SABRINA LEO
IDA CLAUDIA PANETTA

MOBILE WALLET: ASPETTI TEORICI ED EVIDENZE EMPIRICHE A STELLE E STRISCE

Sabrina Leo

Ida Claudia Panetta

Mobile Wallet: aspetti teorici ed evidenze empiriche a stelle e strisce

UniversItalia

Il presente lavoro è frutto di una ricerca condotta dagli autori e di una loro riflessione congiunta.
Tuttavia, sono attribuibili a Ida Claudia Panetta: Cap. 1, paragrafi 1.1; Cap. 2, paragrafi 2.1, 2.2, 2.3; Cap. 3, paragrafi 3.1 (e sotto paragrafi); Cap. 4, paragrafi 4.1.
Sono attribuibili a Sabrina Leo: Cap. 1, paragrafi 1.2 (e sotto paragrafi), 1.3; Cap. 2, paragrafi 2.4, 2.5; Cap. 3, paragrafi 3.2 (e sotto paragrafi); Cap. 4, paragrafi 4.2..
L'Introduzione, i paragrafi 4.3 e 4.4 sono attribuibili a entrambi gli autori.

ISBN 978-88-3293-282-9

Indice

Capitolo 1.
Mobile Wallet industry: elementi qualificanti

Premessa

I *Mobile Wallet* (MW) costituiscono una sottocategoria dei più generali *Digital Wallet* (DW), e consentono di avviare transazioni in presenza e/o in remoto via web o utilizzando un *mobile device* (*M-Device*). Combinando diversamente canale di accesso, luogo della transazione e tecnologie impiegate, è possibile definire modelli operativi ed ecosistemi di business molto differenti tra loro. Pertanto, prima di procedere alla descrizione dei principali modelli presenti negli Stati Uniti, in questo capitolo si fornisce una tassonomia di carattere generale, applicabile a tutti i mercati di MW.

Per comprendere le caratteristiche dell'offerta attuale e potenziale dei MW, occorre soffermarsi brevemente sulle principali tecnologie alla base del loro funzionamento, discriminanti queste, in grado di orientare le scelte degli operatori. Sarà la combinazione dei diversi elementi tecnologici che, definendo le modalità d'interazione tra *user* e *merchant*, caratterizzerà i rapporti di forza e debolezza dei *player* coinvolti nell'erogazione del servizio e sul gra-

dimento da parte degli *user*: in altre parole il successo del *wallet*.

In particolare, nella seconda parte del capitolo, ci si sofferma sulle tecnologie associate ai pagamenti presso gli esercenti (*proximity payment*) e sulla sicurezza; si tratta di due elementi principali alla base della scelta delle soluzioni che il *merchant* può abilitare per vendere i propri prodotti/servizi, e che qualificano gli elementi di differenziazione tra la scelta di un *wallet* rispetto ad un altro.

L'ultima parte del capitolo è dedicata alla rappresentazione dell'industria dell'*M-Wallet* attraverso il paradigma interpretativo dell'ecosistema. L'industria dell'*M-Wallet*, come quella degli *M-Payment* in generale, rappresenta un esempio perfetto di ecosistema: esso, infatti, rispetto ad altre modalità di pagamento vede la partecipazione di differenti attori principali e coprotagonisti, appartenenti a settori anche estranei l'uno all'altro, ma che interagendo tra loro danno vita ad un ecosistema complesso.

1.1 Verso una tassonomia degli *M-Wallet*

Non esistono delle definizioni univoche relative all'*M-Wallet*; tuttavia, analizzando alcune di quelle più citate in letteratura - riportate in Tab. 1.1 - è possibile evidenziare alcuni aspetti che contribuiscono alla sua definizione: a) si tratta di un portafoglio digitale; b) la componente hardware del servizio è costituito dall'*M-Device*; c) la componente software del servizio è costituita da un'applicazione (*M-App*). Di fatto l'*M-Wallet*, inteso come combinazione di

software e hardware, è lo strumento che consente allo *user* di perfezionare operazioni di pagamento e di effettuare altresì operazioni di trasferimenti di disponibilità P2P (*M-Transfer*).

Rispetto ai servizi offerti da un *M-Wallet* è possibile distinguere tra quelli *core*, legati all'intermediazione delle transazioni, e quelli complementari. Con riferimento ai primi è possibile distinguere tra operazioni di:

1. *M-Payment*, ovvero pagamento in senso stretto per l'acquisto di un bene o servizio; si tratta di tutte quelle soluzioni che consentono allo *user* di effettuare operazioni in remoto e in presenza. All'interno di questa categoria si è soliti far rientrare:
   - l'*M-Ticketing*, ossia il servizio con il quale si possono ordinare, pagare, ottenere e/o validare biglietti (per il trasporto, per lo stadio, per i concerti, ecc.) utilizzando un *M-Device*. Con l'*M-Ticketing* le fasi di acquisto e convalida del biglietto avvengono tramite l'utilizzo di *M-App* che sfruttano le tecnologie del QR Code o dell'NFC (vedi infra). I vantaggi dell'*M-Ticketing* sono rilevanti sia per il *merchant*, che beneficia anche di una riduzione dei costi per l'emissione dei biglietti, sia per lo *user*, che ha un vantaggio in termini di praticità e comodità.
   - L'*M-Commerce*, ovvero la possibilità di acquistare servizi e beni materiali (cd. *real good*) tramite *M-Device*.

- Lo *Smart Commerce,* ossia la possibilità di effettuare micro-pagamenti per l'acquisto di App, di contenuti digitali video e/o audio, acquisto/noleggio di giochi, ecc.. Si tratta di fatto della possibilità di ottenere App non gratuite per sfruttare le funzionalità offerte dai più moderni *M-Device* quali *smartphone*, *tablet*, ecc..

2. *M-Transfer*, vale a dire servizi grazie ai quali si trasferiscono somme di denaro tra persone fisiche (P2P) per motivazioni diverse dalla regolazione di un pagamento per l'acquisto di beni e servizi.

