draft-zehavi-oauth-audience-bound-client-authorization-01

OAuth 2.0 Audience-Bound Client Authorization

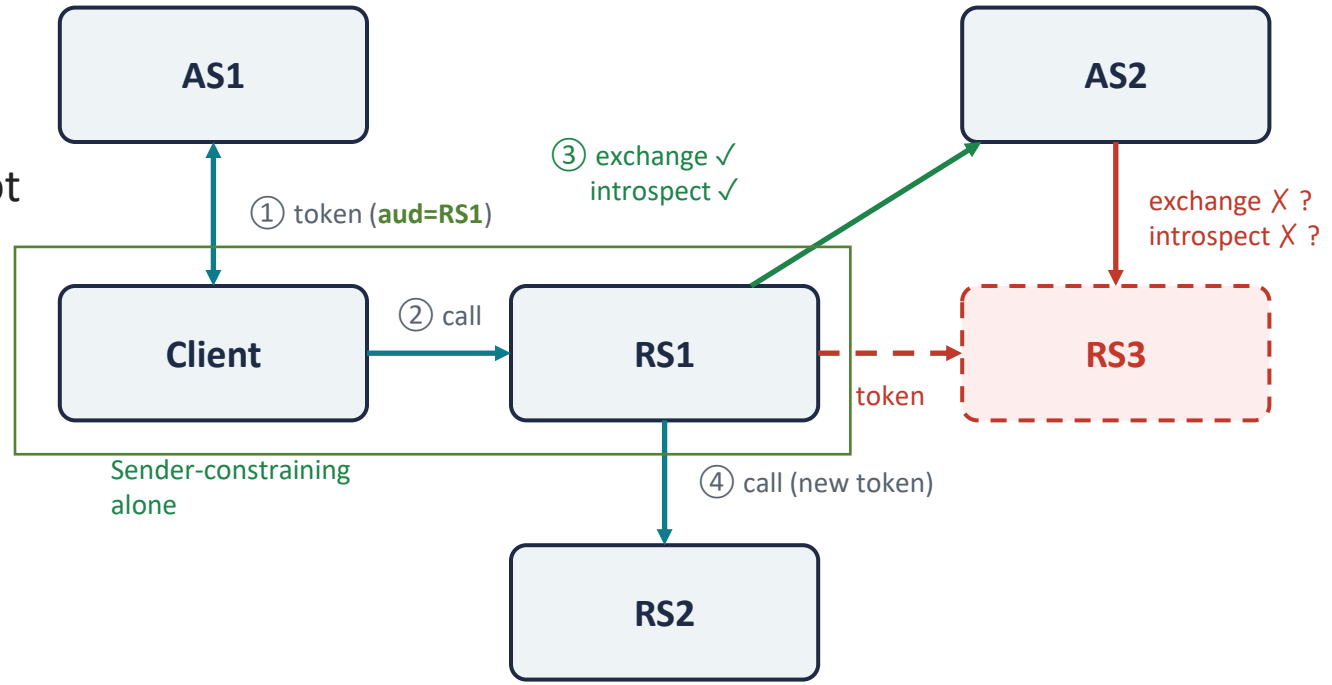


Yaron Zehavi
Raiffeisen Bank International

OAuth Working Group
IETF 127
November 2026

The Audience-to-Client Challenge

- Access tokens are audience-restricted.
- Resources need to act on received tokens.
- A token's (aud) identifies its intended resource, not every authorized client.
- Use cases include token exchange (RFC 8693) and token introspection (RFC 7662).



Key question: **How can an AS verify that a client represents this token's audience?**

Classification: GENERAL

Why This Matters

- Possession of a token alone must not authorize an operation.
- An unauthorized client could learn about a token or misuse it to obtain another.
- Sender-constrained tokens do not prove the **receiving resource is authorized to act on the token**.
- `may_act` is specific to token exchange, and is hard to use when:
  - multiple authorization servers are involved;
  - the issuer cannot predict future client or operation topology.

