Banfico

Open Banking

With Keycloak and OpenResty

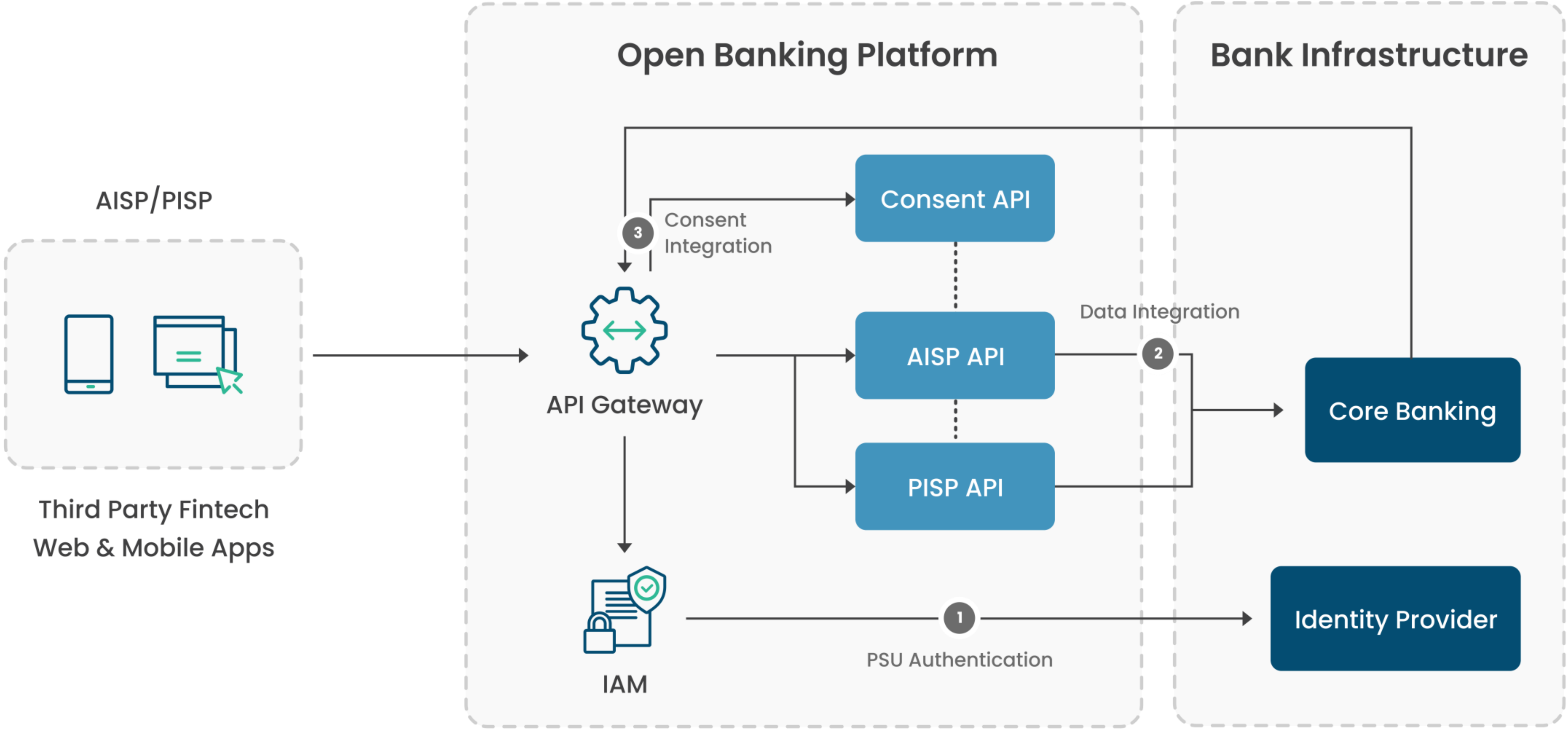
Banfico Ltd.

Open Banking & Key Stakeholders

Open Banking is a system that enables secure sharing of financial data between banks and third-party providers through standardized APIs, with customer consent.

- Banks
- Fintechs
- Regulators
- Customer

Open Banking – High Level



Open Banking – Security for APIs

- **OAuth 2.0 and OpenID Connect Compliance:** Using Keycloak ensures compliance with industry-standard protocols for secure authentication and access control.

- **Fine-grained Access Control:** Keycloak's Role-Based Access Control (RBAC) and policy-based access control (PBAC) allow for granular control over user access to financial data.

