KuppingerCole Report

EXECUTIVE VIEW

By Martin Kuppinger

December 14, 2021

Authlete API Authorization

Authlete is a set of APIs for service providers to implement the standard protocols OAuth and OIDC (OpenID Connect). It enables developers of digital services to offload protocol operations and access token lifecycle management to the backend service and thus simplifies development and operations of modern digital services that require secure API-based communication, authentication, and authorization. Authlete integrates well with all common programming frameworks, and can be deployed from the cloud or on-premises.

By **Martin Kuppinger**
mk@kuppingercole.com

Content

1 Introduction

Identity and Access Management (IAM) is a foundational element of cybersecurity today.

As a set of technologies, IAM encompasses user and entitlement provisioning, identity repositories, authentication mechanisms, authorization systems, web access management (WAM), federation and Single Sign-On (SSO), identity governance, access reconciliation, risk management, and many interfaces to other security systems.

Commonly, IAM is split into three major parts:

- Identity Management: The management of identity lifecycles and their governance. This is commonly referred to as Identity Provisioning (Lifecycle Management) and Access Governance, or as IGA (Identity Governance and Administration),
- Access Management: Enabling access of users, i.e., supporting authentication, identity federation, and authorization.
- Privileged Access Management (PAM): These technologies focus on highly privileged users and the specific requirememts around these users, plus shared accounts. Capabilities include management of passwords for shared accounts and of privileged user sessions.

Many of the components of IAM have become standardized and even commoditized. To interoperate with other solutions and be successful in the marketplace, IAM products generally support the following standards:

- Provisioning: SCIM
- User identity storage: LDAP
- Authentication: Kerberos, RADIUS, PKI/x.509 including SmartCards, FIDO U2F/UAF/2.0, W3C WebAuthn, and more
- Federation: OAuth, OpenID, OpenID Connect (OIDC), and SAML
- Authorization: JSON, JWT, UMA, and XACML, with OAuth and OIDC also serving authorization use cases

Access Management, also referred to as Web Access Management & Identity Federation, as one of the major disciplines is focused on providing access for users to services. They can deliver a SSO (Single Sign-

On) experience to users, by authenticating the users on behalf of the target applications.

Integration can work either via standards for identity federation or -- for legacy web applications that do not support modern identity federation standards -- with methods such as password injection and providing authentication information as part of modified https headers. Authentication should integrate with the authentication standards listed above.

However, there also is increasing demand for providing federation and authorization services to digital services that are custom-built, with tight integration into these services. Again, this is about standards support and platforms that enable efficient delivery of these capabilities to developers, at the API level. This is essential when new digital services are created, where the client apps utilize APIs to connect to API providers, which again might utilize backend services. Common scenarios are in the Finance industry, e.g., around Open Banking and standards such as PSD2 (EU Payment Services Directive). The challenge here is that apps of, e.g., FinTechs, might require also access to backend services of other providers such as banks.

Managing access in such complex environments benefits from specialized solutions that can handle API access and authorization in an efficient manner. A provider of such a specialized solution is Authlete.

2 Product Description

Authlete is a specialized provider of an API authorization solution for the OAuth and OIDC standards. Their sole focus is on API authorization in complex, multi-party environments such as the above-described Finance industry scenarios. However, such scenarios are not limited to a single industry, but arise everywhere where new digital services involving multiple parties -- or internal services -- are involved. The complex ecosystems around connected vehicles, eGovernment use cases, or collaboration in the Pharma industry are some samples where use cases involving multiple API clients (e.g., apps and other frontends, but also services for service-to-service communication), API providers of one or multiple organizations, and backend providers of services are involved.

Authorization of API access is about making the decision about whether an API client gains access to API providers. Authlete, as mentioned, focuses on the two main, modern standards OAuth and OIDC, which are the de-facto industry standard. Unfortunately, it is not just about two simple standards, but a whole series of standards that form what is commonly referred to as OAuth/OIDC. Implementing these capabilities in applications thus is challenging to developers. Authlete delivers a service that simplifies that complexity by off-loading OAuth 2.0 and OpenID Connect protocol operations as well as the related lifecycle management of access tokens to their dedicated service. Thus, developers and the organizations can focus on the functional aspects of OAuth 2.0 and OIDC.

