GlobalLogic®
A Hitachi Group Company

PRACTITIONER PERSPECTIVES

Written by Luis Cepeda, Associate Specialist Engineer, and reviewed by Agustin Silva, Specialist Engineer.

Open Banking

Introduction and implementation through examples

Executive Summary

Open Banking is a business model for the financial sector that brings a new way of exposing services and data through APIs. This new model is designed to provide enhanced products and experiences using data that until now was “hidden” inside banks infrastructure.

Through standardization, the application of technologies and regulations aligned to the needs of the financial business and security, it promotes and facilitates a better user experience and provides financial companies with another form of integration and collaboration, adding greater transparency and flexibility using the user consent as the driver for sharing information.

Written by Luis Cepeda, Associate Specialist Engineer, and reviewed by Agustin Silva, Specialist Engineer.

Research

Overview

Open banking allows the users to be in control of their own data. The owner of the information is no longer the bank. This new business model allows the user, for example, to see the information of each of their financial accounts in a single app or receive personalized offers.

It allows the customer's financial information to be exchanged with other companies with the previous authorization and consent of the customer and its goal is for the customer to be the owner of their data and to be able to decide whether or not to share it with third parties.

For example, users could normally have three bank accounts at three different banks. Before, they had access to the app of each bank to know the balance of each account. Implementing Open Banking, they can see their global position from a single app. Only by authorizing their banks to share the information with third parties, for example with a financial entity or another bank.
Thanks to this system, the user could also ask Alexa or Siri to tell how much money they have in their account, without having to access it or even order it to send money to a person.

Advantages

Enhancement over the customer experience:
The customer can use a single platform to manage their finances instead of multiple platforms for each account.

Transparency and competition:
Can lead to a reduction in costs and an increase in the quality of services since the information is accessible for more entities than the bank. The financial market can create enhanced products and services to achieve necessity that were unreachable before.

Personalization:
Financial solutions can be adapted for each client since there is more data about them. Offers can also be personalized: For example, if a client has a credit taken from a financial institution, or uses a credit card regularly, among others. Open banking allows third parties to know this information and have the ability to analyze their status and offer them better benefits, such as loans at better rates, more profitable accounts, etc.

Centralized visualization:
Visualize from an application the information of all the accounts and cards of different banks. For example,

clients can enter the app of bank A and from there see the balance they have in their accounts of bank B and C.The financial information is gathered and manageable using only 1 application.

Easier transferences: Make transferences without entering the bank app. For example, if a client uses a financial aggregator, it can make transfers from the added accounts to other accounts. When the client starts the transfer, the aggregator will redirect it to the bank's website to authorize the operation.

Third party authentication: It allows third parties (companies) to verify the clients identity by accessing the information that the bank has about them. If they request a loan from a financial company, they can give third parties access to their bank, in this way they will verify who they are and can see their bank statement and approve the loan faster.

Disadvantages

Data security: This is due to the sharing of sensitive financial data with third parties. This raises legitimate concerns about the security and privacy of customer data. To solve this disadvantage, strong security measures and adequate regulations must be focused to protect the personal and financial data of users.

Risk of fraud and cyberattacks: Malicious agents could attempt to breach Open Banking systems to illegally access confidential information or carry out unauthorized transactions. This drawback is attacked by applying security best practices and constant evaluation in that area.

Financial Exclusion: While Open Banking has the potential to improve the financial experience for many, there is also a risk that those who do not have access to or are unfamiliar with technology may be excluded from new services and benefits. This can create a digital and financial divide between those who can take full advantage of Open Banking and those who cannot.

