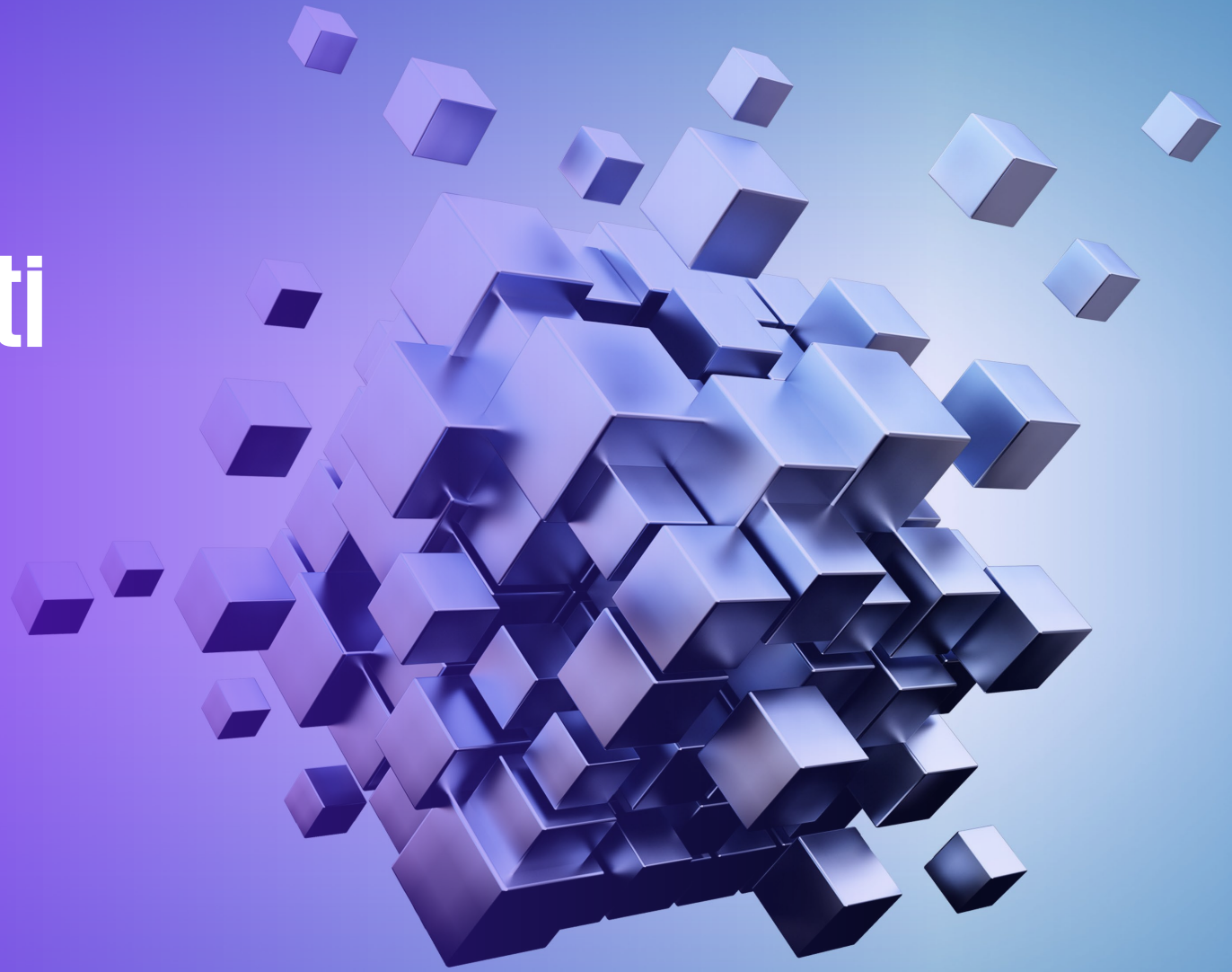
KPMG

Sicurezza nei pagamenti digitali: le novità della proposta di PSR



Il Salone dei Pagamenti 2025 | Milano, 30 Ottobre

Luca Boselli, Partner KPMG, Head of Cyber & Tech Risk

PSR: Le nuove minacce cyber nel nuovo quadro PSR 1/2

Evoluzione dello scenario delle minacce cyber nei pagamenti digitali

Dalla tradizionale sicurezza all'impatto di tecnologie innovative e interoperabilità crescente

Estensione e complessità della superficie d'attacco

- L'adozione di PSD3/PSR e la crescente digitalizzazione **comportano nuove vulnerabilità**, data la **proliferazione di soggetti coinvolti** (PSP, TPP, fornitori esterni).
- **Sistemi più connessi, ampia interoperabilità** e integrazione con terze parti (open banking) moltiplicano i potenziali punti di ingresso per gli attaccanti.

