MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

La «Challenge Sicurezza» nell'era della post PSD2

26/05/2021

La direttiva 2015/2366/UE – PSD2

La direttiva 2015/2366/UE, nota come **PSD2** (Payment System Directive), è un framework regolamentare comune per il mercato dei pagamenti nell'area economica europea avente lo scopo di:

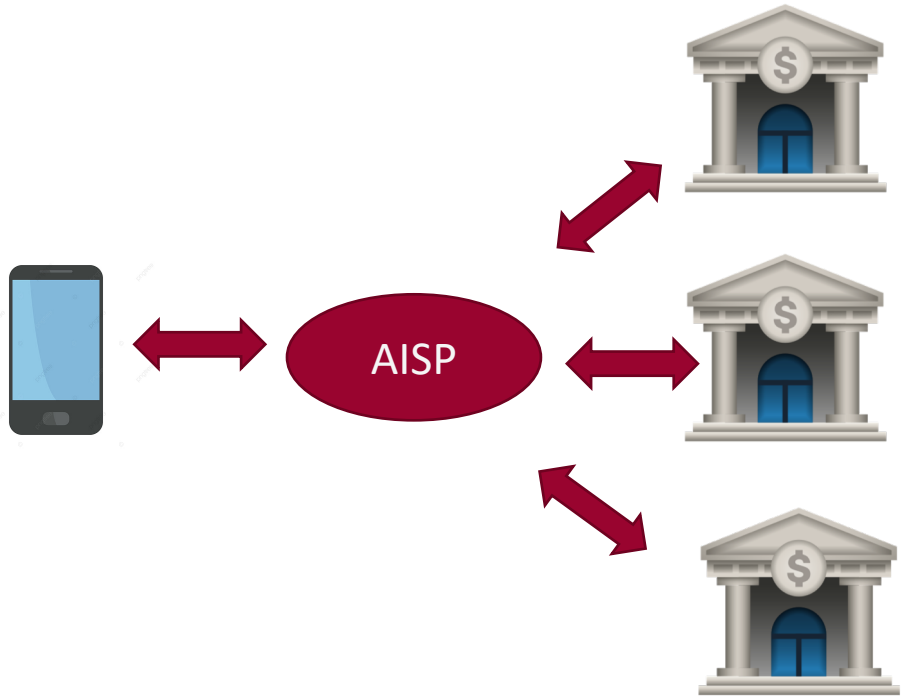
- regolamentare il mercato dei pagamenti, caratterizzato da una complessità crescente in termini di player ed evoluzioni digitali
- ampliare il livello di integrazione ed efficienza dei mercati
- innalzare il livello di fiducia e protezione del consumatore attraverso l'introduzione/impiego di nuovi paradigmi di sicurezza.

La direttiva viene recepita in Italia con il Decreto Legislativo del 15 dicembre 2017, n. 218, pubblicato sulla Gazzetta Ufficiale n. 10 del 13 gennaio 2018.

Nuovi servizi online

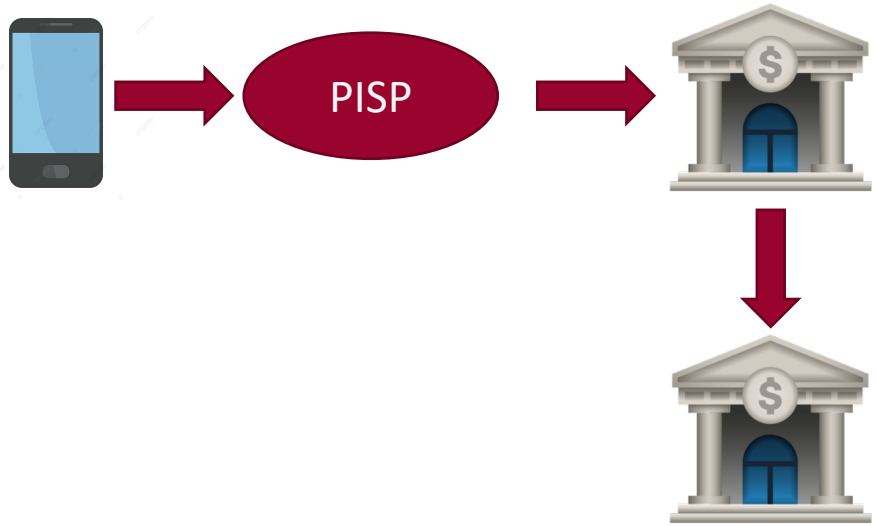
Account Information Service - AIS

Servizio online che fornisce **informazioni consolidate** relativamente a uno o più conti di pagamento di proprietà dell'utente



Payment Initiation Service – PIS

Servizio online che **dispone l'ordine di pagamento** su richiesta dell'utente relativamente ad un conto di pagamento detenuto presso un altro prestatore di servizi di pagamento (ASPSP)



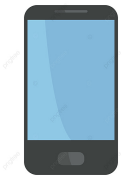
Nuovi attori

Viene richiesta ai Payment Service Provider (PSP) con servizi online di accesso ai conti di radicamento, di fornire almeno un'interfaccia di accesso che consenta un dialogo sicuro con le terze parti (TPP): prestatori di servizi di informazione sui conti, prestatori di servizi di disposizione di ordini di pagamento, prestatori di servizi di pagamento.

