MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA LOTTA ALLA CONTRAFFAZIONE
UFFICIO ITALIANO BREVETTI E MARCHI

DOMANDA DI INVENZIONE NUMERO	**102012902022544**
Data Deposito	**14/02/2012**
Data Pubblicazione	**14/08/2013**

Classifiche IPC

Titolo

SISTEMA DI PAGAMENTO SICURO SEMPLICE DA USARE ED A BASSO COSTO

Sig. Gaetano Salvo

a Bucinasco (MI)

Sistema di pagamento sicuro, semplice da usare ed a basso costo

I sistemi di pagamento attualmente utilizzati, per i pagamenti con POS di qualsiasi tipo (fisici o virtuali e e-Commerce), basano il loro modello di funzionalità su uno schema che prevede da due a quattro soggetti principali e fondamentali che sono, da un lato :

-Il negoziante (merchant)

-il portatore della carta di pagamento

dall'altro lato

-il soggetto preposto all'acquisizione ed alla gestione della transazione (acquirer)

- il soggetto che ha emesso la carta di credito/ debito (issuer)

Il modello tipico di pagamento elettronico vive su un substrato tecnologico reticolare :

presso il negoziante risiede un terminale EFT-POS (Electronic fund Transfer - Point of Sales) collegato in rete sicura con un gestore di terminali che a sua volta colloquia con i sistemi informativi del soggetto nominato dalla banca/*istituto di pagamento* per autorizzare i pagamenti (e di conseguenza l'accredito delle somme al merchant) e verificare la validità/emittente (ovvero non è in black list) della carta e la disponibilità de della carta . Alcune volte

manca la figura del gestore di terminali (ovvero una figura terza rispetto all'acquairer/issuer) in questo caso il gestore dei terminali è l'acquirer.

Stesso discorso per le-commerce/mobile commerce con la differenza che il POS invece che fisico è virtuale (virtual POS), ovvero i dati caratteristici della carta vengono inseriti manualmente dal card-holder e non come nel caso del pos fisico attraverso la lettura di banda magnetica, chip, rfid.

L'EFT-POS è un dispositivo dotato di sicurezza fisica e logica che garantisce il trattamento dei dati sensibili presenti sulla carta e sulle informazioni inerenti la transazione di pagamento ed il colloquio sicuro con i sistemi del soggetto preposto all'acquisizione ed alla gestione della transazione.

Il POS virtuale è sistema software che utilizzi algoritmi e tecniche che rendono sicura la veicolazione dei dati sensibili della carta e della transazione e/o la loro scrittura sui supporti rilevanti.

Allo stesso modo gli host (centri servizio collegati alla rete) preposti alla concentrazione, alla acquisizione ed alla emissione, garantiscono la sicurezza nella gestione di tali dati in ricezione ed emissione.

Il flusso transazionale , ossia la sequenza delle operazioni necessarie all'autorizzazione del pagamento, passa per l'EFT-POS collocato presso il negoziante, o per i virtual POS nel caso di e-commerce, e viaggia fino al " concentratore " ed al soggetto preposto all'acquisizione ed alla gestione della transazione (acquirer) .

Quando la carta utilizzata è stata emessa dallo stesso soggetto (issuer) che autorizza la transazione (acquirer) e che in genere fornisce il POS, la transazione si definisce transazione on-us.

Se invece issuer e acquirer sono soggetti diversi, la transazione viene indirizzata tramite il soggetto preposto all'acquisizione ed alla gestione della transazione (acquirer) sulla rete di servizi interbancari che provvede ad istradarla presso il soggetto che ha emesso la carta (issuer) che autorizza o nega la transazione.

Ogni tratta percorsa dalle transazione ha un costo per cui le transazioni on-us, risultano molto meno onerose delle transazioni tradizionali evitando la tratta interbancaria e consolidando il costo pertinente al soggetto preposto all'acquisizione (aquirer) e quello pertinente il soggetto che ha emesso la carta (issuer) presso il medesimo soggetto.

Inoltre il costo della transazione, merchant fee, server a remunerare in parte l'issuer (la parte più gande) e in parte l'acquirer.

