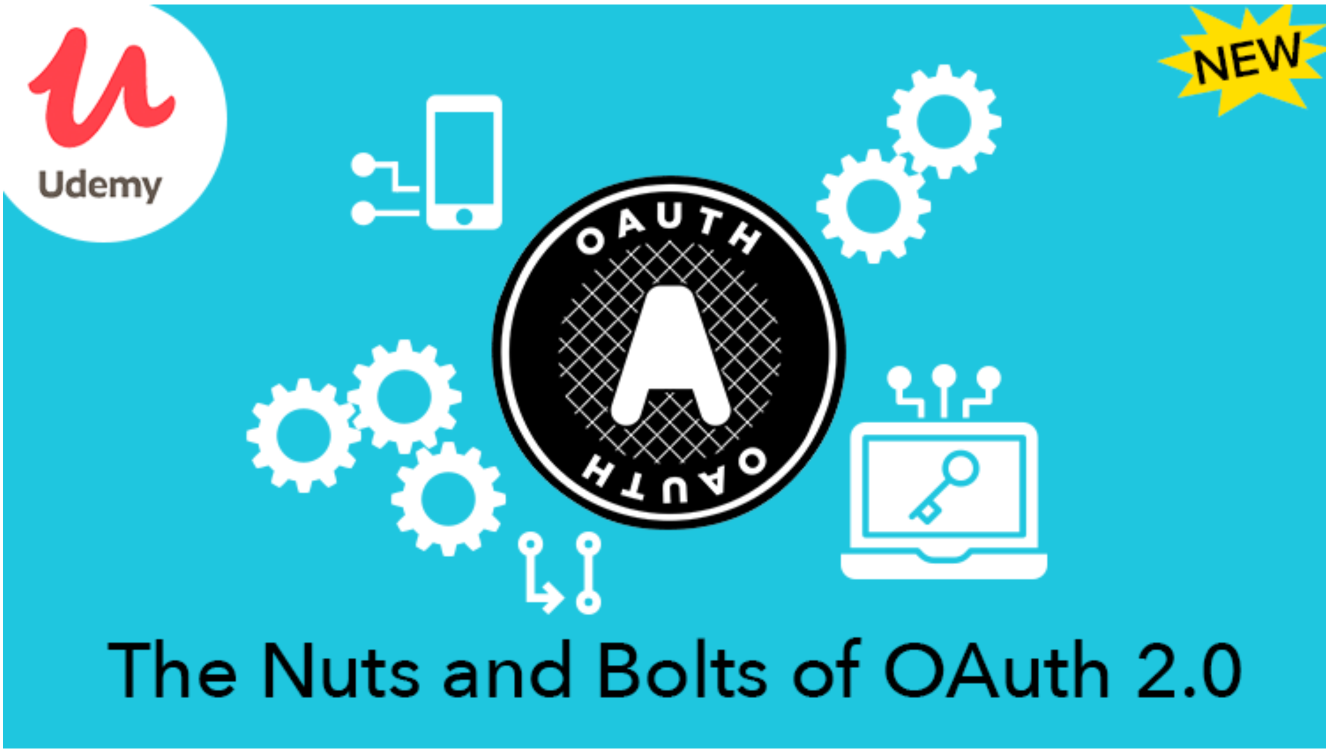
oauth.net/2/

OAuth 2.0

OAuth 2.0 is the industry-standard protocol for authorization. OAuth 2.0 focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices. This specification and its extensions are being developed within the **IETF OAuth Working Group** (https://www.ietf.org/mailman/listinfo/oauth) .

Questions, suggestions and protocol changes should be discussed on the **mailing list** (https://www.ietf.org/mailman/listinfo/oauth) .

Video Course: The Nuts & Bolts of OAuth 2.0



(https://www.udemy.com/course/oauth-2-simplified/?referralCode=B04F59AED67B8DA74FA7)

by Aaron Parecki

OAuth 2.0

- **OAuth 2.0 Framework** (https://tools.ietf.org/html/rfc6749) - RFC 6749
  - **Access Tokens** (/2/access-tokens/)
  - **Refresh Tokens** (/2/refresh-tokens/)
  - **OAuth Scope** (/2/scope/)
- **OAuth Grant Types** (/2/grant-types/)
  - **Authorization Code** (/2/grant-types/authorization-code/)

