KuppingerCole Report

WHITEPAPER

By Martin Kuppinger

April 14, 2022

How to Do Identity Right When Developing Digital Services

In the digital age, digital experience heavily impacts the success of businesses. A main element of digital experience is the registration, authentication and authorization flow. Instead of developing this per service, organizations are well-advised to rely on standards and services provided via APIs. This also helps in reducing the complexity in implementing standards support, such as for OAuth and OpenID Connect (OIDC). Authlete provides a platform that supports simplified integration of OAuth and OIDC capabilities as well as Financial-grade API (FAPI) support into digital services, while shielding the complexity of the protocols by handling these in a backend service.

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

Content

1 Executive Summary 3

2 Key Findings 4

3 The impact of Digital Identities & CIAM for success in the Digital Age 5

4 The need for services: Simplifying identity for developers & admins 7

5 Making it work: How to integrate with your ecosystem 9

6 The Authlete approach on offloading authentication workload 11

7 Recommendations 14

8 Related Research 16

Content of Figures 17

Copyright 18

Commissioned by Authlete

1 Executive Summary

Delivering digital services fast and in the right way decides about the rise and fall of organizations in the digital age. Success is based on many factors, from the business model to delivery at time and cost, to the digital experience and the attack resilience and trustworthiness of digital services.

Identity, and in particular the onboarding journey and recurring authentication and authorization, play a vital role in a successful digital journey. Authentication and authorization are a major element of both digital experience and security. With authentication and authorization being at the forefront of every contact with the consumer, customer, or citizen, it must be seamless. On the other hand, authentication and authorization also impact the level of assurance and thus the level of security of digital services.

A challenge that arises in many organizations is that digital services, such as banking apps or other complex applications with a frontend app and backend services, or partners' customer touchpoints that leverage APIs of the services, require a close integration of authentication and authorization capabilities. Many of the common IAM (Identity and Access Management) and CIAM (Consumer IAM) standard solutions don't deliver the level of integration that is required. On the other hand, building on authentication and authorization backend services for the common protocols, specifically OAuth and OpenID Connect (OIDC) is challenging and error prone. The main reason is that it is not just about a simple protocol, but that such protocols consist of a huge rain of specifications and thus require complex protocol and token handling.

Speed, reliability, and security in delivering digital services are essential, but difficult to achieve in times of skill gaps in IT, and when building complex solutions. Organizations thus are well-advised in building on services that help in offloading complexity in development and operations.

Authlete provides a solution that helps in simplifying the usage of OAuth and OIDC in digital services, by providing an OAuth/OIDC server that can be integrated into the digital services, and backend services for handling the complexity of the protocols and the tokens used by these protocols.

2 Key Findings

- Identity and security are key to success when delivering digital services, serving both digital experience and the security and trustworthiness of these services.
- Efficient delivery of digital services requires to building on services at all levels, from development resources to operations, and to technical services that are provided via standardized APIs.
- Abstracting identity and security services such as user authentication and API authorization ensures that all digital services provide a unified digital experience in that field, and that all build on the same tested, secure, and well-managed platform.
- Standard IAM and CIAM solutions might fail in the scalability and level of integration required when building digital services, specifically in complex and regulated use cases such as in the Financial Services industry, or other use cases where consistent customer experience between business and identity services is the top priority.
- Externalizing these services and the complex aspects of protocols such as token handling and dealing with the variety of protocol specifics while ensuring freedom of development and deployment of the digital services can improve both the time-to-value in delivering digital services, and the operations of these services.

3 The impact of Digital Identities & CIAM for success in the Digital Age

Identity and Security are a central element in delivering reliable, secure, and convenient digital services with a good user experience. For success in the digital journey, organizations must think beyond the business-focused capabilities of digital services and foster interaction and integration between the business, the developers, the operations teams, and the identity and security teams.

