SCALED ACCESS

WHITEPAPER

Accelerating Secure OAuth 2.0 Compliant Advanced Authorization: Authlete & Scaled Access

Intro

Authlete & Scaled Access's cloud services enable organizations to build and operate OAuth 2.0 compliant advanced authorization servers with user-wise access control, including user-to-user, user-to-organization and user-to-application.

Authlete's authorization engine provides backend Web APIs to implement OAuth 2.0 and OpenID Connect and, together with Scaled Access, empowers people to access and share protected resources securely and autonomously.

Organizations have the ability to add relationship types as a condition to get and share access. These relationships are managed in a graph database and correspond with User-Managed Access (UMA) policy conditions.

This future-proof managed service solution is designed to scale self-serviceable, fine-grained access within any ecosystem. Their API-based setup and their commitment to open standards such as OAuth, OpenID Connect & JWT makes integration easy.

The architecture is developer friendly and enables organizations to build authorization server front ends with their favorite programming languages and frameworks.

Future Proof Setup

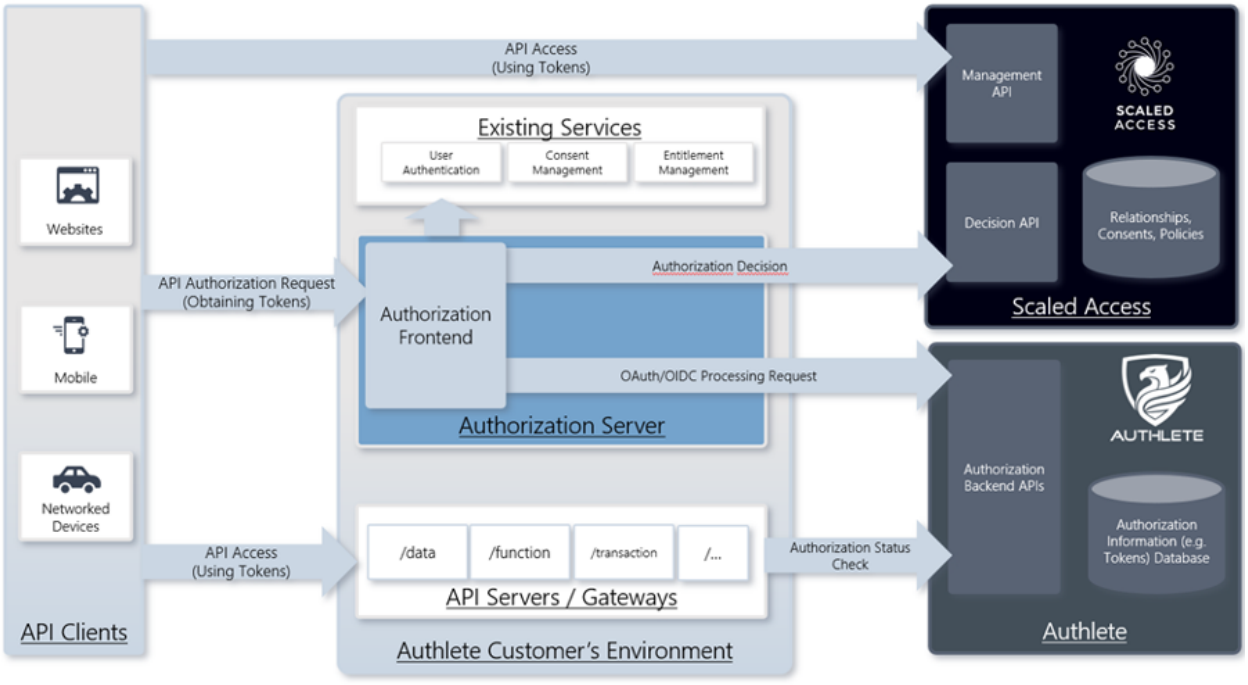
Many companies and organizations rely heavily on their Web API infrastructure to serve their core customers and open up access to protected data, content, devices or functionalities.

In order to provide Web APIs, they need to implement the OAuth 2.0 industry protocol for authorization and OpenID Connect as an identity layer on top of the OAuth 2.0 protocol. However, implementing the right specifications requires a lot of time and effort.

