

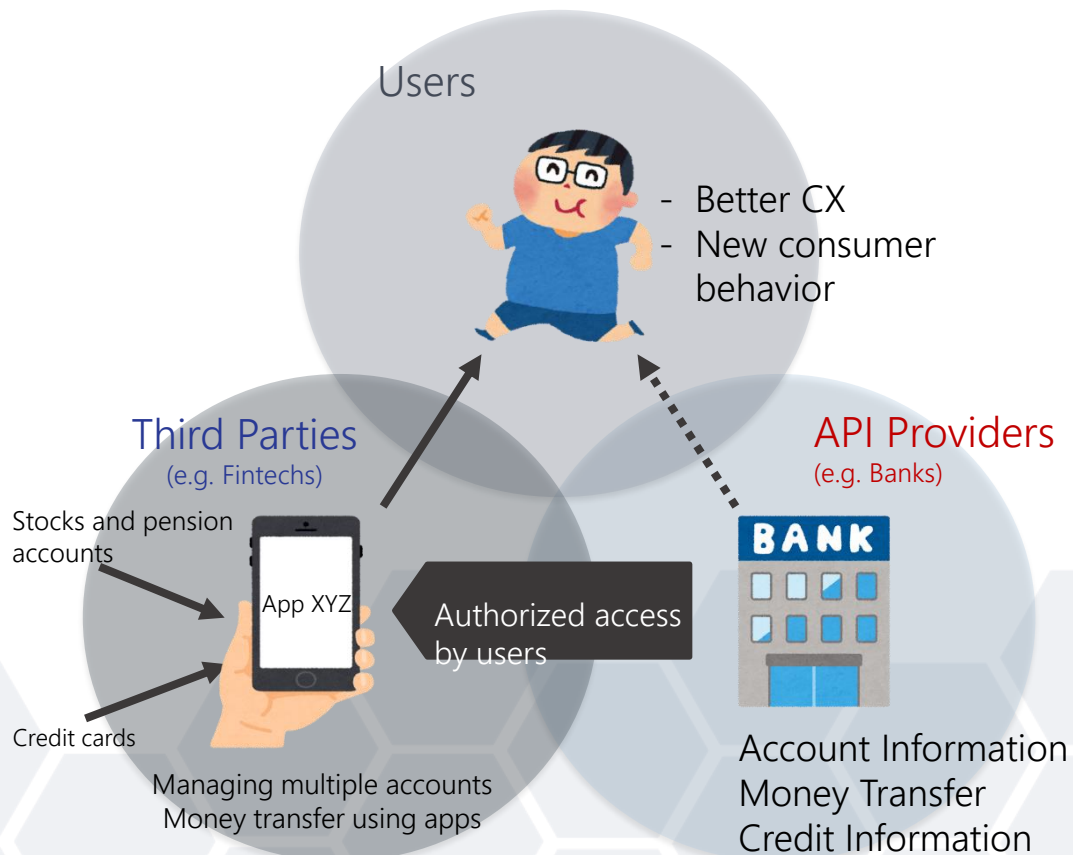
# Introduction to "Authlete"

Your OAuth/OIDC Servers. Simpler Yet More Secure.

Authlete, Inc.



# OAuth and OIDC are the Foundation for Open APIs



## API Access Authorization

Who grants what API access to which third party clients

OAuth 2.0  
OIDC (OpenID Connect)

# Difficulties in Adopting OAuth/OIDC Standards

- 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

The image displays two web browser screenshots. The left screenshot shows the 'OAuth Status Pages' website, which lists various draft documents under categories like 'Working Group Documents', 'Recently Expired', 'IESG Processing', 'RFC-Editor's Queue', and 'Published'. The right screenshot shows the 'OpenID' website, specifically the 'What is the Financial-grade API (FAPI) WG?' page. This page provides an overview of the FAPI WG's goals, lists of specifications, and working group chairs.