We are in the Digital Age. Interaction with consumers, customers, and citizens, but also with business partners, increasingly happens via digital channels. More and more business is done with digital services, instead of physical goods. With many physical goods becoming connected, there also is an increase in hybrid business models, where digital services deliver significantly or even primarily to the revenue stream.

Delivering digital services is not just a matter of creating nicely looking web frontends and mobile apps, but also about availability, security, and the customer journey of the user in its digital identity.

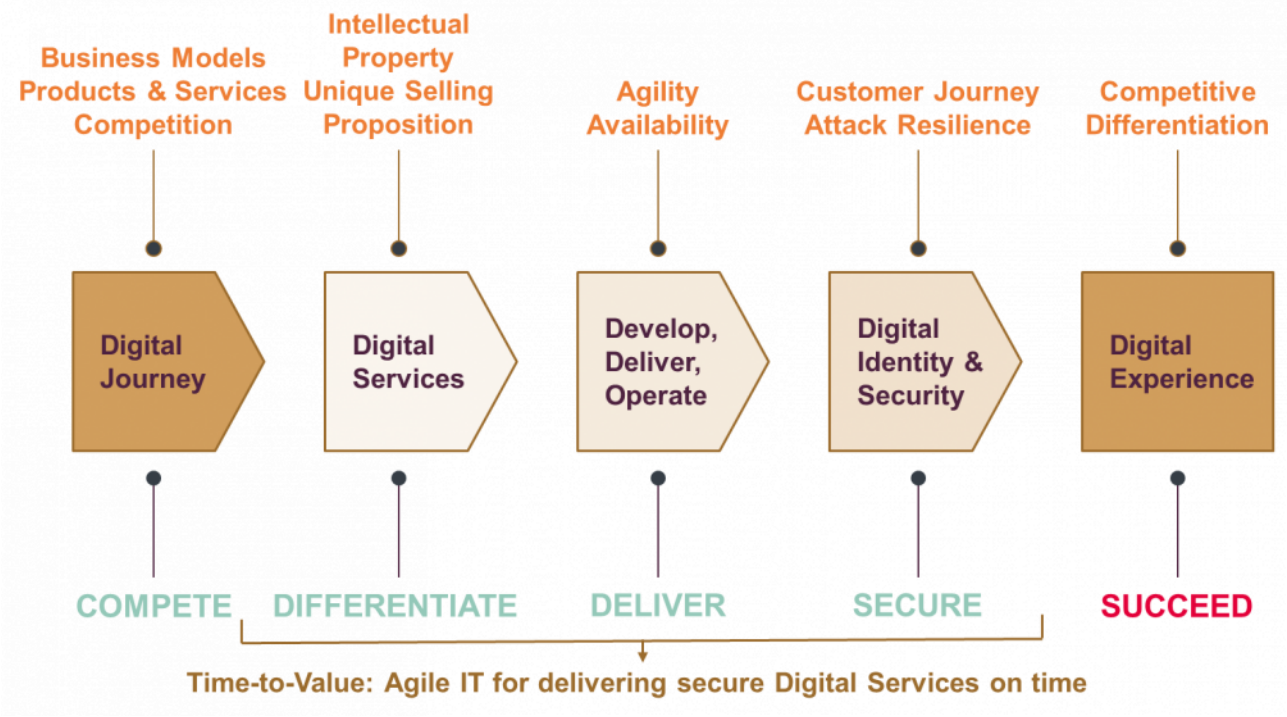

Figure 1: Digital identities and IAM are a foundation for successfully delivering digital services.

While the digital journey starts with evolving or creating new business models for a rapidly changing competitive landscape, the foundation for success is built by the right approach for developing and securing

the digital services, and for enabling a modern, convenient customer journey as part of the overall digital experience.

Organizations must ensure that business, development, operations, identity, and security teams collaborate in delivering digital services on time, with a leading-edge digital experience, and secure. This is a priority task for every CIO.

Development, delivery, security, and identity management are neatly intertwined. The integration of development and delivery has already become the new normal in DevOps (Development & Operations). Securing DevOps environments, from code to runtime, is a rapidly emerging field within cybersecurity.