Risulta pertanto chiaro che nel caso di transazioni on-us il soggetto (issuer=acquirer) massimizza i suoi guadagni e può effettuare al merchant sconti più elevati.

In ambito tecnologico si assiste al proliferare di sistemi " multi banca" ovvero di software client server in grado di ottimizzare la quantità di transazioni on-us e nel contempo si assiste alla nascita di nuove forme di pagamento in cui uno dei nodi reticolari elencati in precedenza cambia la propria forma o i integra con uno o più altri nodi.

Si assiste all'ascesa di dispositivi mobili (telefoni mobili/tablet) dotati di tecnologia NFC (contactless), su cui viene caricata una carta di pagamento e che interagiscono con POS in grado di operare transazioni NFC (Near field communication) e/o in connettività wireless , inoltre si assiste alla nascita

di dispositivi fisici che allegati a telefonini fisicamente o tramite connessioni wireless , sono in grado di rendere il dispositivo cellulare equivalente o quasi ad un POS.

Le soluzioni elencate ed i dispositivi attualmente utilizzati nei sistemi di pagamento non cambiamo l'architettura di base della transazione che richiede in sostanza la presenza di un EFT-POS o di un dispositivo che agisca da POS e legga la carta o recepisca i dati sensibili della carta (e-commerce), sia essa fisica che virtuale, ed un dispositivo che contenga in maniera sicura i dati carta e li comunichi a chi di dovere in caso di transazione.

Il pagamento su web presuppone la presenza di un server sicuro addetto all'archiviazione e mantenimento dei dati delle carte tramite web ed alla gestione di tali dati in una transazione di pagamento. Non è quindi presente un EFT-POS ma i dati sono introdotti manualmente in un PC o telefono o qualsiasi dispositivo connesso alla rete.

Esistono anche sistemi che permettono il salvataggio dei dati della carte presso server sicuri ed il loro utilizzo su richiesta per tramite di codici identificativi non contenenti i dati carta utilizzati su web, o cellulare ovvero qualsiasi dispositivo connesso alla rette.

In ogni caso la transazione web non prevede la persona fisica del portatore della carta presso l'esercizio commerciale , con il conseguente aumento del rischio relativo alla frode ed alla sicurezza dei dati veicolati. Nel caso di pagamento sul mondo web esistono sistemi tipo secure code per rendere più sicura la transazione.

Oggetto del presente trovato è un sistema di pagamento sicuro ed a basso costo che ovvia agli inconvenienti elencati nel rispetto degli attori descritti e delle norme di sicurezza imposte dai circuiti e/o che opera al di fuori dei circuiti (schemi internazionali e locali) e delle reti bancarie nel rispetto delle norme di sicurezza imposte dalla legge.

Secondo il presente trovato il sistema di pagamento sicuro ed a basso costo utilizza un apparecchio "smartphone" ovvero un apparecchio in grado di comunicare in modalità wireless (infrarosso, bluetooth, nfc ecc.), una pluralità e/o nessun apparecchio che funga da ponte a tale comunicazione (a titolo esemplificativo, ma non esclusivo un televisore che recepisca la comunicazione di un telecomando ovvero un televisore con qualunque periferica nativa o aggiunta bluetooth o NFC che recepisca la comunicazione di un telefonino) (i/i dispositivi verranno da ora in poi indicati con il nome di "smartdevice") ed un server (proprietario o appartenente a terzi), sviluppato nel rispetto delle norme PCI DSS e/o al di fuori del perimetro di tali norme quando la sua operatività lo consente e che nel seguito definiremo come "MPOS", per eseguire un pagamento con moneta elettronica sia nel caso in cui il pagamento sia effettuato in negozi reali su strada, sia che il pagamento sia relativo ad e-commerce e /o t-commerce.

In ambedue i casi esistono due tipologie di scenario dei flussi funzionali in relazione al ruolo svolto dallo "smartdevice" nel processo transazionale:

- Uno scenario è quello in cui lo "smartdevice" non contiene i dati carta dell'utente che sono invece memorizzati sull'MPOS parte server del sistema proposto; la responsabilità dello "smartdevice" è quella di

autorizzare l'MPOS ad accedere ai dati carta e di conseguenza eseguire la transazione. Dopo essersi identificato in maniera sicura e univoca con l'MPOS.