Authlete's backend Web APIs enable organizations to easily get the functionality of OAuth 2.0 and OpenID Connect. Authlete implements different endpoints to issue access or ID tokens, register and manage API clients, define audiences and scopes and validate access tokens.

The diagram below shows an example of an Authorization Server built in the Customer Environment:

- Authlete deals with OAuth and OIDC Processing requests and Authorization Status checks
- Scaled Access deals with Authorization Decisions based on ReBAC
- Decisions from Scaled Access are embedded in the OAuth/OIDC Processing request from the authorization server to Authlete, and to be collated with access tokens



Authlete is a backend that's offered as a service that works behind the organization web service and does not interact directly with your end-users, OAuth clients, or relying parties.

Scaled Access evaluates if authorization requests match the access policy in place.

Scaled Access offers advanced authorization capabilities, tailored to each specific organization ecosystem and needs. Its unique authorization model includes the use of relationships to map out policy permissions contained in the authorization/access token.

Utilizing relationships means that organizations can empower their teams or customers to invite the people they know or work with, to get access to the same protected resources.

The configurable access policies also enforce the different types of consent that come with ecosystem sharing (user-to-user, user-to-organization, user-to-application).

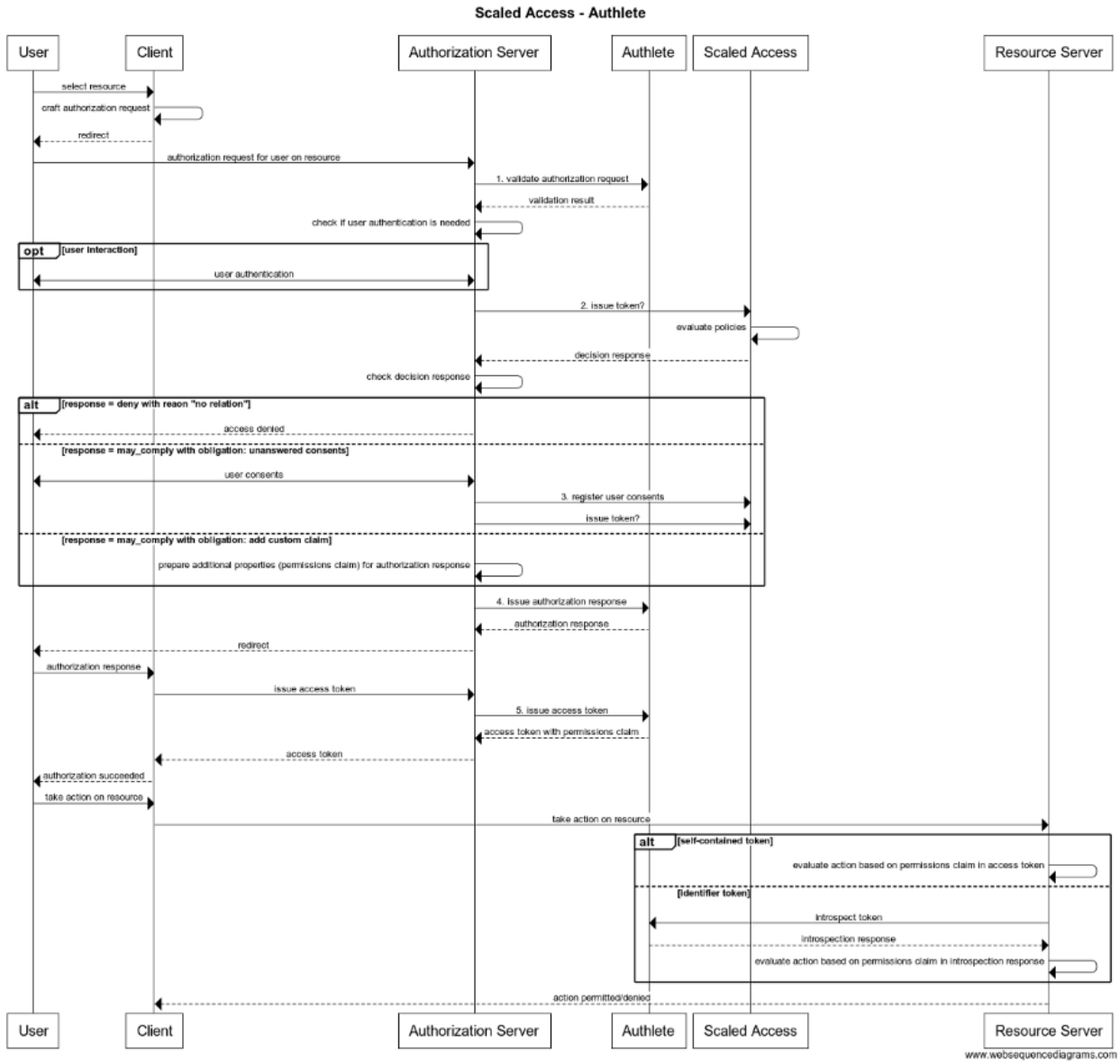
“This architecture allows you to build a solution where API Clients get smart tokens that contain scopes and custom claims in line with the business rules that take into account end-user attributes, relationships and consents. The resulting access tokens have changed from single-user ABAC to multi-user ReBAC-based authorizations.”

