Auth&Authz

Introduction and IVOA perspective

Dr. Giuliano Taffoni

INAF – Osservatorio Astronomico di Trieste

What is Auth and Authz

What is the scope?

Authentication is a process by which you verify that someone is who they claim they are.

Authorization is the process of establishing if the user (who is already authenticated), is permitted to have access to a resource

Who is for?

Researchers, developers, projects …. But each used to have it’s own solution

Once upon a time…Auth&Authz

The Authentication process is **local** to your service and/or resource. The resource and service providers **store identities** and **credentials**. Data is saved in **files** (e.g. passwd, htpasswd) or **databases**. They eventually distribute share them (e.g. NIS, **LDAP**). They implement the authorization locally based on **groups** and **ownership.**

Is Local Auth. Appropriate?

Password proliferation…

- affects projects, resource and service providers
- it is a pain for users

How many accounts do I have?

Another **password to change**?!?!?

It opens a set of security problems

- Everybody must **store credentials**
- Credential are **exchanged** on LAN

The federated identity approach

The main purpose of federated identity management is to allow registered users of a certain domain to access information from other domains in a smooth way without having to provide any extra administrative user information

Gives a delegated mechanism to manage user identification among different entities and within different subjects

Provides a set of attributes to an authenticated users to be used by the final application.

Advantages of Federated Identity

Identity Provider asserts authentication and identity information about users. **Keep your credential at your institute/company.**

Service Providers check and consume this information for authorization and make it available to an application.

Protects User Information

Reduce Work

Provides current A&A info

Insulate from service compromise

Role of federation

A group of organizations running IdPs and SPs that agree on a

common set of rules and standards

Based on TRUST!

Defines agreements and rules

Operates discovery services

An organization may belong to more than one federation

Available technological solutions and implementations

OAuth (Open Authentication)

Security Assertion Markup Language (Shibboleth)

OpenID

Unity (solution for identity, federation and inter-federation management)

DEV&Policy

- **RD-Alliance Interest Group (international cross-domain interest group to work on all issues on A&A)**
- **EU funded projects**
  - **Authentication and Authorization for Research and Collaboration (AARC)**
    - **"[…]build on the very many existing and evolving components *ESFRI clusters, eduGAIN, national AAI federations*[…]",**
  - **Authentication and Authorization for Entrusted Unions (AU2EU)**
  - **PCAS - Personalised Centralized Authentication System**
  - **others**

Federated Identity is…web auth

Designed and developed for services consumed via WEB (e.g. web services, portals, clouds).

May I access my local computing cluster? No

But I can implement hacks

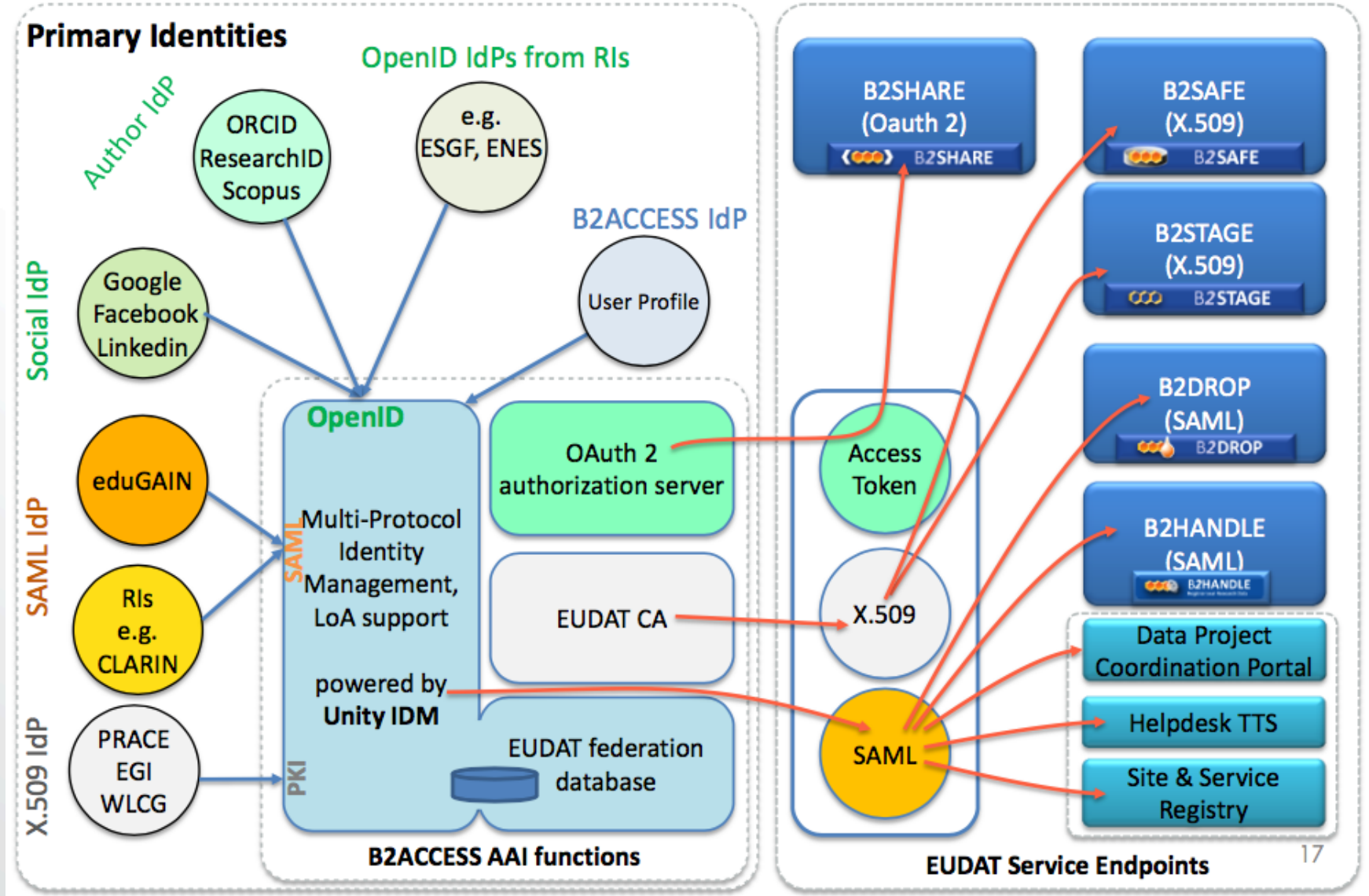
PRACE: x509 and Ldap and meta-users and ssh