Tab. 1.1 - Principali definizioni di M-Wallet

Autore (anno)	Definizione
Mobey Forum (2011)	È una funzionalità presente su un dispositivo *mobile* che può interagire in modo sicuro con valori digitali
GSMA (2012)	Applicazione che gestisce un insieme di servizi NFC sullo *smartphone* e che può anche gestire altri servizi offerti da operatori di telefonia *mobile* e da suoi *partner*
European Payments Council (2013)	*Digital wallet* al quale si accede tramite *M-Device*. Questo servizio può essere "residente" sull'*M-Device* di proprietà del consumatore (vale a dire il proprietario del borsellino digitale), o su un *server* (o una combinazione delle due) o sul sito di un *merchant*. Tipicamente l'emittente dell'*M-Wallet* fornisce le funzionalità del borsellino, ma l'utilizzo e sotto l'esclusivo controllo del *consumer*
Lerner (2013)	*Portable wallet* che è utilizzato come un'applicazione nel più ampio contesto nei servizi di *M-Payment*
Osservatorio Mobile Payment & Commerce (2014)	Applicazione per *smartphone* che consente di gestire e utilizzare, in modo integrato, il proprio *Digital Wallet*, accedendo a servizi di prossimità o a distanza
EBA (2014)	Soluzioni che permettono al cliente di registrare i dati relativi a uno o più strumenti di pagamento, al fine di effettuare pagamenti con diversi operatori commerciali online
Mobile Payments Today (2015)	Luogo in cui i consumatori possono conservare ed organizzare *coupon*, programmi fedeltà, carte di pagamento, biglietti, assicurazione dell'auto e qualsiasi altra cosa cartacea o di plastica che possa essere trasformata in formato digitale

Fonte: Panetta e Leo (2017), p. 65.

Tra i servizi complementari di un *M-Wallet*, invece, rientrano soluzioni di:

1. *mobile marketing*[1], ossia servizi a supporto della relazione *user*/*merchant*, quali ad esempio:
   - il *couponing*, ossia la possibilità per lo *user* di usufruire di un buono sconto al momento del pagamento. I *coupon*, generalmente utilizzati per un primo incentivo, possono costituire uno strumento che contribuisce a fidelizzare il consumatore; il passaggio dai *coupon* cartacei all'*M-Couponing* ne semplifica la gestione portando indubbi vantaggi sia agli *user* che ai *merchant*.
   - I *loyalty program*, atti ad incentivare i clienti a rimanere fedeli al *merchant*[2]. I servizi di *M-Loyalty* consentono di "salvare" le carte fedeltà nell'*M-Wallet* e di utilizzarle contestualmente al pagamento impiegando la tecnologia NFC o QR Code, qualora il sistema lo consenta. Tale tipologia di servizi crea vantaggi sia per i *merchant* che per gli *user*: i primi per la disponibilità di maggiori informazioni sull'acquisto/preferenze del cliente, oltre che per una riduzione dei costi legata alla produzione delle tessere plastificate; i secondi per la maggiore praticità derivante dalla dematerializzazione delle carte fedeltà.

[1] Per approfondimenti sul *mobile advertising* in genere si veda Chang e Huo (2011) e Tapsense (2014).
[2] GSMA, (2014).

2. *Mobile Infotainment System*, si tratta di servizi informativi legati al turismo, agli eventi culturali, all'intrattenimento in genere.
3. Identificazione personale, ovvero quei servizi che consentono ad un utente di indentificarsi presso lo *store* del *merchant*, le Pubbliche Amministrazioni, le filiali bancarie o postali, ecc..

È importante specificare che i servizi complementari sono addizionali e volti a incrementare l'utilità, la frequenza di utilizzo e l'efficienza dell'*M-Wallet*[3]. Essi consentono il raggiungimento di vantaggi su entrambi i lati della domanda[4]: il *consumer* amplia la cosiddetta *user experience*; di conseguenza il *merchant*[5] può raggiungere in modo diverso e più diretto la propria clientela[6] e fidelizzarla.

Per orientarsi tra le molteplici tipologie di *M-Wallet* sul mercato, è possibile classificarle secondo la numerosità e la tipologia di attori coinvolti[7]. In particolare, è possibile distinguere tra:

1. *M-Wallet* verticale (Fig. 1.1), nel quale il *Service Provider* (in figura PSP[8] A) proprietario della piattaforma

[3] Mobey Forum (2012) definisce che "un *Mobile Wallet* che non permette di pagare, non può essere considerato un portafoglio"; ne deriva che il pagamento è la componente fondamentale, ma non è la sola funzione che può determinare l'adozione in larga scala degli *M-Wallet*.
[4] Vedi infra.
[5] Holden (2013a).
[6] FIRST DATA (2011).
[7] Per approfondimenti EPC (2014b).
[8] Si parla di PSP – Payment Service Provider in quanto il servizio offerto è un servizio di pagamento.

(cd. ecosistema proprietario), provvede direttamente sia a fornire i servizi, che alla gestione degli stessi;

2. *M-Wallet* orizzontale (Fig. 1.2), nel quale più *Service Provider* (in figura i PSP A-C), offrono i loro servizi attraverso un unico *M-Wallet (ecosistema aperto)*.

L'*M-Wallet* verticale è quello impiegato nei *closed-loop payment*, ovvero quei pagamenti effettuati con strumenti di pagamento brandizzati (una carta, o un *wallet*), utilizzabili esclusivamente presso il soggetto che li ha emessi. Quando l'*issuer* è il merchant si parla di *Merchant-Centric Wallet* (tipico il caso di Starbucks®[9]), quando, invece, è un intermediario creditizio si parla di *Bank-Centric wallet*[10]. Negli *M-Wallet* verticali alla facilità di gestione, ivi inclusi i costi relativi e la maggiore sicurezza per il *Service Provider*, si associa un più limitato utilizzo da parte del *consumer*.

[9] https://www.starbucks.com.

[10] Vale la pena precisare che talvolta la banca per alcune funzionalità degli M-Wallet usufruisce di piattaforme offerte da altri soggetti (vedi Capitolo 3).

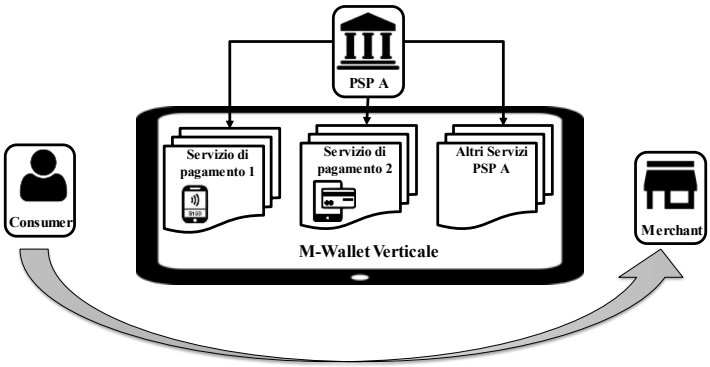

Fig. 1.1 - Schema M-Wallet verticale
Fonte: Panetta e Leo (2017), p. 67.

