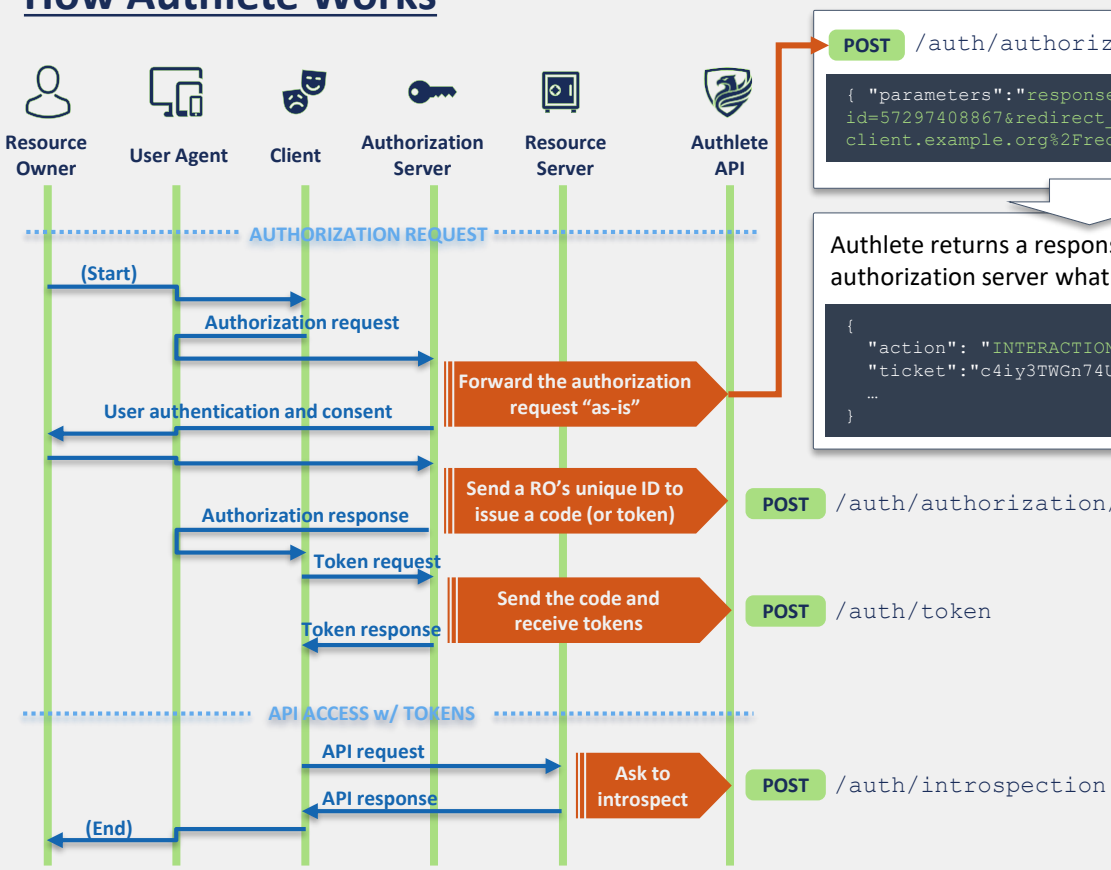
AUTHLETE

FOR DEVELOPERS

Authlete: API Authorization Engine

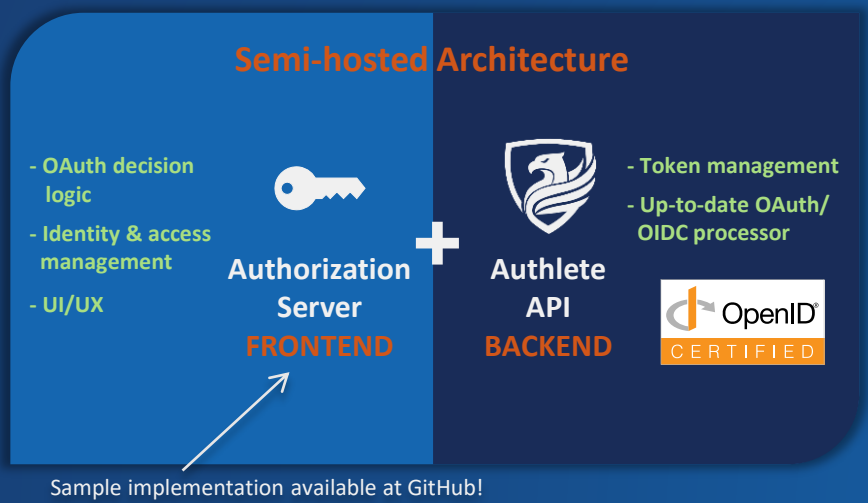
The Authlete OAuth 2.0 and OpenID Connect solution allows developers to quickly implement secure authorization servers and identity providers.