Prestatori di servizio di pagamento di radicamento del conto

ASPSP - Accounting Service Payment Service Provider

Terze Parti (TPP)



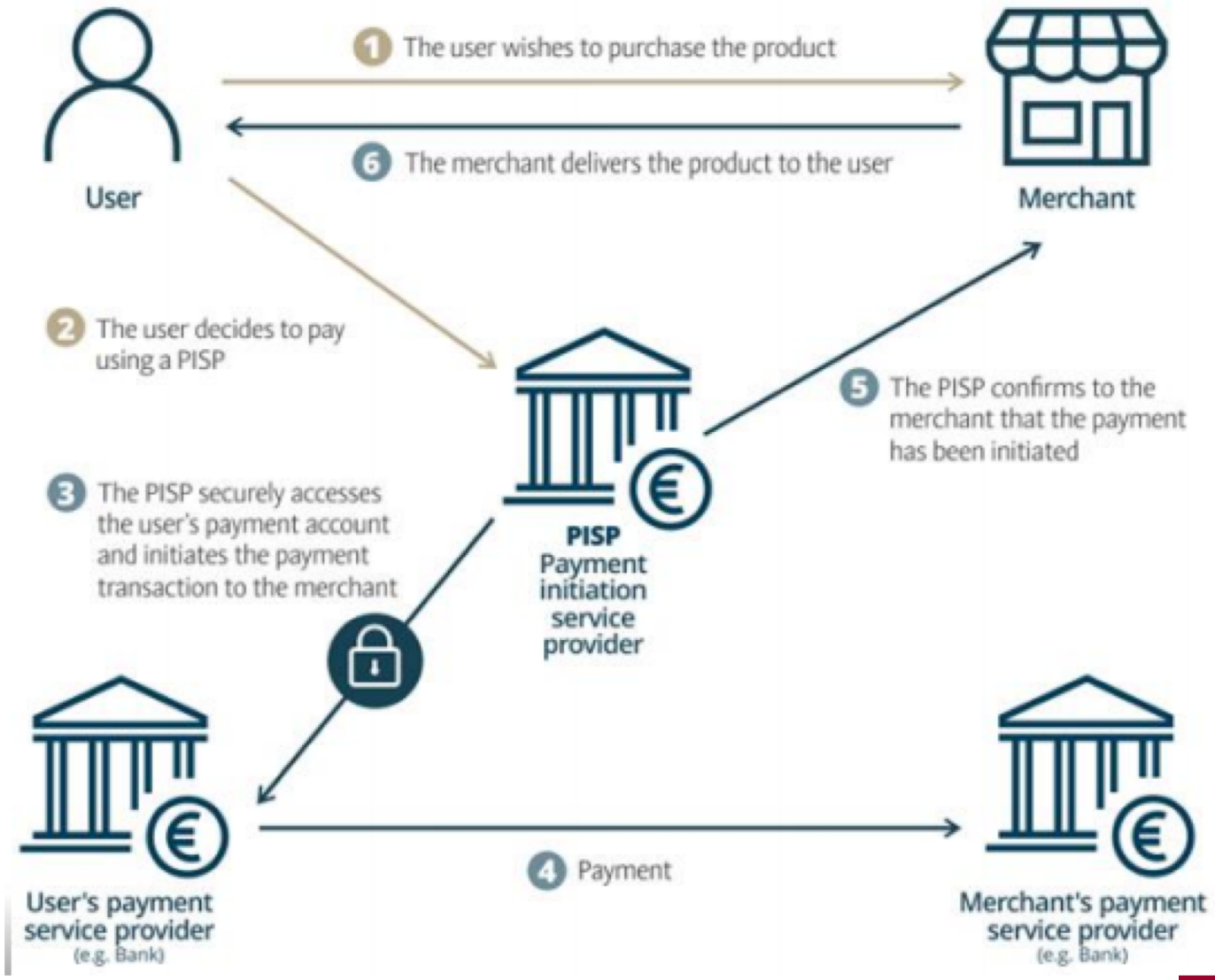
Account Information Service Provider - AISP
Payment Initiation Service Provider - PISP
Card Issuer Service Provider - CISP

L'ecosistema che include: Banche, Istituti di pagamento e Terze Parti, dovrà garantire – a vantaggio della collettività – i **requisiti minimi di sicurezza** previsti dalla Normativa PSD2