Diverso il caso di un *M-Wallet* orizzontale dove vengono distinti due attori principali:

1. il *Mobile Wallet Issuer*, ovvero il soggetto che offre il "contenitore" dei servizi inclusi nell'*M-Wallet*. Di fatto offre la piattaforma o più specificatamente l'*M-App* (*user enabler*) che consente a differenti *Service Provider* di offrire il proprio prodotto. In genere, si occupa della promozione dell'*M-Wallet*, della gestione delle relazioni con i diversi *Service Provider*, dell'identificazione degli standard operativi di riferimento (leggasi di funzionamento e di sicurezza), della gestione delle relazioni di priorità tra i diversi servizi offerti, ecc..
2. Il *Service Provider*, ovvero il proprietario del "contenuto" del servizio offerto dall'*M-Wallet*. Nel caso in cui il servizio offerto si riferisca ai pagamenti parliamo di PSP. Oltre allo sviluppo del servizio è spesso responsabile della promozione dello stesso, della gestione dei

clienti che lo utilizzano, del rispetto degli standard di sicurezza ecc..

Ad evidenza la complessità di un *M-Wallet* di tipo orizzontale risiede nella definizione dei rapporti tra l'*Issuer* e i *Service Provider*; questo presuppone, tra le altre cose, un'accurata gestione dell'interoperabilità tra i diversi servizi da integrare e dei profili di sicurezza (vedi infra). Attraverso questa tipologia di *M-Wallet* lo *user* può decidere di effettuare il pagamento scegliendo tra i diversi strumenti messi a disposizione; il *consumer*, infatti, può aggiungere direttamente le credenziali di pagamento rilasciate dai diversi PSP al proprio *M-Wallet*, senza che vi debba essere un'interazione diretta con il proprio *provider*[11] e scegliere, in fase di pagamento quale strumento utilizzare. Esempi di questa struttura sono i *wallet* forniti dai Mobile Network Operator (*MNO-Centric Wallet*).

[11] È evidente che questo approccio richiedere implicitamente che vi sia una relazione contrattuale tra *user* e PSP.

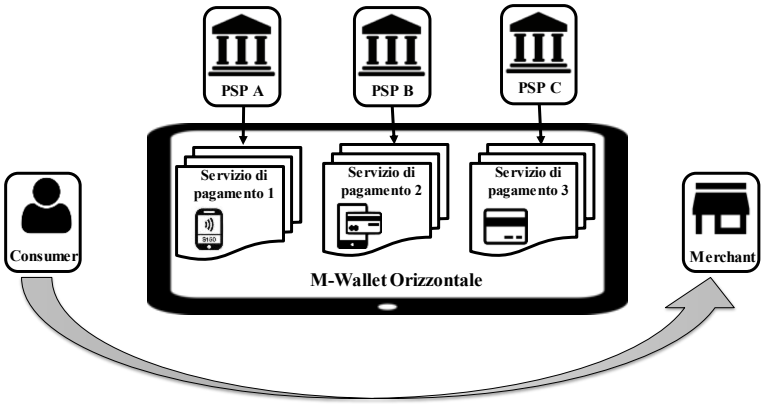

Fig. 1.2 - Schema M-Wallet orizzontale
Fonte: Panetta e Leo (2017), p. 68.

Le due strutture (verticale e orizzontale) possono anche essere viste come il naturale percorso evolutivo degli *M-Wallet*: infatti, le prime esperienze, sono proprio state di tipo verticale con un singolo PSP che controllava l'intero ciclo di vita del servizio di pagamento; l'evoluzione tecnologica, soprattutto con riferimento alla sicurezza, ha consentito il graduale sviluppo di *wallet* con approccio orizzontale nei quali l'utilizzatore ha la possibilità di accedere ai servizi offerti da più PSP utilizzando un unico *wallet* (leggasi piattaforma, *M-App*).

L'*M-Wallet* può essere anche classificato tenendo presente se il soggetto con il quale l'*M-Wallet Issuer* stipula l'accordo sia collocato nella sfera dello *user* o del *merchant*[12]. In questi casi si parla di:

[12] EPC (2013).

1. *Payer's space M-Wallet*, in cui l'*Issuer* ha un accordo con il *consumer* o il suo PSP;
2. *Beneficiary's space M-Wallet*, in cui, invece, l'*Issuer* ha un accordo con il *merchant* o con il suo PSP.

Infine, tenendo conto della tipologia di *Issuer* possiamo distinguere tra gli *M-Wallet*[13] emessi da:

1. istituzioni finanziarie, che possono essere PSP bancari[14] e non (ad esempio PayPal®[15] *wallet*);
2. operatori non finanziari tra i quali è possibile distinguere ulteriormente tra:
   - MNO (Telco), ad esempio M-Pesa®[16];
   - *merchant*, ci si riferisce ai cosiddetti *M-Wallet closed-loop* "brandizzati", quali ad esempio Starbucks®;
   - operatori indipendenti (*Third Parties Operator*) che offrono i propri servizi in favore di più *merchant*; all'interno di questa categoria rientrano ad esempio i cosiddetti *big player* come Apple Pay®[17] o Google Pay®[18], ma anche i meno noti PayUmoney®[19] (India).

---

[13] Altri individuano sulla base dell'*issuer* altre tipologie di classificazioni, ad esempio Arnifield (2015) parlano di: i) *retailer*, che creano il proprio *wallet* dedicato ii) intermediari finanziari, altri intermediari non finanziari (es Apple, Google ecc.).

[14] Kumar e Seri (2014).

[15] https://www.paypal.com/it/home.

[16] https://www.vodafone.com/content/index/what/m-pesa.html.

[17] https://www.apple.com/it/apple-pay.

[18] https://pay.google.com.

[19] https://www.payumoney.com.

Nella tabella che segue si propone una sintesi dei principali criteri di classificazione utilizzati per tassonomizzare gli *M-Wallet*.

Tab. 1.2 – Principali criteri di classificazione degli M-Wallet

Driver	**Tipologie di *Wallet***	
Tipologia di servizi inclusi nell'MW	MW con servizi di pagamento (servizi *core*)	
	MW con servizi complementari	
Ruolo e numero di *Service Provider*	MW Verticale	
	MW orizzontale	
Soggetto con il quale *Issuer* stipula accordo	*Payer's space mobile wallet*	
	Beneficiary's space mobile wallet	
Tipologia di *Issuer*	*Issuer* finanziario	non bancario: tipicamente *Network-Centric walllet*
		Bancario: *Bank-centric wallet*
	Issuer non finanziari	*MNO-Centric Wallet*
		Merchant-Centric Wallet
		Third Parties Operator

1.2 La tecnologia e le configurazioni dei *Mobile Wallet*

L'innovazione tecnologica è l'elemento fondante degli *M-Wallet*. Per comprendere pienamente le strutture di questa tipologia di servizi, occorre, quindi, soffermarsi

sulle caratteristiche essenziali di funzionamento[20] delle principali tecnologie impiegate. Lo scopo non è tanto quello di addentrarsi in dettagli tecnici, quanto quello di evidenziare come talune tecnologie possono incidere sulle scelte degli operatori sia sul lato della domanda che su quello dell'offerta. La maggior parte delle strutture di MW esistenti possono essere considerate come la combinazione di tecnologie vecchie e nuove, declinate nell'interazione di *hardware* e *software* utilizzati. A tali due componenti è necessario aggiungere l'elemento "comunicazione". Infatti, il presupposto delle tecnologie *mobile* è quello della connessione tra *device wireless* per la realizzazione della quale è necessario che vi sia un linguaggio condiviso e una struttura di trasferimenti dei dati e delle informazioni.