Interoperabilità come vettore critico

- **L'interconnessione obbligata tra operatori** (banche, TPP, fornitori tech) crea **catene di dipendenza**: una compromissione a monte può propagarsi all'intero ecosistema dei pagamenti.

Minacce tradizionali e minacce emergenti

- Restano attuali frodi, phishing, malware, DDoS e ransomware, ma **cresce esponenzialmente la sofisticazione degli attacchi**, soprattutto in ottica di social engineering e sfruttamento delle **vulnerabilità cloud/API.**

Impatto dell'Intelligenza Artificiale

- L'AI offre difese più evolute (analisi anomalie, rilevamento in tempo reale) ma è anche vettore di nuove minacce: **deepfake**, attacchi automatizzati, potenziamento ransomware e campagne su larga scala.

*La **cybersecurity nei pagamenti digitali** oggi richiede la gestione di minacce sia '**storiche**' sia **emergenti**, con particolare attenzione ai rischi propagati dall'interoperabilità e dalle nuove tecnologie (AI inclusa).*

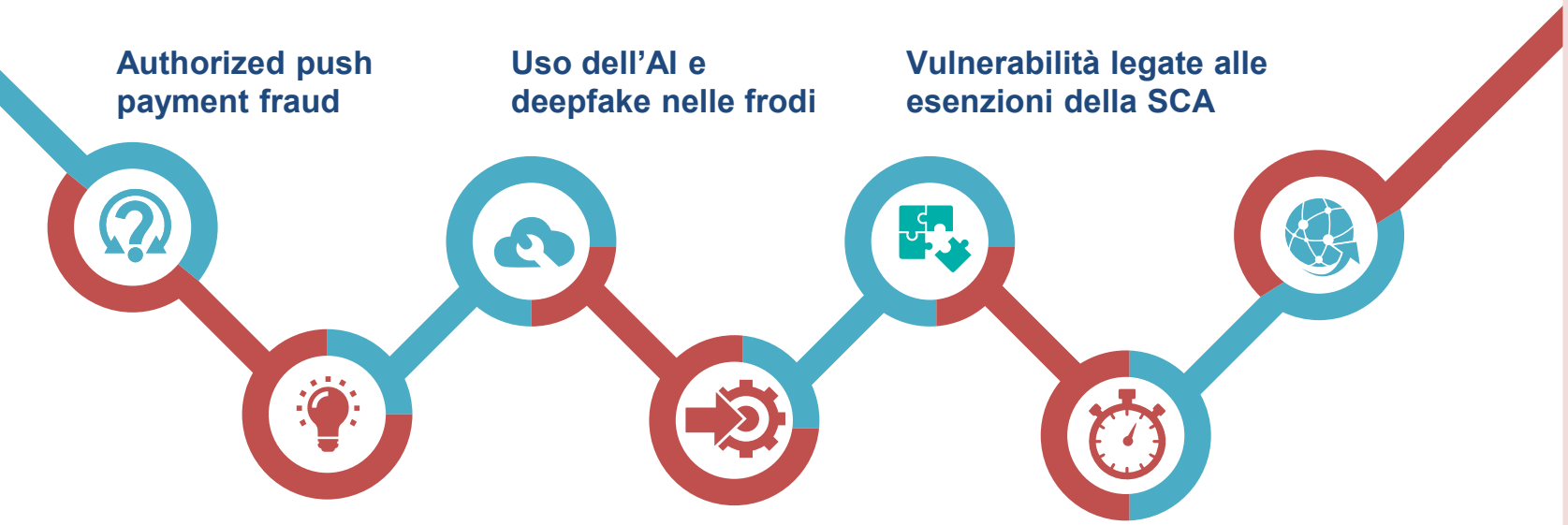
*Questi macro-temi relativi allo scenario delle minacce **generano nuovi scenari di rischio***