**OAuth Status Pages**  
Web Authorization Protocol (Active WG)

**Working Group Documents:**

Draft name	Rev.	Dated	Status	Comments, Issues
Active:				
draft-ietf-oauth-access-token-1st	-03	2019-12-16	Active	
draft-ietf-oauth-browser-based-apps	-04	2019-09-22	Active	
draft-ietf-oauth-incremental-auth	-03	2019-11-04	Active	
draft-ietf-oauth-pint	-01	2020-02-19	Active	
draft-ietf-oauth-rar	-01	2020-02-19	Active	
draft-ietf-oauth-security-topics	-14	2020-02-19	Active	
Recently Expired:				
draft-ietf-oauth-prop-key-distribution	-07	2019-03-27	Expired	
draft-ietf-oauth-ecp-1st	-04	2019-08-01	Expired	
IESG Processing:				
draft-ietf-oauth-1st-introspection-response	-20			
RFC-Editor's Queue:				
draft-ietf-oauth-1st	-17			
draft-ietf-oauth-indicator	-08			
Published:				
Draft name				
draft-ietf-oauth-1st-values	-08			
draft-ietf-oauth-1st-assertions	-18			
draft-ietf-oauth-1st-device-flow	-13			
draft-ietf-oauth-1st-discovery	-19			
draft-ietf-oauth-1st-dyn-reg-management	-15			
draft-ietf-oauth-1st-dyn-reg	-30			
draft-ietf-oauth-1st-introspection	-11			
draft-ietf-oauth-1st-jwt-bearer-token	-32			
draft-ietf-oauth-1st-jwt	-07			
draft-ietf-oauth-1st-jwt-bearer	-12			
draft-ietf-oauth-1st-native-apps	-12			
draft-ietf-oauth-1st-proof-of-possession	-11			
draft-ietf-oauth-1st-revocation	-11			
draft-ietf-oauth-1st-2-bearer	-23			
draft-ietf-oauth-1st-pop	-15			
draft-ietf-oauth-1st-token-exchange	-19			
draft-ietf-oauth-1st-sub-si	-06			
draft-ietf-oauth-1st-v2-bearer	-23			
draft-ietf-oauth-1st-v2-threatmodel	-08			
draft-ietf-oauth-1st-v2	-31			
Expired:				
draft-ietf-oauth-1st-authentication	-01			
draft-ietf-oauth-1st-business-endpoints	-00			

**OpenID**  
About | Charter | Status | Repository

## What is the Financial-grade API (FAPI) WG?

**Overview**

In many cases, Fintech services such as aggregation services use screen scraping and stores user passwords. This model is both brittle and insecure. To cope with the brittleness, it should utilize an API model with structured data and to cope with insecurity, it should utilize a token model such as OAuth [RFC6749, RFC6750].

This working group aims to rectify the situation by developing a REST/JSON model protected by OAuth. Specifically, the FAPI WG aims to provide JSON data schemas, security and privacy recommendations and protocols to:

- enable applications to utilize the data stored in the financial account,
- enable applications to interact with the financial account, and
- enable users to control the security and privacy settings.

Both commercial and investment banking account as well as insurance, and credit card accounts are to be considered.

**Working Group Chairs**

- Nat Sakimura (Nomura Research Institute), Anoop Saxena (JPM), Anthony Nadalin (Microsoft), Dave Tonge (Moneyhub)

The chairs can be reached at [openid-spaces-fapi-owner@lists.openid.net](mailto:openid-spaces-fapi-owner@lists.openid.net).

