



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

DOMANDA NUMERO	102007901525211
Data Deposito	23/05/2007
Data Pubblicazione	23/11/2008

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	Q		

Titolo

SISTEMA E PROCEDIMENTO INFORMATICO PER LA VERIFICA E IL MONITORAGGIO DELLA CIRCOLAZIONE DI PRODOTTI O SERVIZI
--

PT/mr/2128prov.

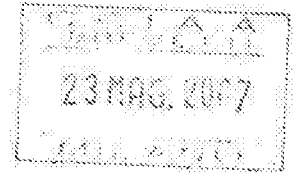
- 2 -

DESCRIZIONE DI BREVETTO PER INVENZIONE

A nome:

CERTILOGO S.R.L.

con sede in: Piazza IV Novembre N.6 – 20124 MILANO



Depositata il:

col n.: MI2007 A 0 0 1 0 4 2

DESCRIZIONE

L'invenzione si riferisce a un procedimento per l'acquisizione, l'analisi, l'interpretazione e la fornitura di dati relativi a beni o servizi ai quali è stato associato un codice identificativo alfanumerico univoco al fine di fornire alle imprese uno strumento capace di monitorare la circolazione dei propri prodotti (ivi inclusa la circolazione su mercati paralleli), eventuali frodi commerciali (fra cui contraffazione, furto, gli abusi legati allo sfruttamento indebito delle licenze ecc.) ed al tempo stesso capace di veicolare attraverso canali bidirezionali ed interattivi informazioni da e verso la rete ispettiva aziendale, la filiera distributiva, le autorità di controllo, i consumatori e/o altri operatori autorizzati in genere.

Non sono noti procedimenti o sistemi che assolvano a tutti questi scopi, in particolare non si conoscono metodi che attraverso l'interazione degli utenti con un sistema informatico siano in grado di reperire informazioni puntuali sull'autenticità, la tracciabilità e la soddisfazione dei clienti riguardo a un prodotto, e a ricavare da tali informazioni elementi utili ad una serie di operatori autorizzati.

Sono noti invece sistemi che utilizzano codici o chip allegati ai

prodotti che sostengono di poter di garantire l'autenticità del bene a fronte di una verifica da parte dell'acquirente.

Ad esempio la domanda di brevetto US2004019791 pubblicata il 29/1/2004 descrive un metodo in cui sono generati dei codici in modo casuale che vengono associati agli oggetti da vendere. Detti codici vengono memorizzati in un database e l'eventuale richiesta di autenticazione di un codice da parte di un cliente restituisce informazioni relative all'oggetto associato.

Sono altresì noti altri sistemi in cui i codici di autenticazione sono memorizzati su un chip non direttamente accessibili al cliente, ma solo a chi è dotato di appositi strumenti elettronici, optoelettronici ecc.; una volta recuperato detto codice si può procedere alla validazione dello stesso attraverso il confronto con i dati memorizzati in un data base locale oppure remoto.

Un tipico modello di funzionamento di questi sistemi prevede che all'invio di una richiesta di informazioni — tramite un codice — riguardo a un prodotto da parte di un utente, il sistema risponda in modo unidirezionale: ossia inviando le informazioni richieste, senza procedere ad alcuna ulteriore elaborazione o ricerca di informazioni.

I limiti che presentano detti sistemi sono molteplici: la sola verifica che un codice appartenga a un data base non è necessariamente indice di autenticità del prodotto; un codice originale, e quindi memorizzato nella banca dati, infatti può essere copiato e applicato a uno o più beni da parte di un produttore disonesto, un utente che richiedesse la validazione dello stesso

codice riceverebbe in ogni caso una risposta affermativa e quindi avrebbe l'illusione di aver acquistato un prodotto originale.

L'utilizzo di chip o di altri sistemi non direttamente accessibili per la validazione di un prodotto poi non è esente da rischi: un produttore disonesto potrebbe imitare gli stessi chip, oltre al prodotto in sé, inoltre non è certamente ipotizzabile che il cliente comune sia dotato dell'apparecchiatura necessaria per la raccolta delle informazioni memorizzate sul supporto elettronico. La stessa operazione di verifica sarebbe quindi affidata al venditore al dettaglio, che dovrebbe controllare tutti i prodotti uno per uno, o più verosimilmente a campione, con conseguente perdita di tempo e aumento dei costi di gestione, e senza alcuna garanzia per il cliente finale, dovendo lo stesso affidarsi ciecamente al negoziante.

Pertanto con tali sistemi risulta estremamente difficile per le aziende reperire informazioni affidabili sull'eventuale contraffazione e vendita dei propri beni: un'eventuale validazione di un codice identificativo da parte di un cliente può infatti dipendere dalla contraffazione del codice stesso, e quindi del prodotto.

Scopo della presente invenzione è quello di proteggere un sistema e un procedimento informatico che consenta a un'azienda, o ad altri enti quali forze dell'ordine, ispettori ecc., di effettuare in tempo reale sia un'analisi specifica che un'analisi statistica delle richieste di verifica dei codici identificativi associati ai prodotti, analizzando il numero di richieste su uno stesso codice, la provenienza geografica, l'istante e l'intervallo temporale tra le stesse, per permettere

un'elaborazione approfondita dei dati e di evidenziare le anomalie riconducibili a eventuali contraffazioni o comportamenti illeciti di produttori o venditori.

Altro scopo della presente invenzione è quello di proteggere un sistema e un procedimento informatico che, assieme all'invio all'utente di informazioni relative a un codice identificativo, quali ad esempio informazioni sulla provenienza, tracciabilità, l'uso e la manutenzione, ecc. del prodotto o del servizio ad esso associato, riceva una serie di feedback dall'utente che permettano di aggiornare le informazioni relative a detto codice identificativo presenti in un data base apposito ovvero che permettano di ottenere specifiche informazioni in caso di anomalie riscontrate in modo da individuare con i maggiori dettagli gli elementi più significativi di tali anomalie. Detto feedback è composto da informazioni quali ad esempio: l'intenzione di acquisto, la soddisfazione dell'utente, ecc. ovvero il negozio in cui si trova il prodotto o dove è stato acquistato il prodotto, eventuali difformità tra le informazioni ricevute e il prodotto oggetto di verifica ecc. ecc.

Non ultimo scopo della presente invenzione è quello di illustrare un procedimento e un sistema informatico che permetta la verifica dell'autenticità di un codice attraverso la comparazione dei dati inviati da un utente attraverso un qualsiasi mezzo di comunicazione con i dati presenti in un data base.

