CLOUDENTITY

Accelerate Open Banking Service Delivery

Automating Authorization, Consent and API Security

Extended 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. To fully realize the capabilities of Open Banking in a way that earns the trust of customers and partners, companies must ensure the utmost security of 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.

Addressing these concerns with Cloudentity's modern application authorization solutions not only mitigate cyber attack and data privacy risks, but also accelerates digital business by modernizing legacy apps and increasing developer velocity for service enhancement and time to market.

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, from account setup and payments to purchases of financial and third-party products. Financial firms gain greater insights about classes of customers and services as part of KYC (Know Your Customer) initiatives. Firms can use a data-driven approach to provide other useful information or facilitate access to other services at customers' fingertips. Open Banking protocols, such as P2D2 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. Aggregation services offer visibility, allowing customers to see all their accounts from different financial institutions consolidated in one place. Services for budgeting, debt management, debt advising, product comparison and recommendations help customers manage and gain more control over their financial lives. The possibilities for Open Banking service innovation are limitless.

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. Applications and APIs can further present this information in a way that is easy for the user to navigate and act upon.

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

Open banking practices carry unlimited potential for new services and insights that benefit both customers and financial service providers. But opening an institution's APIs to third parties is not without security and compliance risks.

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, carry out unauthorized funds transfers, conduct money laundering, or fraudulently take out loans or credit cards under a bona fide customer's name. Competitors could potentially target an institution's existing customers and undercut prices. Even inadvertent data leakage to partners has business and privacy consequences. Other risks include exploitation of API-specific vulnerabilities as listed in the OWASP API Top 10.

What's more, a host of evolving industry and data privacy mandates must be considered. Among the numerous privacy compliance specifications across the globe are GDPR, CCPA, PIPEDA, LGPD, and PDPA. Each of these directives carries data protection obligations and penalties ranging from data leakage notification affecting reputation, to per-instance fines affecting profitability.

Privacy Consent

Another consideration in Open Banking is incorporating customer privacy consent. Financial institutions, whether to meet data privacy regulations or to boost user trust, must provide customers the ability to stipulate how their sensitive personal and financial data is to be used. Depending on the user, service and data privacy obligations, Open Banking consent management will need to cover personal data collection, access, sharing, redaction, protection, subject inquiry response, usage audit and destruction.

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.

Open Banking standards and APIs – PSD2, FDX and others

PSD2 is the European Union's 2018 expansion of the 2007 Payment Service Providers Directive. PSD2 has two main objectives: to boost innovation and competition in the financial sector by enabling third parties to take part in the financial value chain; and to improve security and consumer protections by protecting electronic transactions and consumers' financial data.

- It orders European banks and other financial institutions to, with customer consent, give third party payment service providers access to customer information.
- It introduces new security requirements such as Strong Customer Authentication (SCA), which obligates banks to enforce the use of two-factor authentication protocols.

FDX is a non-profit organization that developed a standard communications protocol, the FDX API, to enable secure consumer and business access to financial data.

Other standards that support Open Banking include Financial-grade API (FAPI), Open Financial Exchange (OFX), and the Durable Data API (DDA), which all serve to advance means to securely exchange financial data and share customer account information.

Authorization governance solutions must be able to support a range of data exchange protocols and standards to enable financial business flexibility, service benefit, and system interoperability.

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. Depending on the scope of the authentication process, such as device configuration or location, it may also include determining the level of access to a system or data.

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, which includes other services, APIs and data, and applies a stateful policy to determine the scope of allowed transactions. 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 inconsistency and operational blind spots, opening the business up to attack and compliance exposures.

Access control lists (ACL) or role-based authorizations are no longer adequate to support the dynamic, detailed transactional control requirements of Open Banking. Given the number of API and service connections, volume of requests, and changing rule sets, decentralized authorization models cannot be maintained or scaled to mitigate Open Banking security risks.

Prolonged service delivery

The lack of a streamlined authorization method also slows down application modernization, business integration and service improvement projects. IT's ability to ensure timely service and app enhancements is often stymied by inefficient and inconsistent authorization management due to variations in app and API visibility, access and 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, thereby retaining customer trust and fulfilling compliance requirements. More so, to quickly bring new services to market that leverage the power of Open Banking, companies must improve development and DevSecOps proficiency by decoupling authentication and authorization to enable more standardized policy and faster security auditing.

Given the challenges of decentralized management, policy granularity, and transactional enforcement mechanisms for authorization, and its impact on enterprise service delivery and attack surface, organizations need a flexible, automated and contextualized way of managing cloud-native authorization.

Cloudentity authorization governance for Open Banking

Accelerating service delivery and increasing DevSecOps proficiency requires moving user, machine and service access and data exchange authorization to the edge. It requires development automation through an externally managed, declarative authorization service that can invoke fine-grained authorization policy as code and dynamic enforcement.

Cloudentity provides a flexible and scalable solution for modern application authorization to enable Open Banking initiatives within an enterprise's existing hybrid, multi-cloud and microservices infrastructure. The approach ensures continuous API access control and personal 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.

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 permissable 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

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. The service automates discovery of services, API gateways and APIs, and classifies them to expedite cataloging authorization context to be normalized and extended. 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 and create policy without coding or configuration expertise. This provides policy as code agility, where granular policy packs can be standardized, centrally managed, and readily provisioned across distributed applications and services.

Cloudentity also enables financial institutions to meet privacy consent requirements with 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.

Once activated, authorization enforcement occurs at the transaction-level and at hyper-scale within on-premises and cloud container/microservices environments such as Kubernetes. High-performance processing of millions of transaction requests per second occurs as close as possible to each service component, with full data lineage to extend policy monitoring, reporting, auditing, and forensics.

