Authentication for Non-Browser Clients: Progress

Mark Taylor (Bristol)
with input from: Pat Dowler (CADC)
Brian Major (CADC)

GWS WG
IVOA Interop
Online

27 April 2022

`$Id: auth.tex,v 1.9 2022/04/26 14:41:34 mbt Exp $`

Outline

- History
- Current proposal ("SSO_next")
- Implementation status, with examples
- Next Steps

History

Working towards authenticated access for non-browser clients

- Clients need to know **how** and **where** (and **whether**) to log in for authenticated access

Previous updates:

- May 2020
  - ▷ Pat Dowler: *Authentication strawman proposal*
- Nov 2020
  - ▷ Brian Major: *Non-browser client authentication with OAuth2 tokens*
  - ▷ Mark Taylor: *Authentication Implementation Report*
- May 2021
  - ▷ Brian Major: *Tokens for Non-Browser Clients Updates*
- Nov 2021:
  - ▷ Mark Taylor: *Authentication for Non-Browser Clients: Update*
- Jan 2022:
  - ▷ Pat Dowler: SSO_next wiki page
    → **agreed specifics for client/server behaviour**

SSO_next Proposals

Summary (SSO_next wiki page, main author Pat Dowler):

- Communicate auth info using only RFC 7235-style `WWW-Authenticate` challenges
  - `securityMethod` elements in capabilities document no longer required
- Introduce VO-specific `ivoa_*` authentication schemes that can carry additional metadata:
  - `access_url`: where to login
  - `standard_id`: how to interact with `access_url`
- Provide authentication confirmation
  - `X-VO-Authenticated` header SHOULD appear in authenticated responses
- Specify how to determine service authentication requirements
  - `/capabilities` endpoint `HEAD`/`BODY` response is 200/401(/403) with or without `WWW-Authenticate` challenge(s)

Impact on standards:

1. VOSI augmented to require HTTP `HEAD` support for `/capabilities` endpoints
2. SSO augmented to define `ivoa_bearer`, `ivoa_cookie`, and `ivoa_x509` challenges
3. SSO `ivo://ivoa.net/sso#tls-with-password` extended to specify the form params
4. SSO challenges describe/specify response form of login endpoint (`access_url`), possibly including `x-vo-bearer` response header
5. SSO requires/recommends authenticated services to include `x-vo-authenticated` header in all authenticated responses
6. Modify VOSI to allow `/capabilities` to respond with 401 (or 403) *(also affects TAP 1.1 sec 2; & others?)*

SSO_next Status

- It works!
- No significant disagreements among participants
- Some minor(?) open issues:
  - How to signal/determine token scope? *(tricky)*
  - Additional auth schemes or login methods may be needed