Questi ed altri aspetti saranno più chiari alla lettura di un modo preferito di realizzare il presente trovato, da leggere a titolo

esemplificativo e non limitativo dei più generali concetti rivendicati.

La descrizione che segue fa riferimento ai disegni allegati, in cui:

al figura 1 è una rappresentazione del flusso di informazioni tra il sistema e i vari utenti ad esso collegati

la figura 2 è una rappresentazione funzionale degli elementi che costituiscono il sistema secondo la presente invenzione

le figure 3a e 3b sono uno schema a blocchi del procedimento di verifica dell'autenticità secondo la presente invenzione.

Facendo riferimento alla figura 1, al sistema 1 sono collegati, attraverso un qualsiasi mezzo di comunicazione, almeno tre tipi di utenti: un utente anonimo 2, ad esempio un acquirente, che non ha una chiave d'accesso riservata e che può accedere a un numero limitato di informazioni, un utente autorizzato 3, ad esempio un ispettore o un agente doganale o altra persona autorizzata, dotato di chiave d'accesso che può accedere a informazioni a lui riservate e infine l'azienda 4, che può ricavare dal sistema tutte le informazioni in esso contenute.

La distinzione tra i diversi tipi di utenti e i diversi livelli di accesso implica che un acquirente possa richiedere informazioni sull'autenticità di un codice senza avere però accesso a informazioni sulle richieste effettuate da altri utenti sullo stesso codice o su codici legati a prodotti simili; per contro un ispettore sarà autorizzato a verificare le informazioni legate alla destinazione dei prodotti, alle richieste effettuate su uno o più codici per evidenziare eventuali

anomalie ecc.; infine l'azienda produttrice avrà accesso a tutte le informazioni legate ai propri prodotti, in modo tale da poter evidenziare eventuali anomalie legate a comportamenti illegali oppure pianificare strategie di mercato sulla base delle informazioni reperite dagli acquirenti.

Lo scambio di informazioni, infatti, tra acquirenti/ispettori e il sistema è bidirezionale, come evidenziato dalle frecce 5: quando il sistema 1 riceve una richiesta di verifica, ad esempio da un acquirente 2, invita lo stesso utente a specificare se è sua intenzione acquistare il prodotto o se lo ha già acquistato, il negozio in cui ha visto o acquistato il prodotto, il grado di soddisfazione ecc. Tali informazioni, oltre a creare un feedback utile per evidenziare eventuali anomalie legate a comportamenti illeciti, come verrà spiegato in seguito, serve all'azienda 4 per effettuare indagini di mercato e/o assecondare i gusti dei propri clienti.

Quando a richiedere la verifica è un utente autorizzato 3, invece, il sistema da una parte fornisce informazioni anche non fornite ad un acquirente finale, mentre dall'altra invita l'utente autorizzato a fornire informazioni particolari: per esempio la provenienza del prodotto legato al codice (se ad esempio l'utente è un ispettore doganale), la destinazione, il numero di prodotti, l'autorizzazione del trasportatore ecc.

Anche in questo caso il feedback ricevuto dall'ispettore 3 è utile per evidenziare eventuali anomalie legate a comportamenti illeciti. Inoltre se il codice identificativo viene riconosciuto come

contraffatto dal sistema 1, l'ispettore 3 può procedere in tempo reale a indagini approfondite e all'eventuale blocco del prodotto.

L'azienda 4 riceve dal sistema 1 tutte le informazioni elaborate sulla base delle richieste di verifica e delle informazioni inviate dagli utenti 2 e 3. Lo scambio bidirezionale di informazioni, schematizzato dalle frecce 5 di figura 1, ha infatti lo scopo di permettere al sistema 1 di raccogliere le informazioni legate alle preferenze, i luoghi e le modalità di acquisto dell'acquirente 2, oltre a informazioni specifiche da parte dell'ispettore 3 e ricavare anzitutto dati sui prodotti e quindi anomalie legate a frodi commerciali; tutte queste informazioni vengono poi passate, all'azienda 4 come schematizzato dalla freccia 6.

Facendo riferimento alla figura 2, il sistema 1 è composto da diversi elementi, in particolare per quanto riguarda la memorizzazione dei dati si sfruttano tre diversi data base: un data base 7, la cui funzione è quella di memorizzare i codici identificativi dei prodotti, assieme a tutte le informazioni relative agli stessi, un data base 8, la cui funzione è quella di memorizzare ogni singola attività svolta all'interno del sistema quali ad esempio configurazioni, inserimenti di dati, dati scambiati durante le operazioni di verifica, ecc. e un data base 9 di backup per il continuo e completo salvataggio delle informazioni per garantire la massima protezione dei dati.

Connessi con i tre data base sono presenti due tipi di server: un primo tipo 10, che possiamo definire col nome di Application

Server, dotato di software che gestisce e analizza i dati secondo il procedimento che verrà illustrato successivamente, e un secondo tipo 11, definito col nome di TTS Server, a cui vengono demandati compiti di generare file audio relativi alle descrizioni dei prodotti associati ai singoli codici identificativi. Questo server viene attivato ogni volta che si esegue una verifica di un codice attraverso un canale "fonico", ossia attraverso telefono o videotelefono.

Connessi con detti server, sono presenti i sistemi specializzati alla gestione della interattività associata ai diversi canali di comunicazione, ossia: dei server Web/Wap 12 per le interfacce http tramite connessione internet, dei server SMS 13 per l'interazione tramite messaggi di testo con telefoni cellulari, dei server IVR 14 per le interfacce audio telefoniche e dei server video IVR 15 per le interfacce video e audio con videotelefoni.

L'accesso a detti sistemi specializzati viene filtrato da un Firewall 16, che controlla tutti gli accessi e le abilitazioni alla richiesta o alla modifica dei dati presenti nei database. Gli accessi, sia per funzioni di inserimento che di consultazione dei dati, vengono garantiti sulla base di autorizzazioni e account configurati in funzione dei privilegi concessi. Privilegi maggiori saranno concessi agli amministratori del sistema, ai titolari dell'azienda o agli organi ispettivi, mentre ci saranno limitazioni maggiori nei confronti dei clienti, che potranno ad esempio solamente verificare l'autenticità del singolo codice identificativo.

Si può accedere al sistema attraverso un qualsiasi mezzo di

comunicazione: per esempio tramite un pc 17 connesso a internet, via telefono cellulare 18 attraverso SMS o Wap, tramite telefono 19 attraverso comandi vocali ecc.