By placing access and data exchange enforcement as close to the service or API as possible, Cloudentity provides Zero Trust controls for all ingress and egress decision points 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. DevSecOps teams can readily verify standard polices, consent management and transactional enforcement for apps, services and API access and data exchange leveraging Cloudentity's platform. Developers, architects, analysts and auditors can inspect and understand policies, see how they have been applied, and have proof of enforcement through a rich analytics dashboard, end-to-end audit log, and tamper-proof privacy consent ledger.

Fast, easy, infrastructure-agnostic deployment

Cloudentity's microservice delivery model and infrastructure-agnostic approach allows 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, such as those from Okta, Google and Microsoft, and is standards-based, supporting protocols such as OAuth 2.1, FAPI R/W, OIDC and SAML2. Since Cloudentity separates authentication sources from app authorization, IdPs can be readily switched or aggregated for added flexibility.

The solution also works with a broad range of popular API gateway platforms, such as those from Axway, Google, Amazon, Microsoft and Kong, to dynamically identify, catalog and on-board APIs and enable dynamic authorization. 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. Beyond built-in analytics, all system changes, user consent and end-to-end transaction events are tracked and can be forwarded to logging, fraud and SIEM systems.

Unique, enterprise-class capabilities

As a pioneer and innovator in authorization governance automation, Cloudentity brings to market a significant set of capabilities. Through Cloudentity's externalized, declarative authorization approach, financial institutions and FinTech companies alike gain engineering, operational and security advantages, while reducing their attack surface and compliance exposures. Cloudentity offers unique, enterprise-class features that align to Open Banking requirements.

Automated user, app, API onboarding into AuthN/AuthZ ecosystems

Cloudentity facilitates user consent management and enables developers to securely register applications, APIs and API gateways to apply authorization policy. As new services and APIs are identified through registered API gateways, authorization policy is dynamically applied and enforced.

Authorization policy orchestration

Cloudentity expedites application, services and API inventory, fine-grained policy development, and declarative authorization provisioning across hybrid, multi-cloud and microservices. Our solutions simplify policy management leveraging a graphical, natural language rules editor, multi-source context normalization, and pre-defined compliance policy packs.

Application and service data governance

Cloudentity dynamically applies data exchange and privacy consent governance guiderails between service and API data requests in order to negate or redact unpermitted information, while capturing the transaction lineage of where data was sourced (for example, the IDP or database) and how that data attribute moved between internal and external systems, ensuring privacy, compliance, forensics and auditability.

Cloudentity Privacy Ledger™ provides a tamper-proof audit of the who, what, where, when and why consent was granted and to whom.

Consent governance workflow

Cloudentity manages user and customer privacy consent process flows end-to-end to meet personal identifiable information (PII) data security and management obligations, including collection, access, sharing, redaction, protection, subject inquiry response, usage audit and destruction. Enterprises can readily extend controls and capabilities within their existing identity, app, service and API infrastructure to support self-service privacy management, Open Data integration, privacy compliance, and data protection measures.

Transaction enforcement at hyperscale

Cloudentity applies real-time enforcement at the transaction level between entities, applications and microservices at the edge, ensuring authenticated access and authorized data exchange for each transaction. Operating at millions of transaction requests per second, Cloudentity delivers 60 times the performance of OAuth token minting and evaluation at 90% lower latency compared to other solutions.

Perimeter and lateral microservice Zero Trust

Cloudentity discovers and catalogues services and APIs, and enforces fine-grained authorization policy for machine-to-machine and service-to-service requests to assure continuous Zero Trust control for all service ingress and egress decision points, mitigating OWASP API vulnerabilities and preventing unauthorized north/south perimeter and east/west lateral access and data leakage risks.

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

Case Study: Achieving compliance with a unified authorization system

Challenge

A large financial institution needed to adhere to the NYDFS cybersecurity regulation's data privacy and audit specifications, one of which, for example, was adaptive multi-factor authentication for sensitive transactions. Decentralized management with disparate authorization and authentication coding, as well as complex business logic, made fulfilling compliance requirements a cumbersome and costly task. The company needed to aggregate user data across directories and domains, while supporting IAM platforms and advancing DevSecOps initiatives.

Solution

Cloudentity provided its modern application authorization solution and rapidly onboarded hundreds of applications, both cloud-first and legacy applications. The new unified system offers a way to centrally govern identity and authorization, and apply policy as code. It aggregates multiple sources of identity data, normalizes authorization context, and integrates with multiple existing IAM and access technologies. Cloudentity's out-of-the-box, standards-based policy packs simplify policy activation and governance, including support for NYDFS controls. The solution also delivers rigorous consent management services at the data object-level, and provides robust and immutable auditability.

Results

The project was completed in four months, at a fraction of the time and cost compared to the previous approach. The firm achieved application modernization with a common user experience across cloud apps and a fortified microservice security approach to enforce data exchange policy for every transaction. The reduced development coding, configuration and on going maintenance effort, and streamlined app security verification amounted to less than one-year payback and a longer-term economic benefit. More so, this authorization governance and API First project serves as a key foundation to advance the financial institution's future Open Banking business endeavors.

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. It will give rise to new types of services and tools to benefit the consumer and it will open up new avenues and touchpoints for financial institutions to reach and serve their customers.

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 to better serve customers, whether by partnering up with a FinTech company developing new customer solutions or investing by themselves in innovation and new services.

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, consent management, and transaction-level enforcement across hybrid, multi-cloud and microservice environments. It cost-effectively "left shifts" engineering 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