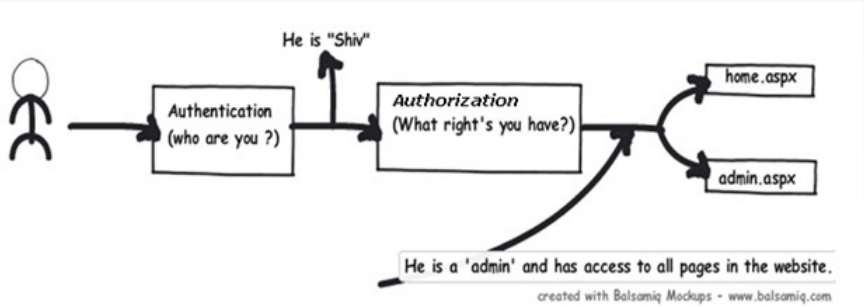



Authorization profile for IVOA?

Auth&Authz

- ***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.***



Authentication

- In general it is a “simple” task
- IVOA SSO document (now version 2.0)
- Currently, the goals of an Identity Federation are:
  - give a delegated mechanism to manage user identification among different entities and within different subjects;
  - provide a set of attributes to an authenticated users to be used by the final application.
- There is a general agreement in the capabilities of IF (EDUGain, EDULink)).


Authorization

- Assigning capabilities to a user
- Authorize user to access a “resource”
- Authorize an application to make requests on behalf of the user

- No general agreement achieved, so far, in the field of authorization.

How can we manage authz?

- Traditionally, identity federations have solved the authorization problems with two opposite approaches:
  - SP managed authorization
  - IdP managed authorization
- A different approach may be followed (leveraging Attributes Authorities and implementing tools) where authorization is delegated to a specific system designed for that purpose.
- What about the policies?

3D complexity

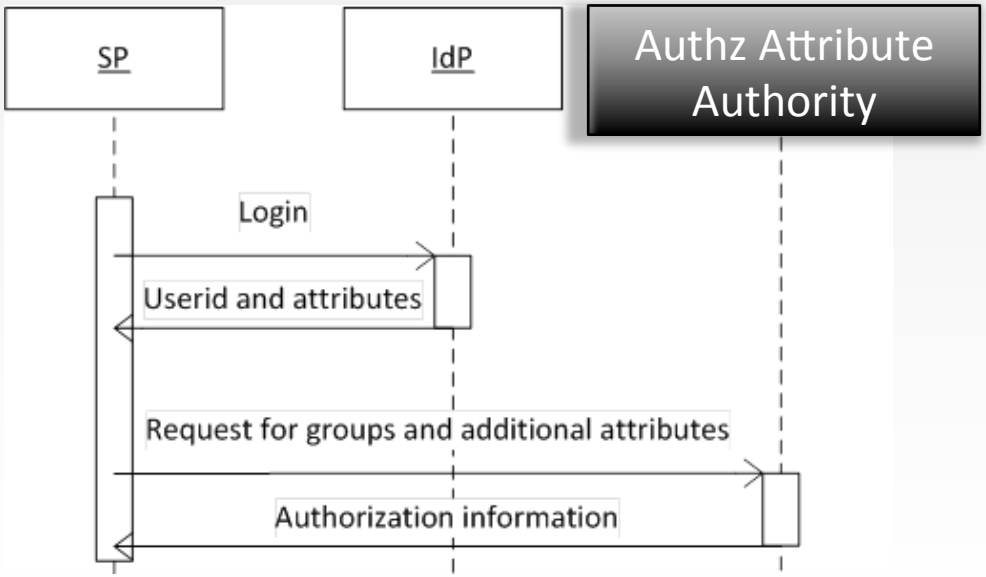
- we are dealing with dynamic environments as globally disaggregated collaborating entities.
- federated identity management.
- Implicit in federation is TRUST

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
- GMS

GEANT example

- Media Wiki: Shibboleth + Grouper

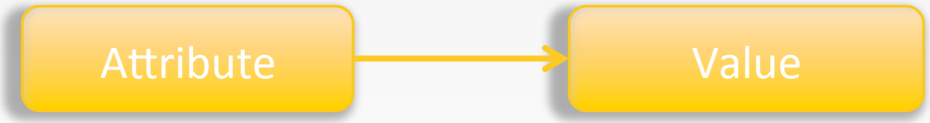



Implement Authz means…

- Identify an approach
- Identify a tool or a set of tools
- Identify Role or attributed based policies
- Define a service related policy

Attribute example 1

- TERENA security policy and security model
- eduPerson schema for LDAP and….SAML
- Attribute based authorization




```
urn:schac:userStatus:au:uq.edu.au:service:mail:receiv
e:disabled
```


Attribute example 2

- OwnCloud @ INAF
- uses the Shibboleth Authentication module + SAML attributes to give a simple authz profile

```
EduPersonEntitlement
urn:mace:inaf.it:owncloud:user:size:10G
```

Some open questions

- do we trust each other and other provides?
- Do we think third party is the proper approach?
- Are we going for local authz attribute and services?
- Do we need an Authz profile in IVOA?
- Are we using Authz? Good to have examples

Going towards multi-dimension

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