

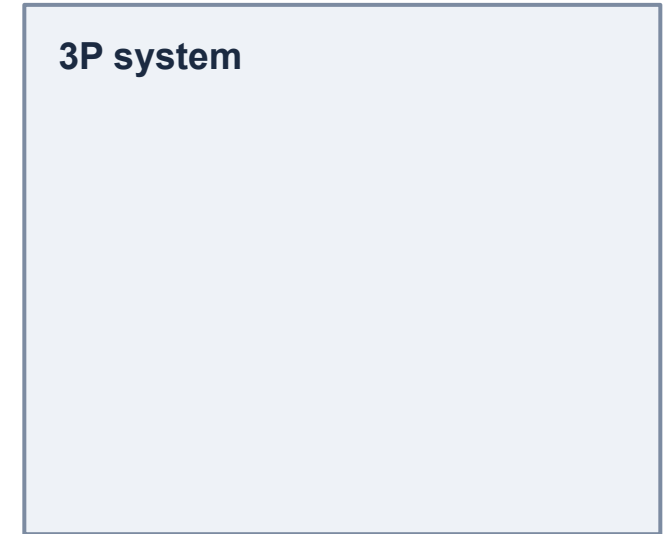
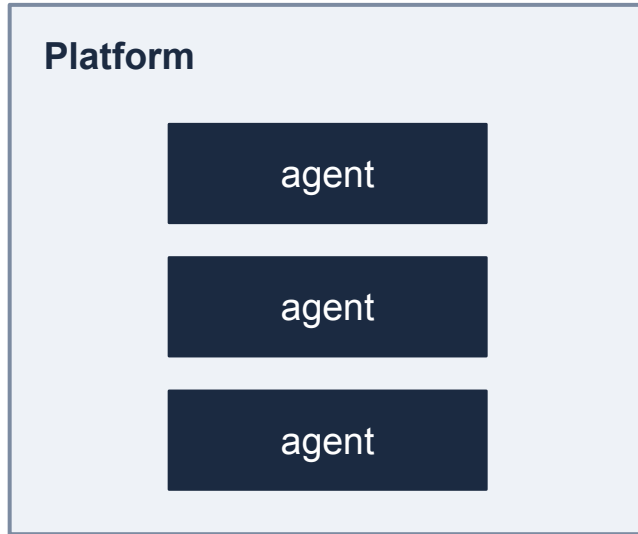
Workload Authorization Grant

draft-carleton-workload-authz-grant-01

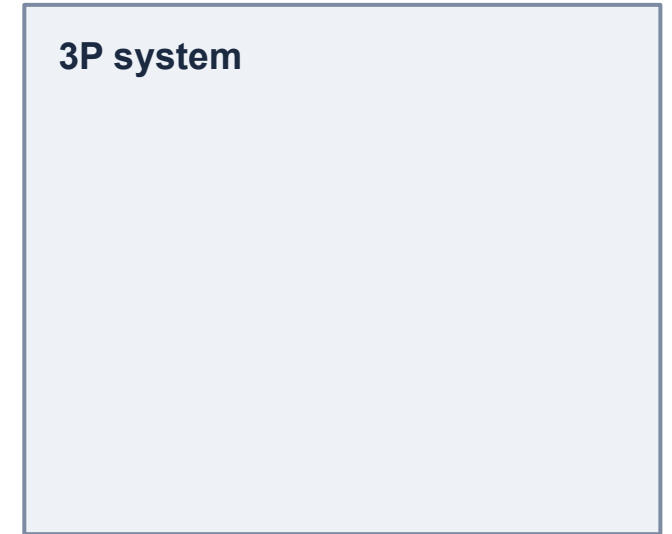
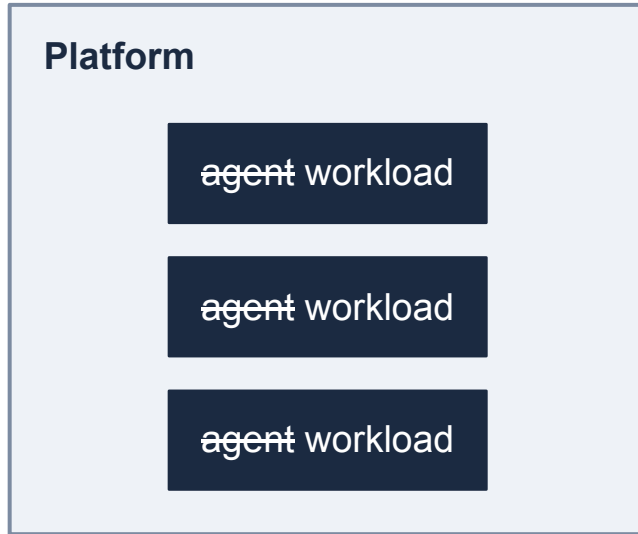
WIMSE interim · 7 October 2026

