



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

DOMANDA DI INVENZIONE NUMERO	102015000067112
Data Deposito	29/10/2015
Data Pubblicazione	29/04/2017

Classifiche IPC

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	Q	10	08

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	K	19	077

Titolo

**SIGILLO ELETTRONICO A RADIOFREQUENZA PER GARANTIRE L'AUTENTICITA' E LA
PROVENIENZA GEOGRAFICA DI OGGETTI O DOCUMENTI**

Descrizione dell'invenzione industriale dal
titolo: SIGILLO ELETTRONICO A RADIOFREQUENZA
PER GARANTIRE L'AUTENTICITA' E LA PROVENIENZA
GEOGRAFICA DI OGGETTI O DOCUMENTI; a nome di
Vincenzo Galletti, cittadino italiano residente
00132 Roma, via Barrali 55.

Inventore: lo stesso richiedente

Il presente trovato riguarda la produzione
di mezzi adoperati per dare validità o per
garantire l'autenticità e la provenienza
geografica di un oggetto o documento, nonché di
mezzi volti a reperire automaticamente le
caratteristiche principali dell'oggetto stesso
attraverso appositi dispositivi digitali, quali
smartphone o tablet.

Più in particolare il trovato riguarda un
sigillo elettronico a radiofrequenza in grado
di garantire l'autenticità e la provenienza
geografica del sigillo stesso, permettendo nel
contempo una immediata lettura delle
informazioni in esso contenute attraverso un
comune smartphone o simile.

Costituiscono parte del trovato anche
l'apparato di scrittura e lettura di detto

sigillo nonché il procedimento per la sua utilizzazione.

E' già noto da tempo il concetto di applicare al singolo oggetto o documento un transponder passivo, con un proprio numero progressivo di identificazione indelebile e imm modificabile, dotato di una memoria, non riscrivibile e non cancellabile, sufficiente per riportare i dati rilevanti dello stesso oggetto e quelli che ne attestano la provenienza e l'autenticità. E' opportuno precisare che con il termine transponder viene indicata comunemente quella apparecchiatura elettronica ricetrasmittente che, quando viene eccitata da un segnale, emette sulla stessa (raramente su una diversa) lunghezza d'onda una risposta precodificata. Il segnale ricevuto viene chiamato "interrogazione" e la risposta "treno d'impulsi codificati".

E' quindi sufficiente uno Scanner in lettura per leggere da detto transponder le caratteristiche principali dell'oggetto o del documento su cui è apposto il sigillo elettronico e verificarne l'autenticità.

Rispetto al passato, le attuali tecnologie

di miniaturizzazione hanno reso disponibili sul mercato dei transponder di ridottissime dimensioni, in cui lo spessore massimo è dell'ordine dei decimi di millimetro ed il peso inferiore al grammo. Oggi un transponder può assumere l'aspetto di una etichetta adesiva oppure di un chip della grandezza di pochi millimetri, resistente alle sollecitazioni ed alle variazioni di temperatura (da -40°C a $+85^{\circ}\text{C}$).

Tuttavia, nonostante il fatto che l'uso dei transponder si sia ampiamente sviluppato da vari decenni in diversi settori industriali, essi presentano ancora notevoli limitazioni in quanto:

- le informazioni in essi contenute non sono facilmente fruibili, in quanto necessitano di uno specifico dispositivo di lettura;
- la loro autenticità non è garantita legalmente e soprattutto
- non vi sono meccanismi in grado di garantire la provenienza geografica, ovvero il luogo in cui le informazioni sono state

effettivamente memorizzate nel
transponder.

La presente invenzione consente di risolvere queste tre problematiche ed è utilizzabile su vasta scala. Infatti il dispositivo di lettura del sigillo digitale non è necessariamente un dispositivo specifico, ma può essere un dispositivo digitale ad alta diffusione, come uno smartphone od un tablet, purchè questi siano dotati di lettore NFC (Near Frequency Communication). Tali dispositivi sono ormai sempre più diffusi sul mercato e sono quindi alla portata di una enorme quantità di consumatori.

