CLOUDENTITY

Accelerate Open Banking Service Delivery

Automating Authorization, Consent and API Security

Abridged Edition

Open Banking promises to revolutionize the experience of banking as we know it. By enabling a vast array of new financial services, Open Banking presents customers with even more avenues to support their financial wellness. It also offers new business and service innovation opportunities for banks and FinTech companies alike. But the sharing of data between financial institutions and FinTech companies required in an Open Banking world introduces cyber threat and privacy concerns, as well as compliance requirements.

Cloudentity addresses these concerns through its cloud-native authorization management solutions to secure access and protect financial, partner and customer data as it flows between users, applications, and services – all the way down to the complex array of distributed APIs that are the underpinnings of all modern financial transactions.

What is Open Banking?

Open Banking is the practice of banks and other financial institutions, with explicit customer consent, sharing customer data among distinct corporate divisions and with third party financial service providers.

The advantages of this data sharing are realized by customers and banks alike. Customers get better and faster access to services offering financial transparency and streamlined journeys. Financial firms gain greater insights about classes of customers and services as part of Customer 360 / KYC (Know Your Customer) initiatives. Open Banking protocols, such as P2D2, CDR, FAPI and FDX, also set the stage for powering up new and future B2B2C applications by providing a mechanism from which to drive third-party services into a standards-based and secure data exchange ecosystem.

The evolution is underway. According to Statista, 24.7 million people worldwide used Open Banking services in 2020, a number that is forecast to more than quintuple to 132.2 million in 2024. Open Banking is already enhancing various kinds of services and personal financial management tools. The data sharing that enables these services happens the way most modern services share information with one another - via APIs. Application Programming Interfaces provide a set of rules and protocols that determine the way systems communicate with each other, allowing data to flow between apps, services, platforms and financial providers.

Open Banking drivers

A number of factors are spurring on the Open Banking transformation. In many regions, the main impetus is compliance and regulation. To stimulate innovation and competition, Europe's PSD2 initiative directed banks to give third party payment service providers access to the information of customers who have consented to sharing that data. Since its 2018 issuance, this initiative has reverberated across the globe, taking different incarnations in different countries.

In other regions such as North America, market factors are the driving force. Customer behavior is changing. Consumers are no longer limited to the offerings of local financial service providers. Whether being a part of the "iPhone generation" or just being stuck at home during a pandemic, users have become accustomed to digital transactions replacing physical ones and seek frictionless, seamless interaction.

Overall, there is a desire for an enhanced orchestrated user experience that merges financial information. Banks and financial service providers who can offer this sort of holistic digital engagement will be in a better position to serve the expectations of a modern customer base.

Risks and Requirements

Security and compliance

A decentralized management approach to authentication and authorization within a financial services API and service portfolio could allow threat actors to perform account takeover or identity theft. Even inadvertent data leakage can result in data protection obligations and penalties in violation of privacy regulations such as GDPR, CCPA, PIPEDA, LGPD, and PDPA. Other risks include exploitation of API-specific vulnerabilities as listed in the OWASP API Top 10.

Privacy Consent

Another consideration in Open Banking is incorporating customer privacy consent, where financial institutions provide customers the ability to stipulate how their sensitive personal and financial data is to be used. Customers and financial partners want to ensure that personal and financial data access and exchange are within the bounds of their approved usage. However, conventional approaches to applying fine-grained access policy according to privacy consent across distributed applications, services and APIs are currently inefficient, inadequate and not scalable.

Current challenges

App and API security exposures

A major challenge with securing apps, services and APIs today is that financial institutions and FinTech providers lack service and API visibility, centralized policy control, and transactional enforcement processes.

The responsibility of access and security controls for each app, service and API often lies with engineering, which can result in controls that are difficult to manage and audit.

Additionally, the sheer volume of APIs and service gateway connections has grown. Developers are contending with increased application access demand and complex multi-cloud workloads, making it an unwieldly process to discover and identify new or shadow services and APIs, as well as include them in standardized, granular access and data protection modes.

The limits of authentication

Authentication is the process of verifying the identity of a user, device, or service, often based on factors of what the entity knows or has. The use of federated authentication mechanisms, such as single sign-on (SSO) and multi-factor authentication (MFA), are commonplace for session-based system access. However, identity-centric, session-based authentication does not provide the breadth of fine-grained policy, nor depth of transactional data exchange enforcement required for Open Banking. Furthermore, most of these authentication solutions do not typically extend granular controls down to service and API data exchange in a uniform manner and at real-world performance requirements.

Inefficient authorization

Authorization verifies that an entity, be it a user, machine, application or API, has permission to access a resource. In most financial service organizations, developers hard-code authorization rules and privacy controls into each application. This inefficient, bespoke process is prone to human error, policy drift and blind spots that opens the business up to attack and compliance exposures.

Prolonged service delivery

The lack of a streamlined authorization method yields variations in app and API authorization controls. This results in more prolonged security validation cycles, delaying application release.

A more effective, automated approach

The security and privacy requirements of Open Banking make it clear that a new approach to authorization management is needed. Financial firms must be able to offer cloud-native, fine-grained authorization controls to secure access to APIs and sensitive personal data, as well as improve development and DevSecOps proficiency by decoupling authentication and authorization to enable more standardized policy and faster security auditing.

