ITALIAN PATENT OFFICE

Document No.

102012902061494A1

Publication Date

20131220

Applicant

SWOPAPP SOLUTIONS S.R.L.

Title

METODO ED APPARATO PER LA GESTIONE DI TRANSAZIONI TRAMITE CARTE DI CREDITO O DI DEBITO

Descrizione dell'Invenzione Industriale dal titolo: -**JC001**-

"METODO ED APPARATO PER LA GESTIONE DI TRANSAZIONI TRAMITE CARTE DI CREDITO O DI DEBITO"

di **SWOPAPP SOLUTIONS S.R.L.** di nazionalità italiana, con sede in Viale Campania 35, 21033 Milano, P.I. 07754760960; **JACOPO VANETTI** di nazionalità italiana con sede in Via Mercallo 25, 21018 Sesto Calende (VA), C.F. VNTJCP87S12B300P; **GIUSEPPE NICOLA SAPONARO** di nazionalità italiana, con sede in Via delle Ortensie 25, 28053 Castelletto Ticino (NO), C.F. SPNGPP86S08F205U ed elettivamente domiciliati per questo incarico presso i Mandatari Ing. Roberto Dini (No. Iscr. Albo 270 BM), Ing. Corrado Borsano (No. Iscr. Albo 466 BM), Ing. Marco Camolese (No. Iscr. Albo 882 BM),Ing. Matteo Baroni (Iscr. Albo N. 1064BM),Dott. Giancarlo Reposio (No. Iscr. Albo 1168 BM) c/o Metroconsult S.r.l., Foro Buonaparte 51, 20121 Milano.

Inventori designati:

JACOPO VANETTI, Via Mercallo 25, 21018 Sesto Calende (VA)

GIUSEPPE NICOLA SAPONARO in Via delle Ortensie, 25 28053 Castelletto Ticino (NO)

Depositata il No.

DESCRIZIONE

Campo di applicazione dell'invenzione

La presente invenzione si riferisce ad un metodo ed apparato per la gestione di transazioni tramite carte di credito o di debito.

Stato della tecnica

L'utilizzo di carte di credito e carte di pagamento (debito) sta subendo una forte crescita conseguente allo sviluppo tecnologico, che garantisce più affidabilità, alla comodità e alle norme anti-riciclaggio che limitano i pagamenti in contanti.

Queste carte sono usate per diversi tipi di transazione: dall'acquisto di beni o servizi a transazioni finanziarie.

L’informazione necessaria per ogni transazione è memorizzata e criptata in diversi modi a seconda della tipologia di carta, ad esempio carte con banda magnetica o smart-card; per le carte con banda magnetica l’informazione è salvata modificando il magnetismo delle particelle presenti sulla banda magnetica, le smart-card, invece, integrano ed utilizzano un chip EMV. EMV (Europay, *MasterCard* e *VISA*) è uno standard per l'utilizzo di smart card, terminali POS e bancomat per l'autenticazione di transazioni con carte di credito e di debito. Un carta con chip EMV possiede tutte le strutture necessarie per seguire questo standard.

I lettori di carte attualmente in commercio, POS (Point of sale), hanno una dimensione poco portabile perché pensati per un utilizzo interno agli esercizi commerciali. I POS utilizzano il modem incorporato per collegarsi con il centro di elaborazione della banca, o del gruppo di banche, che offre il servizio. Questo è incaricato all’autenticazione della richiesta che, nel caso positivo, viene processata.

Lo sviluppo dei cellulari di nuova generazione (Smart Phone) ha fornito gli strumenti necessari per gestire una richiesta di pagamento e interfacciarsi con il centro di elaborazione. Un lettore di carte può essere, infatti, collegato a uno smart-phone e passare le informazioni memorizzate nelle carte. Un canale dati universale presente su tutti i cellulari di ultima generazione è stato individuato nell’ingresso audio. Questo fornisce un canale sicuro per il passaggio di informazioni ma limitato nella velocità. Questo tipo di limite diventa molto vincolante se si vogliono trasportare dati di dimensione elevata.

Per questo motivo, a oggi, i POS portatili di tipo noto che utilizzano il canale audio per scambiare dati, si limitano a transazioni su carte di credito a banda magnetica. Queste ultime sono un tipo di carta poco usato in tutta Europa, per cui un dispositivo del genere sarebbe poco utile e coprirebbe

solamente una piccola percentuale delle transazioni. È quindi di importanza rilevante creare un sistema che gestisca le carte a chip.

Sommario dell'invenzione

Pertanto scopo della presente invenzione è quello di indicare un metodo ed apparato per la gestione di transazioni tramite carte di credito o di debito atto a superare tutti gli inconvenienti suddetti.

L'invenzione concerne in particolare un apparato per la gestione di transazioni tramite carte di credito o di debito, che comprende un lettore smart-card EMV connesso ad un telefono mobile tramite il canale audio del telefono mobile stesso.

Tramite la presente invenzione, oltre a fornire un tipo di connessione alternativa ai POS tradizionali, gli smart-phone, o in generale i dispositivi portatili, dotati di un lettore smart-card EMV connesso all'ingresso audio possono offrire servizi aggiuntivi per la gestione dei pagamenti e la visualizzazione di statistiche di vendita che rendono il sistema molto più di un metodo di pagamento.

E' oggetto della presente invenzione un apparato per la gestione di transazioni tramite carte di credito o di debito, che comprende un lettore di dette carte di credito o di debito, atto ad essere connesso ad un terminale tramite un canale audio di detto terminale, l'apparato comprendente: mezzi di lettura di dette carte di credito o di debito di tipo EMV; almeno un'interfaccia utente per introduzione di codici segreti, importi delle transazioni, e visualizzazione di detti importi; mezzi per il trattamento di dati relativi alle transazioni, tramite organizzazione in pacchetti e modulazione del tipo FSK, e di trasmissione bidirezionale tramite detto canale audio; almeno un'unità di elaborazione, posta in area sicura anti-manomissioni, per dette transazioni anche atta a gestire una connessione con un server centrale di gestione;

mezzi per crittografare detti dati.

E' pure oggetto della presente invenzione un metodo per la gestione di transazioni tramite carte di credito o di debito tramite l'apparato precedente, detto metodo comprendente i passi di: gestione della comunicazione tra detto lettore di dette carte di credito o di debito, e detto terminale tramite detto canale audio di detto terminale; trattamento di detti dati relativi alle transazioni, comprendenti codici segreti, importi delle transazioni, tramite organizzazione in pacchetti e modulazione del tipo FSK, e trasmissione bidirezionale tramite detto canale audio; immissione degli importi delle transazioni su detto terminale, e visualizzazione di detti importi su detto lettore di carte di credito o di debito; immissione dei codici segreti su detto lettore di carte di credito o di debito.

E' particolare oggetto della presente invenzione un metodo ed apparato per la gestione di transazioni tramite carte di credito o di debito, come meglio descritto nelle rivendicazioni, che formano parte integrante della presente descrizione.

Breve descrizione delle figure

Ulteriori scopi e vantaggi della presente invenzione risulteranno chiari dalla descrizione particolareggiata che segue di un esempio di realizzazione della stessa (e di sue varianti) e dai disegni annessi dati a puro titolo esplicativo e non limitativo, in cui:

La figura 1 descrive la struttura del sistema oggetto della presente invenzione e mostra i suoi componenti principali.

La figura 2 descrive il diagramma di flusso delle operazioni svolte dallo dispositivo mobile o lettore di carte durante una transazione.

La figura 3 descrive il diagramma di flusso delle operazioni svolte dal lettore di carte durante una transazione.

La figura 4 descrive il diagramma di flusso delle operazioni

svolte dal server durante una transazione.

La figura 5 descrive il diagramma di flusso della procedura di ricezione messaggi tramite ingresso audio lato dispositivo mobile.

La figura 6 descrive il diagramma di flusso della procedura di ricezione messaggi tramite ingresso audio lato lettore di carte.

La figura 7 descrive il diagramma di flusso della procedura di invio messaggi tramite audio sia dal lato dispositivo mobile che da quello lettore di carte.

La figura 8 descrive un esempio di schema a blocchi di realizzazione del circuito elettronico incorporato nel lettore di carte oggetto dell'invenzione.

Le figure 9a e 9b mostrano due viste di un esempio di realizzazione del contenitore del suddetto lettore di carte.

Gli stessi numeri e le stesse lettere di riferimento nelle figure identificano gli stessi elementi o componenti.

Descrizione di dettaglio di esempi di realizzazione

In figura 1 è mostrato lo schema a blocchi della struttura del dispositivo dell'invenzione e la relazione fra i suoi componenti. I due blocchi principali sono costituiti da un lettore di carte (Card Reader - 101) e da un'applicazione software che risiede sul dispositivo mobile (Mobile Device - 102).

Il sistema è in grado di portare a termine qualsiasi transazione finanziaria da carta di credito o di debito. Le carte devono possedere un chip EMV, come sopra definito, di per sé di tipo noto.

Il lettore (101) è miniaturizzato in modo tale da essere portabile e comunica col dispositivo mobile (102) che gestirà la transazione utilizzando un metodo di crittografia per rendere il trasferimento dati più sicuro.

