MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA TUTELA DELLA PROPRIETA' INDUSTRIALE
UFFICIO ITALIANO BREVETTI E MARCHI

UIBM

DOMANDA NUMERO	**101995900481252**
Data Deposito	**28/11/1995**
Data Pubblicazione	**28/05/1997**

Titolo

PROCEDIMENTO DI GESTIONE DI APPARECCHIATURA TERMINALE PER ACCETTAZIONE NON IN TEMPO REALE DI CARTE MAGNETICHE E SIMILI PARTICOLARMENTE PER IMPIEGO IN AUTOPUBBLICHE E APPARECCHIATURA TERMINALE GESTIBILE TRAMITE TALE PROCEDIMENTO

MODIANO & ASSOCIATI

MODIANO Andrea,

residente a Bruxelles,

MI 95 A 24 80

di nazionalità italiana.

* * * * * * *

28 NOV. 1995

DESCRIZIONE

Il presente trovato riguarda un'apparecchiatura terminale e un procedimento di gestione di apparecchiatura terminale per l'accettazione non in tempo reale di carte magnetiche e simili, particolarmente per impiego in autopubbliche.

Le forme di pagamento tramite carte di credito, carte bancarie, di tipo magnetico, e le cosiddette "carte intelligenti" (smart card) e simili sono attualmente in forte espansione sia per il numero di utenti che ricorrono ad esse, sia per il campo di impiego sempre più vasto a loro disposizione.

La comodità data dalla possibilità di non utilizzare denaro contante per un pagamento è divenuta un'esigenza irrinunciabile a cui sono associati però problemi dovuti alla necessità di garantire un elevato standard di sicurezza contro contraffazioni o alterazioni da parte di terzi.

I pagamenti a mezzo di carte di credito e simili possono, come si è detto, essere facilmente alterati da persone malintenzionate e per contrastare questo fenomeno le banche o le compagnie distributrici di tali carte hanno messo a punto procedure e controlli che tollerano perdite ritenute statisticamente accettabili.

Le procedure di controllo per l'accettazione di pagamenti a mezzi di di tali carte possono generalmente essere classificate secondo due catego-

GIODIANO & ASSOCIATI

rie principali: in linea (on line) e fuori linea (off line).

Nelle procedure in linea i controlli avvengono in tempo reale, al momento dell'inserimento della carta di credito in un terminale elettronico collegato in una rete telematica. In questo modo il pagamento è accettato o respinto in tempo reale.

Diversamente, nelle procedure fuori linea è sempre richiesta la presenza di una persona che verifichi l'identità dell'intestatario della carta di credito. Generalmente una chiamata telefonica alla banca responsabile fornisce rapidamente la conferma dell'accettazione di pagamento o del rifiuto. Solitamente la registrazione dei dati della carta di credito viene effettuata manualmente.

Questo tipo di procedura fuori linea è ad esempio utilizzabile nel caso di autopubbliche per l'utilizzo di carte di credito e simili per il pagamento di una corsa da parte del cliente.

Infatti, in un'autopubblica un terminale elettronico non può essere sempre facilmente ed economicamente collegato in rete in tempo reale. Basti pensare alla necessità di avere a disposizione un apparecchio telefonico a bordo dell'autopubblica per il collegamento in tempo reale alla rete telematica.

Un inconveniente dell'utilizzo di procedure di verifica fuori linea di una transazione effettuata a mezzo di terminale elettronico non collegato in tempo reale ad una rete telematica è che non sono offerte garanzie di sicurezza paragonabili a quelle fornite da un terminale collegato in rete.

Questo è dovuto al fatto che i dati relativi alla transazione effet-

ASSOCIATI MODIANO

tuata rimangono scritti nella memoria del terminale stesso e sono quindi suscettibili di manomissioni.

Compito principale del presente trovato è quindi quello di realizzare un procedimento di gestione di terminale per l'accettazione non in tempo reale di carte magnetiche e simili che offra garanzie di segretezza e sicurezza pari a quelle offerte da un'accettazione effettuata in tempo reale.

Nell'ambito di questo compito uno scopo del presente trovato è quello di realizzare un procedimento di gestione di terminale per l'accettazione non in tempo reale di carte magnetiche e simili che sia di facile implementazione.

Un altro scopo del presente trovato è quello di realizzare un'apparecchiatura per la realizzazione di detto procedimento di gestione di terminale per accettazione non in tempo reale di carte magnetiche e simili.