Authlete provides two components. One is a freely implementable and deployable OAuth/OIDC server, with reference implementations and libraries available in a variety of programming languages, including

- Java
- C#
- PHP
- Python
- Ruby
- Go
- Deno

These then connect to the Authlete service, which is available both as cloud service or as on-premises implementation. The OAuth/OIDC server and the Authlete service again communicate via APIs. This also adds the opportunity to interface to, e.g., API Gateways that might be already in place or that are used as one of the components of the infrastructure. API Gateways can either offload the whole OAuth/OIDC capabilities to Authlete or just consume enhanced services from Authlete, using the APIs provided by

Authlete.

An advantage of the approach chosen by Authlete, with segregating the OAuth/OIDC server and the Authlete backend service for managing the access token lifecycle and the OAuth/OIDC protocol operations, is that the communication between the OAuth/OIDC and the IAM infrastructure remains at the customer. Only the access tokens issued are then managed by Authlete. However, due to that approach, there is no need for Authlete for integrating, e.g., with directory services and other IAM components. This is all done at the OAuth/OIDC server, that commonly is part of a digital service or a set of digital services. The server, provided - as mentioned - in a way that can be flexibly integrated with the common development approaches, can be designed and configured highly flexible. The UX design, the flows such as for authentication and selecting the scopes, and other components can be configured in a highly flexible manner.

The various Authlete services can be managed via its management APIs and from a central console. The "Service Owner" console is targeted at the service owners utilizing the Authlete-provided OAuth/OIDC servers and the Authlete backend services. Additionally, there is also a developer console for the ones developing the API clients, e.g., the consumer apps.

As mentioned, the entire complexity of the OAuth/OIDC protocols is offloaded to the Authlete backend services. Developers can focus on gathering parameters that then are provided to the Authlete service in the backend, which then cares for all the details.

3 Strengths and Challenges

Authlete is a specialized solution for API-based communication utilizing the standard protocols OAuth and OpenID Connect. Due to the fact, that these protocols are the de-facto standard for authentication and authorization of API-based access, the protocols form the backbone of many of today's modern digital services. Authlete helps developers of such digital services by reducing the complexity in development and thus increasing their time-to-value. This is achieved by offloading the specifics and details of protocol handling and access token lifecycle management to the Authlete backend service.

Integration with new services, but also existing API gateways, is efficient. Authlete provides the OAuth/OIDC server for today's common development frameworks in a ready-to-use fashion. The integration to existing environments, such as the IAM environments, is solved in a well-thought-out manner.

Authlete also can serve global customers with locations in Tokyo, Dubai, and London, and a group of global experts that can guide the customers. For developers of modern digital services across all industries, Authlete offers an interesting solution for reducing complexity, helping developers to focus on business functions, and thus delivering digital services faster and with proven capabilities for supporting the OAuth and OIDC standards. It is very worth for development teams to evaluate the benefit Authlete brings to them.

Strengths

- Comprehensive support for OAuth and OIDC, including all specifics and sub-protocols of these standards
- Flexible deployment either as a service from the cloud or on-premises
- Flexible integration into digital services based on broad support for programming languages
- No direct integration of Authlete backend services to IAM infrastructure of customers required
- Shields specifics of OAuth and OIDC from developers, Simplifying development and increasing time-to-value
- Proven ability to deliver in critical use cases, e.g., of the Finance industry
- Team of seasoned experts in OAuth and OIDC to support the customers

Challenges

- Growing but still limited partner network, no location in the U.S./North America yet
- Very focused solution, targeted at developers, not a full-featured authentication and authorization service
- Still a relatively small vendor, but with proven track record

4 Related Research

Advisory Note: Identity Authentication Standards

Advisory Note: The Role of APIs for Business

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.