Il lettore 101 comprende un'interfaccia utente per digitare il codice segreto e visualizzare le informazioni relative alla

transazione (103). Inoltre è provvisto di un sistema di acquisizione e gestione dei dati della carta che si sta utilizzando (104).

Facendo anche riferimento alla figura 8, si descrive un esempio di realizzazione del lettore.

Il lettore 101 è un terminale di pagamento alimentato a batteria per transazioni con carte di debito e credito a chip. È munito di una tastiera sicura a 12 tasti (fig. 9a, 9b) per l'introduzione del pin ed è conforme alle normative EMVL1, EMVL2, PCI3.1 ABI2.

Il lettore ha un display di visualizzazione in tecnologia oled monocromatica (OLED MONO) con dimensione 2 pollici. La tecnologia oled permette di avere consumi ridotti e ampio angolo di vista e buona definizione delle informazioni visualizzate.

Il lettore utilizza per la comunicazione verso altri dispositivi e per il routing della transazione di pagamento o un'interfaccia USB o un'interfaccia audio. Il terminale è anche dotato di un connettore MICRO-USB su cui è possibile aprire una connessione seriale in emulazione come effettuare la ricarica del pacco batterie litio polimero che lo alimenta.

I dati sull'interfaccia audio sono modulati in tecnica FSK, di cui in dettaglio in seguito, in modo da poter essere trasferiti ad un dispositivo esterno che si occupa di terminarli localmente per quanto riguarda lo scambio importo o inviarli in geografico per quanto riguarda la transazione bancaria.

Il lettore ha al suo interno due processori: un processore di sicurezza (SECURE PROCESSOR) ed un processore che gestisce la modulazione e demodulazione FSK (FSK MODEM).

Il processore di sicurezza è del tipo Arm SC100, con sistema operativo e manager di sicurezza, e sovraintende al controllo delle periferiche direttamente coinvolte nel processo di pagamento, quali smart card driver, tastiera, display, tamper

e mesh.

Il processore di sicurezza e le relative periferiche sono racchiusi in un'area sicura, dotata di copertura dei circuiti per sigillarli ed evitare manomissioni.

Il processore di sicurezza interfaccia un processore del tipo Cortex M0 che ha il compito di modulatore/demodulatore FSK dei pacchetti digitali da trasferire da e verso la porta audio.

Più nel particolare, il circuito di fig. 8 comprende inoltre i seguenti componenti:

- BUZZER: segnalatore acustico di tipo magnetico a completamento dell'interfaccia verso l'utente.
- XTAL 32Khz: oscillatore al quarzo richiesto dal real time clock di sistema e dal blocco di sicurezza del processore di sicurezza;
- XTAL 6Mhz: oscillatore al quarzo del processore di sicurezza in grado di generare la frequenza base, poi moltiplicata dal PLL interno;
- SMC connector: elemento di connessione della carta (smart card);
- DRIVER: di tipo TDA8035, è un circuito in gradi di adattare i livelli e le tempistiche di power up e power down dell'alimentazione verso la carta;
- KEYBOARD: tastiera
- 2xMesh:reti filari bipolari allocate nei circuiti stampati che compongono il dispositivo in modo da evitare l'intrusione dall'esterno in aree con componenti sensibili;
- 4xTamper: interruttori posti all'interno di aree sicure, in cui è compreso il processore di sicurezza, per rilevare la penetrazione dall'esterno o l'asportazione/sostituzione di parti/componenti locati nell'area sicura. L'intervento di un tamper o di una mesh causa la cancellazione della chiave master del terminale e quindi un suo non ulteriore utilizzo;
- NOR FLASH,SRAM, DATA FLASH: memorie di servizio;
- LDO: circuiti in grado di adattare il livello di tensione e

di stabilizzarlo come richiesto dai circuiti integrati a cui sono collegati: sono del tipo con bassa caduta di tensione fra ingresso e uscita;

- MAIN BATTERY,BATTERY CHARGER, batteria e relativo caricatore del lettore;
- MICRO USB: connettore micro-usb;
- SCROLL UP/DOWN: pulsanti di scroll per il modem;
- RING DETECT: Rilevatore di richiesta di connessione da parte del dispositivo mobile;
- AUDIO JACK: Presa audio
- OPAMP: amplificatori di segnale audio in ingresso e uscita.

Lo stato dei tasti up/down è trasferito in trasparente al processore di sicurezza mediante ripetizione di segnale su porte del tipo "gpio". La pressione del tasto up per più di 5 secondi provoca lo spegnimento del dispositivo. Dalla porta USB è effettuato anche l'aggiornamento di entrambe i processori.

Il circuito audio, attestato ad un connettore 3.5mm audio jack a 4 vie, adattato in livello e impedenza, entra nel circuito analogico (ADC e DAC) del processore cortex M0.

Il lettore di carte è stato concepito per consentire l'utilizzo dello stesso con qualsiasi dispositivo mobile. Come si può notare nelle figure 9a e 9b, esso è dotato di uno slot 91 per l'inserimento della carta di credito o debito 92.

E' dotato di una tastiera 93, di un display 94, una presa audio 95, una presa micro-USB 96, tasti di scroll up-down 97, descritti in precedenza.

Come anche da figura 1, dal punto di vita funzionale, il sistema di acquisizione e gestione dei dati (104) è realizzato anche tramite un software integrato nel lettore.

Il lettore di carte ed il dispositivo mobile utilizzano, per lo scambio dati, una interfaccia di tipo USB (106) oppure preferibilmente un'organizzazione a pacchetti ed un'apposita codifica FSK (frequency shift keying) del segnale audio,

descritte nel dettaglio in seguito, tramite la presa audio ed un connettore jack (107).

Il lettore di carte ed il dispositivo mobile sono dotati di moduli per la codifica e decodifica audio (107, 108); inoltre il dispositivo mobile è dotato di un sistema per l'acquisizione dei dati tramite USB (109) e un'interfaccia utente (103, 110).

Un altro componente, descritto in seguito, nel dispositivo mobile, si occupa dell'elaborazione delle transazioni (111), che gestisce anche una connessione bidirezionale tra il lettore di carte e un server (112) di gestione del servizio. Il server si occupa di fornire i messaggi delle transazioni dei servizi richiesti verso un blocco funzionale denominato gestore terminali (113). Queste comunicazioni avvengono in accordo con lo standard EMV di cui sopra, in modo in sé noto.

Un database (114) è collegato al server per tenere traccia di statistiche e informazioni utili al possessore del dispositivo mobile.

Il dispositivo mobile può essere di un qualsiasi tipo, purché dotato di ingresso audio. Ad esempio può essere un qualsiasi smart-phone o tablet dotato di sistema operativo Android, iOs e Windows Phone 7.

In alternativa al dispositivo mobile, può essere utilizzato un dispositivo non portabile come personal computer o terminale, dotato di presa audio, capace di gestire le informazioni provenienti dal lettore e comunicare con il server che si occupa dell'interfacciamento con il gestore terminali.

I moduli mostrati in figura 1 all'interno del dispositivo mobile(102) sono ad esempio realizzati come elementi di un'unica applicazione che risiede nella memoria del dispositivo.

L'interfaccia utente 103 presente sul lettore è ad esempio come descritta nelle figure 9a e 9b, quindi come detto

costituita da un tastierino alfa-numerico, ad esempio del tipo touch-screen e da un display per la visualizzazione delle informazioni relative alla transazione.

Il lettore di carte 101 descritto in figura 1 come già detto è configurato per poter leggere le smart-card seguendo lo standard EMV. Di seguito verranno illustrate le caratteristiche tecniche e di design.

Il segnale scambiato tra dispositivo mobile e lettore di carte è organizzato a pacchetti e quindi modulato con modulazione FSK.

Un esempio di struttura dei pacchetti inviati è la seguente:

SOH	ADD	CMD	LEN	PKT	0x02
0x02	Address 1 byte	CMD 1 Byte	Len 2 byte	pacchetto	CMD 1 Byte

Il significato dei campi del pacchetto è il seguente:

SOH = 0x02 inizio del pacchetto

ADD = Address, indica l'appartenenza logica del pacchetto

CMD = indica il tipo di messaggio

LEN = due byte che indicano la dimensione del pacchetto

PKT = payload, pacchetto trasportato

CRC = CRC 16 di controllo del pacchetto

Il campo ADD address in particolare può indicare uno scambio di messaggi tra smart-phone e dispositivo mobile, o tra dispositivo mobile e server.

La parte che invia un pacchetto si preoccupa di indicare l'address. La parte che riceve il pacchetto dovrà confermare la ricezione con un pacchetto ACK, o la mancata ricezione con un pacchetto NACK: in questo modo i due gestori garantiscono il trasporto e gestiscono il NACK, l'ACK o il timeout.

Se un ACK o un NACK non viene ricevuto entro il tempo di time-out, il pacchetto viene reinviato.

Il metodo di correzione errori usato per la trasmissione dei pacchetti è il CRC-16, standard CCITT che consente di evitare

l'aumento della lunghezza dei pacchetti dati.