Diverse realtà di TPP nell'open banking : PISP AISP CISP

PISP - Payment Initiation Service Provider

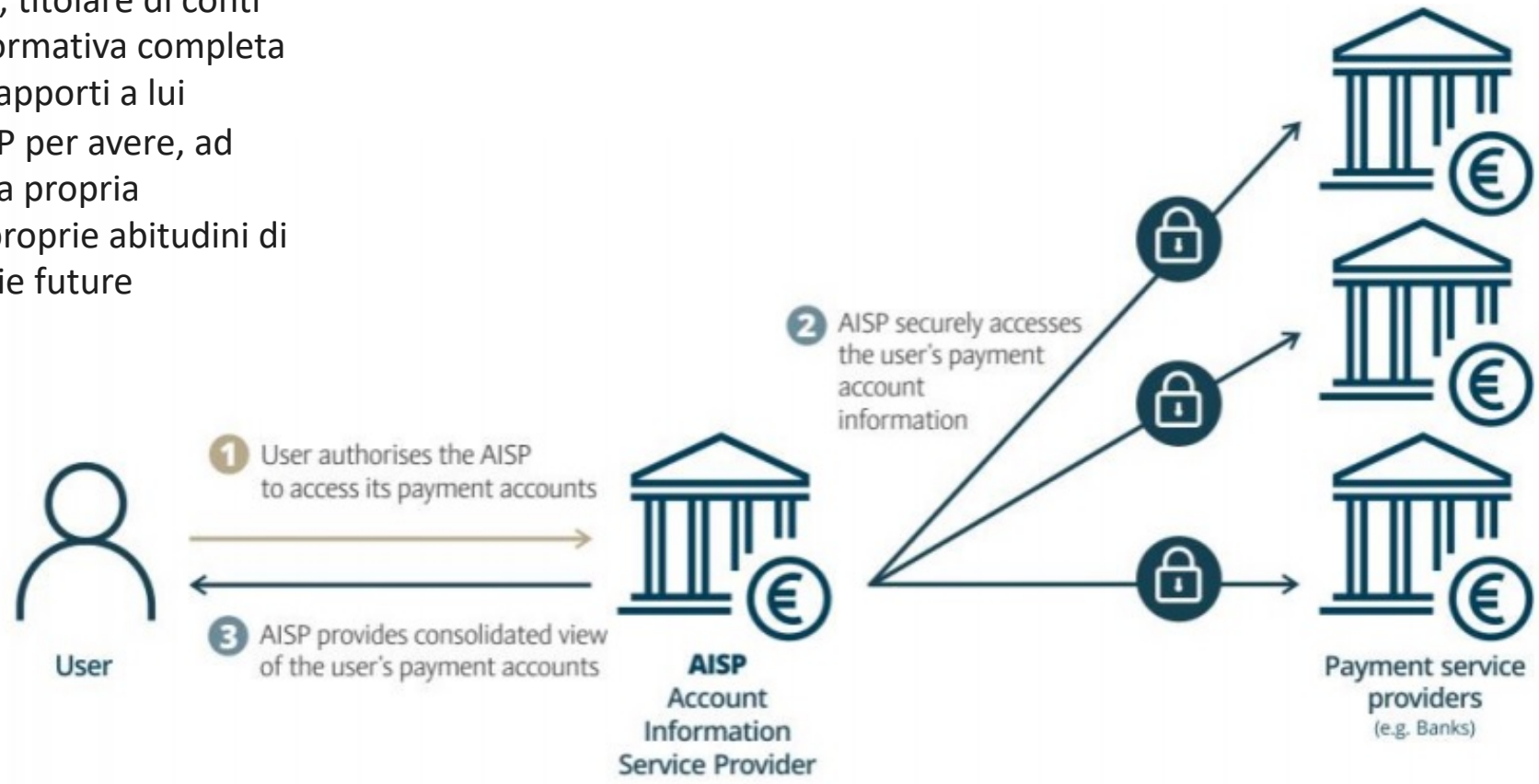
Soggetti che, su espressa autorizzazione del cliente, prestano a favore dell'utente stesso il servizio di disposizione di ordini di pagamento; fungono da tramite tra la Banca ed il titolare del conto di pagamento - accessibile online – e avviano il pagamento a favore di un terzo soggetto, beneficiario della disposizione.
I PISP, ad esempio, permettono all'utente di effettuare un pagamento dal proprio conto ad un venditore, attraverso l'utilizzo di un software 'ponte' tra i due account.



