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 2.
I modelli di *M-Wallet*

Premessa

Nel presente capitolo si intende fornire una panoramica su quelli che sono stati identificati come modelli prevalenti di *Mobile Wallet* negli Stati Uniti. Le tipologie di modelli operativi di seguito presentati si basano su una rielaborazione della tassonomia in genere utilizzata in questo mercato (U.S. *Payments Forum and Secure Technology Alliance*, 2018; Pandy e Crowe, 2017) e derivano la loro fisionomia dalla combinazione di una varietà di piattaforme tecnologiche, processi e strumenti di sicurezza, nonché degli attori coinvolti. Chiude il capitolo un confronto tra i principali *wallet* attivi negli Stati Uniti mettendo in risalto le principali tecnologie sfruttate e i servizi offerti.

2.1 I *Device-centric Mobile Wallet*

Quando si parla di *M-Wallet* si fa in genere implicitamente riferimento al cosiddetto *Device-Centric Mobile Wallet*, qualificato dalla caratteristica della memorizzazione delle credenziali di pagamento in un dispositivo *mobile*.

Questo modello ricomprende diverse fattispecie, distinte a seconda che la transazione sia effettuata in prossimità o in remoto, in:

- *Device-Centric Mobile Proximity Wallet;*
- *Device-Centric Mobile in-app Wallet.*

Il primo sfrutta la tecnologia *Near Field Communication* (NFC) o *Magnetic Secure Transmission* (MST) per consentire i pagamenti in presenza; in questo caso è necessario che presso il *Point of Sales* (POS) vi sia un *Point of Interaction* (POI) che "legga" e decodifichi le informazioni provenienti dal dispositivo *mobile* (*tap*, trasmissione magnetica, ecc.). Il portafoglio è abilitato previa autorizzazione esplicita da parte dell'*Issuer* della carta di pagamento o del conto del *consumer*; tale autorizzazione prevede l'identificazione del *consumer* e la verifica del possesso delle credenziali di pagamento. Successivamente all'ID&V viene rilasciato un token per il pagamento in senso stretto, che rappresenta un elemento di sicurezza nelle transazioni *mobile*: esso, come anticipato, è sostitutivo del numero di conto principale (PAN) e viene rilasciato quando lo *user* effettua l'iscrizione al *wallet*. Una volta generato il token, l'App di pagamento nel *wallet* genera un crittogramma dinamico che viene trasferito con il token nel corso della transazione. La sicurezza di quest'ultima è garantita anche dal sistema di sicurezza di accesso all'App stessa. Di fatto questa tipologia di *wallet* scinde i processi legati all'ID&V (Figura 2.1) dal cosiddetto *transaction flow* (Figure 2.2-2.3). Generalmente, questi

wallet sono conformi al "*EMV® Payment Tokenization Specification – Technical Framework*"[33].

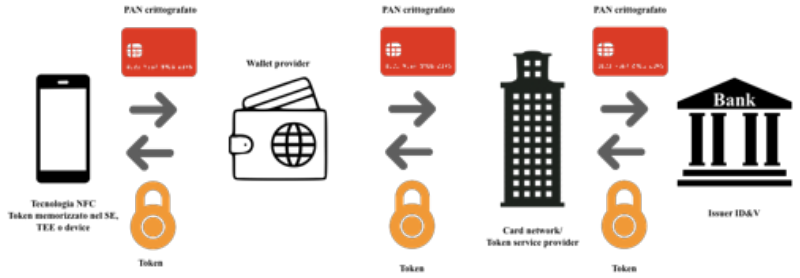

Fig. 2.1 – Rappresentazione del Processo di ID&V

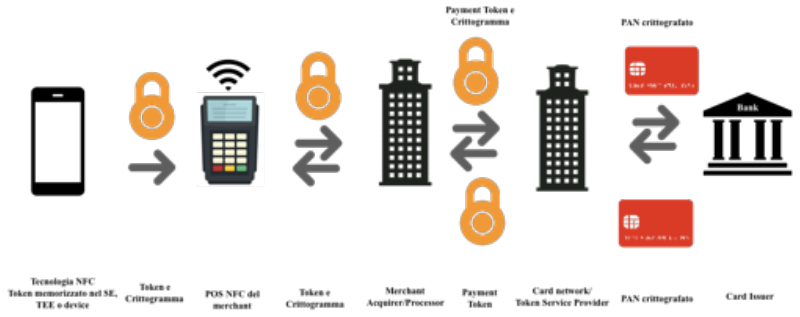

Fig. 2.2 – Rappresentazione del Transaction Flow con Device-centric Mobile proximity Wallet

A caratterizzare ulteriormente questa tipologia di MW è il sistema operativo dell'*M-Device*, in quanto le App di

[33] EMV® Payment Tokenization Specification – Technical Framework, Versione 2.0, EMV®Co, Settembre, 2017.

pagamento sono integrate con lo specifico sistema operativo del dispositivo[34].

I *Device-Centric Mobile Proximity Wallet*, inoltre, sono considerati *open-wallet*, in quanto consentono, da un lato, di associare qualsiasi carta di credito o debito idonea (*wallet* orizzontale) e, dall'altro, di essere "accettati" da ogni *merchant* abilitato o dotato di un POI idoneo (NFC o MST).