- Un altro scenario è quello in cui lo "smartdevice" gestisce i dati carta o parte dei dati carta del cliente finale ed interagisce direttamente con l'Aquirer/Issuer attraverso i servizi offerti dalla parte server del sistema detta "MPOS" (che permette più collegamenti) e che mantiene esclusivamente traccia dei log delle transazioni oppure interagisce direttamente con l'acquirer o con un centro servizi appartenente a terzi. In questo scenario si prevedono quattro differenti configurazioni:
    - in una prima configurazione la transazione viene svolta utilizzando esclusivamente i dati che sono stampati sulla carta dell'utente (es. PAN, Expire Date e CVV2/CVC2) i quali vengono introdotti all'interno del dispositivo e memorizzati completamente ovvero parzialmente mediante operazioni di input eseguite dall'utente.
    - In una seconda configurazione la transazione viene svolta utilizzando esclusivamente i dati carta che sono memorizzati magneticamente/elettronicamente nella carta e che vengono introdotti all'interno del dispositivo e memorizzati completamente ovvero parzialmente mediante l'utilizzo di connessioni di prossimità (es. NFC) o connessioni radio/wireless remote in un centro servizi ovvero in modo autonomo da parte dell'utente.

- In una terza configurazione la transazione viene svolta utilizzando esclusivamente i dati carta che sono memorizzati magneticamente/elettronicamente nella carta e che vengono precaricati da un Operatore di Rete Mobile, eventualmente virtuale, in un area riservata all'interno della SIM Card.
- In una quarta configurazione il sistema intero prevede la creazione di conti carta ad hoc o preventivi, con IBAN, assimilabili alla generazione di moneta elettronica, appoggiati presso il medesimo istituto di pagamento. Le carte fisiche o virtuali possono appartenere unicamente al circuito proprietario dell'istituto di pagamento oppure possedere doppia o tripla interfaccia che le renda parte di uno o più circuiti internazionali e domestici. Questi conti permettono l'immediatezza della transazione in una delle tre precedenti configurazioni o in qualsivoglia configurazione possibile in quanto addebito e accredito avvengono ad opera del medesimo istituto di pagamento e al di fuori di qualunque circuito esterno, assumendo una forma simile e assimilabile al giroconto. Questa configurazione permette di rimanere esterni rispetto al perimetro di certificazione quando la transazione avviene internamente al circuito proprietario dei conti carta.
  Una volta effettuata la transazione sul media prescelto, l'istituto di pagamento che crea i conti di addebito e accredito compensa in tempo reale o in batch e permette di esportare i

fondi su altri conti e supporti di proprietà dell'utente e del merchant, così come permette di importare fondi da conti esterni sui propri conti.

In ogni caso e nelle quattro configurazioni descritte, il sistema di pagamento permette Il sistema di pagamento sicuro, facile da usare ed a basso costo di cui al presente trovato, verrà ora descritto in forme applicative esplicative ma non limitative date con riferimento agli schemi allegati in cui :

1. La fig.1 mostra uno schema a blocchi dei componenti del sistema in caso di "smartdevice" transazionale.
2. La fig. 2 mostra uno schema a blocchi dei componenti del sistema in caso di "smartdevice" dispositivo.
3. La fig. 3 mostra lo schema flussi funzionali per un pagamento e-commerce.
4. La fig. 4 mostra lo schema flussi funzionali per un pagamento su negozio fisico.

In funzione dello scenario cambia la piattaforma che è soggetta alla normativa PCI-DSS e/o PCI-PTS. Nel caso di "smartdevice" transazionale (S2), la piattaforma che è soggetta alle normative citate è il dispositivo mobile, tuttavia nel caso del sistema di pagamento sicuro, facile da usare ed a basso costo ogni dispositivo gestisce i dati di una carta o di più carte intestate al medesimo soggetto, cardholder. In questo caso quindi i dati carta non sono centralizzati presso un singolo Single Point of Failure (SPF) ma distribuiti sulle piattaforme mobili di singoli utenti rendendo ogni utente parzialmente responsabile della corretta custodia e l'ambiente meno

interessante per potenziali attaccanti. Nel caso di "smartdevice" dispositivo (S1), invece, la piattaforma soggetta alla normativa PCI-DSS è il server centrale MPOS.

