ESCAPE

European Science Cluster of Astronomy &
Particle physics ESFRI research Infrastructures

AAI in WP2 - DIOS

Andrea Ceccanti (INFN)

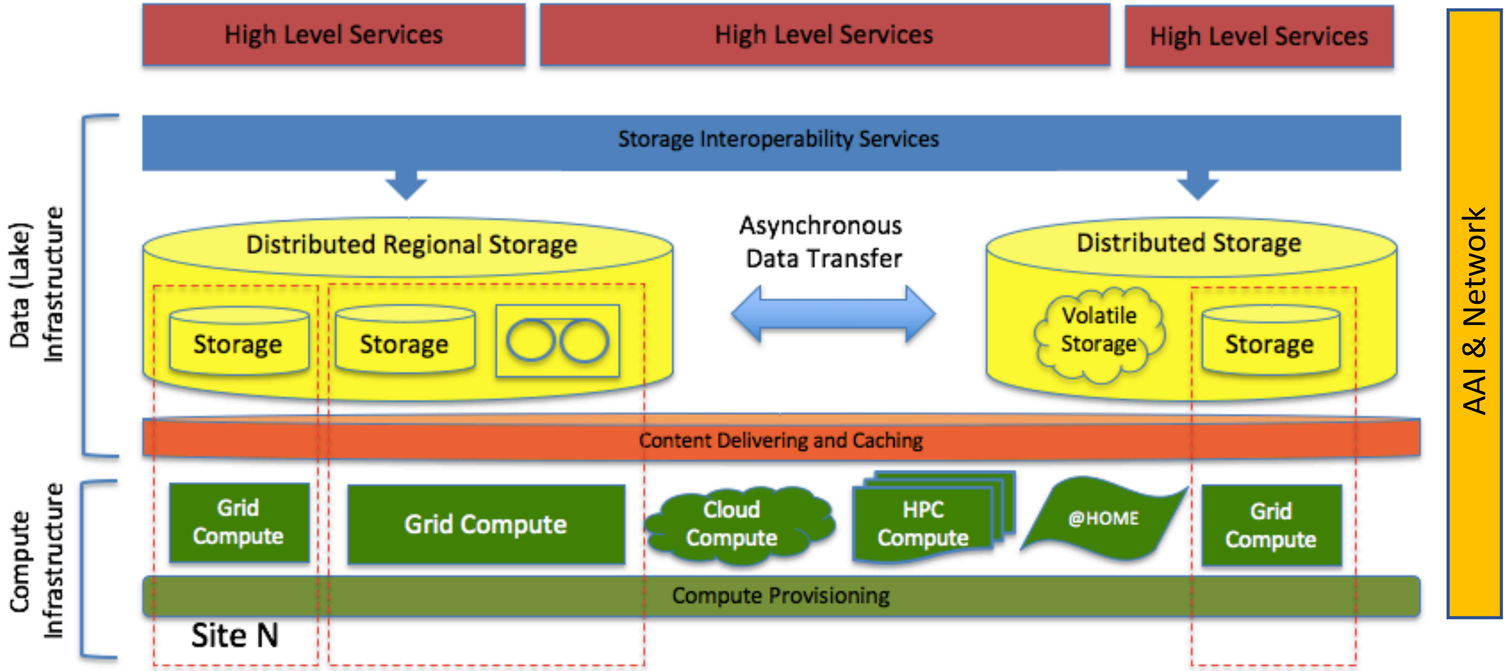
ESCAPE Progress Meeting Bruxelles

February, 26/2/2020

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