SSO_next Implementation

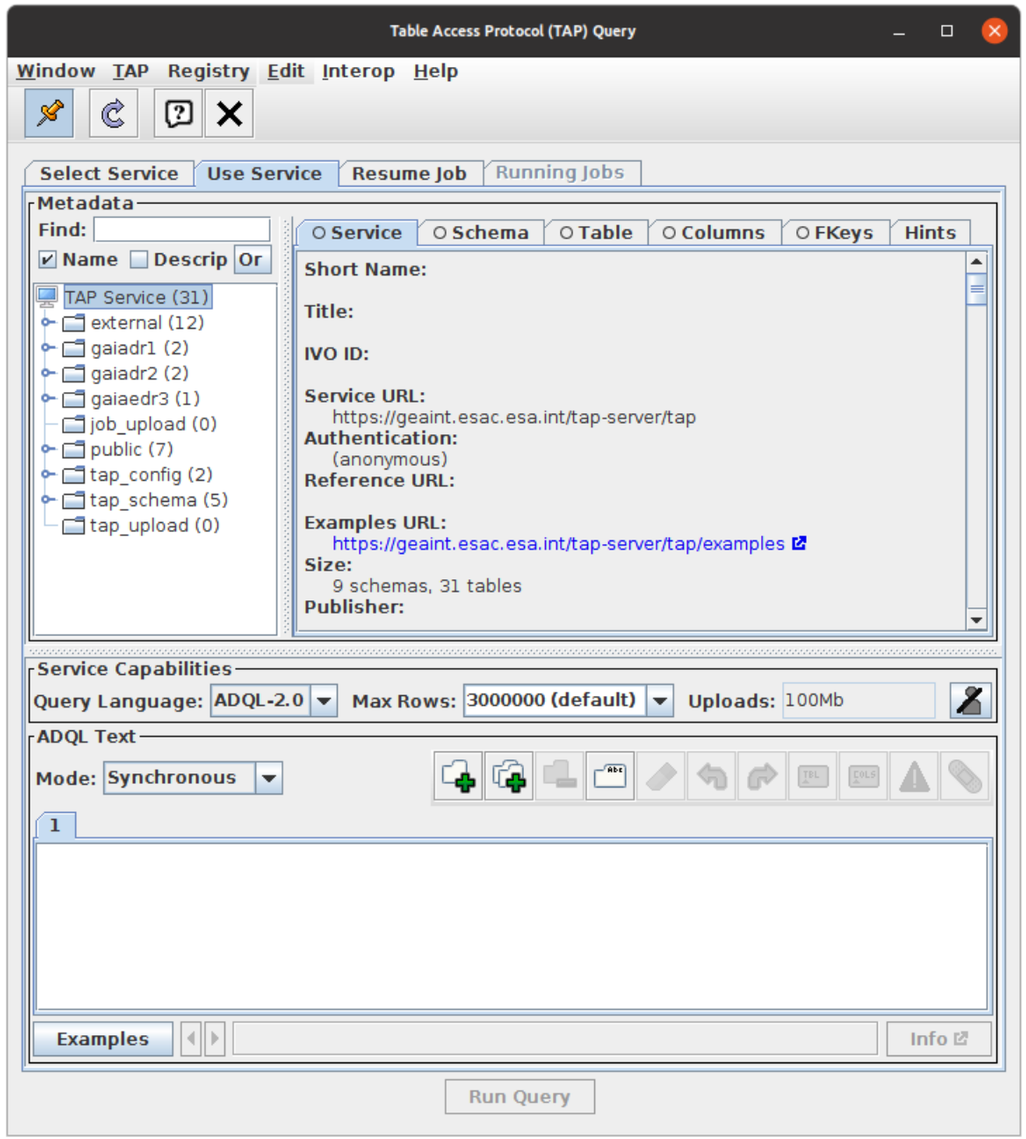
Service implementations:

- CADC
  - Auth modes: optional
  - Auth schemes: `ivoa_bearer`, `ivoa_x509`, `Bearer`
  - Login standard_ids: `ivo://ivoa.net/sso#tls-with-password`, `ivo://ivoa.net/sso#OpenID` `ivo://ivoa.net/sso#BasicAA`
- DaCHS
  - Auth modes: optional, mandatory
  - Auth schemes: `Basic`
- ESA GACS (Development version, partial implementation: no challenges, strange response codes, no auth confirmation)
  - Auth modes: none, optional
  - Auth schemes: `ivoa_cookie`
  - Login standard_id: `ivo://ivoa.net/sso#tls-with-password`

Client implementation:

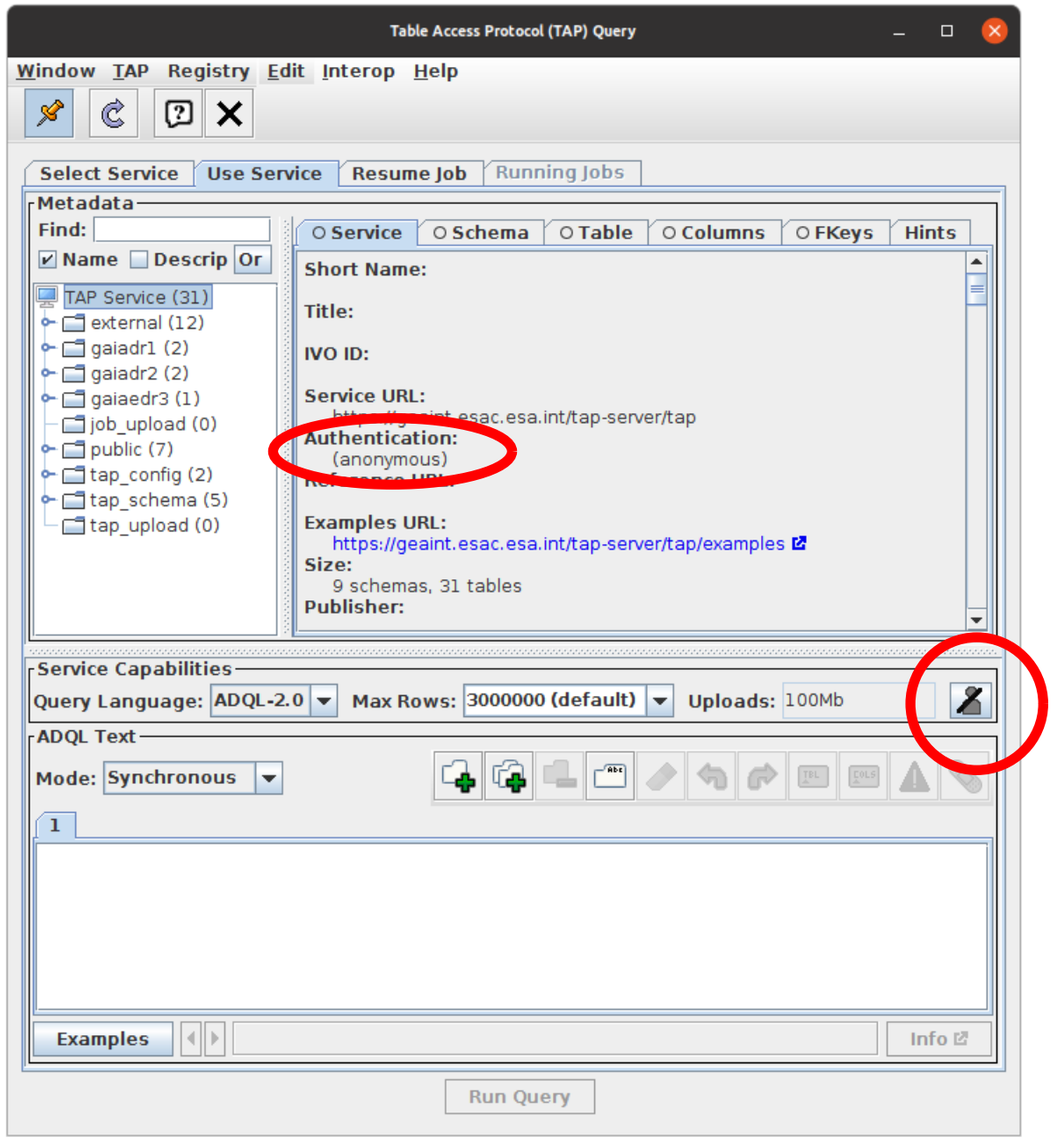
- TOPCAT prototype (`http://andromeda.star.bristol.ac.uk/releases/topcat/pre/topcat-full_auth.jar`)
  - Auth modes: none, optional, mandatory
  - Auth schemes: `ivoa_bearer`, `ivoa_cookie`
  - Login standard_ids: `ivo://ivoa.net/sso#tls-with-password`, `ivo://ivoa.net/sso#BasicAA`
  - Some rough edges (e.g. token expiry may not be handled correctly)