Non ultimo scopo del presente trovato è quello di realizzare un procedimento e un'apparecchiatura che risultino di elevata affidabilità, di relativamente facile realizzazione e a costi competitivi.

Questo compito, nonchè questi e altri scopi che meglio appariranno in seguito, sono raggiunti da un procedimento di gestione di terminale per accettazione non in tempo reale di carte magnetiche e simili, particolarmente per impiego in autopubbliche, comprendente le seguenti fasi:

-riconoscimento dell'apparecchiatura terminale da parte dell'elaboratore centrale, detto elaboratore centrale essendo atto ad effettuare il collegamento con la sede di rilascio di dette carte magnetiche;

-lettura della carta magnetica con cui l'utente intende effettuare la transazione;

ASSOCIATI MODIANO

-memorizzazione dei dati relativi alla carta e alla transazione in mezzi di memoria permanente di detto terminale;

-trasmissione non in tempo reale di detti dati, mediante una chiave crittografica, a detto elaboratore centrale;

caratterizzato dal fatto di comprendere l'ulteriore fase che consiste nel generare, all'installazione di detta apparecchiatura terminale e internamente ad essa, un'ulteriore chiave crittografica, detta ulteriore chiave crittografica essendo atta a proteggere la registrazione di detti dati all'atto della scrittura di detti dati nei mezzi di memoria permanente di detta apparecchiatura terminale.

Ulteriori caratteristiche e vantaggi del trovato risulteranno maggiormente da una forma di realizzazione preferita, ma non esclusiva, del procedimento e dell'apparecchiatura secondo il trovato, illustrata a titolo indicativo e non limitativo negli uniti disegni, in cui:

la Fig. 1 è uno schema a blocchi dell'apparecchiatura secondo il trovato;

la Fig. 2 è un diagramma di flusso delle fasi del procedimento secondo il trovato; e

la Fig. 3 è un diagramma di flusso particolareggiato di una delle fasi mostrate nella Fig. 2.

Con riferimento alla Fig. 1, l'apparecchiatura secondo il trovato, generalmente denominata terminale, comprende mezzi di lettura di carte magnetiche 1, mezzi di lettura di carte "intelligenti" (smart card) 2, mezzi di immissione di dati vantaggiosamente comprendenti una tastiera 3, mezzi di memoria ad accesso casuale (RAM), opportunamente costituiti da una me-

ASSOCIATI MODIANO

moria RAM 4 di tipo flash atta a memorizzare i dati relativi alla carta magnetica o intelligente rilevata e alla transazione in corso, e mezzi logici e di memoria di sola lettura, vantaggiosamente costituiti da una sezione logica e da una EPROM, globalmente indicati con il numero di riferimento 5 e atti rispettivamente a controllare le periferiche dell'apparecchiatura e a memorizzare il programma di gestione del terminale di accettazione di carte magnetiche o intelligenti.

La memoria flash RAM 4 viene istantaneamente cancellata in caso di manomissione del terminale.

Mezzi di stampa 6, opportunamente costituiti da una stampante, provvedono alla stampa della ricevuta della transazione memorizzata nella memoria flash RAM 4.

Mezzi di modulazione/demodulazione 7 consentono l'accesso del terminale alla rete telematica. Tali mezzi di modulazione/demodulazione possono non essere presenti direttamente all'interno del terminale collocato sull'autopubblica in quanto l'accesso alla rete telematica è previsto che avvenga non in tempo reale, ma ad esempio al termine di una giornata lavorativa. I mezzi di modulazione/demodulazione 7 sono collegati ai mezzi di memoria di sola lettura 5 tramite una linea ausiliaria 8.

I mezzi di immissione di dati 3 sono invece collegati ai mezzi di memoria ad accesso casuale 4 tramite una linea seriale 9.

I mezzi di memoria di sola lettura 5 controllano i mezzi di lettura di carte magnetiche 1 e di carte intelligenti 2, i mezzi di modulazione/demodulazione 7, i mezzi di immissione di dati 3 e la flash RAM 4.

Infine, l'apparecchiatura secondo il trovato comprende mezzi di vi-

ASSOCIATI MODIANO

sualizzazione 10 atti a costituire l'interfaccia con l'utente.