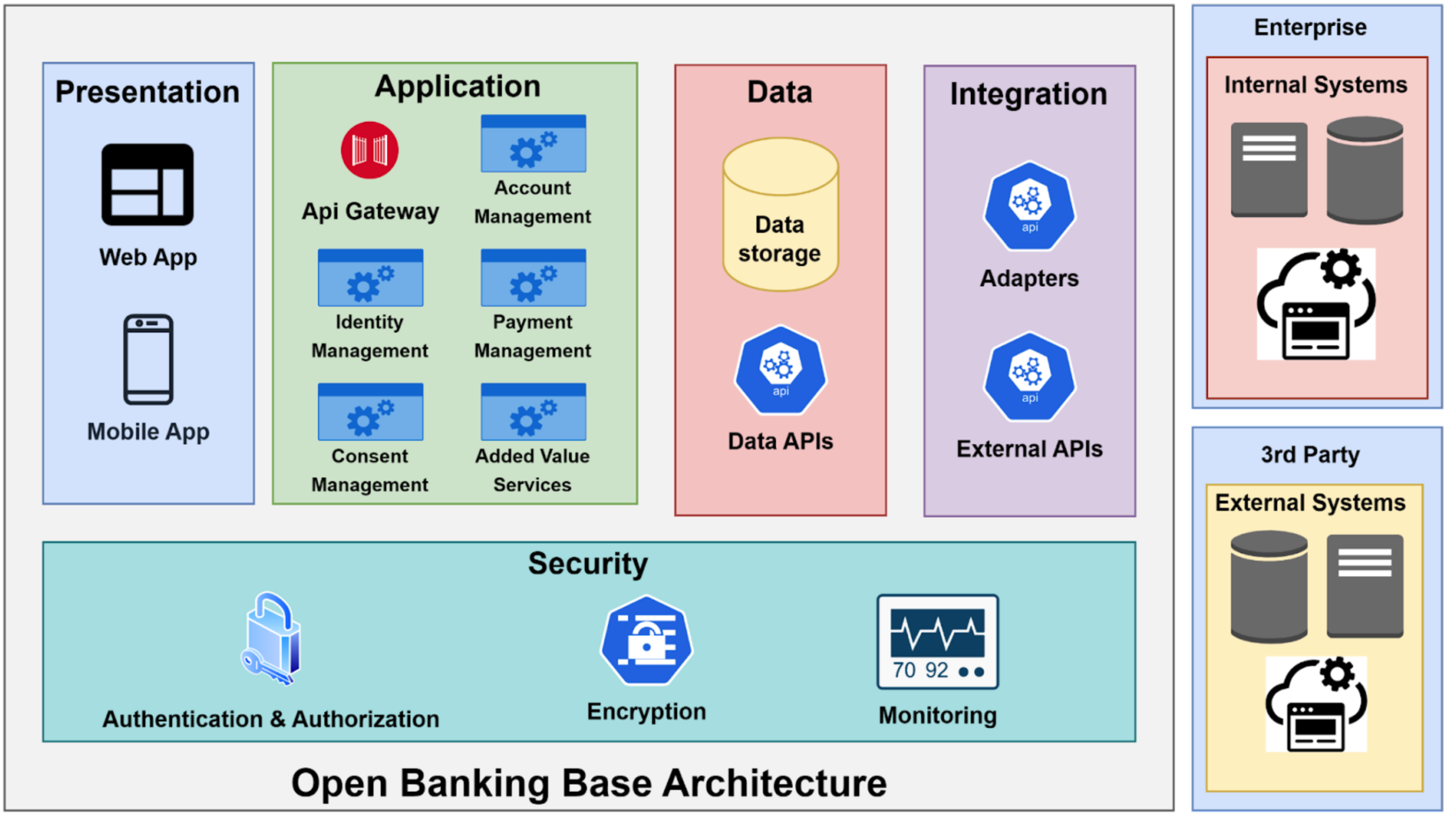
Complexity and fragmentation: The development and implementation of Open Banking can be complex, especially when it comes to integrating different systems and standards. Lack of standardization can lead to fragmented adoption of Open Banking, making interoperability between different providers and financial systems difficult

GlobalLogic®
A Hitachi Group Company

PRACTITIONER PERSPECTIVES

Written by Luis Cepeda, Associate Specialist Engineer, and reviewed by Agustin Silva, Specialist Engineer.

Base Architecture / Building Blocks



The following architecture establishes a set of fundamental layers for the design of an architecture with the Open Banking model. Not all the components are necessarily required to implement it, but it is convenient to have them as a base.

Presentation Layer:

- Mobile or web application for users to access financial services.
- Intuitive user interface for managing accounts, transactions and related services.

Application Layer:

- **API Gateway:** Provides a centralized entry point for all API requests and ensures proper authentication and authorization.

