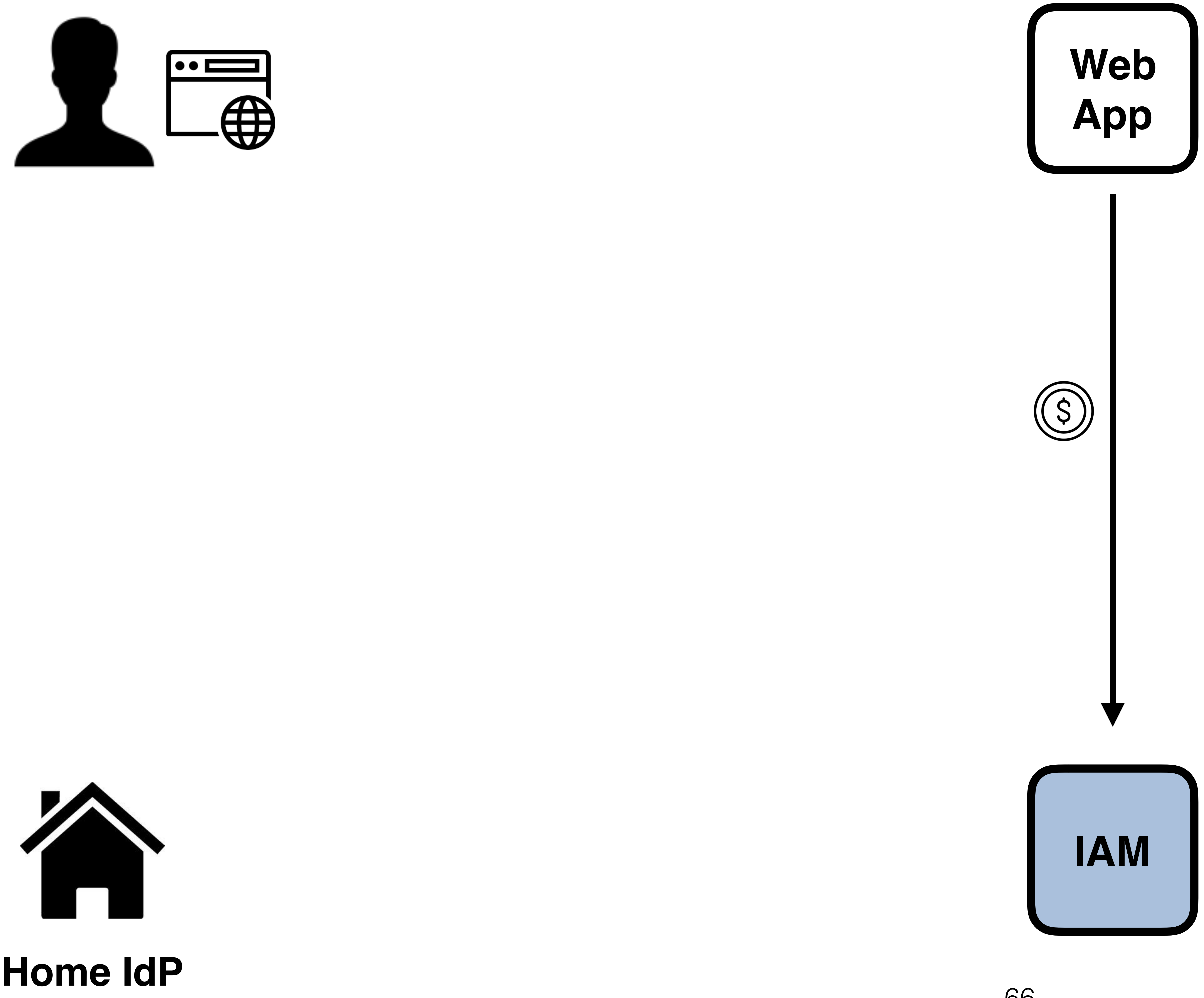
The **id token** provides (mainly) authentication information

Web application: authorization code flow



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

Web application: 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 in practice

