

# ITALIAN PATENT OFFICE

Document No.

102011901976971A1

Publication Date

20130308

Applicant

FG S.R.L. AGENZIA FINANZIARIA

Title

DISPOSITIVO PORTATILE PER TRANSAZIONI FINANZIARIE

Descrizione della domanda di brevetto per Invenzione Industriale  
avente per titolo: Dispositivo portatile per transazioni finanziarie.

a nome: FG s.r.l. Agenzia Finanziaria

di nazionalità: italiana

domiciliata in: Viale dei Parioli 91

00197 Roma

Inventore: Giorgio FIORELLI

---000---

La presente invenzione riguarda un dispositivo portatile per transazioni finanziarie utilizzabile per pagamenti e/o prelievi sicuri come denaro contante in tempo reale e per altre forme di credito e/o operazioni bancarie in genere.

Nel settore tecnico delle transazioni economiche elettroniche si fanno costantemente grandi sforzi per lo sviluppo di sistemi del tipo chiamato portafoglio elettronico, in cui somme di denaro vengono tratte da un conto presso una banca convenzionata e vengono usate per pagare beni o servizi al posto di utilizzare denaro contante.

Sono altresì note transazioni economiche effettuate con mezzi del tipo "bancomat" che utilizzano la digitazione di codici personali, così come mezzi tipo "carta di credito" che necessitano di una conferma con firma del titolare ed eventualmente la presentazione di un documento di riconoscimento. Tuttavia, tali mezzi noti possono in qualche modo essere fraudolentemente riprodotti o utilizzati da altri utilizzatori, diversi dal titolare, in caso di

smarrimento o furto del mezzo stesso.

Sono anche noti sistemi di pagamento che utilizzano carte prepagate, con lo svantaggio che richiedono un aggiornamento della somma disponibile ogni volta che vengono esaurite e che consentono pagamenti limitati dal tipo stesso della carta.

Da WO 01/35334 e US 5.623.552 sono note carte di credito che prevedono la lettura di impronte digitali per l'identificazione del titolare e l'autorizzazione al trasferimento finanziario.

Da US 2007/0220273 è nota una card per transazioni che utilizza dati di riconoscimento biometrici come input e un sistema wireless per comunicare un codice di accesso in prossimità di un lettore o di un sistema di transazione.

Da WO 2011/065807 sono note soluzioni per transazioni economiche in tempo reale ad alta sicurezza che utilizzano telefoni mobili.

Tuttavia, anche se vengono continuamente effettuati miglioramenti per incrementare la sicurezza e praticità dei sistemi noti, nessuno di questi sistemi permette di avere la certezza del fatto che l'utilizzatore sia effettivamente il legittimo proprietario dello strumento di credito, inoltre, nessuno di questi sistemi noti consente di avere un solo strumento o un solo dispositivo eventualmente elettronici che facciano allo stesso tempo le funzioni di carta di credito, di bancomat e di denaro contante.

Inoltre, tutti i sistemi noti che utilizzano mezzi del tipo badge, quali le carte di credito o i bancomat, sono legati a

dimensioni stabilite dalle norme ISO 7810, per cui devono presentare uno spessore massimo ben determinato che obbliga alla scelta, ad esempio per i tipi con riconoscimento delle impronte digitali, di sensori sottili di tipo monodimensionale, meno affidabili di altri tipi di sensori che hanno spessori maggiori e che non sono utilizzabili in tali carte. Infatti, come detto, per rispettare lo standard stabilito dalle norme ISO i mezzi a badge devono avere uno spessore limitato per potersi piegare, o torcersi lungo tutti gli assi senza danneggiarsi.

Tali sistemi noti hanno quindi lo svantaggio di prevedere tre strumenti distinti per le funzioni di uso normale nelle transazioni economiche, vale a dire carte di credito, bancomat e carta moneta.

Peraltro, tali strumenti noti hanno limitazioni di spessore e sono soggetti a danneggiamento, ad esempio in tasca o nel portafoglio, a causa del loro spessore limitato.

Inoltre, il tipo di sensore di riconoscimento di tali strumenti noti deve avere dimensioni di spessore ridotte per poter essere usato con i mezzi di tipo badge, per cui deve essere preferibilmente di tipo monodimensionale, tipicamente in forma di filo singolo, meno affidabile e con difficile capacità lettura. Nel suddetto caso non possono essere utilizzati altri tipi di sensori che prevedano spessori maggiori.

Infine, i mezzi noti non assicurano una corrispondenza biunivoca ed irriproducibile tra il legittimo proprietario dello strumento di credito e l'utilizzatore dello stesso durante una

transazione finanziaria di tipo economico, poiché sia i codici dei bancomat, sia le firme delle carte di credito, sia gli accessi di tipo wireless, ad esempio quelli descritti nella pubblicazione US 2007/022073 possono essere fraudolentemente intercettati, riprodotti e utilizzati da altri non autorizzati.

Un ulteriore svantaggio dei dispositivi noti è l'impossibilità di trasferire somme di denaro da una carta di credito o bancomat tra di loro.

Scopo della presente invenzione è quindi quello di realizzare un dispositivo portatile atto a consentire una transazione economica sicura e in tempo reale, in modo da sostituire le carte di credito, il bancomat e il denaro contante con un unico strumento, il quale dispositivo portatile è in grado di effettuare il rilevamento di dati biometrici, quali ad esempio le impronte digitali, di memorizzare tali dati per successivi utilizzi e di autenticare in modo certo la validità di ogni successiva richiesta di transazione da parte dell'utente, confermando che chi effettua la transazione è il legittimo proprietario dello strumento di credito autorizzato allo scopo, i cui dati biometrici sono quelli memorizzati, senza dover digitare codici, né riprodurre firme, né trasmettere dati a distanza, consentendo un accesso direttamente in banca senza l'uso di codici o PIN.

Altro scopo della presente invenzione è quello di effettuare la comunicazione wireless tra dispositivo e lettore abbinato al terminale POS esclusivamente in uno spazio ristretto e protetto in

modo che le onde elettromagnetiche, ottiche o simili non fuoriescano da detto spazio e si diffondano nell'ambiente.

Un ulteriore scopo della presente invenzione è quello di fornire un dispositivo portatile che non preveda costi aggiuntivi di gestione in caso di uso come denaro contante.

Un ulteriore scopo della presente invenzione è quello di fornire un dispositivo portatile che, in caso di smarrimento o furto non sia utilizzabile da terzi poiché viene meno il riconoscimento dei dati biometrici quali una o più impronte digitali.

Un ulteriore scopo della presente invenzione è quello di fornire un dispositivo portatile che consenta di effettuare il trasferimento di somme di denaro tra dispositivi portatili stessi.

