SECURE API PRODUCT DESIGN FOR OPEN BANKING AND PSD2 COMPLIANT PLATFORMS

Eric Victor

Department of IT, University of Indiana

Abstract:

Open banking has fundamentally transformed the financial services landscape by enabling secure data sharing and service interoperability through standardized application programming interfaces (apis). Under regulatory frameworks such as the second payment services directive (psd2), financial institutions are required to expose customer-authorized data and payment initiation capabilities to licensed third-party providers. While this paradigm fosters innovation and competition, it also introduces significant security, privacy, and operational risks. Apis have become primary attack surfaces for fraud, data leakage, and service disruption in open financial ecosystems. This paper examines secure api product design principles tAIlored for open banking and psd2-compliant platforms. It presents a comprehensive analysis of regulatory requirements, threat models, authentication and authorization mechanisms, consent management, api governance, and operational resilience strategies. By synthesizing industry best practices, academic research, and regulatory guidance, the study proposes a secure-by-design api product framework that integrates strong customer authentication, fine-grAIned access control, cryptographic assurance, and continuous risk monitoring. The paper further discusses implementation challenges, architectural trade-offs, and future directions for secure api ecosystems. The findings emphasize that security in open banking apis must be treated as a core product capability rather than a technical afterthought, ensuring trust, compliance, and sustAInable innovation.

Keywords

Open banking; psd2; secure api design; financial apis; strong customer authentication; fintech security

1. Introduction

The financial services industry has undergone a structural transformation driven by digitalization, regulatory reform, and platform-based innovation. One of the most consequential developments is the rise of open banking, a framework that mandates banks to provide secure, standardized access to customer account data and payment services through apis. In the european union, this transformation has been institutionalized through the second payment services directive (psd2), which AIms to increase competition, improve consumer choice, and foster innovation while mAIntAIning high levels of security and consumer protection.

Apis are the technological foundation of open banking. They enable account information service providers (AIsps) and payment initiation service providers (pisps) to access bank systems in a controlled and consent-driven manner. However, exposing core banking functionality through apis significantly alters the security posture of financial institutions. Unlike traditional closed banking systems, open banking platforms operate in highly distributed, multi-party environments where trust boundaries are fluid and continuously evolving. As a result, apis become high-value targets for cyberattacks, fraud exploitation, and data misuse.

Psd2 explicitly recognizes these risks and introduces stringent security requirements, including strong customer authentication (sca), secure communication standards, dynamic consent management, and auditability. Nevertheless, regulatory compliance alone does not guarantee robust security. Many open banking implementations struggle with api misuse, insufficient authorization granularity, token leakage, replay attacks, denial-of-service threats, and third-party risk propagation. These challenges underscore the need for a holistic approach to secure api product design that aligns regulatory compliance with modern security engineering principles.

This paper argues that secure api design in open banking must be treated as a product discipline rather than a purely technical or compliance-driven exercise. Security controls should be embedded into api lifecycle management, developer experience, consent flows, and operational monitoring. By adopting a secure-by-design and zero-trust-oriented approach, open banking platforms can achieve both regulatory compliance and sustAInable ecosystem growth. The remAInder of this paper explores the regulatory context of psd2, reviews relevant literature, presents a structured secure api design framework, and discusses practical implementation considerations and future trends.

2. Regulatory context: open banking and psd2

Psd2 establishes a legal and technical foundation for open banking in the european economic area. It mandates that account servicing payment service providers (aspsps), typically banks, provide licensed third parties with access to customer account information and payment initiation services, subject to explicit customer consent.

Key psd2 security requirements relevant to api design include:

1. **Strong customer authentication (sca)**
2. Sca requires at least two independent authentication factors from the categories of knowledge, possession, and inherence. Apis must support secure authentication flows that integrate sca while minimizing customer friction.
3. **Secure communication**

4. Psd2 regulatory technical standards (rts) mandate the use of secure communication protocols, including mutual tls, qualified certificates (eidas), and encryption of data in transit.
5. **Consent management**
6. Apis must enforce explicit, granular, and revocable customer consent, ensuring that third parties access only the data and functionality authorized by the customer.
7. **Non-discriminatory access**
8. Banks must provide apis that offer equivalent functionality and avAIlability to those used internally, preventing the degradation of third-party access.
9. **Auditability and traceability**
10. All access and transactions must be logged to support regulatory audits, dispute resolution, and incident investigations.

