

# OPEN BANKING & API SECURITY.

PSD2 requires banks to expose account data and payment initiation to licensed third parties through APIs, with the customer's explicit consent. **The security model shifts from a closed system to a verified, scoped, and cryptographically authenticated one — not an open door.**

- OPEN BANKING APIS
- STRONG CUSTOMER AUTHENTICATION
- DYNAMIC LINKING
- TPP IDENTITY VERIFICATION

## 01 THE MECHANISM

**Three Roles, One API**

A bank exposes account data and payment initiation through APIs to licensed third parties — **account-information providers that read data and payment-initiation providers that move money** — both requiring explicit customer consent.

**Strong Customer Authentication, Dynamically Linked**

PSD2 mandates two-factor authentication for most account access and payments, with payment codes **cryptographically tied to the specific amount and payee** so a captured code can't authorize a different transaction.

**Dedicated APIs Replace Screen Scraping**

Third parties are meant to connect through a bank's dedicated Open Banking API rather than **logging in with the customer's actual banking credentials** to scrape data from the consumer portal.

## 02 THE FLOW

**The Properly Authenticated TPP Connection** CONTAINED

1

A licensed third party authenticates to the bank's API using a **qualified certificate that cryptographically proves its regulated identity**, not a password.

2

The customer's consent is scoped, time-limited, and independently revocable, with **every access logged against exactly what was authorized**.

3

A payment initiated through the API carries an authentication code **dynamically linked to that specific amount and payee**, so it can't be replayed.

**The Screen-Scraping Fallback** EXPOSED

1

A third-party app asks the customer to enter their **actual online banking username and password** directly into the app, bypassing the bank's own login flow.

2

The app now holds a credential that can access the **full banking portal, far beyond** whatever narrow scope the customer actually intended to authorize.

3

A breach of the third-party app exposes not just collected data, but **a working credential to the customer's real banking session**.

## 03 CORE PILLARS & COVERAGE

| PILLAR                               | WHAT IT COVERS                                                                                                                                                            |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Strong Customer Authentication (SCA) | Two-factor authentication required for account access and payments, with payment codes dynamically linked to a specific amount and payee.                                 |
| TPP Identity Verification            | Licensed third parties authenticate to bank APIs using eIDAS-based qualified certificates, letting a bank cryptographically confirm it's talking to a regulated provider. |
| Consent Management                   | Scoped, time-limited, auditable customer authorization that can be revoked at any time, with every API access traceable against what was actually granted.                |
| Dedicated API Availability           | Bank-provided APIs robust enough to make the screen-scraping fallback interface genuinely unnecessary.                                                                    |

## 04 DETECTION APPROACHES COMPARED

| APPROACH                                                                            | SUFFICIENT ALONE? | WHAT IT MISSES                                                                                                                                 |
|-------------------------------------------------------------------------------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Screen Scraping With Customer-Provided Bank Credentials                             | No                | Gives the third party a working credential to the full banking portal, far beyond any narrow scope the customer intended to authorize.         |
| Static Authentication Codes Not Linked to Transaction Details                       | No                | A captured or replayed code could be reused to authorize a different amount or payee than the one the customer actually approved.              |
| Unlicensed or Unverified Third-Party Access                                         | No                | Without cryptographic proof of a regulated identity, a bank has no way to confirm it's talking to a licensed provider rather than an imposter. |
| Broad, Indefinite Consent With No Revocation Path                                   | No                | Consent that can't be scoped, checked, or revoked leaves customers unable to actually control what a third party continues to access.          |
| Dedicated API + Qualified Certificates + Dynamically Linked SCA + Auditable Consent | Yes               | Matches what PSD2's technical standards were actually built to require.                                                                        |

OPEN BANKING & API SECURITY.

VERIFY · CONSENT · LINK

05 PROGRAM OPERATIONS

Screen scraping requires a third party to hold the customer's actual banking credentials — exactly the anti-pattern PSD2's technical standards were designed to eliminate in favor of dedicated APIs.