  - **PKCE** (/2/pkce/)
  - **Client Credentials** (/2/grant-types/client-credentials/)
  - **Device Code** (/2/grant-types/device-code/)
  - **Refresh Token** (/2/grant-types/refresh-token/)
  - Legacy: **Implicit Flow** (/2/grant-types/implicit/)
  - Legacy: **Password Grant** (/2/grant-types/password/)
- **Client Types - Confidential and Public Applications** (/2/client-types/)
- **Bearer Tokens** (/2/bearer-tokens/) - RFC 6750
- **Threat Model and Security Considerations** (/2/security-considerations/) - RFC 6819
- **OAuth Security Best Current Practice** (/2/oauth-best-practice/)

Mobile and Other Devices

- **Native Apps** (/2/native-apps/) - Recommendations for using OAuth with native apps
- **Browser-Based Apps** (/2/browser-based-apps/) - Recommendations for using OAuth with browser-based apps (e.g. an SPA)
- **Device Authorization Grant** (/2/device-flow/) - OAuth for devices with no browser or no keyboard

Token and Token Management

- **JWT Profile for Access Tokens** (/2/jwt-access-tokens/) - RFC 9068, a standard for structured access tokens
- **Token Introspection** (/2/token-introspection/) - RFC 7662, to determine the active state and meta-information of a token
- **Token Revocation** (/2/token-revocation/) - RFC 7009, to signal that a previously obtained token is no longer needed
- **JSON Web Token** (/2/jwt/) - RFC 7519
- **Token Exchange** (/2/token-exchange/) - RFC 8693

Discovery and Registration

- **Authorization Server Metadata** (/2/authorization-server-metadata/) - RFC 8414, for clients to discover OAuth endpoints and authorization server capabilities
- **Dynamic Client Registration** (/2/dynamic-client-registration/) - RFC 7591, to programmatically register OAuth clients
- **Dynamic Client Registration Management** (/2/dynamic-client-management/) - Experimental RFC 7592, for updating and managing dynamically registered OAuth clients

Experimental and Draft Specs

The specs below are either experimental or in draft status and are still active working group items. They will likely change before they are finalized as RFCs or BCPs.

- **Rich Authorization Requests (RAR)** (/2/rich-authorization-requests/)
- **Pushed Authorization Requests (PAR)** (/2/pushed-authorization-requests/)
- **Demonstration of Proof of Possession (DPoP)** (/2/dpop/)
- **Incremental Authorization** (https://tools.ietf.org/html/draft-ietf-oauth-incremental-authz)
- **All OAuth Working Group Documents** (/specs/)

Related Specs and Extensions

- **OAuth Extension Parameter Registry** (https://www.iana.org/assignments/oauth-parameters/oauth-parameters.xhtml)
- **OAuth Assertions Framework** (https://tools.ietf.org/html/rfc7521) - RFC 7521
- **SAML2 Bearer Assertion** (https://tools.ietf.org/html/rfc7522) - RFC 7522, for integrating with existing identity systems
- **JWT Bearer Assertion** (https://tools.ietf.org/html/rfc7523) - RFC 7523, for integrating with existing identity systems
- **WebAuthn - Web Authentication** (/webauthn/)
- **Signing HTTP Messages** (/http-signatures/) - A generic HTTP message signing spec
- **ID Tokens vs Access Tokens** (/id-tokens-vs-access-tokens/)

Community Resources

- **OAuth 2.0 Simplified** (https://aaronparecki.com/oauth-2-simplified/)
- **Books about OAuth** (/books/)
  - **OAuth 2.0 Simplified** (https://oauth2simplified.com) by Aaron Parecki
  - **OAuth 2 in Action** (https://www.amazon.com/OAuth-2-Action-Justin-Richer/dp/161729327X/?tag=oauthnet-20) by Justin Richer and Antonio Sanso
  - **Mastering OAuth 2.0** (https://www.amazon.com/Mastering-OAuth-2-0-Charles-Bihis/dp/1784395404?tag=oauthnet-20) by Charles Bihis
  - **OAuth 2.0 Cookbook** (https://www.amazon.com/dp/178829596X?tag=oauthnet-20) by Adolfo Eloy Nascimento
- **OAuth articles by Alex Bilbie** (https://alexbilbie.com/tag/oauth/)

Protocols Built on OAuth 2.0

- **OpenID Connect** (https://openid.net/connect/) (OpenID Foundation)
- **UMA 2.0** (https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html) (Kantara)
- **IndieAuth** (https://indieauth.spec.indieweb.org/) (W3C)

Code and Services

- **OAuth 2.0 Code and Services** (/code/)

OAuth 2.1

- **OAuth 2.1** (/2.1/) - An in-progress update to simplify OAuth 2.0
- **It's Time for OAuth 2.1** (https://aaronparecki.com/2019/12/12/21/its-time-for-oauth-2-dot-1) (by Aaron Parecki)