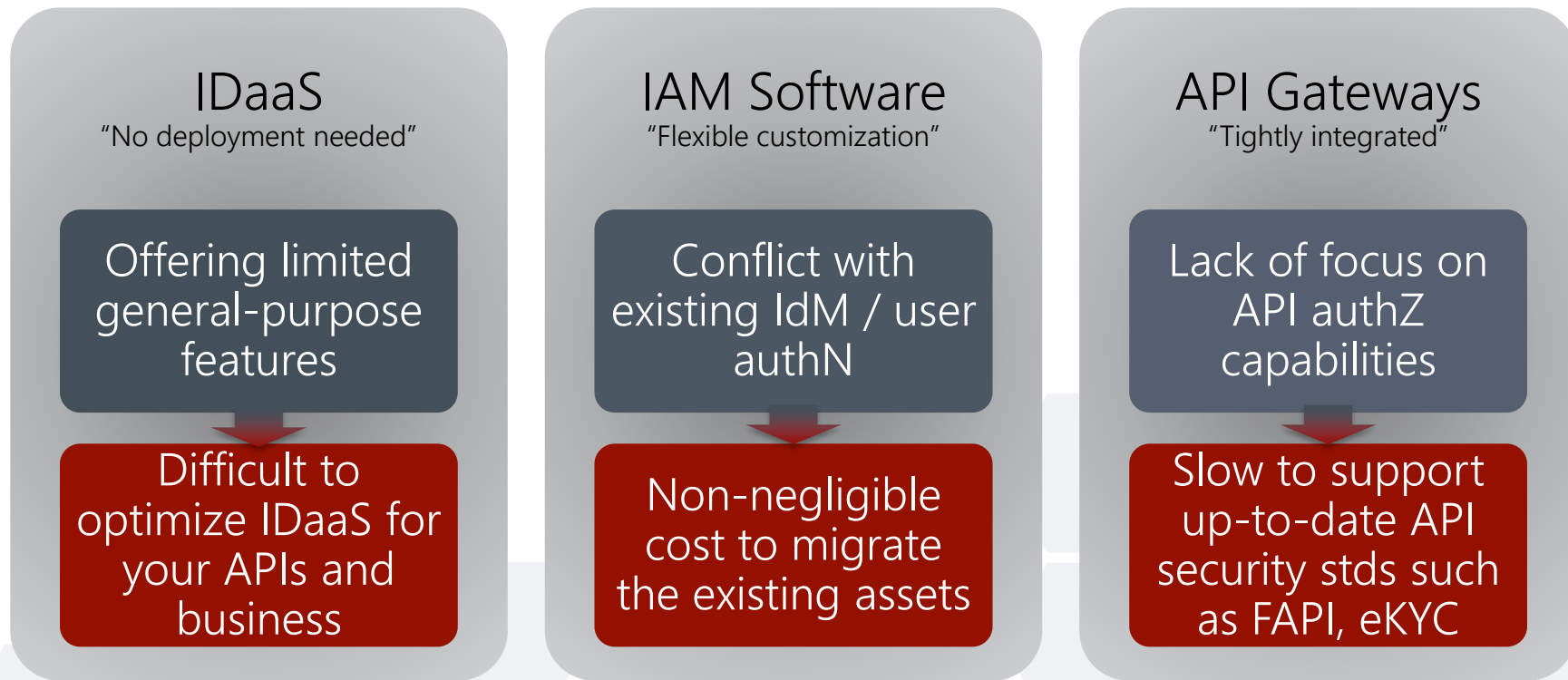
## List of Specifications

- Financial-grade API -- Part 1: Read Only API Security Profile (Implementer's Draft).
- Financial-grade API -- Part 2: Read & Write API Security Profile (Implementer's Draft).
- Financial-grade API -- JWT Secured Authorization Response Mode for OAuth 2.0 (JARM) (Working Draft).
- Financial-grade API -- CIBA Profile (Working Draft).

Followings are skeletons of the future works. The structure may well be changed.

- Financial-grade API -- Open Data API (Working Draft).
- Financial-grade API -- Read Only API (Working Draft).
- Financial-grade API -- Read & Write API (Working Draft).