Al fine di garantire una comunicazione sicura tra la parte periferica e quella centrale del sistema di pagamento sicuro, facile da usare ed a basso costo al primo avvio dell'applicazione per "smartdevice" viene generata una coppia di chiavi (i.e. pubblica e privata) ed un certificato digitale per la presentazione della propria chiave pubblica alla controparte della comunicazione, la porzione centrale del sistema. La componente privata della coppia di credenziali generate sarà dotata di una sicurezza equivalente a 112 bit (i.e. TDES): l'accesso alla componente privata da parte dell'applicazione sarà possibile solo previa autenticazione dell'utente attraverso l'utilizzo di una passphrase sicura che consentirà l'accesso alla busta crittografica che custodisce la componente segreta delle credenziali utente. La presentazione delle credenziali pubbliche dell'applicazione alla porzione centrale del sistema avverrà mediante l'utilizzo di un canale di comunicazione confidenziale instaurato grazie all'utilizzo di un certificato digitale firmato da un'autorità di certificazione riconosciuta precaricato dall'utente all'interno della soluzione nativa per la gestione della lista di certificati validi prevista dalla specifica piattaforma tecnologica.

Attraverso queste credenziali verranno opportunamente protette le comunicazioni tra le parti periferiche e quella centrale del presente trovato.

Nel caso di "smartdevice" transazionale (S2) per le configurazione C1 e C2, nella fase di inizializzazione oltre alla generazione delle credenziali necessarie per la creazione di un canale di comunicazione sicuro verrà predisposta la fase di acquisizione dei dati carta differenziando sulla base della tipologia di dati utilizzati (i.e. dati leggibili sulla carta ovvero dati presenti in supporti di memorizzazione interni alla carta). Nel caso di configurazione C1, l'input dei dati carta da parte dell'utente si avvarrà di soluzioni tecnologiche in grado di rendere il processo di inserimento dei dati meno-soggetto ad intercettazione da parte di componenti applicative esterne e residenti sullo stesso dispositivo (es. tastierini numerici on screen costituiti da immagini non soggette a processi di riconoscimento automatizzato e randomizzati nella posizione delle varie cifre). Nel caso di configurazione C2, il processo di caricamento dei dati carta salvati all'interno della stessa su banda magnetica ovvero su microcircuito avverrà utilizzando soluzioni hardware e processi compliant alle specifiche PCI-DSS. I dati carta acquisiti verranno opportunamente protetti all'interno del dispositivo mediante l'utilizzo di una chiave segreta derivata dalla chiave privata dell'utente e da alcune informazioni del dispositivo rese disponibili all'applicazione mobile direttamente dal sistema operativo rispettando le linee guide suggerite dalle specifiche PCI-DSS.

Nella configurazione C3, invece, la fase di inizializzazione prevede la realizzazione di una chiamata di test per verificare che la SIM card inserita nel dispositivo disponga delle interfacce di comunicazione necessarie per l'accesso ai dati carta preventivamente memorizzati.

Una volta che i dati carta sono disponibili presso la componente centrale MPOS, sia nel caso di "smartdevice" dispositivo (S1) che nel caso di "smartdevice" transazionale (S2), sarà responsabilità dell'MPOS reperire i dati necessari per il completamento della transazione e per il suo confezionamento secondo lo standard ISO8583.

Qui di seguito vengono schematicamente descritti i flussi funzionali con riferimento a due impieghi tipici

- Flussi funzionali e-commerce (FIG.3)

  L'utente completa il carrello ed esegue la funzione "checkout"; tra le alternative di pagamento disponibili il cliente seleziona l'icona che identifica il sistema di cui al presente trovato. Il cliente in funzione del grado di integrazione del merchant al sistema:

  a) Accede ad una sezione del portale del sistema per l'inserimento del proprio identificativo nel sistema descritto nel presente trovato.
  b) Dall'interno del sito e-commerce del merchant inserisce il proprio identificativo nel sistema descritto nel presente trovato.