Con riferimento alle Fig. 2 e 3, il procedimento secondo il trovato di gestione dell'apparecchiatura terminale sopra descritta per l'accettazione di carte magnetiche e simili, non in tempo reale, è come segue.

In primo luogo, si ha la fase di inizio 20 a cui segue una fase 30 di inizializzazione e generazione interna di una prima chiave crittografica.

questa prima chiave crittografica, generata ad esempio mediante un numero casuale, è impiegata per proteggere da possibili alterazioni i dati relativi alle carte magnetiche utilizzate e alle singole transazioni, all'atto della scrittura di tali dati nella memoria flash RAM 4 dell'apparecchiatura terminale precedentemente descritta.

Segue quindi una fase 40 di verifica in cui viene valutato se il terminale è già conosciuto all'elaboratore centrale (server), non mostrato nelle figure, la cui funzione è quella di collegamento e scambio di dati con la sede interessata che cura il rilascio della carta magnetica, al fine di effettuare una procedura non in tempo reale di verifica e di informazione della transazione effettuata da un utente.

Se il terminale non è già noto all'elaboratore centrale, viene eseguita una fase 50 in cui è effettuata una chiamata telefonica con inserzione manuale, mediante la tastiera 3, del numero di identificazione del terminale in questione.

Alla fase 50 segue una fase 60 di instaurazione della procedura di comunicazione, mediante il modulatore/demodulatore 7, con l'elaboratore centrale, di trasmissione del numero di identificazione e di conferma delle chiavi crittografiche, nonchè di accettazione del terminale. Le chiavi

ASSOCIATI MODIANO

crittografiche consistono in una prima e in una seconda chiave. La seconda chiave crittografica, che va ad aggiungersi alla prima generata alla fase 30, viene ricevuta dall'elaboratore centrale al primo collegamento via modulatore/demodulatore 7 con il terminale.

Segue quindi una fase 65 di verifica di correttezza. Nel caso in cui la verifica dia esito positivo, l'elaborazione prosegue alla fase 70 di scrittura dei dati nella flash RAM, altrimenti si ritorna alla fase iniziale 20.

Ritornando alla fase 40, se il terminale è già noto all'elaboratore centrale, si passa alla fase 90 di visualizzazione, tramite i mezzi di visualizzazione 10, delle opzioni disponibili per l'utente.

Quindi, alla fase 100, viene verificato se l'utente è a bordo dell'autopubblica. Se la risposta a questa domanda è negativa l'elaborazione salta ad un sottoprogramma 110 responsabile dello scarico dei dati relativi alle carte di credito e alle transazioni effettuate nel corso della giornata lavorativa nell'elaboratore centrale.

Altrimenti, se l'utente è effettivamente a bordo di un'autopubblica, si passa alla fase 120 di prova dell'apparecchiatura terminale e di conferma.

La fase seguente 125 attende il risultato della prova.

Se il risultato è negativo si ha, fase 130, la generazione di un messaggio di errore.

Altrimenti, fase 140, viene proposto, tramite sempre i mezzi di visualizzazione 10, di inserire manualmente, mediante la tastiera 3, il prezzo totale della corsa sull'autopubblica e l'eventuale mancia.

ASSOCIATI MODIANO

Quindi, alla fase 150 viene effettuata la lettura della carta magnetica, mediante il lettore di carte magnetiche 1 o il lettore di carte intelligenti 2.

La fase 160 è una fase di attesa di conferma. Nel caso in cui non si abbia conferma, si passa alla fase 170 dove viene verificato se la lettura della carta magnetica è stata eseguita almeno più di cinque volte consecutive. Nel caso in cui ciò sia avvenuto si ha, fase 180, la visualizzazione di un messaggio di errore, la cancellazione dell'operazione in corso, e il ritorno alla fase iniziale 20; altrimenti, in caso di risposta negativa, l'elaborazione ritorna alla fase 150 di lettura della carta magnetica.

Ritornando alla fase 160, se la risposta alla richiesta di conferma è positiva, si passa alla fase 190 di esecuzione di procedure di verifica del numero della carta magnetica letta. Queste procedure possono consistere ad esempio nell'esecuzione di un algoritmo noto di verifica del numero della carta magnetica, denominato modulo 10.