L'FSK è la più comune modulazione digitale sulle alte frequenze radio. I dati sono trasportati mediante lo shifting in frequenza di un'onda sinusoidale. Nella sua forma più semplice il segnale può shiftare in modo discreto fra due frequenze dette space (corrispondente a 0, ad esempio a 3 Khz) e mark (corrispondente a 1, ad esempio a 7 Khz). Il tempo necessario per trasmettere un singolo bit viene chiamato periodo di bit. Il suo inverso ci da` la velocità di trasmissione spesso misurata in bauds o bps. Il periodo di bit è vincolato dalle frequenze utilizzate che a loro volta sono vincolate dalla frequenza di campionamento degli apparecchi comunicanti.

La codifica FSK può essere coerente o non coerente.

Il segnale generato in maniera coerente è simile a quello prodotto passando discretamente dalla frequenze di mark a quella di space.

La condizione di continuità di fase della modulazione FSK (glitch free) obbliga, nel caso coerente, ad avere una relazione tra lo shift e il periodo di bit.

L'FSK incoerente consente una maggiore libertà nella scelta dei parametri ma è più sensibile agli errori.

L'FSK può essere usato in maniera sincrona o asincrona.

I metodi di ricezione e decodifica si basano sulla tecnica di frequency-detection. La frequency-detection può lavorare tramite demodulazione sia nel dominio del tempo che nel dominio delle frequenze.

Se si realizza un algoritmo di demodulazione che lavora nel dominio delle frequenze, è preferibile utilizzare filtri passa banda, per isolare le frequenze di interesse nel segnale in input e sopprimere possibili disturbi su di esso. Una volta applicati i filtri il demodulatore si occupa di decidere se il segnale analizzato corrisponde a un 1 o a uno zero.

Questi metodi hanno una complessità di calcolo elevata

rispetto a quelli che lavorano nel dominio del tempo ma sono più resistenti alle perturbazioni.

Particolare cura è utilizzata nella finestratura del segnale (tipo di finestra, dimensione).

Una possibile implementazione dell'algoritmo di demodulazione che lavora nel dominio delle frequenze prevede i seguenti passi:

(a) monitorare il segnale fino a che questo non supera il valore di una soglia determinata empiricamente: in tal caso procedere;

(b) acquisizione e finestratura segnale;

(c) filtraggio segnale con filtro passa banda intorno alla frequenza di mark;

(d) filtraggio segnale con filtro passa banda intorno alla frequenza di space;

(e) confronto dei due segnali filtrati e determinazione bit;

(f) ripetere i punti b, c, d fino a che il segnale non è sotto il threshold citato, altrimenti passare a f;

(g) ricostruzione codice binario ricevuto.

Nel caso invece di utilizzo di un algoritmo di demodulazione che lavora nel dominio del tempo, esistono diversi approcci al problema di demodulazione e riconoscimento della frequenza.

Per la demodulazione nel dominio del tempo è preferibile finestrare il segnale con una finestra di dimensione inferiore al periodo di bit e step ulteriormente inferiore per minimizzare gli errori(ad esempio finestra lunga 1/2 e step 1/3 del periodo di bit). Una volta analizzato il segnale ed estratti i bit bisogna tener conto di questi particolari per ricostruire il codice binario inviato.

Una possibile implementazione dell'algoritmo di demodulazione che lavora nel dominio del tempo prevede i seguenti passi:

(a) monitorare il segnale fino a che questo non supera il valore di una soglia determinata empiricamente; in tal caso procedere;

(b) acquisizione e finestratura del segnale;

(c) procedere con la regola di discriminazione binaria (descritta nel seguito);

(d) ripetere i punti b e c fino a che il segnale non è sotto la soglia citata, altrimenti passare a (e);

(e) ricostruzione codice binario ricevuto tenuto conto della dimensione della finestra utilizzata e dello step di finestratura.

Le regole di discriminazione binaria differiscono a seconda dello strumento di analisi utilizzato. Di seguito un elenco di strumenti maggiormente utilizzati e rispettive possibili implementazioni.

- Peak detection:

(a) analizzare il segnale fino a che non supera una di due soglie (una negativa e una positiva) individuate empiricamente.

(b) attendere che il segnale attraversi nuovamente la soglia facendo attenzione a rapide variazioni del segnale che possono trarre in inganno l'algoritmo;

(c) una volta attraversata la soglia, analizzare i cambi di pendenza del segnale compreso tra i due attraversamenti ed estrarre il punto di massimo. Se sono individuati più campi di pendenza, si esegue la media tra i due campioni che indicano l'attraversamento della soglia;

(d) assicurarsi che il picco trovato al passo precedente sia più alto in ampiezza dei picchi precedenti, altrimenti scartarlo;

(e) assicurarsi che il picco abbia cambiato polarità: se sì, sostituire il picco precedente con quello corrente, altrimenti aggiungere semplicemente il picco alla lista;

(f) a seconda del numero di picchi determinati, stimare la frequenza del segnale analizzato e assegnare un 1 o uno 0.

- Un approccio simile è quello dello zero-crossing rate. In questo caso a essere individuati non sono i picchi ma il

numero di volte che il segnale attraversa lo 0. Ancora una volta questo numero ci determina il bit da assegnare.

- Altri metodi sfruttano la cross-correlazione come strumento per riconoscere la frequenza del segnale preso in analisi.

La cross-correlazione viene utilizzata come una misura di somiglianza. Una sua spiegazione intuitiva è la seguente: è l'integrale del prodotto tra un segnale x e un segnale y anticipato sull'asse del tempo di una quantità i. Il processo viene ripetuto per ogni possibile valore di i. Quando i due segnali (il primo e quello ritardato) sono simili, il valore della cross-correlazione per quel determinato valore di i è massimizzato. Analiticamente:

$$r(i) = \sum_{m=-\infty}^{\infty} y(n)^* \cdot x(n-i)$$

Utilizzando questo strumento con x = y ci si riferisce alla auto-correlazione. L'auto-correlazione ci fornisce una misura del periodo del segnale in esame e quindi della frequenza. In modo diverso si può utilizzare come y il segnale da analizzare e come x due sinusoidi alle frequenze di mark e di space. Il valore massimo tra le due correlazioni determina il bit associato al segnale.

I metodi sopra citati hanno una complessità molto bassa, ma sono sensibili agli errori sul segnale. Per evitarle gli errori si possono usare in serie filtri passa banda che comprendono le frequenze di mark e space.

Il sistema oggetto dell'invenzione permette di effettuare transazioni finanziarie in mobilità ma può essere utilizzato anche in sostituzione dei POS tradizionali.

Un comune utilizzo può essere operato tra due soggetti nel seguito definiti cliente ed esercente. L'esercente rappresenta il possessore del lettore di carte e del dispositivo mobile su cui è installata l'applicazione. Il cliente è il possessore

della carta a cui verrà addebitata la transazione.

L'esercente ha a disposizione un'interfaccia (110) fornita dall'applicazione installata sul proprio dispositivo mobile che gli permette di inserire l'importo della transazione e ulteriori informazioni relative all'operazione. Per inserimento dell'importo si intende sia un inserimento diretto sia indiretto tramite la selezione di prodotti associati all'esercente. A questo punto il cliente deve digitare il codice di sicurezza della carta sull'interfaccia presente nel lettore dopo aver inserito la carta nell'apparecchio.

L'applicazione si occupa di portare a termine la transazione e ne mostra l'esito sia all'esercente che al cliente.

Se necessario, sarà richiesta al cliente la firma mediante un sistema di acquisizione presente sull'applicazione.

La lista di prodotti associati all'esercente risiede nel database (114) e può essere modificata e aggiornata tramite l'interfaccia utente (110).

La privacy del cliente è protetta durante l'intera transazione:infatti le informazioni immesse nel sistema sono crittografate e passano direttamente all'elaboratore senza passare dall'interfaccia utente dell'applicazione; inoltre vi è un disaccoppiamento delle interfacce (una per il cliente e una per l'esercente).

E' inoltre generata una ricevuta della transazione e consegnata al cliente secondo la modalità scelta.

Alcune informazioni della transazione, non sensibili, sono catturate dal database (114) per la formazione di statistiche consultabili, come già detto, dall'interfaccia dell'applicazione (110).

Il dispositivo mobile comunica con il server centrale (112) attraverso un network di comunicazione che utilizza un protocollo come ad esempio il protocollo TCP/IP. Network di questo genere possono essere ad esempio internet, Wi-Fi e network di comunicazione mobile (3G, 4G ecc.).

Nel seguito vengono descritte le operazioni eseguite dalla applicazione software oggetto dell'invenzione.

Con riferimento alla figura 2, si descrive il diagramma di flusso delle operazioni svolte dalla parte di applicazione residente nello smart-phone o mobile device durante una transazione.

All'apertura dell'applicazione (Blocco 201 - Application opened), si verifica se il lettore è connesso (Blocco 202 - is the device plugged in?).

Se no, l'applicazione emette un messaggio negativo (Blocco 203 - output message: "plug in the device").

