www.pwc.com/it/psd2

Il colloquio tra Third Party Provider e le Banche.
Quale sarà l'impatto tecnologico?

Pillola di PSD2 n° 2

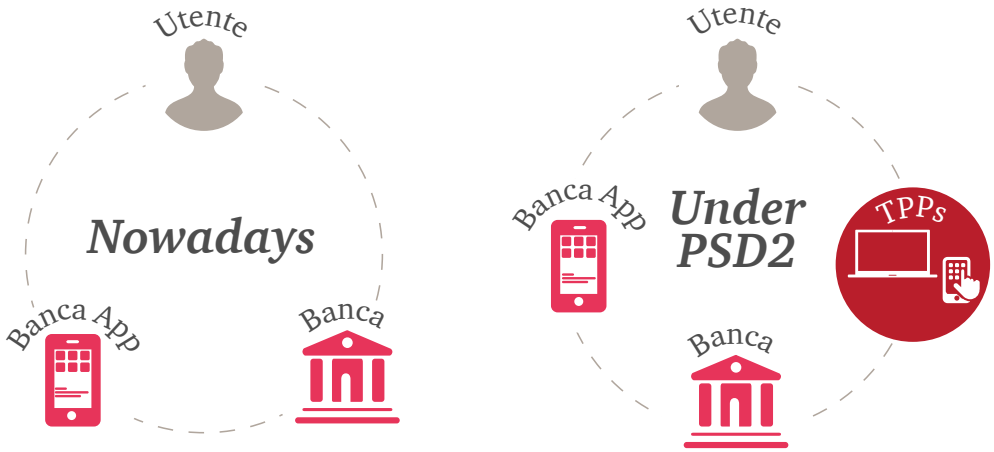
pwc

Summary

Il sistema bancario si trova ad una svolta decisiva, sotto la pressione del mercato e di emergenti operatori che introducono una forte spinta tecnologica; in tale contesto le Banche dovranno decidere se competere per mantenere il rapporto diretto con la propria clientela o limitare il proprio ruolo a provider di servizi bancari.

L'entrata in vigore della nuova **direttiva sui servizi di pagamento** (PSD2), introduce, infatti, per gli utenti che utilizzano un conto corrente online la possibilità di effettuare pagamenti o accedere alla rendicontazione bancaria attraverso software realizzati da terze parti autorizzate (PISP e AISP).

I nuovi player, se autorizzati, potranno operare sui conti correnti degli utenti finali, introducendo con tutta evidenza il rischio di disintermediazione tra le Banche e la propria clientela.



Tale apertura verso il mercato permetterà, sfruttando le interfacce di accesso ai conti correnti che le Banche dovranno rendere disponibili, di sviluppare nuovi servizi ai clienti anche grazie all'integrazione e alla cooperazione con altri attori dell'ecosistema.

L'aumento di c**omplessità nella catena del processo dei pagamenti** e l'esigenza di assicurare **maggiore sicurezza ai pagatori** sono alla base dei presidi che la Direttiva richiede di inserire:

1. **Standard sicuri per il colloquio tra *Third Party Provider* e Banche**
   I provider di servizi di pagamento autorizzati dai clienti finali dovranno essere abilitati all'accesso ai conti correnti online attraverso interfacce facilmente integrabili.
   Il principio appartenente alla nuova cornice regolatoria rappresenta nel contempo un'opportunità di mercato ed un elemento di grande preoccupazione per le Banche più tradizionali che rischiano una disintermediazione dalla loro clientela.

2. **Armonizzazione e rafforzamento del processo di autenticazione**
   L'utilizzo di stringenti standard di sicurezza, nel rispetto delle disposizioni BCE, diventa un requisito obbligatorio, che richiede l'accertamento dell'identità attraverso due o più strumenti di autenticazione, rafforzato dall'utilizzo di link dinamici che certifichino l'unicità della transazione.

Focus su standard sicuri per il colloquio tra Third Party Provider e Banche

Il più significativo impatto sul piano tecnico riguarda la richiesta della direttiva di facilitare le operazioni di accesso ai conti da parte di provider esterni, per la raccolta di informazioni o per l'elaborazione di un pagamento.

Risultano evidenti i contrasti tra le potenzialità derivanti dallo sviluppo di un linguaggio comune tra Banche e terze parti coinvolte nelle operatività di pagamento, ed il rischio di definire standard troppo rigidi che imbriglino la futura innovazione.