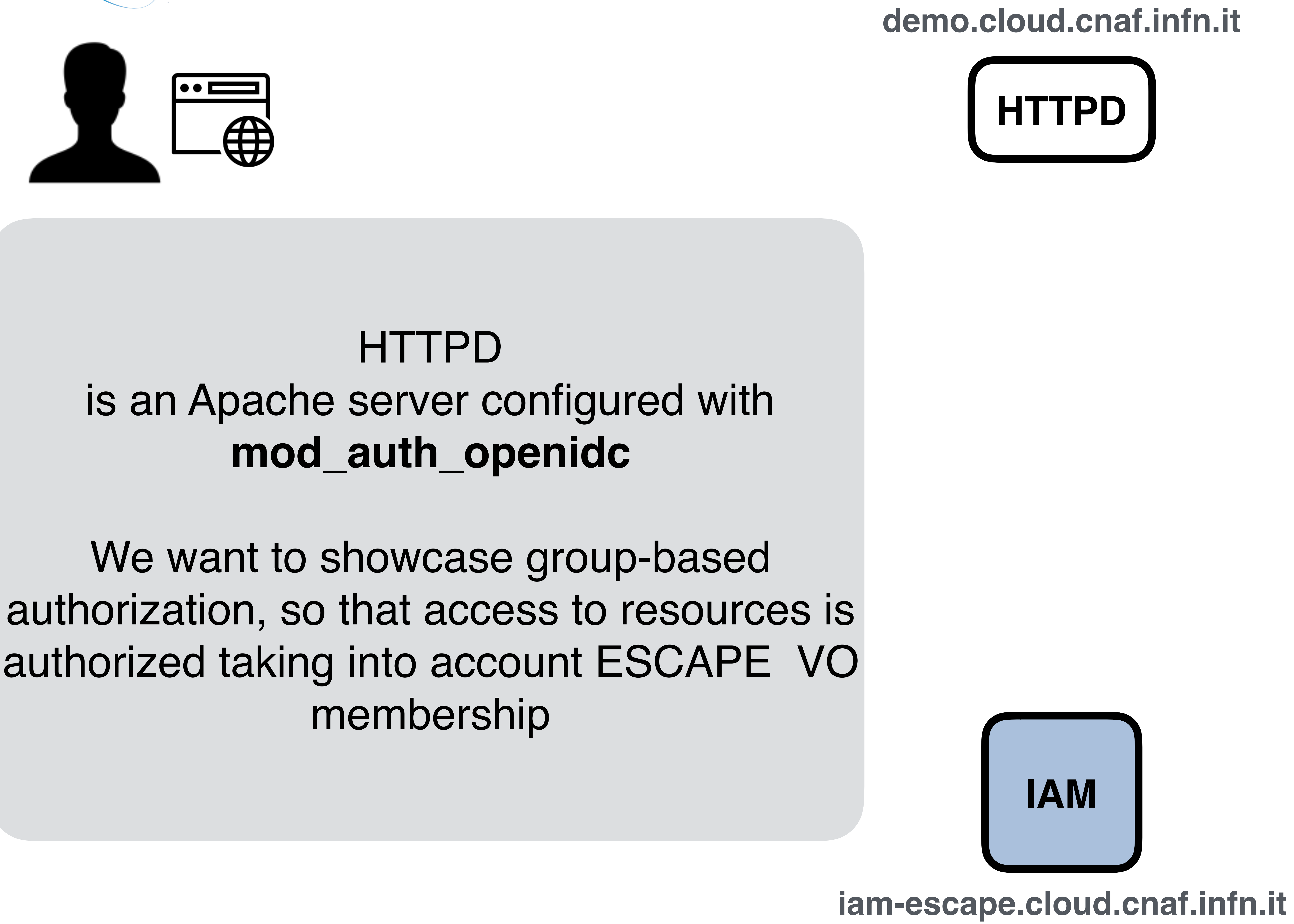
- In practice, decent OAuth/OpenID Connect client libraries implement all the above **behind the scenes.**

- 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

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Integration Demo setup



HTTPD
is an Apache server configured with
mod_auth_openidc

We want to showcase group-based authorization, so that access to resources is authorized taking into account ESCAPE VO membership

Integration Demo setup

demo.cloud.cnaf.infn.it

HTTPD

HTTPD
is an Apache server configured with
mod_auth_openidc

We want to showcase group-based authorization, so that access to resources is authorized taking into account ESCAPE VO membership

Access policies

/escape is accessible from all members of the **ESCAPE** organization

/lofar is accessible from members of the **/escape/lofar** group in the ESCAPE organization

IAM

iam-escape.cloud.cnaf.infn.it

Integration demo

Apache mod_auth_openidc configuration

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

<VirtualHost _default_:80>

  OIDCProviderMetadataURL https://iam-escape.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 /escape>
    …
    AuthType openid-connect
    Require valid-user
    LogLevel debug
  </Location>

…
```

Apache mod_auth_openidc configuration

```
   <Location /lofar>
    …
    AuthType openid-connect
    Require claim groups:escape/lofar
  </Location>

</VirtualHost>
```

AuthN/Z in the ESCAPE Data-lake testbed

1. Start with “traditional” Grid AuthN/Z approach
   - GSI X.509 authN + VOMS authorization
   - Coarse-grained VO-level authorization
   - Fine-grained group/role-based authorization

2. Demonstrate Token-based AuthN/Z approach
   - Flexible AuthN (e.g., EduGAIN) + OAuth-based authorization
   - Coarse-grained VO-level authorization
   - Fine-grained, group or scope-based authorization

Both approaches are supported **now** by IAM and most data management services

Funded by the European Union’s
Horizon 2020 - Grant N° 824064

AuthN/Z in the Datalake demo

What will be demonstrated

- Registering a client in IAM using oidc-agent
- Obtaining tokens out of IAM using oidc-agent
- Data access and management with DAVIX and VOMS authn/z
- Data access and management with DAVIX and token-based authn/z

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Installing oidc-agent on your system

- OIDC agent is a useful too to get tokens in your terminal session

- To install oidc-agent in your system, see:
    - https://github.com/indigo-dc/oidc-agent

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Thanks for your attention!

Questions?

Useful references

- IAM ESCAPE docs: https://indigo-iam.github.io/escape-docs
- IAM on GitHub: https://github.com/indigo-iam/iam
- IAM documentation: https://indigo-iam.github.io/docs
- IAM in action video: https://www.youtube.com/watch?v=1rZlvJADOnY
- Apache integration demo: https://github.com/andreaceccanti/iam-tutorial/tree/master/apache-integration-demo
- Contacts:
  - andrea.ceccanti@cnaf.infn.it
  - enrico.vianello@cnaf.infn.it
  - indigo-aai.slack.com