Se invece il lettore è connesso, l'applicazione attende un input dall'utente (Blocco 204 - wait for the user input).

Quando l'utente inizia a selezionare l'opzione di utilizzo del lettore (Blocco 205 - "pay with card" option selected), l'applicazione attende l'immissione dell'importo (Blocco 206 - wait for the amount).

Dopo l'introduzione della carta, prepara un messaggio modulato in FSK e lo invia all'uscita audio (Blocco 207 - modulate a message containing the amount via FSK and send it to the audio output).

Quindi l'applicazione inizia la comunicazione con il lettore ed il server (Blocco 208 - wait for the message from the card reader and forward it to the server), (Blocco 209 - wait for the server response and forward it to the card reader).

Quindi dopo l'immissione dell'importo l'applicazione invia, tramite modulazione FSK, un messaggio contenente l'informazione appena acquisita. A questo punto aspetta il messaggio da parte del lettore da inoltrare al server che successivamente lo girerà al gestore terminali. Quindi attende la risposta del server e inoltra quest'ultima al lettore.

Al termine controlla se la transazione si è svolta correttamente (Blocco 210 - was the transactions successfull?). Se no, controlla se l'utente sceglie di

riprovare (Blocco 211 – is "retry" selected). Se no, ritorna al punto 204 di cui sopra. Se sì, ritorna al punto 207 di cui sopra.

Se invece la transazione si è svolta correttamente, chiede di scegliere il sistema di fatturazione e la firma se necessario (Blocco 212 – ask for the billing mode and for the sign, if necessary).

Al termine della procedura formatta la fattura e la spedisce, eventualmente corredata da informazioni supplementari, quali ad es. fotografie, coordinate bancarie, ecc… (Blocco 213 – send the bill together with extra infos (photos, coordinates).

Quindi genera un messaggio in uscita di transazione completata correttamente (Blocco 214 – output message "transaction successfully completed").

Poi ritorna al punto 204 in attesa di un altro input dall'utente.

La figura 3 descrive il diagramma di flusso delle operazioni svolte dal lettore di carte durante una transazione.

All'inizio il lettore viene acceso (Blocco 301 –Awakening).

Poi attende un messaggio proveniente attraverso la porta audio (Blocco 302 – wait for messages coming from the audio port).

Quindi il lettore si mette in ascolto sulla porta audio (Blocco 303 – amount message). Inoltre visualizza l'importo (Blocco 304 – show the amount).

Se riceve un messaggio con l'importo da pagare allora si predispone ad attendere l'inserimento della carta (Blocco 305 – wait for the card to be inserted).

Se è richiesto di inserire un PIN di riconoscimento (Blocco 306 – is the pin required?), richiede il PIN (Blocco 307 – ask for the pin). Poi gestisce l'inserimento del PIN controllandone la correttezza (Blocco 308 – is the pin correct?).

Al termine dell'inserimento del PIN, crea il messaggio

contenente l'importo da inviare al dispositivo mobile (Blocco 309 - create the message to be sent).

Quindi modula in FSK il messaggio e lo invia in uscita (Blocco 310 - modulate via FSK the signal and send it to the audio output).

Poi si predispone in attesa di risposta dal dispositivo mobile (Blocco 311 - wait for the response), e poi mostra sul display il risultato e spedisce il messaggio al dispositivo mobile (Blocco 312 - show the transaction result on the screen and send it to the phone).

La figura 4 descrive il diagramma di flusso delle operazioni svolte dal server per gestire il colloquio con il dispositivo mobile.

Quando il server avverte che il dispositivo mobile gli sta inviando un messaggio (Blocco 401 - message received from the mobile device), apre un colloquio con il gestore dei terminali 113 (Blocco 402 - open a socket to the GT).

Quindi spedisce il messaggio al gestore terminali (Blocco 403 - send the message).

Poi attende la risposta dal gestore terminali (Blocco 404 - wait for the GT's response).

Infine ritorna un messaggio di risposta al dispositivo mobile (Blocco 405 - send the response to the iPhone).

La figura 5 descrive il diagramma di flusso della procedura di ricezione messaggi tramite ingresso audio lato dispositivo mobile. La comunicazione avviene a pacchetti per facilitare e rendere più veloce l'invio di messaggi nel caso si presenti qualche errore.

Lo stato iniziale è di attesa della ricezione di un pacchetto del messaggio (Blocco 501 - wait for an incoming packet)

Al ricevimento del massaggio controlla la correttezza della ricezione (Blocco 502 - is the message received correctly?).

Se non è corretta spedisce un segnale di riconoscimento di non correttezza al lettore (Blocco 503 - send back a NACK). Se

invece è corretta, spedisce un segnale di riconoscimento di correttezza al lettore (Blocco 504 – send back an ACK).

Quindi verifica la correttezza della destinazione e riempie il buffer corrispondente (Blocco 505 – verify destination and fill the correspondent buffer). La destinazione definisce l'oggetto a cui deve essere inoltrato il messaggio. Può essere il dispositivo stesso o il gestore terminali.

Quando il messaggio è completo (Blocco 506 – is the message complete?) legge o spedisce il messaggio (Blocco 507 – read or forward the message), poi ritorna all'inizio (punto 501), altrimenti attende un altro pacchetto fino al termine dei pacchetti del messaggio ritornando al punto 501.

La figura 6 descrive il diagramma di flusso della procedura di ricezione messaggi tramite ingresso audio lato lettore di carte, simile e speculare alla precedente.

Lo stato iniziale è di attesa della ricezione di un pacchetto del messaggio (Blocco 601 – wait for an incoming packet)

Al ricevimento del massaggio controlla la correttezza della ricezione (Blocco 602 – is the message received correctly?).

Se non è corretta spedisce un segnale di riconoscimento di non correttezza al lettore (Blocco 603 – send back a NACK). Se invece è corretta, spedisce un segnale di riconoscimento di correttezza al lettore (Blocco 604 – send back an ACK).

Quindi verifica la correttezza della sorgente del messaggio e riempie il buffer corrispondente (Blocco 605 – verify the source of the message and fill the correspondent buffer). La sorgente definisce il soggetto che ha inviato il messaggio. Può essere il lettore carte o il dispositivo mobile.

Quando il messaggio è completo (Blocco 606 – is the message complete?) legge o spedisce il messaggio (Blocco 607 – read or forward the message), poi ritorna all'inizio (punto 601), altrimenti attende un altro pacchetto fino al termine dei pacchetti del messaggio ritornando al punto 601.

La figura 7 descrive il diagramma di flusso della procedura

di invio messaggi tramite audio sia dal lato smart-phone che da quello lettore di carte.

Lo stato iniziale è di attesa di un messaggio da trasmettere (Blocco 701 - waiting for a message to send).

Poi il messaggio viene organizzato in pacchetti (Blocco 702 - fragment the message into smaller packets).

Quindi si predispone all'invio dei pacchetti uno di seguito all'altro (Blocco 703 - is there a packet to send?), aggiungendo ad ogni pacchetto un header secondo quanto descritto sopra (Blocco 704 - envelop the packet with an header). Inoltre ogni pacchetto è modulato FSK e spedito all'uscita (Blocco 705 - modulate the packet into an FSK signal and send it out).

Per ogni pacchetto svolge iterativamente la seguente procedura ritornando per ogni pacchetto al punto 703.

Attende la risposta dell'altra parte ricevente (Blocco 706 - wait for the response), e verifica se è trascorso il tempo massimo di attesa (Blocco 707 - is time-out occurred?)

Verifica il corretto riconoscimento del messaggio attendendo di ricevere un messaggio ACK positivo oppure NACK negativo, con la procedura su descritta (Blocco 708 - is the response an ACK?). Se la ricezione non è corretta, richiede la ritrasmissione ritornando al punto 705, altrimenti ritorna al punto 703, fino al termine dei pacchetti del messaggio.

La presente invenzione può essere vantaggiosamente realizzata tramite un programma per computer che comprende mezzi di codifica per la realizzazione di uno o più passi del metodo, quando questo programma è eseguito su di un computer. Pertanto si intende che l'ambito di protezione si estende a detto programma per computer ed inoltre a mezzi leggibili da computer che comprendono un messaggio registrato, detti mezzi leggibili da computer comprendendo mezzi di codifica di programma per la realizzazione di uno o più passi del metodo, quando detto programma è eseguito su di un computer.

JC001

Sono possibili varianti realizzative all'esempio non limitativo descritto, senza per altro uscire dall’ambito di protezione della presente invenzione, comprendendo tutte le realizzazioni equivalenti per un tecnico del ramo.

Dalla descrizione sopra riportata il tecnico del ramo è in grado di realizzare l’oggetto dell’invenzione senza introdurre ulteriori dettagli costruttivi.