Per consentire che il colloquio tra le parti possa avvenire con criteri omogenei e certificati, è stato demandato ad EBA l'incarico di indirizzare i requisiti per la comunicazione di standard quanto più possibile aperti all'innovazione, attraverso la pubblicazione dei Regulatory Technical Standards.

A tal proposito la versione definitiva dell'RTS in materia di "Strong Customer Authentication and Secure Communication" verrà rilasciato entro il 13 Gennaio 2017, mentre un Consultation Paper è atteso per agosto 2016.

Qualunque sia la tecnologia che si deciderà di adottare per definire gli standard di colloquio tra le parti, la scelta che ogni Banca si troverà a prendere è relativa all'approccio progettuale. Si dovrà decidere se attendere le evoluzioni normative e di mercato (Approccio Reactive) o se anticiparle interpretando la direttiva come un'opportunità di sviluppare il proprio business (Approccio Proactive).

Reactive

L'approccio progettuale orientato al mero adeguamento normativo, potrebbe portare ad attendere l'emissione in forma definitiva dei Regulatory Technical Standards e solo in seguito a recepire le soluzioni più efficaci e di veloce adozione identificate dai competitor e fintech.

Le banche che decideranno di adottare questo approccio rischiano che i competitor ottengano un vantaggio difficile da colmare ed una possibile disintermediazione nei confronti della propria clientela.

Cosa succederebbe se (o quando) uno dei grandi player attivi nei social network dovesse integrare i pagamenti fra i propri servizi?

Se ogni cliente dovesse inserire il codice IBAN nel proprio account social, la maggior parte dei clienti di servizi di pagamento online sarebbe subito attivo, creando potenzialmente la più grande rete tra consumatori finali.

Proactive

L'apertura tecnologica indirizzata dalla direttiva per il sistema bancario è abilitante per la creazione di nuovi servizi e prodotti e per massimizzare il contributo che la comunità fintech sta dimostrando di poter attuare.

Le scelte tecnologiche dovranno sempre più essere coordinate e orientate dagli obiettivi strategici del business.

Porsi come first mover richiede l'avvio di progettualità volte a verificare il disegno architetturale dei propri sistemi software, assicurandosi che siano realmente orientati ai servizi e supportati da un impianto applicativo pronto per sostenere le crescenti esigenze di business e a snellire i processi interni.

Anche le architetture applicative già pronte per la gestione di applicazioni multicanale over internet (ad es. APP) dovranno essere valutate nell'ottica di utilizzo open che la nuova Direttiva richiede.

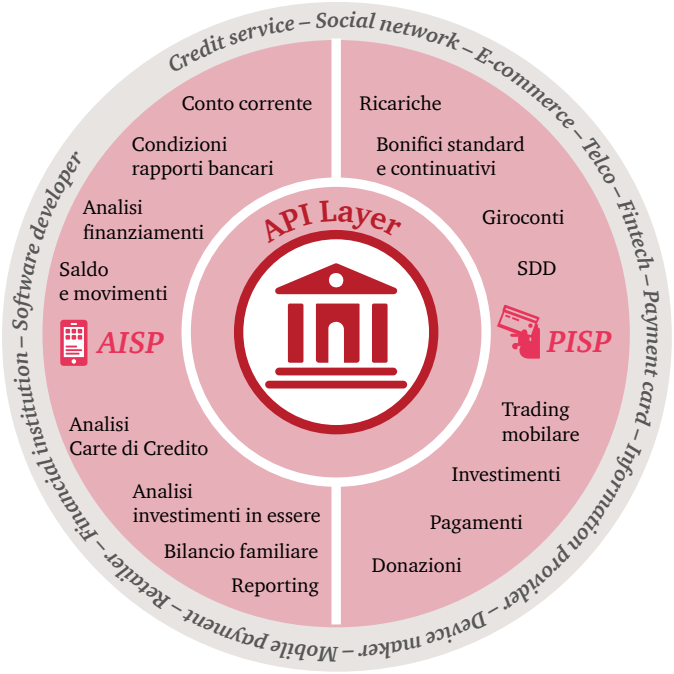
Le API, una via di implementazione

La normativa non indica la tecnologia che le Banche dovranno adottare per il colloquio con le terze parti, delegandone eventualmente il compito all'EBA. Quest'ultima intende orientare le proprie indicazioni nell'ottica di preservare l'innovazione e la cooperazione, evitando di introdurre rigidità non necessarie. D'altro canto, la definizione di uno standard, indirizzato dal regolatore o dal mercato, dovrà necessariamente essere introdotto al fine di non disperdere inutilmente le energie del settore nel riconciliare le diverse interfacce sviluppate in autonomia dagli Istituti.

