SSO V2.1

What do we need?

ESCAPE - The European Science Cluster of Astronomy & Particle Physics ESFRI Research Infrastructures has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement n° 824064.

Single Sign On today

- No authentication required.
- HTTP Basic Authentication. (RFC7235 updating RFC2617)
- Transport Layer Security (TLS) with passwords. (RFC5246)
- Transport Layer Security (TLS) with client certificates. (RFC5246 & RFC6818)
- Cookies. (RFC6265)
- Open ~~Authentication~~ Authorization (OAuth2). (RFC6749)
- Security Assertion Markup Language (SAML). (saml-core-2.0-os OASIS standard)
- OpenID. (OpenID Foundation standards)

IVOA service providers exposing secured services register in the IVOA registry metadata expressing conformance to one or more of the authentication mechanisms approved in the IVOA SSO profile using the *securityMethod*

element.

SSO mechanism	***<securityMethod>***
HTTP Basic Authentication	*ivo://ivoa.net/sso#BasicAA*
TLS with password	*ivo://ivoa.net/sso#tls-with-password*
TLS with client certificate	*ivo://ivoa.net/sso#tls-with-certificate*
Cookies	*ivo://ivoa.net/sso#cookie*
Open Authentication	*ivo://ivoa.net/sso#OAuth*
SAML	*ivo://ivoa.net/sso#saml2.0*
OpenID	*ivo://ivoa.net/sso#OpenID*

(“the dream of SSO-1.0 was that everyone had a personal client certificate from a trusted CA”)

Funded by the European Union’s Horizon 2020 - Grant N° 824064

SSO Today

- Only the security method is not enough
- "We can only expect clients (TOPCAT, pyVO, . . .) to support auth if it's halfway clear what they need to implement" Markus 2019
- Various Proposal and Ideas and implementations
  - https://wiki.ivoa.net/internal/IVOA/InterOpOct2019DAL/authlessons.pdf
  - https://wiki.ivoa.net/internal/IVOA/InterOpMay2020GWS/auth-reqs-strawman.pdf
  - https://wiki.ivoa.net/internal/IVOA/InterOpNov2020GWS/TokensForCLI.pdf
  - https://wiki.ivoa.net/internal/IVOA/InterOpMay2020GWS/SSO_session_intro.pdf
  - https://wiki.ivoa.net/internal/IVOA/InterOpMay2019GWS/Access_Control_with_All_the_Protocols.pdf
  - https://wiki.ivoa.net/internal/IVOA/InterOpNov2020GWS/auth.pdf

Funded by the European Union's Horizon 2020 - Grant N° 824064

What is missing?

- “How does a service tell users (client software) **how** and **where** to log in?”

```
<securityMethod standardID="ivo://ivoa.net/sso#RFC6750">
          <tokenGetter type="userpass">https://<cadc>/anywhere/login </tokenGetter>
</securityMethod>
```

- “Explain how to use SSO the security methods”

- VOSI-Capability style or challenge using HTTP Header?

Funded by the European Union’s Horizon 2020 - Grant N° 824064

CADC proposal

Anonymous query to partially private TAP service

```
REQUEST:
    HTTP GET to /tap/sync

RESPONSE:
    HTTP/1.1 200, 401, or 404
    WWW-Authenticate:
        vo-sso securitymethod="ivo://ivoa.net/sso#tls-with-certificate"
    WWW-Authenticate:
        vo-sso securitymethod="ivo://ivoa.net/sso#oauth",
            accessURL="https://proto.canfar.net/ac/authorize"
    WWW-Authenticate:
        vo-sso securitymethod="tls-with-password",
            accessURL="https://proto.canfar.net/ac/login"
```

- 200 (OK) response has VO-Table with possible omitted content
- 401 (Unauthorized) response if query not allowed
- 404 (Not Found) response if query not allowed (but don't want to reveal that)

Funded by the European Union's Horizon 2020 - Grant N° 824064

CADC proposal

Successful (TLS) call to /login

```
REQUEST:
    HTTP GET/POST to <base-url>/login?
        userid=<userid>&password=<password>
        &scope=<my-tap-ivoid>

RESPONSE:
    HTTP/1.1 200 OK
    X-Auth-Token: <token>
    X-VO-Authenticated: <user-id>

BODY:
    <json-token-bundle>
```