RIVENDICAZIONI

1. Apparato per la gestione di transazioni tramite carte di credito o di debito, che comprende un lettore (101) di dette carte di credito o di debito, atto ad essere connesso ad un terminale (102) tramite un canale audio di detto terminale, l'apparato comprendente:

- mezzi di lettura di dette carte di credito o di debito di tipo EMV;
- almeno un'interfaccia utente per introduzione di codici segreti, importi delle transazioni, e visualizzazione di detti importi;
- mezzi per il trattamento di dati relativi alle transazioni, tramite organizzazione in pacchetti e modulazione del tipo FSK, e di trasmissione bidirezionale tramite detto canale audio;
- almeno un'unità di elaborazione, posta in area sicura anti-manomissioni, per dette transazioni anche atta a gestire una connessione con un server centrale di gestione;
- mezzi per crittografare detti dati.

2. Apparato come nella rivendicazione 1, in cui detta interfaccia utente comprende un display di tipo OLED monocromatico, e una tastiera sicura a 12 tasti.

3. Apparato come nella rivendicazione 1, comprendente mezzi di interfacciamento di tipo USB tra detto lettore (101) di carte di credito o di debito e detto terminale

4. Apparato come nella rivendicazione 1, in cui detta area sicura anti-manomissioni comprende reti filari bipolari tipo MESH, interruttori tipo TAMPER, atti a rilevare la penetrazione dall'esterno o l'asportazione/sostituzione di parti/componenti locati nell'area sicura.

5. Metodo per la gestione di transazioni tramite carte di credito o di debito tramite un apparato come in una qualsiasi delle rivendicazioni precedenti, detto metodo comprendente i passi di:

- gestione della comunicazione tra detto lettore (101) di dette carte di credito o di debito, e detto terminale (102) tramite

detto canale audio di detto terminale;

- trattamento di detti dati relativi alle transazioni, comprendenti codici segreti, importi delle transazioni, tramite organizzazione in pacchetti e modulazione del tipo FSK, e trasmissione bidirezionale tramite detto canale audio;

- immissione degli importi delle transazioni su detto terminale, e visualizzazione di detti importi su detto lettore di carte di credito o di debito;

- immissione dei codici segreti su detto lettore di carte di credito o di debito.

CLAIMS

1. An apparatus for managing transactions through credit or debit cards, which comprises a reader (101) of said credit or debit cards, the reader adapted to be connected to a terminal (102) via an audio channel of said terminal, the apparatus comprising:
- means for reading said credit or debit cards of the EMV type;
- at least one user interface for entering secret codes and transaction amounts, and for displaying said amounts;
- means for treating transaction-related data through packet arrangement and FSK modulation, and for bidirectional transmission via said audio channel;
- at least one processing unit, placed in an anti-tamper secure area, for processing said transactions, which is also adapted to handle a connection to a central management server;
- means for encrypting said data.

2. An apparatus according to claim 1, wherein said user interface comprises a display of the monochromatic OLED type and a 12-key secure keypad.

3. An apparatus according to claim 1, comprising USB interface means between said reader (101) of credit or debit cards and said terminal.

4. An apparatus according to claim 1, wherein said anti-tamper secure area comprises wired two-pole networks of the MESH type and switches of the TAMPER type adapted to detect intrusion from the outside or removal/substitution of parts/components located in the secure area.

5. A method for managing transactions through credit or debit cards by means of an apparatus according to any one of the preceding claims, said method comprising the steps of:
- managing the communication between said credit or debit card reader (101) and said terminal (102) via said audio

channel of said terminal;

- treating said transaction-related data, comprising secret codes and transaction amounts, through packet organization and FSK modulation, and bidirectional transmission via said audio channel;

- entering transaction amounts into said terminal, and displaying said amounts on said reader of credit or debit card;

- entering secret codes into said credit or debit card reader.

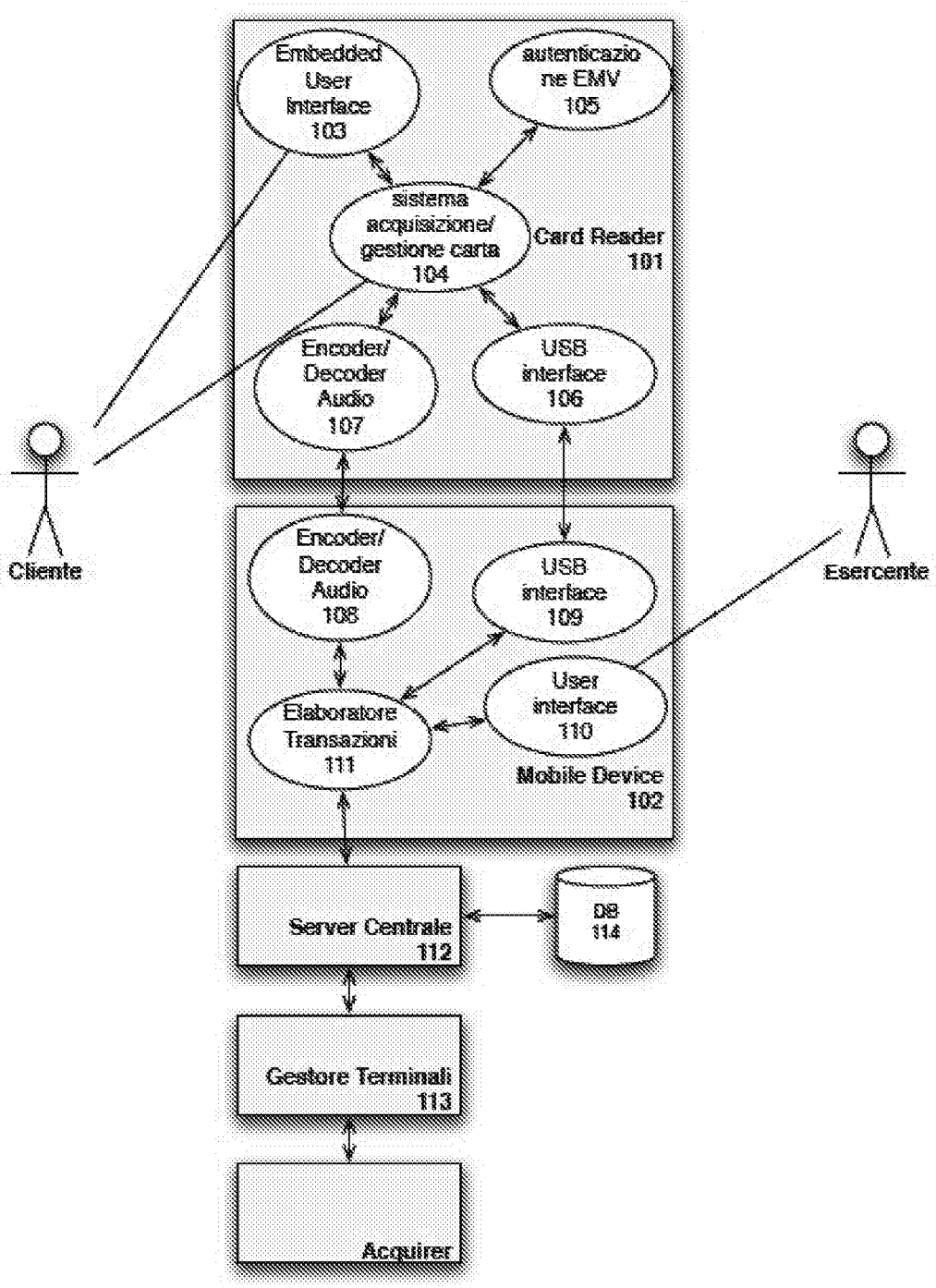
Embedded User Interface 103
autenticazione EMV 105
sistema acquisizione/ gestione carta 104
Card Reader 101
Encoder/ Decoder Audio 107
USB interface 106
Cliente
Esercente
Encoder/ Decoder Audio 108
USB interface 109
User interface 110
Elaboratore Transazioni 111
Mobile Device 102
Server Centrale 112
DB 114
Gestore Terminali 113
Acquirer