Demo



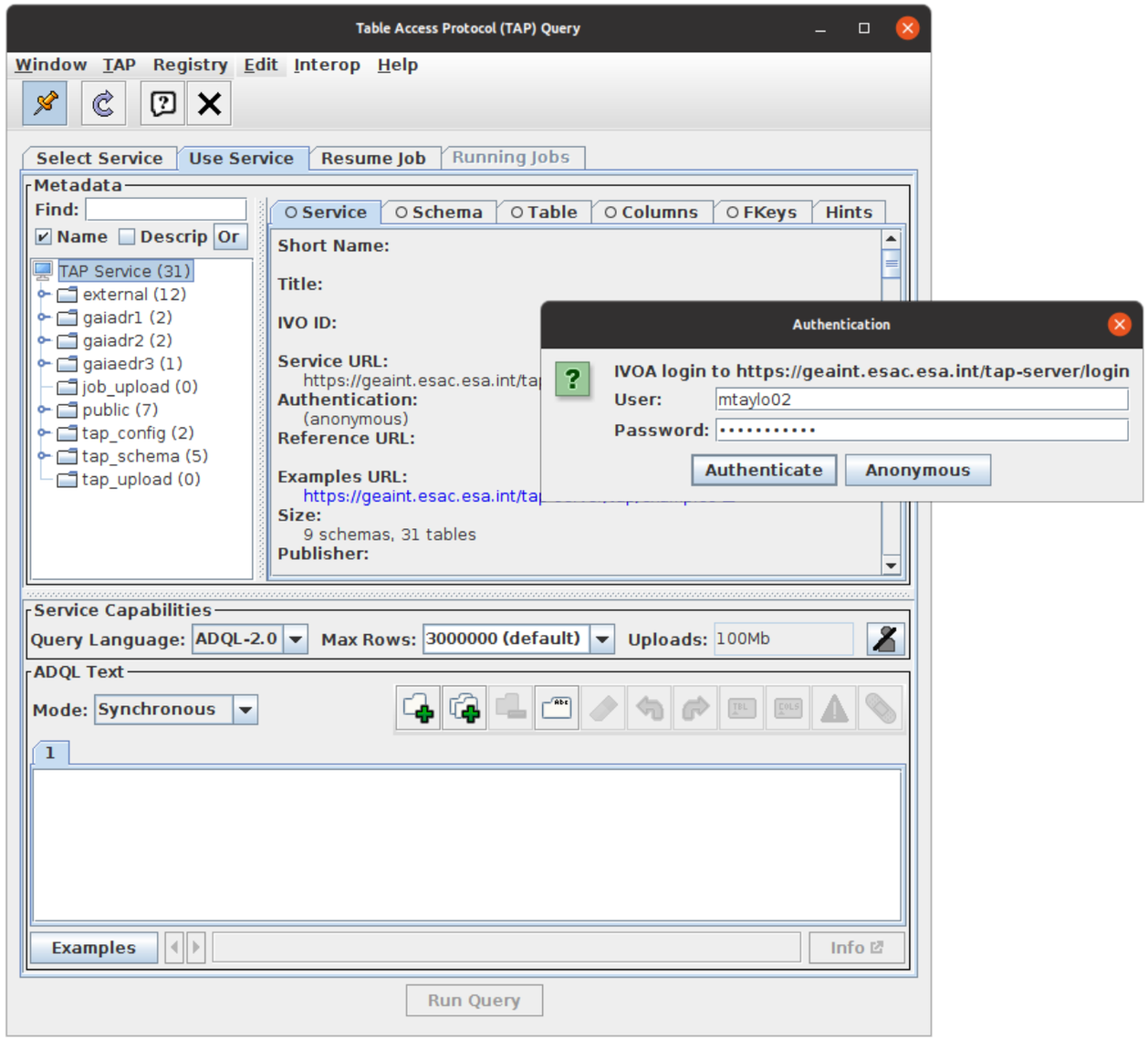
Prototype: http://andromeda.star.bristol.ac.uk/releases/topcat/pre/topcat-full_auth.jar

