# 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

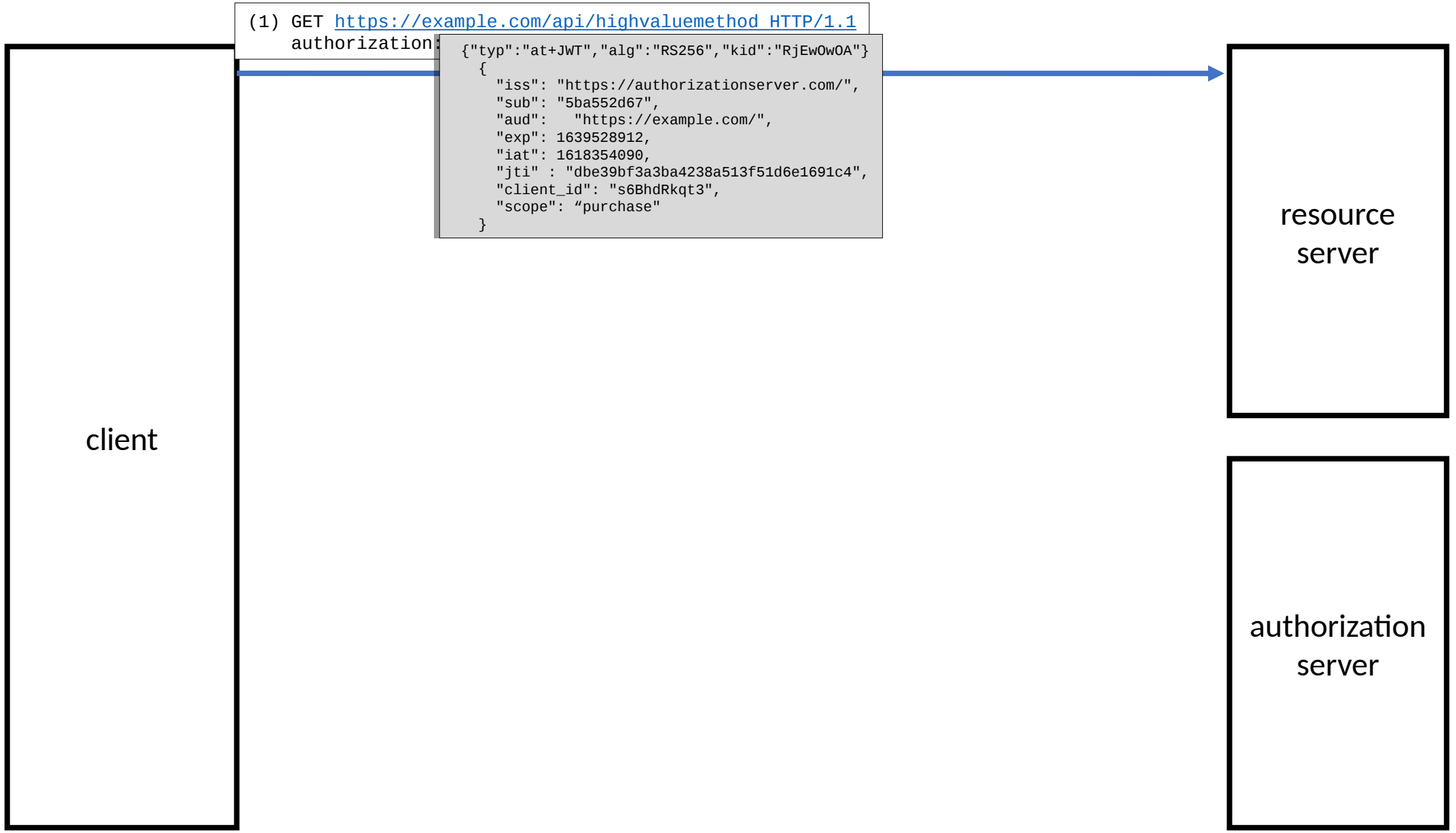
# Proposal

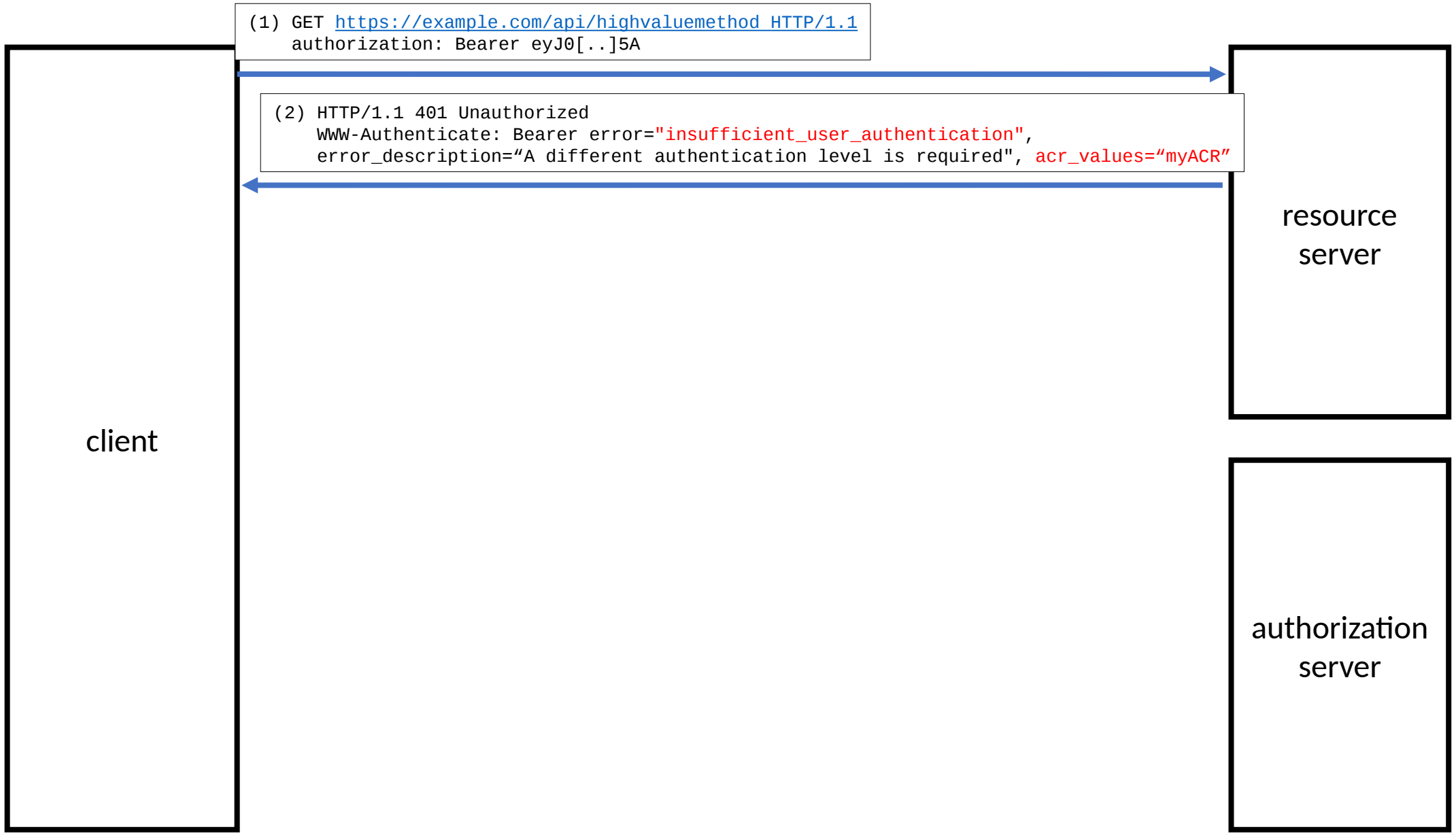
- Extend RFC6750 with
  - error code `insufficient_user_authentication`
  - New `WWW-Authenticate` params `acr_values`, `max_age`
- Require support for AS request parameters `acr_values`, `max_age`
- Provide guidance for JWT ATs and Introspection response to express auth levels in interoperable fashion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

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


client
resource server
authorization server


(1) GET https://example.com/api/highvaluemethod HTTP/1.1
authorization: Bearer eyJ0[..]5A
client
resource server
authorization server