Le caratteristiche innovative del trovato sono comunque nelle modalità con cui vengono garantite l'autenticità e la provenienza delle informazioni contenute nel transponder. Per quanto riguarda l'autenticità, questa viene garantita tramite il fatto che le informazioni memorizzate nel transponder vengono firmate, dal produttore dell'oggetto o del documento, con firma digitale, ovvero un particolare tipo di firma elettronica qualificata, basato su crittografia asimmetrica e su un certificato

digitale rilasciato da un ente certificatore accreditato. L'ordinamento giuridico italiano attribuisce a tale tipo di firma una particolare efficacia probatoria, tale da potersi equiparare, sul piano sostanziale, alla firma autografa.

Altre invenzioni hanno adottato la firma digitale per garantire l'autenticità delle informazioni contenute in un transponder, ma la presente invenzione è caratterizzata da un elemento assolutamente originale, ovvero la provenienza geografica. Questa viene garantita in quanto, all'atto della scrittura del sigillo, la presente invenzione inserisce automaticamente anche le coordinate GPS (Global Positioning System) del luogo in cui avviene la scrittura del sigillo stesso. Le coordinate GPS rientrano nella categoria delle coordinate geografiche in quanto consentono di determinare la posizione sul globo terrestre attraverso i dati di latitudine e longitudine.

Quest'ultima caratteristica consente numerosi vantaggi in funzione del contesto di utilizzo del sigillo digitale, soprattutto nel campo della lotta alla contraffazione.

Ad esempio, nel caso di prodotti esposti in un punto vendita, il sigillo può essere letto da un acquirente in modo tale da verificare le caratteristiche del prodotto stesso e quindi facilitare un acquisto più consapevole e informato. Contemporaneamente, l'acquirente può verificare non solo l'autenticità delle informazioni, ma anche la loro provenienza geografica. Tale esempio, per quanto non esaustivo rispetto a tutti i possibili utilizzi del trovato, dimostra come il sigillo digitale costituisca una soluzione particolarmente efficace per la tutela dei prodotti "Made in Italy" nel campo agroalimentare, della moda e della componentistica.

La produzione del sigillo elettronico prevede le seguenti apparecchiature:

a) almeno un transponder passivo, preferibilmente della serie NTAG, su cui scrivere i dati del sigillo digitale: (i Tag NTAG sono infatti i Tag NFC con la migliore compatibilità verso tutti i dispositivi NFC, sono dotati di chip di ultima generazione che offrono prestazioni migliori sia in termini di

velocità di trasmissione dati che per quanto riguarda il range di lettura e sono compatibili con i diversi sistemi operativi mobili come Android, Windows Phone, Blackberry, ecc.;

b) Un dispositivo di lettura/scrittura di transponder NFC, già disponibile sul mercato, collegato via cavo USB ad un Personal Computer;

c) Un dispositivo elettronico, noto con il nome "Beacon", che interagisce con il Personal Computer preferibilmente attraverso protocollo di rete Bluetooth 4.0 ed incorpora una antenna GPS. La tecnologia Beacon basata sul Bluetooth, ormai nota da tempo , consente ai dispositivi bluetooth di trasmettere e ricevere piccoli messaggi entro brevi distanze;

d) un apposito programma software installato sul detto Personal Computer, che gestisce l'acquisizione delle coordinate geografiche attraverso interrogazione al Beacon tramite interfaccia BlueTooth, assieme alle informazioni sul codice identificativo dello stesso Beacon, previa verifica del suo stato (se il dispositivo è stato spostato o meno dalla sua sede) e l'operazione di scrittura vera e propria del sigillo;

e) un lettore smartcard per firma digitale collegato via cavo USB a detto Personal Computer.