How Authlete Works



Tutorials here!

Why Authlete



The Authlete semi-hosted architecture enables you to:

- Use your favorite programming languages
- Customize UI/UX with no limit
- Bring API gateway and identity & access management solution of your choice
- Keep your users' credentials internal
- Process requests with up-to-date OAuth/OIDC specs, including FAPI, CIBA and Device Flow

Spec Sheet

AUTHLETE

Supported Endpoints	Authorization Endpoint, Token Endpoint, Revocation Endpoint, Introspection Endpoint, JWK Set Endpoint, User Info Endpoint, Backchannel Authentication Endpoint, Device Authorization Endpoint
Supported Grant Type	authorization_code, implicit, password, client_credentials, refresh_token, urn:openid:params:grant-type:ciba (CIBA), urn:ietf:params:oauth:grant-type:device_code (Device Flow)
Supported Response Types	none, code, token, id_token, code token, code id_token, id_token token, code id_token token
Supported Response Modes	query, fragment, form_post, jwt, query.jwt, fragment.jwt, form_post.jwt
Supported Client Authentication Methods	none, client_secret_basic, client_secret_post, client_secret_jwt, private_key_jwt, tls_client_auth, self_signed_tls_client_auth
Access Token Expiry	configurable per service and scope
Refresh Token Expiry	configurable per service and scope
ID Token Expiry	configurable per service
Supported Signature Algorithm	HS256, HS384, HS512, RS256, RS384, RS512, ES256, ES384, ES512, PS256, PS384, PS512
Supported Encryption Algorithm	RSA1_5, RSA_OAEP, RSA_OAEP_256, A128KW, A192KW, A256KW, DIR, ECDH_ES, ECDH_ES_A128KW, ECDH_ES_A192KW, ECDH_ES_A256KW, A128GCMKW, A192GCMKW, A256GCMKW, PBES2_HS256_A128KW, PBES2_HS384_A192KW, PBES2_HS512_A256KW
Supported Encryption Encoding Algorithm	A128CBC_HS256, A192CBC_HS384, A256CBC_HS512, A128GCM, A192GCM, A256GCM
Supported Specifications	RFC 6749: The OAuth 2.0 Authorization Framework RFC 6750: The OAuth 2.0 Authorization Framework: Bearer Token Usage RFC 7009: OAuth 2.0 Token Revocation RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants RFC 7591: OAuth 2.0 Dynamic Client Registration Protocol RFC 7592: OAuth 2.0 Dynamic Client Registration Management Protocol RFC 7636: Proof Key for Code Exchange by OAuth Public Clients RFC 7662: OAuth 2.0 Token Introspection RFC 8628: OAuth 2.0 Device Authorization Grant OAuth 2.0 Multiple Response Type Encoding Practices OAuth 2.0 Form Post Response Mode OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens OpenID Connect Core 1.0 OpenID Connect Discovery 1.0 OpenID Connect Dynamic Client Registration 1.0 OpenID Connect Client Initiated Backchannel Authentication Flow - Core 1.0 Financial-grade API - Part 1: Read-Only API Security Profile Financial-grade API - Part 2: Read and Write API Security Profile Financial-grade API: JWT Secured Authorization Response Mode for OAuth 2.0 (JARM) Financial-grade API: Client Initiated Backchannel Authentication Profile UK Open Banking Security Profile
Unique Authlete Functionality	ClientID Alias Extra Token Properties Scope Attribute Refresh Token Kept Single Access Token Per Subject Granted Scopes Management

Hosting Options	Business plan: shared managed cloud Enterprise plan: dedicated managed cloud or on-premise
Service Level Objective	99.9 – 99.99 % Availability for managed cloud (on-premise can go even higher!)
Performance	100+ transactions per second on the best effort basis for managed cloud
Support Level	Technical for Business plan / Enterprise or Premium for Enterprise plan Delivered by OAuth/OIDC spec committers Professional Service available