  Alla ricezione del codice identificativo dell'utente il sistema attraverso l'utilizzo di una forma di comunicazione asincrona (es. SMS notifica pus) invia al dispositivo dell'utente i dati della transazione (es. merchant code, ossia identificativo univoco del negoziante, Partita IVA, persona giuridica, ragione sociale, importo, breve descrizione,...) utili al cliente per identificare la corrispondenza con quanto presente nel carrello e sufficienti a permettergli di effettuare il pagamento

tramite l'applicazione di cui al presente trovato. L'utente dispone già sul proprio dispositivo dell'applicazione e di conseguenza il messaggio asincrono determina l'avvio della applicazione. In caso di conferma della transazione l'applicazione confeziona i dati transazionali in modo conforme alle due possibilità illustrate ("smartdevice" dispositivo o transazionale) e si pone in attesa di risposta. Il sistema riceve in maniera sicura i dati transazionali e in funzione dello scenario ("smartdevice" dispositivo o transazionale) provvede a comporre la transazione ed inoltrarle direttamente all'Acquirer/Issuer .

I sistemi dell'Acquirer/Issuer completano la transazione e restituiscono l'esito all'MPOS che provvede a recapitarlo in modo indipendente al cliente ed al merchant. Il cliente riceve l'esito direttamente sull'applicazione mobile attraverso una comunicazione autentica dall'MPOS; il merchant riceve l'esito sull'interfaccia che ha esposto verso l'MPOS attraverso una comunicazione autentica.

- 2. Flussi funzionali negozio fisico (Fig.4)

Il cliente seleziona un bene/servizio che il merchant è tenuto a consegnare/erogare. Il cliente decide di pagare attraverso il sistema di cui al presente trovato, avvia l'applicazione e chiede al merchant di acquisire il dati necessari all'avvio della transazione (i.e. merchant code, valore della transazione, ...) mediante l'ausilio di meccanismi di comunicazione automatici (es. comunicazioni a corto raggio) o parzialmente automatici (es. codici bidimensionali). Nel caso in cui non sia possibile avvalersi di soluzioni anche solo parzialmente

automatizzate il cliente provvede ad inserire il merchant code, eventualmente recuperandolo da una lista di merchant salvati, e le altre informazioni necessarie per la transazione. Il dispositivo interagendo con l'MPOS sulla base dello scenario ("smartdevice" transazionale o dispositivo) ed utilizzando un protocollo proprietario provvede ad attivare l'esecuzione della transazione. L'MPOS, a questo punto inoltra la transazione ai sistemi dell'Acquirer/Issuer i quali completano la transazione e restituiscono l'esito al sistema MPOS. L'MPOS provvede a recapitare l'esito della transazione in modo indipendente al cliente ed al merchant. Il cliente riceve l'esito direttamente sull'applicazione mobile attraverso una comunicazione autentica dall'MPOS; il merchant riceve l'esito su una interfaccia che dipende dal grado di affiliazione del merchant stesso nel sistema del presente trovato. Nel caso di merchant affiliato l'esito viene consegnato su una applicazione mobile su dispositivo mobile, ovvero su una interfaccia web ovvero su un dispositivo hardware dedicato (es. display, stampante). Nel caso di merchant non affiliato la prova di avvenuta transazione può viaggiare su uno dei canali di comunicazione che si ipotizzano essere disponibili all'interno di un generico esercizio:

- attraverso il telefono fisso con un IVR (Interactive Voice Repsonse) a cui il merchant può rivolgersi in tempo reale digitando un codice transazione o comunicando altri dati identificativi;

- attraverso il telefono mobile mediante l'invio di un SMS di conferma;
- attraverso Internet dove i merchant possono trovare nel backoffice un area senza autenticazione in cui inserendo alcuni parametri (Partita IVA e codice transazione) possono controllare lo stato della transazione gestita.