È evidente che in un siffatto contesto, un ruolo chiave è giocato anche dal grado di sviluppo e di diffusione delle singole tecnologie nei diversi mercati, anche geografici.

Nel confezionamento dell'offerta di MW le principali scelte di progettazione del portafoglio hanno per oggetto i seguenti elementi principali:

- modalità di interazione tra *consumer* e *merchant* per i pagamenti in prossimità: Near Field Comunication (NFC), QR Code, Magnetic Secure Transmission (MST);
- luogo di archiviazione delle credenziali di pagamento: *Secure Element* (SE) su *device* o su scheda SIM, Host Card Emulation (HCE) *cloud*, Card on File (CoF). HCE *cloud* implica che il *provisioning*

[20] Camponovo e Pigneur (2003); Seah *et al*. (2001).

delle credenziali sia correlato ai pagamenti *mobile* NFC, mentre il CoF è una soluzione *web-oriented* nel quale le credenziali di pagamento non sono legate al dispositivo *mobile*;

- possesso delle credenziali di pagamento (vedi infra);
- opzioni di pagamento: *proximity in-store*, *in-app*, *e-commerce* remoto o *m-commerce* remoto dal browser web;
- presenza della carta di pagamento: *Card present* (CP), *Card Not Present* (CNP). Tale scelta impatta sui costi sopportati dal *merchant*;
- avvio della transazione *push* o *pull*;
- processo di identificazione e verifica dello *user IDentification & Verification* (ID&V).

Nei paragrafi successivi è offerta una panoramica delle tecnologie utilizzate dai diversi modelli di *wallet* considerati nell'analisi. In particolare, ci si sofferma sulle tecnologie alla base del funzionamento dei *proximity payment* e dei relativi profili di sicurezza; la scelta è motivata dal fatto che, mentre nell'*e-commerce* e nel *m-commerce* l'esercente è "quasi" obbligato a scegliere alternative di pagamento che includono uno o più *wallet*, questo non è del tutto sottinteso nel caso dei *proximity payment*: in primo luogo perché l'esercente, sostenendo dei costi, accetta già pagamenti con una molteplicità di strumenti alternativi al contante che necessitano di sistemi di lettura dedicati; in secondo luogo perché l'utilizzo di *device* portatili per il completamento degli acquisti non ha mostrato una diffusione massiva presso

gli *user*, a volte perché influenzati da timori legati alla sicurezza[21].

1.2.1 La tecnologia NFC e HCE: lo starter dei proximity payment

L'NFC è un protocollo di comunicazione *wireless* basato su standard a radiofrequenza, che consente lo scambio di dati tra dispositivi distanti pochi centimetri. Le transazioni di pagamento NFC tra un dispositivo *mobile* e un terminale POS utilizzano lo stesso protocollo di comunicazione standard ISO/IEC 14443 utilizzato dalle carte di pagamento *contactless* EMV® (vedi infra), che consente all'*M-Device* di simularne il funzionamento.

L'NFC è impiegata nei *wallet* che effettuano pagamenti *proximity* esclusivamente tramite *mobile device* (*Device-Centric Mobile Proximity Wallet*[22]). Questo modello di *wallet* è indipendente dal sistema operativo utilizzato, e si basa su un'applicazione *software* presente sul *device* che avvia e gestisce i pagamenti. Di fatto, l'MW è il tramite che permette di accedere alle credenziali delle carte di pagamento, dei conti bancari, dei coupon, delle *fidelity card*, o alle informazioni finanziarie, memorizzate sul telefono cellulare in un ambiente sicuro. È evidente che al momento del pagamento, lo *user* dovrà essere in possesso dell'*M-Device* con il quale toccherà (*tap*) o si avvicinerà (*wave*) a un terminale POS *contactless* abilitato. In aggiunta questi porta-

[21] Nel Capitolo 4 è fornita un'analisi dei dati sui fattori che influenzano l'utilizzo degli MW nel mercato americano.

[22] Il cd. *Device-Centric Wallet* è identificato dalla caratteristica della memorizzazione delle credenziali di pagamento nell'*M-Device*, (cfr. cap. 2).

fogli digitali che fruttano le funzionalità NFC possono essere utilizzati anche con alcuni POS *contactless* configurati per transazioni a banda magnetica MST (*hover*).

I pagamenti in prossimità possono essere effettuati anche *in-app* presso lo *store*. In questo caso il cliente al momento del *check-out* in negozio avvia l'App del *merchant*[23], avvicina lo *smartphone* al POS *contactless* e autorizza il pagamento dall'App; dopo l'autorizzazione le credenziali di pagamento e le informazioni di fatturazione del cliente, archiviate in modo sicuro nel telefono, vengono inviate con token e crittogramma al (App del) *merchant*.

Alla base di tutti questi sistemi vi è il processo di tokenizzazione, ovvero la sostituzione di dati sensibili con un token, vale a dire un dato generato da diversi algoritmi che non consentono di risalire ai dati d'origine (la cosiddetta non reversibilità); i dati d'origine possono essere "raggiunti" solo dalle entità e dai soggetti proprietari degli stessi[24]. Nel caso dei pagamenti tramite *M-Device* la tokenizzazione consente di sostituire il Personal Autentication Number (PAN) della carta di pagamento dello *user*, la data di scadenza e il codice di sicurezza con un valore sostitutivo, chiamato appunto token. Il vero valore PAN è, quindi, protetto perché non "esposto" durante la transazione. Quando una carta di pagamento viene associata a un MW il PAN viene tokenizzato e memorizzato in un ambiente sicuro. L'autenticazione biometrica impedisce l'utilizzo non autorizzato del *device* per i pagamenti. Infatti, quando il token viene utilizzato in un *M-Payment* viene

[23] L'identificazione può avvenire tramite Touch ID o Face ID per i device Apple® o "Acquista con Android Pay" per Android.
[24] Panetta e Leo (2017), p. 56-57.

generato, e trasferito con il token nel processo di pagamento, un crittogramma dinamico. In questo modo il token diviene inutilizzabile in quanto associato ad una specifica transazione. I sistemi di tokenizzazione hanno dato un forte impulso ai pagamenti NFC con le ultime generazioni di *M-Device*.