The ESCAPE data lake

Data Lake building blocks



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

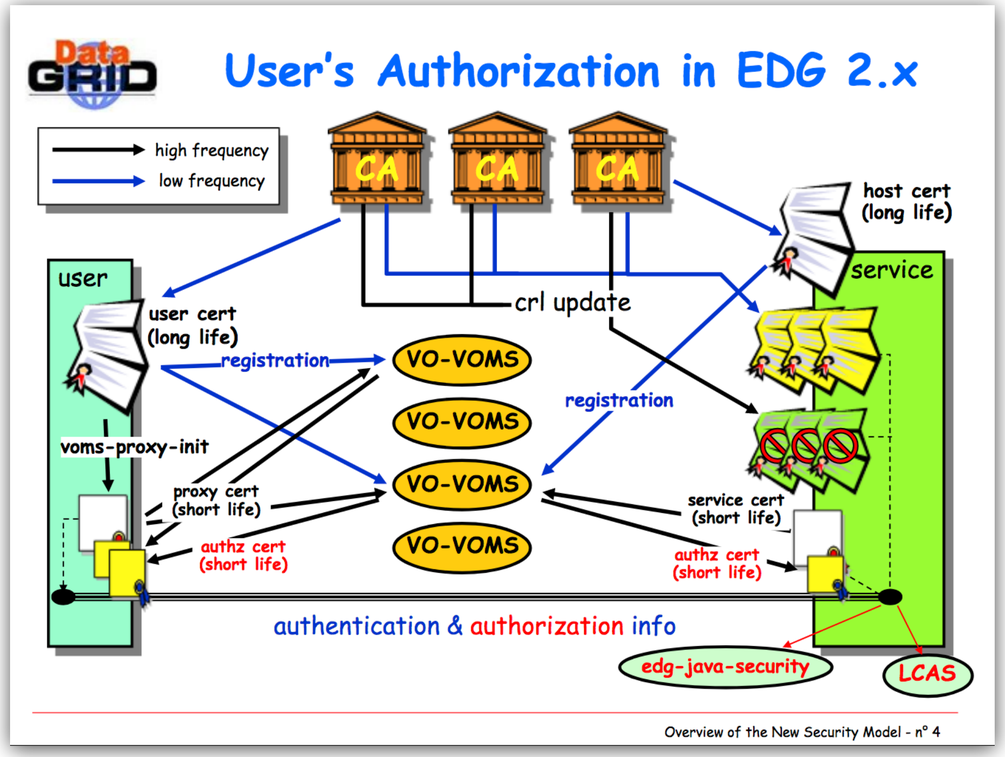
Leaves to the science projects the flexibility to choose the services and layout most suitable to their needs. Provides a reference implementation