FIGURA 1

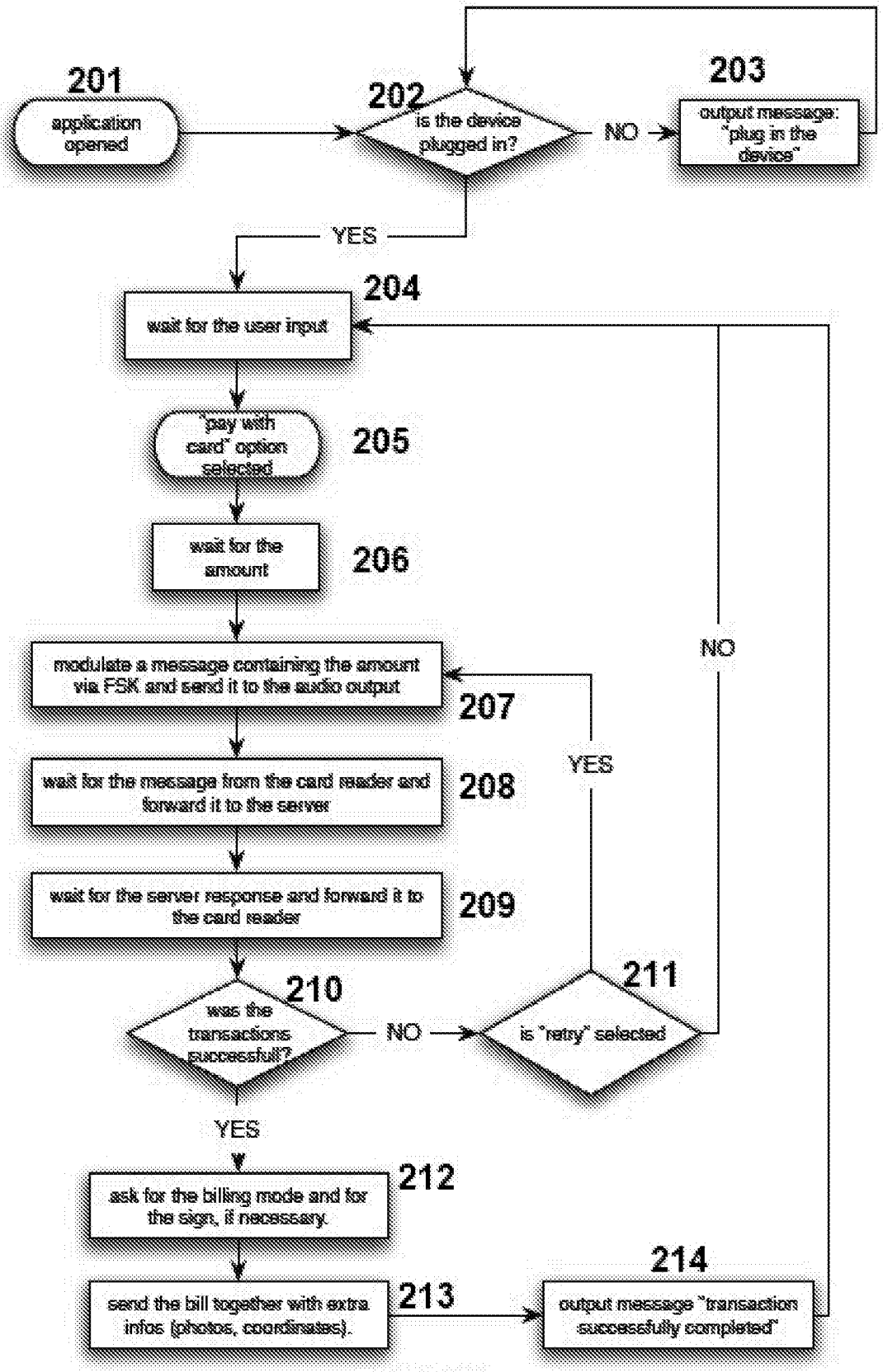
201
application opened
202
is the device plugged in?
NO
203
output message: "plug in the device"
YES
204
wait for the user input
"pay with card" option selected
205
wait for the amount
206
modulate a message containing the amount via FSK and send it to the audio output
207
wait for the message from the card reader and forward it to the server
208
wait for the server response and forward it to the card reader
209
was the transactions successful?
210
NO
is "retry" selected
211
YES
NO
YES
ask for the billing mode and for the sign, if necessary.
212
send the bill together with extra infos (photos, coordinates).
213
output message "transaction successfully completed"
214

FIGURA 2

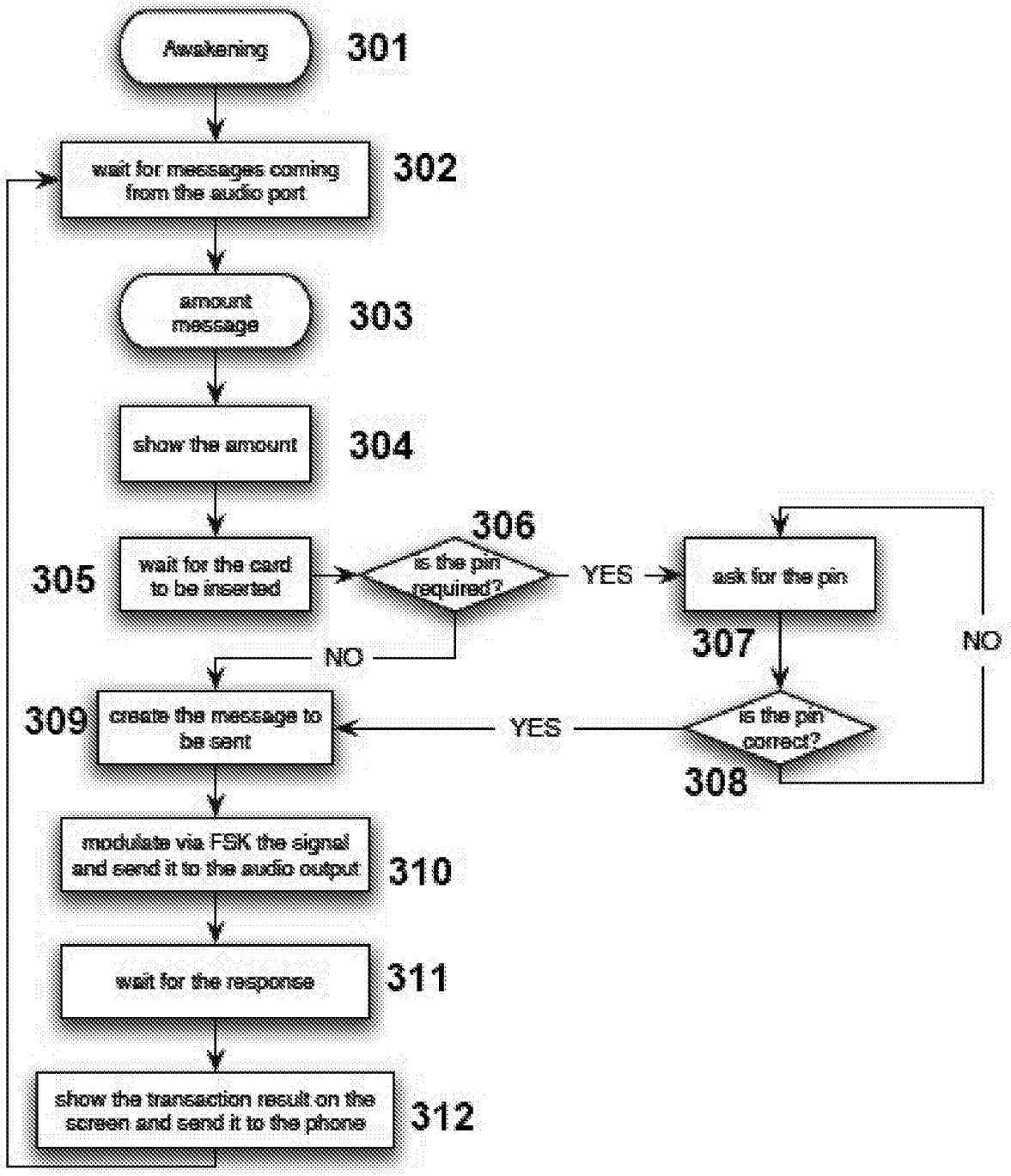
Awakening
301
wait for messages coming from the audio port
302
amount message
303
show the amount
304
306
wait for the card to be inserted
305
is the pin required?
YES
ask for the pin
307
NO
NO
309
create the message to be sent
YES
is the pin correct?
308
modulate via FSK the signal and send it to the audio output
310
wait for the response
311
show the transaction result on the screen and send it to the phone
312

FIGURA 3

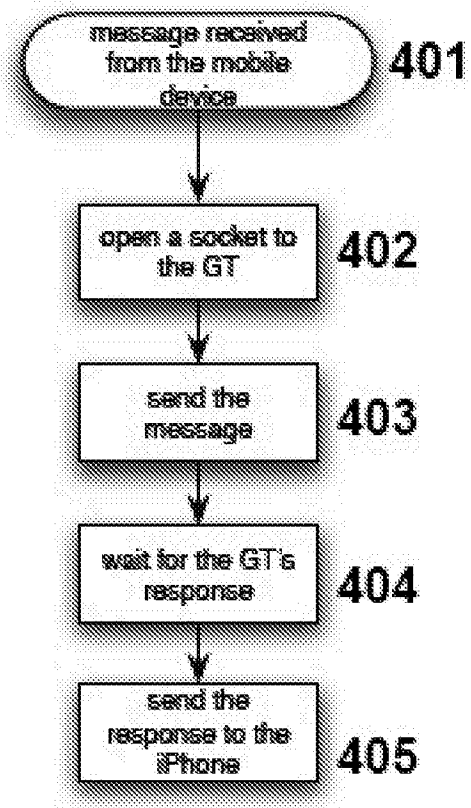
message received from the mobile device
401
open a socket to the GT
402
send the message
403
wait for the GT's response
404
send the response to the iPhone
405