Diverse realtà di TPP nell'open banking : PISP AISP CISP

AISP - Account Information Service Provider

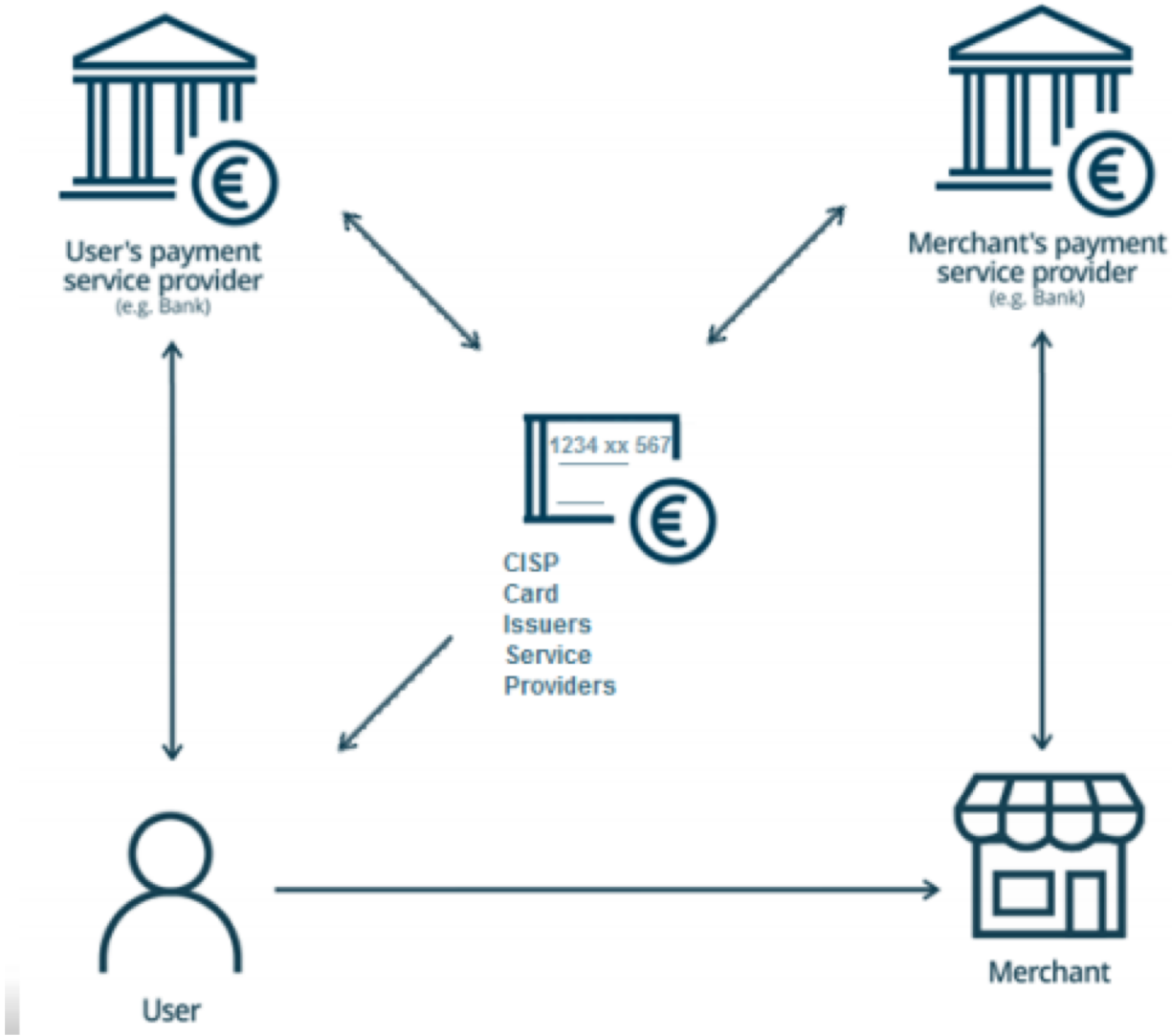
Operatori che consentono all'utente, titolare di conti accessibili online, di ottenere un'informativa completa relativa ai servizi di pagamento dei rapporti a lui intestati. L'utente potrà usare gli AISP per avere, ad esempio, una visione di insieme della propria situazione finanziaria, analizzare le proprie abitudini di spesa e le proprie esigenze finanziarie future



Diverse realtà di TPP nell'open banking : PISP AISP CISP

CISP - Card Information Service Provider

Soggetti che emettono carte di pagamento, regolate su un conto di pagamento accessibile online di un istituto di credito diverso da quello che ha emesso la carta. I CISP non detengono direttamente fondi dei clienti, ma possono interrogare preventivamente la Banca presso cui il conto è attivo, per verificare la disponibilità dei fondi oggetto della transazione disposta.



Elementi innovativi della PSD2 in ambito sicurezza

I Regulatory Technical Standard (RTS) definiscono le linee guida e gli standard di sviluppo della tecnologia e della sicurezza dei nuovi servizi introdotti dalla PSD2. Tra questi spiccano elementi innovativi sui pagamenti, in particolare sugli aspetti di sicurezza ed interfaccia con le altre realtà finanziarie, siano esse Banche, Fin-Tech o Digital Player.

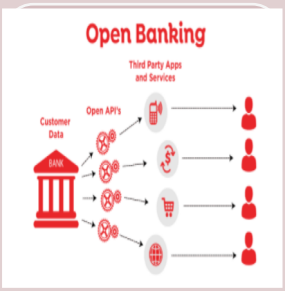
Per quanto riguarda gli strumenti sicurezza , gli elementi principali sono:

STRONG CUSTOMER AUTHENTICATION (SCA)

DYNAMIC LINKING

RIESAME DELLE MISURE DI SICUREZZA DA STRUTTURA INDIPENDENTE

GESTIONE DELLE ESENZIONI NELL'UTILIZZO DELLA SCA



OPEN BANKING

Gateway PSD2 – Insourced vs Outsourced

La PSD2 introduce, in ottica open banking, la necessità di operare attraverso una interfaccia condivisa per dialogare con i vari player del mercato.

Meglio una soluzione interna o esterna per gestire le comunicazioni con le Terze Parti?