Carleton · Steele · Parecki · Schwenkschuster · Campbell

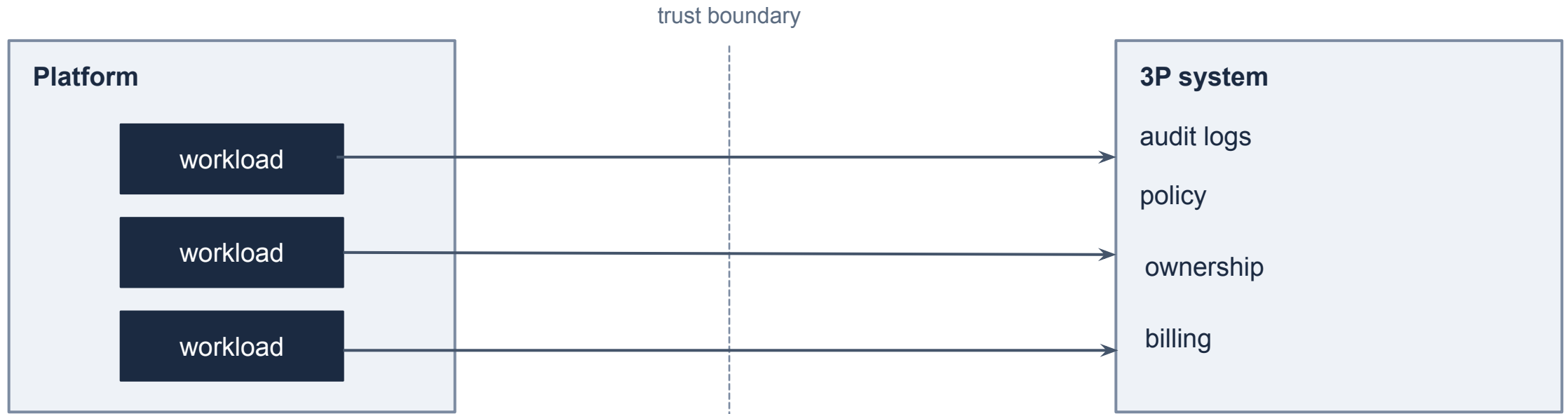
The problem



The problem

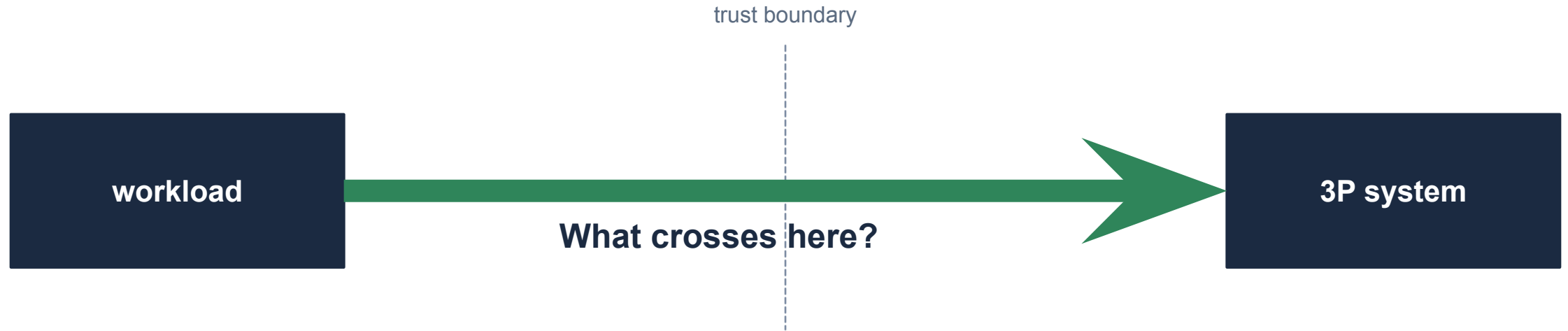


The problem



The 3P system wants to tell the workloads apart.

WAG aims to standardize only this arrow



Constraint: little to no setup per workload.