Classification: GENERAL

Proposal in One Sentence

Anchor authorization for operations on a token in the **token's audience**.

1

Identify the protected resource from aud

→

2

Establish that the requesting client represents that resource

→

3

Then apply policy for the requested operation

Classification: GENERAL

Scope and Non-Goals

This draft defines

- Token-audience processing.
- How an AS establishes an audience-client relationship.
- Local policy, resource-published keys, and metadata mechanisms.
- `resource_clients` protected-resource metadata.

This draft does not define

- A new token claim.
- A replacement for `act` or `may_act`.
- Actor-chain semantics.
- Changes to RFC 8693 or RFC 7662 semantics.

Classification: GENERAL

Use Cases: Exchange & Introspection

1. Authenticate and identify the requesting client.
2. Validate the token under the requested operation's rules.
3. **Establish the audience-client relationship.**
4. Apply operation-specific authorization policy:
   - Token exchange (RFC 8693): authorize the new token. Introspection (RFC 7662): decide what token data to disclose.
5. Perform the operation only if all checks pass.

Classification: GENERAL

Establishing the Audience-Client Relationship

A. Local policy

- Static AS configuration:
- `api://orders` → `rs-orders-client`
- Supports HTTPS and non-HTTPS audience identifiers.

B. Resource-published key

- Resource metadata provides `jwks_uri`.
- Client authenticates using `private_key_jwt`.
- AS validates the client assertion with the resource's key.

C. Protected-resource metadata

- Resource publishes client identities in `resource_clients`.
- AS matches the authenticated client against an applicable entry.

Mechanisms may be combined; AS policy may require more than one to succeed.

Classification: GENERAL

New Metadata Parameter: `resource_clients`

JSON array of OAuth clients representing the protected resource for operations on tokens with that audience.

```
{
  "resource_clients": [
    {
      "authorization_server": "https://as-a.example",
      "client_id": "rs-client-at-as-a"
    },
    {
      "client_id": "https://api.example.com/oauth-client"
    }
  ]
}
```

- `authorization_server`
  - Required for AS-local client IDs.
  - Omitted for globally scoped client IDs.
- `client_id`
  - Required.
  - Identifies an OAuth client representing the resource. AS policy authorizes operations.

Classification: GENERAL

Metadata Discovery and Validation

- Metadata discovery for:
  - HTTPS audience identifiers;
  - audiences already accepted by AS policy.
- Construct the RFC 9728 metadata URL for that resource.
- Metadata `resource` value must match the selected audience.

Classification: GENERAL

Select One Audience Context

- aud can be a string or an array.
- If no candidate matches: **reject**.
- If multiple candidates match but context is ambiguous: **reject**.

Goal: prevent a client associated with one audience from acting under another audience context.

Classification: GENERAL

Interaction with `jwks_uri` and `resource_clients`

- A protected resource may publish:
  - only `jwks_uri`;
  - only `resource_clients`;
  - both.
- If both are used:
  - The authenticated client ID must match an applicable metadata entry.
  - A mismatch is rejected unless AS policy explicitly allows precedence.
- AS policy may require multiple mechanisms to succeed.

Classification: GENERAL

Relationship to `may_act`

- The generalized model does **not** replace RFC 8693 `may_act`.
- `may_act` remains specific to token exchange when the issuer knows the actor at issuance.
- An AS MAY require both:
  - the audience-client relationship for the request; and
  - an appropriate `may_act` claim in the subject token.
- An AS MAY use audience-bound client authorization without `may_act` when local policy permits.
- A `jwks_uri`-validated `private_key_jwt` assertion does not create or replace a `may_act` claim.

Classification: GENERAL

Feedback & Discussion

- Comments welcome on the OAuth WG mailing list: oauth@ietf.org
- Source & issues: github.com/yaron-zehavi/oauth-audience-bound-token-exchange
- Draft: datatracker.ietf.org/doc/draft-zehavi-oauth-audience-bound-client-authorization/

Questions?

Classification: GENERAL