Future Perspectives for Token-based AuthN/Z

Rizart Dona

CERN

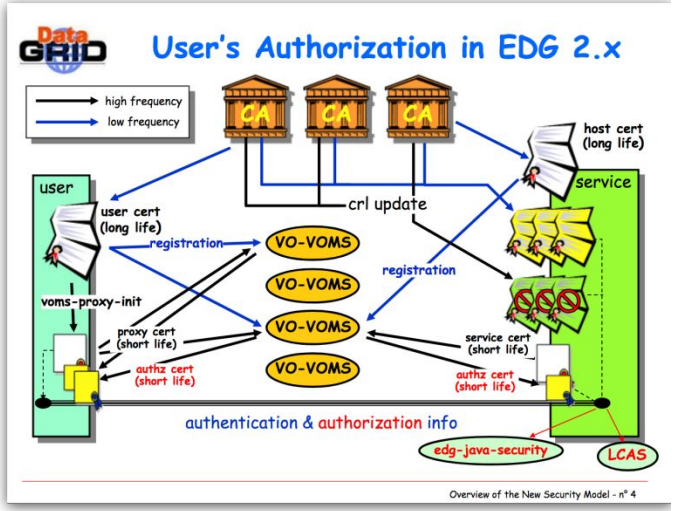
March 23, 2022 - 3rd ESCAPE DIOS Workshop

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 current WLCG AAI

In operation since ~2003, and still working nicely:

- **X.509 trust fabric** provided by **IGTF** (tells services which CAs are trusted)
- **X.509 certificates** provided to users for authentication
- **Proxy certificates** for Single Sign-On (SSO) and delegation
- **VOMS attribute certificates** for attribute-based authorization (issued and signed by VO-scoped VOMS servers)



Slide by Ákos Frohner

@Andrea Ceccanti

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

Current WLCG AAI: the weak points

Usability

- X.509 certificates are **difficult** to handle for users
- VOMS does not work in browsers

Inflexible authentication

- Only one authentication mechanism supported: X.509 certificates
- Hard to integrate identity federations

Authorization tightly bound to authentication mechanism

- VOMS attributes are inherently linked to an X.509 certificate subject

Ad-hoc solution

- We had to invent our own standard and develop ad-hoc libraries and central services to implement our own AAI

Can we do better today? @Andrea Ceccanti

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

A novel AAI for WLCG: 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**

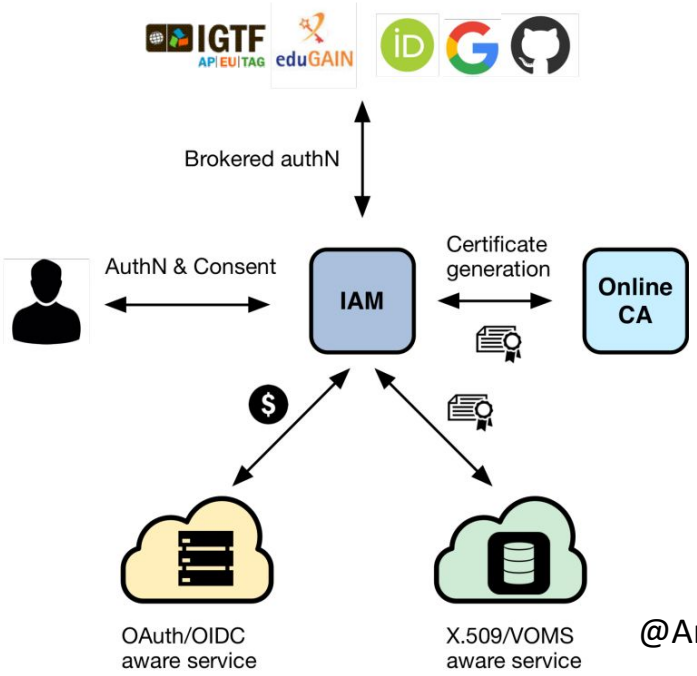
@Andrea Ceccanti

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

The future token-based WLCG AAI

Introduce a central VO-scoped authz 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**



@Andrea Ceccanti

5

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

Token-based AuthN/Z concerns several components

- Rucio
- FTS (Gfal)
- Storages
- Other Services
  - CRIC
  - DLaaS
  - <any other service that needs to be integrated>

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

Questions & topics for the community to consider

- What type of authentication and authorisation scenarios would token based AuthN/Z enable for you?
- Which Identity provider to use?
  - A common one for smaller experiments maybe makes more sense
  - Who will be offering the service?
- Definition of the tokens profile, it will specify
  - How to map defined scopes to local authZ
  - How to map group-based to local authZ
- Tutorials & documentation is needed for users to become familiar with the tools/logic of these new authentication methods
- How to leverage, coordinate and link with activities being carried on in different fora
  - Common effort to develop token support for services & tools
  - Establishing communication channels to keep track of progress & share experience and expertise

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

References (I)

- Beyond X.509: A token-based AAI for WLCG, Andrea Ceccanti, 14/06/2019 https://indico.cern.ch/event/776832/contributions/3378561/attachments/1862219/3061139/WLCG-AAI-DPM-Workshop-140619-2.pdf
- DOMA TPC: Token-based AuthZ Testbed, Andrea Ceccanti, 20/05/2020 https://indico.cern.ch/event/918191/contributions/3859170/attachments/2042527/3421225/DOMA-TPC-TokenBasedAuhtZTestbed200520.pdf
- Rucio token evolution, Martin Barisits, 03/03/2022 https://indico.cern.ch/event/1131014/contributions/4746616/subcontributions/368509/attachments/2401409/4106887/2022-03%20Token%20Workflow%20Evolution.pdf
- Token-based AuthN/Z for WLCG: https://wlcg-authz-wg.github.io/wlcg-authz-docs/
- WLCG Common JWT Profiles: https://zenodo.org/record/3460258

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

References (II)

- An Illustrated Guide to OAuth and OpenID Connect https://developer.okta.com/blog/2019/10/21/illustrated-guide-to-oauth-and-oidc
- oidc-agent https://github.com/indigo-dc/oidc-agent
- OAuth 2.0 https://oauth.net/2/
- OpenID Connect https://openid.net/connect/

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