Identity management relates to both security and the Digital Experience. Identity management is about providing security in authentication and access. Identity management is also about providing an excellent digital experience in onboarding users, authenticating recurring users, authorizing access to services and providing self-services management to them.

Organizations need to take an approach that integrates all efforts, from the business model to delivery and security, to succeed in the digital business. This puts DevOps, security, and identity management at the centre of successful digital journeys.

4 The need for services: Simplifying identity for developers & admins

Rapid delivery of digital services requires a well thought out use of services. Services can provide a range of benefits such as improved time-for-value, a consistent digital experience across apps, but also fewer bugs and higher security.

The challenge that arises is that neither security nor identity management is the home turf of most developers. There are development teams, there are cybersecurity professionals, and there are identity management professionals. Specialization is needed due to the complexity. To make matters worse, the skills gap in IT makes it difficult for organizations to find the talent needed. This situation inevitably leads to services, at various levels:

- People: Outsourcing development services, relying on MSSPs (Managed Security Service Providers) in cybersecurity, or using system integrators for operating some of the IAM (Identity and Access Management) services has already become the norm.
- Technology: In some areas, building on external services such as MDR (Managed Detection & Response) also is a common approach.
- Interfaces: Close to development is the provision of APIs (Application Programming Interfaces) to the developers, based on backend services. The advantage of delivering such an API layer is that development and the management and operations of cybersecurity and identity become segregated, allowing to run and optimize the underlying infrastructure without requiring code changes.

In times of major skill gaps in IT, utilizing services is essential for providing the time-to-value required in delivering digital services, and the efficiency in operations.

While there are proven approaches in place at all levels, all these approaches aren't "no brainers". They need to be well thought out to work as expected. On the other hand, there are immediate benefits provided by a well-planned utilization of services at all levels. Looking at the interface level and the utilization of APIs, these include

- Improved time-to-value: If developers can consume services, instead of creating or recreating, e.g., security or identity services, again and again, the workload is reduced, and developers can focus on the digital services, instead of foundational technologies. This results in a better time-to-value in

delivering digital services.

- Unification of digital experience: Specifically for identity, utilizing APIs helps in unifying the customer experience, by delivering a consistent user experience for onboarding, authentication, authorization, and other capabilities, in an integrated manner as such identity service is obviously a part of whole digital experience. Too many organizations today don't deliver this consistency, but require customers, consumers, or citizens to work with multiple apps and, sometimes, even multiple different identities.
- Defined interaction: APIs are not only technical interfaces. They also provide segregation, but also an interface between developers and the experts on the other side, allowing to clearly define responsibilities.
- Reduction of errors: By relying on a standardized backend, the risk of creating bugs in coding these capabilities, again and again, is reduced. If there is one service delivering a capability instead of many such services, there will be fewer errors.
- Simplified patching: In parallel, patching is simplified, because there is one known place in the backend for patching, instead of multiple places where changes in custom code are required.

An additional aspect is that the specific expertise required in many areas can be consolidated and focused. Some of the standards are highly complex, because it is not just about a set of standards such as OAuth and OIDC (OpenID Connect), but frequently dozens of detailed specifications around. Thus, as in many other areas, multiple layers of services might be needed for a good solution, from experts supporting in the implementation to solutions offloading the complexity, and APIs that then can be consumed by the developers.

5 Making it work: How to integrate with your ecosystem

Solutions must integrate well with the existing ecosystem. On the other hand, organizations must carefully evaluate whether existing solutions serve the requirements in building digital services, e.g., for security and scalability requirements.

When looking at the IAM aspect and, therein, specifically the authentication and authorization to modern digital services, a challenge is that this rarely happens in any type of greenfield approach. There are existing solutions. There are specific enhancements to protocols and related protocols such as, in finance, the FAPI (Financial-grade API) for high-stakes APIs such as open banking, there might be existing security solutions such as API gateways, and more. It frequently is not just about an API-based authentication via OAuth/OIDC to an OAuth/OIDC server for, subsequently, accessing the resource server. Most commonly, there are various other components involved.