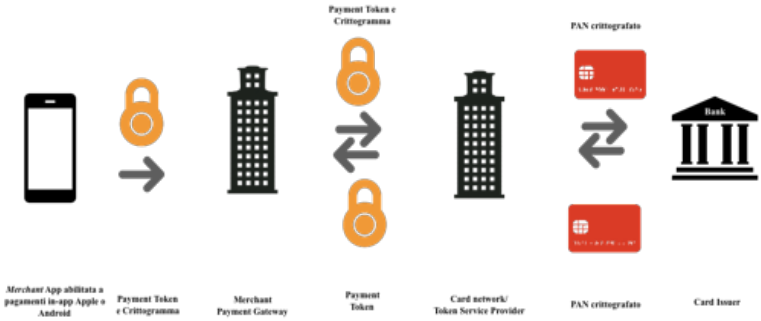

Fig. 2.3 - Rappresentazione Transaction Flow con in-app Device-centric Mobile (con tokenizzazione)

Nei *Device-Centric Mobile in-app Wallet* l'*M-Device* è utilizzato per condurre transazioni tramite le cd. *in-app Card Not Present* (*in-app* CNP). Si tratta di una modalità di intermediazione delle transazioni in remoto, o comunque senza la necessità per chi riceve il pagamento di un POI. Il modello di MW in oggetto consente di fatto transazioni di

[34] Si pensi ad esempio ad Apple Pay che funziona solo su dispositivi Apple®, o a Google Pay e Samsung Pay che lavorano solo su dispositivi con sistema operativo Android.

e-commerce in-app e pagamenti tokenizzati *mobile* effettuati utilizzando le applicazioni dei *merchant*, oppure attraverso il *mobile browsing* (un esempio può essere il pulsante Apple Pay® nei siti degli esercenti). Nella sostanza tali tipologie di *wallet* essendo abilitate per effettuare *remote payment* consentono comunque allo *user* di concludere la transazione presso l'esercente, ma senza la necessità di avvicinare il *device* ad un lettore abilitato.

Quando l'App utilizzata per effettuare gli acquisti non è quella nativa del *merchant* (*closed-loop wallet*, ad esempio l'App di Starbacks), il *wallet* utilizza l'ID&V e la tokenizzazione dei pagamenti EMV®. Le credenziali di pagamento con token possono essere memorizzate alternativamente nel telefono cellulare o nel *cloud*. I consumatori si autenticano e autorizzano il pagamento con un codice biometrico o un *passcode*.

Vala pena sottolineare, infine, che in generale i *Device-Centric Wallet* sono offerti da *Issuer* non finanziari, prevalentemente *Third Parties Operator e merchant*.

2.2 I *Device-agnostic Wallet*

La seconda grande famiglia di *wallet* è costituita da quelle tipologie di portafogli che possono essere utilizzati anche senza *M-Device*. Si tratta di portafogli che spesso hanno temporalmente preceduto la nascita degli *M-Wallet* e che possono essere utilizzati sia tramite web, sia tramite *mobile web*, che tramite App.

A questa tipologia di *Digital Wallet* appartengono i cosiddetti *CNP Card-on-File (CoF)*. *Card-on file* si riferisce al fatto che le credenziali relative allo strumento di pagamento collegato al *wallet*, sono memorizzate presso il *Service Provider* sia esso un *merchant* o un fornitore di servizi di pagamento (PSP); ciò consente al consumatore di effettuare transazioni CNP ripetute o automatiche, senza reinserire le credenziali di pagamento ogni volta. I dati di pagamento memorizzati possono essere utilizzati da uno o più *merchant* che hanno integrato questa tipologia di *wallet* come soluzione di pagamento tra quelle disponibili per la propria clientela (alcuni esempi sono PayPal®, Pay with Amazon® o l'App nativa del venditore).

Vale la pena precisare che il servizio non è fornito dal soggetto che ha emesso lo strumento di pagamento, quanto piuttosto dal fornitore del portafoglio digitale; in generale questi *wallet* CoF accettano più strumenti di pagamento quali carte di credito, di debito, carte prepagate, *giftcard*, carte di credito ACH, ecc...

I CoF offerti da PSP sono considerati *open-wallet*, non solo perché sono ancorabili a quasi tutti gli strumenti di pagamento e perché sono slegati dagli *M-Device*, ma anche perché possono essere utilizzati presso qualsiasi commerciante aderente al circuito.

Dal punto di vista dei *merchant* la facilità di utilizzo è garantita dall'implementazione nel proprio sito di *e-commerce* delle diverse modalità di pagamento presenti. Essi, infatti, oltre a creare un *wallet* proprietario possono utilizzare le interfacce di programmazione API per aggiungere portafogli CoF offerti da PSP (ad esempio Pay with Amazon® o PayPal®). In questo caso al momento

dell'acquisto lo *user* seleziona la modalità di pagamento desiderata, accede al *wallet* e procede a finalizzare l'operazione. Quando, invece, il CoF è offerto dal *merchant*, lo *user* dovrà procedere alla creazione di un account sul quale registrare le informazioni relative alla carta di pagamento da utilizzare per gli acquisti futuri.

