

Interoperable Step Up Authentication for OAuth 2

IETF 113

<https://datatracker.ietf.org/doc/draft-bertocci-oauth-step-up-authn-challenge/>

Vittorio Bertocci

Brian Campbell

Agenda

- Problem
- Proposal
- Discussion

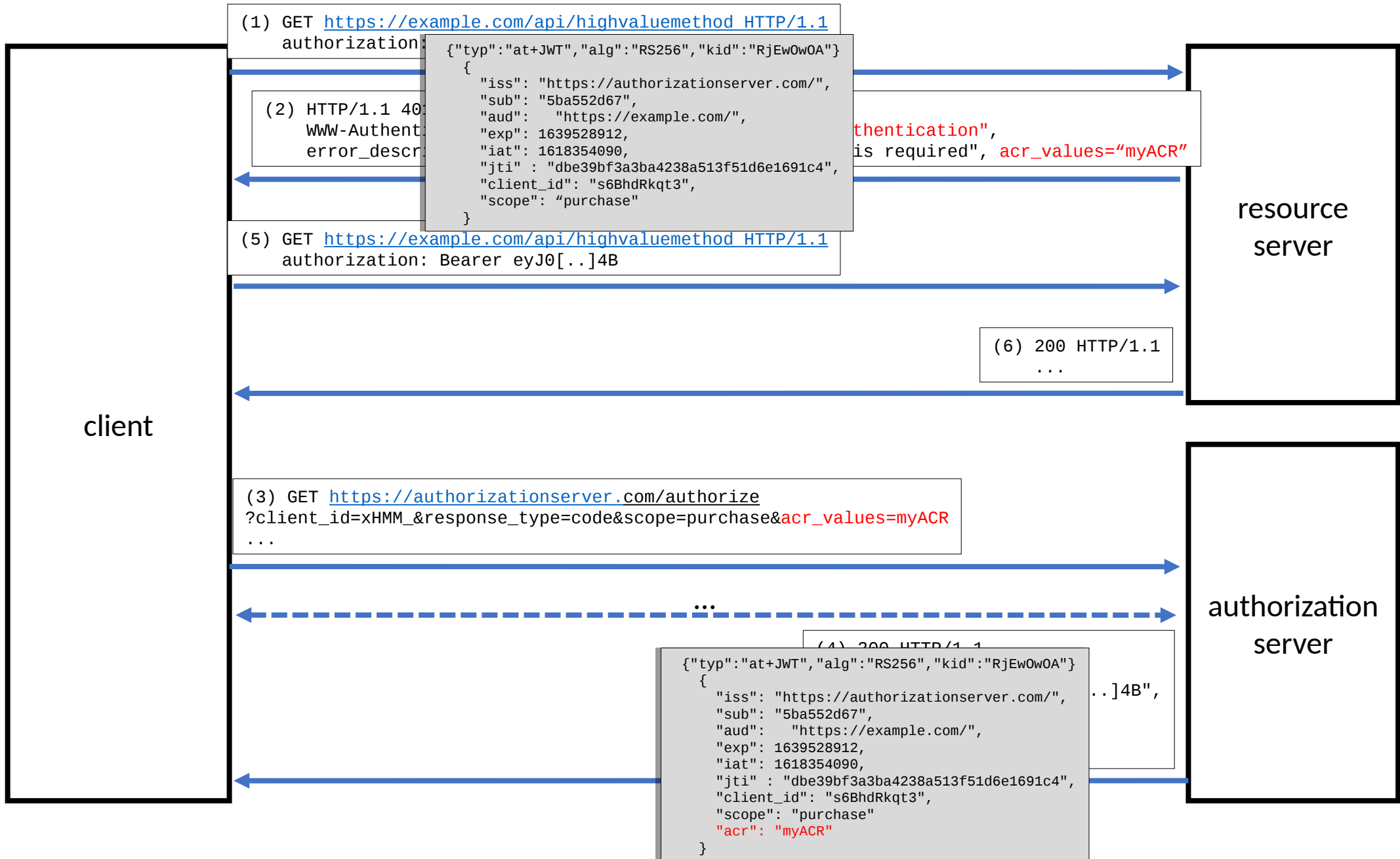
Problem

- An API can reject an access token at any time
 - Even if the token is technically still valid, etc
- Most common reasons
 - Authentication strength deemed insufficient for a particular request
 - Freshness requirements stricter than what the AS-determined expiration would allow
 - E.g. risk management engine determines a fresher token is required
- No obvious way for a client to remediate the error situation

Proposal

- Extend RFC6750 with
 - error code `insufficient_user_authentication`
 - New WWW-Authenticate params `acr_values`, `max_age`
- Require support for AS request parameters `acr_values`, `max_age`
- Provide guidance for JWT ATs and Introspection response to express auth levels in interoperable fashion so that RS can read them

<https://datatracker.ietf.org/doc/draft-bertocci-oauth-step-up-authn-challenge/>



(1) GET <https://example.com/api/highvaluemethod> HTTP/1.1
authorization: Bearer eyJ0[...].4B

```

{"typ": "at+JWT", "alg": "RS256", "kid": "RjEwOw0A"}
{
  "iss": "https://authorizationserver.com/",
  "sub": "5ba552d67",
  "aud": "https://example.com/",
  "exp": 1639528912,
  "iat": 1618354090,
  "jti": "dbe39bf3a3ba4238a513f51d6e1691c4",
  "client_id": "s6BhdRkqt3",
  "scope": "purchase"
}
  
```

(2) HTTP/1.1 401
WWW-Authenticate: Bearer realm="example.com", error_description="Authentication is required", acr_values="myACR"

(5) GET <https://example.com/api/highvaluemethod> HTTP/1.1
authorization: Bearer eyJ0[...].4B

(6) 200 HTTP/1.1
...

(3) GET <https://authorizationserver.com/authorize>
?client_id=xHMM_&response_type=code&scope=purchase&acr_values=myACR
...

```

{"typ": "at+JWT", "alg": "RS256", "kid": "RjEwOw0A"}
{
  "iss": "https://authorizationserver.com/",
  "sub": "5ba552d67",
  "aud": "https://example.com/",
  "exp": 1639528912,
  "iat": 1618354090,
  "jti": "dbe39bf3a3ba4238a513f51d6e1691c4",
  "client_id": "s6BhdRkqt3",
  "scope": "purchase"
  "acr": "myACR"
}
  
```

(4) 200 HTTP/1.1 ...]4B", ...

Advantages

- Interoperable stepup can now be enshrined in client SDKs, API gateways/SDKs, AS
- Very small incremental step on existing feature sets

Discussion