- **API Security with OpenResty:** Custom build policies in OpenResty provides additional security layers through API protection mechanisms such as token introspection, rate limiting, IP filtering, and request/response validation.

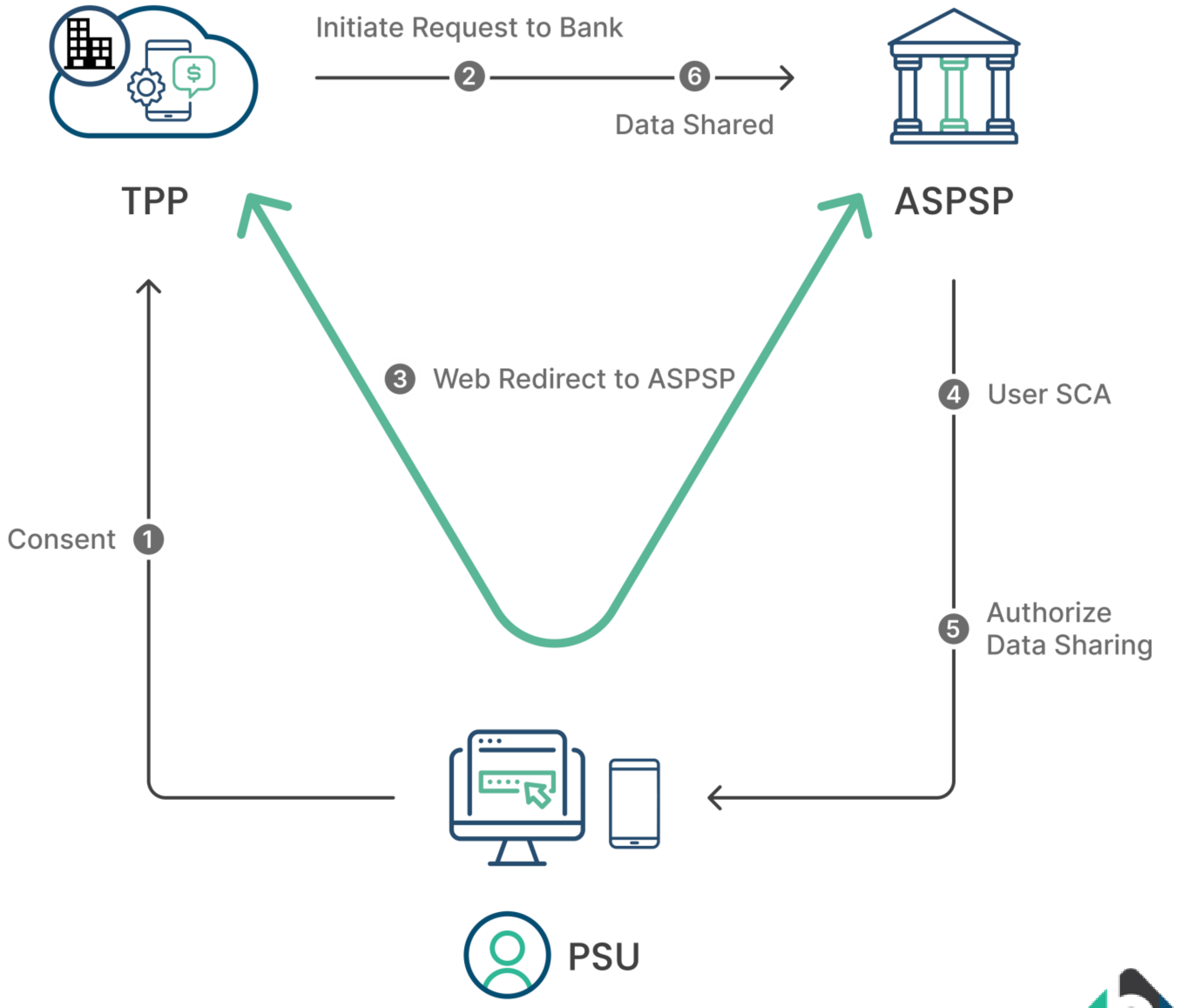
Key Challenges in Implementation

1. Legacy System Integration
2. API Security and PSU Authentication
3. Data Standardization and Interoperability
4. Scalability and Performance Optimization
5. Having Offline Sessions for Long Lived Consents.
6. Different security profiles for each region.
7. Supporting multiple trust framework for each region.

