# PoP: AS <-> Client Key Distribution

**draft-ietf-oauth-pop-key-distribution**

John Bradley, Phil Hunt, Mike Jones, Hannes Tschofenig

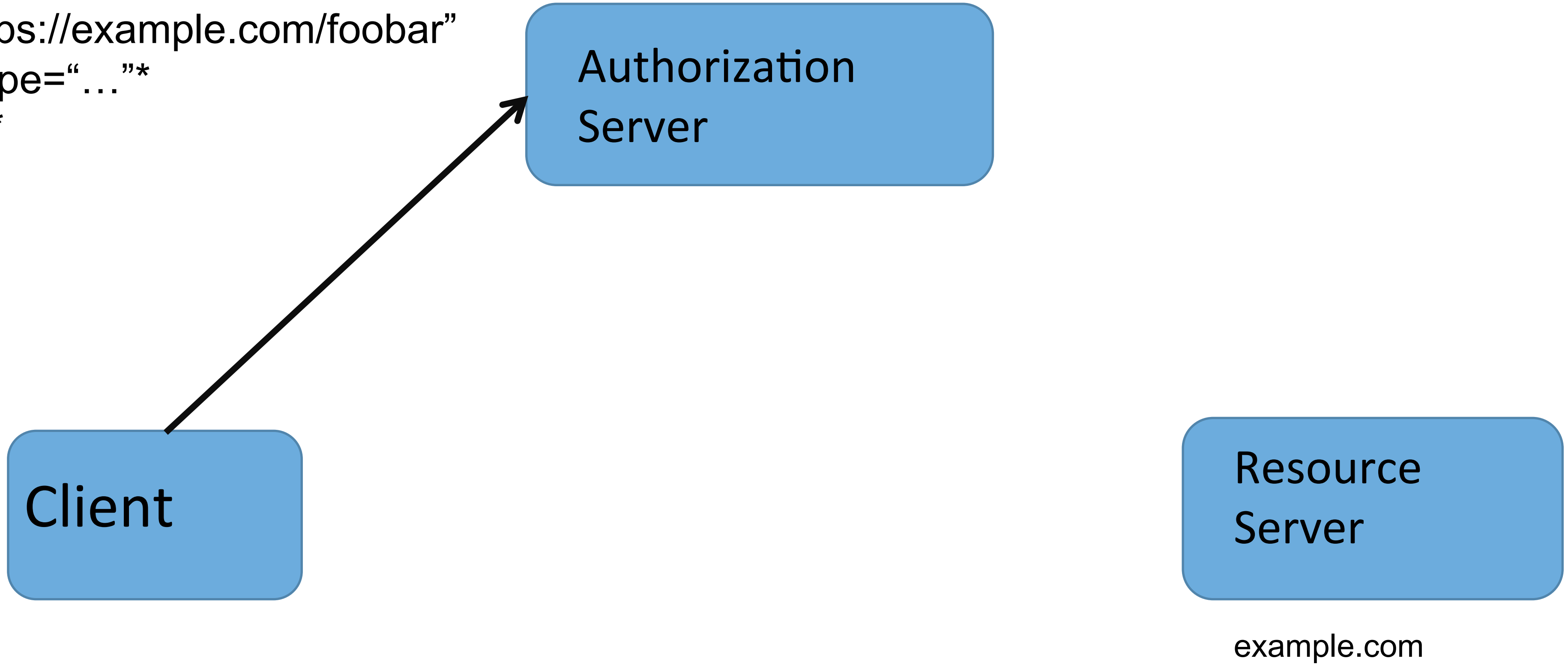
# Agenda

- Overview
- Summary
- Open issues

# AS <-> Client Interaction

**Request**

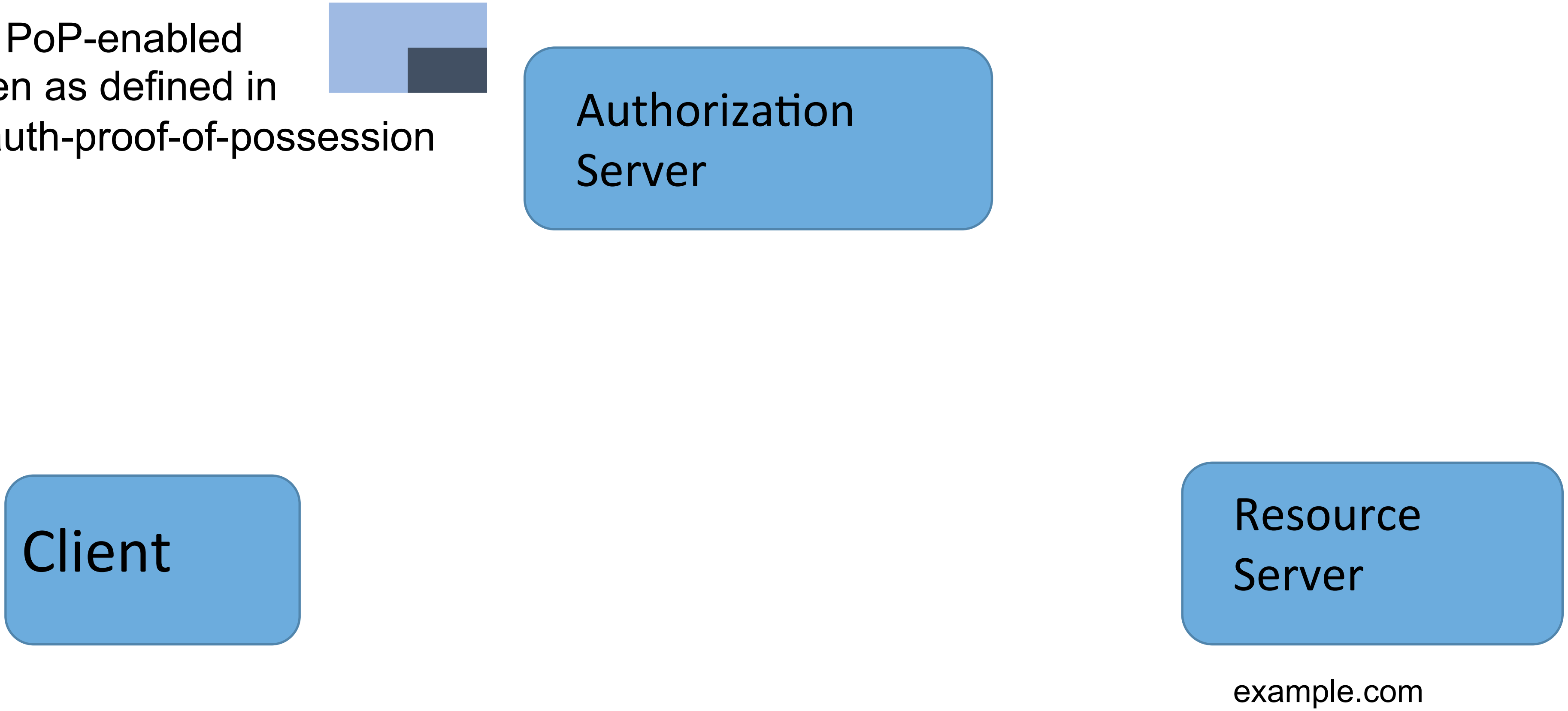
1. aud="https://example.com/foobar"
2. token_type="…"*
3. alg="…"*