Ancora uno scopo della presente invenzione è quello di prevedere una maggiore comodità, praticità di uso e robustezza rispetto ai sistemi noti, comprese anche le carte di credito che prevedono un riconoscimento attraverso le impronte digitali. Infatti, secondo la presente invenzione, non vi sono limitazioni di spessore, come nei badge tradizionali, di conseguenza non vi sono pericoli di danneggiamento per piegatura o altro, permettendo di utilizzare sensori più sensibili ed affidabili.

Altro ulteriore scopo della presente invenzione è quello di realizzare un dispositivo che sia direttamente collegato al conto bancario e che possa essere utilizzato per la sua praticità e immediatezza anche per gestire costi irrisori, come ad esempio il pagamento di un caffè, di un biglietto dell'autobus o di un giornale,

senza costi aggiuntivi, gestendo inoltre il contante in modo diverso, poiché potendo prelevare cifre esatte, si conferisce al dispositivo un potere di acquisto fino all'ultimo centesimo senza avere rimanenze in tasca di spiccioli, che spesso vengono non più considerati, persi o ignorati come contante.

Secondo la presente invenzione, viene fornito un dispositivo portatile che comprende sostanzialmente un lettore di dati biometrici, preferibilmente un qualsiasi tipo di sensore di dati ed in particolare ad esempio un sensore di impronte digitali di tipo bidimensionale capacitivo, resistivo, ottico o simili; un alimentatore atto a fornire energia elettrica al dispositivo portatile, chiaramente cooperante con un relativo sistema di ricarica; circuiti di lettura e memorizzazione dei dati biometrici, preferibilmente ad esempio delle impronte digitali, nonché del loro successivo riconoscimento e validazione, allo scopo di abbinare in modo certo il dispositivo portatile secondo l'invenzione al legittimo proprietario e consentire susseguenti identificazioni, riconoscimenti e validazioni degli stessi dati biometrici del proprietario.

Il dispositivo portatile della presente invenzione viene inoltre previsto in grado di comunicare wireless con un lettore abbinato ad un terminale POS (Point Of Sale) di un punto di vendita. Tale comunicazione wireless avviene esclusivamente in uno spazio o ricettacolo estremamente ristretto e protetto in modo che le radiazioni elettromagnetiche, ottiche o simili della comunicazione tra il dispositivo portatile e il lettore abbinato al

terminale POS non fuoriescano dal ricettacolo e non si diffondano nell'ambiente, evitandone così la loro eventuale intercettazione e riproduzione.

Queste ed altre caratteristiche della presente invenzione risulteranno evidenti dalla descrizione dettagliata che segue di un esempio non limitativo di una forma di realizzazione preferita del dispositivo portatile dell'invenzione con riferimento alle figure dei disegni allegati, in cui:

la Figura 1 mostra lo schema a blocchi del dispositivo portatile secondo l'invenzione;

la Figura 2 mostra lo schema a blocchi del lettore abbinato al terminale POS e previsto in comunicazione con il dispositivo portatile dell'invenzione;

la Figura 3 mostra, secondo l'invenzione, in modo schematico uno di fronte all'altro un dispositivo portatile e un corrispondente lettore;

La Figura 4 mostra in particolare lo schema a blocchi del programma per il funzionamento del microprocessore MCU; e

la Figura 5 mostra il diagramma di flusso di una transazione esemplificativa che impiega, secondo l'invenzione, il dispositivo portatile in associazione con il relativo lettore abbinato al POS.

Con riferimento alle Figure 1 e 2 viene rappresentato lo schema a blocchi di una forma di realizzazione preferita di un dispositivo portatile 100 dell'invenzione e di un relativo lettore 110



in comunicazione con questo.

In particolare, il dispositivo portatile 100 comprende una unità a microprocessore MCU 1 (Micro Controller Unit) a cui sono connessi un lettore biometrico 2 di qualunque tipo noto, un modulo di comunicazione 3, eventualmente un display 4 con relativi circuiti di gestione 5. Sono inoltre connessi al microprocessore MCU 1 una batteria di alimentazione 6 tramite un gestore di ricarica 7 che comanda un mezzo di ricarica 8 di qualsiasi tipo adatto, ad esempio preferibilmente di tipo induttivo.

Sempre al microprocessore MCU 1 stesso può essere connessa una eventuale memoria aggiuntiva 9 ed un eventuale sistema antimanomissione 10.

Il lettore 110 rappresentato in Figura 2 comprende sostanzialmente un modulo di comunicazione 11 atto a comunicare da e verso il modulo di comunicazione 3 del dispositivo portatile 100, una interfaccia 12 preferibilmente di tipo USB, e di tipo tale da non mandare onde all'esterno, abbinata ad un terminale POS. Fa inoltre parte essenziale del lettore 110 un dispositivo di ricarica 13 di qualsiasi tipo adatto, ad esempio di tipo induttivo, connesso tramite un modulo di alimentazione 14 alla rete elettrica.

Più in particolare, il dispositivo 100 è contenuto in un involucro avente una forma comoda per essere usato in modo semplice ed ergonomico con una mano, indifferentemente destra o sinistra, con dimensioni approssimative ad esempio dell'ordine di quelle di un accendino o di una chiave elettronica da autovettura.

Entro tale involucro sono previsti gli elementi visualizzati nello schema a blocchi di Figura 1, ed in particolare l'unità a microprocessore MCU 1 che governa l'intero dispositivo portatile 100 ed è attivata dal posizionamento sulla superficie del lettore biometrico 2 di almeno un dito prescelto del legittimo utilizzatore il quale, esercitando o meno una leggera pressione sulla detta superficie chiude un qualsiasi mezzo di attivazione che fornisca l'alimentazione all'intero dispositivo 100. I mezzi di attivazione possono essere ad esempio costituiti da un microinterruttore posizionato al disotto del detto sensore biometrico 2, ovvero da un sensore capacitivo, resistivo, o di prossimità il quale viene previsto in qualunque posizione conveniente del dispositivo.

La avvenuta accensione del dispositivo viene confermata visualizzando un opportuno messaggio su un display, oppure tramite l'accensione di uno o più micro led.

Più in particolare, il lettore biometrico 2 può essere un lettore qualsiasi di impronte digitali, preferibilmente un sensore di tipo bidimensionale capacitivo, resistivo ottico o simili.

Il sensore biometrico 2 legge l'impronta che si trova sulla sua superficie e ne informa l'unità MCU 1, la quale ne fa in prima istanza una valutazione qualitativa. Una volta approvata la qualità, l'unità MCU 1, attraverso il modulo di comunicazione-dispositivo 3 connesso con un modulo di comunicazione-lettore 11 di Figura 2, riceve l'informazione di:

- iniziare le operazioni di registrazione di una o più impronte nella memoria dell'unità MCU 1 e/o nella memoria aggiuntiva 9 del dispositivo e, una volta completata tutta l'operazione di registrazione, impedire che vengano aggiunti e/o variati i dati registrati, se tale lettore si trova presso la banca, oppure
- verificare che l'impronta stessa appartenga al legittimo utilizzatore e che quindi sia già registrata nella memoria dell'unità MCU e/o nella memoria aggiuntiva 9, se tale lettore si trova collegato a un punto vendita POS.