L'elaborazione passa quindi alla fase 200 di attesa di conferma a cui segue, in caso positivo, la fase 220 di stampa, mediante la stampante 6, della ricevuta della transazione effettuata e di registrazione della transazione crittografata, mediante la prima chiave crittografica generata alla fase 30, nella memoria flash RAM 4 dell'apparecchiatura terminale. A questo segue poi il ritorno alla fase iniziale 20.

Invece, nel caso in cui non si abbia conferma di correttezza alla fase 200, si passa alla fase 210 di visualizzazione di un messaggio di errore di lettura della carta magnetica e di cancellazione dell'operazione in corso. A questa fase segue quindi il ritorno alla fase iniziale 20.

ASSOCIATI MODIANO

Facendo riferimento ora alla Fig. 3, verrà descritta in dettaglio la procedura innescata alla fase 110 che prevede lo scarico dei dati già precedentemente memorizzati nella flash RAM 4 dell'apparecchiatura terminale, nell'elaboratore centrale per il successivo collegamento con la centrale operativa della sede di rilascio della carta magnetica letta.

Tale procedura ha inizio con la fase 230 di visualizzazione delle opzioni per la chiamata telefonica di collegamento del terminale, tramite rete telematica, all'elaboratore centrale, e di trasmissione dei dati crittografati mediante la prima chiave crittografica.

Segue quindi la fase 240 in cui viene verificato se la chiamata telefonica è manuale o meno.

Se la risposta è positiva si passa alla fase 350 di procedura di chiamata manuale a cui segue la fase 360 di richiesta di memorizzazione di tale procedura.

Se la risposta alla fase 360 è positiva, si passa alla fase 370 di memorizzazione permanente da cui si salta alla fase 250 di procedura di chiamata automatica.

Se invece la risposta alla fase 360 è negativa si passa direttamente alla fase 250.

Dalla fase 240, in caso di risposta negativa, si passa quindi alla fase 250 di procedura di chiamata telefonica automatica.

Alla fase 260 viene verificato se si desidera effettuare tale procedura automatica o meno.

Se la risposta è negativa, si passa alla fase 330 dove viene verificato se il numero di richieste di chiamata automatica è maggiore di 3: se

ASSOCIATI MODIANO

lo è si ritorna alla fase iniziale 110 della procedura, altrimenti si visualizza, fase 340, un messaggio di errore e si torna alla fase iniziale generale 20, uscendo dalla procedura di scarico di dati all'elaboratore centrale.

Invece, alla fase 260, se la domanda ha una risposta positiva, si passa alla procedura di identificazione del terminale e di trasmissione di dati che arriva alla fase di verifica 280 da cui, se la risposta è positiva, si passa alla visualizzazione, fase 290, di un messaggio di congedo e quindi si esce dalla procedura di scarico di dati per tornare alla fase iniziale generale 20; altrimenti, in caso di risposta negativa si passa ad una nuova fase di verifica 310 a cui fa seguito, in caso di risposta positiva, il passaggio alla suddetta fase 320, e in caso di risposta negativa il ritorno alla fase 270.

Si è in pratica constatato come l'apparecchiatura e il procedimento secondo il trovato assolvano pienamente il compito prefissato in quanto consentono di effettuare transazioni a mezzo di carte di credito e simili, ad esempio su autopubbliche, non in tempo reale, garantendo uno standard di segretezza e sicurezza pari a quello fornito dalle procedure in linea mediante collegamento del terminale ad una rete telematica.

La possibilità offerta dal presente trovato di crittografare i dati relativi alla carta di credito al momento stesso del loro rilevamento e successiva memorizzazione nella memoria del terminale rende infatti immediatamente inaccessibili i dati garantendo quindi un elevato standard di sicurezza.

In particolare la presenza di due distinte chiavi crittografiche, di

ASSOCIATI MODIANO

cui la prima è generata automaticamente, internamente al momento di installazione del terminale fornisce una doppia protezione ai dati relativi alla carta magnetica e alla transazione effettuata.

Il dispositivo così concepito è suscettibile di numerose modifiche e varianti, tutte rientranti nell'ambito del concetto inventivo; inoltre tutti i dettagli potranno essere sostituiti da altri elementi tecnicamente equivalenti.

In pratica i materiali impiegati, purchè compatibili con l'uso specifico, nonchè le dimensioni, potranno essere qualsiasi secondo le esigenze e lo stato della tecnica.