I dispositivi basati sul sistema operativo Android® utilizzano l'NFC, ma possono impiegare un metodo diverso per la memorizzazione e l'invio delle informazioni sulle carte di pagamento. Tali dispositivi, infatti, utilizzano l'*Host Card Emulation* (HCE), un emulatore di carte di pagamento basato su un *software* che consente all'MW di inviare le credenziali di carte o token di pagamento attraverso il *controller* NFC a un terminale POS o lettore *contactless* NFC, rimovendo la necessità di utilizzare un SE (vedi infra). Una transazione HCE ha luogo come segue:

- lo *user* tocca il POS *contactless* con il proprio *M-Device*;
- l'HCE abilita il *controller* NFC dell'*M-Device* così da consentire la richiesta del token di pagamento del POS al MW;
- il token di pagamento e il relativo crittogramma dinamico sono trasmessi al POS per completare la transazione.

L'HCE utilizza protocolli di sicurezza quali la tokenizzazione e/o un *Trusted Execution Environment* (TEE) per soddisfare i requisiti di sicurezza richiesti dalla regolamentazione dei sistemi di pagamento.

Un'altra tecnologia utilizzata negli *M-Payment* è costituita dal QR Code. Si tratta di un codice a barre 2D che codifica dati numerici, alfanumerici o binari in un codice

a barre bidimensionale che può essere scansionato e decodificato rapidamente per eseguire un pagamento al POS.

1.2.2 NFC e sicurezza

I pagamenti *mobile* basati su NFC sono un'estensione delle transazioni con carta di pagamento dotata *chip* EMV®; si tratta di una tecnologia che rappresenta uno standard globalmente riconosciuto per l'interazione tra smart card e terminali POS/sportelli ATM, per l'autenticazione di transazioni con carte di credito e di debito.

All'avvio del pagamento mobile, l'EMV® protegge la transazione di pagamento utilizzando dati dinamici unici che vengono generati impiegando una chiave crittografica; i dati dinamici sono usati per autenticare la transazione e hanno validità per intermediare un solo scambio. È, infatti, impossibile tentare di riutilizzare i dati di un pagamento per un'altra transazione: in questo caso l'*issuer* respingerebbe l'autorizzazione al completamento dell'operazione. L'impossibilità del riuso dei dati dinamici ha l'obiettivo di disincentivare i tentativi di illecita acquisizione dei dati utilizzabili.

Le soluzioni di MW NFC più diffuse e disponibili si differenziano per la gestione e memorizzazione dei token di pagamento EMV®[25]; infatti, alcuni memorizzano i token di pagamento nei SE incorporati nei *device* (*embedded*), altri utilizzano l'HCE per archiviare token nel sistema

[25] Per ulteriori informazioni sull'uso della tokenizzazione dei pagamenti si veda Crowe M. *et al*. (2015).

operativo Android®, ed altri ancora impiegano sia l'NFC che l'HCE ma memorizzano i token di pagamento e le chiavi crittografiche nel TEE del *device*.

Il SE *embedded* incorporato nel device, invece che sulla scheda SIM offerta da un MNO, comunica con il terminale del *merchant* attraverso l'antenna del telefono. Tale tipologia di SE è protetta da manomissioni e ospita in modo sicuro più applicazioni e dati crittografici. Apple Pay® si differenzia dagli altri *wallet* poiché utilizza l'*embedded* SE per memorizzare il token di pagamento che rappresenta il PAN, e in qualità di produttore dei *device* ne controlla l'accesso.

Alcuni *wallet* utilizzano l'HCE anziché il SE e memorizza una chiave rappresentativa del PAN nel *cloud*. I token di pagamento e le token-key (LUK) a uso limitato o monouso sono archiviati in un'area protetta del sistema operativo che tramite un software crittografa e oscura i dati. I LUK generano crittogrammi che vengono inviati con il token di pagamento EMV® per ogni transazione. Le chiavi vengono aggiornate ogni volta che l'utente si connette a una rete, il che consente di completare le transazioni anche senza connessione. Anziché richiedere un token al cloud ogni volta che è necessario effettuare un pagamento, le soluzioni che utilizzano LUK risolvono i problemi derivanti dalla possibilità che una connessione Internet non sia disponibile per il download di un token. L'HCE non ha gli stessi livelli di sicurezza dell'*embedded* SE e per questo motivo sono necessarie ulteriori misure di protezione, come la tokenizzazione dei pagamenti.

In ultimo, le credenziali di pagamento e le chiavi associate che generano un crittogramma dinamico per ogni transazione, possono anche essere memorizzate nel TEE, che però non ha livelli di sicurezza pari a quelli di un SE in quanto non resistente a possibili manomissioni esterne. Esistono tuttavia soluzioni che rendono l'utilizzo del TEE meno vulnerabile.

1.2.3 HCE e sicurezza

Gli *M-Payment* basati su HCE sono spesso associati a livelli di sicurezza minori; tale criticità è legata al cd. rooting, ovvero il processo informatico che permette agli utenti dotati di *device* con sistema operativo Android® di ottenere controlli privilegiati (permessi di root) su diversi sottosistemi Android®. In linea teorica è proprio il *rooting* a rendere un *device* più vulnerabile ad attacchi esterni; ad esempio il *rooting* può esporre le informazioni riservate, come le credenziali di pagamento, a un accesso fraudolento e facilitare lo sfruttamento di tali dati da parte di *malware*.

Di conseguenza, poiché negli *M-Wallet* che sfruttano la tecnologia HCE la comunicazione passa attraverso il sistema operativo Android®, i controlli di sicurezza di base sono limitati, in quanto Android® non impedisce il *rooting*. Alcuni *M-Wallet* per ovviare a tale fragilità, inibiscono l'istallazione delle relative applicazioni su telefoni "rootati". Considerati i rischi associati al *rooting*, i fornitori di MW HCE devono assicurarsi che le soluzioni di pagamento offerte controllino le possibili violazioni e prevedano piani d'azione al verificarsi delle stesse.

Oltre ai rischi associati al *rooting*, un ulteriore *vulnus* legato all'HCE, indipendente dal luogo "fisico" nel quale le credenziali di pagamento sono memorizzate, è la non tokenizzazione delle stesse. Essendo lo *storage* del *software* più vulnerabile alle violazioni della sicurezza e alle frodi rispetto ai casi in cui l'archiviazione avviene su SE, il fatto che le credenziali non siano tokenizzate fa aumentare l'esposizione delle transazioni a fattori critici.

Possibili miglioramenti alla sicurezza degli MW basati su HCE includono:

- l'ID&V dello *user* basati su *username-password* o PIN, riconoscimento biometrico, localizzazione geografica, o ID del dispositivo;
- vincoli alle transazioni in termini di canali (online o POS), *merchant* specifici, o in termini di importo riducendo in tal modo l'esposizione dei token a un utilizzo fraudolento;
- la sostituzione del PAN con un parametro equivalente;
- l'affidamento a terze parti degli strumenti di rafforzamento dell'autenticazione a livello di dispositivo e di sistema operativo;
- l'uso della crittografia delle credenziali di pagamento.