Esistono diversi tipi di autenticazione che riguardano la carta, il cliente e il dispositivo. Ai fini del presente lavoro, ciò che rileva è l'autenticazione del cliente, ovvero il processo di verifica dell'identità del soggetto che consente di abbinare la titolarità dello strumento di pagamento al possessore del *wallet*.

La maggior parte dei PSP e dei grandi *retailer* richiedono al consumatore di creare un nome utente e una password per accedere al portafoglio digitale. In più, il PSP può attivare procedure aggiuntive di autenticazione più o meno forte dell'utente. Al primo utilizzo il titolare di una carta di pagamento collegata al *wallet* si autentica con le credenziali di accesso, permettendo al PSP o al *merchant* di effettuare l'abbinamento *on file* tra il nome del titolare e la carta di pagamento che legittima la transazione. Ulteriori codici di sicurezza possono essere richiesti per verificare che il titolare sia in possesso della carta (ad esempio il CVV) e/o avviati sistemi di verifica dell'indirizzo (AVS) per un'ulteriore autenticazione.

Fanno parte dei *Device-agnostic wallet* anche i cd. *Digital wallet cloud-based*. Tale tipologia di portafoglio digitale è caratterizzata dal fatto che le informazioni di pagamento, utilizzate per avviare e autorizzare la transazione, sono memorizzate su un server remoto sicuro, appunto un cloud, anziché nell'*M-Device*. In tali tipologie di portafogli

digitali le autorizzazioni o il token non vengono inviati al *merchant*, ma all'*M-Device* che avvia il pagamento, e successivamente da questo al terminale di pagamento.

I *Digital wallet cloud-based* sono offerti sia dai *merchant* che dai PSP. Essi sono caratterizzati da maggiore flessibilità poiché non sono necessariamente legati all'utilizzo di POS; questo perché il *DW-cloud-based* non àncora l'acquisto al pagamento e supporta tutti i metodi di pagamento, tradizionali e innovativi, che possono offrire all'esercente opzioni meno costose. Il *Wallet cloud-based*, quindi, non è legato all'utilizzo di uno specifico *M-Device*, per questo è chiamato più genericamente portafoglio digitale. Ciò richiede che sia il commerciante che lo *user* siano iscritti allo stesso circuito, o che, a seconda della soluzione di portafoglio, i clienti siano registrati presso un fornitore di DW prima di effettuare un pagamento.

Il processo tipico di transazione prevede che lo *user* sia in possesso di un'App specifica e che sia iscritto al servizio. L'*M-Device* diventa un'estensione del POS, che comunica le informazioni sulla transazione di pagamento al cloud per l'autorizzazione. Una volta completato il pagamento lo *user* riceverà una notifica di avvenuta transazione tramite e-mail o messaggi di testo.

Un'altra tipologia di *wallet device-agnostic* è costituita dai cosiddetti QR Code *wallet*. Si tratta di portafogli CNP basati su *cloud* che consentono di concludere acquisti in presenza presso esercenti dotati di POI in grado di "leggere" QR Code. Quando il QR Code rappresenta un numero di carta questo può essere crittografato.

Attualmente il QR Code per eseguire un pagamento al POS può essere fornito dallo *user* o dal *merchant*.

Nel primo caso la generazione del QR Code può avvenire in due modi: o lo *user* scansiona al POS un QR Code memorizzato sul MW e precedentemente generato, o l'App del *wallet* genera un codice dinamico monouso, che viene presentato al *merchant*.

L'implementazione di tale tipologia è facile e poco costosa in quanto dal lato dello *user* i QR Code possono essere generati da numerose App, dal lato del *merchant* il POS ha bisogno solo di uno scanner e di un software di lettura del codice.

Nel secondo caso, invece, il QR Code è generato dal terminale POS dell'esercente, che il cliente scansiona con la fotocamera del cellulare. Il MW dello *user* utilizza le informazioni ottenute dal codice QR per avviare la transazione di pagamento.

Si tratta in genere di *wallet closed-loop* utilizzati da alcune grandi catene negli States. I QR Code sono utilizzati anche dai distributori di benzina per identificare o autorizzare le pompe di carburante.

L'uso di codici QR nei portafogli digitali ha avuto una grande diffusione, soprattutto presso istituti finanziari e commercianti, per i seguenti motivi:

- facilità di implementazione: gli esercenti possono utilizzare i loro attuali scanner di codici a barre presso il POS, che si basano su standard di progettazione del settore, per leggere i QR Code;
- non è richiesto l'NFC sull'*M-Device*;
- facilità d'uso: utilizzando una fotocamera del cellulare e la relativa App *mobile*, gli *user* possono scansionare i QR Code non solo per effettuare pa-

gamenti, ma anche per accedere a siti Internet, scaricare prodotti o trovare recensioni e informazioni sul prodotto.