*La **normativa** spinge verso una **difesa olistica dei sistemi di pagamento digitali**, promuovendo **collaborazione** tra operatori, condivisione delle informazioni su frodi e **aggiornamento** continuo delle strategie di sicurezza.*

PSR: Le nuove minacce cyber nel nuovo quadro PSR 2/2

L'innovazione introdotta da PSD3 e PSR amplia le opportunità nel mercato dei pagamenti, ma aumenta anche la superficie d'attacco dei PSP, a causa della maggiore digitalizzazione, interoperabilità e apertura verso terze parti.

Nuovi Scenari di Rischio



- **Authorized Push Payment (APP) fraud:** gli attaccanti usano social engineering per indurre le vittime a pagamenti verso conti fraudolenti, richiedendo prevenzione e sensibilizzazione degli utenti.
- **Attacchi ai sistemi di pagamento**: ATM, POS e wallet digitali restano bersagli di malware e attacchi man-in-the-middle; l'aumento dei Third Party Provider e dei servizi connessi accresce i rischi sulla supply chain.
- **Uso dell'AI e dei deepfake nelle frodi**: l'intelligenza artificiale generativa consente attacchi più sofisticati con contenuti realistici, richiedendo controlli biometrici e comportamentali.
- **Identità sintetiche e furto d'identità digitale**: L'onboarding remoto e i controlli «KYC» automatizzati favoriscono identità ibride reali/sintetiche, aumentando i rischi AML.
- **Esenzioni SCA e falle di sicurezza**: le esenzioni per facilitare i pagamenti possono essere sfruttate da malintenzionati; servono policy di rischio aggiornate e controlli dinamici.
- **Estensione della SCA a 180 giorni**: il potenziale allungamento della validità del consenso amplia la finestra di esposizione e il rischio sistemico in caso di compromissione degli AISP.

PSR: Quadro di Riferimento Normativo

Con l'aumentare dell'utilizzo dei pagamenti digitali e con la crescente attenzione alle minacce informatiche che mirano al settore finanziario, l'Unione Europea ha costruito un ecosistema normativo con un grado di interconnessione sempre maggiore, allo scopo di rafforzare il settore finanziario.

***PSR**: pone l'accento su **sicurezza dei pagamenti, incident reporting** e controlli proporzionati*

***DORA**: estende tali principi alla **resilienza operativa ICT**, includendo **fornitori critici** e supply chain.*

*Insieme creano un **modello integrato di gestione e reporting dei rischi digitali** nei servizi di pagamento.*

Il Regolamento PSR rappresenta un punto di armonizzazione per l'operatività di tutti i PSPs in Europa

- Il **PSR** e la **PSD3** definiscono una governance solida dei rischi operativi e di sicurezza, rafforzando la **responsabilità del management.**
- Il **DORA** completa il quadro normativo introducendo requisiti di **resilienza digitale**, gestione dei rischi ICT e procedure di **segnalazione degli incidenti**.
- Il Regolamento **IPR** obbliga i PSP a offrire bonifici istantanei senza costi aggiuntivi e introduce la **verifica del beneficiario** per ridurre il rischio di frode.
- Il **GDPR** garantisce la liceità e la sicurezza dei dati, promuovendo il principio di accountability e la **protezione delle informazioni nei servizi di pagamento digitali.**