Verrà ora descritto come viene associato un codice univoco a ogni prodotto e l'innovativo procedimento di verifica dell'autenticità dello stesso, in particolare facendo riferimento alle figure 2, 3a e 3b.

Il codice identificativo viene generato a partire da una sequenza numerica di partenza, detta sequenza numerica viene stabilita dalla ditta produttrice che associa ad ogni prodotto un numero diverso, anche sequenziale, che ad esempio identifica il lotto di produzione, l'elemento prodotto in quel lotto ecc.

Detta sequenza numerica viene poi cifrata attraverso un algoritmo matematico opportunamente sviluppato in grado di generare codici composti da svariati caratteri (ad esempio 12, 14, 16, 18 , 20 ecc.). I codici così generati non sono sequenziali e non è possibile generare un codice valido se non si è a conoscenza dell'algoritmo. Il numero elevato di caratteri permette la generazione di oltre un miliardo di codici diversi, rendendo possibile associare un codice univoco ad ogni prodotto che si intende proteggere anche per produzioni di grande massa.

Una volta associato il codice identificativo al prodotto, si memorizza il codice nel database 1 e, assieme ad esso, vengono memorizzate tutte le informazioni relative al prodotto stesso: per esempio ditta produttrice, tracciabilità, eventuali dati del venditore, eventuale manuale d'uso ecc. . Lo stesso codice viene unito o

associato al prodotto, per esempio stampato sul prodotto o su un'etichetta o un altro supporto utilizzabile.

Quando un acquirente intende verificare un codice identificativo, il sistema si attiva ricavando automaticamente per prima cosa, in relazione allo specifico canale utilizzato (ossia connessione internet, sms, telefono ecc.) alcune informazioni base tra cui per esempio la possibile nazionalità dell'acquirente, la geolocalizzazione dello stesso e l'istante temporale in cui ha inviato la richiesta di verifica. Tali informazioni vengono memorizzate nel data base 8 e associate al codice identificativo.

Il sistema inizia chiedendo all'acquirente di indicare il codice identificativo del prodotto. Se il codice immesso corrisponde a un codice abilitato ed esistente nel data base 7 il sistema chiede all'acquirente se ha già acquistato, oppure se ha intenzione o meno di acquistare il prodotto, memorizzando la risposta nel data base 8.

Successivamente il sistema comunica la descrizione del prodotto associata al codice identificativo e quindi richiede all'acquirente se la descrizione corrisponde al prodotto. Se la risposta è affermativa il sistema prosegue fornendo ogni informazione legata al prodotto stesso (per esempio origine, qualità, manutenzione e quant'altro anche di tipo interattivo è previsto quale interazione conseguente). Se la risposta è negativa il sistema interagisce con l'acquirente con richieste specifiche per poter ottenere dati utili alla comprensione dell'accaduto, eventualmente comunicando che il prodotto di cui si intende verificare l'autenticità non può essere

originale.

Se il codice immesso non corrisponde a nessun codice presente nel data base 7, il sistema interagisce con l'acquirente con richieste specifiche per poter ottenere dati utili alla comprensione dell'accaduto, eventualmente comunicando che il codice non risulta esistente o che il prodotto di cui si intende verificare l'autenticità è probabilmente non originale.

Può anche succedere che il codice immesso, pur esistente ed abilitato, presenti anomalie legate alle informazioni associate nel data base 7 (per esempio il codice è associato a un prodotto destinato in un'area geografica diversa dalla zona di provenienza della richiesta di verifica): in questo caso il sistema interagisce con l'acquirente per ottenere informazioni del luogo ove è presente il prodotto, pur fornendo informazioni legate all'autenticità come prima indicato. Il sistema infatti prevede che nel data base 7 possano essere memorizzate informazioni relative alla distribuzione del prodotto (tracciabilità), ossia le informazioni relative all'area o al punto vendita in cui il prodotto originale viene destinato / commercializzato.

Se si è in presenza di un codice associato a un prodotto destinato ad un'altra zona geografica rispetto alla zona di provenienza della richiesta di verifica, il sistema rileva l'anomalia: un evento simile potrebbe infatti dipendere dalla messa in commercio di prodotti con codici identificativi copiati dagli originali e venduti altrove.

Dalla prima verifica possono avverarsi successive richieste di

verifica sul medesimo codice identificativo, allora il sistema si comporta in modo diverso in relazione alla tipologia, geolocalizzazione, arco temporale ecc. delle richieste successive che vengono acquisite e interpretate come "coerenti", per esempio se il prodotto risulta successivamente acquistato dopo una verifica prima dell'acquisto e nella stessa area geografica) ovvero come "anomalie".

Per esempio se il codice immesso dal cliente, pur essendo presente nel data base 7, è stato già utilizzato per una verifica di autenticità per un prodotto di cui l'acquirente ha comunicato l'intenzione di acquisto, ma in una localizzazione geografica non corrispondente alla localizzazione precedente, il sistema rileva l'anomalia, interagisce con l'acquirente e, in base ai dati ricevuti, può direttamente informare che potrebbe essere in presenza di una contraffazione.

Similmente, se lo stesso codice è stato utilizzato in precedenza per una verifica di autenticità e il prodotto risultava essere stato venduto in occasione di detta verifica, il sistema interagisce, acquisisce ulteriori informazioni e segnala l'anomalia all'acquirente. In questo caso, infatti, il prodotto venduto è uscito dal mercato e incontrare di nuovo lo stesso codice in vendita implica che il prodotto venduto precedentemente oppure quello di cui l'acquirente chiede la verifica è contraffatto.

Un acquirente può tuttavia controllare più volte lo stesso prodotto anche dopo l'acquisto, verosimilmente tali controlli saranno

contraddistinti da alcuni elementi indicativi tipo un breve intervallo temporale, la stessa provenienza della richiesta (numero telefonico, indirizzo IP), stessa area ecc.: ad esempio una volta nel negozio e poco dopo una volta arrivato a casa col prodotto acquistato. In questo caso il sistema tiene conto del breve lasso di tempo tra una verifica e l'altra e non considera come anomala la seconda richiesta di verifica.

Nel caso il sistema evidenzi un'anomalia, il sistema prevede che vengano poste alcune domande specifiche all'acquirente in base alla tipologia dell'anomalia, per esempio lasciare i dati relativi al luogo in cui il prodotto è stato visto o acquistato.

Tutte le informazioni così raccolte vengono utilizzate per fornire all'azienda produttrice dati più precisi possibile per poter procedere alle verifiche del caso o anche tramite gli organi ispettivi su segnalazione alla stessa.