Redirect Authentication – Web/App

Banks should provide “app to app” redirect should it provide mobile app-based authentication. Otherwise, it’s discriminatory and consider as an obstacle to customer experience

TPP tend to favour “app to app” redirect for smooth customer experience

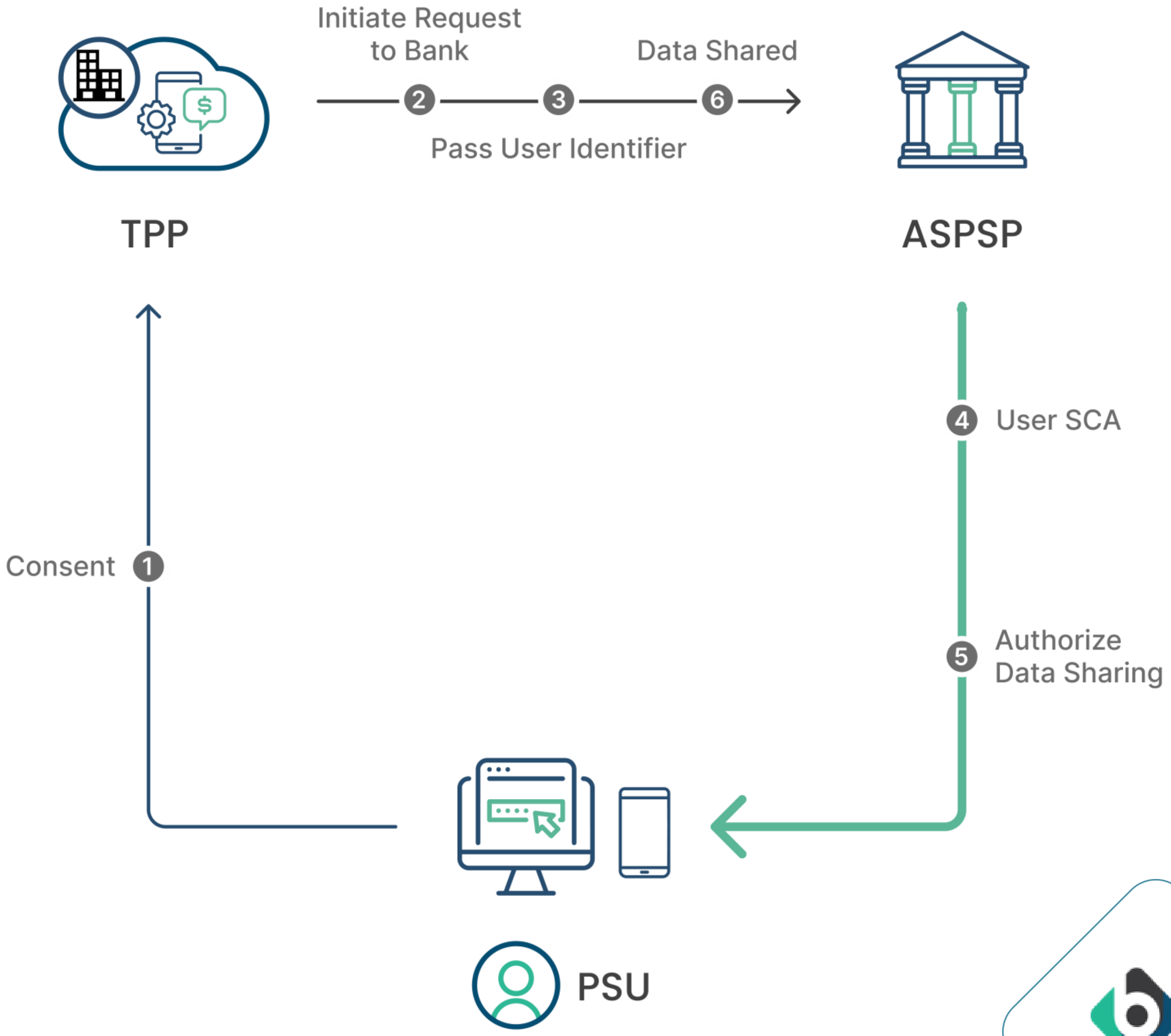


Decoupled Customer Authentication (CIBA)