Many organizations underestimate the complexity of standard protocols and their implementation. Services can help in delivering these capabilities on time, and securely.

Solutions that provide specialized API services for digital services must, on the one hand, be evaluated against what is already available, and, on the other hand, be able to integrate with existing services.

IAM

Most organizations already have solutions for IAM deployed. These solutions handle many aspects of user management, provisioning of accounts to target systems, access governance, and also authentication and access management at runtime. However, being mostly targeted at the workforce, these solutions are not targeted at digital services for customers, consumers, or citizens, which require a fundamentally different level of scalability.

Developing digital services frequently requires a close integration of OAuth/OIDC server capabilities with the digital service, and a high degree of scalability. Depending on the use case, segregation of identities also can be a requirement.

Integration with IAM solutions to, e.g., access directories or forward authentication in the respective use cases is a requirement, but IAM solutions come to their limits when it is about neat integration with digital services and delivering a high degree of scalability.

CIAM

Over the past years, CIAM (Consumer IAM) solutions have evolved that are targeted at delivering customer authentication and integration to marketing automation solutions at scale. While these deliver the scalability,

however, the integration into digital services as well as the integration of digital services with specific backends such as legacy solutions in the Finance industry also might be a limitation, in contrast to specialized authentication services.

External Identity Providers

On the other hand, we see a massive uptake in external identity providers that deliver trusted, verified identities. This includes specialized solutions for identity proofing and authentication, but also emerging global networks such as GAIN (Global Assured Identity Network). GAIN is built on the financial services organizations for providing trust on identities. These networks commonly use OAuth and OIDC as standards, thus allowing for a close integration with the related backend services used in digital services.

Modern solutions must be open to external identities. OAuth and OpenID Connect support in integration.

The challenge is to make a modern, API-driven and service-based approach work in these scenarios. Basically, there are two common approaches, aside from building home-grown OAuth/OIDC servers. Building home-grown solutions has never been a good idea on the long run. For the other approaches, there either is the option to go for a solution that provides a rich feature-set, with the authentication and authorization just being a piece of it. This leads to lengthy processes in selecting such solutions, e.g., Access Management or CIAM (Consumer IAM) solutions, and implementing another complex product. On the other hand, there is the option of focusing on the core capabilities and delivering the right set of APIs and backend services, which can be -- depending on the capabilities that are already in place for further services -- the faster, more efficient, and more adequate approach.

6 The Authlete approach on offloading authentication workload

Authlete is a provider of a specialized solution consisting of an OAuth/OIDC server that can be easily integrated into digital backend services, and the Authlete services which offload protocol handling and perform the protocol processing and token management.

Authlete is a specialized provider of an API authorization solution for the OAuth and OIDC standards. They also provide strong support for FAPI and its derived open banking standards. Their sole focus is on API authorization in complex, multi-party environments such as the common Finance industry scenarios where banks must securely work with clients, but also clients of other banks such as in the TPP (Third Party Provider) scenarios obliged by the PSD2 regulation (Payment Services Directive 2).

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 and ensuring these capabilities in applications is thus 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 organizations can focus on the functional aspects of OAuth 2.0 and OIDC.

Authlete delivers a specialized solution that helps in providing OAuth and OIDC capabilities in digital services, while offloading the complexity of protocol handling to a backend service.

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.