Tuttavia, oltre a quanto analizzato in termini sicurezza nel capitolo che precede questa soluzione presenta dei punti di debolezza:

- a differenza di quanto accade per la loro progettazione, non ci sono standard per l'utilizzo dei QR Code nei pagamenti. Ciò vuol dire che le soluzioni di implementazione e le specifiche tecniche sono differenti per ogni esercente con *user experience* diverse;
- il processo con il quale il POS "legge" il QR Code non è semplice come quello "*touch and pay*" NFC.

Infine, si stanno affermando *wallet* digitali offerti da *payment network* (tipicamente gli emittenti di carte di credito) che offrono servizi integrati sia agli *issuer* che ai *merchant*. Si tratta dei cosiddetti *Digital Checkout Wallet* accessibili attraverso i canali web, *m-App*, e *in-app*[35]. Essendo un servizio offerto attraverso *payment network*, ai tradizionali canali di accesso si può aggiungere quello diretto utilizzando le credenziali bancarie o del PSP dello *user*. Questo approccio può avere l'indubbio vantaggio di aggregare in un'unica *App* tutti gli strumenti, nonché l'accesso diretto ai conti a disposizione dello *user*.

Le credenziali di pagamento possono essere memorizzate e utilizzate come credenziali CoF, in modo che il consumatore non abbia bisogno di reinserirle ogni volta che effettua un acquisto tramite *wallet*. A seconda della moda-

[35] In alcuni casi sono possibili acquisti in presenza CNP *contactless*.

lità di accesso al portafogli, gli *user* potrebbero doversi autenticare con una password o un fattore biometrico, ad esempio un'impronta digitale.

La registrazione dei consumatori è un prerequisito per questi portafogli, e può avvenire attraverso tre opzioni:

- preiscrizione tramite la piattaforma di online banking o di *M-Payment* dell'emittente;
- preiscrizione attraverso il sito;
- iscrizione precedente all'acquisto.

Per iscriversi, lo *user* crea un nome utente e una password e inserisce anche il proprio nome, indirizzo e-mail e numero di cellulare. Le informazioni personali e le credenziali di pagamento possono essere inserite manualmente o utilizzando la fotocamera sul *device* per scansionare la carta di pagamento dell'*Issuer*. Se le informazioni vengono scansionate, il codice di sicurezza della carta deve essere inserito manualmente. Lo *user* potrebbe anche aver bisogno di rispondere a domande di sicurezza per facilitare l'autenticazione futura o ripristinare una password dimenticata. Al termine dell'iscrizione, lo *user* riceve una conferma via e-mail.

I *Digital Checkout Wallet* basati sulla rete di pagamento (*network*) eliminano la necessità per i *merchant* di raccogliere o archiviare le credenziali di pagamento in chiaro.

Per effettuare un acquisto, lo *user* clicca sull'icona nel carrello del sito del *merchant*, accede all'account di pagamento o utilizza le credenziali memorizzate nell'App e conferma il pagamento. Per una maggiore protezione, il PAN completo non viene visualizzato durante la procedura di pagamento sul sito web del *merchant*.

Il *transaction flow* con i *Digital Checkout Wallet* (Figura 2.4) può essere meglio spiegato come segue:

- lo *user* accede al sito di *e-commerce* tramite il browser *mobile* o l'App *mobile*. Al momento del pagamento, lo *user* accede al *wallet* per confermare le informazioni di spedizione e autorizzare il pagamento;
- quando lo *user* avvia il pagamento, il token di pagamento viene inviato al sito del *merchant*;
- il *merchant* passa il token al gateway come parte della richiesta di autorizzazione;
- lo *user* riceve il token e lo invia, insieme alla richiesta di autorizzazione, all'*Issuer*;
- il network di pagamento/fornitore di servizi token invia il token/PAN, i dettagli della carta di pagamento e la richiesta di autorizzazione all'emittente;
- l'emittente invia la decisione sull'autorizzazione e il token/PAN al *network* di pagamento, che indirizza il token e il messaggio di autorizzazione all'*acquirer*;
- viene infine inviato un messaggio di conferma allo *user*.

Per impedire l'accesso non autorizzato alle credenziali di pagamento, queste soluzioni applicano molteplici livelli di sicurezza e solidi sistemi di gestione dei rischi monitorando il comportamento dei titolari di carte e degli account per prevenire le frodi.

Ovviamente, anche in questo caso, il successo del *wallet* dipende dalla diffusione presso i *merchant*.

Fig. 2.4 – Rappresentazione del Transaction Flow con Digital Checkout Wallet

2.3 I *Person to Person Wallet*

Con il termine *Person to Person Payment* (P2P) si intendono tutti quei servizi che consentono il trasferimento di denaro tra due persone fisiche, e che – in genere – non servono per intermediare una transazione commerciale[36]; in questi casi, infatti, non si parla di *consumer* e *merchant*, ma piuttosto di *sender* e *receiver*. Si tratta di una tendenza generale, in quanto questa modalità ricomprende anche transazioni legate, ad esempio, al riuso di beni nelle piattaforme dedicate allo scambio di oggetti senza configurare un'attività commerciale in senso stretto.

I pagamenti P2P sono considerati un *M-Payment* quando o il *sender* o il *receiver*, o entrambi, utilizzano un *M-Device* per il trasferimento di fondi: in questi casi si ha rispettivamente la fattispecie del *mobile to cash* (M2C), *cash to mobile* (C2M) o *mobile to mobile* (M2M).

