# 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.

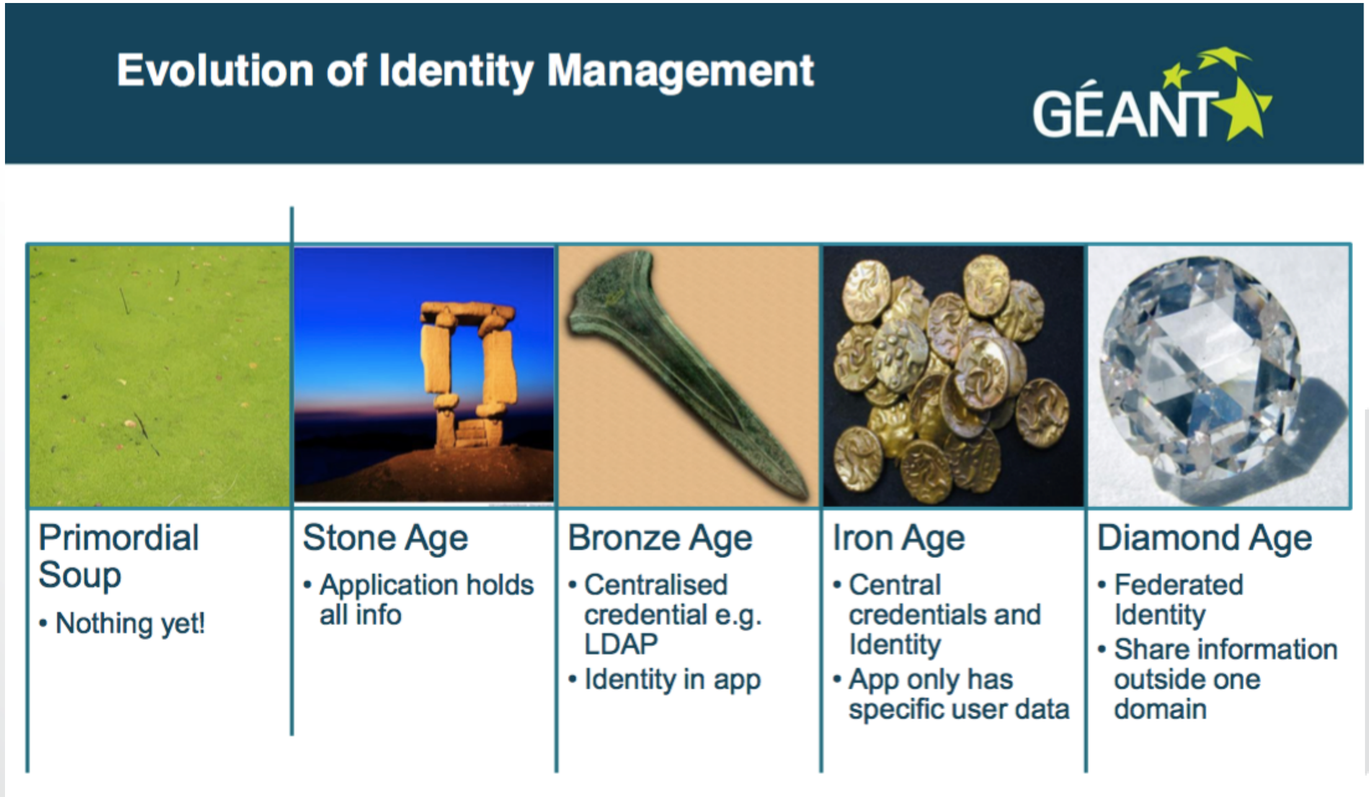
Authorization is the process of establishing if the user (who is already authenticated), is permitted to have access to a resource

## 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.**



## Evolution of Identity Management

GÉANT

| Primordial Soup | Stone Age | Bronze Age | Iron Age | Diamond Age |
|---|---|---|---|---|
| • Nothing yet! | • Application holds all info | • Centralised credential e.g. LDAP<br>• Identity in app | • Central credentials and Identity<br>• App only has specific user data | • Federated Identity<br>• Share information outside one domain |

# 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 identity providers 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
X.509 certificates

System requires a different Auth approach: web services, portals, clouds differ from

computing cluster

# Astronomy and Astrophysics

- CTA Authorization and Authentication is under discussion

- SKA Authorization and Authentication is under discussion

- IVOA and EuroVO
  - Single Sign On, Credential Delegation
  - Authorization to be discussed

# 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.

Actually ✉ X.509

But also other protocols as oAuth

# Authorization

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

Is my application aware of service authorization?

- Not necessary
- Implement  standard messages (eg. 501 Error: Authorization failed)

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**

**Group Management System developed by CADC in IVOA.**

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

# 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**