Sempre nell'involucro del dispositivo viene previsto un gestore di ricarica 7. Con tale definizione si intende preferibilmente un qualunque mezzo atto a controllare periodicamente lo stato di carica della batteria 6 del dispositivo portatile 100 e, se del caso, a richiederne una sollecita ricarica.

Le operazioni fino a qui descritte sono attuabili se il gestore di ricarica 7 dà il proprio consenso, avendo verificato che il livello di tensione presente nella batteria 6 è sufficiente ad alimentare le necessarie componenti di Figura 1 per il positivo completamento dell'operazione richiesta. In caso contrario, il gestore di ricarica 7 segnala la necessità di ricarica e/o richiede l'attivazione di un mezzo di ricarica 8 ad esempio preferibilmente di tipo induttivo.

La sicurezza dell'integrità e della veridicità delle informazioni biometriche contenute nella memoria dell'unità MCU 1 e/o nell'eventuale memoria aggiuntiva 9 (informazioni che nella forma di esecuzione esemplificativa della presente invenzione sono

costituite ad esempio da una o più impronte digitali, fino a dieci impronte) viene garantita da uno o più sistemi antimanomissione 10 che, in caso di tentata apertura forzata del dispositivo portatile 100 lo rendono istantaneamente illeggibile ed inutilizzabile.

Un esempio non limitativo di sistema antimanomissione 10 potrà prevedere mezzi tali da inviare tutta la tensione residua della batteria 6 sui piedini del circuito di memoria dell'unità MCU 1 e della memoria aggiuntiva 9 causandone la distruzione immediata.

Chiaramente, può essere prevista una batteria, ad esempio di tipo al litio, dedicata al solo sistema antimanomissione 10, che non viene mai utilizzata per altri scopi.

In alternativa possono essere previsti mezzi meccanici a frattura preordinata o mezzi chimici, quali ad esempio fiale contenenti una sostanza corrosiva adatta.

Il dispositivo portatile della presente invenzione può inoltre prevedere che una o più delle impronte registrate venga utilizzata dal sistema per lanciare un allarme silenzioso che il circuito interessato utilizzerà nel modo opportuno, segnalando un funzionamento forzato o anomalo del dispositivo.

Nelle Figure 1, 2 ed in particolare nella Figura 3, viene mostrata una forma di realizzazione esemplificativa preferita dell'assieme del dispositivo portatile 100 e del corrispondente lettore 110 al quale è previsto essere connesso. Il contatto fisico reciproco tra il dispositivo (100) e il lettore (110) è mantenuto da

almeno un mezzo magnetico (37, 39) associato all'uno o all'altro del dispositivo 100 o del lettore 110 e agente su un elemento di accoppiamento complementare (39, 37) disposto sul lettore 110 o sul dispositivo portatile 100.

Ancora più in particolare, nella forma di realizzazione rappresentata, il dispositivo portatile 100 prevede una estremità anteriore 36 dotata di almeno un mezzo magnetico 37 preferibilmente costituito da almeno una coppia di magneti 37, mentre il lettore 110 prevede un ricettacolo 38 che prevede al suo interno almeno un elemento di accoppiamento complementare magnetico 39, preferibilmente costituito da almeno una coppia di magneti 39. Quando viene inserita l'estremità anteriore 36 del dispositivo portatile 100 nel ricettacolo 38 del lettore 110, i magneti 37 e 39 rispettivamente previsti come detto sull'estremità 36 del dispositivo portatile 100 e all'interno del ricettacolo 38 del lettore 110 in posizioni corrispondenti, provvedono a trattenere saldamente in contatto il dispositivo portatile 100 con il lettore 110 in modo che i rispettivi moduli di comunicazione-dispositivo 3 e di comunicazione-lettore 11 si mantengano in stretto contatto fisico e possano scambiarsi i dati senza far uscire onde di qualsiasi tipo all'esterno.

La forma simmetrica del dispositivo 100 potrebbe dar luogo ad un posizionamento scorretto del dispositivo stesso all'interno del lettore 110, ad esempio, nel caso ci si riferisca ad una eventuale unità ottica di comunicazione ricezione-trasmissione (RX TX) tra i

due elementi dispositivo e lettore. Infatti, al fine di soddisfare la necessità di mantenere in un ambito spaziale estremamente limitato lo scambio di informazioni, l’RX lato dispositivo 110 deve essere posto in contatto fisico con il TX lato dispositivo 100, e viceversa. Tale risultato si ottiene prevedendo in opportuna posizione all’interno del ricettacolo 38 del lettore 110 due magneti 39, le cui polarità si affacciano per entrare in contatto con due analoghi magneti 37 disposti sulla superficie della estremità anteriore 36 del dispositivo 100. Le polarità dei magneti faranno in modo che ad un corretto posizionamento del dispositivo 100 all’interno del lettore 110 corrisponda un bloccaggio sicuro tra i due elementi, mentre ad uno scorretto posizionamento del dispositivo 100 all’interno del lettore 110 corrisponda una espulsione del dispositivo dal lettore dovuta alla repulsione magnetica.

Chiaramente, se i mezzi magnetici 39 del lettore 110 sono costituiti da elettromagneti, la forza di questi potrà essere regolata in modo tale da essere massima durante l’uso e quasi nulla al termine delle operazioni, per una agevole estrazione del dispositivo dal ricettacolo 38.

Preferibilmente, come mostrato in Figura 3, per comodità di uso la disposizione delle parti che costituiscono il dispositivo 100 ed il corrispondente lettore 110 è tale da consentire l’inserimento orizzontale del dispositivo 100 nel lettore 110.

Può essere anche prevista una diversa disposizione delle parti (non mostrata) secondo la quale i due elementi dispositivo 100 e lettore 110 sono disposti verticalmente, in questo caso, ad esempio, i mezzi magnetici 39 del lettore 110 agiscono su un elemento di accoppiamento complementare 37 in materiale ferromagnetico disposto sul dispositivo portatile 100, o viceversa, in modo da mantenere la possibilità di uso indifferentemente con la mano destra e la mano sinistra.

La corretta introduzione nel ricettacolo e il corretto riconoscimento dell'impronta vengono preferibilmente segnalate da una opportuna accensione di almeno un led previsto allo scopo, come verrà meglio spiegato qui di seguito.

Sul dispositivo portatile 100 sono previsti ad esempio led 44, 45, 46, e 47 aventi specifiche funzioni e significati:

- il led 44 indica il corretto inserimento e posizionamento del dispositivo 100 nel lettore 110 e l'avvenuto bloccaggio dei magneti 37, 39;
- il led 45 indica che l'impronta è stata memorizzata correttamente;
- il led 46 indica che l'impronta è stata riconosciuta valida, appartenente quindi al legittimo utente;
- il led 47 indica che si è verificata una condizione di errore: l'impronta non è registrabile o non è stata riconosciuta come appartenente al corretto utente.