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

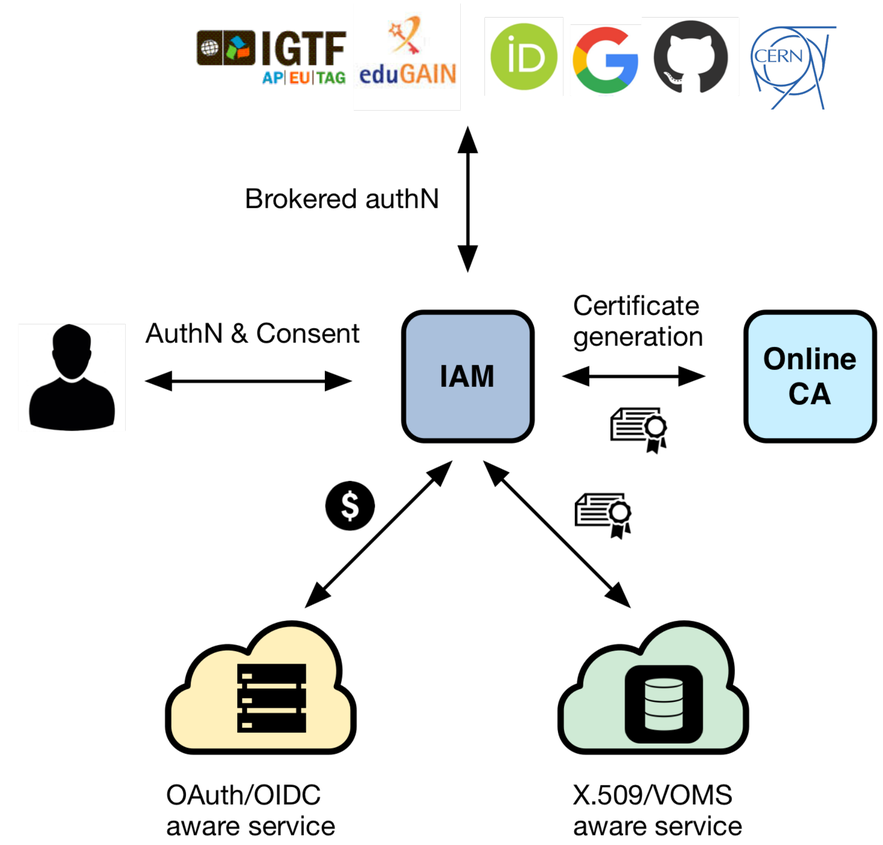
ESCAPE Data Lake AAI and WLCG

Current, X.509 based AAI



Move beyond X.509

Future, token-based AAI



Approach: leverage and build upon the WLCG experience

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

Moving beyond X.509: main challenges

- **Authentication**
  - **Flexible**, able to accomodate various authentication mechanisms
    - X.509, username & password, EduGAIN, …
- **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**

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

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**
    applications
    provisioning of
    ng resources
  - Enable **integration with legacy services through controlled credential translation**

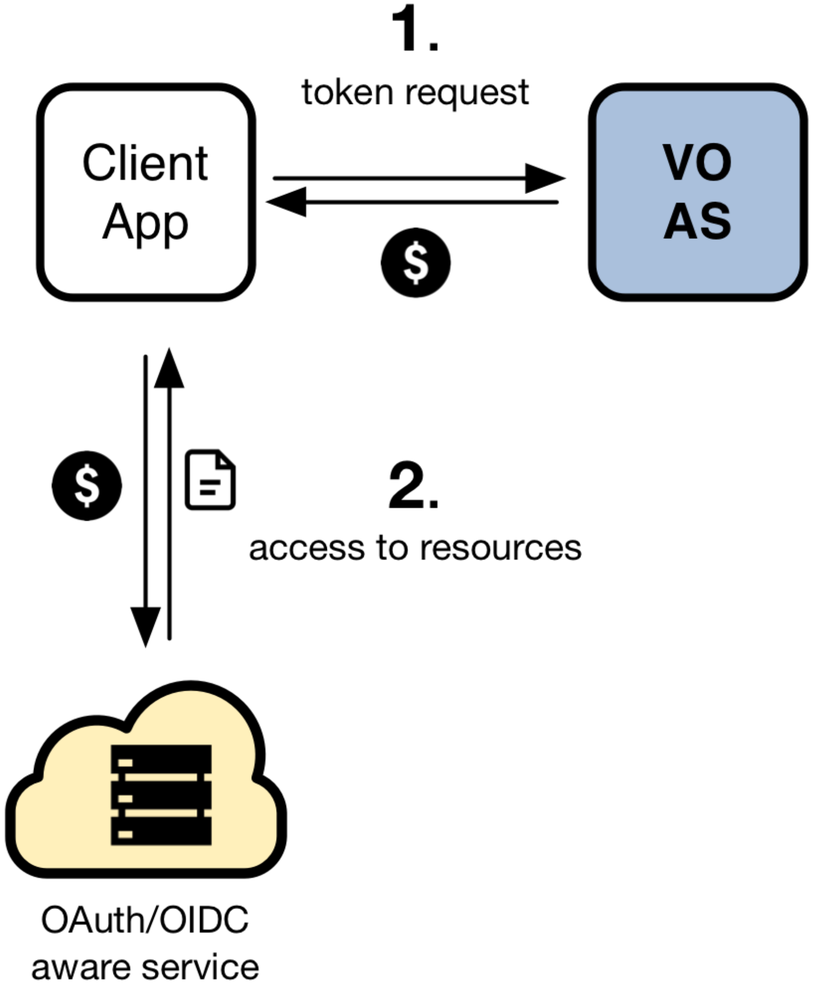
Key challenge:

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

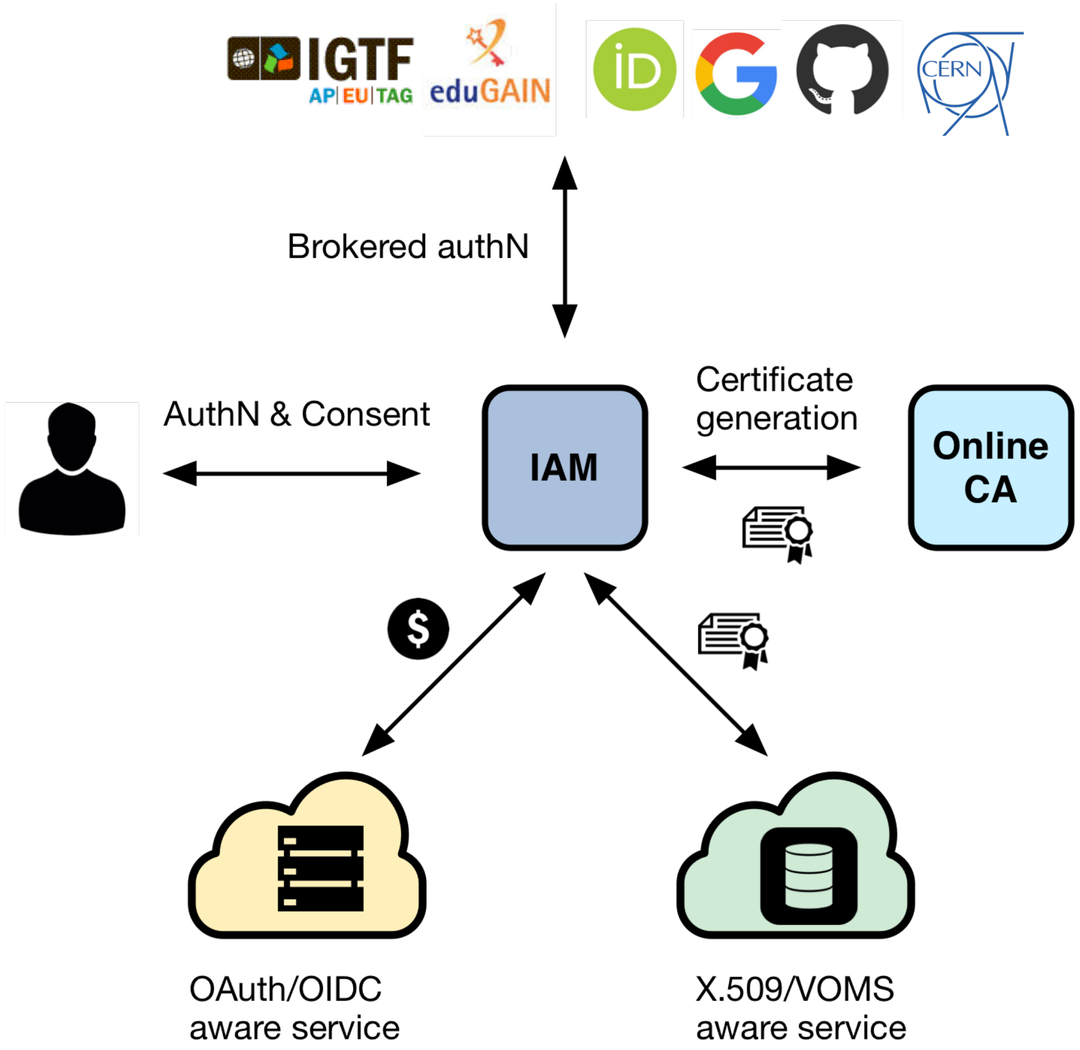


Funded by the European Union's Horizon 2020 - Grant N° 824064

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**

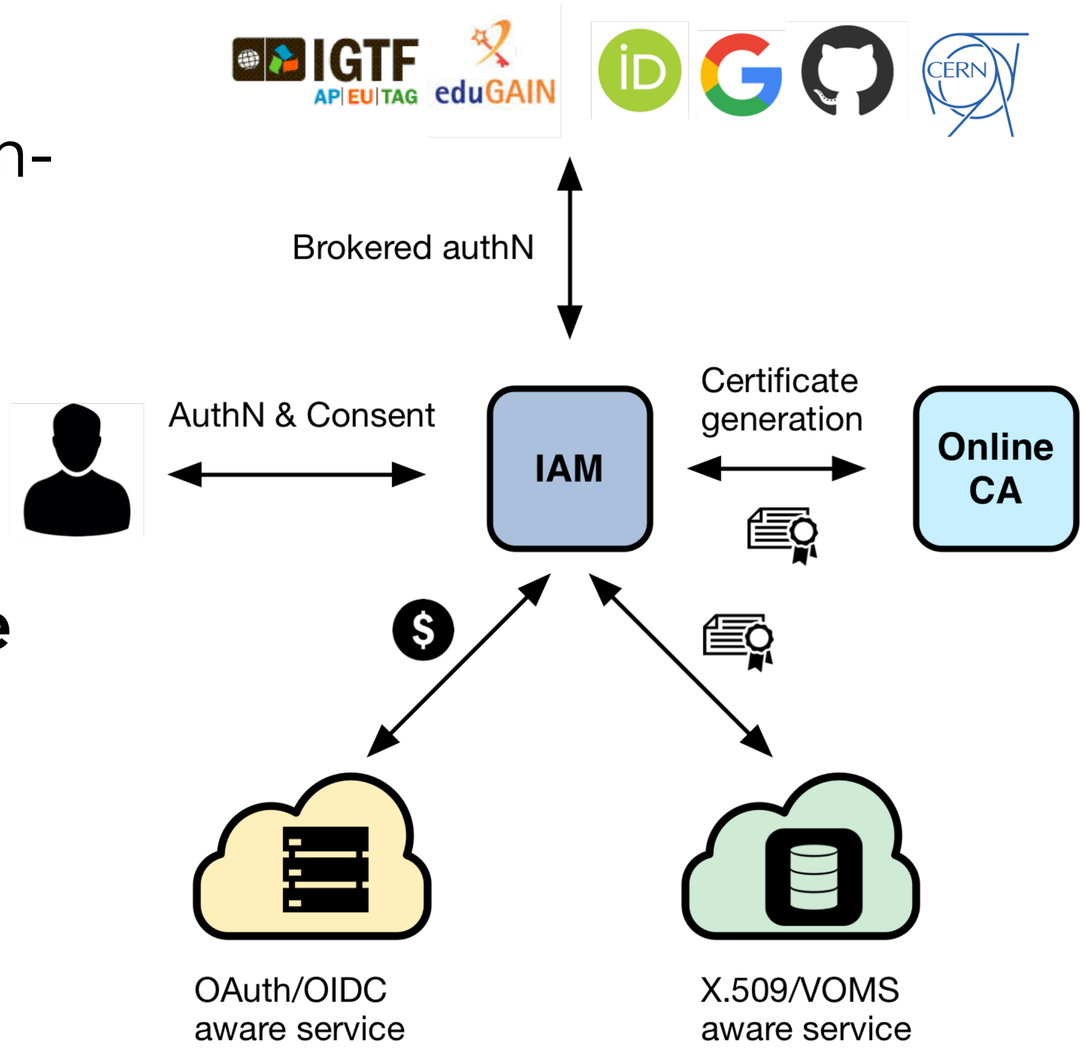
