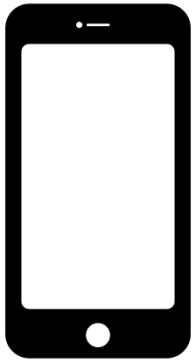
OAuth Interim
June 2024

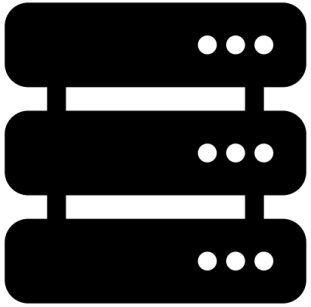
Aaron Parecki

OAuth Global Token Revocation

https://datatracker.ietf.org/doc/html/draft-parecki-oauth-global-token-revocation
draft -03



Token Acquisition

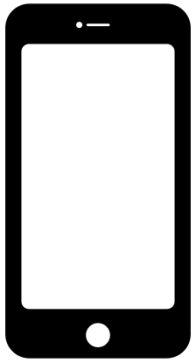


Client

“App”

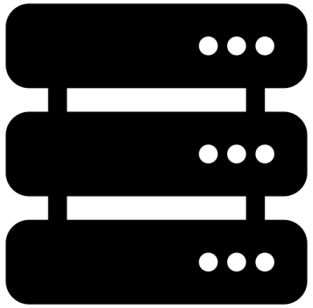
Authorization Server

“App Backend/API”



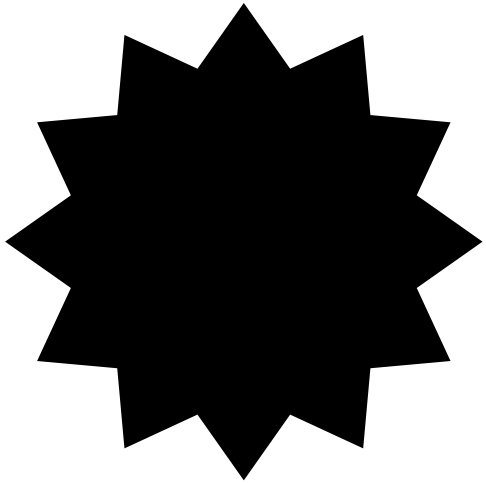
Client

“App”



Authorization Server

“App Backend/API”



Identity Provider
or
Security Monitoring Tools

Global Token Revocation

Input

- Subject Identifier for Security Event Token (RFC 9493)

Authentication:

- Required, but out of scope, just like Token Introspection (RFC 7662)
- (Current implementation is a RFC 7523 JWT sent in a "Bearer" header, similar to OpenID's "Private Key JWT" client authentication)

Outcome:

- MUST revoke refresh tokens
- SHOULD revoke access tokens
- MUST re-authenticate the user before issuing new access tokens or refresh tokens

Global Token Revocation

https://datatracker.ietf.org/doc/html/draft-parecki-oauth-global-token-revocation-03

```
POST /global-token-revocation
Host: example.com
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6Imdsb2JhbC10...

{
  "sub_id": {
    "format": "email",
    "email": "user@example.com"
  }
}
```

Global Token Revocation

https://datatracker.ietf.org/doc/html/draft-parecki-oauth-global-token-revocation-03

```
POST /global-token-revocation
Host: example.com
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6Imdsb2JhbC10...

{
  "sub_id": {
    "format": "opaque",
    "id": "U1234567890"
  }
}
```

Global Token Revocation

https://datatracker.ietf.org/doc/html/draft-parecki-oauth-global-token-revocation-03

```
POST /global-token-revocation
Host: example.com
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6Imdsb2JhbC10...

{
  "sub_id": {
    "format": "iss_sub",
    "iss": "https://authorization-server.com/",
    "sub": "af19c476f1dc4470fa3d0d9a25"
  }
}
```

Global Token Revocation

https://datatracker.ietf.org/doc/html/draft-parecki-oauth-global-token-revocation-03

HTTP response code indicates success/failure

```
HTTP/1.1 204 No Content

HTTP/1.1 400 Bad Request

HTTP/1.1 404 Not Found

etc
```

Existing Token Revocation / Logout Standards

- RFC 7009: Token Revocation
  - Client-initiated, input is the token itself
- OpenID Connect Front-Channel Logout
  - Client-initiated
- OpenID Connect Back-Channel Logout
  - Mostly about terminating sessions
  - "refresh tokens with offline_access SHOULD NOT be revoked"
- OpenID Shared Signals Framework: CAEP / RISC
  - A signal about something that happened, not a command
  - Requires significant infrastructure to receive events

Other Revocation Drafts in this Interim

- OAuth Status Assertions
  - Analogous to a client making a resource request with an access token and including an authorization-server-signed JWT stating that the access token is still valid
- Token Status List
  - A way for the authorization server to publish revocation lists for individual tokens that can be checked by a resource server

Global Token Revocation could be an input to a system that uses either of these, to cause the authorization server to revoke a user's tokens