Il sistema utilizza vari parametri, in parte definiti direttamente dalla ditta produttrice in base ai propri obiettivi od esigenze, per stabilire se si è in presenza di un'anomalia.

Per esempio il sistema, oltre a analizzare la localizzazione e l'intervallo temporale tra le richieste di verifica, memorizza anche il numero di richieste relative a uno stesso codice identificativo: un numero di richieste troppo elevato, anche se non si è in presenza di anomalie geografiche o temporali, potrebbe implicare la clonazione del codice stesso. Poiché il cliente può fare una verifica anche prima di acquistare un prodotto e, a seguito della verifica, può decidere se

acquistarlo o meno, il numero di verifiche su un singolo codice non è indicativo di per sé di una possibile clonazione. E' stato quindi sviluppato un metodo che tenga conto anche delle risposte date dal cliente una volta verificato un codice. Se il cliente comunica che ha acquistato il prodotto, alla verifica da lui eseguita si assegna un peso *Pacq* maggiore, se il cliente comunica l'intenzione di acquistare il prodotto si assegna alla verifica un peso *Pint* minore, infine se la verifica non implica l'acquisto il peso *Pver* assegnato è ancora minore.

Per ogni codice si contano le verifiche effettuate, *Nacq* è il numero di volte che il codice è stato verificato in seguito a un acquisto (se non ci sono contraffazioni $Nacq=1$, perché è il solo prodotto originale ad essere stato acquistato), *Nint* è il numero di volte che il codice è stato verificato a seguito dell'intenzione di acquisto e *Nver* è il numero di volte che il codice è stato verificato senza implicare l'acquisto. Il numero di verifiche effettuate viene memorizzato nel data base 2 ed elaborato dall'Application Server 4.

Il server 4 calcola una cifra K nel seguente modo:

$$K = Nacq \times Pacq + Nint \times Pint + Nver \times Pver$$

Se K è maggiore o uguale a un valore di soglia stabilito, il sistema evidenzia il codice anomalo. I valori dei pesi *P* e della soglia vengono impostati dall'azienda produttrice o dall'amministratore del sistema per conto della stessa.

Ogni anomalia riscontrata viene evidenziata o meno all'acquirente (alcune anomalie sono di interesse esclusivo

dell'azienda produttrice, ad esempio la tracciabilità) ma in ogni caso viene comunicata in tempo reale all'azienda produttrice che può attivarsi per scoprire l'eventuale frode commerciale.

Riassumendo e facendo riferimento alle figure 3a e 3b, le operazioni eseguite per la verifica dell'autenticità di un prodotto sono le seguenti:

- generazione di un codice univoco per ogni prodotto
- stampa del codice sul prodotto ovvero su un supporto che viene unito / associato al prodotto o al servizio
- memorizzazione del codice in un data base 7, in cui assieme a detto codice vengono memorizzate tutte le informazioni utili relative al prodotto o al servizio ad esso associato
- l'invio attraverso un qualsiasi mezzo di comunicazione di un codice da verificare da parte di un acquirente o di un ispettore
- l'acquisizione automatica da parte del sistema di una serie di informazioni relative a localizzazione geografica e temporale della richiesta di verifica, al numero telefonico o all'indirizzo IP del richiedente, al numero progressivo della richiesta per detto codice e il salvataggio di dette informazioni in un data base dedicato 2 collegato sempre al codice identificativo richiesto
- la verifica della presenza del codice inviato nel data base 1 contenente i codici originali e, in caso affermativo, la richiesta di conformità del prodotto o del servizio
- la verifica di eventuali anomalie: geografiche, temporali nel numero di richieste attraverso il calcolo della cifra K ecc.

- l'interazione con chi effettua la richiesta di verifica con una serie di domande variabili al fine di acquisire informazioni, nel caso si evidenzia una qualunque anomalia

- la comunicazione dell'esito della verifica all'acquirente o all'ispettore

- la comunicazione all'azienda produttrice dell'insieme delle verifiche effettuate (comprehensive di ogni dato collegato) nonché in particolare delle anomalie riscontrate corredate delle informazioni raccolte, interpretate ed evidenziate in modo da fornire dati utili alle decisioni aziendali e agli interventi relativi.

Tutte le richieste, informazioni ecc. vengono sempre memorizzate nel data base 8, associate a ciascun codice identificativo, in modo tale da permettere all'azienda produttrice di tenere sotto controllo e verificare in qualsiasi momento lo stato delle richieste di verifica relative a tutti i prodotti e le problematiche eventualmente evidenziate..

La possibilità di eseguire verifiche e ottenere informazioni privilegiate può essere concessa anche a organi di controllo o ispettivi: tramite un account dedicato possono accedere al database 8, normalmente riservato all'azienda e in ogni caso non accessibile dall'utente comune, e procedere con l'analisi delle richieste di verifica di autenticità per risalire a possibili situazioni di frode commerciale.

Si realizza così un procedimento di verifica e monitoraggio dei prodotti il cui elemento essenziale consiste nell'utilizzare i prodotti fisici distribuiti sul mercato quale veicolo per generare delle

interrogazioni di tipo bidirezionale e interattivo con un sistema informatico finalizzato alla generazione, raccolta, analisi e interpretazione di dati idonei alla comprensione di fenomeni legati al mercato, alle frodi commerciali, nonché alle preferenze, ai gusti, ai luoghi e alle modalità di acquisto del consumatore.

RIVENDICAZIONI

1. Sistema e procedimento informatico per la verifica e il monitoraggio della circolazione dei prodotti o dei servizi di un'azienda e/o ente e di eventuali frodi commerciali caratterizzato dal fatto di attivare canali bidirezionali, attraverso i quali agli utilizzatori di detto sistema (consumatori, ispettori, dogane, aziende produttrici e/o enti) vengono sia fornite sia richieste informazioni specifiche su detti prodotti o servizi, informazioni che vengono elaborate e interpretate dal sistema per essere fornite in maniera differenziata agli stessi utilizzatori sulla base di specifiche autorizzazioni di accesso a detto sistema.

2. Sistema e procedimento informatico per la verifica e il monitoraggio della circolazione dei prodotti o dei servizi e di eventuali frodi commerciali secondo la rivendicazione precedente, caratterizzato dal fatto che vengono utilizzati i prodotti fisici o i servizi distribuiti sul mercato, ai quali viene associato un codice identificativo univoco, quale veicolo per indurre nell'acquirente o nell'ispettore l'invio della richiesta di verifica della validità del codice stesso, detta richiesta essendo veicolata attraverso un qualsiasi mezzo di comunicazione e generando una interazione con detto sistema informatico per ricavare in modo intenzionale, attraverso domande specifiche, oppure non intenzionale, attraverso il numero telefonico, l'indirizzo IP ecc., dati utili alla verifica e al monitoraggio della circolazione di detti prodotti o servizi, e della eventuale presenza di frodi commerciali.

