Authentication And Authorization in the VO

IVOA Interop, Cape Town
GWS and Apps Working Groups
May 2016

ivoa.net/astronomers/using_the_vo.html

Single Sign-on
So far, VO tools and services have concentrated on fully public data services, but of course every day astronomers are using data to which they have private access - because they have PI time on a space mission, or because they are a member of a consortium that owns the data. The usual practice is enter a username and password at the relevant website. The IVOA is discussing how to standardise expressing identity, so that secure data services can be included in the VO, and you only need to "sign on" once. Watch this space.

A&A Terminology

Authentication - User identification through credentials.

The IVOA and authentication:

- IVOA Single-Sign-On Profile: Authentication Mechanisms. Outlines a way that users' credentials of various types can be used between numerous VO services. (username/password, TLS client certificates, identity providers oAuth, openID).
- VOResource and securityMethod. VOSI *capabilities* states that you can have securityMethods in VO service interfaces.

A&A Terminology

Authorization - Making the decision of whether to grant permission to a given resource. The decision can involve knowing an authenticated user's credentials.

No standards discuss authorization in a general manner yet.

A&A Terminology

Resources may require authorization for access.

Some examples of resources are:

- Services (SIA, VOSpace, Datalink, etc..)
- Data files
- Metadata (queries: row-level, table-level)

A&A Terminology

Groups are sets of users who have access to a resource.

VOSpace uses standard *groupRead* and *groupWrite* properties for Node authorization. In this case, the VOSpace *Node* is the *Resource*.

We'll hear about how membership in groups authorized to access a resource are used for authorization.

A&A Goals

1) To allow only certain individuals to access certain resources.

2) To allow the sharing of proprietary resources with others.

Proprietary Period

Most facilities have a period of time in which only the Principal Investigator’s team has access to the metadata and data files.

Even without a proprietary period, time is required to verify and validate observations before they can be made public.

Until the VO Supports A&A, the querying of metadata and access to the files must be done outside of the VO.

Removing facilities’ custom query service

Currently, for facilities to support queries on proprietary metadata, a custom query service is needed.

With the addition of A&A, the various VO query services (TAP, SIA, Datalink, …), could be used directly from the project query interface to support both proprietary and public metadata.

A&A Spans the VO

From clients to services to resources--A&A is orthogonal to most of the VO.

This is why it’s a joint Apps and GWS session.

Technical A&A Challenges

1) Apps: Applications and tools gathering credentials from users.

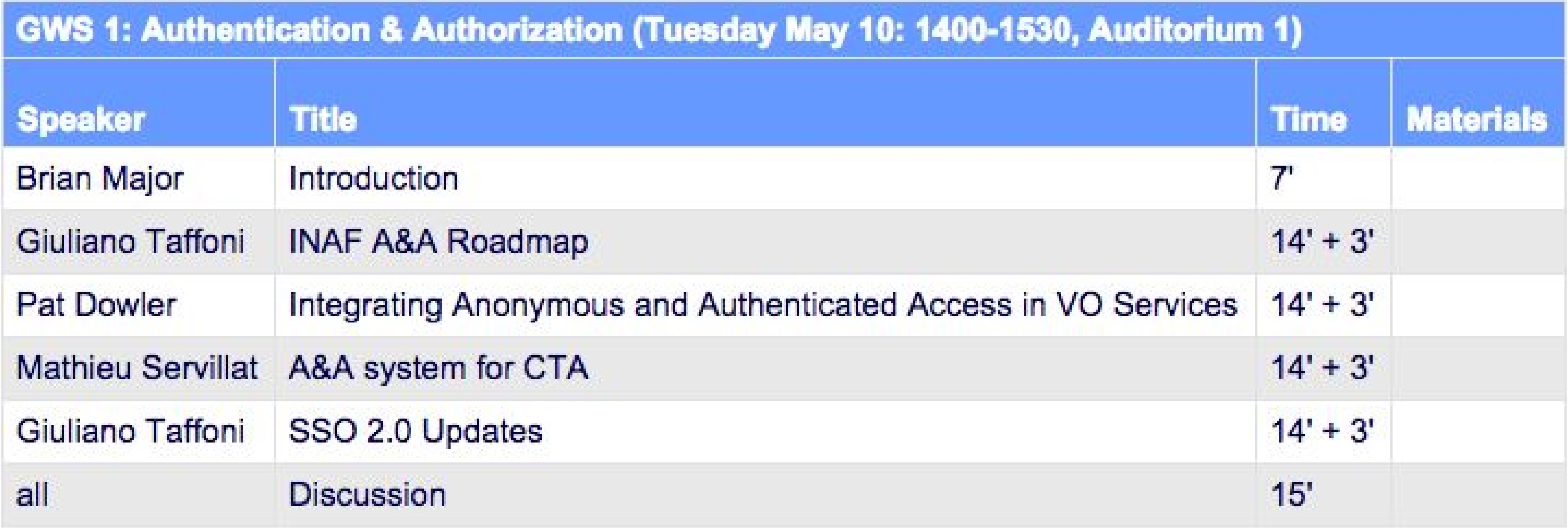
2) Apps/GWS: clients negotiating with services on securityMethods (authentication method).

3) Apps/GWS: clients and services working with external identity providers.

4) GWS: services making authorization decisions

5) Apps/GWS: associating authorization with a resource (granting).

Schedule



GWS 1: Authentication & Authorization (Tuesday May 10: 1400-1530, Auditorium 1)

Speaker	Title	Time	Materials
Brian Major	Introduction	7'	
Giuliano Taffoni	INAF A&A Roadmap	14' + 3'	
Pat Dowler	Integrating Anonymous and Authenticated Access in VO Services	14' + 3'	
Mathieu Servillat	A&A system for CTA	14' + 3'	
Giuliano Taffoni	SSO 2.0 Updates	14' + 3'	
all	Discussion	15'	