SALT

Open Banking and PSD2: Securing Financial APIs

PSD2 increases competition and innovation in the European payments market by requiring banks to provide APIs for third-party providers (TPPs) to access customer account information. It mandates Strong Customer Authentication (SCA) for online transactions using multi-factor authentication (MFA). Additionally, PSD2 requires secure authentication and authorization for financial APIs, ensuring transaction integrity. By complying with PSD2, banks can foster innovation in financial services while safeguarding customer data and preventing fraud.

- Strong Customer Authentication (SCA):
  - Use of multi-factor authentication (MFA) to verify user identities.
  - Implementation of secure authentication protocols like OAuth 2.0.
  - Dynamic linking of transactions to protect against fraud.
- Open API Standards:
  - Development and publication of standardized APIs for TPP access.
  - Implementation of secure communication channels for API access.
  - Adherence to industry best practices for API security.
- API Security:
  - Implementation of secure authentication and authorization mechanisms.
  - Encryption of sensitive data in transit and at rest.
  - Regular security testing and vulnerability assessments.

Why It Matters: PSD2 compliance is essential for securing financial transactions and protecting customer data in the open banking ecosystem. Non-compliance can lead to financial penalties, legal action, and damage to a financial institution's reputation, hindering innovation and eroding customer trust.

API Security Requirements:

- **OAuth 2.0 & mTLS:** APIs must enforce secure authentication.
- **Rate Limiting:** Prevent DDoS and API scraping attacks.

Relevant Sections Referencing APIs:

- **Article 30:** APIs must enforce secure authentication and access control.

How Salt Security Helps: Salt Security helps financial institutions comply with PSD2 by providing API discovery, vulnerability assessment, and threat protection. Its authentication and authorization enforcement features ensure secure access to financial APIs, supporting the implementation of Strong Customer Authentication (SCA) and other PSD2 requirements. Security's data security feature provides visibility into sensitive financial data in motion through APIs, which is essential for fraud prevention and PSD2 compliance. Learn more about API Security and Compliance in our **White-paper.**