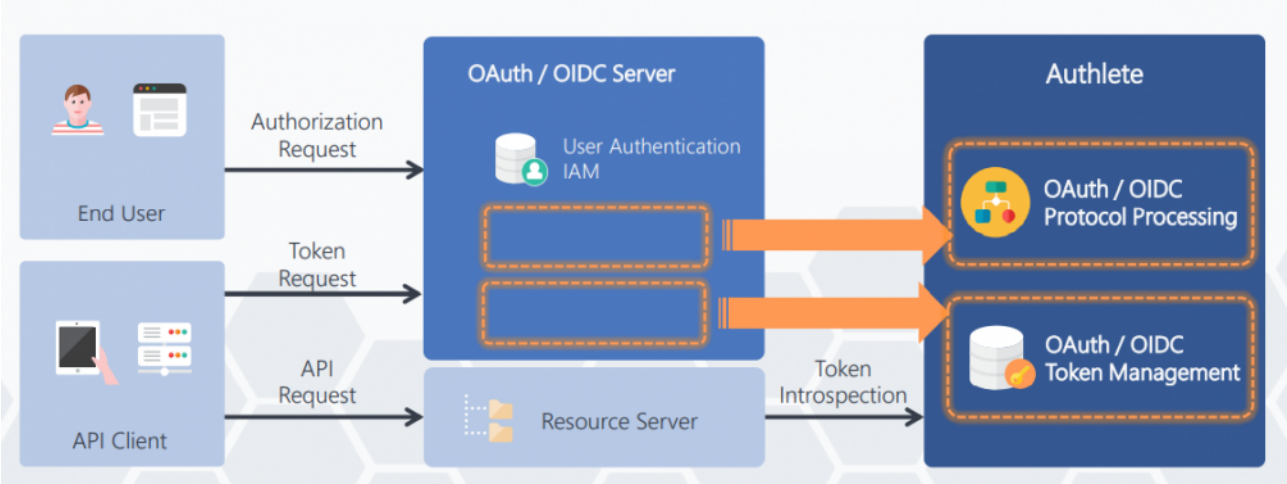

Figure 2: Authlete provides an OAuth/OIDC server and backend services for handling the protocol and token complexity (source: Authlete).

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, which 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.

Authlete consequently follows and API first approach, with excellent support for the developers.

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.

7 Recommendations

Doing digital services right is not as easy as it may appear at first glance. The challenges arise in many areas, from secure development lifecycles to efficient and secure operations, but also in providing both convenience and security in onboarding and recurring authentication and authorization.

Standard solutions that deliver authentication frequently aren't the right fit for digital services, because a neat integration between the authentication and authorization service, commonly an OAuth/OIDC server, and the backend services or "resource servers" is required in the more complex digital services.

To figure out what needs to be done, we recommend evaluating the following aspects:

1. Cooperation: The first step is enabling a close collaboration with defined responsibilities and both organizational and technical (APIs) interfaces between the teams building digital services, and the identity and security teams. It is a CIO's task to make CISOs and CDOs (Chief Digital Officers) collaborate.
2. Requirements: In such collaboration, the specific requirements for dealing with identities and security can be defined, such as scalability needs, security needs, technical requirements such as integration into the digital services, and the registration, authentication and authorization flow.
3. Definition: Based on this, the future architecture can be defined as a blueprint on how to deal with identities today and in the future in the digital business.
4. Portfolio Analysis: Such architecture then serves as the blueprint that is mapped to the current IT infrastructure, for a fit-gap analysis. This helps in identifying the weak spot and additional requirements. It also helps in identifying with a type of solution for authentication and authorization to digital services is required in addition to what exists, and how to integrate this with existing IAM and security components.
5. Selection: Following this, required add-ons can be selected and thoroughly analyzed.
6. Production: Once deployed, these can be put into production.
7. Operations: Finally, an efficient operational approach is required, that helps in delivering the required identity backend services efficiently. Shielding the complexity of APIs and protocols is an enabler of efficient operations.

Success in the digital age depends on a strong, positive digital experience. Authentication and authorization are a core element of this experience. Authentication and authorization are also a core element of security.

Thus, organizations must think about how to do this well.

8 Related Research

Executive View Authlete API Authorization
Leadership Compass Access Management

Content of Figures

Figure 1: Digital identities and IAM are a foundation for successfully delivering digital services.

Figure 2: Authlete provides an OAuth/OIDC server and backend services for handling the protocol and token complexity (source: Authlete).

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.