Demo



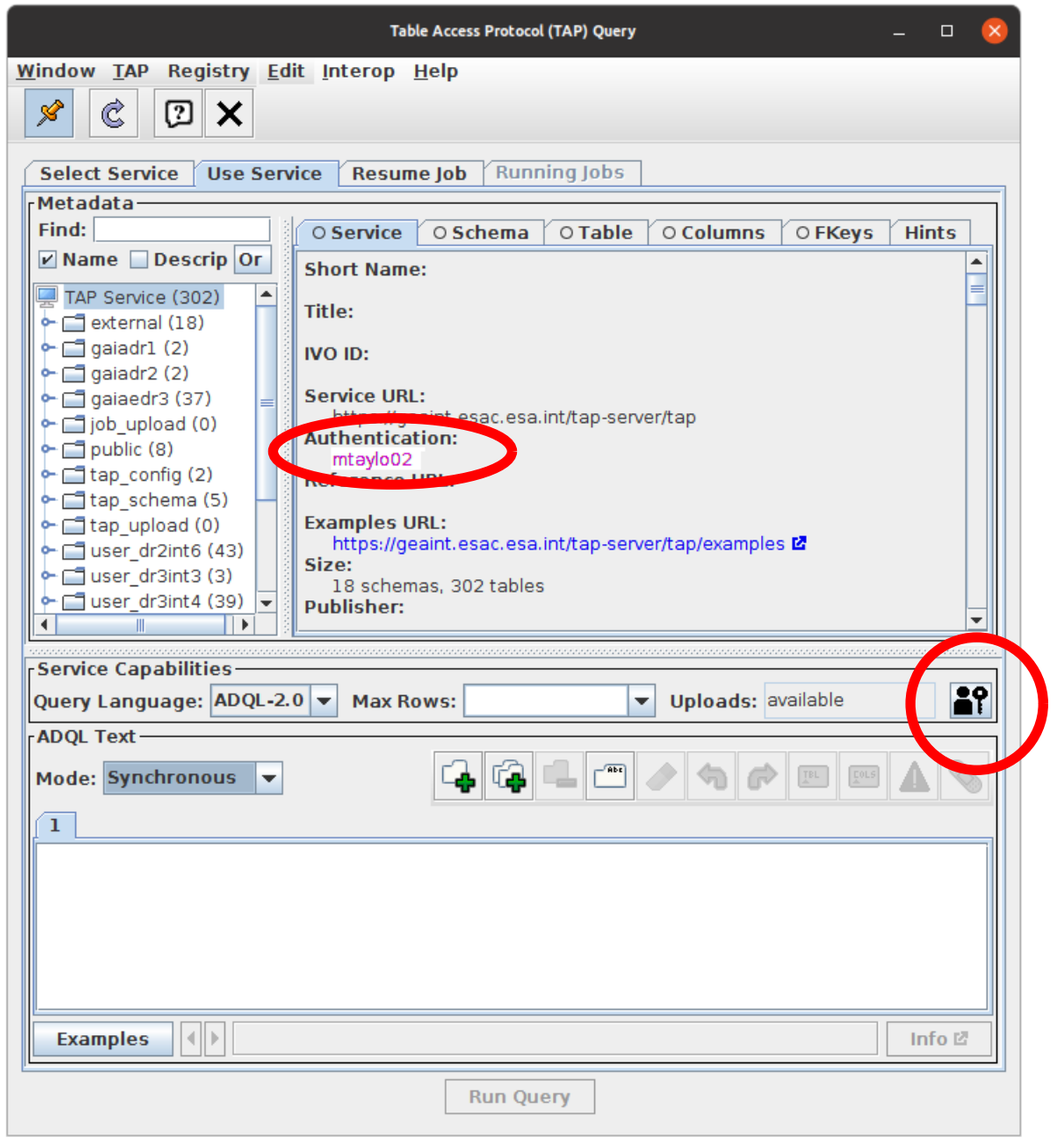
Prototype: `http://andromeda.star.bristol.ac.uk/releases/topcat/pre/topcat-full_auth.jar`