La scelta della soluzione «Insourced vs Outsourced» è legata da molteplici fattori:

- ✓ Sicurezza del servizio (autenticazione TPP e PSU)
- ✓ Gestione del consenso
- ✓ Standardizzazione
- ✓ Complessità tecnologica
- ✓ Economie di scala

MODELLO OUTSOURCED

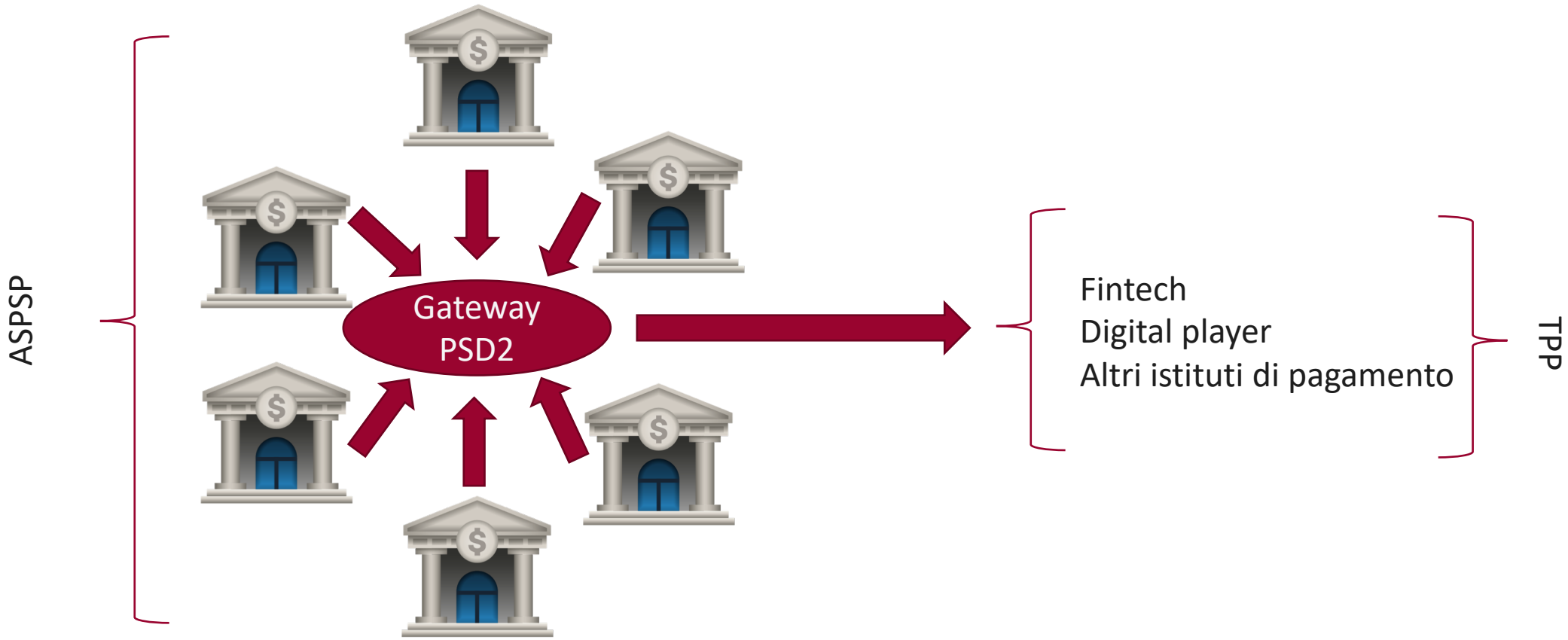
assicura visione comune e livelli di sicurezza condivisi tra realtà appartenenti allo stesso settore, ottimizzazione di costi e di scelte tecnologiche nonché standardizzazione

MODELLO INSOURCED

assicura un pieno controllo della soluzione, possibilità di personalizzazioni spinte, costi elevati e difficoltà di mantenimento della soluzione a seguito di novità

Terze parti - TPP

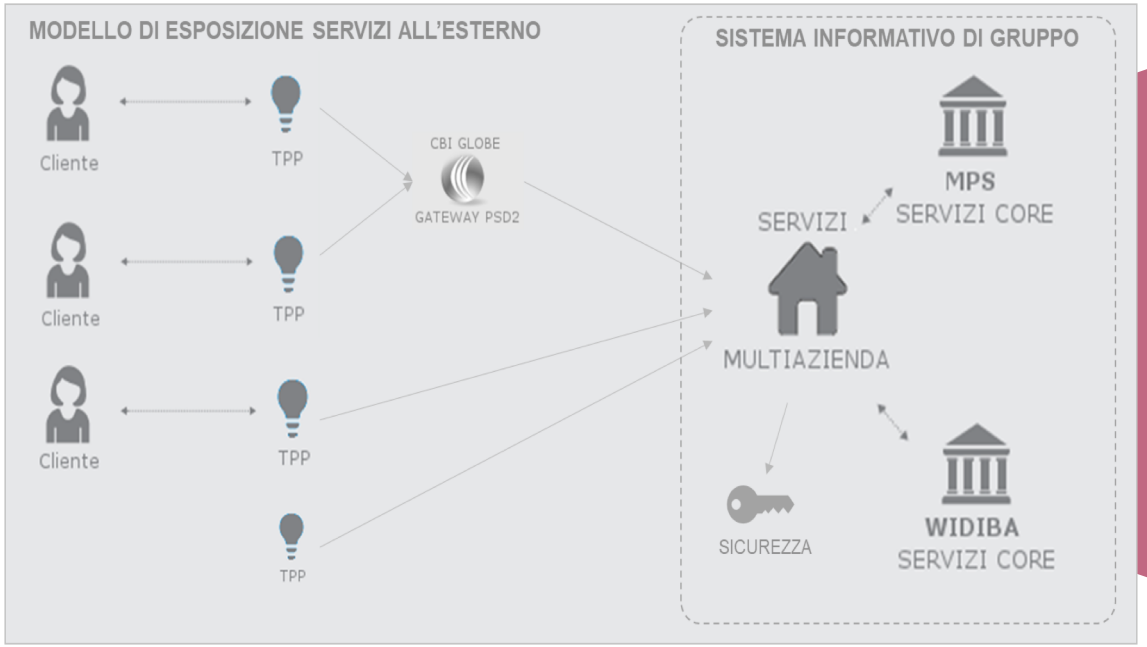
Banca MPS si avvale del supporto di un Consorzio che ha realizzato una soluzione tecnico-operativa – c.d. GATEWAY PSD2 CBI – in grado di facilitare l'interconnessione fra ASPSP e TPP ed efficientare gli investimenti dei soggetti aderenti mediante la centralizzazione di servizi comuni (riconoscimento TPP, monitoraggio attività e reporting, Help Desk, gestione dispute, TRA, aggiornamento soluzione...)