PSR: Quadro di Riferimento Normativo – Focus on DORA

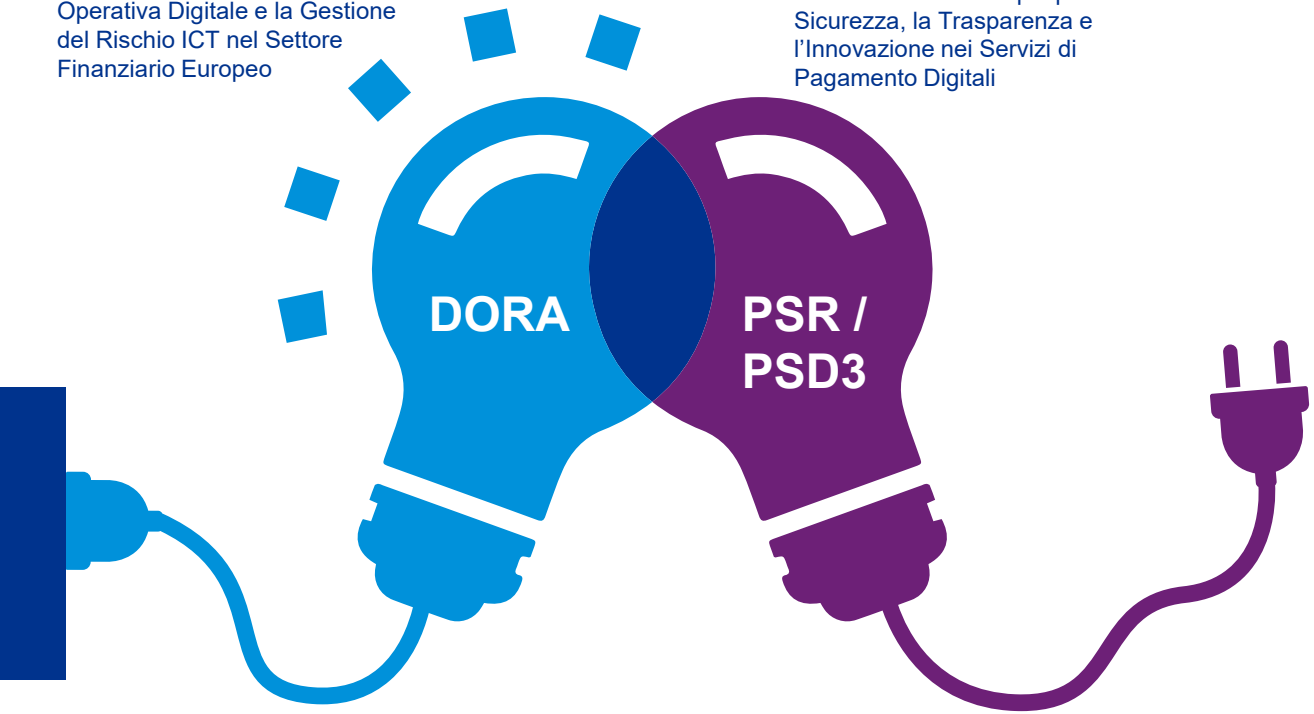
Dal **DORA al PSR/PSD3**: come si integrano **le regole su Resilienza ICT** e **Sicurezza dei Pagamenti** nel nuovo ecosistema normativo

DORA:

Rafforzare la Resilienza Operativa Digitale e la Gestione del Rischio ICT nel Settore Finanziario Europeo

PSR e PSD3:

Nuovi Standard Europei per la Sicurezza, la Trasparenza e l'Innovazione nei Servizi di Pagamento Digitali



DORA rafforza il quadro regolamentare europeo **estendendo i principi di resilienza operativa ICT**, già richiamati da PSR e PSD3, **a tutto il settore finanziario e dei pagamenti**, in particolare:

- **Segnalazione degli incidenti ICT**: procedure standard e tempi rigorosi per la detection, comunicazione e risposta agli incidenti che coinvolgono sistemi critici o dati sensibili.
- **Piani di resilienza operativa**: obbligo di disporre di strategie, risorse e test periodici mirati a garantire la continuità dei servizi, anche in scenari di attacco o malfunzionamento prolungato.
- **Quantificazione, gestione e testing dei rischi operativi**: valutazione continua delle vulnerabilità, simulazioni e formazione del personale per assicurare prontezza ed efficacia nella risposta.
- **Coinvolgimento di fornitori critici e supply chain**: DORA impone la gestione del rischio ICT anche verso terze parti e fornitori esterni (es. cloud, TPP), richiedendo accordi contrattuali chiari, capacità di auditing e piani di emergenza condivisi.

In sintesi, **DORA funge da collante** che coordina e **integra le misure di sicurezza**, **incident reporting e gestione della resilienza** già previste in ambito PSD3 e PSR, elevando il '**livello minimo**' di sicurezza digitale richiesto a tutti gli attori del panorama dei pagamenti europei.

kpmg.com/socialmedia