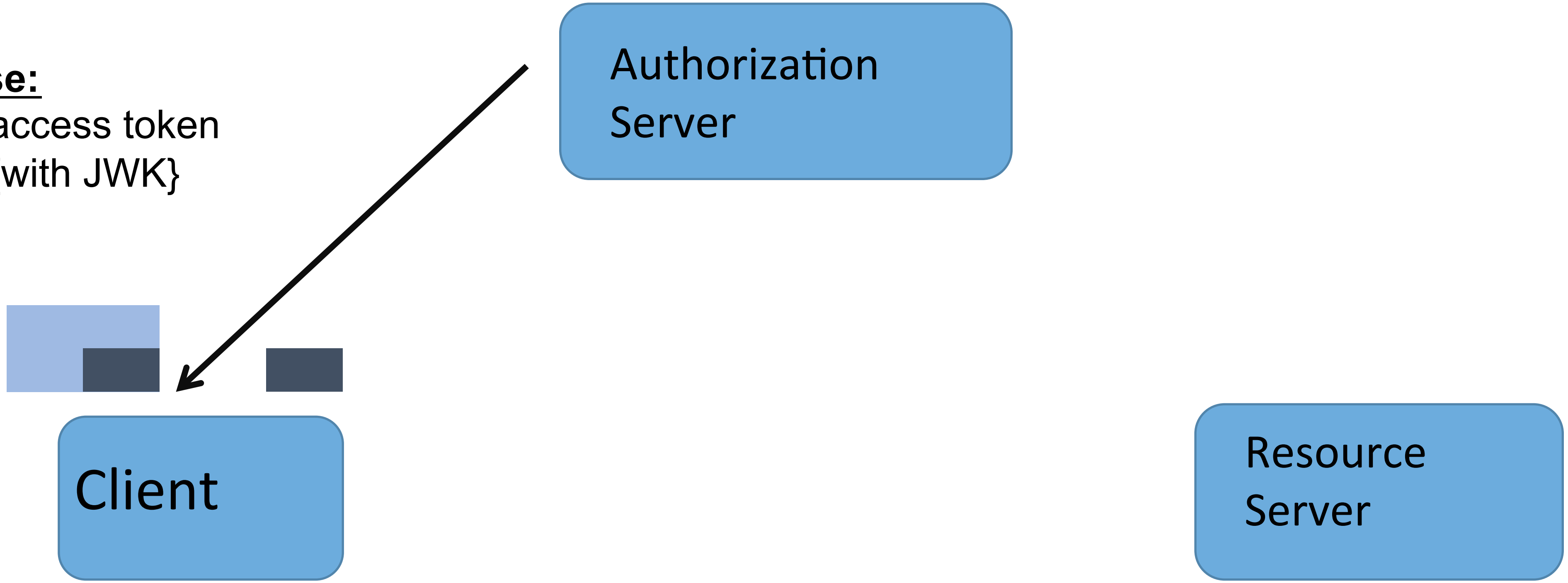
(*): Values defined by protocol specification utilizing the PoP token.

# AS <-> Client Interaction

AS creates PoP-enabled access token as defined in draft-ietf-oauth-proof-of-possession



# AS <-> Client Interaction



**Reponse:**

1. PoP access token
2. key={with JWK}

Note: Specification also allows the client to send key attribute in the request to the AS.

# Summary

- Four new fields defined in this spec:
  - Audience (aud)
  - Key (key)
  - Algorithm (alg)
  - Token Type (token_type)

# Open Issues

1. Asymmetric key could be used with more than one resource server. Should the audience parameter contain a list of values?
2. Should we register alg and token_type for use with the dynamic client registration protocol?
3. Should the PoP functionality also be applicable to the refresh token (and not just to the access token as currently specified)?