3. Sistema e procedimento informatico per la verifica e il monitoraggio della circolazione dei prodotti o dei servizi e di eventuali frodi commerciali secondo la rivendicazione precedente, caratterizzato dal fatto che detti dati utili ricavati in modo intenzionale o non intenzionale attraverso l'interazione con detto sistema informatico, vengono memorizzati elaborati ed interpretati, per essere poi inviati in modo differenziato agli utilizzatori del sistema attraverso detti canali di comunicazione.

4. Sistema e procedimento informatico per la verifica e il monitoraggio della circolazione dei prodotti o dei servizi e di eventuali frodi commerciali secondo le rivendicazioni precedenti, caratterizzato dal fatto che è composto da un primo data base in cui sono memorizzati i codici identificativi e tutte le informazioni utili, quali ad esempio tracciabilità, filiera produttiva, qualità ecc., legati a detti beni o servizi, un sistema di server per accedere a detto database e un secondo sistema di server per gestire dette richieste di verifica dei codici identificativi, essendo inoltre presente un secondo data base in cui vengono memorizzate dette richieste di verifica e i dati ad esse relativi, detto secondo database essendo inaccessibile a terzi non autorizzati.

5. Sistema e procedimento informatico per la verifica e il monitoraggio della circolazione dei prodotti o dei servizi e di eventuali frodi commerciali secondo la rivendicazione precedente caratterizzato dal fatto che l'accesso a detto secondo data base è riservato, oltre all'azienda produttrice o all'ente che può accedere a

tutti i dati presenti in esso, ai soli utenti autorizzati, quali ispettori o organi di controllo, che, previa autenticazione, possono ottenere informazioni su un qualsiasi codice e su una qualsiasi anomalia legata a eventuali illeciti o frodi commerciali

6. Sistema e procedimento informatico per la verifica e il monitoraggio della circolazione dei prodotti o dei servizi e di eventuali frodi commerciali secondo la rivendicazione 4 caratterizzato dal fatto che un acquirente, ossia un utente non dotato di autorizzazione, può ottenere dal sistema informazioni limitate al singolo codice identificativo da lui immesso.

7. Sistema e procedimento informatico per la verifica e il monitoraggio della circolazione dei prodotti o dei servizi e di eventuali frodi commerciali secondo la rivendicazione 4, caratterizzato dal fatto che detta procedura di verifica e di monitoraggio comprende una qualsiasi combinazione delle seguenti fasi:

- generazione di un codice univoco per ogni prodotto o servizio
- stampa del codice sul prodotto ovvero su un supporto che viene unito al prodotto o al servizio
- memorizzazione del codice in detto primo data base, in cui assieme a detto codice vengono memorizzate tutte le informazioni utili relative al prodotto o al servizio ad esso associato
- l'invio attraverso un qualsiasi mezzo di comunicazione di un codice da verificare da parte di un acquirente o un ispettore
- l'acquisizione automatica da parte del sistema di una serie di informazioni relative a localizzazione geografica e temporale della

richiesta di verifica, il numero telefonico o l'indirizzo IP del richiedente, il numero progressivo della richiesta per detto codice e il salvataggio di dette informazioni in detto secondo data base dedicato e collegato al codice identificativo richiesto

- la verifica della presenza del codice inviato nel primo data base contenente i codici originali e, in caso affermativo, la richiesta di conformità del prodotto in mano al cliente o all'ispettore col prodotto o il servizio memorizzato in detto primo data base

- la verifica di eventuali anomalie geografiche, ossia tra la provenienza della richiesta e il luogo memorizzato nel primo o nel secondo data base in relazione a detto codice

- la verifica di eventuali anomalie temporali, ossia una eccessiva distanza temporale tra una verifica e la successiva per il medesimo codice

- la verifica di eventuali anomalie nel numero di richieste su uno stesso codice, ossia il verificarsi di un numero eccessivo di richieste di verifica per il medesimo codice

- l'interazione con chi effettua la richiesta di verifica con una serie di domande variabili, al fine di acquisire informazioni aggiuntive sul prodotto o sul servizio legato al codice di cui si chiede la verifica

- la comunicazione dell'esito della verifica all'acquirente o all'ispettore

- la comunicazione all'azienda produttrice dell'insieme delle verifiche effettuate, comprensive di ogni dato collegato, nonché in particolare delle eventuali anomalie riscontrate corredate delle

informazioni raccolte, interpretate ed evidenziate in modo da fornire dati utili in relazione a possibili frodi commerciali o a indagini di mercato.

8. Sistema e procedimento informatico per la verifica e il monitoraggio della circolazione dei prodotti o dei servizi e di eventuali frodi commerciali secondo la rivendicazione precedente caratterizzato dal fatto che detta combinazione può essere sia temporale, ossia implicare l'attuazione di dette fasi in un qualsiasi ordine, sia selettiva, ossia implicare l'esclusione di una o più fasi da detta procedura di verifica.

9. Sistema e procedimento informatico per la verifica e il monitoraggio della circolazione dei prodotti o dei servizi e di eventuali frodi commerciali secondo la rivendicazione 7 caratterizzato dal fatto che dette domande variabili al fine di acquisire informazioni aggiuntive sul prodotto legato al codice di cui si chiede la verifica comprendono, nel caso l'utente venga identificato come un acquirente, la richiesta dell'intenzione di procedere all'acquisto del prodotto oppure se detto prodotto è già stato acquistato, il luogo d'acquisto, la soddisfazione dell'acquirente e tutte le informazioni che l'azienda produttrice ritiene importanti per il monitoraggio dei propri prodotti.

10. Sistema e procedimento informatico per la verifica e il monitoraggio della circolazione dei prodotti o dei servizi e di eventuali frodi commerciali secondo la rivendicazione 7, caratterizzato dal fatto che dette domande variabili al fine di acquisire informazioni

aggiuntive sul prodotto legato al codice di cui si chiede la verifica comprendono, nel caso l'utente si sia autenticato come un ispettore, domande sul luogo in cui si effettua l'indagine (dogana, esercizio commerciale ecc.), provenienza del prodotto, destinazione, autorizzazioni al trasporto e/o alla vendita e tutte le informazioni che l'azienda produttrice ritiene importanti per il monitoraggio dei propri prodotti.

