IMPORTANT

For the latest stable version, please use Spring Security 7.1.0!

OAuth 2.1 Authorization Server

OAuth 2.1 Authorization Server

The OAuth 2.1 Authorization Server features provide support for the Authorization Server role as defined in the OAuth 2.1 Authorization Framework.

The Authorization Server features provide implementations of the OAuth 2.1 and OpenID Connect 1.0 specifications and other related specifications. It provides a secure, light-weight, and customizable foundation for building OpenID Connect 1.0 Identity Providers and OAuth 2.1 Authorization Server products.

Use Cases

The following list provides some use cases for using Spring Security Authorization Server compared to using an open source or commercial OAuth2 or OpenID Connect 1.0 Provider product.

- Provides full control of configuration and customization when advanced customization scenarios are required.

Category	Feature	Related specifications

Authorization Grant	• Authorization Code
	  ◦ User Consent
	• Client Credentials
	• Refresh Token
	• Device Code
	  ◦ User Consent
	• Token Exchange
		• The OAuth 2.1 Authorization Framework (draft)
		  ◦ Authorization Code Grant
		  ◦ Client Credentials Grant
		  ◦ Refresh Token Grant
		• OpenID Connect Core 1.0 (spec)
		  ◦ Authorization Code Flow
		• OAuth 2.0 Device Authorization Grant (spec)
		  ◦ Device Flow
		• OAuth 2.0 Token Exchange (spec)
		  ◦ Token Exchange Flow

Token Formats	• Self-contained (JWT) • Reference (Opaque)	• JSON Web Token (JWT) (RFC 7519) • JSON Web Signature (JWS) (RFC 7515)
Token Types	• DPoP-bound Access Tokens	• OAuth 2.0 Demonstrating Proof of Possession (DPoP) (RFC 9449)
Client Authentication	• `client_secret_basic` • `client_secret_post` • `client_secret_jwt` • `private_key_jwt` • `tls_client_auth` • `self_signed_tls_client_auth` • `none` (public clients)	• The OAuth 2.1 Authorization Framework (Client Authentication) • JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication (RFC 7523) • OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens (RFC 8705) • Proof Key for Code Exchange by OAuth Public Clients (PKCE) (RFC 7636)

Category	Feature	Related specifications

Protocol Endpoints	• OAuth2 Authorization Endpoint
	• OAuth2 Pushed Authorization Request Endpoint
	• OAuth2 Device Authorization Endpoint
	• OAuth2 Device Verification Endpoint
	• OAuth2 Token Endpoint
	• OAuth2 Token Introspection Endpoint
	• OAuth2 Token Revocation Endpoint
	• OAuth2 Client Registration Endpoint
	• OAuth2 Authorization Server Metadata Endpoint
	• JWK Set Endpoint
	• OpenID Connect 1.0 Provider Configuration Endpoint
	• OpenID Connect 1.0 Logout Endpoint
	• OpenID Connect 1.0 UserInfo Endpoint
	• OpenID Connect 1.0 Client Registration Endpoint
		• The OAuth 2.1 Authorization Framework (draft)
		  ◦ Authorization Endpoint
		  ◦ Token Endpoint
		• OAuth 2.0 Pushed Authorization Requests (RFC 9126)
		  ◦ Pushed Authorization Request Endpoint
		• OAuth 2.0 Device Authorization Grant (RFC 8628)
		  ◦ Device Authorization Endpoint
		  ◦ Device Verification Endpoint
		• OAuth 2.0 Token Introspection (RFC 7662)
		• OAuth 2.0 Token Revocation (RFC 7009)
		• OAuth 2.0 Dynamic Client Registration Protocol (RFC 7591)
		• OAuth 2.0 Authorization Server Metadata (RFC 8414)
		• JSON Web Key (JWK) (RFC 7517)
		• OpenID Connect Discovery 1.0 (spec)
		  ◦ Provider Configuration Endpoint
		• OpenID Connect RP-Initiated Logout 1.0 (spec)
		  ◦ Logout Endpoint
		• OpenID Connect Core 1.0 (spec)
		  ◦ UserInfo Endpoint
		• OpenID Connect Dynamic Client Registration 1.0 (spec)

- Protocol Endpoints