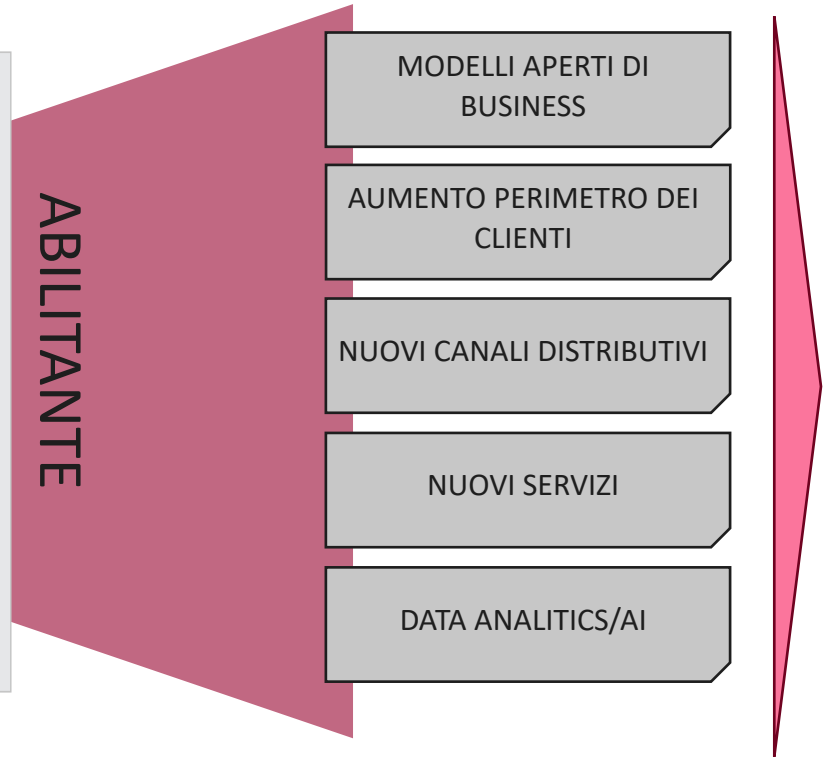


Open Banking – Architettura unica

L'architettura unica sviluppata per Open Banking abilita la condivisione di dati e funzionalità, tra i diversi attori dell'ecosistema bancario, per consentire alla Banca di esporre servizi esterni sotto forma di API come canale alternativo a quelli tradizionali.

Il nuovo canale Open Banking si integra quindi all'interno del Sistema Informativo di Banca Monte dei Paschi di Siena e Banca Widiba con un'architettura e infrastruttura centralizzata in grado di gestire le esigenze di Sicurezza, Trattamento dei dati e Livelli di servizio del canale stesso.





Servizi esposti verso l'esterno:

- Nexi (Informazioni clienti per carte)
- CBI Globe (Check IBAN)
- Facile.it (Servizi Axa)
- Experian (Servizi anagrafici)