Anche in presenza di queste aree di incertezza è tuttavia ampiamente condiviso, tra le istituzioni finanziarie e le fintech attive nel settore, che le API potrebbero essere una auspicabile tecnologia da adottare.

Le API rappresentano uno specifico approccio architetturale che garantisce scalabilità, sicurezza e riusabilità del codice. Tale soluzione consentirebbe alle Banche di ridurre i costi di integrazione, aumentandone la velocità e rendendo disponibile una piattaforma di innovazione rivolta anche a sviluppatori e fintech.

La maggior parte delle iniziative legate al mercato digitale sono tecnologicamente basate sulle API, utilizzate nell'ottica di aprire i sistemi alle parti coinvolte nell'ecosistema aumentando il valore del servizio per il cliente finale. Ad esempio, i principali player attivi in ambito social e marketplace hanno adottato le API per rendere disponibili a terze parti funzionalità e design modulare, creando nel contempo valore e dipendenza dai loro sistemi.



L'accesso di terze parti ai conti correnti è già una prassi!

Se il cambiamento richiesto dalla Direttiva, nell'apertura che impone verso il mercato, può sembrare eccessivo, è da considerare che già oggi sono attive applicazioni di terze parti che consentono agli utenti di accedere al proprio conto corrente.

Questo avviene ad esempio attraverso lo *screen scraping*, tecnica che consente di simulare il comportamento del cliente, collegandosi al suo sito di home banking, per disporre operazioni o richiedere informazioni sulla movimentazione.

Tale modalità operativa introduce diversi rischi, non ultimo quello relativo all'integrità delle credenziali della clientela, la cui mitigazione (attraverso la regolamentazione e l'indirizzo di modalità sicure di accesso ai conti corrente) è tra gli scopi principali della Direttiva.

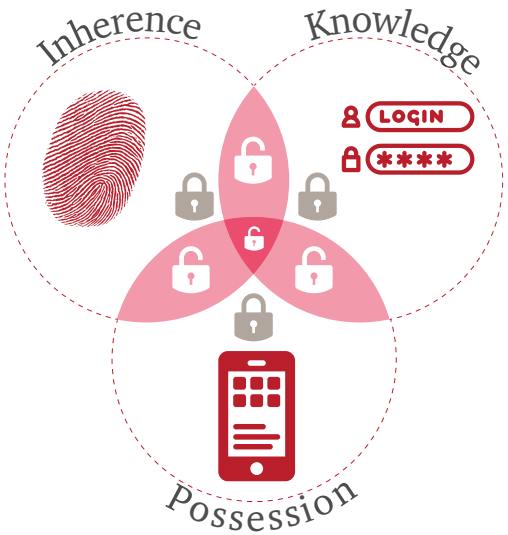
Le Banche potrebbero non sapere se la propria clientela sta già autorizzando delle terze parti ad accedere ai loro conti correnti.

Focus su armonizzazione e rafforzamento del processo di autenticazione

L'esigenza di armonizzazione nell'utilizzo per tutte le Banche di stringenti criteri di sicurezza (Strong Customer Authentication) rappresenta l'altra principale innovazione della Direttiva, ribadita ed anticipata anche dal 16° aggiornamento della circolare 285 di Bankit.

L'identità degli utenti dovrà essere accertata attraverso due o più strumenti di autenticazione classificati come:

- knowledge (qualcosa che solo l'utente conosce, ad esempio un PIN)
- possession (qualcosa che solo l'utente ha, ad es. un Token)
- inherence (qualcosa che solo l'utente è, ad es. l'impronta digitale)



Il 16° aggiornamento della circolare n. 285 del 17 maggio 2016 "Disposizioni di Vigilanza per le banche" introduce la nuova Sezione VII "Principi organizzativi relativi a specifiche attività o profili di rischio" che rende obbligatoria per le Banche l'attuazione dei requisiti riportati negli "Orientamenti finali sulla sicurezza dei pagamenti via Internet" emanata da EBA il 19 dicembre 2014.

Alle Banche è richiesto di documentare l'adozione di misure di autenticazione forte per rafforzare la verifica dell'identità del cliente relativamente alla sicurezza delle transazioni tramite canale remoto. L'adeguamento alla normativa dovrà avvenire entro il 30 settembre 2016 ed entro il 30 ottobre 2016 sarà richiesto alle Banche di trasmettere alla BCE o alla Banca d'Italia una relazione sugli interventi effettuati sulla struttura organizzativa e sui sistemi informativi.

