White Paper

Introduction to Authlete

June 2020

Authlete, Inc.

Preface

OAuth 2.0 and OpenID Connect are essential open standards for API access authorization. In order to implement them properly, you need to follow-up the standardization process and adopt the latest practices. It is merely possible for almost all of service providers.

Existing solutions would provide access authorization features to mitigate the difficulties. But their weaknesses in scalability, flexibility, migration process and standards compliance are another concern.

This white paper covers these topics and describes the value proposition of the new architecture enabled by Authlete's unique approach.

Contents

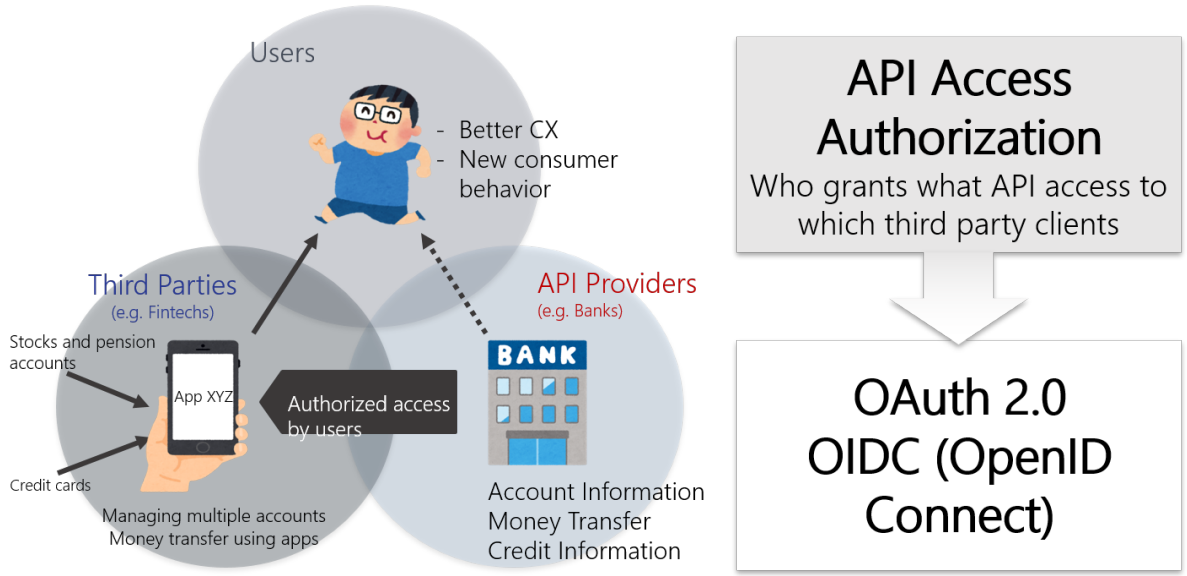
OAuth and OIDC are the Foundation for Open APIs

What is API access authorization? It is about how API providers control API access based on the following factors:

- What kind of access
- Which API clients are granted access
- Who grant access

Adequate API access authorization enables the providers to have a relationship with third parties in conformance with an end user's consent. It enhances customer experience and further brings higher usage and revenue.

OAuth 2.0 is the industry standard of API access authorization. OpenID Connect is another standard that extends OAuth 2.0 for identity information exchange.



Difficulties in Adopting OAuth/OIDC

In general, it is still difficult to implement and operate OAuth and OIDC properly.

In some aspects, this is due to complexity in API access authorization itself. Another reason why is that the standards are moving targets; a lot of new extensions and practices are being created.

It is merely possible for service providers to follow the standardization process without specialists in that domain.

The situation gets even worse once they implement API access authorization service without an appropriate understanding of the specification and operate it without knowing the best current practice. It could lead to security incidents such as illegal API access.

Victims could be not only service providers of the APIs but also end users - customers of the providers, who permitted such API access.

- Service providers can't follow the standardization process
  - A lot of new extensions and practices are being created
- Poor API access authorization could lead to security incidents
  - Customers of the providers could become victims

Source: https://tools.ietf.org/wg/oauth/, https://openid.net/wg/fapi/

Access Authorization Capabilities in Existing Solutions

It's not too much to say that developing and operating OAuth/OIDC servers by each service provider is virtually impossible without API access authorization specialists. Furthermore, such professionals are hard to be found.