Il P2P a seconda della destinazione finale dei fondi è definito domestico o internazionale. All'interno di

[36] Holden (2013b).

quest'ultima fattispecie è possibile ricondurre il fenomeno del *M-Remittance*, ovvero le rimesse di denaro degli emigrati nei propri Paesi d'origine (*Alternative Rails*, nel mercato americano). Nella successiva Tabella 2.1 sono riassunte le principali tipologie di *wallet* in oggetto includendo le tecnologie necessarie al loro utilizzo.

Tab. 2.1 – Principali tipologie di P2P Wallet

Destinazione dei fondi	**Possesso *M-Device***	**Funzioni dell'*M-Device* richieste**	**Tipo di *M-Device***	**Protocolli di connessione**
Domestica	M2C	SMS, M-App		A partire dal 2G
	C2M			
	M2M	M-App, NFC/BLE		
Internazionale	M2C	SMS, M-App		
	C2M			
	M2M	M-App, NFC/BLE		

Fonte: Panetta e Leo (2017), pag. 74.

Dal punto di vista operativo[37] è possibile distinguere tra servizi P2P offerti a soggetti che appartengono alla stessa piattaforma di trasferimento fondi, o a piattaforme distinte. La piattaforma può essere costituita/offerta, ad esempio, dalla stessa banca utilizzata sia dal *sender* che dal *receiver*, o da una piattaforma terza creata da un consorzio di banche o più genericamente da PSP; oppure, infine, da un soggetto terzo che, in base ad accordi stipulati con PSP, offre la possibilità di effettuare trasferimenti di

[37] Per approfondimenti Kohli (2013).

denaro (ad esempio PayPal® o in generale *M-Wallet* orizzontali).

Caratteristica distintiva di questi tipi di trasferimenti è costituita dall'identificazione, sia del *sender*, che del *receiver* tramite indirizzo e-mail o tramite numero di telefono cellulare. Nel caso in cui entrambi i soggetti coinvolti nella transazione di P2P (M2M) siano afferenti alla stessa piattaforma, il trasferimento dei fondi avviene in modo istantaneo; viceversa negli altri casi il processo di identificazione e trasferimento dei soggetti si esaurisce in più fasi: il *receiver*, identificato attraverso l'indirizzo mail o numero di cellulare, ricevuta la comunicazione dell'esistenza di un trasferimento a proprio favore, dovrà accedere alla piattaforma, inserire il proprio numero di conto corrente, digitare il codice di sicurezza e accettare il trasferimento dei fondi

A differenza di altri contesti geografici, i P2P *wallet* sono poco sviluppati negli USA; solo in tempi più recenti si stanno diffondendo come un servizio aggiuntivo al *wallet* originario, oppure su impulso o in modo complementare allo sviluppo delle piattaforme di *social network*.

2.4 Altre tipologie di *M-Wallet*

Un'altra tipologia di portafoglio digitale non ancora pienamente diffusa è costituita dai cosiddetti *invisible in-app payments*; tramite tale tipologia di strumento i clienti potranno entrare in negozio, scegliere la merce da acquistare e uscire dal negozio senza passare dalla cassa. Il pagamento avverrà automaticamente *in-app*, grazie alla to-

kenizzazione sicura della carta e alla tecnologia basata su onde ultrasonore che permettono il riconoscimento del prodotto acquistato e del cliente, e il collegamento agli strumenti di pagamento (un esempio è costituito da Amazon Go®). Un'altra tipologia di *invisible in-app payment* è quella costituita dalla possibilità di concludere acquisti tramite assistente vocale, in remoto; essa si basa su tecnologie in corso di sviluppo che permettono il riconoscimento vocale e l'associazione degli strumenti di pagamento alle App che gestiscono gli *smart home assistant* (Apple HomePod, Google home, e Alexa).

Nelle tabelle che seguono si fornisce una panoramica sulle principali tipologie di *Digital Wallet* sopra descritte (tabella 2.2).

Tab. 2.2 – Principali tipologie di Digital wallet operativi negli US

Modello	**Tipologia di *wallet***	**Tipo di *accesso***	**Tipo di pagamento**
Device Centric Mobile wallet	*Device Centric Mobile Proximity wallet*	Issuer Mobile App Merchant App	In-Store payment
	Device Centric Mobile In-app	Issuer Mobile App Merchant App	In-App payment
Device-agnostic wallet	*CNP Card-on-File*	Issuer Mobile App Merchant Website Merchant App	In-Store, In-App e e-commerce payment
	QR Code wallet	Issuer Mobile App Merchant App	In-Store e In-App payment
	Digital Checkout Wallet	Issuer Mobile App	In-Store, In-App e e-commerce payment

		Merchant Web-site	
		Merchant App	
Person to Person wallet	Domestico (P2P)	Issuer Mobile App	
		Issuer web-app	
	Internazionale (*M-Remittance* o *Alternative Rails*)	Issuer Mobile App	In-app transfer
		Issuer web-app	
Other *wallet*	Invisible In-app	Issuer Mobi-le App	In-app payments
		Merchant App	

La tabella che segue propone un raccordo con le tecnologie analizzate nel Capitolo 1, focalizzando l'attenzione sui *proximity payment*, e mettendo a sistema i principali modelli operativi di portafogli digitali analizzati in questo Capitolo.