High friction means folks end up with a shared API key

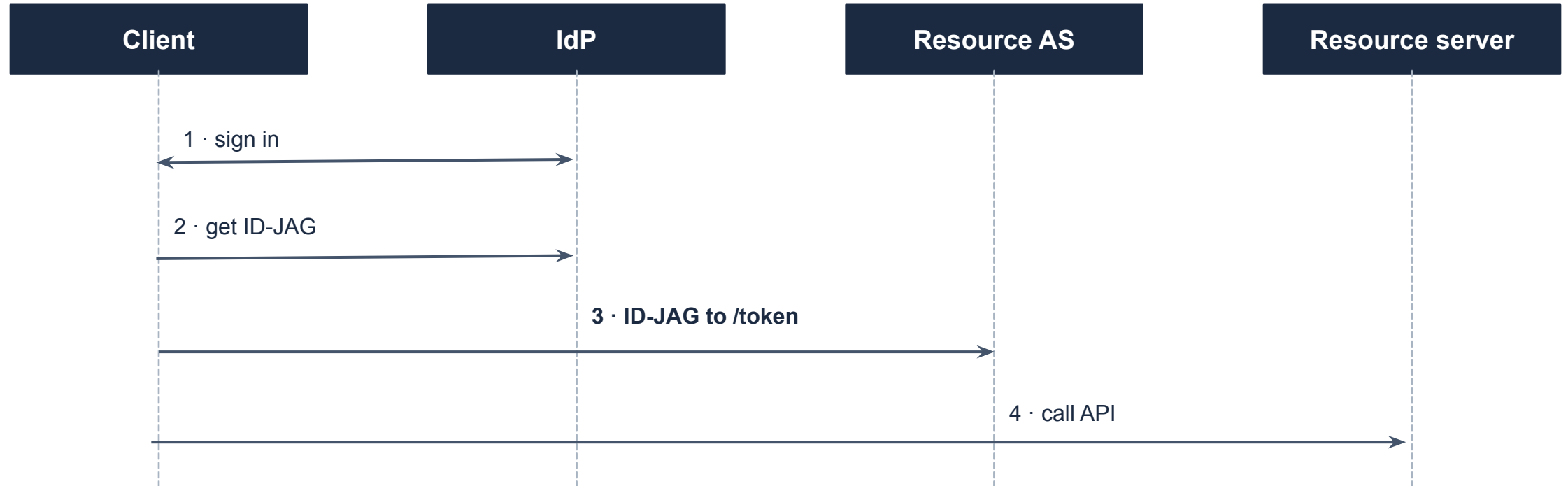
**Workloads, so WIMSE is the
place**

Aside: ID-JAG

- OAuth Draft
- Tackles a similarly shaped problem for humans
- Adopted by MCP
- Has seen adoption

Want to borrow what we can from it for the workload case

Aside: ID-JAG



The ID-JAG pattern we're adapting

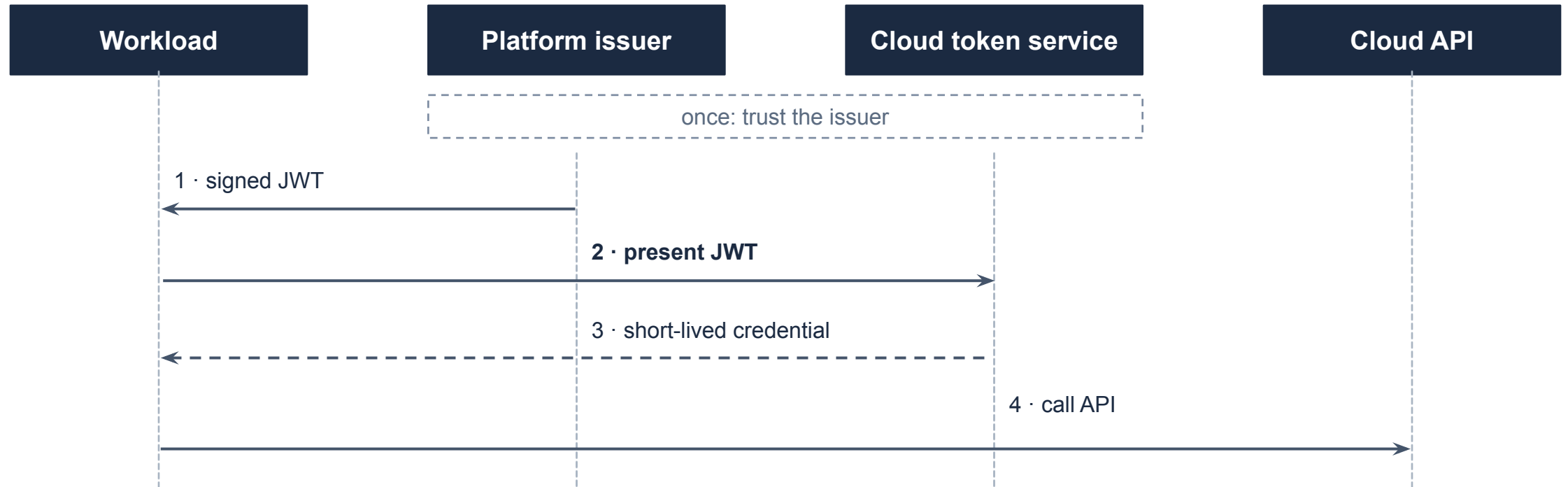
ID-JAG is for humans with SSO. This is for workloads.

