INTEROPERABILITY MEETING

Distributed Services & Protocols

Working Group

Opening

Chairs Jesús Salgado · Sara Bertocco

Perth, Australia

6–8 November 2026

DURING THIS MEETING

From federated identity to an AI-ready VO

AI-ready astronomy
data access · metadata · provenance · computing integration

SRC node A	SRC node B	Data centre C
TAP · DataLink · SODA	TAP · DataLink · SODA	TAP · DataLink · SODA

AuthVO · Protected Resource Metadata · Bearer tokens
which service may a token be sent to — the shared trust layer

Federated identity · OIDC peer to peer
one identity, many local nodes, each keeping local control

THEMES THIS MEETING

- AI-ready astronomy: what is still missing
- Federated identity across SRCNet
- AuthVO status and the bearer token problem
- Discussion: the road to RFC

THEME

Theme 1 of 2

01

AI-ready Astronomy

How ready are IVOA standards and infrastructure for AI-driven research, and which gaps should the IVOA close first?

- **Chenzhou Cui** IVOA for AI-ready Astronomy: What Is Still Missing? · 15'+5'

Gaps in data access, metadata, provenance and computing integration — building on the keynote “AI-empowered Astronomy and Open Science” (ISC Beijing Science Dialogue).

THEME

Theme 2 of 2

02

Identity, AuthVO & Tokens

From peer-to-peer identity federation across SRCNet to the AuthVO bearer-token profile, and what must change before RFC.

- **Adrian Damian** One Identity, Many Local Nodes: P2P federation for SRCNet with OIDC
- **James Tocknell** AuthVO implementation: status update
- **Mark Taylor** AuthVO in practice: integration testing and issue #22
- **Me + All** Moderated discussion: AuthVO towards RFC

THEME 02

Identity, AuthVO & Tokens

1 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'

2 James Tocknell

AuthVO implementation: status update

What works today, what implementing the current draft revealed, and open questions for the specification on its way to RFC.

15'

3 Mark Taylor

AuthVO in practice: issue #22

Integration testing between clients and services, a significant bearer-token problem, and a proposal: RFC 9728 with DPoP (RFC 9449).

10'

Where AuthVO stands since Strasbourg

June 2026
Strasbourg

Status and security of tokens presented; bearer-token open issues raised.

Issue #22
Design flaw

The old design was not RFC 9728-conformant: the resource metadata was served from the IAM's origin by a sidecar.

PR #23
Fix proposed

RFC 9728-conformant Bearer profile plus errata: the resource server publishes its own PRM; the issuer vouches via protected_resources.

Oct 2026
Implemented

Python and Java reference clients and a Docker test harness implement the revised draft (WD 2025-05-27, rev. 2026-10-09).

Reference implementation: github.com/jesusjuansalgado/authvo-clients — clients, INDIGO IAM harness and live test scenarios

The problem, and the flow that closes it

THE “EVIL SERVICE”

Plain OAuth2 does not tell a client which resource server a token may be sent to. A malicious service can name a real IAM in its own metadata, lure the user into logging in, and capture a valid token.

Key idea: only the issuer can vouch for which resources it serves.

1	**Probe**	401 ⟶ resource_metadata pointer (untrusted)
2	**PRM at the resource server**	RFC 9728: its resource must cover the requested URL
3	**Resource check at the issuer**	RFC 8414 metadata: same issuer, protected_resources lists the resource
4	**Register**	preconfigured client, or dynamic registration (RFC 7591)
5	**Device login**	RFC 8628, sending resource= (RFC 8707); user sees resource and issuer
6	**Access**	RS checks signature, iss, scope, expiry, aud if present

before any login

SESSION · DSP

DSP Working Group Session

Sat 7 Nov · 09:00–10:30 AWST

Perth · The Hub

Speaker	Title	Time
Chenzhou Cui	IVOA for AI-ready Astronomy: What Is Still Missing?	15'+5'
Adrian Damian	One Identity, Many Local Nodes: Peer-to-Peer Federation for SRCNet with OIDC	15'+5'
James Tocknell	AuthVO implementation: status update	15'
Mark Taylor	AuthVO in practice: integration testing and the bearer token problem (issue #22)	15'
Me+All	Discussions (moderated)	15'

Moderator: Jesús Salgado · Notetakers: Jesús Salgado & Sara Bertocco

Let's get started.

Thank you

Looking forward to the discussions

dsp@ivoa.net