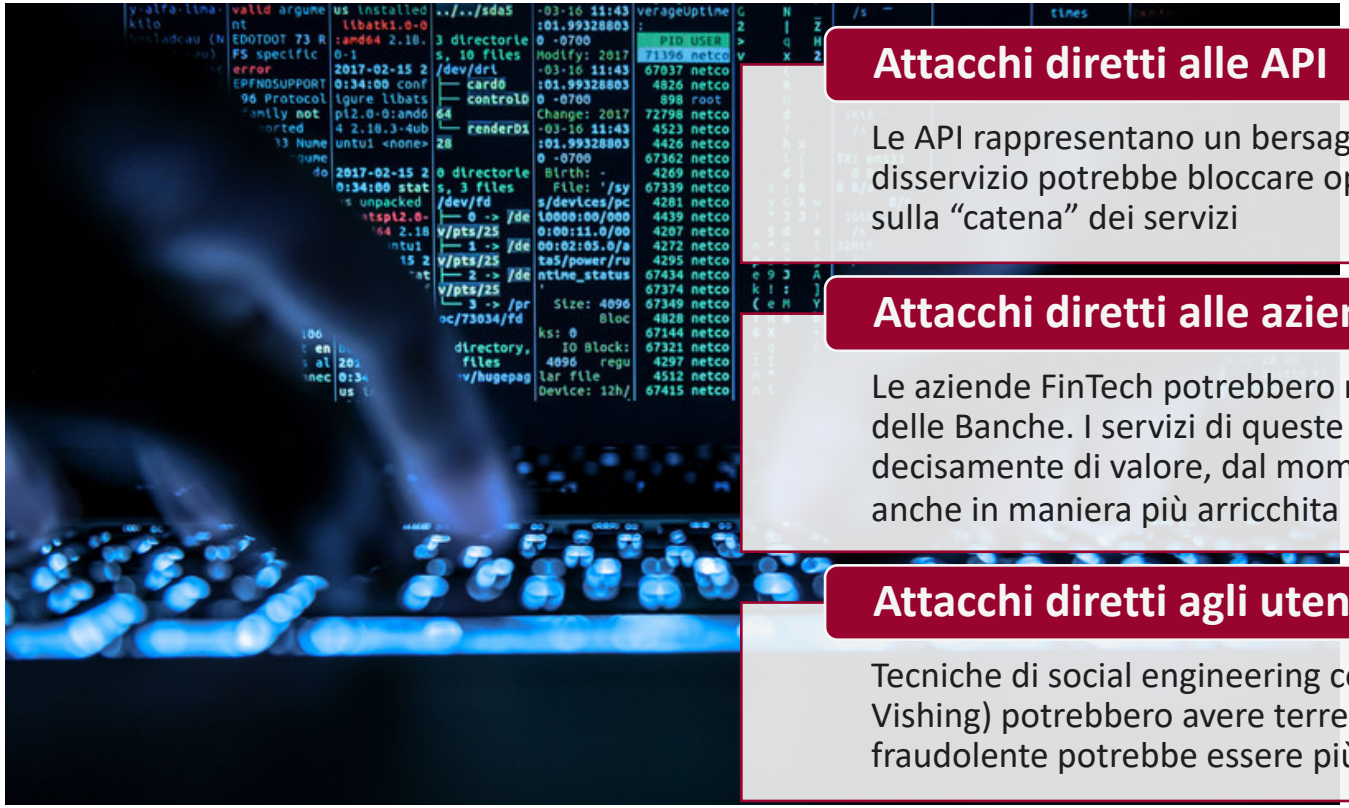
Servizi fruiti all'esterno

- Account Aggregator (Consultazioni conti e carte della Clientela)

PSD2 Open Banking e nuove sfide sicurezza

Obiettivo del paradigma Open Banking è quello di innovare il meccanismo delle transazioni bancarie all'interno dell'Unione Europea cercando di renderle più efficienti, meno costose, intuitive e più sicure. Tutto questo grazie alla attivazione di **interfacce di programmazione (API) delle banche nei confronti delle aziende FinTech**, che garantiscono l'estensione di servizi come i suggerimenti finanziari o l'automazione dei pagamenti.

Il nuovo paradigma di servizi, crea opportunità ma genera preoccupazione in ambito sicurezza, alcuni rischi di attacco:



Attacchi diretti alle API

Le API rappresentano un bersaglio dovendo essere necessariamente pubbliche. Qualsiasi disservizio potrebbe bloccare operazioni e transazioni bancarie, con ripercussioni sostanziali sulla "catena" dei servizi

Attacchi diretti alle aziende FinTech

Le aziende FinTech potrebbero non tutte possedere gli stessi livelli di sicurezza ed esperienza delle Banche. I servizi di queste aziende potrebbero diventare un bersaglio facile e decisamente di valore, dal momento che contengono dati finanziari della propria clientela anche in maniera più arricchita del conto di radicamento originario

Attacchi diretti agli utenti finali

Tecniche di social engineering combinate con quelle di phishing (e sue varianti Smishing e Vishing) potrebbero avere terreno fertile presso i fruitori dei servizi. Nei casi di transazioni fraudolente potrebbe essere più difficile individuare le responsabilità.

Evoluzione Reportistica Frodi EBA

La PSD2 definisce un framework dettagliato ed articolato riguardante le frodi, quindi maggiore standardizzazione nella rappresentazione e nella gestione/analisi delle informazioni raccolte da parte delle Autorità di Controllo.

La normativa prevede la produzione e l'invio di una **reportistica periodica** (a cadenza **semestrale**) a Banca d'Italia secondo lo schema EBAF.

Al fine di ridurre gli oneri segnaletici, la base informativa EBAF sarà dismessa dopo la segnalazione dei dati riferibili dalla data contabile del **31 dicembre 2021** e confluirà nella segnalazione «*statistiche sui servizi di pagamento*» con cadenza **trimestrale**. Verrà predisposto un nuovo framework di segnalazione, attualmente in corso di sviluppo da parte di Banca d'Italia.

Gestione degli Incidenti

La PSD2 interviene anche in tema gestione degli incidenti con un maggiore rafforzamento del presidio degli incidenti di sicurezza lato strumenti di pagamento (nelle sue componenti: classificazione incidenti, segnalazioni a BdI).

