Open Banking Security Framework

* TLS 1.2+ required
* Certificate pinning
* mTLS for API calls

eIDAS Certificates:
- QWAC: Website authentication
- QSEAL: Message signing
- Issued by qualified TSPs
- Required for PSD2 API access

* eIDAS certificates
* SCA (2-factor auth)
* OAuth 2.0 + OIDC

* Consent management
* Scope-based access
* Token lifecycle

* Encryption at rest
* Data minimization
* GDPR compliance

Common Threats:
- Man-in-the-middle attacks
- Token theft/replay
- Phishing for consent
- Screen scraping fallback
- API abuse/DoS

* API logging
* Fraud detection
* Incident response

Compliance Requirements:
- PSD2/RTS Technical Standards
- eIDAS Regulation
- GDPR (data protection)
- National cybersecurity laws

Source: PSD2 RTS, EBA Guidelines on ICT and Security Risk Management