RIVENDICAZIONI

1- Sistema di pagamento sicuro ed a basso costo in cui le parti coinvolte sono:

A) Un apparecchio/sistema intelligente di tipo "smartdevice", con sistemi operativi ANDROID o APPLE o WINDOWS o SIMBIAN o qualunque sistema operativo sottostia al dispositivo in questione;

B) Un ponte comunicativo e o integrativo e una parte server MPOS in grado di ricevere la transazione dallo "smartdevice", gestirla in modo sicuro da e verso gli acquirer e/o verso gli issuer in caso di pagamento con carta di credito o debito;

C) Un ponte comunicativo e o integrativo e una parte server MPOS in grado di ricevere la transazione dallo "smartdevice" e gestirla come "giroconto" nel caso di spostamento di denaro tra conti correnti gestiti da un Istituto autorizzato operando con l'apertura di conti ad hoc preso se stesso per pagante e pagato anche in modalità immediata;

caratterizzato dal fatto che l'MPOS è in grado di gestire e conservare chiavi acquirer cifrate in modo sicuro su dispositivi HSM secondo standard PCI DSS; è in grado di gestire piattaforme DB relazionali, sulle quali memorizzare certificati o dati utente cifrati; deve essere in grado di gestire molteplici transazioni al secondo in modo cifrato e sicuro, su canali diversi e con protocolli diversi (tra cui l'ISO8583 e XML); è' in grado di memorizzare su log di sistema i dati relativi a tutte le transazioni gestite e al loro esito.

2. Il sistema di pagamento sicuro e a basso costo secondo la rivendicazione 1, **caratterizzato** dal fatto la componente "smartdevice", è certificabile PCI DSS o (se richiesto) PTS, per la conservazione dei dati sensibili della carta necessari per le transazioni di pagamento (anche attraverso l'utilizzo di SD card o SIM).

3. Sistema di pagamento sicuro e a basso costo secondo la rivendicazione 1, **caratterizzato** dal fatto che lo "smartdevice" funge da carta e POS nello stesso momento, ospita una applicazione in grado di reperire i dati carta, memorizzati in modo sicuro sullo "smartdevice", e reperire le chiavi acquirer attraverso l'MPOS.

4. Sistema di pagamento sicuro e a basso costo secondo la rivendicazione 1, **caratterizzato** dal fatto che lo "smartdevice" e l'MPOS, in modalità "giroconto", rispondono alle caratteristiche di utilizzabilità e sicurezza richieste dagli Istituti di Pagamento a cui fanno riferimento i conti.

5. Sistema di pagamento sicuro e a basso costo secondo la rivendicazione 1, **caratterizzato** dall' essere in grado di gestire conti extrabancari e che per la sua caratterizzazione ne permetta la vendita anche ad operatori non finanziari secondo legge.

6. Sistema di pagamento sicuro e a basso costo secondo la rivendicazione 1, **caratterizzato** dal consentire il pagamento con carta di credito nei negozi fisici, anche in assenza di dispositivo fisico EFTPOS o PINPAD e senza che il merchant abbia un contratto di lungo termine con un acquirer.

7. Sistema di pagamento sicuro e a basso costo secondo la rivendicazione 1, caratterizzato dal consentire il pagamento su siti WEB, semplicemente inserendo il numero telefonico associato allo "smartdevice".

ORDINE NAZIONALE DEI CONSULENTI IN PROPRIETA' INDUSTRIALE
Dr. Arch. Massimo Sneider
Iscrizione n. 274