Authlete and Scaled Access accelerate the development of a secure OAuth/OIDC-compliant authorization server that can handle complex use cases and grant permissions based on user-to-user relationships.

Sequence Diagram

The sequence diagram on the next page shows the interactions between the different participants in the above architecture diagram.

The most important steps in the sequence diagram have been numbered and are explained below the diagram.



1. **Processing and validating the authorization request**
   A ticket parameter is used between an authorization server and the Authlete server.
   First, Authlete /auth/authorization API returns a ticket in its response to an authorization request. Then, auth/authorization/issue or auth/authorization/fail API receives the ticket and processes the authorization request to issue tokens or codes or return errors.

   https://kb.authlete.com/en/s/oauth-and-openid-connect/a/ticket-parameter-in-authorization-endpoint

2. **Evaluating the applicable policy to determine the user permissions**
   Scaled Access provides an API-based system to:

   - define and customize types of resources and relationships (Config API)
   - create and manage users, resources, and relationships (Relationship Management API)
   - take relationships into account when making access decisions (Authorization API)

   https://docs.scaledaccess.com/#relationship-based-access-control and
   https://docs.scaledaccess.com/#relationship-config-api

3. **Verifying and enforcing the required user consents**
   Scaled Access provides an API-based system to:
   - define customized consents (Config API)
   - register user consents and log each action with regard to these consents (Consent Management API)
   - take user consents into account to make access decisions.(Authorization API)

   https://docs.scaledaccess.com/#consent-enforcement

4. **Updating the tokens with scopes and custom-claims representing the authorizations**
   Authlete provides a feature that enables an authorization server to add extra properties to an access token or authorization token. The authorization server can easily share the properties with resource servers so that they can consume such information for its authorization enforcement as well as making a response. The resource server can find the values from the access token included in an API request from the client. The resource server doesn't need to communicate with the database.
   https://kb.authlete.com/en/s/oauth-and-openid-connect/a/extra-properties

5. **Issuing the tokens**
   https://docs.authlete.com/#auth-authorization-issue-api

About Authlete

Authlete provides OAuth 2.0 and OpenID Connect implementation solutions through cloud and on-premises software service integral to API (Application Programming Interface) Security. APIs reduce friction in communication and interaction between programs and help to integrate systems. Financial Institutes, Healthcare, IoT have been using APIs to provide value to customers and businesses.

Authlete is unique as the platform stores tokens “off-site”, reducing vulnerability of the main apps/servers/databases. Also, authentication and authorization is separated, meaning authorization credentials can be anonymized and are very loosely tied to identity, reducing the impact of breaches and leaks.

About Scaled Access

Scaled Access lets organizations adapt authorization to their business needs. Scaled Access deploys a unique authorization model that uses attributes, context and relationships to map out permissions.

Its cloud-based solution manages permissions to multiple systems from a single platform, streamlining the access process and reducing administrative burden. Its graph database can manage an unlimited number of users, resources and applications.

Scaled Access has a Zero trust infrastructure and automatically verifies each access request and offers CARTA-inspired access controls and visibility.

Scaled Access is already being used by 26 million consumers worldwide and is trusted by global enterprises, such as, Coca-Cola, Mars, Johnson & Johnson, Merck and Shell.