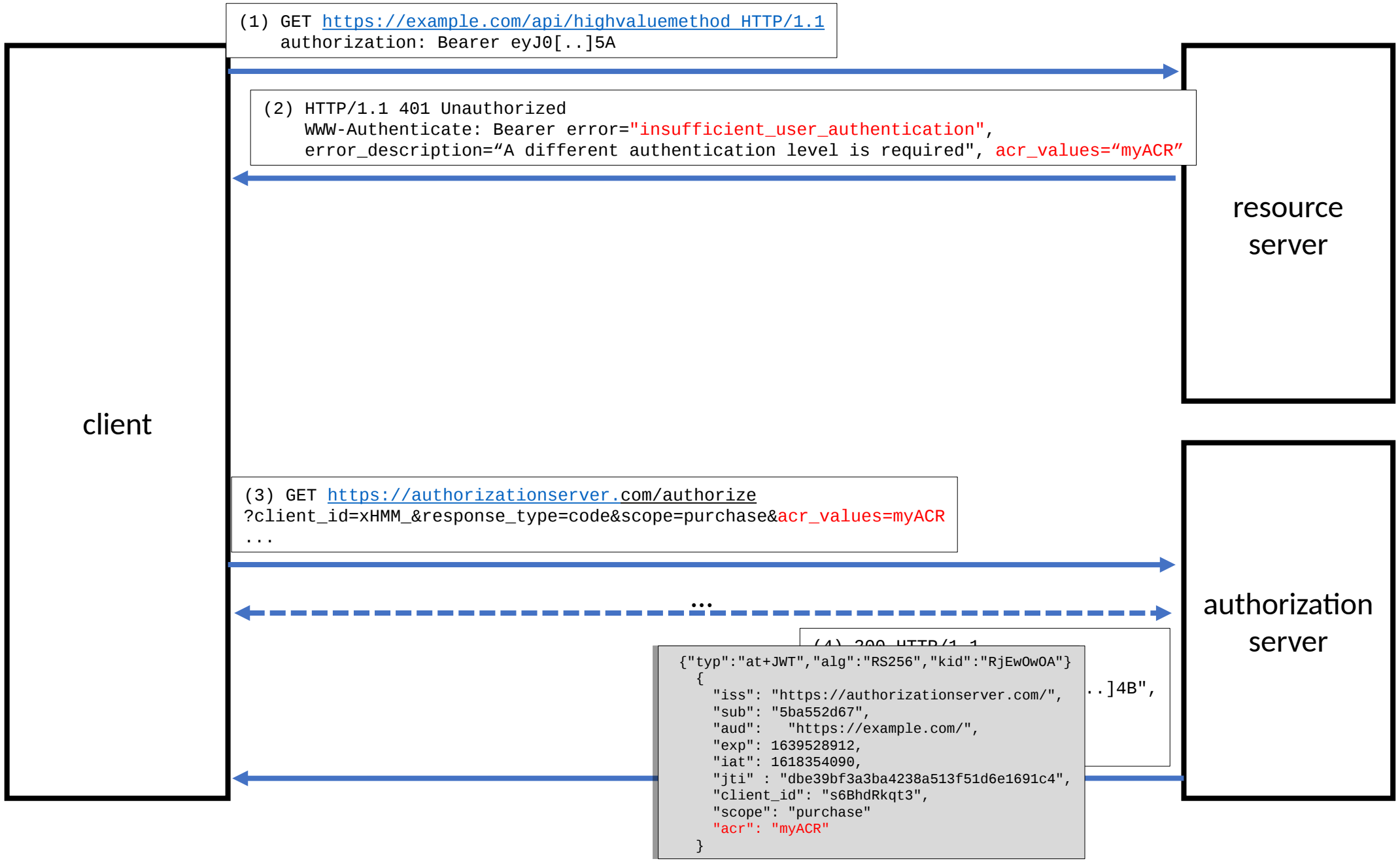

(1) GET https://example.com/api/highvaluemethod HTTP/1.1
authorization:
{"typ":"at+JWT","alg":"RS256","kid":"RjEwOwOA"}
{
"iss": "https://authorizationserver.com/",
"sub": "5ba552d67",
"aud": "https://example.com/",
"exp": 1639528912,
"iat": 1618354090,
"jti" : "dbe39bf3a3ba4238a513f51d6e1691c4",
"client_id": "s6BhdRkqt3",
"scope": “purchase"
}
client
resource server
authorization server


(1) GET https://example.com/api/highvaluemethod HTTP/1.1
authorization: Bearer eyJ0[..]5A
(2) HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer error="insufficient_user_authentication",
error_description="A different authentication level is required", acr_values="myACR"
client
resource server
authorization server