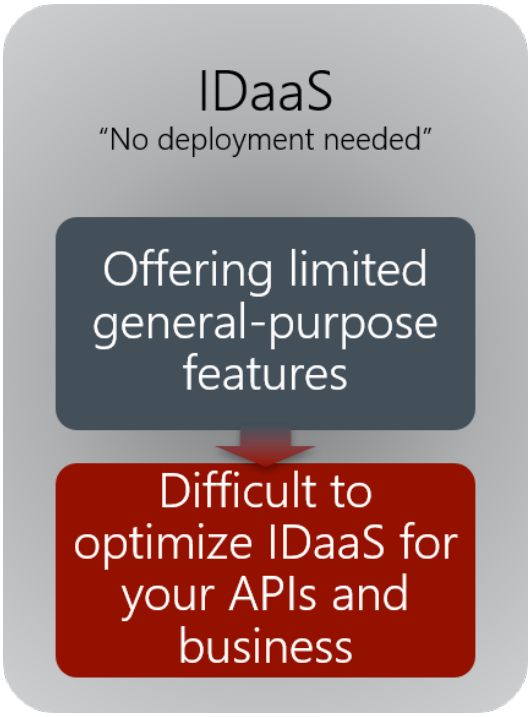
While there are a couple of solutions providing access authorization to solve the issue, each has its pros and cons. Here are examples of three solutions.

- IDaaS
- IAM software
- API gateways

IDaaS (Identity as a Service)

IDaaS is an attractive choice because it is a SaaS-type offering that could reduce deployment cost.

But their functionalities are optimized for typical use cases; it doesn't have enough flexibility to profile API authorization functions for characteristics of the service providers' APIs.



IAM (Identity and Access Management) Software

There are a lot of software vendors that provide a deployable package of IAM software onto your site and allow you to customize it.

A concern is that such IAM software has pre-built functions such as identity management, user authentication, and these are tightly integrated into a single package.

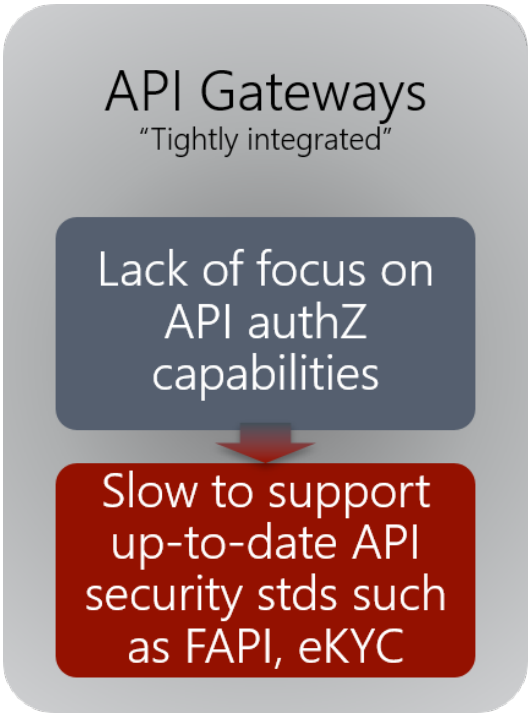
While you could fully control an API authorization system with the installed software, you have to migrate customer identity data and user authentication service from your existing infrastructure to the new IAM software system. You may spend more time and cost for the migration and replacement.

API Gateways

API gateways often have their access management functionality, which may be sufficient for some sort of APIs.

Its advantage over other approaches is that the feature is built into the API gateways. But you should consider that the access authorization function is often not the first priority in the whole features (e.g. protocol transformation, usage tracking, traffic control) of API gateways.

It may lead to lagged adoption of advanced standards such as FAPI (Financial-grade API). In the worst case scenario, service providers themselves have to understand and implement security provisions of FAPI on the deployed API gateway from scratch.



Authlete: A New Approach of Authorization Engine

What would be the best solution? We have tackled this challenge and taken a unique approach, which is different from other existing ones.

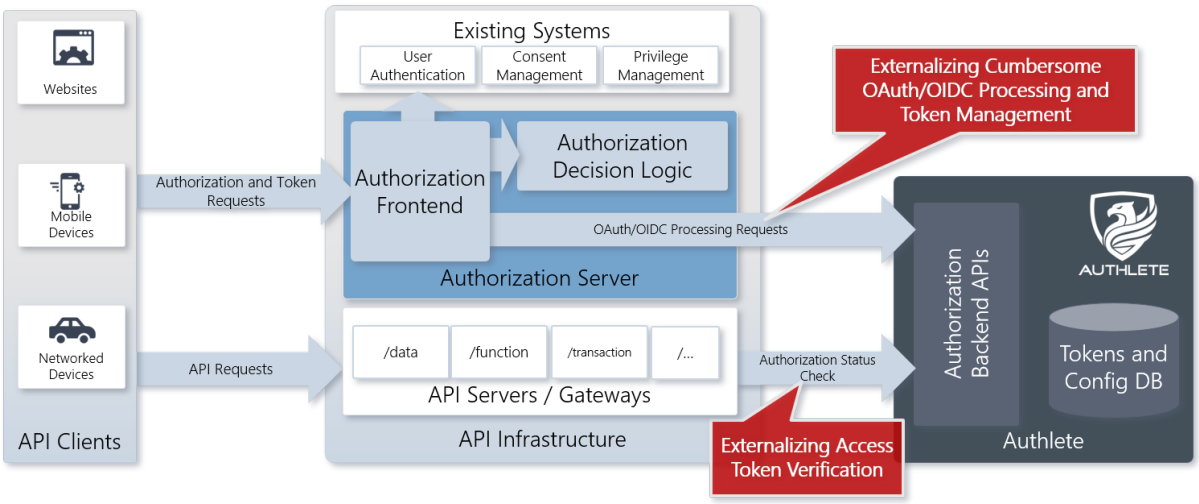
We call the approach “Semi-hosted Architecture.” It splits OAuth/OIDC server functions into two parts; You can freely implement one part while we provide another OAuth/OIDC specific part as APIs. It brings more flexibility for service providers to customize UI/UX of user registration, user authentication, user consent etc. on their business objectives, and eliminates the burden of implementation of OAuth/OIDC processing as they can be offloaded to Authlete.