Written by Luis Cepeda, Associate Specialist Engineer, and reviewed by Agustin Silva, Specialist Engineer.

- **Identity Management:** Responsible for user authentication and permission management.
- **Consent Management:** Manages the consent of users to share their financial data with third parties.
- **Account Management:** Allows users to view and manage their financial accounts, balances and transactions.
- **Payment Management:** Facilitates payments and money transfers between accounts.
- **Added Value Services:** Provides additional services, such as financial analysis, advice, and personalized recommendations.

Integration Layer:

- **Internal Systems Adapters:** Connects the Open Banking solution with the bank's internal systems, such as core banking, payment systems, regulatory compliance systems, etc.
- **External APIs:** Allows integration with third parties, such as other financial institutions, payment service providers, fintech companies, etc.

Data Layer:

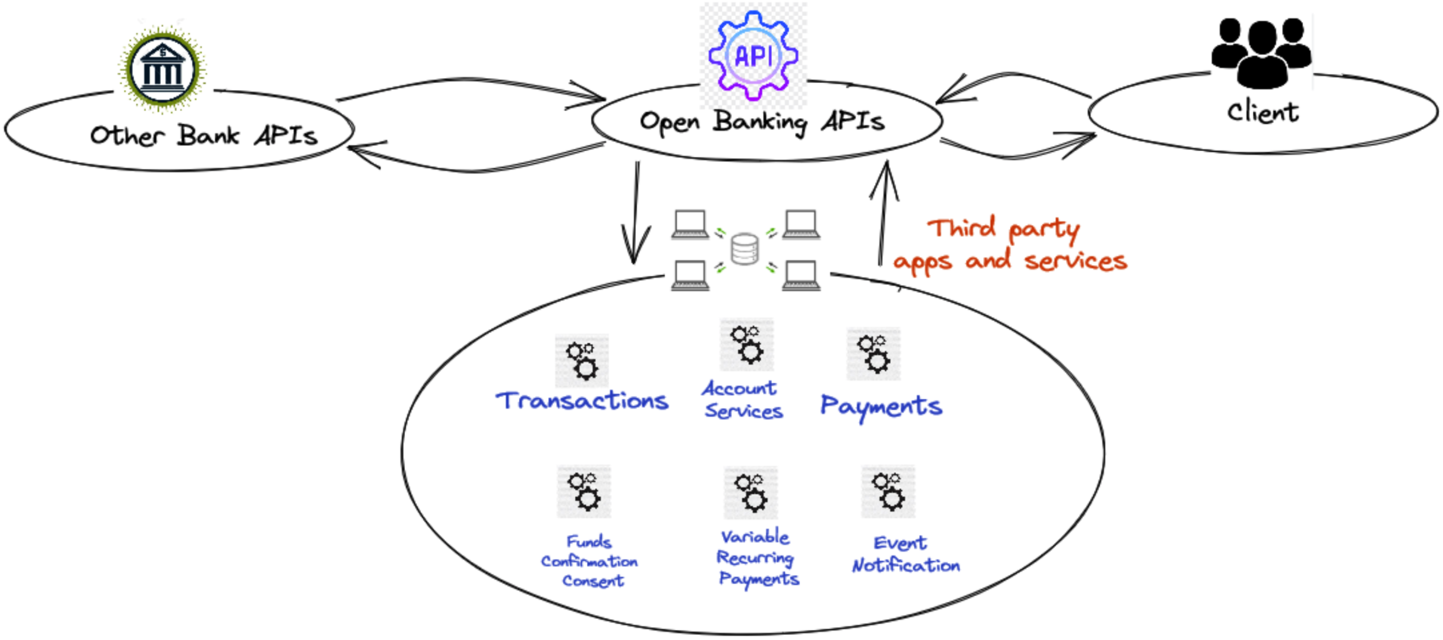
- **Data Storage:** Database to store account information, transactions, user profiles, etc.
- **Data API:** Provides access to users' financial data in a secure and controlled manner, following consent and privacy policies.