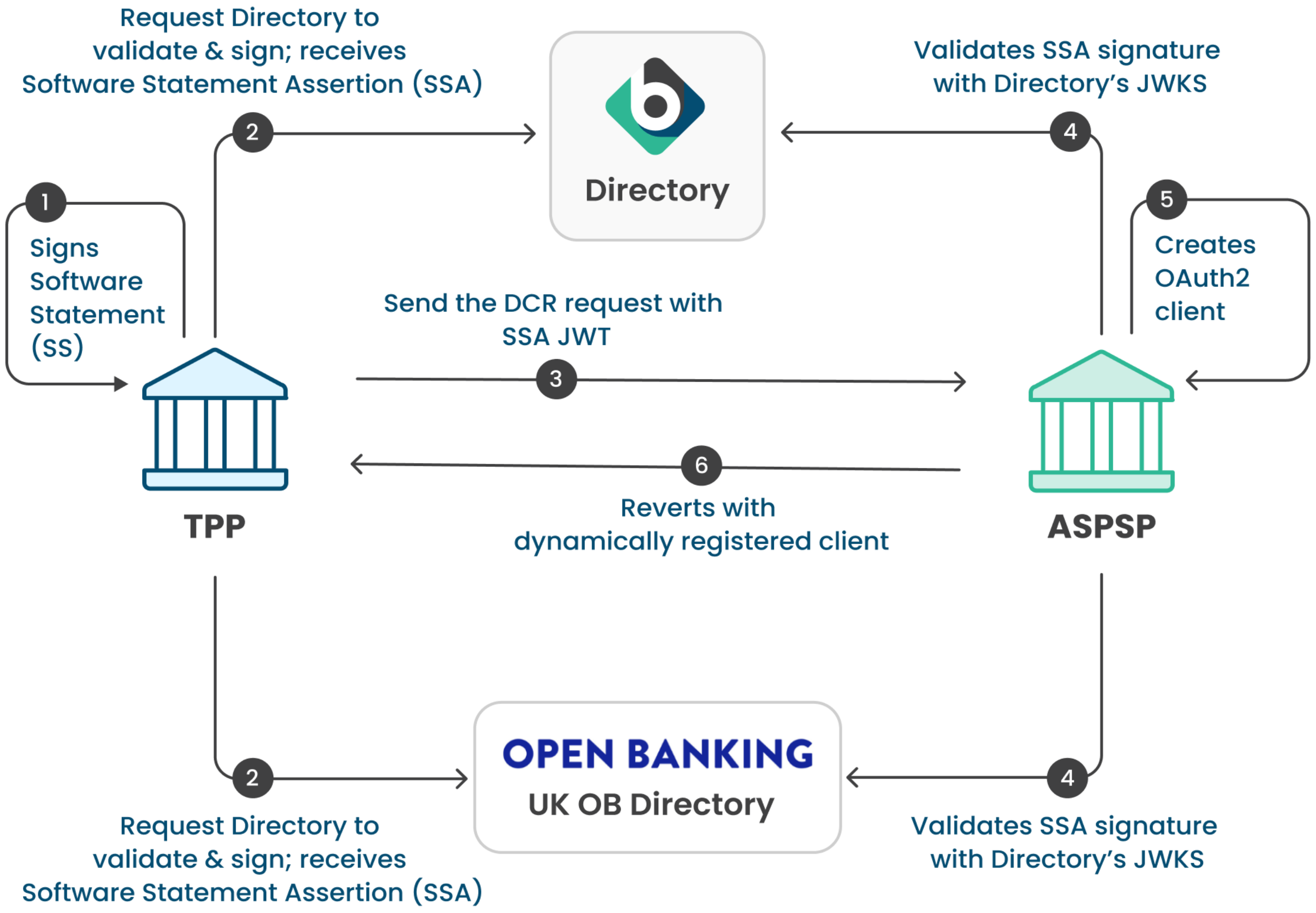
Decoupled is the most Customer Experience friendly. However, it needs a PSU Identifier to trigger the authentication flow. To conform with SCA, it's usually used in conjunction with Embedded SCA

The most commonly used identifiers are

- IBAN
- Registered Mobile Number



Dynamic Client Registration – Multiple Trust Anchors Support


Request Directory to validate & sign; receives Software Statement Assertion (SSA)
2
Directory
Validates SSA signature with Directory's JWKS
4
1
Signs Software Statement (SS)
5
Creates OAuth2 client
Send the DCR request with SSA JWT
3
6
TPP
ASPSP
Reverts with dynamically registered client
2
OPEN BANKING
UK OB Directory
4
Request Directory to validate & sign; receives Software Statement Assertion (SSA)
Validates SSA signature with Directory's JWKS

Where ASPSPs make such changes, they should:

1. A TPP can get SSA from any of the trust anchors.
2. As Banfico authorization server supports multiple trust anchors, it can validate request with appropriate directory.
3. For service desk and notifications, the bank can use Banfico Directory.

Banfico

Thank you!

Banfico Ltd.

1 Canada Square, Level39, Canary Wharf
London E14 5AB

Web: www.banfico.com
Email: openbanking@banfico.com