1.2.4 QR Code e sicurezza

Anche l'uso del QR Code comporta diversi rischi, dovuti alla sua vulnerabilità alle frodi e all'assenza di standard di riferimento per preservarne la sicurezza. I codici QR possono essere, infatti, utilizzati per scopi fraudolenti, quando, ad esempio, contengono URL associati a *malware*

nascosti, o che reindirizzano l'utente verso siti web falsi per scopi disonesti.

Per preservare la sicurezza di una transazione presso l'esercente con QR code, quindi con lettura del codice da parte di un POS, occorre che la rete Wi-Fi o il servizio di telefonia cellulare, che supporta la comunicazione dei dati, sia perfettamente funzionante e sufficientemente sicura. Infine, se il *device* non protetto da password viene smarrito o rubato e il *merchant* non richiede la verifica del cliente, il truffatore può accedere all'App e utilizzare il codice QR per effettuare un acquisto, accedere al PAN o alle altre informazioni sull'account memorizzate nel cloud.

La carenza di sicurezza dei pagamenti basati su QR code non ne ha limitato l'utilizzo, anzi; soprattutto in contesti come quello cinese e in India i casi di *M-Wallet* che utilizzano questo meccanismo di comunicazione sono piuttosto diffusi. Ciò in parte è dovuto alla possibilità di adottare alcune cautele, sia da parte degli *user* che da parte degli *issuer*, che aiutino, o possano aiutare, a ridurre i rischi. I primi possono far ricorso a software antivirus e anti-malware sui loro telefoni cellulari o alla protezione tramire *passcode* che impedisce l'uso del *device* in caso di smarrimento o furto (al momento dell'utilizzo dell'App di pagamento con codice QR, quale quella di Starbucks®, il cliente deve inserire un ID e una password). I secondi, che siano il *merchant* o meno, devono archiviare in modo sicuro le credenziali di pagamento del cliente. In linea generale il QR Code non deve mai includere informazioni sulla carta di credito o di debito.

La combinazione di questi presidi è necessaria per rendere sicuri i pagamenti tramite QR Code, oltre che efficaci ed efficienti.

Discorso a parte merita la tokenizzazione. Alcuni *M-Wallet* in aggiunta al QR code generano un token singolo per ciascuna carta di pagamento associata al *wallet* da utilizzare congiuntamente al PAN per gli acquisti. In questi casi l'*issuer* non condivide con il *merchant* il PAN, ma, oltre ovviamente al token di pagamento, le sole informazioni che il cliente generalmente fornisce in una transazione online (e-mail, telefono e indirizzo di spedizione).

1.2.5 L'identificazione e la validazione

Quando si effettua un'operazione di acquisto tramite *M-Wallet*, l'abilitazione a concludere la transazione avviene solo dopo che il consumatore è stato identificato ed è stato verificato; si tratta della fase di ID&V – *IDentification and Verification*. Ciò vuol dire che vi deve essere una esplicita autorizzazione da parte dell'*issuer* della carta di pagamento o del conto del *consumer*, successivamente alla quale viene rilasciato il token per il pagamento in senso stretto.

L'ID&V svolge un ruolo chiave nel determinare se lo *user* sia il legittimo proprietario delle credenziali dell'account collegate al MW; se non viene eseguito in modo efficace, l'ID&V si trasforma in una criticità rilevante di questo strumento. Il livello o la forza del metodo di autenticazione, infatti, è indissolubilmente associato alla mitigazione dei rischi e, per questo motivo, è il profilo più sfidante che *merchant* e *issuer* affrontano sia nell'*e-commerce* che nell'*m-commerce*.

Nei *Device-centric wallet* le credenziali di pagamento con token non vengono inviate all'area protetta del *device* finché l'*issuer* non ha autenticato il titolare del *wallet* e il suo account.

Durante il processo di *provisioning*, il fornitore di *Device-centric wallet* può inviare all'emittente uno score per la quantificazione del rischio e quindi per rendere maggiormente sicuro il processo di identificazione; gli score si basano sui dati raccolti dal provider del MW come l'ID del dispositivo, la geolocalizzazione, la cronologia dell'account iTunes o Google, ecc..

Nei *wallet cd. cloud-based*[26], dopo che lo *user* ha "caricato" le credenziali di pagamento, il *Service provider* del *wallet* esegue un processo aggiuntivo di gestione dei rischi che verifica gli indirizzi di posta elettronica e fatturazione e raccoglie informazioni sul dispositivo *mobile*, inclusi l'ID dell'*M-Device* e i dati dell'IP. Possono anche essere eseguiti i controlli del codice di sicurezza della carta, il monitoraggio dell'account o la revisione degli attributi di registrazione dello *user*.

L'autenticazione non si basa su un solo test, ma utilizza anche tecniche multilivello o multifattoriali: la prima utilizza più metodi di autenticazione a fattore singolo, come nome utente e password o la domanda di sicurezza; la seconda crea una difesa a più livelli, che rende più difficile, a soggetti non autorizzati, l'accesso al *device*. Con queste partiche, la compromissione di un fattore di auten-

[26] Il cd. Digital Wallet colud-based è identificato dalla caratteristica della memorizzazione delle credenziali di pagamento nel cloud; per questa ragione si parla di Digital Wallet in quanto il loro utilizzo prescinde dalla presenza di un M-Device (cfr. cap. 2).

ticazione è protetta dagli ulteriori livelli necessari al completamento del processo.

1.2.5.1 Autenticazione dello user 3-Domain Secure

Il protocollo denominato 3-*Domain Secure* (3DS)[27] è un sistema di autenticazione condotto tramite App integrabile nei *wallet* e nei digital payment in generale. Si tratta di un protocollo di messaggistica nato per ridurre l'uso fraudolento di carte online; esso è utilizzato anche per proteggere i *merchant* dal rischio di illecito storno dei pagamenti ricevuti.

EMV®Co ha recentemente pubblicato una nuova versione di 3DS, che consente agli emittenti e agli esercenti di scambiarsi dati relativi al rischio, come sopra identificato, durante il processo sia di ID&V, sia durante le transazioni. I *merchant* possono attivare lo standard 3DS nel caso di transazioni a rischio maggiore che richiedono un'autenticazione più robusta. In questi casi, nel momento in cui lo *user* avvia il pagamento sul sito web *mobile* del *merchant*, le informazioni sull'acquisto, i dati del dispositivo e altri dettagli vengono inviati all'emittente affinché autentichi il titolare della carta e confermi l'acquisto. L'emittente può alternativamente autenticare passivamente il titolare della carta o, in base al profilo di rischio, utilizzare l'autenticazione potenziata e chiedere al titolare della carta di inserire una password unica o rispondere a una chiamata telefonica (Figura 1.4).