Il lettore 110, attraverso l'interfaccia 12, preferibilmente di tipo USB e tale da non mandare onde all'esterno, relativo cavo elettrico 40 e connettore 41, riceve dal terminale POS o dal calcolatore di arruolamento della banca istruzioni opportune relativamente a ciò che il dispositivo 100 deve fare:

- predisporre il pagamento di quanto richiesto dal punto vendita
- valutare l'impronta disposta sul lettore biometrico 2 e
- registrarla nelle memorie dell'unità MCU 1 ed aggiuntiva 9 dello stesso dispositivo 100.

In questa fase delle operazioni il lettore 110 e il dispositivo 100 mantengono in stretto contatto anche gli induttori di ricarica rispettivamente 13 e 8, in modo che per il loro tramite possa essere fornita una corretta alimentazione al dispositivo 100, nel caso in cui eventualmente la ricarica del dispositivo 100 sia non sufficiente per effettuare le operazioni richieste.

Nella Figura 4, viene rappresentato in particolare il programma di funzionamento del microprocessore MCU 1 che comprende un motore per la gestione delle operazioni 30, che sviluppa le funzioni logiche per la gestione del lettore biometrico 31. Il motore per la gestione delle operazioni 30 sviluppa anche le funzioni logiche di I/O per la gestione della batteria 32. Sempre il motore per la gestione delle operazioni 30 gestisce il protocollo di comunicazione 33 verso il lettore 110, preferibilmente attraverso una routine di criptaggio 34.



Il motore per la gestione delle operazioni 30 si occupa infine dell'I/O dell'eventuale sistema antimanomissione 35.

Più in particolare, in Figura 4 vengono rappresentate le funzioni che si svolgono all'interno dell'unità MCU 1 sotto il suo diretto controllo.

In particolare, il motore per la gestione delle operazioni 30 controlla ciclicamente i canali di comunicazione da e verso:

- la routine di criptaggio 34 del protocollo di comunicazione 33,
- controlla eventuali notifiche da parte del sistema antimanomissione 35,
- la routine di gestione 31 del lettore biometrico 2
- controlla i segnali di I/O del gestore della batteria 32.

Considerando la sequenza temporale delle operazioni, queste si svolgono nel seguente modo.

- attivazione del dispositivo generata dall'introduzione dello stesso all'interno del lettore,
- comunicazione da parte del lettore al motore di gestione delle operazioni 30, tramite il protocollo di comunicazione 33 e la routine di criptaggio 34, delle operazioni che dovranno essere svolte,
- lettura dell'impronta o delle impronte tramite la routine di gestione 31 del lettore biometrico 2:
  - memorizzazione dell'impronta o delle impronte (se si è in banca per l'attribuzione all'utente del dispositivo)

- riconoscimento dell'impronta o delle impronte per dare il consenso allo svolgimento di una operazione finanziaria
- nelle more dei tempi di I/O di uno qualunque dei canali connessi al motore di gestione delle operazioni 30, il motore di gestione stesso interroga la routine di gestione della batteria 32 e/o la routine di gestione del sistema antimanomissione 35.

Nella Figura 5, viene rappresentato il diagramma di flusso di una transazione finanziaria esemplificativa standard che comprende le fasi di:

- 50 immissione dell'importo sul POS
- 51 ricezione richiesta dal POS
- 52 richiesta convalida impronta
- 53 funzione di verifica da parte della gestione del lettore biometrico 31 che l'impronta appartenga al legittimo portatore del dispositivo portatile 100
- 54 termine dell'operazione se l'impronta non viene convalidata dalla funzione di verifica 53
- 55 invio della conferma al POS se l'impronta viene convalidata
- 56 richiesta dal POS alla banca del pagamento
- 57 risposta della banca al POS
- 58 verifica della disponibilità finanziaria
- 59 in caso affermativo invio OK al dispositivo portatile 100
- 60 registrazione dell'operazione
- 61 in caso negativo invio diniego al dispositivo portatile 100

- 62 termine operazione.

Più in particolare, la situazione rappresentata nel diagramma di flusso di Figura 5, può riferirsi ad una operazione di acquisto di beni o servizi da effettuarsi presso un esercizio commerciale convenzionato tramite una banca che ha adottato il sistema di utilizzo del dispositivo portatile 100.

Pertanto, l'operazione (blocco 50) di immissione dell'importo da corrispondere al terminale POS si verifica come conclusione dell'operazione di vendita. A questo punto, il terminale POS richiede all'acquirente l'introduzione del dispositivo portatile 100 nella propria unità di lettura 110. Susseguentemente, la richiesta (blocco 51) del pagamento da parte del terminale POS viene ricevuta dall'unità MCU 1 la quale richiede a sua volta (blocco 52), ad esempio tramite l'accensione di un led di segnalazione, che il portatore del dispositivo 100 ponga una delle sue impronte, preventivamente registrate in banca, sul lettore biometrico 2 al fine di consentirne la verifica.

Il risultato dell'operazione di verifica ha due possibilità (blocco 53)

- la verifica non ha avuto esito positivo, il che conduce al termine dell'operazione (blocco 54)
- la verifica ha avuto esito positivo, il che conduce al blocco 55 di invio della conferma dell'identità del portatore come valida.

Tutto ciò consente al terminale POS di inviare alla banca la richiesta di disponibilità della somma relativa alla operazione di

vendita in corso (blocco 56). Il blocco 57 indica, unitamente al blocco 58, la risposta di disponibilità finanziaria che la banca fornisce al terminale POS e che può essere:

- negativa (blocco 61), che conduce direttamente al termine e dell'operazione (blocco 62), o
- positiva (blocco 59), che conduce alla regolare operazione di registrazione contabile e alla chiusura con successo dell'operazione di vendita (blocco 60).

In quanto sopra riportato, è stata descritta una forma di realizzazione preferita dell'invenzione senza peraltro limitarla in alcun modo alle caratteristiche descritte. Gli esperti del ramo comprenderanno che, alla luce di quanto qui reso noto, possono essere apportate modifiche e numerosi cambiamenti senza uscire dall'ambito della presente invenzione come definita dalle rivendicazioni allegate.

## RIVENDICAZIONI

1. Dispositivo portatile per transazioni finanziarie e/o operazioni bancarie in genere, caratterizzato dal fatto che comprende un lettore di dati biometrici (2) di un legittimo proprietario; dispositivi (1, 2, 9) di lettura, decodifica, memorizzazione e successivo riconoscimento dei dati biometrici, atti a definire un accoppiamento certo tra il dispositivo e il legittimo proprietario; mezzi (37) di accoppiamento con corrispondenti mezzi entro un ricettacolo (38) abbinato a un terminale POS; mezzi di alimentazione e di ricarica (6, 7, 8) atti a fornire energia elettrica al dispositivo portatile.