FIGURA 4

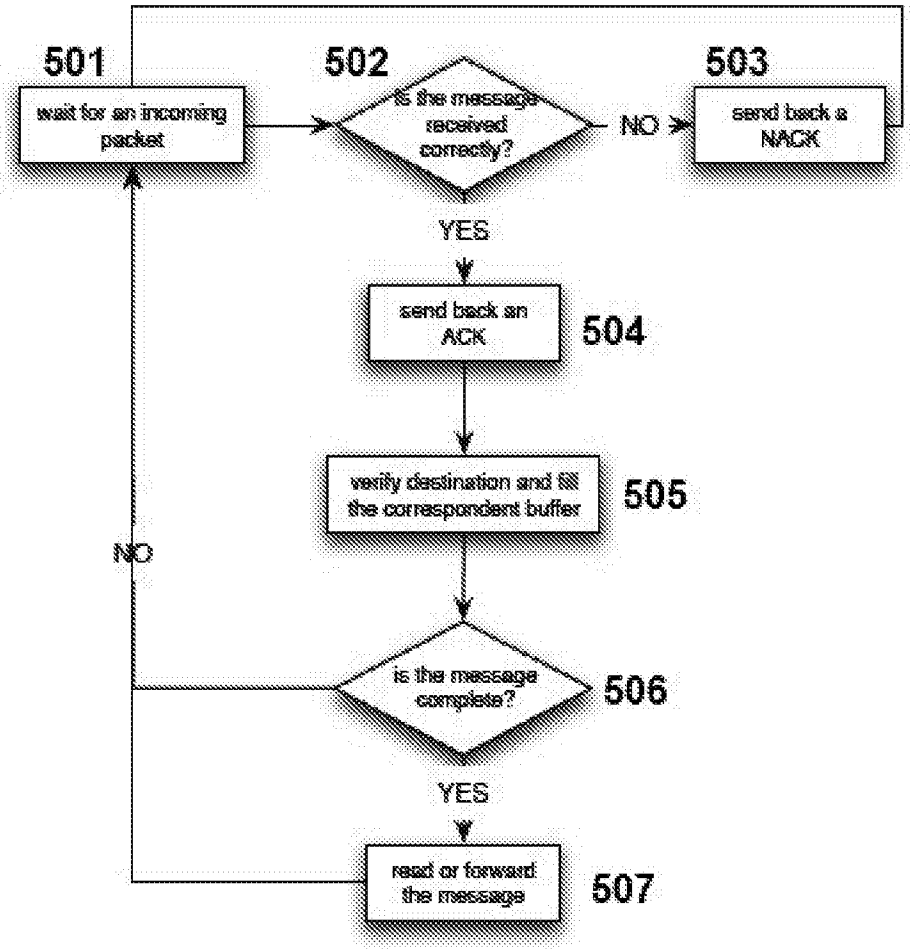
501
wait for an incoming packet
502
is the message received correctly?
NO
503
send back a NACK
YES
send back an ACK
504
verify destination and fill the correspondent buffer
505
NO
is the message complete?
506
YES
read or forward the message
507

FIGURA 5

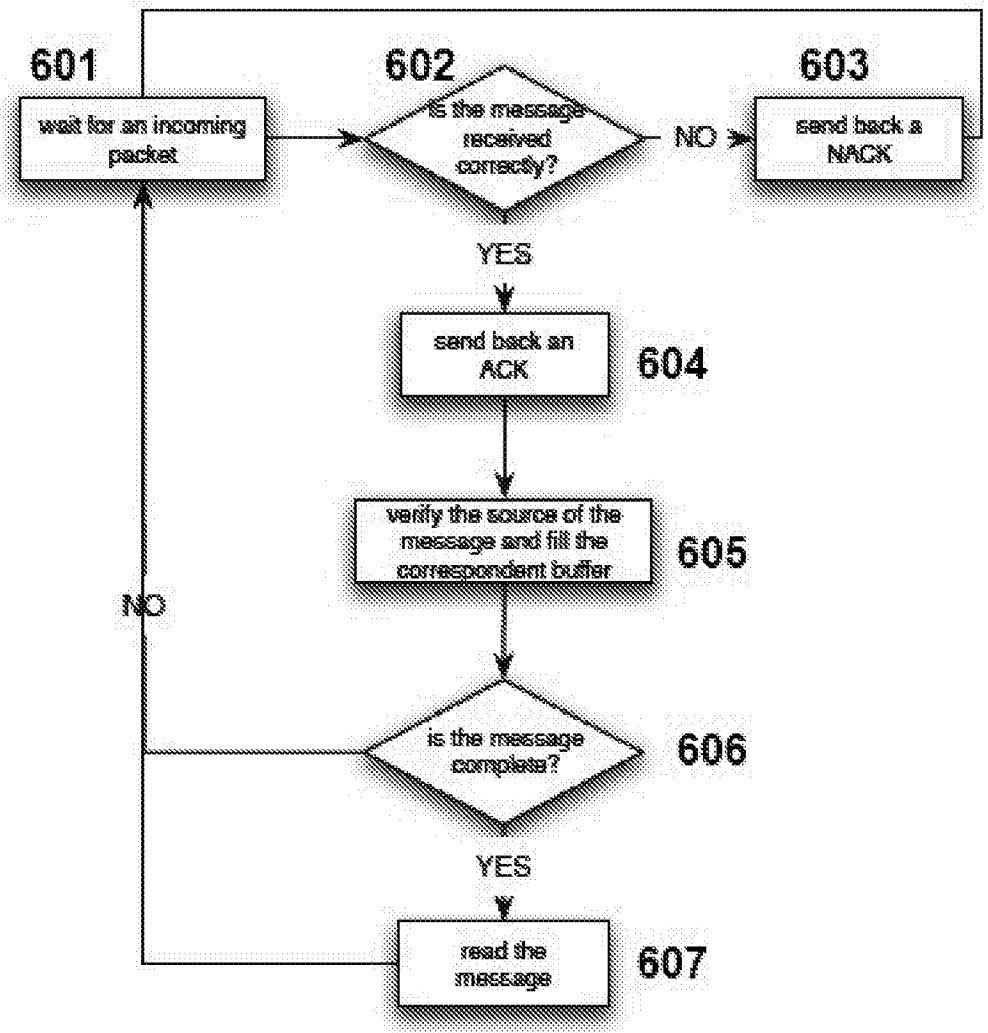
601
wait for an incoming packet
602
is the message received correctly?
NO
603
send back a NACK
YES
send back an ACK
604
verify the source of the message and fill the correspondent buffer
605
NO
is the message complete?
606
YES
read the message
607

FIGURA 6

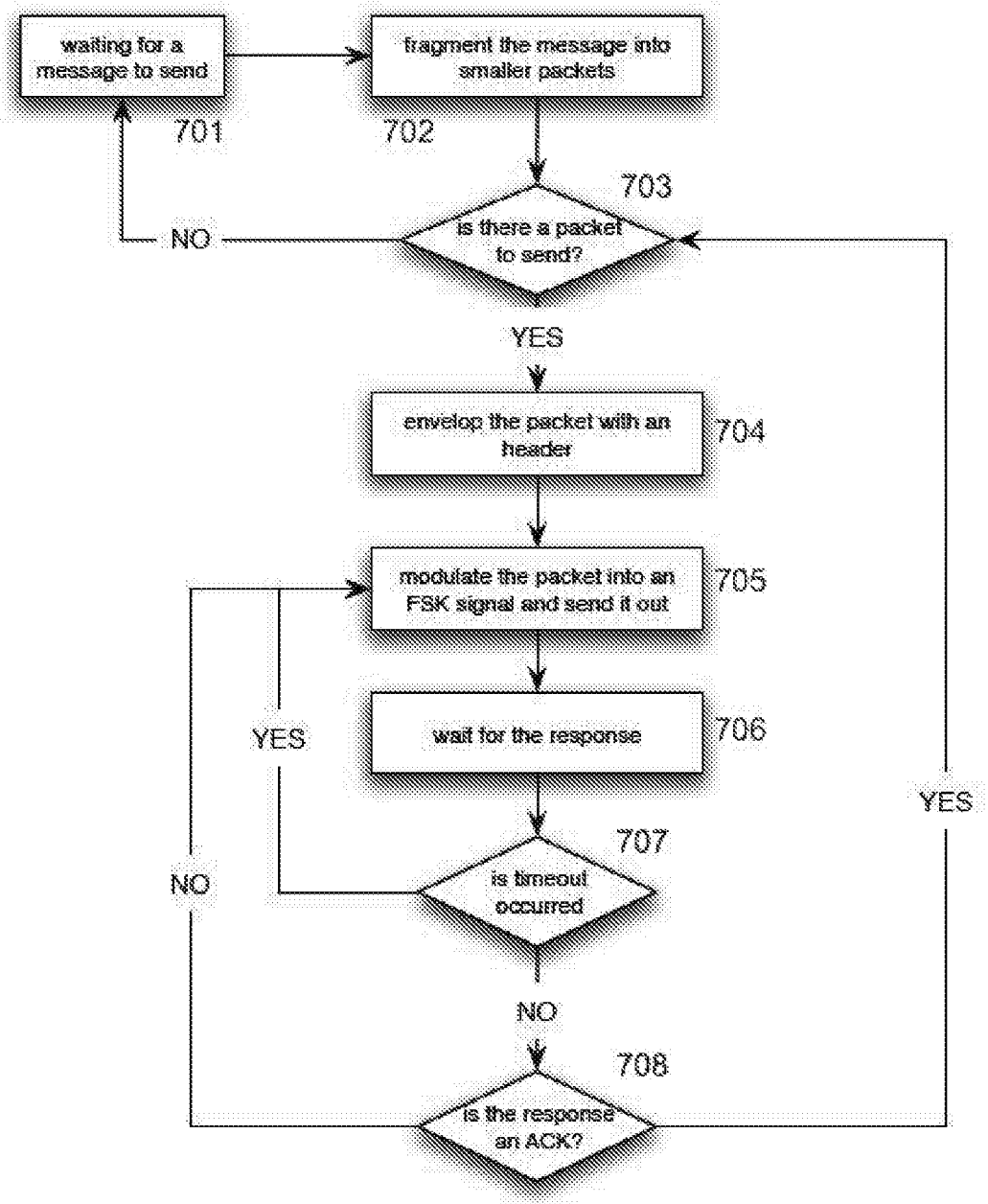
waiting for a message to send
701
fragment the message into smaller packets
702
703
is there a packet to send?
NO
YES
envelop the packet with an header
704
modulate the packet into an FSK signal and send it out
705
wait for the response
706
YES
707
is timeout occurred
NO
NO
YES
708
is the response an ACK?

