



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

DOMANDA DI INVENZIONE NUMERO	102015000047917
Data Deposito	02/09/2015
Data Pubblicazione	02/03/2017

Priorità	102014902290027
Nazione Priorità	IT
Data Deposito Priorità	02-SEP-14
Priorità	IB2015/056637
Nazione Priorità	IB
Data Deposito Priorità	01-SEP-15

Classifiche IPC

Titolo

METODO ANTICONTRAFFAZIONE ROBUSTO A CODICI DINAMICI E RELATIVO SISTEMA

METODO ANTICONTRAFFAZIONE ROBUSTO A CODICI DINAMICI E RELATIVO SISTEMA

DESCRIZIONE

Campo tecnico

Il campo tecnico dell'invenzione proposta è quello dei metodi e sistemi anticontraffazione per beni mobili o circolanti e riguarda tutti i settori commerciali in cui vi sia una richiesta di controllo di originalità di un prodotto, quale un capo di abbigliamento, prodotti di occhialeria, alimentari, farmaceutici, ecc.

Definizioni e nomenclatura utilizzata

Nella presente descrizione e nelle annesse rivendicazioni i seguenti termini devono essere intesi secondo le definizioni date qui di seguito.

Marcatura anticontraffazione: è una modalità di "marcatura" degli oggetti, in produzione o in una fase in cui se ne ha ancora il completo controllo, tale da poter "certificare" e distinguere in modo sicuro i prodotti da copie non autorizzate. Questa marcatura permette di stabilire se i prodotti sono originali, ossia provenienti da una determinata azienda autorizzata.

Marchiatore: oggetto esogeno al prodotto marcato, utilizzato per riconoscere il prodotto stesso attraverso segni o codici associati al marchiatore.

CF: codice fisso, un codice che non viene modificato durante il ciclo di vita del prodotto.

CD: codice dinamico, un codice che viene modificato durante il ciclo di vita del prodotto.

TAG: identifica l'oggetto fisico che funge da etichetta, identificatore o supporto su cui risiede l'uno o più codici che definiscono il "marchiatore" e permettono di certificare l'autenticità.

RFID: (dall'inglese "radio-frequency identification", in italiano "identificazione a radio frequenza") si intende una tecnologia per l'identificazione e/o memorizzazione automatica di dati tramite scambio via radio-frequenza. È basata sulla capacità di memorizzare e leggere dati a distanza in particolari dispositivi elettronici (detti transponder) con l'utilizzo di appositi apparati fissi o portatili

chiamati per semplicità lettori (aventi però anche proprietà di scrittura).

NFC: (dall'inglese "Near Field Communication"; in italiano letteralmente "Comunicazione in prossimità") si intende una tecnologia che permette memorizzazione e lettura di dati in appositi dispositivi, del tutto simile a quella RFID ma con protocolli e tecnologia che consente connettività wireless bidirezionale solo a corto raggio (fino a un massimo di 10 cm).

APP: una variante delle applicazioni informatiche dedicate principalmente ai dispositivi di tipo mobile, quali smartphone e tablet.

Sistema remoto di gestione e controllo: un insieme di hardware e software esogeni al marcatore, che permette di interfacciarsi da remoto con il singolo marcatore e gestire i dati ed i flussi dei dati da e verso lo stesso.

Prodotti "consumer": prodotti o beni mobili, commercializzati per un elevato numero di consumatori.

Tipologie dei TAG

- *Con memoria READ/WRITE oppure READ ONLY:* nella prima varietà è ammessa la riscrittura dei dati, nella seconda i dati possono essere scritti una sola volta (tipicamente in fase di produzione)

- * memoria di 128-512 (o superiori) bit;

- * memoria di 32-128 bit, più economici e generalmente idonee per etichette per prodotti "consumer"

- * Bassissimo costo

- A bassa potenza di calcolo

- * potenza di calcolo non sufficiente per la crittografia o la firma digitale

- * costo maggiore (costo alto per marcature "a perdere" di tipo "consumer")