2. Dispositivo portatile secondo la rivendicazione 1 caratterizzato dal fatto che i dati biometrici sono costituiti da almeno una impronta digitale.

3. Dispositivo portatile secondo la rivendicazione 2, caratterizzato dal fatto che il lettore di dati biometrici (2) è un sensore di impronte digitali di tipo bidimensionale capacitivo, resistivo, ottico o simili.

4. Dispositivo portatile secondo la rivendicazione 1, caratterizzato dal fatto che comprende una unità a microprocessore MCU (1) (Micro Controller Unit) a cui sono connessi un lettore biometrico (2); un modulo di comunicazione (3); un display (4) con relativi circuiti di gestione (5); una batteria di alimentazione (6) e un gestore di ricarica (7), che comanda un mezzo di ricarica (8).

5. Dispositivo portatile secondo una qualsiasi delle rivendicazioni precedenti, caratterizzato dal fatto che al microprocessore MCU (1) è connessa una memoria aggiuntiva (9).

6 Dispositivo portatile secondo la rivendicazione 4 o 5, caratterizzato dal fatto che i dati biometrici (2) sono contenuti nella memoria dell'unità MCU (1) e/o nella memoria aggiuntiva (9).

7. Dispositivo portatile secondo una qualsiasi delle rivendicazioni precedenti, caratterizzato dal fatto che i mezzi di ricarica (8) compresi nel dispositivo portatile (100) sono di tipo induttivo.

8. Dispositivo portatile secondo una qualsiasi delle rivendicazioni precedenti, caratterizzato dal fatto che al microprocessore MCU (1) è connesso un sistema antimanomissione (10).

9 Dispositivo portatile secondo la rivendicazione 8 caratterizzato dal fatto che il sistema antimanomissione (10) comprende mezzi atti ad inviare tutta la tensione residua della batteria (6) sui piedini del circuito di memoria dell'unità MCU (1) e della memoria aggiuntiva (9) causandone la distruzione immediata.

10 Dispositivo portatile secondo la rivendicazione 8, caratterizzato dal fatto che il sistema antimanomissione comprende mezzi meccanici a frattura preordinata o mezzi chimici.

11. Dispositivo portatile secondo una qualsiasi delle rivendicazioni precedenti, caratterizzato dal fatto che comprende una batteria dedicata al solo sistema antimanomissione (10).

12 Dispositivo portatile secondo una qualsiasi delle rivendicazioni precedenti, caratterizzato dal fatto che l'unità a microprocessore MCU (1) del dispositivo portatile (100) è associata a mezzi di attivazione dell'alimentazione all'intero dispositivo (100), attivati dal posizionamento sulla superficie del lettore biometrico (2) di almeno un dito prescelto del legittimo utilizzatore.

13. Dispositivo portatile secondo la rivendicazione 12, caratterizzato dal fatto che detti mezzi di attivazione sono costituiti da un microinterruttore posizionato sotto il sensore biometrico (2), ovvero da un sensore capacitivo, resistivo, o di prossimità previsto in qualunque posizione conveniente del dispositivo.

14. Dispositivo portatile secondo una qualsiasi delle rivendicazioni precedenti, caratterizzato dal fatto che presenta mezzi di visualizzazione della avvenuta accensione del dispositivo, detti mezzi comprendendo un display (4, 5) di visualizzazione di un opportuno messaggio, oppure uno o più micro led (44, 45, 46, 47) accesi all'avvio.

15. Dispositivo portatile secondo una qualsiasi delle rivendicazioni precedenti, caratterizzato dal fatto che almeno un dato biometrico è previsto per l'invio di un segnale di allarme silenzioso.

16. Dispositivo portatile secondo una qualsiasi delle rivendicazioni precedenti, caratterizzato dal fatto che il gestore di ricarica (7) dà il proprio consenso se il livello di tensione presente nella batteria (6) è sufficiente ad alimentare le necessarie componenti del dispositivo, segnalando la necessità di ricarica e/o richiedendo

l'attivazione di un mezzo di ricarica (8) di tipo induttivo, in caso contrario.

17. Dispositivo portatile secondo una qualsiasi delle rivendicazioni precedenti, caratterizzato dal fatto che i mezzi di accoppiamento comprendono almeno un magnete (37).

18. Assieme di un dispositivo portatile (100) per transazioni finanziarie e di un lettore (110) collegato ad una interfaccia (12) abbinata ad un terminale POS, caratterizzato dal fatto che il dispositivo portatile è attuato secondo la rivendicazione 1 e il lettore (110) abbinato ad un terminale POS comprende un ricettacolo (38) di accoppiamento con il dispositivo portatile (100) e un modulo di comunicazione (11) atto a comunicare da e verso il modulo di comunicazione (3) del dispositivo portatile (100).

19. Assieme di dispositivo portatile (100) e lettore (110) secondo la rivendicazione 18, caratterizzato dal fatto che detto ricettacolo (38) presenta un volume ridotto e protetto atto a limitare la dissipazione verso l'esterno delle onde di comunicazione tra il dispositivo portatile (100) e il lettore (110) e che detta interfaccia (12) è di tipo USB e di tipo tale da non mandare onde all'esterno.

20. Assieme secondo la rivendicazione 19 caratterizzato dal fatto che il contatto fisico reciproco tra il dispositivo (100) e il lettore (110) è mantenuto da almeno un mezzo magnetico (37, 39) associato all'uno o all'altro del dispositivo (100) o del lettore (110) e agente su un elemento di accoppiamento complementare (39, 37) disposto sul lettore (110) o sul dispositivo portatile (100).



21. Assieme secondo una qualsiasi delle rivendicazioni 18-20, caratterizzato dal fatto che l'almeno un mezzo magnetico (39) comprende un elettromagnete, detto elemento di accoppiamento complementare (37) essendo un magnete.

22. Assieme secondo una qualsiasi delle rivendicazioni 18-20, caratterizzato dal fatto che l'almeno un mezzo magnetico (37, 39) comprende un magnete o un materiale ferromagnetico con corrispondente elemento di accoppiamento complementare.

23. Assieme secondo una qualsiasi delle rivendicazioni 18-22, caratterizzato dal fatto che il lettore (110) comprende un dispositivo di ricarica (13) collegabile alla rete elettrica tramite un modulo di alimentazione (14).

24. Assieme secondo una qualsiasi delle rivendicazioni 18-23 caratterizzato dal fatto che i mezzi di ricarica (8, 13) previsti nel dispositivo portatile (100) e nel lettore (110) sono di tipo induttivo.

25. Assieme secondo una qualsiasi delle rivendicazioni 18 a 24, caratterizzato dal fatto che comprende uno o più led (44, 45, 46, 47) la cui accensione segnala l'attivazione del dispositivo (100), la corretta introduzione del dispositivo nel ricettacolo (38) del lettore (110), la validità e/o il riconoscimento dell'informazione biometrica oppure una condizione di errore.