EduGAIN

"The eduGAIN service interconnects identity federations around the World, simplifying access to content, services and resources for the global research and education community. eduGAIN enables the trustworthy exchange of information related to identity, authentication and authorisation (AAI).

IDM Integration

https://b2access.eudat.eu



Nothing is simple….

AARC

EUDAT

Astronomy and Astrophysics

- CTA Authorization and Authentication is under discussion
  - Different approaches to integrate (ldap+web portals+X.509)
  - UNITY
  - GROUPER
- SKA Authorization and Authentication is under discussion
  - See Cristina Talk
- IVOA and EuroVO
  - Single Sign On, Credential Delegation
  - Authorization under discussion

The Virtual Observatory Approach

- "single-sign-on architecture is a system in which users assign cryptographic credentials to user agents so that the agents may act with the user's identity and access rights."

- "This standard describes how agents use those credentials to authenticate the user's identity in requests to services."

- SSO recommendation "is a profile against existing security standards"

Single Sign On

Allow “clients” to access a service that requires authentication.

HOW?

No authentication required.

HTTP Basic Authentication

Transport Layer Security (TLS) with passwords.

Transport Layer Security (TLS) with client certificates.

Cookies

Open Authentication (OAuth)

Security Assertion Markup Language (SAML)

OpenID

Credential Delegation

The credential delegation protocol allows a client program to delegate a user's credentials to a service such that that service may make requests of other services in the name of that user. The protocol defines a REST service that works alongside other IVO services.

Authorization

Authentication is a relatively "simple" task to tackle and we are comfortable with the level of trusts given by federated identity.

Authorization: here comes the problem!

There is no general agreement achieved, so far, in the field of authorization.

Authorization issues

Traditionally, identity federations have solved the authorization problems with two opposite approaches:

- **Service managed authorization**
- **Identity providers managed authorization**

Data privacy, resource allocation….

How are you using my resources!

MAIN ISSUE FOR MEDICAL DATA

Authorization approaches

Trend in projects and infrastructures is: “take care of your own authorization”

Identify your own policies

Choose an implementation

You know your requirements you develop your Authz.

But please do not reinvent the software!

Some technical approaches

SAML

- identify and authorize users thanks to **attributes**.

Grouper:

- Centralized groups, roles, and permissions
- Delegated control
- Provision to LDAP/SAML etc.
- Auditing
- https://spaces.internet2.edu/display/Grouper/Grouper+Wiki+Home

Grouper™

Group Management Sistem developed by CADC in IVOA.

But also LDAP or a local database if you like….

More complexity to come…

If I open my data/computing center how can I measures the resources a user consumes during access?

Accounting

Conclusions

- **Find a method to identify their users**
  - **Federated Identity approach**
- **Implement your own Authorization framework**
  - **Based on your policies**
  - **Choose one of the software available**
  - **Do it “locally”**
- **Use EU or International standards as much as possible**