Secondo una caratteristica peculiare del presente trovato, su tale dispositivo Beacon vengono memorizzate due informazioni: il proprio codice univoco identificativo e le coordinate dello stabilimento dove viene prodotto il sigillo. Le informazioni sono inserite univocamente sulla memoria non cancellabile del dispositivo Beacon. Detto dispositivo viene fissato con viti o tasselli nell'ambiente destinato alla produzione del geotag in modo da impedirne spostamenti casuali o involontari e, in una forma preferita di realizzazione, viene dotato al proprio interno di un sensore di movimento (accelerometro) che registra eventuali spostamenti del dispositivo stesso dalla sede dove è stato montato originariamente, ed in questo caso, ipotizzando una causa dolosa, genera uno stato di blocco.

Le fasi del processo di scrittura sono le seguenti:

a) Richiamando sul PC l'apposito programma, un operatore digita il testo del

sigillo;

b) Il programma legge dal transponder il numero identificativo attraverso il lettore/scrittore del transponder NFC;

c) Il programma legge dal Beacon le informazioni, in esso memorizzate, relative al suo codice univoco, alle coordinate geografiche dello stabilimento ed allo stato del dispositivo stesso. Se il dispositivo ha registrato dei movimenti, restituirà uno stato di blocco ed il programma di scrittura assume che il dispositivo sia stato spostato dal luogo originario. In tal caso il programma si bloccherà e non procederà alla produzione del tag.

d) In assenza di blocco, il contenuto del sigillo, costituito da testo, numero identificativo del transponder e coordinate geografiche è pronto per la scrittura. Come ulteriore elemento conoscitivo, tali informazioni possono essere completate inserendo anche il codice identificativo del Beacon. Il programma richiede all'operatore le credenziali per la firma digitale e firma digitalmente il contenuto.

e) Il programma scrive il contenuto firmato sul transponder.

A questo punto il sigillo digitale può essere apposto sull'oggetto nel modo più conveniente, in base alla tipologia dell'oggetto stesso.

L'introduzione del Beacon come fonte delle coordinate geografiche è di particolare interesse rispetto all'adozione di una normale antenna GPS in quanto:

- a) E' utilizzabile anche in ambienti chiusi, ove il segnale GPS sarebbe di difficile o addirittura impossibile rilevazione.
- b) Offre maggiore garanzia in quanto non alterabile e soprattutto non spostabile. Infatti nel caso in cui il Beacon si sposti, il sensore accelerometro interno manda in blocco l'apparecchiatura. Questa può essere ripristinata solo tramite apposito intervento da parte di un tecnico abilitato.

La lettura del sigillo avviene tramite uno smartphone provvisto di chip NFC, su cui è

installata una apposita APP. Avvicinando lo smartphone all'oggetto, l'APP legge il contenuto del transponder, decodifica il contenuto e visualizza sul dispositivo le seguenti informazioni:

a) testo e codice identificativo del transponder;

b) Informazioni sulla persona giuridica che ha emesso l'etichetta;

c) Coordinate geografiche del luogo in cui l'etichetta è stata prodotta.

E' evidente che la contraffazione dell'etichetta stessa non è possibile, in quanto l'APP verifica che il codice identificativo del transponder sia lo stesso di quello memorizzato all'interno del sigillo stesso. Nel caso in cui i due valori non corrispondano, l'APP avvisa l'utente della contraffazione e invia automaticamente una notifica al produttore, che potrà così essere avvisato della contraffazione e potrà procedere ad eventuali azioni legali di tutela del marchio. Quanto ad un eventuale spostamento del Beacon rispetto alla posizione in cui ha effettuato originariamente il rilievo delle

coordinate geografiche, l'accelerometro in esso montato provvede a mandare in blocco la trasmissione al PC, impedendo l'avvio del programma di scrittura sul trasponder.

La provenienza geografica dell'etichetta è un elemento di reale tutela del produttore e costituisce un potente ed economico strumento di tutela e di promozione soprattutto per i piccoli produttori, che costituiscono il nucleo portante dell'economia italiana.

Ulteriori caratteristiche e vantaggi del trovato risulteranno dalla descrizione particolareggiata che segue, sulla base della allegata tavola di disegni che ne rappresentano, a solo titolo di esempio non limitativo, una preferita forma realizzativa. Nella tavola:

la fig. 1 mostra l'insieme delle apparecchiature necessarie per la produzione del sigillo elettronico secondo il presente trovato.