26. Procedimento per l'effettuazione di una transazione finanziaria standard in tempo reale caratterizzato dal fatto che comprende l'accoppiamento di un dispositivo portatile secondo la rivendicazione 1 con un lettore (110) abbinato ad un terminale

POS di un punto di vendita secondo la rivendicazione 16, con cui il dispositivo portatile (100) è in grado di comunicare senza fili in tempo reale, tale comunicazione avvenendo tra il modulo di comunicazione-dispositivo 3 e il modulo-comunicazione lettore 11 in uno spazio o ricettacolo (38) estremamente ristretto e protetto.

27. Procedimento secondo la rivendicazione 26, caratterizzato dal fatto che comprende le fasi di:

- 50 immissione dell'importo sul POS
- 51 ricezione richiesta dal POS
- 52 richiesta di convalida dell' almeno una impronta
- 53 funzione di verifica da parte della gestione del lettore biometrico (31) che l'impronta appartenga al legittimo portatore del dispositivo portatile (100)
- 54 termine dell'operazione se l'impronta non viene convalidata dalla funzione di verifica 53
- 55 invio della conferma al POS se l'impronta viene convalidata
- 56 richiesta dal POS alla banca del pagamento
- 57 risposta della banca al POS
- 58 verifica della disponibilità finanziaria
- 59 in caso affermativo invio OK al dispositivo portatile 100
- 60 registrazione dell'operazione
- 61 in caso negativo invio diniego al dispositivo portatile 100
- 62 termine operazione.

CLAIMS

1. A portable device for financial transactions and/or banking operations in general, characterized in that it comprises a reader (2) of the biometric data belonging to the legitimate owner; devices (1, 2, 9) for reading, decoding, storing and subsequent identification of the biometric data, able to establish a safe link between the device and the legitimate owner; means (37) for engaging with corresponding means inside a receiving seat (38) combined with a POS terminal; power supply and recharging means (6, 7, 8) able to supply electric power to the portable device.
2. The portable device according to Claim 1, characterized in that the biometric data consist of at least one finger print.
3. The portable device according to Claim 2, characterized in that the biometric data reader (2) is a finger-print sensor of the two-dimensional, capacitive, resistive, optical or similar type.
4. The portable device according to Claim 1, characterized in that it comprises a microprocessor (Micro Controller Unit) MCU (1) to which the following are connected: a biometric reader (2); a communication module (3); a display with associated control circuits (5); a power supply battery (6); and a recharging controller (7) which controls recharging means (8).
5. The portable device according to any one of the preceding claims, characterized in that an additional memory (9) is connected to the microprocessor MCU (1).

6. The portable device according to Claim 4 or 5, characterized in that the biometric data (2) are contained in the memory of the unit MCU (1) and/or in the additional memory (9).

7. The portable device according to any one of the preceding claims, characterized in that the recharging means (8) comprised in the portable device (100) are of the inductive type.

8. The portable device according to any one of the preceding claims, characterized in that an anti-tamper system (10) is connected to the microprocessor MCU (1).

9. The portable device according to Claim 8, characterized in that the anti-tamper system (10) comprises means for sending all the residual voltage of the battery (6) to the pins of the memory circuit of the unit MCU (1) and the additional memory (9), causing the immediate destruction thereof.

10. The portable device according to Claim 8, characterized in that the anti-tamper system comprises mechanical predefined-breakage means or chemical means.

11. The portable device according to any one of the preceding claims, characterized in that it comprises a dedicated battery for the anti-tamper system (10) alone.

12. The portable device according to any one of the preceding claims, characterized in that the microprocessor MCU (1) of the portable device (100) is associated with means for activating the power supply to the entire device (100), activated by the positioning, on the surface of the biometric reader (2), of at least

one prechosen finger of the legitimate user.

13. The portable device according to Claim 12, characterized in that said activation means consist of a microswitch positioned underneath the biometric sensor (2), or a capacitive, resistive or proximity sensor, provided in any convenient position of the device.

14. The portable device according to any one of the preceding claims, characterized in that it has means for displaying switching on of the device, said means comprising a display (4, 5) showing a suitable message or one or more LEDs (44, 45, 46, 47) which are lit upon start-up.

15. The portable device according to any one of the preceding claims, characterized in that at least one item of biometric data is used for sending a silent alarm signal.

16. The portable device according to any one of the preceding claims, characterized in that the recharging controller (7) gives its consent if the voltage level present in the battery (6) is sufficient to power the necessary components of the device, indicating the need for recharging and/or requesting activation of a recharging means (8) of the inductive type, if this is not the case.

17. The portable device according to any one of the preceding claims, characterized in that the engaging means comprise at least one magnet (37).

18. An assembly consisting of a portable device (100) for financial transactions and a reader (110) connected to an interface

(12) combined with a POS terminal, characterized in that the portable device is realized according to Claim 1 and the reader (110) combined with a POS terminal comprises a receiving seat (38) for engagement with the portable device (100) and a communication module (11) suitable for communication to and from the communication module (3) of the portable device (100).

19. The assembly consisting of portable device (100) and reader (110) according to Claim 18, characterized in that said receiving seat (38) has a small and protected volume able to limit dissipation externally of the communication waves sent between the portable device (100) and the reader (110) and in that said interface (12) is of the USB type and is of the kind without transmission of waves externally.

20. The assembly according to Claim 19, characterized in the physical mutual contact between the device (100) and the reader (110) is maintained by at least one magnetic means (37, 39) associated with one or other of the device (100) or the reader (110) and acting on a complementary engaging element (39, 37) arranged on the reader (110) or on the portable device (100).

21. The assembly according to any one of Claims 18 to 20, characterized in that the at least one magnetic means (39) comprises an electromagnet, said complementary engaging element (37) being a magnet.

22. The assembly according to any one of Claims 18 to 20, characterized in that the at least one magnetic means (37)

comprises a magnet or a ferromagnetic material with corresponding complementary engaging element.

23. The assembly according to any one of Claims 18 to 22, characterized in that the reader (110) comprises a recharging device (13) which can be connected to the electrical network by means of a power supply module (14).

24. The assembly according to any one of Claims 18 to 23, characterized in the recharging means (8, 13) provided in the portable device (100) and in the reader (100) are of the inductive type.