* * * * * *

MODIANO & ASSOCIATI

RIVENDICAZIONI

1. Procedimento di gestione di apparecchiatura terminale per accettazione non in tempo reale di carte magnetiche e simili, particolarmente per impiego in autopubbliche, comprendente le seguenti fasi:

-riconoscimento dell'apparecchiatura terminale da parte dell'elaboratore centrale, detto elaboratore centrale essendo atto ad effettuare il collegamento con la sede di rilascio di dette carte magnetiche;

-lettura della carta magnetica con cui l'utente intende effettuare la transazione;

-memorizzazione dei dati relativi alla carta e alla transazione in mezzi di memoria permanente di detta apparecchiatura terminale;

-trasmissione non in tempo reale di detti dati, mediante una chiave crittografica, a detto elaboratore centrale;

caratterizzato dal fatto di comprendere l'ulteriore fase che consiste nel generare, all'installazione di detta apparecchiatura terminale e internamente ad essa, un'ulteriore chiave crittografica, detta ulteriore chiave crittografica essendo atta a proteggere la registrazione di detti dati all'atto della scrittura di detti dati nei mezzi di memoria permanente di detta apparecchiatura terminale.

2. Procedimento secondo la rivendicazione 1, caratterizzato dal fatto di comprendere una fase che consiste nel verificare se l'apparecchiatura terminale è o meno sull'autopubblica e ad eseguire, in caso negativo la trasmissione di detti dati a detto elaboratore centrale oppure ad eseguire, in caso positivo, una fase di inserimento manuale del prezzo della corsa che l'utente deve pagare.

MODIANO & ASSOCIATI

3. Procedimento secondo la rivendicazione 1, caratterizzato dal fatto che detta fase di lettura della carta magnetica, in caso di mancata lettura di detta carta magnetica, è eseguita un numero predeterminato di volte prima dell'emissione di un messaggio di errore.

4. Procedimento secondo la rivendicazione 1, caratterizzato dal fatto che successivamente a detta fase di lettura di dette carte magnetiche viene eseguita una fase di verifica dell'autenticità di dette carte magnetiche.

5. Procedimento secondo la rivendicazione 4, caratterizzato dal fatto che detta fase di verifica è seguita, in caso positivo, dalla registrazione di detti dati letti da detta carta magnetica e relativi alla transazione effettuata, crittografati mediante detta ulteriore chiave crittografica, in detti mezzi di memoria permanente di detta apparecchiatura terminale.

6. Procedimento secondo la rivendicazione 1, caratterizzato dal fatto che detta fase di trasmissione di detti dati all'elaboratore centrale è preceduta da una fase di richiesta della modalità di chiamata telefonica per il collegamento con detto elaboratore, detta modalità essendo manuale o automatica.

7. Procedimento secondo la rivendicazione 1, caratterizzato dal fatto che detti dati memorizzatati in detti mezzi di memoria permanente di detta apparecchiatura terminale vengono cancellati automaticamente in caso di manomissione di detto terminale.

8. Procedimento secondo una o più delle rivendicazioni precedenti, caratterizzato dal fatto di comprendere una o più delle caratteristiche

MODIANO & ASSOCIATI

descritte e/o illustrate.

9. Apparecchiatura terminale per la realizzazione del procedimento definito nelle precedenti rivendicazioni, caratterizzata dal fatto di comprendere mezzi di lettura di carte magnetiche, mezzi di lettura di carte intelligenti, mezzi di immissione di dati, mezzi di memoria permanente atti a memorizzare i dati relativi a dette carte magnetiche e/o intelligenti e alle transazioni effettuate, e mezzi di memoria permanente di sola lettura atti a memorizzare le fasi del procedimento di gestione di detta apparecchiatura.

10. Apparecchiatura terminale secondo la rivendicazione 9, caratterizzata dal fatto di comprendere mezzi di modulazione/demodulazione atti a collegare detta apparecchiatura ad un elaboratore centrale preposto al collegamento con la sede di rilascio di dette carte magnetiche.

11. Apparecchiatura terminale secondo la rivendicazione 10, caratterizzata dal fatto che detti mezzi di modulazione/demodulazione sono interni a detta apparecchiatura.

12. Apparecchiatura terminale secondo la rivendicazione 10, caratterizzata dal fatto che detti mezzi di modulazione/demodulazione sono esterni a detta apparecchiatura.