Dynamic linking ties a payment authentication code to a specific amount and payee, not just proof that authentication happened at some point — a subtle but important distinction from generic MFA.

A licensed third party authenticates with a qualified certificate, not a password, so a bank can cryptographically verify it's talking to a regulated provider before granting access.

Opening account data and payment initiation to third parties genuinely expands the attack surface compared to a closed banking system — the API, and every TPP connected to it, has to be defended.

06 CONTROL MAPPING

PSD2 & REGULATORY TECHNICAL STANDARDS

The EU directive and its technical standards mandating open API access, Strong Customer Authentication, and dynamic linking for payments.

EIDAS QUALIFIED CERTIFICATES (QWAC/QSEALC)

The certificate standards licensed third parties use to cryptographically authenticate their regulated identity to bank APIs.

FAPI SECURITY PROFILE

A stricter OAuth2/OIDC security profile developed specifically for high-value financial APIs, addressing gaps in generic OAuth implementations.

UK OPEN BANKING STANDARD

A more prescriptive, standardized API specification implementing PSD2's requirements domestically, often cited as more consistent than the broader EU rollout.

07 WHAT THIS DOES NOT SOLVE

Inconsistent API Implementations Across Banks

PSD2 mandates that APIs exist, but doesn't fully standardize their design, leaving **real variation in quality across institutions**.

Third-Party Provider Security Itself

Verifying a TPP's regulated identity doesn't guarantee **its own systems are well-secured** once it actually holds customer data or payment capability.

Concentrated Aggregator Risk

A popular TPP connected to many banks becomes a **high-value, concentrated target**, since a single breach can expose data from many institutions at once.

API-Layer Implementation Bugs

Standards like SCA and dynamic linking only work if implemented correctly; a **broken authorization check** can still expose one customer's data to another's session.

08 MYTHS VS. REALITY

|                                                                                                |                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>MYTH</div> <div>"Open Banking means banks have no choice but to expose everything."</div> | <div>REALITY</div> <div>Access is <b>scoped to what the customer explicitly consents to</b>, through a defined API, not a blanket data dump.</div>                                                   |
| <div>MYTH</div> <div>"Screen scraping and API access are basically the same thing."</div>      | <div>REALITY</div> <div>Screen scraping requires holding the customer's actual banking credentials, while API access uses <b>scoped, revocable authorization and a regulated TPP identity</b>.</div> |
| <div>MYTH</div> <div>"Two-factor authentication on a payment is the same everywhere."</div>    | <div>REALITY</div> <div>PSD2's dynamic linking requirement <b>ties the authentication code to the specific amount and payee</b>, which generic MFA doesn't necessarily do.</div>                     |
| <div>MYTH</div> <div>"Any app can become an Open Banking third-party provider."</div>          | <div>REALITY</div> <div>TPPs must be licensed and registered with a national competent authority, <b>authenticating with qualified certificates</b> rather than a generic developer account.</div>   |
| <div>MYTH</div> <div>"Open Banking APIs are all built to the same standard."</div>             | <div>REALITY</div> <div>PSD2 sets requirements, but <b>individual bank API implementations still vary</b> meaningfully in design and consistency across the EU.</div>                                |

09 SPEAK THE PROGRAM — KEY TERMS

ASPSP

Account Servicing Payment Service Provider — the bank or institution that holds the customer's account and is **required to expose it via API**.

AISP

Account Information Service Provider — a licensed third party that can **read account data with customer consent**.

PISP

Payment Initiation Service Provider — a licensed third party that can **initiate a payment directly** from a customer's account with consent.

STRONG CUSTOMER AUTHENTICATION (SCA)

PSD2's **mandatory two-factor authentication requirement** for most electronic payments and account access.

DYNAMIC LINKING

The requirement that a payment authentication code be **cryptographically tied to the specific amount and payee** of that transaction.

QWAC / QSEALC

eIDAS-based qualified certificates that let a licensed third party **cryptographically prove its regulated identity** to a bank's API.