Tab. 2.3 – Principali tipologie di Digital wallet operativi negli US per proximity payment

Modello	**Tipologia di *wallet***	**Tecnologie utilizzate**
Device Centric Mobile wallet	*Device Centric Mobile Proximity wallet*	NFC, HCE, QR code
	Device Centric Mobile In-App	
Device-agnostic wallet	*CNP Card-on-File*	NFC, HCE
	QR Code wallet	QR code
	Digital Checkout Wallet	NFC, HCE
Person to Person wallet	Domestico (P2P)	NFC, HCE
	Internazionale (*M-Remittance* o *Alternative Rails*)	No proximity

2.5 I *Proximity Payment* tramite *M-Wallet*: principali tipologie a confronto

In questo paragrafo si è inteso prendere in esame l'offerta dei MW negli Stati Uniti seguendo la tassonomia adottata nelle pagine che precedono. L'analisi si è focalizzata sui *proximity payment* che rappresentano la maggiore sfida negli USA. Nel 2018, infatti, 55 milioni di persone hanno utilizzato il proprio *M-Device* per effettuare un pagamento in un punto vendita fisico, sia attraverso App *closed-loop* che attraverso MW di tipo *open*. Gli *user* rappresentano circa il 20% della popolazione americana di età pari o superiore a 15 anni, e circa il 25% dei possessori di *M-Device*.

Le variabili rilevate per ciascun portafoglio analizzato riguardano:

- metodo di pagamento;
- *device* compatibili;
- NFC-based *Wallet*;
- richiesta di hardware aggiuntivo;
- compatibilità con i POS;
- funzione pagamenti P2P;
- requisiti di sicurezza;
- servizi aggiuntivi;
- possibilità di caricare Loyalty/Gift Card;
- interazione con Social Media;
- piattaforma Social Media;
- transit System Compatibility;
- livello di accettazione presso i *merchant*.

I prodotti sono presentati in tabelle suddivisi tenendo presente oltre alla tipologia di *wallet* anche sugli *issuer* portatori di strategie differenti.

Dall'analisi è emerso che negli Stati Uniti, la maggior parte degli *M-Payment* è *tap and pay* o *contactless* (Tabella 2.4 e 2.5) affiancate da pagamenti basati su QR Code (Tabella 2.6).

Le tre principali soluzioni di MW NFC disponibili oggi negli Stati Uniti sono Apple Pay®, Android Pay® e Samsung Pay®. Tutte e tre utilizzano l'NFC ma ognuna di loro gestisce e memorizza i token di pagamento EMV®[38] in modo diverso:

- Apple Pay® memorizza i token di pagamento nei SE *embedded* (incorporati nei *device*);
- Google Pay® utilizza l'HCE per archiviare token nel sistema operativo Android®;
- Samsung Pay® utilizza sia l'NFC che l'HCE ma memorizza i token di pagamento e le chiavi crittografiche nel TEE del *device*.

Come accennato precedentemente Apple Pay® utilizza l'*embedded* SE per memorizzare il token di pagamento rappresentativo del PAN. Google Pay® utilizza l'HCE anziché il SE e memorizza una chiave rappresentativa del PAN nel cloud. Samsung Pay utilizza il TEE con NFC, ma supporta anche una seconda tecnologia MST che consente a *device* Samsung® compatibili di trasmettere i dati di pagamento a un POS abilitato a leggere schede a banda magnetica, senza richiedere la tecnologia NFC. Il telefono

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

cellulare emette un segnale magnetico sicuro che riproduce la "strisciata" di una tradizionale carta di pagamento. Per impostazione predefinita, Samsung Pay® utilizza l'NFC se l'*M-Device* rileva un campo NFC sul terminale POS, altrimenti utilizza l'MST. Samsung Pay® supporta la tokenizzazione dei pagamenti EMV® per le transazioni NFC e MST.

Tabella 2.4 Device Centric Wallet offerti da Terze Parti

	Apple Pay®	**Google Pay®**	**Samsung Pay®**
Metodo di pagamento	Carte di credito tradizionali incluso Visa Checkout® e MasterPass®	Carte di credito tradizionali incluso Visa Checkout® e MasterPass®, PayPal checkout®, Raccolta punti	Carte di credito tradizionali incluso Visa Checkout® e MasterPass®, PayPal checkout®, Raccolta punti
Device compatibili	iPhone® e iWatch®	Android®	Samsung Galaxy® *device*
NFC-based *Wallet*	NFC	NFC	NFC, MST
Richiesta di hardware aggiuntivo	SE enbedded	HCE	SE enbedded
Compatibilità con i POS	SI	SI	SI
Funzione pagamenti P2P	SI	SI	NO
Requisiti di sicurezza	PIN, impronta digitale, riconoscimento biometrico	PIN, impronta digitale	PIN, impronta digitale
Servizi aggiuntivi	Promozioni offerta	Salvataggio dati	Salvataggio dati