Open Banking security requirements:

- Capturing and managing consent and authorization scope from users, customers, applications and APIs
- Discovering, identifying and on-boarding a multitude of apps, services and APIs into the identity and authorization ecosystem
- Managing fine-grained authorization policy to ensure conditional access and compliant data exchange
- Enabling internal and third-party "tokenized" access via Open Authorization (OAuth), rather than passing actual entity credentials, with granular permissible data scope
- Enforcing granular access and data exchange controls at the transaction-level between entities, apps, APIs and services
- Orchestrating authorization control provisioning across identity, microservice, security and fraud systems

Cloudentity authorization governance for Open Banking

Cloudentity provides a flexible, scalable and proven solution for modern application authorization to fortify Open Banking initiatives within an enterprise's existing hybrid, multi-cloud and microservices infrastructure. The approach ensures continuous access control and data privacy for the high-value, sensitive information in the care of financial institutions.

Through Cloudentity's cloud-native authorization service, financial institutions can decouple identity and authorization, orchestrate service and app on-boarding, enable fine-grained authorization policy as code, assure privacy consent, and gain transaction-level enforcement at hyperscale.

On-boarding, fine-grained policy management and privacy consent - at scale

Developers can make use of Cloudentity's automated onboarding to bring apps and APIs into the identity and authorization ecosystem. As new services are identified, they can be incorporated into existing policy-based enforcement controls.

Instead of deciphering hard-coded authorization policy for each application and API, Cloudentity enables the creation of fine-grained authorization policies through a graphical editor, so even non-developers can understand, create and provision policies without coding or configuration expertise.

Cloudentity has built-in self-service consent workflows and dynamically applied data governance guiderails to prevent unpermitted information leakage while capturing user permissions and API/service transaction activity logs.

By placing access and data exchange enforcement as close to the service or API as possible, Cloudentity provides Zero Trust controls to prevent north/south perimeter and east/west lateral attack, unauthorized access and data leakage risks.

Development at the speed of business

With authorization and consent management decoupled from the application and by encompassing this management as a service, the need for prolonged security verification for new apps is removed, increasing developer velocity.

Fast, easy, infrastructure-agnostic deployment
Cloudentity solutions are distributed as a lightweight Linux package, platform specific serverless component, or as a Docker container via container orchestration platforms. Operating within a Kubernetes cluster, the solution provides east/west lateral connection visibility, tracking and policy enforcement.

Cloudentity enables customers to seamlessly integrate authorization governance into their existing identity, API, container and security management ecosystem. The solution offers pre-built connectors that work with popular identity management and IdP sources, as well as a broad range of popular API gateway platforms. Beyond built-in analytics, all system and transaction events are recorded and can be forwarded to logging, fraud and SIEM system.

Unique, enterprise-class capabilities

Cloudentity offers unique, enterprise-class features that align to Open Banking requirements.

Automated user, app, API onboarding into AuthN/AuthZ ecosystems
Enables developer app/API registration, inventory and discovery.

Authorization policy orchestration

Simplifies policy management with expedited GUI policy editor, natural language code, pre-defined policy packs and dynamic provisioning.

Application and service data governance
Applies data exchange guiderails for each request to negate or redact unpermitted information while capturing data lineage in tamper-proof Privacy Ledger™.

Consent governance workflow
Manages full customer privacy consent process and enforces at the transaction level to meet PII data security obligations.

Transaction enforcement at hyperscale
Enforces millions of requests per second - 60x OAuth token minting and eval performance at 90% lower latency.

Perimeter and lateral microservice Zero Trust
Provides Continuous Zero Trust control at all service ingress and egress decision points to address OWASP API vulnerabilities and attacks.

With Cloudentity, you can...

- Streamline on-boarding apps and APIs into the identity ecosystem
- Integrate seamlessly with existing IdPs and API gateways
- Aggregate context data across IAMs, IdPs, apps and other sources
- Externalize Open Data management for consent, API security, authorization and reporting
- Satisfy business, industry and regulatory compliance leveraging built-in and extensible policy packs, as well as end-to-end data lineage
- Dynamically enforce all app and API access / data exchange at the transaction level
- Gain high-performance control that negates OAuth token examination and re-tokenization latency
- Expedite adhering to Open Banking, FDX, PSD2 and CDR specifications

Conclusion

Open Banking adoption is swiftly advancing, whether due to competitive market factors or through purposeful legislation. Although it will take different incarnations in different regions of the world, one thing is certain: Open Banking is set to disrupt the financial marketplace.

Financial institutions have a choice: take a wait-and-see approach, meeting bare minimum compliance requirements, and risk being left behind; or take advantage of Open Banking.

Cloud-native authorization management is a cornerstone technology to enable Open Banking and mitigate risks. Cloudentity automates the necessary fine-grained authorization policy management and provisioning, privacy consent management, and transaction-level enforcement across hybrid, multi-cloud and microservice environments. It cost-effectively “left shifts” development and DevSecOps for the benefit of application modernization and expedited service delivery.

With security, privacy and compliance exposures mitigated by Cloudentity, financial institutions can streamline application and API access and personal data security with confidence. They can rapidly develop innovative services, offering customers insightful tools to boost their financial well-being while keeping customer data safe in the process.

Learn how Cloudentity modern application authorization solutions can expedite and further your Open Banking programs by visiting www.cloudentity.com.

CLOUDENTITY

Cloudentity is a pioneer and innovator in modern application authorization. Through its externalized, declarative authorization solution, enterprises can take advantage of digital business and open data opportunities, increase development velocity, and mitigate API access and personal data privacy risks. For more information, visit www.cloudentity.com.

206.483.2255

info@cloudentity.com

2815 2nd Ave
Seattle, WA 98121 • USA