- A elevata potenza di calcolo

- * costo elevato (del tutto inutilizzabile per marcature "a perdere" di tipo "consumer")

Un sistema di anticontraffazione robusto (sicuro) si può definire come un sistema di marcatura, controllo e verifica soddisfacente i seguenti 4 requisiti:

Verificabilità: implica il poter riconoscere/verificare che un articolo è uscito dalla propria catena produttiva:

Non generabilità: implica che un malintenzionato non possa generare facilmente un contrassegno che passi la verifica di autenticità;

Non replicabilità: implica che, dato un contrassegno, non è possibile crearne una serie di copie utili irrinconoscibili dall'originale;

Verificabilità delle manomissioni: significa che dev'essere possibile individuare se un contrassegno è stato manomesso o il sistema di protezione è in qualche modo alterato.

Stato della tecnica anteriore

I sistemi anticontraffazione attualmente presenti sul mercato si possono dividere in due sottogruppi:

"a basso costo relativo", ossia quei sistemi il cui costo industriale ha una bassa incidenza sul costo del prodotto, ad esempio in relazione al costo e/o al margine operativo del prodotto stesso;

"ad alto costo relativo", ossia tutti gli altri sistemi.

Fra i principali sistemi a basso costo ad oggi utilizzati si possono elencare ad esempio i codici a barre, i codici QR, i laser code, le etichette olografiche, la filigrana, gli inchiostri particolari, ...; tutti questi sistemi noti garantiscono una economicità produttiva, a scapito tuttavia della robustezza/sicurezza del sistema. In particolare ciascuno dei metodi conosciuti, non garantisce il requisito della "non replicabilità" del marchatore.

Fra i sistemi a basso costo, ad oggi nel mercato sono annoverati anche semplici TAG NFC, di tipo passivo, che sfruttando un codice identificativo univoco registrato al loro interno dai produttori con apposite procedure di sicurezza (non del tutto invulnerabili).

Fra i sistemi ad alto costo, invece, si possono trovare marcatori utilizzando tecnologia RFID con potenza di calcolo.

Problemi della tecnica anteriore

Allo stato dell'arte delle attuali soluzioni presenti nel mercato non si rileva alcuna soluzione a basso costo in grado di garantire la robustezza del sistema.

In particolare ogni metodologia economicamente vantaggiosa per il produttore, che adotti marcatori di prodotto, non garantisce la non riproducibilità del marchatore.

I principali processi/impianti attualmente presenti nel mercato, in grado di garantire realmente la sicurezza del sistema anticontraffazione, sono basati su tecnologia a microcontrollore o tecnologia RFID con TAG ad elevata potenza di calcolo, ossia sistemi in grado di elaborare il messaggio eventualmente ricevuto fornendo una risposta conseguente all'elaborazione del messaggio. Molti di questi

utilizzano "pre" e "post" elaborazioni anche su sistemi remoti, ma il problema principale sino ad ora irrisolto è la necessità di avere unitamente al prodotto un marcatore complesso e costoso ed un sistema in grado di elaborare attivamente i dati. I sistemi ad oggi conosciuti rendono il processo di marcatura e controllo industrialmente oneroso ed impraticabile per tutti i prodotti "consumer".

Si stanno proponendo nel mercato anche soluzioni che utilizzano TAG NFC a basso costo e media o bassa potenza di calcolo, che risultano economicamente più vantaggiosi; in questi casi sono proposte soluzioni con crittografia dei dati o l'utilizzo di un particolare codice identificativo unico (UID) inserito nei TAG dai produttori degli stessi.

Tuttavia la crittografia non è completamente esente da possibili attacchi, ciò che rende necessario mettere in opera continui aggiornamenti dei sistemi e relativa gestione delle "revisioni"; inoltre le comunicazioni "Wi-Fi" hanno la peculiarità di essere vulnerabili ad attacchi denominati "man in the middle", che semplificano l'attività illecita di inserimento per riuscire a decrittare le comunicazioni ed i codici per creare delle copie; per altro verso, l'utilizzo del UID non offre una certezza sul requisito della "non replicabilità", in quanto può essere riprodotto da un produttore diverso (peraltro utilizzando tecniche di "*mirroring*" del codice dei microchip NFC che sono divenute standard di mercato).