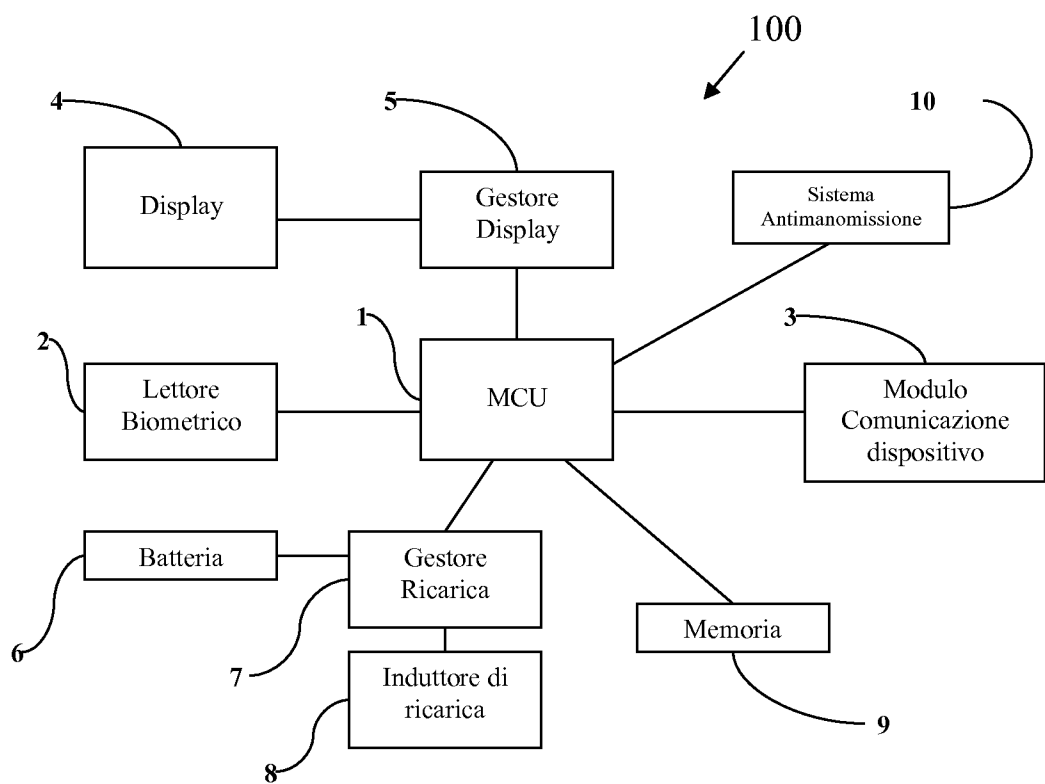
25. The assembly according to any one of Claims 18 to 24, characterized in that it comprises one or more LEDs (44, 45, 46, 47), lighting up of which signals activation of the device (100), the correct introduction of the device inside the receiving seat (38) of the reader (110), and the validity and/or identification of the biometric information or an error condition.

26. A method for performing a standard financial transaction in real time, characterized in that it comprises the engagement of a portable device (100) according to Claim 1 with a reader (110) combined with a POS terminal of a sales point according to Claim 16, with which the portable device (100) is able to communicate wirelessly in real time, this communication taking place between the device communication module (3) and the reader communication module (11) in an extremely restricted and protected space or receiving seat (38).

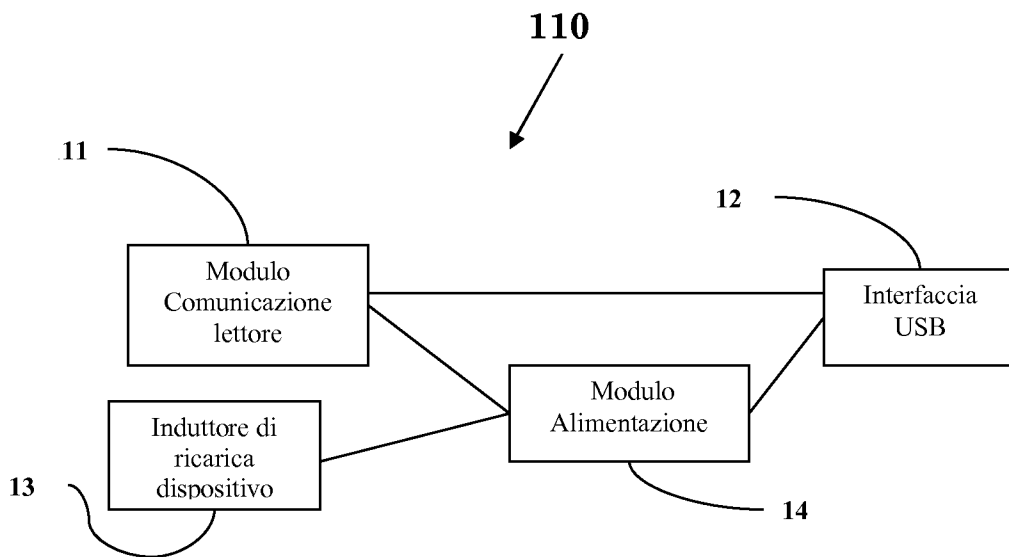
27. The method according to Claim 26, characterized in that it comprises the steps of:

- 50 introduction of the amount on the POS
- 51 reception of the request from the POS
- 52 request for convalidation of the at least one finger print
- 53 verification by the biometric reader control unit (31) that the finger-print belongs to the legitimate owner of the portable device (100)
- 54 termination of the operation if the finger-print is not convalidated by the verification function 53
- 55 sending of confirmation to the POS if the finger-print is convalidated
- 56 request from the POS to the bank for payment
- 57 response of the bank to the POS
- 58 verification of the financial availability
- 59 if response is affirmative, sending of OK to portable device 100
- 60 recording of the operation
- 61 if response is negative, rejection of portable device 100
- 62 end of operation.