*VO = Virtual Organization



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

INDIGO Identity and Access Management Service

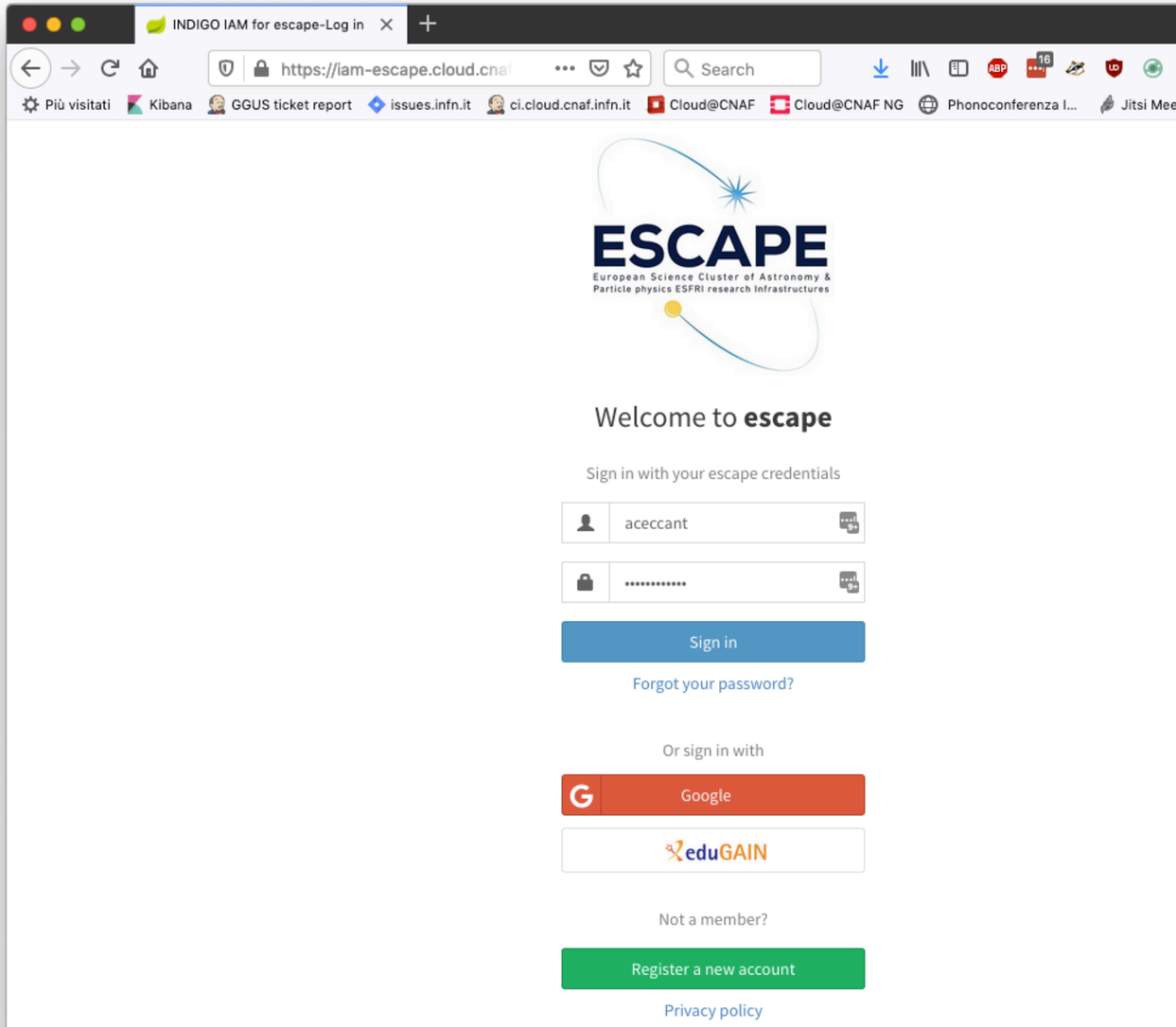
- **Selected by the WLCG Management Board** to be the core of the future, token-based WLCG AAI
  - while ensuring backward compatibility with the existing infrastructure
- **Sustained by INFN for the foreseeable future**, with current support from:



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
  - 50 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