Security Layer:

- **Authentication and Authorization:** Ensures that only authorized users can access information and perform transactions.
- **Encryption:** Ensures protected data through different encryption methods.
- **Security Monitoring:** Monitors and detects suspicious activities or attempted attacks.

Written by Luis Cepeda, Associate Specialist Engineer, and reviewed by Agustin Silva, Specialist Engineer.

Integration



APIs are the core of the **Open Banking** architecture. They allow banks to share data and services with other financial service providers in a secure and efficient manner.
Open Banking APIs allow third-party service providers to **access** bank customers' financial data, such as account information, balances, transactions, and other relevant data.
They also allow third-party service providers to make payments on behalf of customers.

Open Banking APIs are designed to be secure, scalable, and stable, allowing third-party service providers to develop high-quality, reliable solutions. In addition, the APIs are standardized and regulated, ensuring that security and privacy requirements are met to protect customers' financial data.

Written by Luis Cepeda, Associate Specialist Engineer, and reviewed by Agustin Silva, Specialist Engineer.

Consent Management

Consent is a fundamental aspect of the **Open Banking** architecture and refers to the permission that the user gives to a third party to access their financial information and carry out transactions on their behalf. In other words, it is the authorization that the bank account holder must give so that a third party, such as an application or a financial service provider, can access their financial information and carry out transactions on their behalf.

Consent is managed through a **secure authentication** process that requires the bank account holder to provide explicit consent for access to their financial information and the completion of transactions. This is accomplished by authenticating the account holder through their bank and granting specific permissions to the third party.

Consent is obtained through a **process** in which the user **grants permission** for the app or financial service provider to access their financial information and conduct transactions on their behalf. Once consent is granted, the third party can access the information and perform the transactions specified in the permission granted.

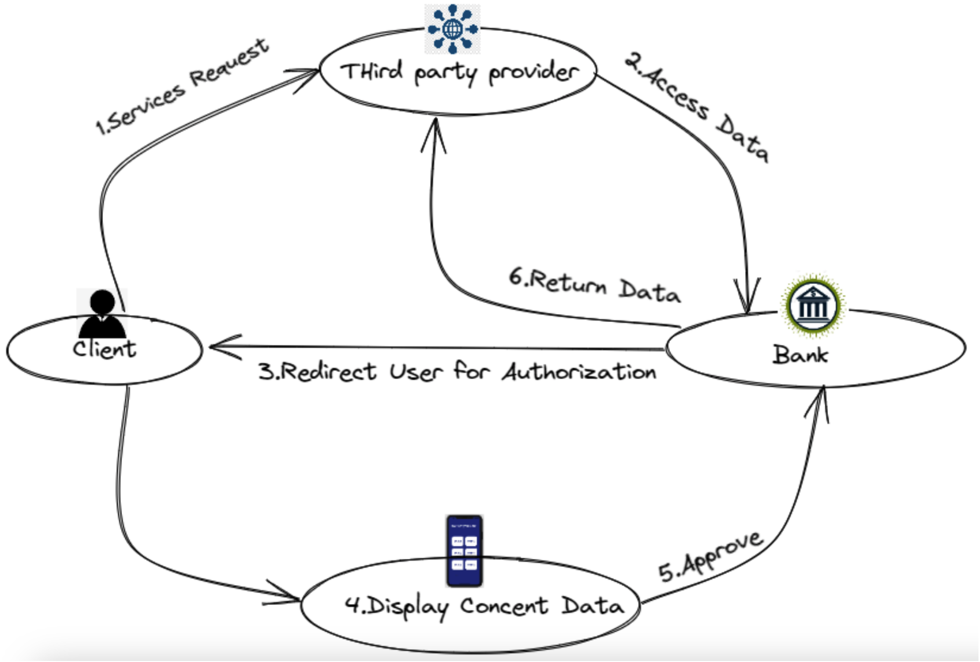
Consent can be revoked at any time by the bank account holder if they change their mind or decide not to allow the third party access to their financial information.
The revocation process is also managed by the bank and requires secure authentication of the bank account holder to ensure that unauthorized access does not occur.

In the context of open banking, consent management can be divided into three phases.

1. The consent phase.
2. The authentication phase.
3. The authorization phase.

Written by Luis Cepeda, Associate Specialist Engineer, and reviewed by Agustin Silva, Specialist Engineer.