13. Apparecchiatura terminale secondo la rivendicazione 9, caratterizzata dal fatto che detti mezzi di memoria permanente comprendono mezzi di memoria ad accesso casuale.

14. Apparecchiatura terminale secondo la rivendicazione 13, caratterizzata dal fatto che detti mezzi di memoria ad accesso casuale comprendono una flash RAM.

15. Apparecchiatura terminale secondo la rivendicazione 9, caratterizzata dal fatto che detti mezzi di memoria permanente di sola lettura comprendono una EPROM.

16. Apparecchiatura terminale secondo la rivendicazione 9, caratterizzata dal fatto di comprendere mezzi di stampa atti a stampare la ricevuta della transazione crittografata in detti mezzi di memoria permanente.

17. Apparecchiatura terminale secondo la rivendicazione 9, caratterizzata dal fatto che detti mezzi di immissione di dati comprendono una tastiera.

18. Apparecchiatura terminale secondo una o più delle rivendicazioni precedenti, caratterizzata dal fatto di comprendere una o più delle caratteristiche descritte e/o illustrate.

Il Mandatario:

- Dr. Ing. Guido MODIANO -



MI 95 A 2480

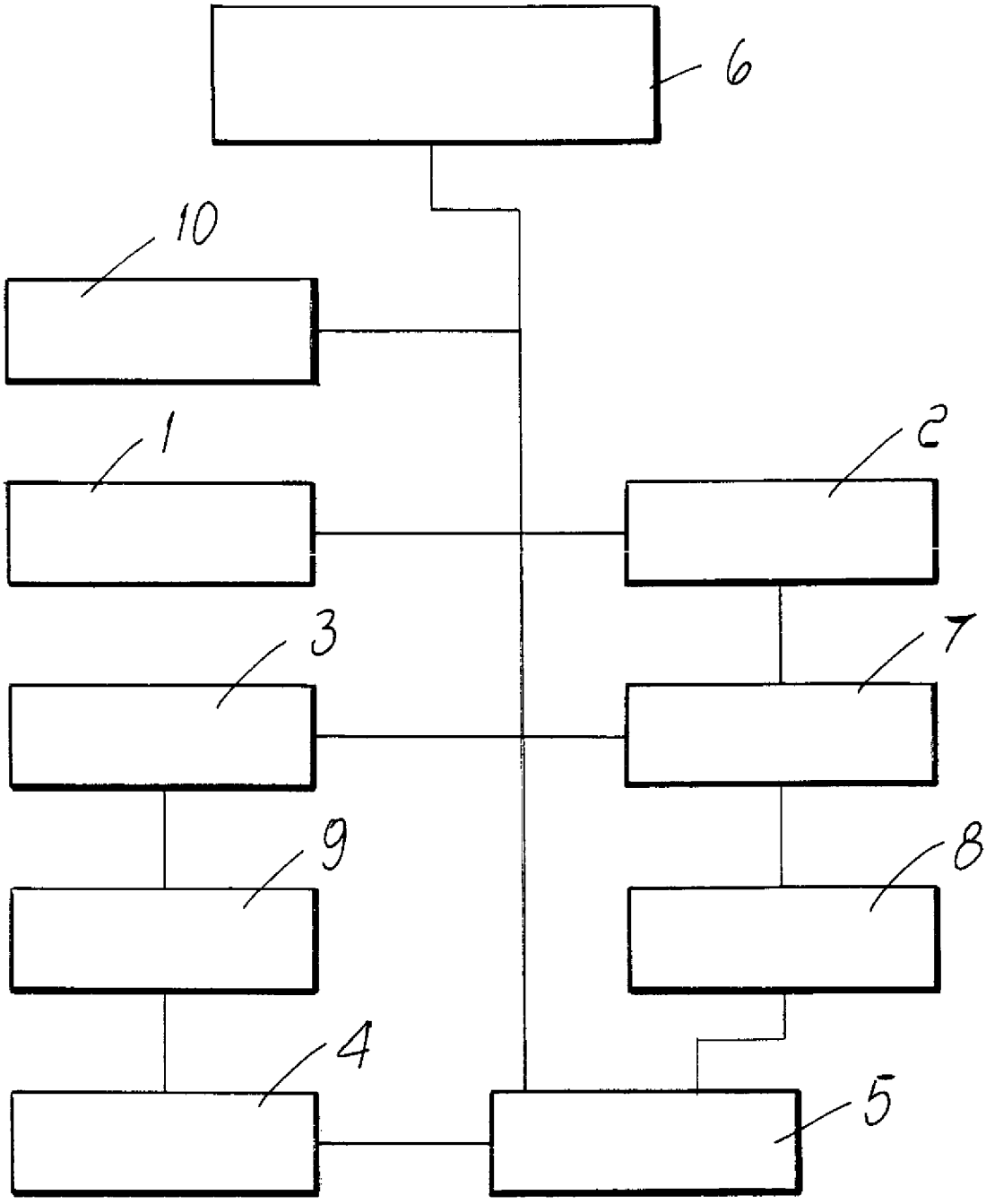
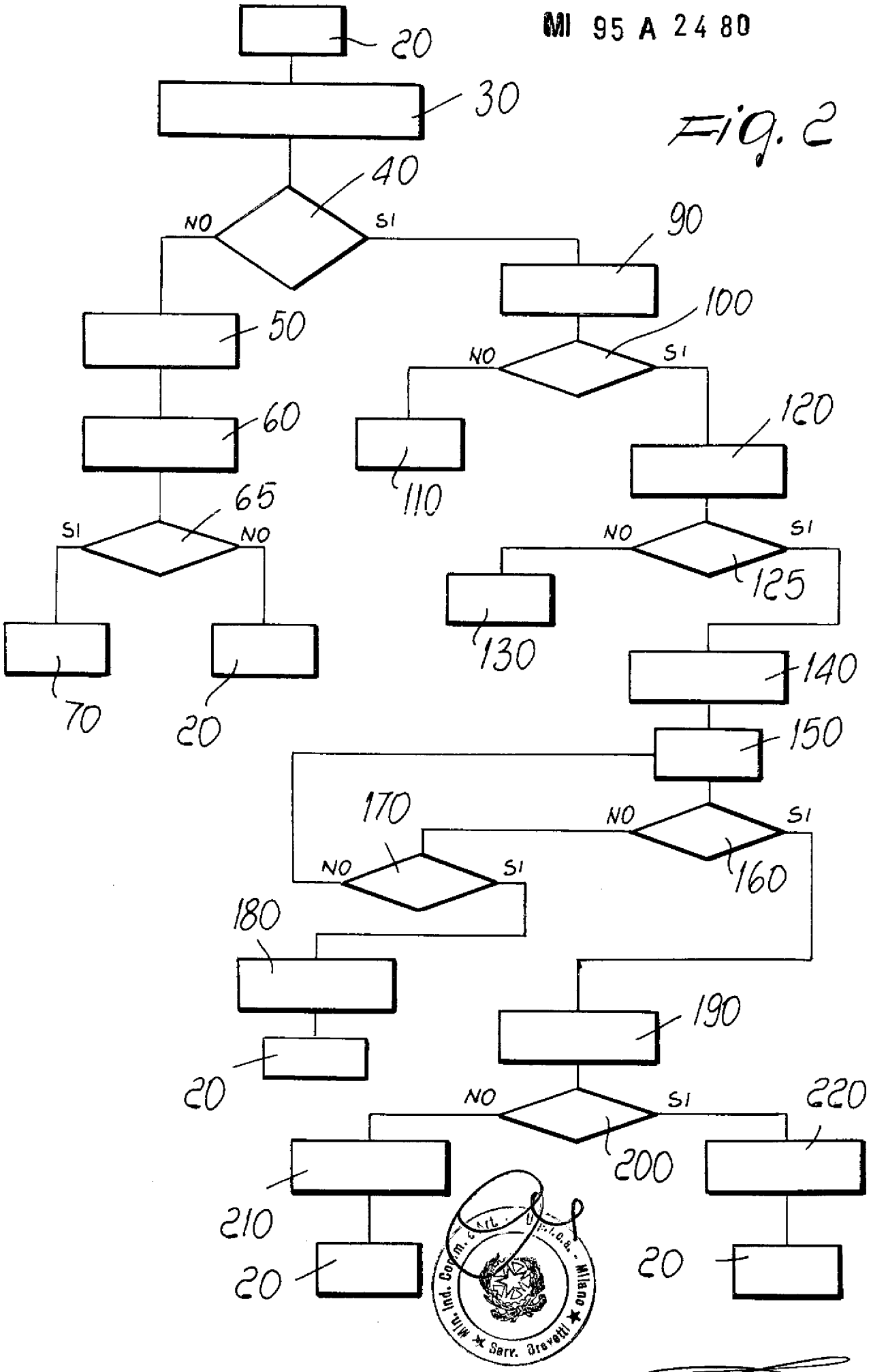


