Extended FAQ:
Open Banking

This FAQ addresses key questions about Open Banking, helping business and technical teams understand value and platform implementation.

1. General & Strategic Questions

1.1. What are the key strategic benefits of adopting Open Banking?

Open Banking enables institutions to accelerate revenue growth through new business models, drive financial inclusion by reaching underserved segments, enhance customer experience with personalized services, and future-proof their operations by building a modern, collaborative ecosystem.

1.2. How can Open Banking help our bank compete with agile fintechs?

Open Banking transforms the competitive landscape from a zero-sum game to a collaborative ecosystem. By exposing your data via standardized APIs (with customer consent), you enable partnerships with fintechs to innovate faster and offer new services, while retaining customer trust and brand identity.

2. Technical & Implementation Questions

2.1. How do you obtain, manage, and track explicit, informed, and granular customer consent for data sharing? What mechanisms are in place to allow customers to easily revoke consent?

WSO2 Open Banking provides a dedicated Consent Manager to collect explicit, informed and granular consent at the time of authorization, show scopes/data categories, store consent metadata (who/what/when/purpose/expiry), and expose dashboards and APIs for audit and lifecycle tracking. Customers can revoke consent at any time via self-service (portal or mobile) or assisted channels; revocations propagate to tokens/sessions so downstream access is blocked.

2.2. Are you adhering to the prescribed security standards, such as using OAuth 2.0 for authorization and TLS encryption for data transmission? What is your process for conducting regular penetration testing and vulnerability assessments?

Yes. All open-banking APIs run over TLS with OAuth 2.0/OpenID Connect, support FAPI-style (WSO2 Solution is FAPI certified) hardening and mutual TLS (mTLS) enforcement, plus JWT/message-level signing where required. We run regular vulnerability assessments and pen-tests and maintain incident and breach procedures consistent with the Guidelines' Information Security (Section 9.3), Cybersecurity Incident Reporting (Section 11.7), and Testing (Section 9.6) plus the Security Standards in Appendix III (OAuth2.0, REST, JSON, JWT, TLS). WSO2 provides out-of-the-box mTLS enforcement policies and MFA/adaptive auth.

2.3. Are your APIs meeting the minimum performance standards set by the CBN, such as the required average API processing time? What systems do you have in place to monitor and report on API performance?

WSO2 Open Banking solution meets the minimum performance standards set by major Open Banking specifications like PSD2, UK and CDS. API performance reporting requirements vary according to the specification. However WSO2 Open Banking solution is equipped with the core components required to monitor API analytics. Once CBN announces their performance thresholds and reporting requirements, these can be supported.

2.4. What are the defined roles and responsibilities of your organization as an API Provider or API Consumer?

WSO2 provides a platform for the API Provider to adhere to the OB guidelines demanded by the regulator. API consumers will be facilitated with standard communication and security methods to integrate with the API provider.

3. Security & Compliance Questions

3.1. How does opening up to third parties impact our bank's security posture?

Open Banking is built on robust security protocols. Instead of exposing your entire system, APIs provide a controlled, secure entry point. Our solutions implement multi-layered security, advanced threat protection, and continuous monitoring to safeguard your systems and data.

3.2. How do we manage third-party risk with our new partners?

The regulatory framework includes a central registry to identify and authenticate all licensed participants, mitigating some risk. Additionally, robust API security, rigorous partner onboarding processes, and continuous monitoring of API interactions are essential for managing third-party risk.

3.3. How do we ensure data privacy within the ecosystem?

Compliance hinges on a 'privacy-by-design' approach. Your consent management platform must be fully transparent to the user, and data sharing must be strictly limited to what was consented to. Anonymization and pseudonymization techniques should be employed where possible. Our solutions are built to ensure strict adherence to global data protection regulations and local privacy laws.

3.4. What is the process for customers to give and revoke consent for data sharing?

Customers must provide explicit, granular consent for data sharing, specifying the data to be shared, the purpose, and the duration. A key component of the framework is a user-friendly mechanism for customers to view and revoke this consent at any time, maintaining their sovereignty over their financial data.

4. Cost & Benefits Questions

4.1. What are the primary revenue opportunities for banks in the Open Banking ecosystem?

Revenue can be generated by charging for premium APIs, enabling new embedded finance services with partners, offering enhanced data analytics, and providing specialized services to fintechs. Open Banking expands your revenue models beyond traditional lending and deposits.

4.2. How can we demonstrate return on investment (ROI) for our Open Banking initiative?

ROI can be measured through increased customer acquisition from new channels, improved customer retention through superior services, reduced operational costs from automated processes, and new revenue streams from partnerships and data-driven insights.

4.3. Does Open Banking implementation require a full overhaul of our IT infrastructure?

Not necessarily. Our solutions are designed to work with your existing infrastructure. We provide an API-led integration layer that connects your legacy systems to the Open Banking ecosystem, allowing for a phased approach that minimizes disruption and upfront costs.

4.4. How can we use Open Banking to develop new products and services?

By securely accessing a customer's financial data with their consent, you can gain a holistic view of their needs. This allows you to develop hyper-personalized products like tailored loan offerings, customized savings plans, and automated financial management tools that directly meet their specific needs.

4.5. How does a strong Open Banking strategy help attract and retain talent?

Embracing cutting-edge technology and innovation makes your bank a more attractive employer for tech talent. Furthermore, a modern API-first infrastructure empowers your internal teams to develop and deploy new solutions faster, improving internal productivity and job satisfaction.



Visit wso2.com for more