Example of a client requesting his account balance from a bank X.



1. The customer initiates an account inquiry in the Open Banking app.
2. The Open Banking app requests the customer's consent to access bank account information and sends a consent request to Keycloak (authentication/authorization server).
3. Keycloak returns a URL with a token for the Open Banking app to redirect the customer to the Keycloak consent page.
4. The user completes the consent process on the Keycloak page, and Keycloak validates the token.
5. Keycloak returns the consent response to the Open Banking app.
6. The Open Banking app shows the result of the query to the customer.

Regarding regulations, it is important to mention that the Open Banking architecture is designed to comply with data protection and financial privacy regulations, such as the GDPR in the European Union and the personal data protection law in other countries. In addition, financial service providers that use the Open Banking architecture must comply with licensing and regulatory requirements by local financial authorities.

Written by Luis Cepeda, Associate Specialist Engineer, and reviewed by Agustin Silva, Specialist Engineer.

Application Examples

Here are some examples of Open Banking's application:

- **Account aggregation platforms**, which allow customers to view all of their accounts on a single platform.
- **Mobile payment solutions**, which allow customers to make payments directly from their mobile devices.
- **Loan solutions**, which use customers' financial data to offer personalized loans.

Open Banking is a revolutionary technology that is transforming the way financial services are delivered. Through Open Banking APIs, banks and other financial service providers can share data and services securely and efficiently, leading to greater convenience and ease of use for customers, greater transparency, and market competition, finance, and greater innovation and development of personalized financial solutions.

Apps which already use Open Banking APIs:

- **Revolut:** Fintech that offers online and mobile financial services. With Open Banking, Revolut can access financial information from other banks to offer personalized services to its customers.

- **BBVA:** Spanish bank that has implemented Open Banking on its BBVA API Market platform. This platform allows developers to create financial applications and services using BBVA and Open Banking technology.

- **Stripe:** Online payment platform that uses Open Banking to improve the payment experience for users. It allows users to make payments directly from their bank accounts using Open Banking technology.

Written by Luis Cepeda, Associate Specialist Engineer, and reviewed by Agustin Silva, Specialist Engineer.

These are just a few examples of companies and applications that have implemented Open Banking. The list continues to grow as more companies join the open banking trend and look to take advantage of Open Banking technology to offer more personalized and efficient financial services.

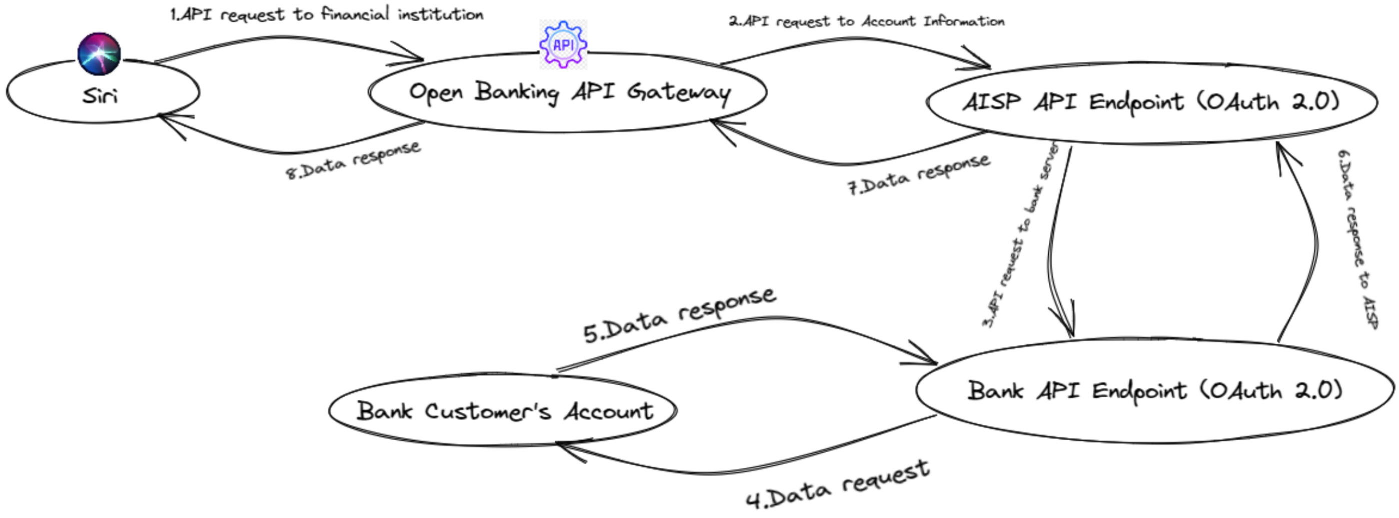
Written by Luis Cepeda, Associate Specialist Engineer, and reviewed by Agustin Silva, Specialist Engineer.