Fig. 1

MI 95 A 2480

Fig. 2



MI 95 A 2480

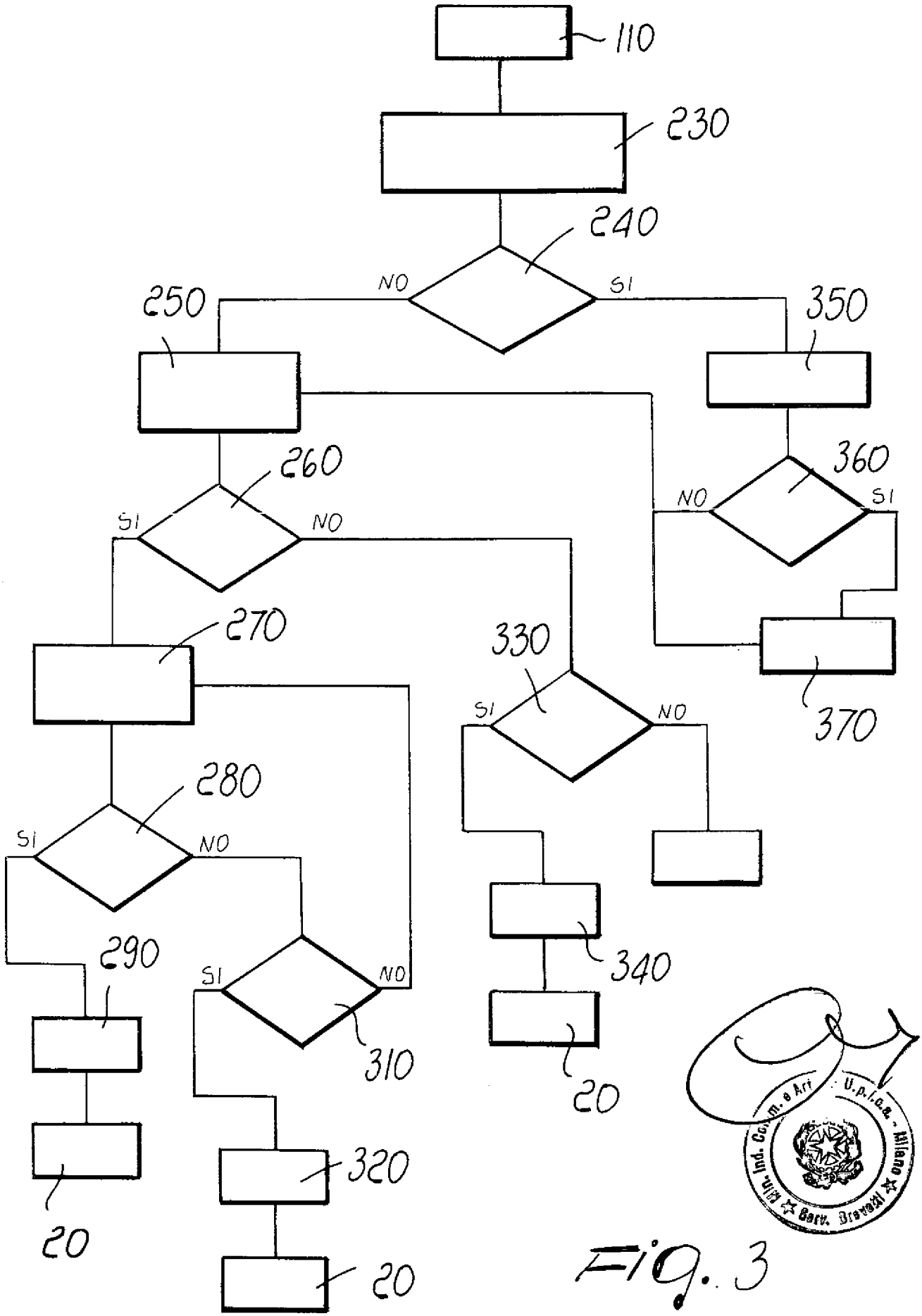


Fig. 3