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

Next steps

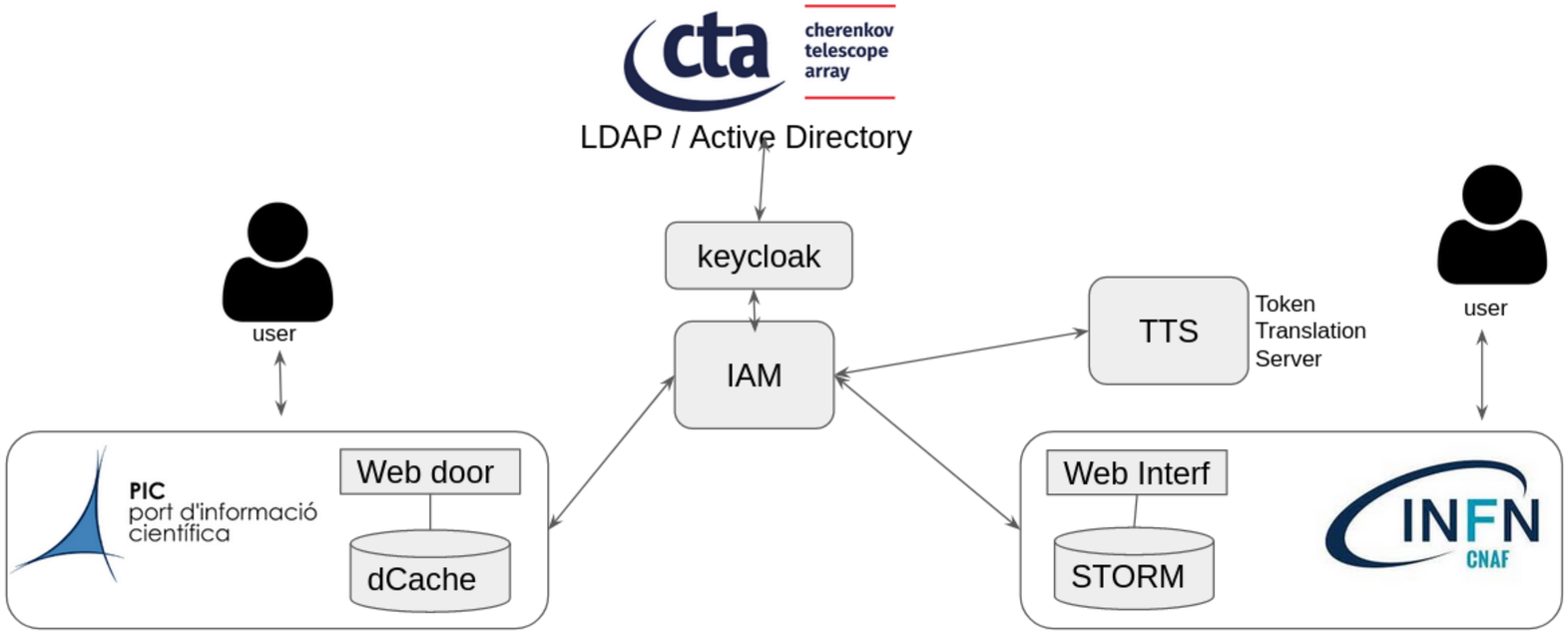
LOFAR EGI CheckIn integration

- Integrate IAM with the EGI CheckIn managed LOFAR organization:
  - Allow users to login in the ESCAPE VO using their LOFAR credentials
    - Integration already working on an test instance
  - Allow users to automatically onboard the ESCAPE VO (without administrator approval) when authenticated using their LOFAR credentials, and placed in an ESCAPE IAM lofar group
    - Requires some development on the IAM side, ETA: March 2020

- Use this as a pilot experience to showcase how we can integrate and interoperate with other, standards-based AAI

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

CNAF-PIC data transfers in support of LST1



- Deploy an IAM instance @ PIC, integrated with the CTA LDAP, to provide support for VOMS and token-based AuthN/Z for LST1

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

IAM/Token-based AuthN/Z webinar

- IAM and token-based AuthN/Z training event
- Audience:
  - Service developers and AAI experts from other ESCAPE technical Work Packages
- Focus on:
  - OAuth/OpenID Connect basics
  - Service Integration
  - Web-based and CLI user access
- When: right after Brussels!

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

Conclusions

- AAI in WP2 is in good shape
  - ESCAPE IAM instance deployed and integrated with EduGAIN
  - GSI/VOMS AuthN/Z supported by all data management services
  - Token-based AuthN/Z supported by most data management services

- Next steps:
  - Demonstrate interoperability/integration for communities already having their own AAI solution/user database
  - Showcase fine-grained AuthZ in support of use cases with embargoed data
  - Support other WPs integration efforts with training events/f2f hackathons

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

Thanks for your attention.
Questions?