Demo



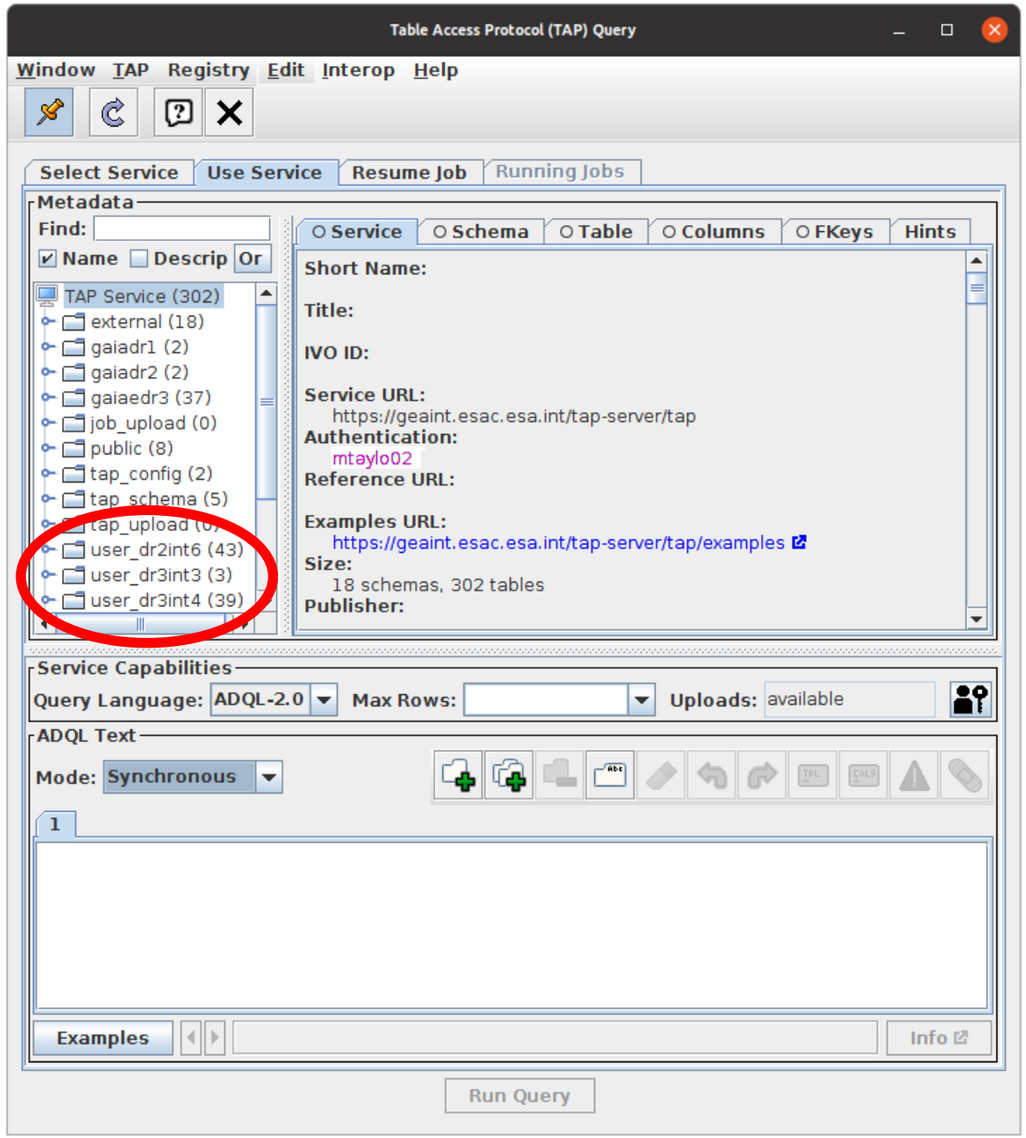
Prototype: http://andromeda.star.bristol.ac.uk/releases/topcat/pre/topcat-full_auth.jar

Demo



Prototype: http://andromeda.star.bristol.ac.uk/releases/topcat/pre/topcat-full_auth.jar

Demo



Prototype: `http://andromeda.star.bristol.ac.uk/releases/topcat/pre/topcat-full_auth.jar`

CADC (ivoa_bearer)

```
% curl --head https://ws.cadc-ccda.hia-iha.nrc-cnrc.gc.ca/argus/capabilities
HTTP/1.1 200
server: OpenCADC/cadc-rest
www-authenticate: ivoa_bearer standard_id="ivo://ivoa.net/sso#tls-with-password", access_url="https://ws-cadc.canfar.net/ac/login"
www-authenticate: ivoa_bearer standard_id="ivo://ivoa.net/sso#OpenID", access_url="https://ws-cadc.canfar.net/ac"
www-authenticate: Bearer
www-authenticate: ivoa_x509 standard_id="ivo://ivoa.net/sso#BasicAA", access_url="https://ws.cadc-ccda.hia-iha.nrc-cnrc.gc.ca/cred/auth/priv"
www-authenticate: ivoa_x509
transfer-encoding: chunked
date: Mon, 25 Apr 2022 14:22:45 GMT

% curl -d username=mbt -d password=xxxx https://ws-cadc.canfar.net/ac/login -D - -s
HTTP/1.1 200
x-vo-authenticated: mbt
x-vo-bearer: ZXhwaXJ5dGltZT0xNjUxMDY5NDI2NDc1Jm51bWVyaWNJRD0wMDAwMDAwMC0w...
content-type: text/plain;charset=ISO-8859-1
content-length: 760
date: Mon, 25 Apr 2022 14:23:45 GMT

% curl -D - --header 'Authorization: Bearer ZXhwaXJ5dGltZT0xNjUxMDY5NjMwMzg3Jm51bWVyaWNJRD0wMDAwMDAwMC0w...' https://ws.cadc-ccda.hia-iha.nrc-cnrc.gc.ca/argus/async
HTTP/1.1 200
server: OpenCADC/cadc-rest
x-vo-authenticated: mbt
content-type: text/xml
transfer-encoding: chunked
date: Mon, 25 Apr 2022 14:30:18 GMT

<?xml version="1.0" encoding="UTF-8"?>
<uws:jobs xmlns:uws="http://www.ivoa.net/xml/UWS/v1.0" xmlns:xlink="http://www.w3.org/1999/xlink" version="1.1">
  <uws:jobref id="dmw3r6jh8qd7mkg0">
  ...
```