These requirements impose significant design constrAInts on api products, necessitating careful alignment between regulatory compliance, security engineering, and usability.

3. Literature review

Academic and industry literature on open banking security highlights both the opportunities and challenges associated with api-based financial ecosystems. Early studies emphasize the economic benefits of open banking, including increased competition and innovation. However, subsequent research identifies apis as a dominant attack vector in modern financial systems.

Security research highlights common api vulnerabilities, such as broken object-level authorization, excessive data exposure, inadequate rate limiting, and insufficient monitoring. In open banking contexts, these vulnerabilities are exacerbated by the involvement of multiple external actors with varying security maturity levels.

Several studies advocate for oauth 2.0 and openid connect as foundational authorization frameworks for open banking apis. While these standards provide a solid baseline, researchers note that improper implementation and insufficient contextual validation often undermine their effectiveness. Recent work emphasizes the need for fine-grAIned authorization, contextual access control, and continuous risk assessment.

Regulatory technology (regtech) literature highlights the role of automation in enforcing compliance requirements such as sca, consent tracking, and audit logging. However, there is limited consensus on how

to integrate these controls seamlessly into api product design without degrading developer experience or system performance.

Overall, the literature reveals a gap between regulatory intent and practical implementation, underscoring the need for integrated secure api design frameworks tAIlored specifically for open banking and psd2 environments.

4. Threat modeling for open banking apis

Effective secure api design begins with a clear understanding of the threat landscape. Open banking apis face a unique combination of traditional cybersecurity threats and financial fraud risks.

4.1 key threat categories

- **Unauthorized api access**: exploitation of weak authentication or authorization mechanisms.
- **Token theft and replay attacks**: abuse of oauth tokens to gAIn persistent access.
- **Consent abuse**: accessing data beyond the scope or duration of customer consent.
- **Api abuse and denial of service**: excessive requests disrupting service avAIlability.
- **Man-in-the-middle attacks**: interception or manipulation of api traffic.
- **Third-party risk propagation**: compromised tpp systems used as entry points.

4.2 threat modeling approaches

Structured threat modeling frameworks such as stride and mitre att&ck can be adapted to open banking architectures. However, effective protection requires continuous threat modeling aligned with evolving api usage patterns and regulatory changes.

5. Secure api product design framework

This section presents a secure api product design framework for open banking platforms, structured across six interdependent layers.

5.1 identity and authentication layer

Secure identity management is foundational. Psd2-compliant apis typically use:

- Mutual tls with qualified certificates
- Oauth 2.0 authorization flows

- Openid connect for user identity federation

Strong customer authentication should be enforced dynamically, applying exemptions where permitted (e.g., low-risk transactions) while mAIntAIning regulatory compliance.

5.2 authorization and access control

Authorization must be fine-grAIned and context-aware. Best practices include:

- Scope-based and attribute-based access control
- Separation of account access and payment initiation privileges
- Real-time validation of consent scope and validity

Apis should never rely solely on static scopes; contextual attributes such as transaction value, device risk, and behavioral anomalies must inform access decisions.

5.3 consent management as a product capability

Consent management should be treated as a first-class product feature. Key requirements include:

- Explicit customer consent capture
- Granular permission definition
- Easy revocation mechanisms
- Transparent consent dashboards

Apis must enforce consent at runtime, ensuring that every request is validated agAInst active consent records.

5.4 secure communication and data protection

All api communications must be encrypted using modern cryptographic standards. Sensitive data should be minimized and tokenized where possible. Message signing and integrity checks further reduce the risk of tampering.