(1) GET https://example.com/api/highvaluemethod HTTP/1.1
authorization: Bearer eyJ0[..]5A
(2) HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer error="insufficient_user_authentication",
error_description="A different authentication level is required", acr_values="myACR"
client
resource server
(3) GET https://authorizationserver.com/authorize
?client_id=xHMM_&response_type=code&scope=purchase&acr_values=myACR
...
authorization server


(1) GET https://example.com/api/highvaluemethod HTTP/1.1
authorization: Bearer eyJ0[..]5A
(2) HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer error="insufficient_user_authentication",
error_description="A different authentication level is required", acr_values="myACR"
resource server
client
(3) GET https://authorizationserver.com/authorize
?client_id=xHMM_&response_type=code&scope=purchase&acr_values=myACR
...
...
authorization server


(1) GET https://example.com/api/highvaluemethod HTTP/1.1
authorization: Bearer eyJ0[..]5A
(2) HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer error="insufficient_user_authentication",
error_description="A different authentication level is required", acr_values="myACR"
resource server
client
(3) GET https://authorizationserver.com/authorize
?client_id=xHMM_&response_type=code&scope=purchase&acr_values=myACR
...
...
(4) 200 HTTP/1.1
{
"access_token" : "eyJ0[..]4B",
"expires_in" : 86400,
"token_type" : "Bearer"
}
authorization server


(1) GET https://example.com/api/highvaluemethod HTTP/1.1
authorization: Bearer eyJ0[..]5A
(2) HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer error="insufficient_user_authentication",
error_description="A different authentication level is required", acr_values="myACR"
client
resource server
(3) GET https://authorizationserver.com/authorize
?client_id=xHMM_&response_type=code&scope=purchase&acr_values=myACR
...
...
authorization server
{"typ":"at+JWT","alg":"RS256","kid":"RjEwOwOA"}
{
"iss": "https://authorizationserver.com/",
"sub": "5ba552d67",
"aud": "https://example.com/",
"exp": 1639528912,
"iat": 1618354090,
"jti" : "dbe39bf3a3ba4238a513f51d6e1691c4",
"client_id": "s6BhdRkqt3",
"scope": "purchase"
"acr": "myACR"
}