	sconti, premi su acquisti in-app e web, salvataggio dati dell'account della carta, salvataggio/rimborso coupon	dell'account della carta, salvataggio/rimborso coupon, salvataggio biglietti del treno monorotaia Las Vegas	dell'account della carta, salvataggio/rimborso coupon, raccolta premi Samsung Pay
Possibilità di caricare Loyalty/Gift Card	SI	SI	SI
Interazione con Social Media	NO	SI	SI
Piattaforma Social Media	Facebook®	Google+®	Facebook®
Transit System Compatibility	Qualsiasi sistema a tariffa aperta negli Stati Uniti e la metropolitana di Londra	Qualsiasi sistema a tariffa aperta negli Stati Uniti e la metropolitana di Londra	Qualsiasi sistema a tariffa aperta negli Stati Uniti e la metropolitana di Londra
Livello di accettazione presso i *merchant*	Milioni di POS negli USA e nel mondo	Milioni di POS	Milioni di POS

Tabella 2.5 Device Centric Wallet offerti da Banche

	Capital One®	**City Pay®**	**Chase Pay®**
Metodo di pagamento	Carte di credito Capital One® e MasterPass®	Carte di credito City Pay® e MasterPass®	Carte di credito Chase Pay®
Device compatibili	Android®	Android®	iPhone®, Android®
NFC-based *Wallet*	NFC	NFC	NFC, MST
Richiesta di hardware aggiuntivo	HCE	HCE	N/A
Compatibilità con i POS	SI	SI	SI
Funzione pagamenti P2P	N/A	SI	N/A
Servizi aggiuntivi	Accredito immediato dei premi	N/A	Sistema di pagamento integrato in alcune app *closed-loop* dei *merchant*
Livello di accettazione presso i *merchant*	Presso tutti i POS	Presso tutti i POS	Presso tutti i POS

Nonostante presentino delle criticità, negli Stati Uniti vi sono molti MW che utilizzano il QR Code. I pagamenti basati su QR Code preservano la sicurezza di una transazione presso l'esercente con lettura del codice da parte di un POS. Non è un caso, infatti, che la maggior parte dei *wallet* che utilizzano QR Code sono offerti da *merchant*. A questa fattispecie appartiene ad esempio il *device-centric wallet* di Walmart®[39] che ha la tokenizzizzazione associata al QR Code che protegge le credenziali di pagamento. Più in dettaglio in questo caso, Walmart®, durante la transazione, genera un codice QR che funge da token per autorizzare un pagamento senza esporre (a potenziali occhi indiscreti) il PAN; al livello cd. *back-end*, Walmart® genera e memorizza un token di sicurezza al posto del PAN. Questo portafoglio archivia anche i dati relativi alle carte di pagamento (acquisiti durante la fase di registrazione) sul proprio *cloud* affinché vengano elaborati dopo la conclusione della transazione.

Un altro esempio è costituito da Level-Up®[40], portafoglio che genera in modo casuale un token che viene mappato su un secondo token sul server di Level Up® stesso, che quindi esegue il mapping a un terzo token nel cloud Braintree®[41]. La combinazione di questi token e altri due fattori di autenticazione è necessaria per avviare una transazione.

[39] https://www.walmart.com.
[40] https://www.thelevelup.com.
[41] https://www.braintreepayments.com.

Tabella 2.6 Device Centric Wallet offerti da Merchant

	Starbucks®	**Level Up®**	**Walmart Pay®**	**Yelp Eat24®**
Metodo di pagamento	Carte di credito tradizionali	Carte di credito tradizionali	Carte di credito tradizionali	Pay Pal o Google Pay®
Device compatibili	iPhone® Android®	iPhone® Android®	iPhone® Android®	iPhone® Android®
NFC-based *Wallet*	QR Code sul *device*	N/A	QR Code del *merchant*	N/A
Richiesta di hardware aggiuntivo	NO	N/A	N/A	N/A
Compatibilità con i POS	SI	N/A	SI	N/A
Funzione pagamenti P2P	NO	N/A	NO	NO
Requisiti di sicurezza	N/A	N/A	PIN o impronta digitale	N/A
Servizi aggiuntivi	Sistema di ricarica del creditol	N/A	N/A	N/A
Caricamento Loyalty/Gift Card	SI	SI	SI	SI
Interazione con Social Media	N/A	N/A	N/A	N/A
Piattaforma Social Media	N/A	N/A	N/A	N/A
Livello di accettazione presso i *merchant*	Starbucks®	Level Up®	Walmart®	35.000 ristoranti in 1.500 citta

Tra i *wallet* maggiormente diffusi vi sono quelli offerti da PSP che hanno sviluppato i servizi di checkout per gli acquisti online quali American Express®[42], Mastercard®[43] e Visa®[44] (Tabella 2.7). I tre PSP offrono, ognuno, un approccio diverso: Amex Express Checkout®[45] consente ai titolari di carte di riempire automaticamente i loro dati sui siti commerciali; Masterpass®[46] connette tramite API tutti i DW legati ad uno stesso soggetto; Visa Checkout®[47] viene utilizzato in via prevalente per l'*e-commerce*.