CAMERA DI COMMERCIO ROMA

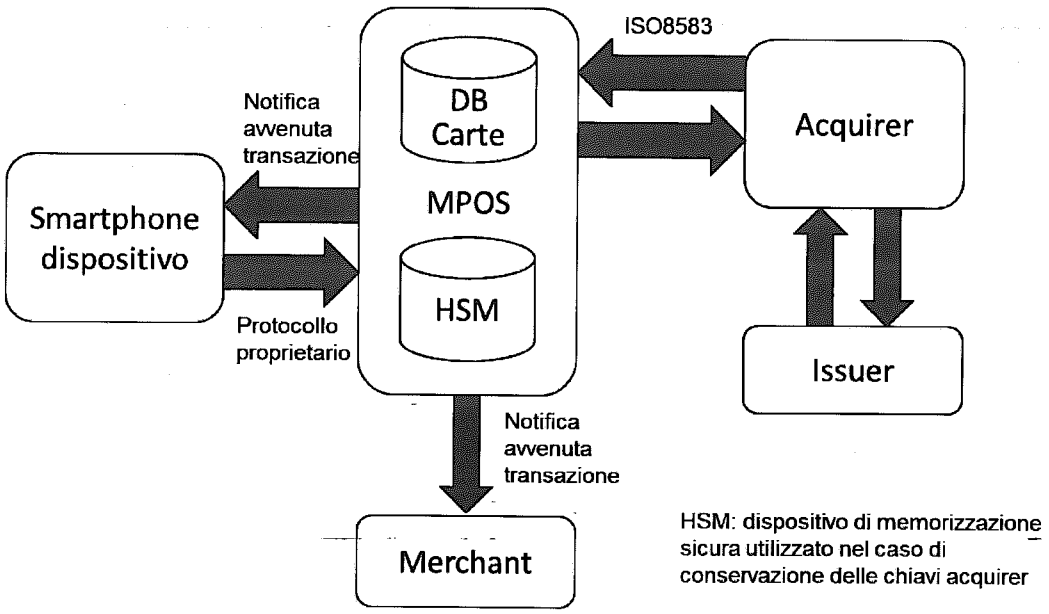

Figura 1: Scenario con "smartdevice" dispositivo (S1)

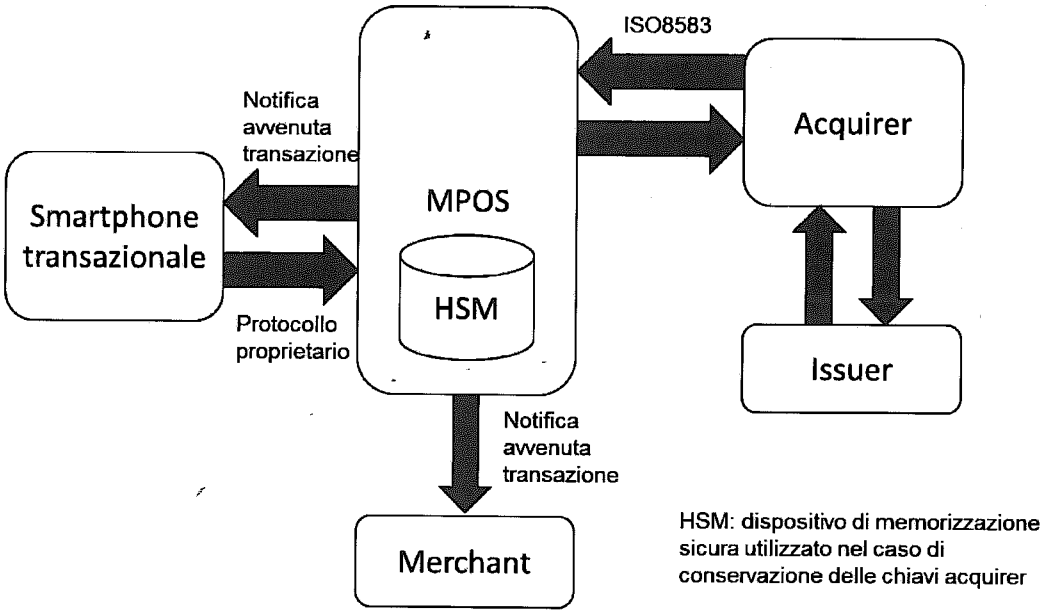

Figura 2: Scenario con "smartdevice" transazionale (S2)