- Same response as authenticated call to /authorize
- scope param optional

Funded by the European Union's Horizon 2020 - Grant N° 824064

CADC proposal

TAP Capabilities TBD

```
<capability standardID="ivo://ivoa.net/std/TAP"
xmlns:tr="http://www.ivoa.net/xml/TAPRegExt/v1.0" xsi:type="tr:TableAccess">
     <interface xsi:type="vs:ParamHTTP" role="std" version="1.1">
          <accessURL use="base">https://ws-cadc.canfar.net/youcat</accessURL>
          <securityMethod/>
          <securityMethod standardID="ivo://ivoa.net/sso#tls-with-certificate"/>
          <securityMethod standardID="ivo://ivoa.net/sso#oauth"/>
     </interface>
</capability>
```

Problem: need more info to use 'oauth'

- No room in securityMethod class in XSD
- Add oauth capability (with accessURL) to this list?

```
<securityMethod standardID="ivo://ivoa.net/sso#oauth">
          <AccessURL use=”base”>https://<cadc>/anywhere/login </AccessURL>
</securityMethod>


maybe

<AccessURL use=”token”>
```


Funded by the European Union’s Horizon 2020 - Grant N° 824064

Mark Client proposal

Challenge Details

Challenge syntax

- RFC 7235:
  - General format:

    `WWW-Authenticate: <auth-scheme-name> <scheme-params>`
  - Example (Basic Auth, RFC 7617):

    `WWW-Authenticate: Basic realm="WallyWorld"`
- `<auth-scheme-name>` must match RFC7230 *token* syntax
  - "`ivo://ivoa.net/std/SSO#cookie`" is not syntactically legal (contains "/")
  - Could use:
    - `WWW-Authenticate: vo-sso-cookie loginurl="https://..."`
    - `WWW-Authenticate: vo-sso securityMethod="ivo://ivoa.net/std/SSO#cookie" loginurl="https://..."`
    - ... or something else
  - Easy to solve — just choose one
  - There is an IANA registry of these `<auth-scheme-name>s`, but registration not required

Challenge specifics:

- Define `<scheme-params>` for cookie login protocol
- + similar questions for other SSO auth mechanisms that we want to use

Mark Taylor, Authentication Implementation, IVOA virtual meeting, 19 November 2020 5/10

Funded by the European Union's Horizon 2020 - Grant N° 824064

Mark…again

Bootstrapping

How to establish auth context for TAP-like service?

- Get login instructions from /capabilities endpoint (new `<securityMethod>` extensions)
  - ▷ Preferred by Gaia/ESA?
  - ▷ Duplicates challenge-based login instructions, more standardisation required
- Wait for challenge with 401 during normal service interaction?
  - ▷ User may find out they are unauthenticated at late stage (e.g. after entering ADQL)
  - ▷ Doesn't work for services that work in both Anon + Auth mode (401 is never encountered)
- Get challenge some other way using existing endpoints?
  - ▷ Provoke 401 with dummy request `WWW-Authenticate: tell-me-how`?
  - ▷ All service responses (including 200s) include `WWW-Authenticate` challenges?
  - ▷ Either would work if services cooperate, but what endpoint to use?
    - ○ `/capabilities`? `/tables`? Might have different auth than query endpoints
    - ○ TAP `/sync`//`async` query endpoint? might fail for non-auth reasons
- Dedicated authentication endpoint? (Markus suggestion):
  - ▷ Dedicated endpoint just to issue `WWW-Authenticate` challenges
  - ▷ Response is 200 for auth/anon service, 401/403 for auth-only service
  - ▷ DaCHS has prototyped this as `<tap-base-url>/authcheck` endpoint
    - ○ Seems to work nicely

Mark Taylor, Authentication Implementation, IVOA virtual meeting, 19 November 2020 6/10

Funded by the European Union's Horizon 2020 - Grant N° 824064

Brian Today

Final matters

- 'authcheck' endpoint? (eg `https://ws-cadc.canfar.net/youcat/authcheck`)
  - a sibling to the capabilities endpoint
- What should clients use as an index for user identification? Should the value of x-vo-authenticated be deterministic?
- Client implementations
  - TopCat - Comments Mark?
  - CADC networking libraries (Java)
  - PyVO next?

- Tokens (OAuth, ivoa) in Credential Delegation Protocol (CDP)

Funded by the European Union's Horizon 2020 - Grant N° 824064

What do we need?

- Technically
  - Review each of the SecurityMethods and identify and standardize “how/where” (**extensions**!!!!)
  - Define a standard challenge
  - Implement a Token method
- In practice:
  - A team of experts that works on the new standard for a few months (target next Interop)
  - Involve Apps and SciPlats
  - A meeting each month Jun, Jul, Sept

Funded by the European Union’s Horizon 2020 - Grant N° 824064