11. Sistema e procedimento informatico per la verifica e il monitoraggio della circolazione dei prodotti o dei servizi e di eventuali frodi commerciali secondo la rivendicazione 7, caratterizzato dal fatto che la comunicazione dell'esito della verifica, nel caso l'utente si sia autenticato come un ispettore, comprende la comunicazione dettagliata delle eventuali anomalie riscontrate in relazione al codice verificato.

12. Sistema e procedimento informatico per la verifica e il monitoraggio della circolazione dei prodotti o dei servizi e di eventuali frodi commerciali secondo le rivendicazioni 7 e 8 caratterizzato dal fatto che la verifica di eventuali anomalie nel numero di richieste su uno stesso codice si basa sul superamento di un livello di soglia arbitrario di una cifra K calcolata secondo l'espressione:

$$K = N_{acq} \times P_{acq} + N_{int} \times P_{int} + N_{ver} \times P_{ver}$$

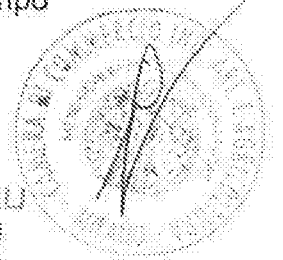
in cui N_{acq} è il numero di volte che il codice è stato verificato in seguito a un acquisto, N_{int} è il numero di volte che il codice è stato verificato a seguito dell'intenzione di acquisto, N_{ver} è il numero di volte che il codice è stato verificato senza implicare l'acquisto e

Pacq, *Pint* e *Pver* sono dei coefficienti arbitrari che tengono conto dell'importanza attribuita dall'azienda produttrice ad ognuno dei tre tipi di verifica.

13. Sistema e procedimento informatico per la verifica e il monitoraggio della circolazione dei prodotti o dei servizi e di eventuali frodi commerciali secondo la rivendicazione 2, caratterizzato dal fatto che detta interazione tra chi effettua la verifica e detto sistema informatico consiste nella fornitura di informazioni legate al prodotto nel caso non si siano evidenziate anomalie, oppure di informazioni utili a localizzare l'eventuale frode commerciale nel caso tali anomalie fossero presenti.

14. Sistema e procedimento informatico per la verifica e il monitoraggio della circolazione dei prodotti o dei servizi e di eventuali frodi commerciali secondo la rivendicazione 1 caratterizzato dal fatto di permette di ottenere informazioni di Marketing da parte dei consumatori quali per esempio preferenze, modalità di acquisto, soddisfazione ecc.

15. Sistema e procedimento informatico per la verifica e il monitoraggio della circolazione dei prodotti o dei servizi e di eventuali frodi commerciali secondo la rivendicazione 1 caratterizzato dal fatto che permette di offrire agli organi di controllo, ad esempio le dogane, un mezzo semplice ed immediato per controllare e rilevare in tempo reale eventuali anomalie o frodi commerciali.



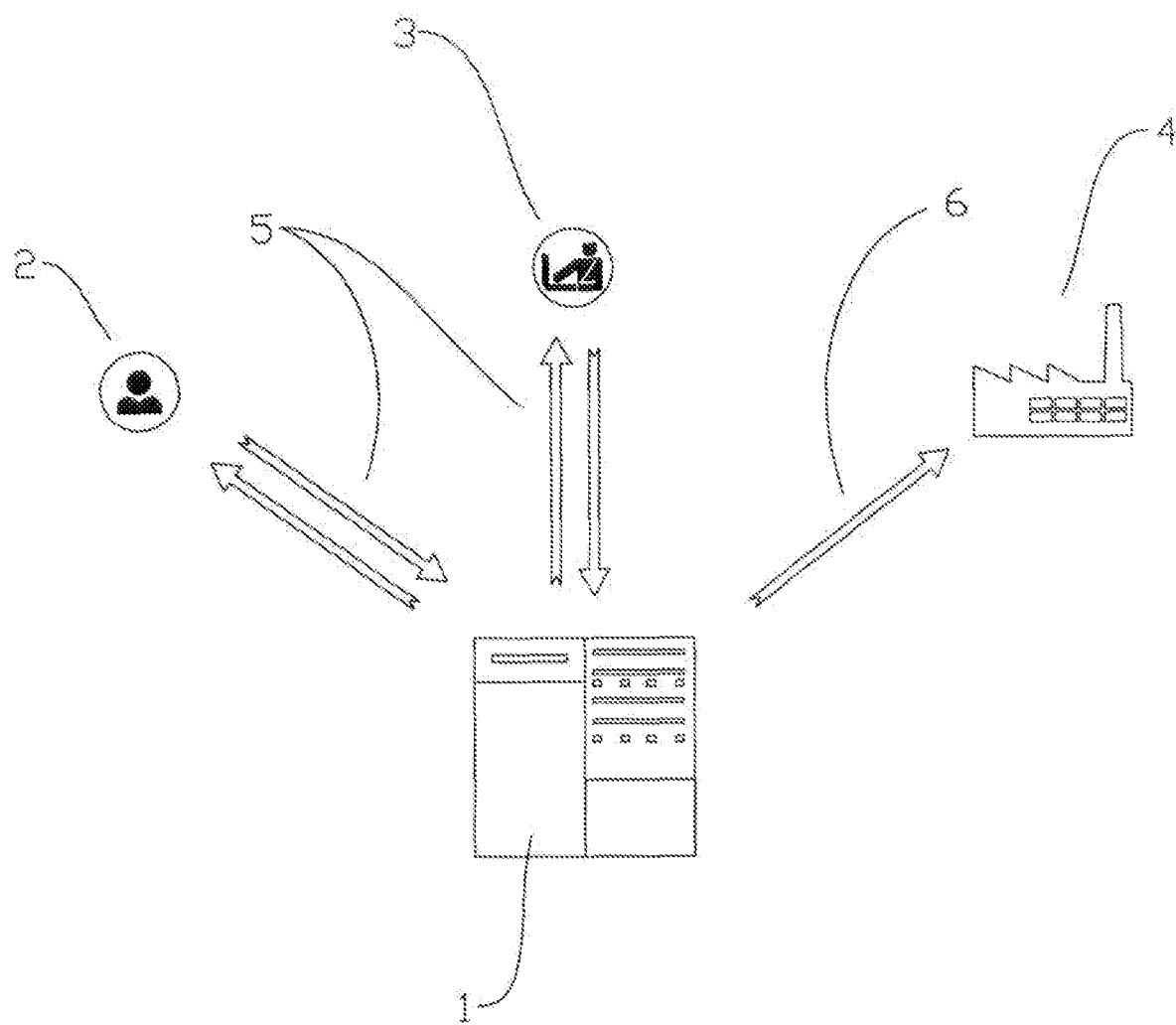
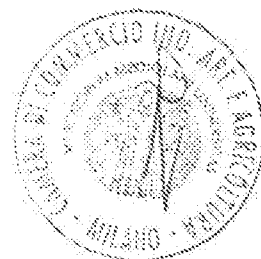