Vale la pena precisare che Visa Checkout® e Masterpass® sono indipendenti dal marchio della carta, i consumatori possono aggiungere qualsiasi carta di credito o debito idonea.

In linea generale i *Device-Agnostic Wallet* non nascono specificatamente per operazioni *in person*, tuttavia si sta diffondendo il loro utilizzo anche per i *proximity payment*; nell'analisi è emerso, infatti, che alcuni di questi (PayPal® e Mastepass®) offrono la possibilità di effettuare pagamenti in prossimità anche presso i POS.

[42] https://www.americanexpress.com.
[43] https://www.mastercard.com.
[44] https://www.visa.com.
[45] Cfr. nota 42.
[46] Cfr. nota 43.
[47] Cfr. nota 44.

Tabella 2.7 Device Agnostic Wallet offerti da Terze Parti/Network Checkout

	Pay Pal®	**Amex Express Checkout®**	**Masterpass®**	**Visa Checkout®**
Metodo di pagamento	Carte di credito tradizionali incluso Visa Checkout® e MasterPass®, PayPal checkout®, AHC	Carte di Credito American Express®	Maggiori carte di credito e di debito	Maggiori carte di credito e di debito
Device compatibili	iPhone® Android®	N/A	Android App®	Google Pay®, Samsung Pay®
NFC-based *Wallet*	NFC, QR Code, le transazioni in-store sono confermate con il numero di telefono associato all'account e il PIN	NO	NFC, MST	NO
Richiesta di hardware aggiuntivo	NO	N/A	N/A	N/A
Compatibilità con i POS	SI	NO	SI	NO
Funzione pagamenti P2P	SI	NO	NO	NO
Requisiti di sicurezza	PIN, impronta	N/A	N/A	N/A

	digitale			
Servizi aggiuntivi	Salvataggio dati dell'account della carta, salvataggio/rimborso coupon	CoF	N/A	N/A
Possibilità di caricare Loyalty/Gift Card	SI	N/A	N/A	N/A
Interazione con Social Media	NO	N/A	N/A	N/A
Piattaforma Social Media	Facebook	N/A	N/A	N/A
Transit System Compatibility	NO	NO	NO	NO
Livello di accettazione presso i *merchant*	Oltre 20.000 *merchant* in USA accettano pagamenti in-store con Pay Pal®	Presso tutti i *merchant*	Presso tutti i *merchant*	Presso tutti i *merchant*

In ultimo viene fornita nella Tabella 2.8 una panoramica sui principali P2P *wallet* attivi in USA, ossia tutti quei servizi che consentono il trasferimento di denaro tra due persone fisiche, e che – in genere – non servono per intermediare una transazione commerciale.

Come specificato precedentemente i P2P a seconda della destinazione finale dei fondi sono definiti domestici o internazionali, o se la destinazione dei fondi è nel Paese di origine *M-Remittance* (*Alternative Rails*, nel mercato americano).

È possibile distinguere tra servizi P2P offerti a soggetti che appartengono alla stessa piattaforma di trasferimento fondi, o a piattaforme distinte, che sono costituite/offerte, ad esempio:

- dalla stessa banca utilizzata sia dal *sender* che dal *receiver*;
- da una piattaforma terza creata da un consorzio di banche o più genericamente da PSP;
- da un soggetto terzo che, in base ad accordi stipulati con PSP, offre la possibilità di effettuare trasferimenti di denaro.

Anche in questo caso alcuni dei MW analizzati (Venmo®[48]) hanno inserito nella loro offerta la possibilità di effettuare pagamenti presso i *merchant*.

Va sottolineato, inoltre, l'avvio della diffusione di Facebook Messenger®[49] che apre (anche da un punto di vista tecnico) a pagamenti digitali anche negli USA che utilizzano piattaforme di messaggistica istantanea avanzati.

[48] https://venmo.com.

[49] https://www.facebook.com/messenger.

Tabella 2.8 P2P Wallet

	Venmo®	**Zelle®**	**Facebook Messenger®**	**Popmoney®**	**Dwolla®**
Metodo di pagamento	Venmo Account, Bank account o carte di debito	Carta di debito	Carta di debito Mastercard o Visa	N/A	N/A
Device compatibili	iPhone®, Android®	iPhone®, Android®	iPhone®, Android®	iPhone®, Android®	iPhone®, Android®
NFC-based *Wallet*	NO, in-app	NO	NO	NO	N/A
Compatibilità con i POS	NO	NO	NO	NO	N/A
Funzione pagamenti P2P	SI	SI	SI	SI	SI
Servizi aggiuntivi	N/A	Invio denaro	Richiesta/invio di denaro via Messenger	Invio denaro	Instant payment e trasferimenti di denaro
Cricamento di Loyalty/Gift Card	SI	N/A	N/A	N/A	N/A
Interazione con Social Media	SI	N/A	SI	N/A	N/A
Piattaforma Social Media	N/A	N/A	Facebook	N/A	N/A
Livello di accettazione presso i *merchant*	*Merchant* selezionati	0	0	0	N/A

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