Change as little as possible: just the token endpoint.

**“Workload identity federation”:
this pattern exists**

WIF in practice

Three cloud providers, roughly this shape



WIF Bits that work well

[RFC 7523](#) on the wire

- the standard used as OAuth intended.

Central trust establishment

- trust established once, used by many identities

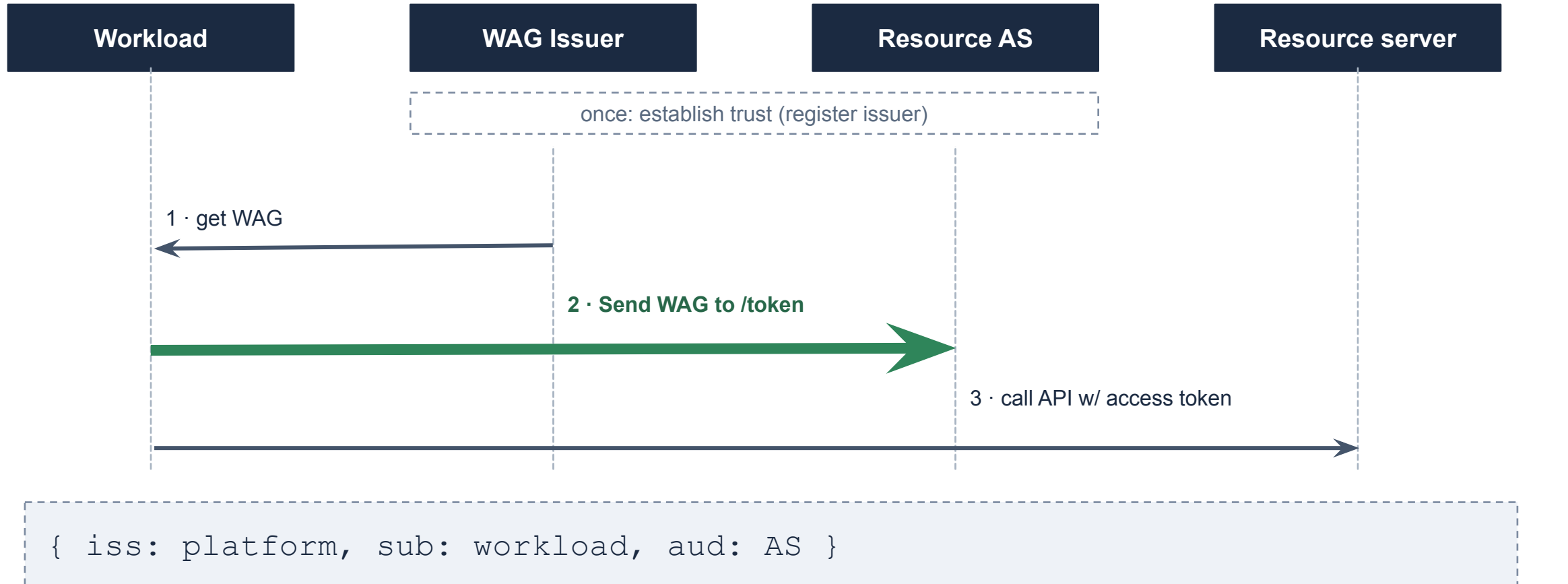
OIDC discovery of the issuer keys

- high adoption

Access is directly given to issuer+subject combinations

- no separate lifecycle, allows for ephemeral subjects

WAG



The grant: an [RFC 7523](#) JWT

Out of scope:

delivery of WAG to the workload · specific claims · fine-grained authz

Is this a problem for WIMSE to tackle?

potential post-adoption topics:

claim mapping · tenancy · IdPs · cardinality



[draft-carleton-workload-authz-grant-01](#)