All functionalities we host are available as Web APIs as described later.

One of the best value propositions of Authlete is that we have committed to standardize and implement the latest OAuth/OIDC specifications. Our customers can enable such advanced industry standards such as FAPI requiring higher security provisions aimed for APIs in financial services, “Identity Assurance” for eKYC (Electronic Know Your Customer) ahead of their competitors.

Integration with Existing Systems

The following diagram is a general integration architecture of Authlete and other components.

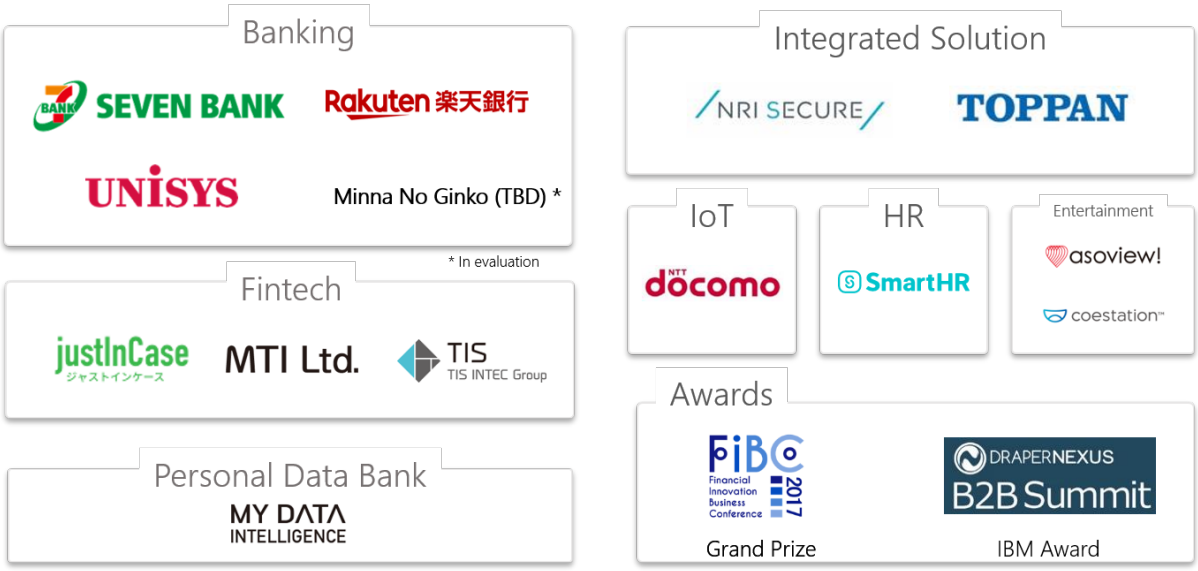


- Service providers that deploy Authlete would fully manage “API service infrastructure,” including an authorization server. The server can be freely implemented by the providers themselves in accordance with their business and technical requirements, from user authentication and consent to integration with existing systems.
- Authlete manages all of OAuth/OIDC processing operations so that the providers can offload them onto us. Authlete accepts requests from the providers through Web APIs, and then handle authorization flows as well as issuing and management of API access information called tokens.
- When API clients make requests using tokens, your API servers/gateways don’t have to verify them; Authlete does token introspection on their behalf.

This architecture enables service providers to externalize complicated implementations and operations in terms of OAuth/OIDC while gaining governance and control their API infrastructure.

A Broad Range of Use Cases

Authlete helps a wide range of industries, from high-security use cases in banking, fintechs and personal data services area, to customer experience-oriented businesses such as entertainments.



A Case Study: SmartHR

SmartHR, one of our customers in SaaS space, have implemented OAuth in their HRtech offerings. We are delighted that they value Authlete especially in terms of a rich set of Web APIs, high maintenance ability, and continuous adoption of the latest standards.

About Authlete

Authlete, Inc is based in Tokyo and London and comprised of a team of experts who have a wealth of experience specialized in authorization and identity management and are actively involved in providing specifications of open standards serving a variety of industries, such as UK Open Banking.

For more information, please visit www.authlete.com.