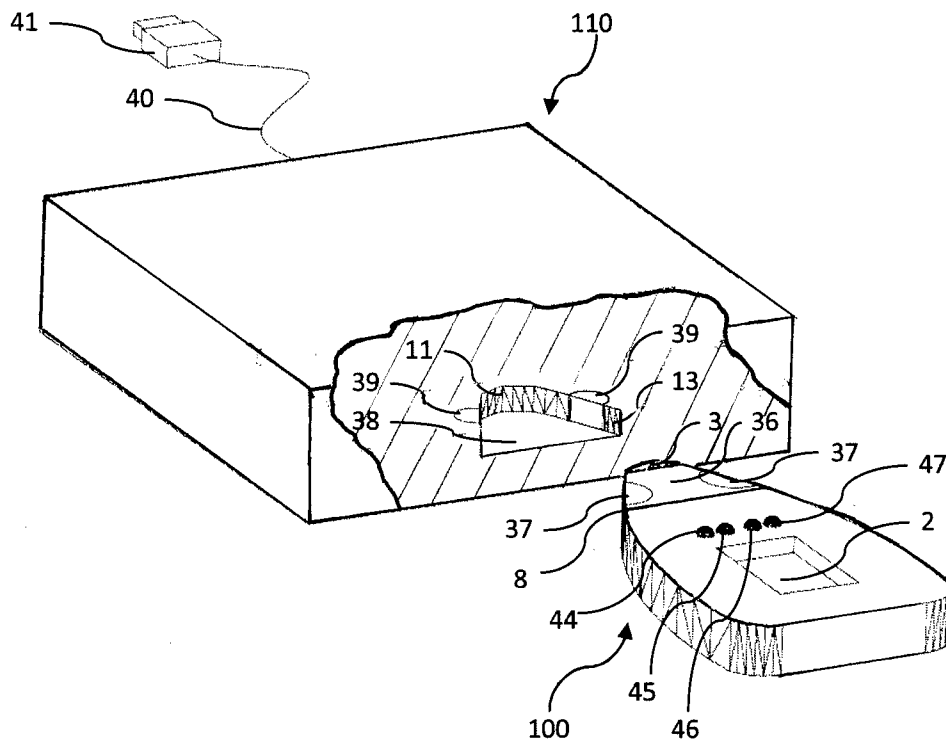




**Fig. 1**

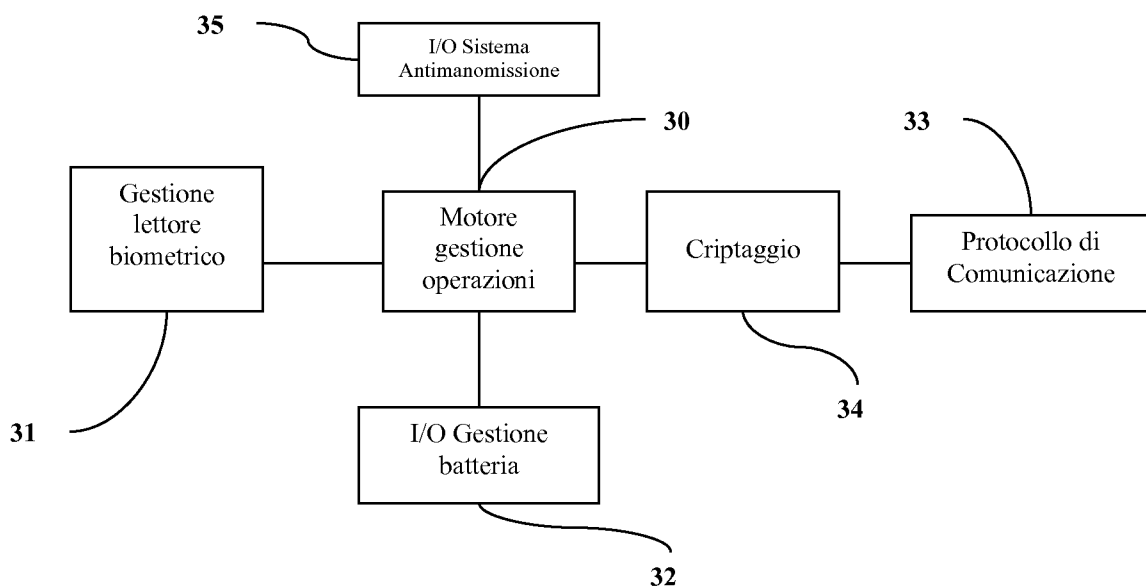


**Fig. 2**

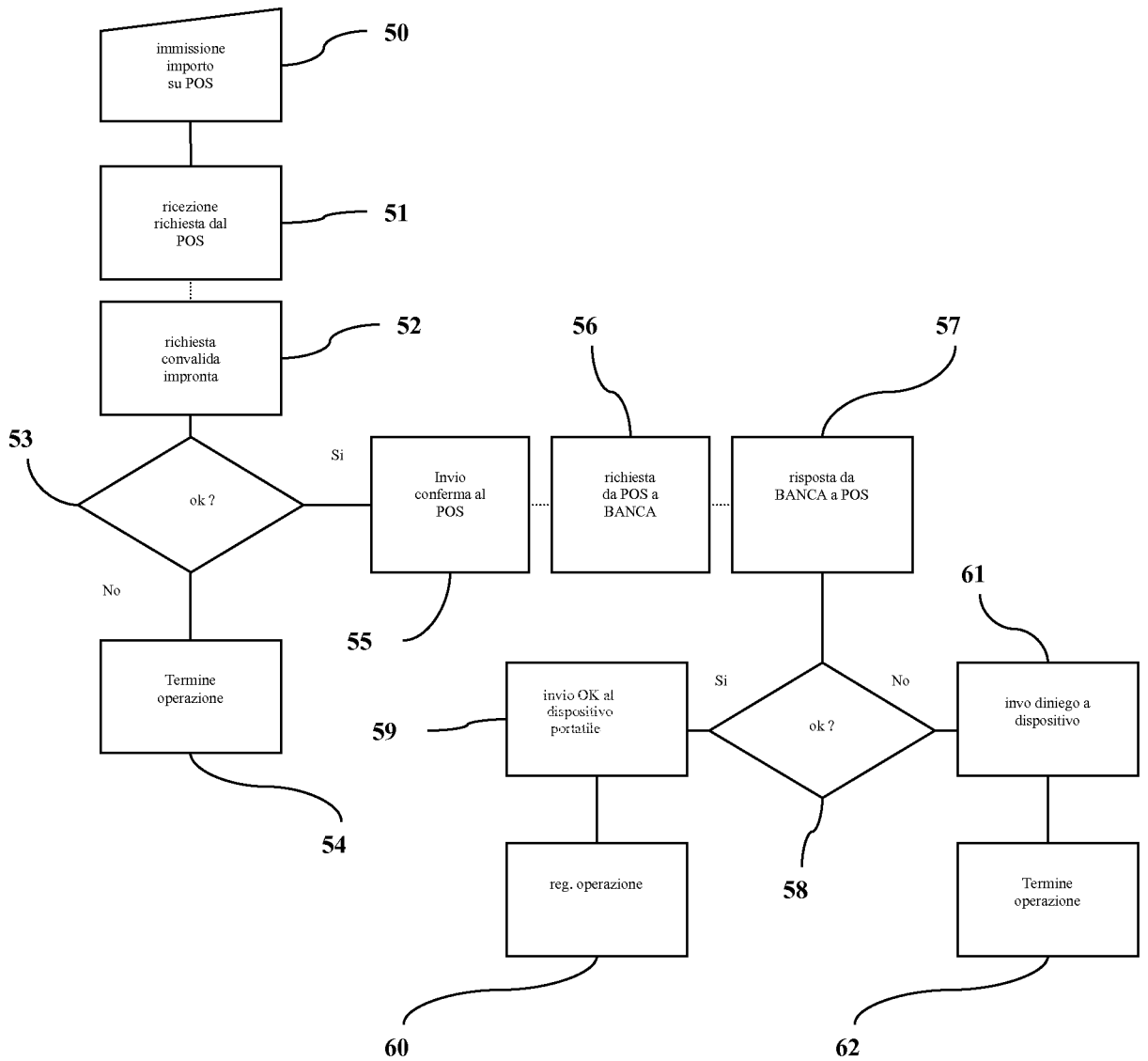


**Fig. 3**

p.i. di FG s.r.l. Agenzia Finanziaria  
Dott. Ing. Adriana Raimondi



**Fig. 4**



**Fig. 5**