5.5 api governance and lifecycle management

Secure api design extends beyond runtime controls to lifecycle governance:

- Secure api onboarding for third parties
- Automated certificate and key rotation

- Versioning and deprecation policies
- Secure developer portals and documentation

Governance ensures consistency, compliance, and resilience as the ecosystem scales.

5.6 monitoring, detection, and incident response

Continuous monitoring is essential for detecting abuse and fraud. Effective platforms implement:

- Real-time api usage analytics
- Anomaly detection and behavioral baselining
- Automated throttling and blocking
- Integrated incident response workflows

Operational telemetry enables rapid response to security incidents and supports regulatory reporting.

6. Implementation challenges and trade-offs

Despite clear design principles, implementing secure open banking apis presents practical challenges. These include balancing security with performance, minimizing customer friction during sca, managing third-party variability, and integrating legacy banking systems. Overly rigid security controls may hinder adoption, while insufficient controls expose platforms to unacceptable risk.

Successful implementations adopt a risk-based approach, tAIloring security measures to transaction context and continuously refining controls based on operational data.

7. Future directions

Future open banking api security will increasingly leverage artificial intelligence, zero-trust architectures, and continuous authorization models. Emerging standards such as financial-grade api (fapi) 2.0 promise stronger security guarantees, while advances in behavioral biometrics and decentralized identity may further enhance trust and usability.

8. Conclusion

Secure api product design is a cornerstone of successful open banking and psd2-compliant platforms. As apis become the primary interface between banks, third parties, and consumers, their security directly impacts trust, regulatory compliance, and ecosystem sustAInability. This paper has shown that effective api security extends beyond technical controls to encompass product design, governance, and operational

resilience. By embedding strong authentication, fine-grAIned authorization, consent enforcement, and continuous monitoring into the api lifecycle, financial institutions can mitigate risks while enabling innovation. Ultimately, secure-by-design apis are not only a regulatory necessity but a strategic enabler for the future of open financial ecosystems.

References

1. Arooj Hassan, Malik Arfat Hassan, & Muhammad Ahsan Khan. (2025). Quantum-Resistant Cryptography in Cloud-Based Fintech Solutions. *Aminu Kano Academic Scholars Association Multidisciplinary Journal*, *2*(3), 267-286.
2. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "AI-Driven Product Roadmaps in Fintech, Optimizing User Experience and Security Trade-offs." *International Journal of Business & Digital Economy* 1, no. 01 (2025): 1-13.
3. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "Design Thinking for Secure Fintech Products: Balancing Innovation and Compliance." *Econova* 2, no. 1 (2025): 1-16.
4. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "Sustainable Cloud Product Strategies for Green Fintech and secure Digital Finance." *CogNexus* 1, no. 03 (2025): 162-176.
5. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "Product Management Challenges in AI-Enhanced Fintech Fraud." *International Journal of Business & Digital Economy* 1, no. 01 (2025): 14-28.
6. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "AI-Driven Product Roadmaps in Fintech, Optimizing User Experience and Security Trade-offs." *International Journal of Business & Digital Economy* 1, no. 01 (2025): 1-13.
7. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "Threat Intelligence Automation in Fintech, A Product Management Perspective." *Multiverse Journal* 1, no. 2 (2024): 50-62.
8. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "Impact of Regulatory Compliance PSD2, GDPR on Fintech Product Design." *Frontiers in Multidisciplinary Studies* 1, no. 01 (2024): 59-72.
9. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "Integrating Cyber Risk Metrics into Fintech Product Lifecycle Management." *Econova* 1, no. 01 (2024): 42-53.
10. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "Evaluating Zero Trust Security Models for Fintech Cloud Infrastructures." *Multiverse Journal* 1, no. 1 (2024): 52-60.
11. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "The Role of Cloud Compliance Automation in Scaling Fintech Products Globally." *Journal of Educational Research in Developing Areas* 4, no. 2 (2023): 245-255.

12. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "Multi-Cloud Strategies for Scalable and Secure Fintech Applications." *Journal of Educational Research in Developing Areas* 4, no. 1 (2023): 123-133.
13. Nabi, Hussain Abdul, Ali Abbas Hussain, Abdul Karim Sajid Ali, and Haroon Arif. "Data-Driven ERP Solutions Integrated with AI for Streamlined Marketing Operations and Resilient Supply Chain Networks." *The Asian Bulletin of Big Data Management* 5, no. 2 (2025): 115-128.
14. Arif, Haroon, Abdul Karim Sajid Ali, Aamir Raza, and Aashesh Kumar. "Adversarial Attacks on AI Diagnostic Tools: Assessing Risks and Developing Mitigation Strategies." *Frontier in Medical and Health Research* 3, no. 1 (2025): 317-332.
15. Arif, Haroon, Ali Abbas Hussain, Hussain Abdul Nabi, and Abdul Karim Sajid Ali. "AI POWERED DETECTION OF ADVERSARIAL AND SUPPLY CHAIN ATTACKS ON GENERATIVE MODELS."
16. Arif, H., Ali, A. K. S., & Nabi, H. A. (2025). IoT Security through ML/DL: Software Engineering Challenges and Directions. ICCK Journal of Software Engineering, 1(2), 90–108. https://doi.org/10.62762/JSE.2025.372865
17. Arif, Haroon, Aashesh Kumar, Muhammad Fahad, and Hafiz Khawar Hussain. "Future horizons: AI-enhanced threat detection in cloud environments: Unveiling opportunities for research." *International journal of multidisciplinary sciences and arts* 3, no. 1 (2024): 242-251.
18. Ali, Abdul Karim Sajid, Aamir Raza, Haroon Arif, and Ali Abbas Hussain. "INTELLIGENT INTRUSION DETECTION AND DATA PROTECTION IN INFORMATION SECURITY USING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING TECHNIQUES." *Spectrum of Engineering Sciences* 3, no. 4 (2025): 818-828.
19. Fahad, Muhammad, Aashesh Kumar, Haroon Arif, and Hafiz Khawar Hussain. "Mastering apt defense: strategies, technologies, and collaboration." *BIN: Bulletin Of Informatics* 1 (2023): 84-94.
20. Ghelani, Harshitkumar. "AI-Driven Quality Control in PCB Manufacturing: Enhancing Production Efficiency and Precision." *Valley International Journal Digital Library* (2024): 1549-1564.
21. Ghelani, Harshitkumar. "Advanced AI Technologies for Defect Prevention and Yield Optimization in PCB Manufacturing." *International Journal Of Engineering And Computer Science* 13, no. 10 (2024).
22. Ghelani, Harshitkumar. "Six Sigma and Continuous Improvement Strategies: A Comparative Analysis in Global Manufacturing Industries." *Valley International Journal Digital Library* (2023): 954-972.
23. Ghelani, Harshitkumar. "Automated Defect Detection in Printed Circuit Boards: Exploring the Impact of Convolutional Neural Networks on Quality Assurance and Environmental Sustainability in Manufacturing." *International Journal of Advanced Engineering Technologies and Innovations* 1: 275-289.

24. Ghelani, Harshitkumar. "Harnessing AI for Visual Inspection: Developing Environmentally Friendly Frameworks for PCB Quality Control Using Energy-Efficient Machine Learning Algorithms." *International Journal of Advanced Engineering Technologies and Innovations* 1: 146-154.
25. Ghelani, Harshitkumar. "Enhancing PCB Quality Control through AI-Driven Inspection: Leveraging Convolutional Neural Networks for Automated Defect Detection in Electronic Manufacturing Environments." *Available at SSRN 5160737* (2024).
26. Ghelani, Harshitkumar. "Advances in lean manufacturing: improving quality and efficiency in modern production systems." *Valley International Journal Digital Library* (2021): 611-625.
27. Ghelani, Harshitkumar. "Revolutionizing Visual Inspection Frameworks: The Integration of Machine Learning and Energy-Efficient Techniques in PCB Quality Control Systems for Sustainable Production." *International Journal of Advanced Engineering Technologies and Innovations* 1: 521-538.