Implementation Example - Connect Siri With Open Banking

In order for Siri to connect to an Open Banking architecture, Apple and the bank need to work together to enable a specific integration using an Open Banking API.
Since iOS 11, Siri has bank support. That means if the bank adds support, you'll be able to transfer money from one account to another, check your balances, find out what transactions are still pending, and more.
1. Apple and the bank establish a connection using an Open Banking API.
2. The user authorizes access to their financial information through a consent process in the bank's mobile application.
3. The mobile application uses the Open Banking API to access the user's financial information.
4. The mobile application transmits the requested information to Siri using the Open Banking API.
5. Siri processes the information and presents a response to the user through the bank's mobile app.

Written by Luis Cepeda, Associate Specialist Engineer, and reviewed by Agustin Silva, Specialist Engineer.

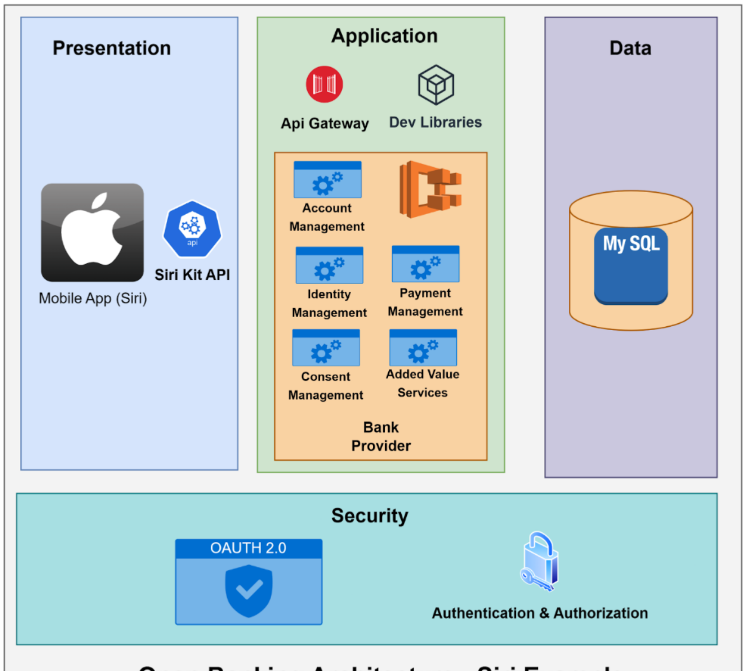
Example of steps that an account query would follow after requesting it from SIRI


1.API request to financial institution
2.API request to Account Information
Siri
API
Open Banking API Gateway
AISP API Endpoint (OAuth 2.0)
8.Data response
7.Data response
3.API request to bank server
6.Data response to AISP
5.Data response
Bank Customer's Account
Bank API Endpoint (OAuth 2.0)
4.Data request

1. Siri processes the voice request and sends an API request to the financial institution.
2. The API request is received by the Open Banking API Gateway.
3. The API Gateway sends the API request to an Account Information Service Provider (AISP) through its endpoint API (OAuth 2.0).
4. The account information service provider sends an API request to the bank's server through its endpoint API (OAuth 2.0).
5. The bank's server retrieves the customer's account data and sends an API response to the account information service provider.
6. The account information service provider sends the API response back to the Open Banking API Gateway via its endpoint API (OAuth 2.0).
7. The Open Banking API Gateway sends the API response to Siri on the iOS device.
8. Siri presents bank account information to the user on their iOS device.