In ambito servizio Open Banking diventa centrale il tema della gestione dei gravi incidenti visti i tempi stringenti richiesti per la segnalazione.

Nel caso di outsourcing del modello Open banking, la presenza di un player che tramita il servizio rende difficile l'individuazione delle responsabilità in caso di incidente e la raccolta di informazioni utili a dimensionare correttamente l'incidente per poterlo classificare.
Risulta fondamentale definire un Protocollo di comunicazione e di azioni tra Banca e Fornitore Open Banking per ottimizzare i tempi della gestione

Tutela del cliente

Le soluzioni tecnologiche adottate da **Banca Monte dei Paschi di Siena** e **Banca Widiba** in ambito Open Banking (sia per i servizi obbligatori che per le iniziative innovative) garantiscono **piena conformità** e supporto per le modalità di autenticazione e autorizzazione delle operazioni previste dalla normativa e dai più **elevati standard di sicurezza**, con particolare riferimento alla **strong customer authentication** (SCA) basata su combinazioni dei fattori di conoscenza (password), inerenza (biometria – face-id/fingerprint) e possesso (SMS su cellulare convalidato, mobile token).

Recependo le previsioni della Direttiva, i contratti dei conti di pagamento offerti alla clientela sono stati integrati con le sezioni che disciplinano l'accesso ai conti in caso di utilizzo da parte del cliente dei servizi di: i) disposizione di ordini di pagamento; ii) informazione sui conti; iii) conferma della disponibilità dei fondi ai prestatori di servizi di pagamento emittenti strumenti di pagamento basati su carta.

L'accettazione delle credenziali di sicurezza personalizzate avviene in maniera analoga all'accesso diretto ai portali della Banca. Il cliente viene reindirizzato sulle interfacce della Banca (SCA redirect) che consente al cliente di inserire le proprie credenziali in un ambiente protetto.

La reciproca autenticazione fra Terze Parti e Banca è basata sul protocollo TLS, così come la crittografia dei dati scambiati. È previsto il riconoscimento reciproco con certificati eIDAS

Nell'ambito del canale Open Banking le piattaforme di sistema adottate permettono la corretta **gestione del ciclo vita dei consensi** forniti dal cliente per autorizzare le Terze Parti all'utilizzo dei servizi AISP, PISP, CISP, tracciando le scadenze degli stessi e mettendo a disposizione del cliente le funzionalità online per la **consultazione, conferma e revoca dei consensi rilasciati**.

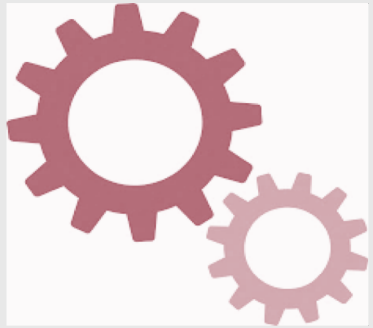
Inoltre, con particolare riferimento alle iniziative di «banca attiva», la Banca applica ai dati per i quali il cliente ha fornito il consenso (ad es. saldo e movimenti di carte prepagate e conti aperti presso altre banche) i **medesimi livelli di privacy, garanzie e criteri previsti dal GDPR**[1] sui dati direttamente gestiti dalla Banca stessa (ad es. saldo e movimenti di conti aperti presso la Banca).

Sicurezza

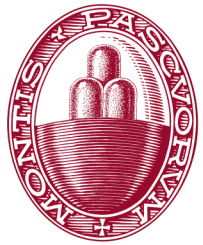
Banca Monte dei Paschi di Siena e **Banca Widiba** investono costantemente sull'introduzione di **strumenti antifrode** evoluti, specializzati nella **prevenzione** delle diverse tipologie di attacco possibili, e sull'adozione di piattaforme di **monitoraggio e analytics** per garantire un costante seguimento e rendicontazione dei **tentativi di frode** sui canali digitali (incluso l'Open Banking).

Il modulo di *Fraud Detection,* presente nell'interfaccia dedicata, consente il monitoraggio e l'analisi delle transazioni dispositive messe in atto dal cliente, ovvero disposizioni di pagamento online con addebito diretto sul conto bancario del cliente a favore di beneficiari anche tramite TPP.

La piattaforma antifrode permette, tramite regole native di prodotto che si aggiornano nel tempo, regole impostate dagli operatori, di indentificare transazioni fraudolente o a rischio frode (le transazioni vengono classificate con diversi gradi di rischio) che possono poi essere analizzate dagli operatori del team antifrode per eventuali approfondimenti sulle singole transazioni o per blocco o conferma delle stesse.



Sono stati definiti i **dati sensibili di pagamento** ("dati utili per perpetrare frodi ai danni del Cliente"), per accedere ai quali è sempre richiesta autenticazione forte. A tutela della confidenzialità delle informazioni trasmesse, il Gruppo Montepaschi adotta sistemi di cifratura end-to-end e adeguate tecniche crittografiche. I dati "sensibili" relativi ai pagamenti non sono mai inclusi in eventuali sms o e-mail inviate al cliente.



MONTE
DEI PASCHI
DI SIENA
BANCA DAL 1472