[27] Per approfondimenti, le specifiche tecniche di EMV®®®® 3-D Secure sono disponibili al seguente sito:
https://www.EMV®®®co.com/EMV®®®-technologies/3d-secure/.

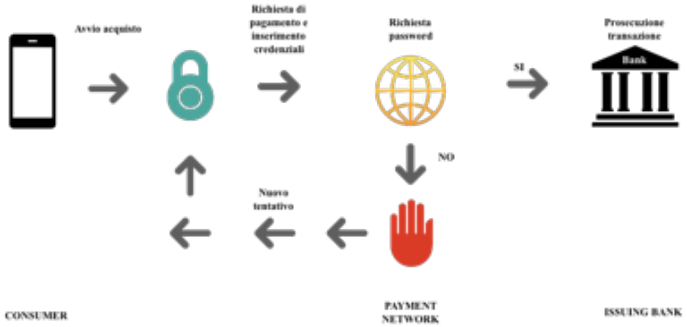

Fig. 1.4 – Rappresentazione del funzionamento del 3-D Secure

1.3 L'ecosistema dell'*M-Wallet*

Il sistema dei pagamenti tramite *M-Device* è un esempio perfetto di ecosistema[28], perché a differenza di altri settori (e di altre modalità di pagamento) è caratterizzato dalla presenza di molteplici attori principali e coprotagonisti, appartenenti a settori anche estranei l'uno all'altro, ma che, interagendo tra loro, danno vita a quella che potremmo definire *M-Payment industry*. Tra i due estremi della transazione, *user* e *merchant*, operano diversi *player* che variano dagli MNO, alle istituzioni finanziarie, dai produttori di dispositivi *mobile*, di *software* e fornitori di

[28] Un ecosistema di *business* rappresenta l'interazione tra diversi settori, consentendo di mettere in luce gli elementi che connotano l'esistenza di una pluralità di soggetti, che operano in un unico ambiente di riferimento e contribuiscono a comporre un'unica entità (Panetta e Leo, 2017; Chesbrough e Appleyard, 2007).

tecnologia, ai *Regulator* e *Supervisor* attivi nei diversi settori produttivi coinvolti[29].

Ognuno di questi soggetti può assumere nel sistema ruoli differenti. A seconda della prevalenza del ruolo assunto da uno o più soggetti e dalle modalità d'interazione tra gli stessi, è possibile identificare strategie e *business model* che variano nel tempo e nello spazio. Per facilitarne l'esplorazione, l'ecosistema può essere suddiviso nei sottoinsiemi *Tech-Ecosys*, *Fin-Ecosys*, *Net-Ecosys* (Fig. 1.5)

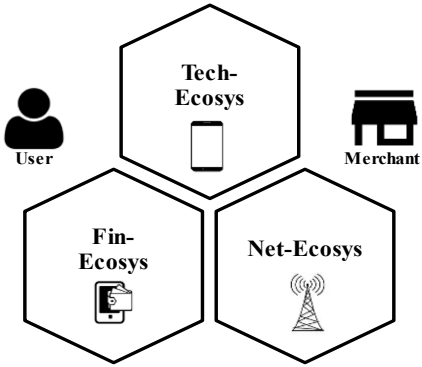

Fig. 1.5 - Rappresentazione del TechFinNet-Ecosys del M-Payment industry
Fonte: Panetta e Leo (2017), pag. 98.

L'intero ecosistema così rappresentato, di fatto, riproduce sinteticamente le componenti del mercato: la domanda, rappresentata da *user* e *merchant* (rammentando che ci si trova in un *two sided market*), e l'offerta costituita

[29] Contini *et al*. (2011); Dahlberg et al. (2007); FINsights (2008); Karnouskos e Fokus (2004); Lu et al. (2011); Pandy (2014).

dai tre *sub-ecosys*.

I due *player* che di fatto devono essere "convinti" a ricorrere ai servizi di *M-Payment* sono gli *user* e i *merchant;* pur se costituiscono entrambi le componenti della domanda, esprimono preferenze parzialmente differenti, ma complementari:

- gli esercenti[30] hanno generiche aspettative direttamente associate al regolamento della transazione in termini di rapidità, certezza e basso costo dello stesso, e indirettamente connesse alla soddisfazione del cliente e alla sua fidelizzazione. Nel caso degli *M-Wallet* come si avrà modo di approfondire, manifestano anche esigenze commerciali complesse (vedi Cap. 2);
- il consumatore[31], invece, è il principale decisore di acquisto: di fatto è colui che decide in via esclusiva e non condizionata di dotarsi di *M-Device*, di scegliere e scaricare App, di renderle operative (collegando ad esempio una carta di pagamento) e, infine, di usufruire o meno del servizio di *M-Payment*. Tra le variabili un ruolo importante nella decisione è giocato dalla velocità, trasparenza e sicurezza del processo, dalla facilità di utilizzo e dal livello di personalizzazione.

Non è sempre agevole definire in modo univoco il ruolo di ciascun attore all'interno dell'ecosistema. Si pensi ad esempio all'esercente che assume con riferimento ad un *wallet* il ruolo di:

---

[30] First Data (2011).

[31] Ewing et al. (2013).

- semplice *wallet Acceptor*, ovvero esercente che include lo specifico *wallet* tra gli strumenti di pagamento a disposizione del cliente;
- *wallet owner o service provider*, ovvero il titolare di un *wallet* che consente alla propria clientela di conservare in un unico luogo le credenziali di uno o più strumenti di pagamento e di trasferire i fondi solo a proprio vantaggio, o a favore di differenti soggetti;
- nel caso in cui sia un produttore di *M-Device*, assumere la triplice veste di *merchant* puro, *wallet acceptor* e *wallet owner*.

Pertanto, ogni soggetto all'interno dell'ecosistema può assumere - e di fatto assume - un ruolo apparentemente di pertinenza di un altro settore o sub-ecosistema.

Con la locuzione ***Tech-Ecosys*** si intende rappresentare l'insieme di prodotti, servizi e soggetti che si riconoscono, interagiscono ed evolvono intorno a un prodotto o tecnologia particolari, i quali con una stretta rete di relazioni e interazioni che producono valore, danno vita all'ecosistema stesso. I protagonisti di questo ecosistema sono di fatto i produttori delle tecnologie impiegate nell'hardware e nel software utilizzati nei diversi servizi di pagamento[32] con *M-Device*. In primo luogo, vi sono i produttori di dispositivi mobili e i fornitori di software e di tecnologie, che registrano una presenza costante in ogni sistema di *M-Payment*, indipendentemente dal modello di *business* adottato dai singoli soggetti che erogano il servizio. Tale peculiare ruolo li porta, in genere, a poter

[32] Hayashi e Klee (2003).

essere considerati alla stregua di "*Integration partner*" nell'erogazione del servizio di pagamento, quand'anche, non sono essi stessi ad erogare il servizio (*service provider*).