EBA, nell'ottica di presidiare il rischio di compromissione dei requisiti di autenticazione, sta indirizzando i suoi approfondimenti circa l'interdipendenza dei singoli elementi per evitare che l'eventuale violazione di una delle credenziali abbia effetti sulle altre.

La direttiva prevede inoltre che la sicurezza delle operazioni di pagamento sia rafforzata da meccanismi di collegamento dinamico ("dynamic linking") che contengano almeno l'importo ed un beneficiario specifico. Si vuole infatti garantire che l'autenticazione per una transazione a distanza non venga utilizzata per altri scopi rispetto a quanto originariamente previsto dal pagatore.

Sono inoltre in corso valutazioni sulle possibili sinergie tra le procedure di autenticazione sopra citate e gli standard per l'identità digitale adottate dalla pubblica amministrazione e indirizzati dalle normative internazionali (e-IDAS) e nazionali (SPID) che prevedono requisiti fra loro compatibili.

L'eventuale adesione a SPID potrebbe portare benefici alle Banche, tra cui la potenziale possibilità di ampliamento della base della clientela e l'ampliamento dell'offerta di servizi fruibili dagli utenti finali.

Appare evidente l'esigenza di riconciliazione tra le comprensibili richieste di rendere stringenti ed omogenei i criteri di autenticazione e sicurezza con l'esigenza del mercato di rendere sempre più fluidi e senza soluzione di continuità i pagamenti online, anche utilizzando al meglio le possibili esenzioni previste dalla normativa.

Blockchain e Strong Customer Authentication

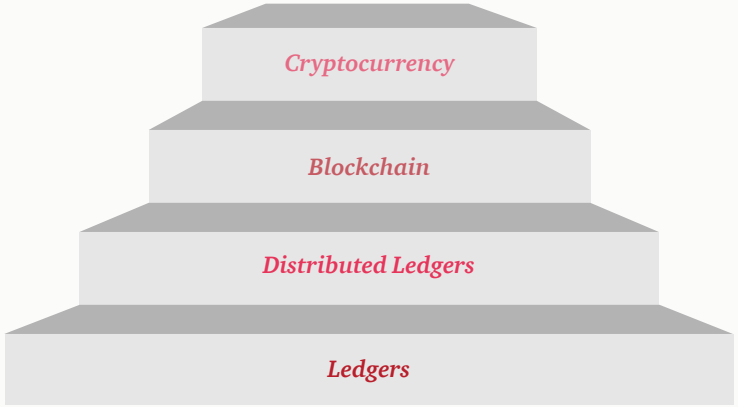
DLT, acronimo di Distributed Ledger Transaction, è una tecnologia che prevede la replica di un ledger dedicato alla gestione di asset tra più entità di pari livello, abilitando le stesse ad effettuare transazioni in contesti trustless senza necessità di intermediari.

Blockchain è una particolare declinazione di DLT che prevede di raggruppare le transazioni in blocchi legati tra loro che consente di conferisce al ledger una caratteristica di immutabilità che garantisce maggior trasparenza e sicurezza.

Molte tecnologie Blockchain gestiscono l'autorizzazione delle transazioni attraverso un'infrastruttura nella quale ad ogni chiave pubblica sono associati degli asset e la relativa chiave privata permette di validare la transazione. Il processo è molto simile a quello della firma digitale, senza l'obbligo di utilizzare una Certification Authority accreditata e consente di utilizzare KeyPair autogenerate, custodite unicamente su un Mobile Device.

Si offre in questo modo la possibilità di considerare il dispositivo come elemento di possesso a cui solo l'utente ha accesso, proprio come i dispositivi OTP attualmente in uso.

Sarebbe, ad esempio, possibile realizzare il fattore *possession* "qualcosa che solo l'utente ha" della Strong Customer Authentication, utilizzando la tecnologia blockchain per legare un particolare utente ad uno specifico dispositivo mobile device.



www.pwc.com/it/psd2

Marco Folcia

Partner | Strategy & Operations
+39 347 3786843
+39 02 66720433
marco.folcia@it.pwc.com

Fabrizio Cascinelli

Director | Regulatory
+39 345 6981767
+39 02 91605293
fabrizio.cascinelli@it.pwc.com

Gianmarco Zanetti

Director | Technology
+39 342 3039480
+39 02 66720567
gianmarco.zanetti@it.pwc.com

Sara Marcozzi

Senior Manager | Strategy & Operations
+39 346 7809698
sara.marcozzi@it.pwc.com