Secondo l'arte nota i transponder tradizionali, sono composti da tre elementi:

- a) Un tag: il componente elettronico che ha la funzione intelligente di gestire

tutta la parte di comunicazione e identificazione.

- b) Una antenna: l'apparato che permette al tag di essere alimentato (se non ha già una batteria a bordo) e di ricevere ed eventualmente trasmettere le comunicazioni con il mondo esterno; ed
- c) Un supporto: la parte di materiale che sostiene e protegge i primi due elementi.

Come si è detto nel preambolo, il presente trovato prevede l'uso di un tag NTAG dotato di un chip che consente di memorizzare grandi quantità di dati.

Una prima caratteristica peculiare del trovato sta nel fatto che si prevede di inserire automaticamente, all'atto di memorizzare nel chip del transponder di un sigillo digitale le informazioni che attestano l'autenticità e la provenienza di un oggetto, compresa la firma digitale, anche le coordinate GPS del luogo dove dette informazioni sono state introdotte, individuando in pratica il luogo dove il sigillo digitale che accompagna un prodotto, ha avuto origine.

In fig.1, è illustrato l'insieme dei dispositivi che concorrono alla produzione del sigillo elettronico.

Con 2 è indicato un dispositivo di lettura/scrittura di transponder NFC collegato via cavo USB ad un Personal Computer 1

Con 3 è indicato un lettore smartcard per firma digitale collegato via cavo USB a detto Personal Computer.

Con 9 è indicato un programma software da installare sul PC 1 per gestire l'operazione di scrittura del sigillo digitale. Con 4 è indicato il dispositivo Beacon sul quale vengono memorizzati il codice che lo identifica e le coordinate geografiche del luogo di memorizzazione/stampa del sigillo, cioè il sito 6 dove detto Beacon 4 è fissato stabilmente. Su detto dispositivo Beacon è montato un sensore di movimento 8, preferibilmente un accelerometro, che consente di rilevare ogni spostamento effettuato dal Beacon rispetto alla sua sede originale.

Il processo di scrittura del sigillo digitale avviene con la seguente modalità:

1. L'operatore a cui è demandato il

compito di preparare il sigillo, richiama sul computer l'apposito programma e provvede a digitare il testo che deve essere memorizzato nel sigillo.

2. Il programma legge dal trasponder il numero identificativo dello stesso attraverso il lettore/scrittore 2.

3. Il programma legge sul dispositivo Beacon 4, vincolato fermamente nella propria posizione di lavoro 6, i dati in esso memorizzati vale a dire sia il suo codice identificativo che le coordinate geografiche del luogo dove tale memorizzazione è stata effettuata, nonché l'eventuale stato di blocco dello stesso dispositivo, che interviene qualora il dispositivo risulti essere stato spostato dal luogo dove era stato fissato originariamente; in assenza di spostamenti, il programma abilita la trasmissione degli stessi dati al PC.

4. Il programma memorizza sul chip del transponder il testo relativo

all'oggetto, il codice identificativo del transponder, e le coordinate geografiche del luogo di produzione; vantaggiosamente, come ulteriore elemento conoscitivo, tali informazioni possono essere completate dal codice identificativo del dispositivo Beacon.

5. Il programma richiede all'operatore la sua firma digitale e provvede a firmare digitalmente quanto memorizzato sul chip del transponder.

Una volta applicato il sigillo elettronico sul prodotto che deve contraddistinguere, potrà essere letto in un qualunque momento attraverso uno smartphone o simile, provvisto di chip NFC, su cui è installata una apposita APP, senza la necessità di ricorrere ad uno specifico dispositivo di lettura.

Avvicinando lo smartphone all'oggetto, l'APP legge il contenuto del transponder, decodifica il contenuto e visualizza sul dispositivo le seguenti informazioni:

- a) testo e codice identificativo del transponder;

b) Informazioni sulla persona giuridica che ha emesso l'etichetta;

c) Coordinate geografiche del luogo in cui l'etichetta è stata prodotta.