Fig. 1



Avv. A. PETRUZZELLI
CENTRO INTELLETTUALE BREVETTI
Iscr. Albo Cons. n° 31

MI2007 A 001042

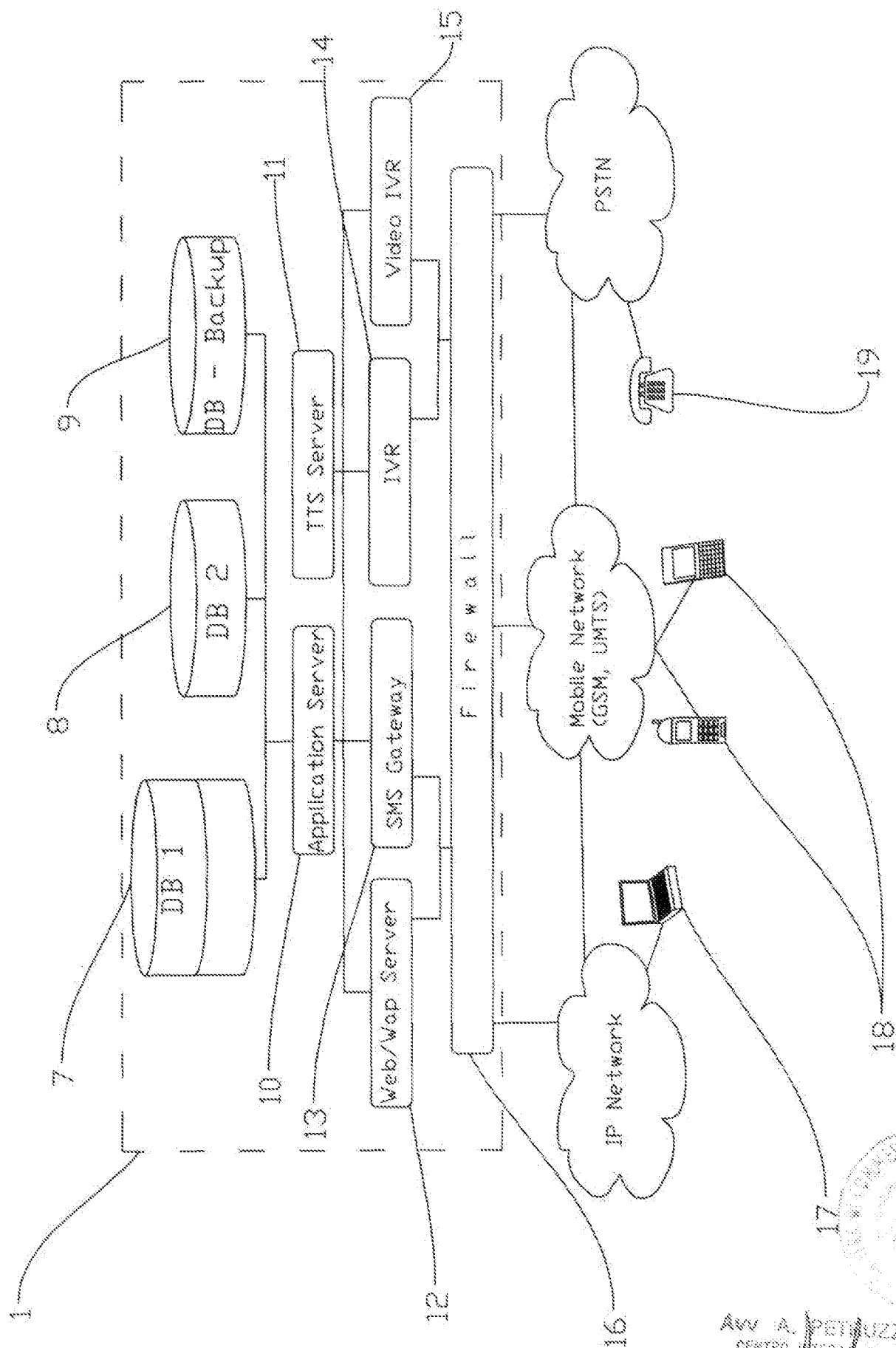


Fig. 2

MI2007 A 001042

Avv. A. PETRUZZELLI
CENTRO INTERL. GREGETTI
Iscr. Albo Cons. n° 81

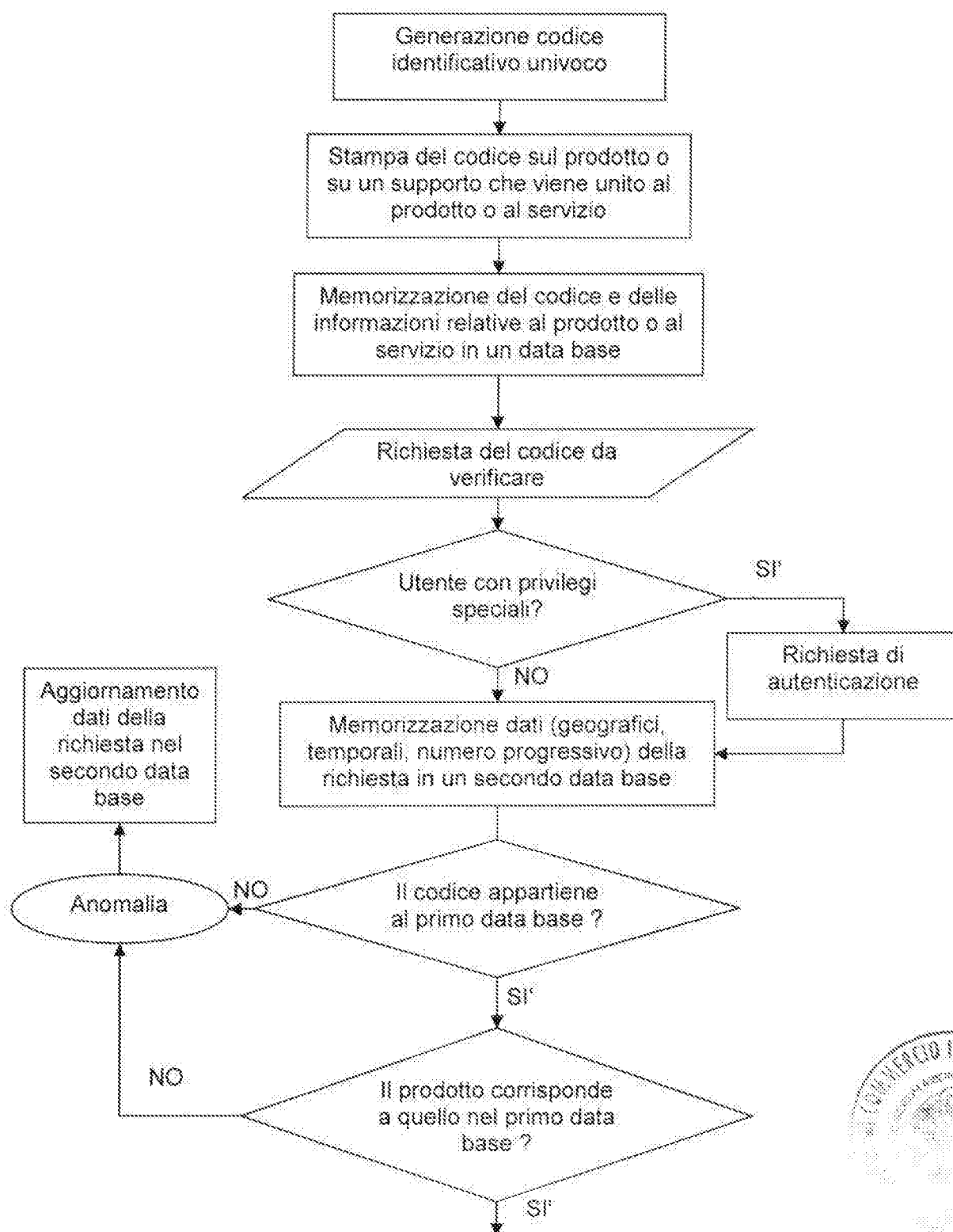