FIGURA 7

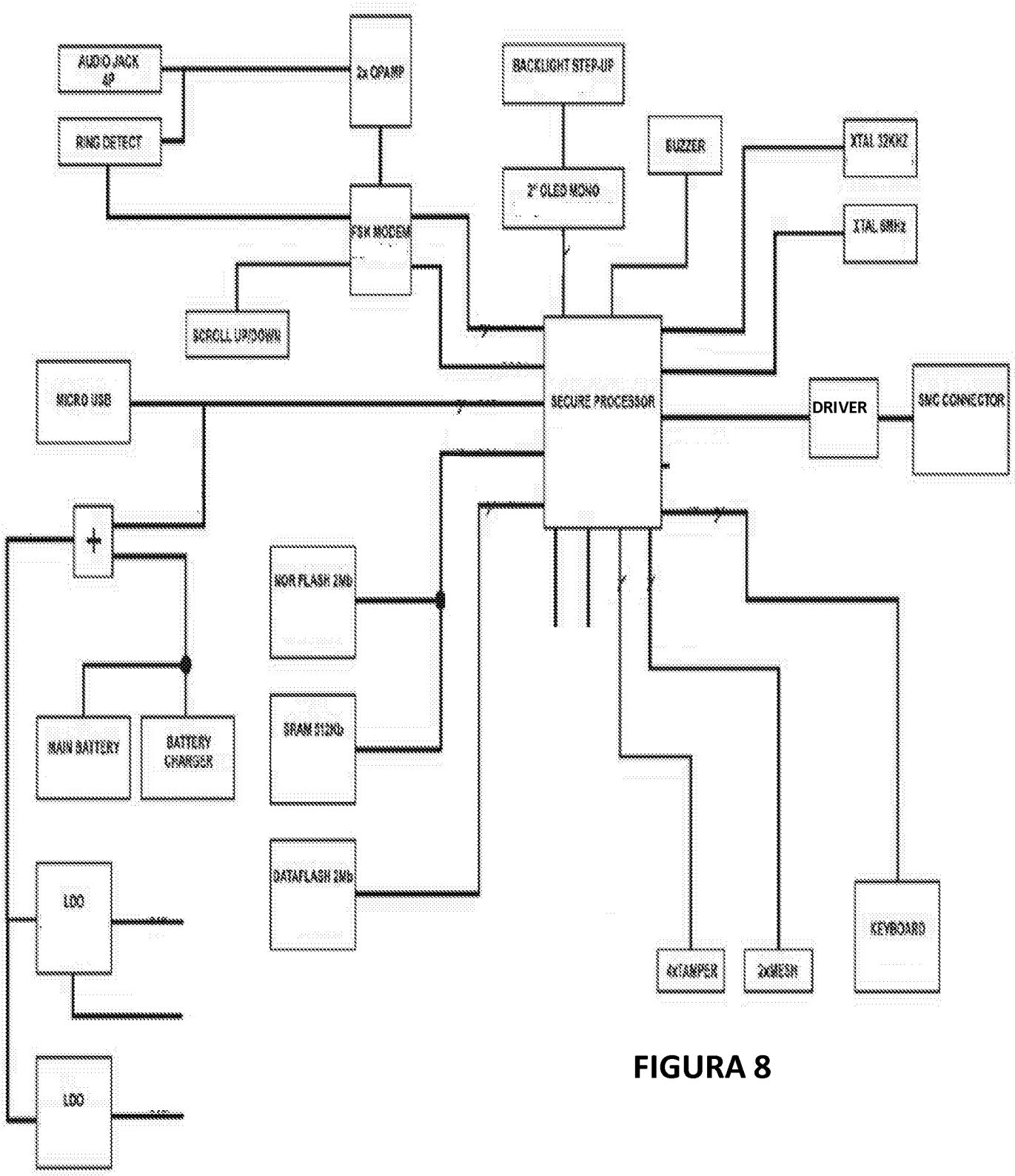
AUDIO JACK
2x OPAMP
BACKLIGHT STEP-UP
RING DETECT
BUZZER
XTAL 32KHZ
2" OLED MONO
FSK MODEM
XTAL 8MHz
SCROLL UP/DOWN
MICRO USB
SECURE PROCESSOR
DRIVER
SMC CONNECTOR
NOR FLASH 2MB
MAIN BATTERY
BATTERY CHARGER
SRAM 512Kb
DATAFLASH 2Mb
LDO
LDO
KEYBOARD

FIGURA 8

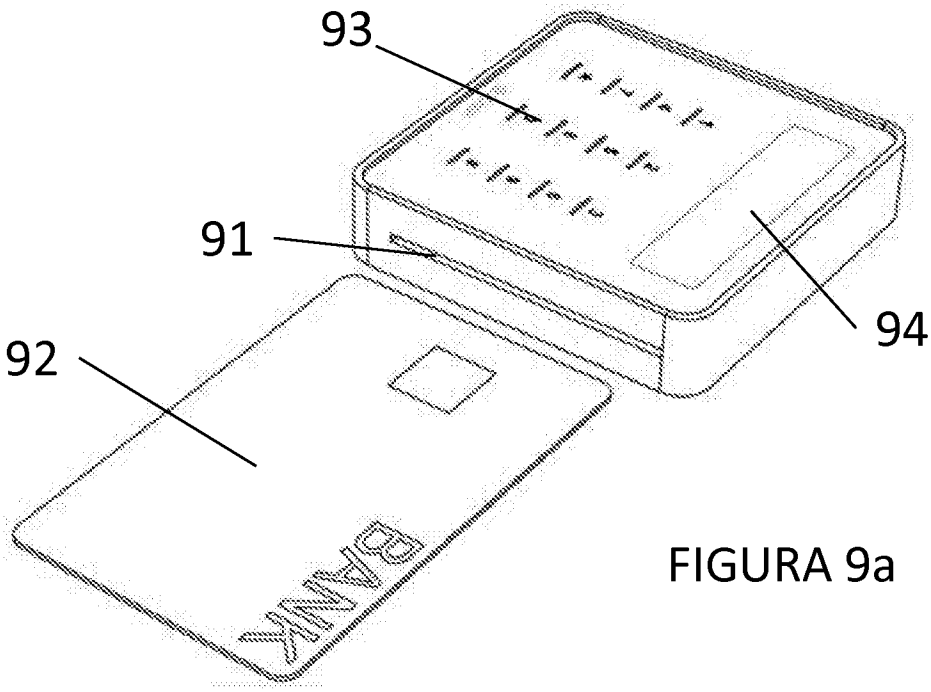

FIGURA 9a

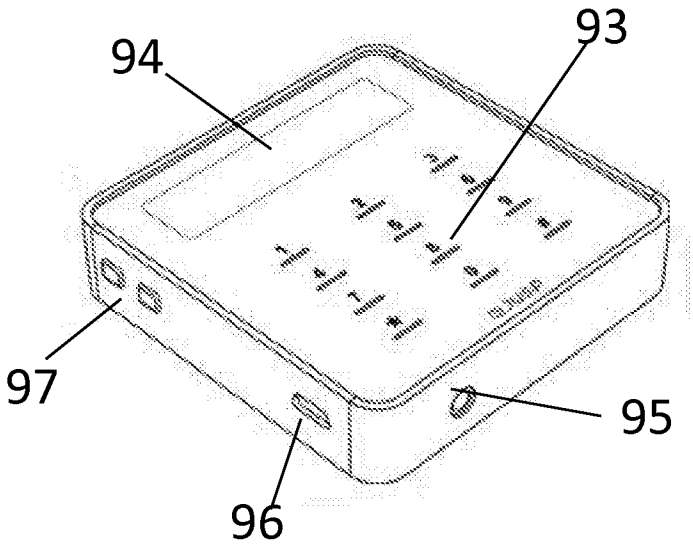

FIGURA 9b