Il semplice confronto tra i dati riportati direttamente sull'etichetta e riscontrabili a vista e quelli letti dallo smartphone, permette di individuare eventuali casi di contraffazione, che potranno eventualmente essere segnalati in automatico dalla stessa APP installata sul chip NFC del trasponder NFC.

RIVENDICAZIONI

1) Metodo per la realizzazione e la lettura di un sigillo elettronico a radiofrequenza in grado di garantire l'autenticità e la provenienza geografica di un oggetto o documento su cui detto sigillo è applicato, caratterizzato dal fatto che prevede di:

predisporre almeno un transponder passivo NFC su cui scrivere i dati identificativi dello stesso transponder attraverso un dispositivo di lettura/scrittura (2) di transponder NFC;

collegare via cavo USB detto dispositivo di lettura/scrittura (2) ad3 un Personal Computer (1);

collegare via cavo USB allo stesso Personal Computer (1) un lettore smartcard (3) per firma digitale;

memorizzare su un dispositivo Beacon (4), dotato di un'antenna GPS, il suo codice identificativo e le coordinate geografiche del luogo dove tale memorizzazione è stata effettuata;

collegare tramite interfaccia Bluetooth detto dispositivo Beacon (4) allo stesso Personal Computer (1); ed

installare su detto Personal Computer (1) un apposito programma software (9) in grado di gestire l'operazione di scrittura vera e propria del sigillo previa acquisizione dei dati relativi alle coordinate geografiche del luogo in cui detto sigillo elettronico viene prodotto, memorizzate su detto dispositivo Beacon, in modo che:

un operatore richiamato sul PC detto apposito programma, possa digitare il testo del sigillo;

il programma legga dal transponder il suo codice identificativo;

il programma legga dal dispositivo Beacon le informazioni, su di esso memorizzate, relative al suo codice identificativo e le coordinate geografiche del luogo di produzione;

con il contenuto del sigillo, costituito da testo, numero identificativo del transponder e coordinate geografiche del luogo di produzione del sigillo pronto per la scrittura, il programma richieda all'operatore le credenziali per la firma digitale e firmi digitalmente il contenuto tramite il lettore di smartcard;

il programma scriva il contenuto firmato sul transponder; e successivamente

il sigillo digitale sia apposto sull'oggetto nel modo più conveniente, in base alla tipologia dell'oggetto stesso.

2) Metodo come alla rivendicazione 1 caratterizzato dal fatto che il transponder è della serie NTAG.

3) Metodo come alla rivendicazione 1 caratterizzato dal fatto che il contenuto del sigillo, costituito da testo, numero identificativo del transponder e coordinate geografiche del luogo di produzione del sigillo stesso, è completato dal codice identificativo del dispositivo Beacon.

4) Metodo come ad una qualunque delle rivendicazioni precedenti caratterizzato dal fatto che il dispositivo Beacon (4) è vincolato fermamente sul luogo di produzione (6) in modo da evitare spostamenti casuali e non voluti.

5) Metodo come alla rivendicazione precedente caratterizzato dal fatto che ogni spostamento di detto dispositivo Beacon dal luogo di produzione dove è stato fissato, è rilevato da un accelerometro che porta in blocco detto

dispositivo impedendo la trasmissione dei dati in esso memorizzati al computer.

6) Metodo come ad una qualunque delle rivendicazioni precedenti caratterizzato dal fatto che per la lettura del sigillo è previsto l'uso di uno smartphone od un tablet provvisto di chip NFC, su cui è installata una apposita APP atta a leggere, avvicinando lo smartphone od il tablet all'oggetto, il contenuto del transponder, a decodificare il contenuto ed a visualizzare sul dispositivo le seguenti informazioni:

- a) testo e numero identificativo del transponder ;

- b) Informazioni sulla persona giuridica che ha emesso l'etichetta;

- c) Coordinate geografiche del luogo in cui l'etichetta è stata prodotta ed, eventualmente, il codice identificativo del dispositivo Beacon.