DaCHS (Basic Auth)

```
% curl --head http://www.g-vo.org:8080/tap/capabilities
HTTP/1.1 401 Unauthorized
Server: DaCHS/2.5.5 twistedWeb/20.3.0
Date: Mon, 25 Apr 2022 14:47:42 GMT
WWW-Authenticate: Basic realm="Shangri-la"
Content-Type: text/html

% curl -u tap:xxxx http://www.g-vo.org:8080/tap/async -D - -s
HTTP/1.1 200 OK
Server: DaCHS/2.5.5 twistedWeb/20.3.0
Date: Mon, 25 Apr 2022 14:55:07 GMT
X-Vo-Authenticated: tap
Content-Type: text/xml
Content-Length: 594

<?xml-stylesheet href='/static/xsl/tap-joblist-to-html.xsl' type='text/xsl'?>
<uws:jobs version="1.1" xmlns:uws="http://www.ivoa.net/xml/UWS/v1.0" xmlns:xlink="http://www.w3.org/1999/xlink" ...
  <uws:jobref id="7qarnpw6" xlink:href="http://www.g-vo.org:8080/__system__/tap/run/async/7qarnpw6">
  ...
```

GACS (ivoa_cookie)

```
% curl --head https://geaint.esac.esa.int/tap-server/tap/capabilities
HTTP/1.1 500 500  ---> HTTP/1.1 200 200
Date: Mon, 25 Apr 2022 15:07:14 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.2k-fips mod_jk/1.2.43
---> WWW-Authenticate: ivoa_cookie standard_id="ivo://ivoa.net/sso#tls-with-password", access_url="https://geaint.esac.esa.int/tap-server/login"
Connection: close
Content-Type: text/html;charset=ISO-8859-1
...

% curl -D - -d username=mtaylo02 -d password=xxxx https://geaint.esac.esa.int/tap-server/login -s -o /dev/null
HTTP/1.1 200 200
Date: Mon, 25 Apr 2022 15:08:53 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.2k-fips mod_jk/1.2.43
---> X-VO-Authenticated: mtaylo02
Set-Cookie: JSESSIONID=108FF2B1379BEFAE6FF580BFxxxxxxxx; Path=/tap-server; Secure; HttpOnly
Transfer-Encoding: chunked
Content-Type: text/plain; charset=UTF-8
...

% curl --header 'Cookie: JSESSIONID=108FF2B1379BEFAE6FF580BFxxxxxxxx' https://geaint.esac.esa.int/tap-server/tap/async -D -
HTTP/1.1 200 200
Date: Mon, 25 Apr 2022 15:28:34 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.2k-fips mod_jk/1.2.43
---> X-VO-Authenticated: mtaylo02
Transfer-Encoding: chunked
Content-Type: text/xml;charset=UTF-8
...

<?xml version="1.0" encoding="UTF-8"?>
<uws:jobs  xmlns:uws="http://www.ivoa.net/xml/UWS/v1.0" xmlns:xlink="http://www.w3.org/1999/xlink" xmlns:xs="http://www.w3.org/2001/XMLSchema" ...>
  <uws:jobref id="1650899420107I" xlink:href="https://geaint.esac.esa.int/tap-server/tap/async/1650899420107I"><uws:phase>COMPLETED</uws:phase></uws:jobref>
  ...
```

Content in magenta
is not currently provided
by the service
(it's hacked in by TOPCAT)

Next Steps

Standardisation:

- Draft next SSO version *(Brian is on it! https://github.com/ivoa-std/SSO/)*
- Draft changes to other affected standards (VOSI, TAP, others?)

Implementation:

- Server
  - ▷ GACS updates to implement cookies properly soon?
  - ▷ Anybody else?
- Client
  - ▷ TOPCAT implementation ready for public release?
  - ▷ Provide TOPCAT's Auth library for third parties?

Open questions:

- Token scope (where else is authentication info valid?)
- Other Auth schemes or login methods required?
- Other issues arising from experience?