SSO Specification Restructure

S. Bertocco (GWS Vice Chair) - remote

INAF
ISTITUTO NAZIONALE
DI ASTROFISICA

IVOA Spring Inteop, Sydney 20-24 May 2024

Temptative SSO restructure

https://github.com/bertocco

No pull request:

- Re-organized
- Proposed changes

the /capability end-point of the service to know if and which authentication method is supported The declaration of the supported authentication mechanism in the service registration is not mandatory, the client has to call the */capability* end-point of the service to know if and which authentication method is supported Editor's (Sara) note: the following must be confirmed: they MAY use either the IVOA-standard mechanisms or others that are not IVOA standards, but they MUST answer with the challenge described in section 4.1.1 "Bootstrapping and IVOA challenge-response protocol".

3.4 Commentary

The IVOA SSO profile allows the development of a "realm" of interoperable services and clients. Service providers opt in to this realm by implementing this current standard. The IVOA challenge-response authentication mechanism allows clients to know if a service is secured and to be able to use it without being customized for the details of the specific service.

Services within the Virtual Observatory that are not intended to be widely interoperable need not opt in to the SSO realm. In particular, "private" services, accessed by web browsers and protected by passwords, are allowed. However, these private services SHOULD be reworked to follow the IVOA standard if they are later promoted to a wider audience.

4 Authentication mechanisms implementation and usage examples in IVOA framework

Approved authentication mechanisms are briefly introduced with reference

Feedback (1)

“there's quite a bit of text that's not serving much purpose.”

“It contains a list of auth technologies "approved for use in the IVOA-SSO profile", but since these don't have to be interoperable”

“don't see much point in providing an "approved" list of web-based technologies for authentication”

“We no longer require the SecurityMethod definitions, having decided that this is not a Registry matter”

Feedback (2)

Mark Taylor:

“the scope of this document should be reconsidered.”

“I make the provocative suggestion that the SSO document should be rewritten more or less from scratch, including some but not much text from its current form, describing only(?) how non-browser clients can interact with authenticated services in a VO-standard way.”

“The document would perhaps acquire a new name or become a different document in the process. If GWS agrees this is a good way forward, I'm willing to draft such a document.”

Feedback (3)

James Tocknell:
“I know the ESO archive uses at least the "resource owner credentials flow" (or "password grant", there's various names for the same thing), which is unfortunately going away in OAuth 2.1, as otherwise it would be the easiest for non- browser clients to implement, having written a wrapper around it for accessing the ESO archive, but what do other groups use? Should we make a page under the SSO next page where we tabulate that?”

Feedback (3)

Paul Harrison:
“it seems that if there were true SSO for the VO then there would probably only really need to be a small number of SSO servers (often called proxies in AAI literature) that could be “well-known” to clients in much the same way as registries are.”

Feedback (4)

Markus Demleitner:

…

List of review comments

...

“I'm happy to contribute whatever I can to SSO-reform (but realistically, I'm afraid that'll mainly be the Registry aspects...)”

My proposal

Write a new document different from SSO

I volunteer myself to write a draft

- Collecting changes available information in the wiki SSO-next (https://wiki.ivoa.net/twiki/bin/view/IVOA/SSO_next)
- Keeping into account contributions coming from the gws mailing list
- Underlining open points to facilitate authors contributions

Discussion

Decision needed