7) Apparato per la realizzazione e la lettura di un sigillo elettronico a radiofrequenza in grado di garantire l'autenticità e la provenienza geografica di un oggetto o documento su cui detto sigillo è applicato,

caratterizzato dal fatto che comprende, per la fase di scrittura del sigillo:

a) Un transponder passivo NFC, su cui scrivere i dati del sigillo digitale, compatibile con tutti i dispositivi NFC e con i diversi sistemi operativi mobili come Android, Windows Phone, Blackberry e simili;

b) Un dispositivo di lettura/scrittura di transponder NFC, collegato via cavo USB ad un Personal Computer;

c) Un dispositivo Beacon dotato di un'antenna GPS e collegato via Bluetooth allo stesso Personal Computer e sul quale sono memorizzati il proprio codice identificativo e le coordinate geografiche del luogo di produzione del sigillo;

d) un lettore smartcard per firma digitale collegato via cavo USB a detto Personal Computer; ed

e) Un apposito programma software installato sul detto Personal Computer, che gestisce l'operazione di scrittura vera e propria del sigillo con la contemporanea acquisizione attraverso detto dispositivo Beacon delle coordinate geografiche del luogo

di produzione del sigillo ed eventualmente del codice identificativo dello stesso dispositivo, e, attraverso detto dispositivo di lettura/scrittura di transponder, del codice identificativo del transponder stesso ; e richieda all'operatore le credenziali per la firma digitale e firmi digitalmente il contenuto; e

per la fase di lettura del sigillo apposto sull'oggetto o documento,

uno smartphone od un tablet provvisto di chip NFC, su cui è installata una apposita APP atta a leggere, avvicinando lo smartphone od il tablet all'oggetto, il contenuto del transponder, a decodificare detto contenuto e a visualizzare detto contenuto decodificato sullo stesso smartphone o tablet.

Per il Richiedente

Il Rappresentante

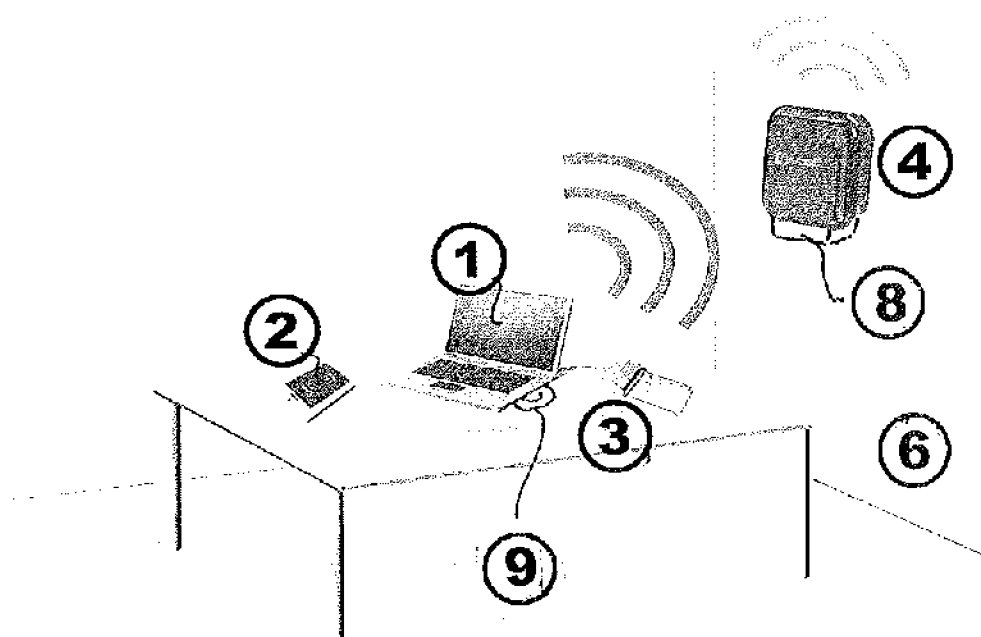


FIG. 1