Written by Luis Cepeda, Associate Specialist Engineer, and reviewed by Agustin Silva, Specialist Engineer.

Below we can detail some of the tools that should be used to carry out the steps detailed in the previous point:



Open Banking Architecture - Siri Example

1. An Open Banking API server: To enable communication between Siri and the banking system, an Open Banking API server is required. This could be provided by the financial institution or by an Open Banking service provider.

2. A SiriKit API: SiriKit is Apple's development framework for integrating apps and services with Siri. To connect Siri to an Open Banking architecture, a specific SiriKit API is required that allows Siri to send voice commands to the Open Banking API.

3. OAuth 2.0 Authentication: OAuth 2.0 is an authorization protocol used to protect sensitive user data. In an Open Banking architecture, OAuth 2.0 is used to authenticate users and ensure that only they have access to their financial data. Siri must also be configured to authenticate with OAuth 2.0 to access the user's financial information.

4. Development libraries: There are several development libraries available to work with Open Banking and OAuth 2.0 APIs in various programming languages, such as Java, Python, Ruby, and JavaScript. These libraries facilitate the development of applications and services that integrate with the Open Banking architecture.

5. Cloud development platforms: To simplify the development and implementation of Open Banking services, cloud development platforms such as AWS, Google Cloud, and Microsoft Azure can be used. These platforms offer integrated services and development tools, such as data warehousing and data analytics, which can help in the development of more complex Open Banking services.

Written by Luis Cepeda, Associate Specialist Engineer, and reviewed by Agustin Silva, Specialist Engineer.

Conclusion

Although there are risks in applying an open banking model, they are easily resolved by applying the best security practices and market standards. The beneficiaries are all parties, both users and financial institutions, opening the game to a broader digital model, easier to implement and use and above all governed by transparency and access to data. Payment management has never been as easy as it has been up to now, so it is recommended that financial institutions keep such a strategy in mind within their business model.

Open banking enables a broader and more accessible digital model, driven by transparency and access to data, it will allow users to benefit from a wide range of financial services, greater convenience and a personalized experience. At the same time, financial institutions can expand their reach, offer innovative solutions, and foster collaboration with other market players.

To maximize the benefits and minimize the risks, it is crucial to focus on security and data protection. These must be a priority, implementing strong cyber security and data protection measures, such as the use of data encryption tools, multi-factor authentication, among others. Add secure APIs, with strong authentication and authorization mechanisms. Identity management and privacy policies.

In turn, the education and awareness of users and bank staff are also essential to promote responsible and safe use of open banking. Informed user consent, adoption of interoperability standards and protocols, and constant monitoring help ensure smooth and secure integration. Transparency in data management and the active participation of financial institutions in the definition of common policies and standards strengthen user confidence and promote a more solid open banking environment.

Open banking represents an exciting opportunity to transform the financial industry, bringing benefits to both users and financial institutions. By following the aforementioned recommendations and adopting an open banking strategy in the business model, financial institutions can adapt to a broader digital environment that is easy to implement and use. Managing payments and financial services has never been easier and more accessible than it is right now, and it is essential that financial institutions are prepared to take advantage of this evolution in the financial landscape.

Written by Luis Cepeda, Associate Specialist Engineer, and reviewed by Agustin Silva, Specialist Engineer.

Glossary

Financial Aggregator	Application or function within an application that allows the user to organize the information of all their accounts and credit cards in the same platform, regardless of which bank they belong to.
GDPR (General Data Protection Regulation)	Regulation of the European law that acts on privacy and data protection.
Keycloak	Solution for identity and access management provides authorization and authentication functionalities.
OAuth 2.0	Stands for "Open Authorization", is a standard designed to allow a website or application to access resources hosted by other web apps on behalf of a user.
PSD2 (Payment Services Directive)	European legislation that seeks to regulate payment services in the European market.
Siri	Siri is a virtual assistant that is part of Apple Inc.'s iOS, iPadOS, watchOS, macOS, tvOS, and audioOS operating systems

References

1 - Open Banking and psd2
2 - Open Banking architecture with WSO2
3 - Open Banking architecture perspective
4 - Open Banking standards