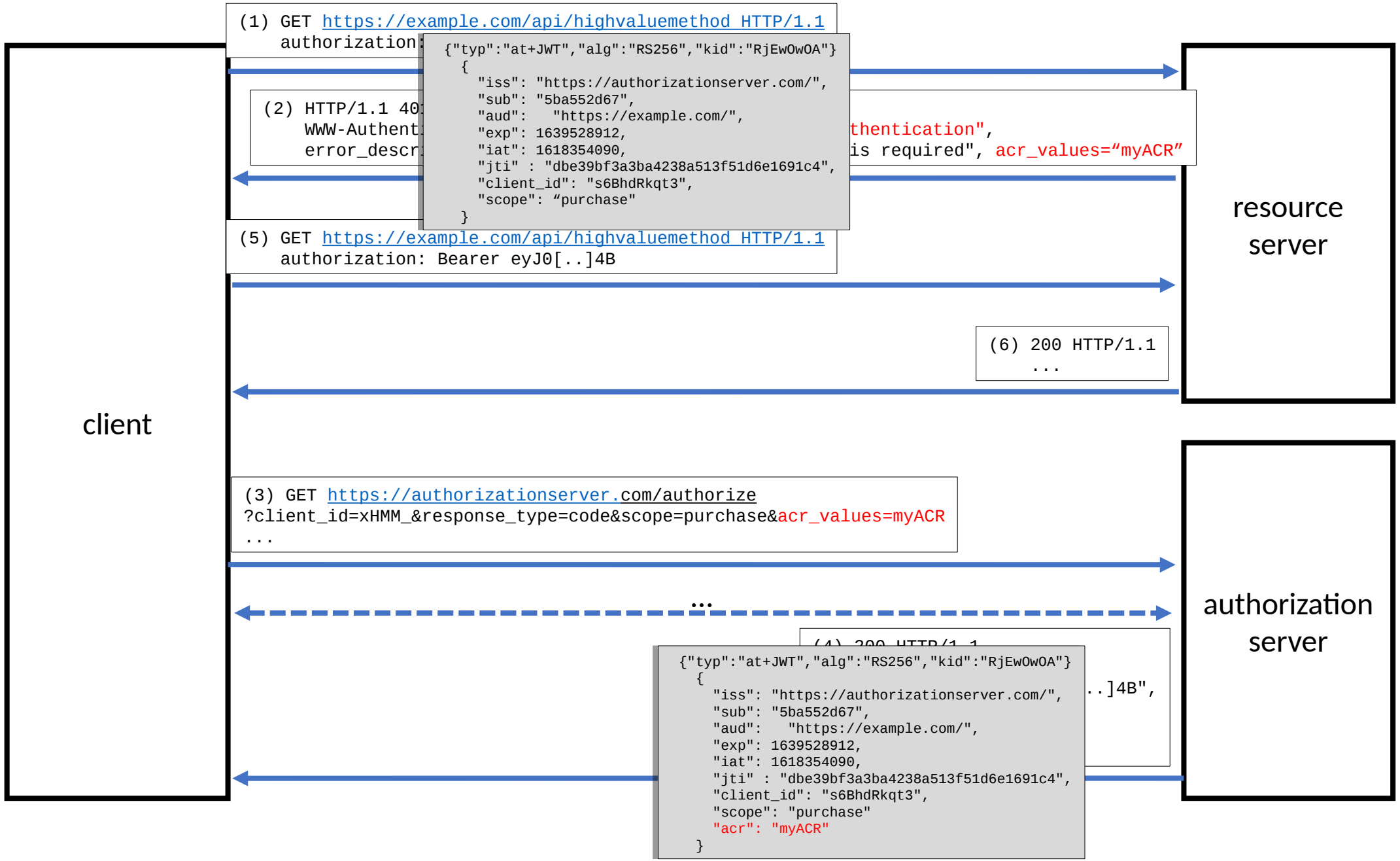

(1) GET https://example.com/api/highvaluemethod HTTP/1.1
authorization: Bearer eyJ0[..]5A
(2) HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer error="insufficient_user_authentication",
error_description="A different authentication level is required", acr_values="myACR"
(5) GET https://example.com/api/highvaluemethod HTTP/1.1
authorization: Bearer eyJ0[..]4B
resource server
client
(3) GET https://authorizationserver.com/authorize
?client_id=xHMM_&response_type=code&scope=purchase&acr_values=myACR
...
...
(4) 200 HTTP/1.1
{
"access_token" : "eyJ0[..]4B",
"expires_in" : 86400,
"token_type" : "Bearer"
}
authorization server


(1) GET https://example.com/api/highvaluemethod HTTP/1.1
authorization: Bearer eyJ0[..]5A
(2) HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer error="insufficient_user_authentication",
error_description="A different authentication level is required", acr_values="myACR"
(5) GET https://example.com/api/highvaluemethod HTTP/1.1
authorization: Bearer eyJ0[..]4B
(6) 200 HTTP/1.1
...
client
resource server
(3) GET https://authorizationserver.com/authorize
?client_id=xHMM_&response_type=code&scope=purchase&acr_values=myACR
...
...
(4) 200 HTTP/1.1
{
"access_token" : "eyJ0[..]4B",
"expires_in" : 86400,
"token_type" : "Bearer"
}
authorization server

# Advantages

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

# Discussion


(1) GET https://example.com/api/highvaluemethod HTTP/1.1
authorization:
{"typ":"at+JWT","alg":"RS256","kid":"RjEwOwOA"}
{
"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-Authenti
error_descri
thentication",
is required", acr_values=“myACR”
resource server
(5) GET https://example.com/api/highvaluemethod HTTP/1.1
authorization: Bearer eyJ0[..]4B
(6) 200 HTTP/1.1
...
client
(3) GET https://authorizationserver.com/authorize
?client_id=xHMM_&response_type=code&scope=purchase&acr_values=myACR
...
...
authorization server
..]4B",
{"typ":"at+JWT","alg":"RS256","kid":"RjEwOwOA"}
{
"iss": "https://authorizationserver.com/",
"sub": "5ba552d67",
"aud": "https://example.com/",
"exp": 1639528912,
"iat": 1618354090,
"jti" : "dbe39bf3a3ba4238a513f51d6e1691c4",
"client_id": "s6BhdRkqt3",
"scope": "purchase"
"acr": "myACR"
}