Fig. 3a.

MI2007 A 001042

Avv. A. PETRUZZELLI
CENTRO INTELLETTUALE
loc. Aldo Moro, n° 81

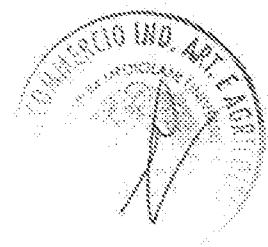
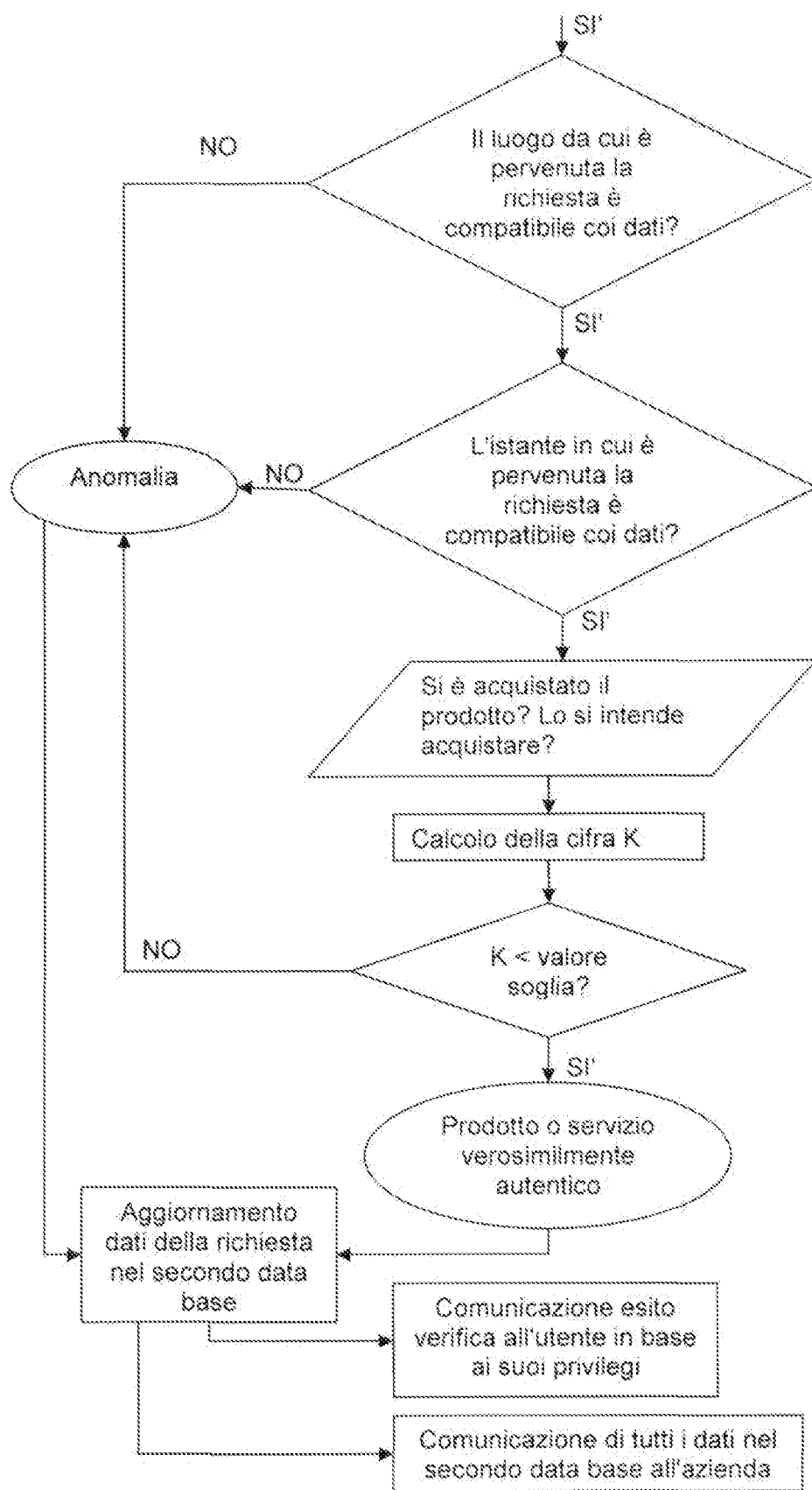


Fig. 3b

MI2007 A 001042

Avv. A. PETRUZZELLI
CENTRO INTER. BREVETTI
Isot. A. 001042, n° 31