INTEROPERABILITY MEETING

Distributed Services & Protocols

Working Group

Closing

Chairs Jesús Salgado · Sara Bertocco

Perth, Australia

6–8 November 2026

The meeting at a glance

One session, four talks and a moderated discussion: from an AI-ready VO to the first public AuthVO Working Draft.

KEY OUTCOME

First AuthVO Working Draft

WD-AuthVO-1.0-20261029 published. Cookie and X.509 challenges stable and in production; bearer tokens converging on RFC 9728 with a mandatory resource check.

DELIVERED

Implementations on both sides

Data Central: pyvo and vollt pull requests, Apereo CAS tested. SKAO: reference clients, plus an INDIGO IAM fork that publishes protected_resources.

01 AI-ready astronomy

What the IVOA must add so agents can discover, invoke and combine capabilities

02 Federated identity

One identity across SRCNet nodes, each keeping local control

03 AuthVO & bearer tokens

Implementation status, phishing attacks and how to block them, IAM support

SESSION · DSP · SAT 7 NOV

AI-ready Astronomy, Identity & AuthVO

1 CHENZHOU CUI

IVOA for AI-ready Astronomy: What Is Still Missing?

The IVOA made resources interoperable; AI-era science needs capabilities to be. Gaps in data fusion, capability description, workflows and models, and trust.

15'+5'

2 ADRIAN DAMIAN

One Identity, Many Local Nodes

SRCNet Keycloak prototype: nodes federate peer to peer with OpenID Connect, so a user keeps one identity while each node keeps local control.

15'+5'

3 JAMES TOCKNELL

AuthVO at Data Central: status update

pyvo and vollt pull requests, Apereo CAS fully tested with AuthVO, and a dynamic client registration helper ready for Data Central 3.0.

15'

4 MARK TAYLOR

AuthVO: Status and Bearer Tokens

First Working Draft published. Two phishing attacks on RFC 9728 discovery, and what blocks each: the resource check and RFC 8707.

10'

THEME 01 · CHENZHOU CUI

AI-ready astronomy: what is still missing

From data access to capability access: agents must discover, invoke, compose and verify astronomical capabilities, not only find data.

A Data fusion

From catalogue cross-match to pixel-level and learned, multimodal representations

B Capabilities & tools

What a capability does, when it applies, and whether outputs can be chained

C Workflows & models

Workflow, execution-environment and AI model profiles on top of UWS, PDL, ProvenanceDM

D Trust & identity

Provenance of agent decisions, scoped authorisation and delegation for agents

PROPOSED PLAN

NOW

Collect use cases, map gaps, cross-WG activity, Use Cases & Gap Analysis Note

NEXT

Capability, workflow, model and provenance profiles; prototypes

THEN

Reference implementations and interop tests

LATER

Standardise only where implementations show the need

REUSE → PROFILE → INTEGRATE → PROTOTYPE → STANDARDISE ONLY WHEN NECESSARY

THEME 03 · JAMES TOCKNELL

AuthVO at Data Central

pyvo pull request

astropy/pyvo #785: AuthVO with OAuth 2 and the device code flow. Open question: which OAuth library, given maintenance concerns about requests-oauthlib.

vollt pull request

gmantele/vollt #165: authorised and anonymous TAP queries work with pyvo. Part of the new Data Central 3.0 TAP service.

Apereo CAS

Provides every feature AuthVO needs. A device-code scope bug is fixed in CAS 8.1, to be deployed when released.

Client registration helper

Controls which clients register: blocks unneeded scopes and wrong redirect URLs. Ready for Data Central 3.0.

Next at Data Central: AuthVO for SIA, SSA and SCS; the pyvo pull request in the May 2027 release; Data Central 3.0 launched with discoverable authentication.

THEME 03 · MARK TAYLOR

Two phishing attacks, and what blocks them

Basic procedure agreed: RFC 9728 discovery, RFC 8414 metadata, RFC 7591 registration, RFC 8628 device grant. RFC 9728 alone says nothing about whether the named server can be trusted.

Attack 1

A malicious service names a real authorization server

The client gets a genuine token and hands it to the malicious service.

Blocked by the resource check

The server's metadata MUST list protected_resources, and the client checks the URL is covered.

Attack 2

A malicious service names a malicious server that reuses the real endpoints

Its fake list includes the malicious service, so the resource check passes.

Blocked by audience restriction (RFC 8707)

The client sends resource; the real server MUST reject a value it does not recognise.

RFC 8707 is not implemented everywhere. Options: require RFC 8707 · RFC 9207 issuer identification (not clearly applicable to the device grant) · DPoP, RFC 9449 · require the endpoints to share the issuer's origin (no standards basis).

MODERATED DISCUSSION · JESÚS SALGADO

AuthVO towards RFC: status and IAM support

Draft

PR #23 merged after two review rounds: PRM on the resource server with an exact match, the issuer's protected_resources list mandatory.

Reference clients

Python and Java, nine scenarios. 22 of 22 checks pass on INDIGO IAM 1.15 with a metadata add-on; 20 of 20 on a patched IAM alone.

INDIGO IAM fork

Publishes RFC 8414 metadata and protected_resources, writes every requested resource in aud, and can refuse unlisted ones with invalid_target.

LINK TO ATTACK 2

The released INDIGO IAM 1.15 issues a token for an unlisted resource, so attack 2 succeeds there. The fork rejects it with invalid_target: the RFC 8707 behaviour the draft needs, ready to propose upstream.

OPEN FOR THE GROUP

1 Require RFC 8707 rejection from authorization servers?

2 How much RFC text the draft should repeat

3 Which IAMs to test: INDIGO, Apereo CAS, Keycloak

KEY OUTCOME

AuthVO: a public Working Draft and a clear bearer-token path

The challenge framework is stable; for bearer tokens, each known attack now has a named defence based on standard RFCs.

Discovery

RFC 9728 resource metadata and RFC 8414 server metadata; registration RFC 7591; device grant RFC 8628.

Resource check

The server's protected_resources list is mandatory and covers the URL: stops attack 1.

Audience restriction

RFC 8707: the server rejects unknown resources: stops attack 2. Implemented in the INDIGO IAM fork.

AFTER PERTH

Next steps

1

AuthVO security

Agree how to close attack 2 where RFC 8707 is missing: require it, DPoP, or an endpoint-origin rule. Record it in the next Working Draft.

2

Implementations

pyvo (#785) and vollt (#165) merged; Data Central 3.0; INDIGO IAM change proposed upstream; tests against a second IAM; new INDIGO IAM deployed at SKAO.

3

Road to RFC

Publish the updated WD, provide real client and server implementations, move towards Proposed Recommendation.

4

AI-ready VO

Collect AI-native use cases and map the gaps; a cross-WG activity and a Use Cases & Gap Analysis Note.

That's a wrap.

Thank you

A first public AuthVO Working Draft and a map towards an AI-ready VO — see you at the next InterOp.

dsp@ivoa.net