I ruoli che specifici soggetti assumono nell'ecosistema ne definiscono anche i compiti all'interno dello spazio economico, che è identificato dalle soluzioni implementate. È il caso ad esempio dei:

- *Token Service Provider* (TSP), vale a dire coloro che gestiscono il ciclo di vita di un token. I servizi tipici offerti da un TSP sono:
    - la creazione e archiviazione dei token;
    - la gestione del ciclo di vita del token;
    - l'elaborazione di transazioni tokenizzate;
    - l'esecuzione di *token-to-PAN mapping*;
    - il riconoscimento del titolare della carta, compresi i servizi di *provisioning*;
    - la gestione delle chiavi nei *device-centric wallet* che usano la tecnologia HCE;
    - i servizi di verifica per transazione e *device*, compresa la convalida crittografica e restrizioni di controllo del dominio;
- *Trusted service manager* (TSM), coloro che collegano i fornitori di servizi (come banche emittenti, depositi di token e *merchant*) e i controllori del *device* di pagamento o il sistema operativo dello stesso. Il TSM facilita il *provisioning* e la gestione di elementi sicuri che vengono inviati al dispositivo *mobile*, quali token e chiavi crittografiche.

Con la locuzione ***Net-Ecosys*** si vuole, invece, intendere la vasta area dei soggetti che competono e collaborano nell'offerta dei servizi di comunicazione intersoggettiva

tramite *M-Device*. Ovvero tutti i *player* che operano nei servizi di connessione, trasmissione e comunicazione.

L'ecosistema così definito tiene conto dei mutamenti nei comportamenti dei singoli operatori economici e degli utenti, innescati dal *World Wide Web* e accelerati dall'evoluzione degli *M-Device*. Questi ultimi, infatti, hanno determinato, tra le altre cose, la necessità/opportunità per i *player* di questo ecosistema di strutturare combinazioni di prodotti/servizi che tengano conto:

- da un lato di *user* sempre più connessi per finalità informative (*infoteiment*), lavorative (*call-conference, file sharing, e-envoicing*, ecc.), ricreative (audio/video on demand, *social network, gaming/betting online*, ecc.), di investimento (*trading online*) e di *shopping online*;
- dall'altro di *merchant* costantemente connessi tra loro per finalità di approvvigionamento dei magazzini, di gestione degli ordini, ecc..

Infine, l'ecosistema finanziario, ***Fin-Ecosys*** esamina lo spazio definito con l'individuazione di quegli operatori che forniscono servizi di pagamento a favore degli *user* tramite *M-Device*. Tenuto conto della realtà operativa si tratta di un insieme più ampio della fattispecie dei *Payment Service Provider* (PSP), i cui profili sono specificati dalla regolamentazione esistente nei singoli Paesi. La dimensione "Fin" di questo ecosistema non è tanto identificata dalla natura finanziaria degli attori coinvolti, che, invero, possono appartenere a settori molto diversi e distanti tra loro, quanto piuttosto dal contenuto finanziario della prestazione del servizio finale offerto all'utente: pagamento tramite *M-Device*. Il ruolo svolto in generale dai

provider di servizi di pagamento è quello di fare in modo che gli strumenti e i servizi gestiti siano usufruibili, sia in termini tecnici che di convenienza, attraverso il canale *mobile*. Un esempio è costituito dai circuiti delle carte di pagamento (*payment network*) che partecipano attivamente allo sviluppo dei servizi di *M-Payment* prima e degli *M-Wallet* più di recente, seppur probabilmente per una strategia difensiva. Con l'avvento del canale internet si sono sviluppate figure in grado di offrire agli esercenti la possibilità di "processare" i pagamenti attraverso carte e *credit transfer*, senza la necessità di avere un rapporto bancario o con gli emittenti delle carte; stiamo parlando dei cosiddetti *aggregator* o *payment gateway*.

Il Fin-Ecosys si presenta pertanto popolato non solo da vecchi e nuovi player alla ricerca di nuovi modi di convivenza, ma anche da istituzioni dai confini produttivi non sempre chiaramente definiti e comunque in evoluzione.

Nell'ambito di questo lavoro ci si soffermerà (Cap. 3) sulle strategie perseguibili dagli intermediari finanziari nell'offerta di *M-Wallet*.

Sabrina Leo è Ricercatore TD in Economia degli intermediari finanziari presso Sapienza Università di Roma. Per lo stesso ateneo è docente di Economia degli intermediari finanziari. È stata Osservatore scientifico dell'*Italian Advisory Board* presso la *Taskforce on Social Impact Investments* del G8. I suoi principali temi di ricerca riguardano il credito, il Credit Crunch, la microfinanza, i Social Impact Investments, l'IT governance nelle banche, i Digital Payments, il Sustainable banking, la regolamentazione degli Intermediari finanziari non bancari e la finanza del settore Audiovisivo.

Ida Claudia Panetta è Professore Associato in Economia degli intermediari Finanziari presso Sapienza Università di Roma. Per lo stesso ateneo è docente di Economia dei mercati e degli intermediari finanziari internazionali e di Economia e gestione della banca, modelli di business e organizzazione. È coordinatrice dell'*Economic Sciences Working Group del CIS-Centro di Ricerca di Cyber Intelligence and Information Security* della Sapienza e membro del *CINI Cyber Security National Lab*. I suoi principali temi di ricerca riguardano il liquidity risk management, gli schemi di garanzia del credito, la regolamentazione del settore finanziario, l'IT governance e la corporate governance nelle banche e, più di recente, la cyber-security nel sistema finanziario e i Digital Payments.

Per comprendere le dinamiche attuali e prospettiche della *Mobile Wallet Industry* occorre soffermarsi sull'intricato intreccio di relazioni che si instaurano tra i diversi attori sul lato della domanda e su quello dell'offerta. Compito, questo, non semplice perché non è agevole l'identificazione univoca dei diversi soggetti che interagiscono in questo ecosistema. Sul lato della domanda bisogna distinguere le due componenti, quella degli *user* e dei *merchant* che esprimono preferenze differenti anche se complementari; dall'altro accanto ai provider tradizionali, vi sono anche i *merchant*, che seppur attivi sul versante *demand*, possono essere *Mobile Wallet Issuer*.
Il lavoro fornisce le chiavi interpretative per l'accesso alla *Mobile Wallet Industry*, utilizzando per tale fine il caso americano. La scelta dell'esperienza americana è giustificata dal fatto che le tecnologie sfruttate da questo prodotto sono native degli Stati Uniti, così come i primi e i principali wallet *digitali*.

ISBN 978-88-3293-282-9

Euro 12,00