# Problems in Traditional API Authorization Approaches



# Authlete: A New Approach of "API Authorization Engine"



**AUTHLETE**

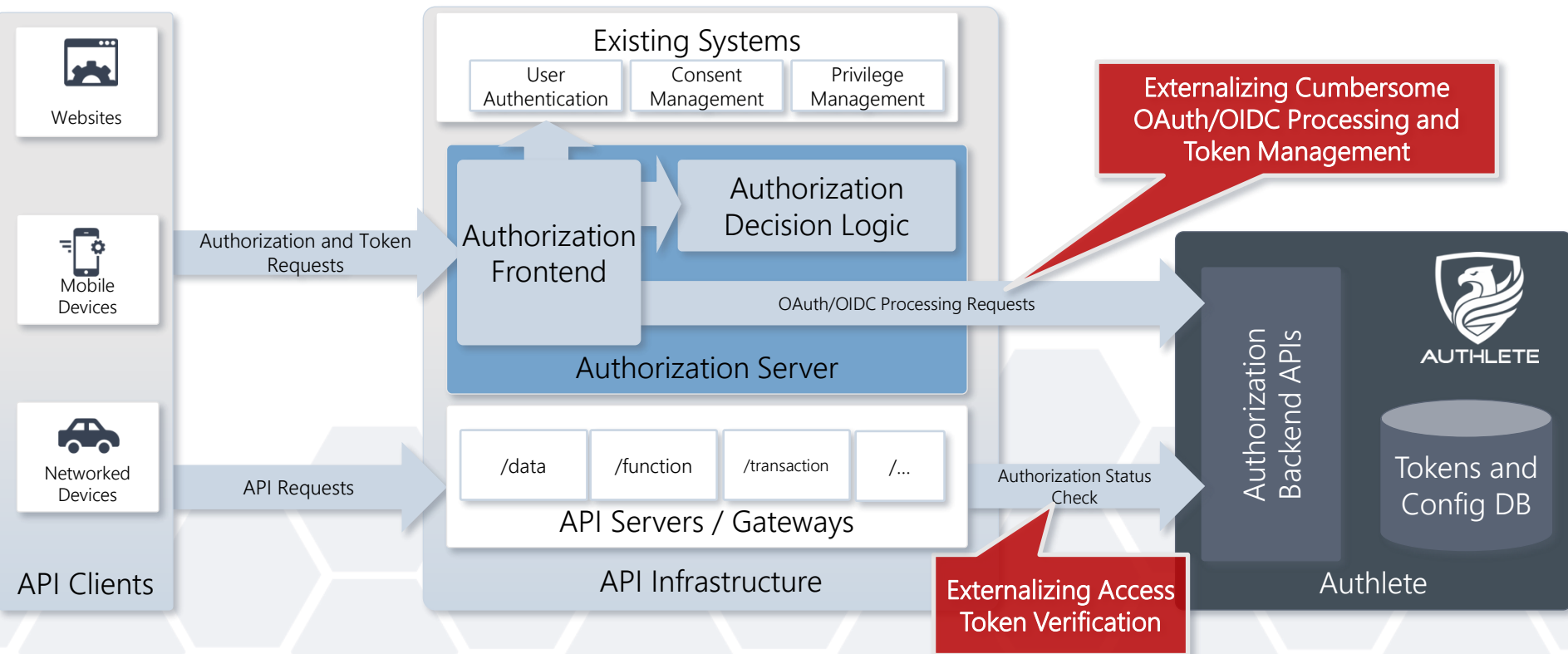
"Semi-hosted" Architecture

Providing All Features as APIs

The Leader in Supporting the Latest OAuth/OIDC Standards

# Authlete Fits in Any Form of Existing Systems

Exposing Web APIs for OAuth/OIDC Processing and Token Management



# A Broad Range of Use Cases

From Banks to Entertainments

## Banking



**SEVEN BANK**

**Rakuten 楽天銀行**

**UNISYS**

Minna No Ginko (TBD) \*

\* In evaluation

## Fintech

**justInCase**  
ジャストインケース

**MTI Ltd.**

 **TIS**  
TIS INTEC Group

## Personal Data Bank

**MY DATA**  
INTELLIGENCE

## Integrated Solution

 **NRI SECURE**

**TOPPAN**

## IoT

**NTT docomo**

## HR

 **SmartHR**

## Entertainment

 **asoview!**

 **coestation™**

## Awards

**FiBC**  
Financial  
Innovation  
Business  
Conference  
2017

Grand Prize

 **DRAPER NEXUS**  
**B2B Summit**

IBM Award

# SmartHR

One of the Largest HR Management SaaS in Japan Has Been Utilizing Authlete For Years

## Authlete in SmartHR



“Quite a rich set of Web APIs”



“High maintenance ability for anyone from anywhere”



“Continuous adoption of the latest standards is trustworthy”



# Try Authlete for Free at [www.authlete.com](https://www.authlete.com)



The screenshot shows the Authlete website with a dark navigation bar. The main heading reads "Your OAuth/OIDC Servers. Simpler Yet More Secure With Authlete." Below this is a diagram illustrating the system architecture. The diagram consists of three main components: "API Clients", "Your API Stack", and "Authlete". "API Clients" includes "Metadata Discovery", "Authorization and Token Requests", and "API Requests with Tokens". "Your API Stack" includes "Identity and Authentication", "OAuth/OIDC Server Frontend", and "API Servers / Gateways". "Authlete" includes "OAuth/OIDC Backend APIs", "OAuth/OIDC Protocol Operations", and "Tokens and Metadata Management". Arrows show the flow of requests from API Clients through the API Stack to Authlete. A red arrow points to the "FREE TRIAL" button in the top right corner of the navigation bar.

**AUTHLETE** Customers Developers Pricing Contact Login **FREE TRIAL**

Your OAuth/OIDC Servers. Simpler Yet More Secure With Authlete.

**API Clients**

- Metadata Discovery
- Authorization and Token Requests
- API Requests with Tokens

**Your API Stack**

- Identity and Authentication
- OAuth/OIDC Server Frontend
- API Servers / Gateways

**Authlete**

- OAuth/OIDC Backend APIs
- OAuth/OIDC Protocol Operations
- Tokens and Metadata Management

**GETTING STARTED**

# Thank You

[www.authlete.com](http://www.authlete.com)