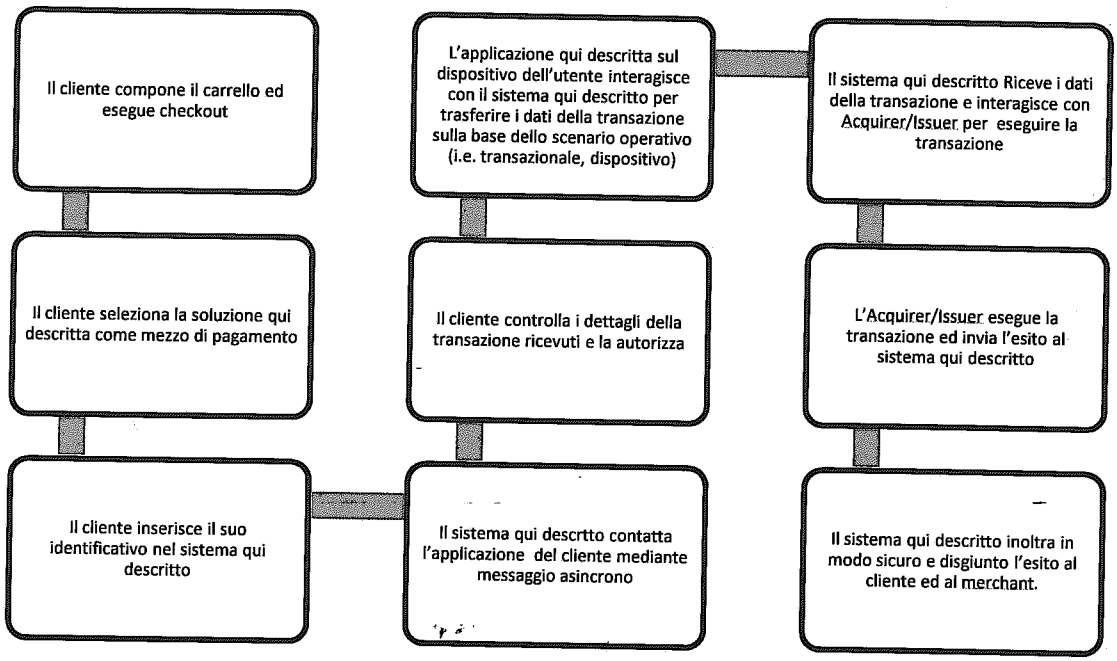

Figura 3: use case e-commerce

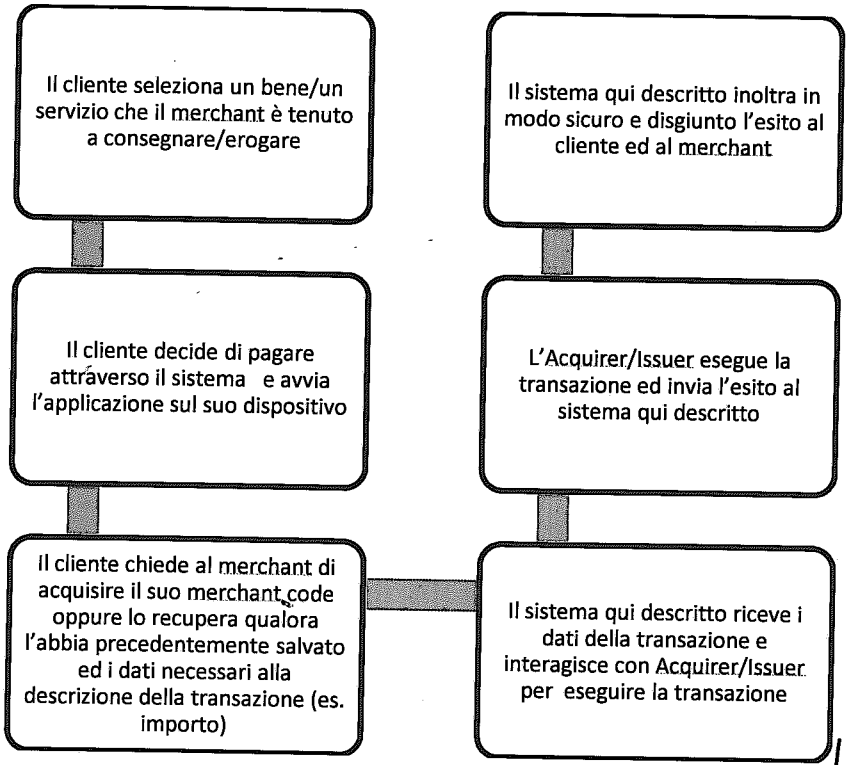

Figura 4: use case shop