Nel mercato sono stati anche già proposti TAG RFID contenenti un doppio codice, almeno uno dei due riscrivibile. Esempi di marcatori con due codici, di cui uno variabile, sono descritti in JP2007/328567, US 2002/125997, JP2001/005931.

Una applicazione che è stata proposta per questi marcatori in combinazione con un sistema remoto di gestione e controllo, è quella di identificare il TAG (tramite un primo codice statico) ed autorizzarne o inibirne la lettura, tramite il secondo codice variabile che conserva una sorta di "firma storica" univoca di quel TAG di cui viene tenuta traccia nel sistema remoto di controllo. Un esempio di questa applicazione è descritto in "Dirk Henrici and Paul Mueller, Hash-based enhancement of Location privacy for radio-frequency identification devices using varying identifiers", nei Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW'04), PISCATANAY, NJ, USA, IEEE", in cui si presenta un sistema destinato a impedire che il marcatore del prodotto possa essere letto da terze parti non autorizzate, ciò che configurerebbe problemi di privacy.

Descrizione sommaria dell'invenzione

Scopo dell'invenzione

Scopo della presente invenzione è quello di fornire un sistema ed un metodo anticontraffazione per beni "consumer" che sia economico, sia nella sua costruzione che nella sua gestione, e che permetta di ridurre drasticamente altri costi connessi alla verifica delle produzioni parallele.

Infatti, un problema esistente nelle catene distributive dei prodotti è quello delle produzioni parallele. Nel mercato, alcuni grossisti o rivenditori possono acquistare, oltre ad un certo numero di prodotti autentici (genuine) anche alcuni prodotti falsi (fake), da offrire all'acquirente finale in modo illegale ma con margini di guadagno più elevati. Per evitare questi fenomeni di contraffazione, che producono importanti danni economici ai produttori, questi ultimi sono obbligati a definire un servizio di investigazione, inviando operatori addestrati presso i propri grossisti/rivenditori e svolgere onerose indagini sui prodotti a magazzino per verificare eventuali giacenze di prodotti falsi di produzioni parallele.

Non esiste ad oggi una metodologia che permetta ai produttori di monitorare a distanza la presenza di prodotti paralleli falsi nelle proprie catene distributive.

Il metodo ed il sistema dell'invenzione risolvono contemporaneamente le richieste di robustezza (sicurezza) ed economicità del sistema anticontraffazione, utilizzando le tecnologie a basso costo presenti nel mercato, e le esigenze di sorveglianza della catena distributiva a distanza senza dover ricorrere ad onerose ed invasive tecniche di investigazione.

Concetto dell'invenzione

Il sistema prevede l'utilizzo di:

1. un marcatore prodotto secondo la tecnologia RFID (TAG), provvisto di almeno un codice identificativo univoco riscrivibile;
2. un sistema remoto di gestione e controllo che si occupa della verifica e della gestione dei dati, in entrata ed in uscita, relativi al marcatore;
3. un apparato di interfaccia fra il marcatore, il sistema remoto di gestione e controllo ed un utente.

Il sistema prevede l'utilizzo di un codice dinamico, generato dal sistema remoto di gestione e controllo ed associato al singolo prodotto tramite un rispettivo TAG RFID, durante il processo produttivo, o eventualmente distributivo o eventualmente di vendita, o eventualmente in una fase in cui se ne ha ancora il

controllo. Tale codice dinamico è parallelamente registrato all'interno del sistema remoto di gestione e controllo ed ivi continuamente aggiornato in base agli eventi storici che si verificano sul singolo prodotto; in altre parole, la dinamicità del codice viene determinata dalla vita stessa del prodotto: il codice viene modificato in relazione a controlli o aggiornamenti effettuati sul prodotto - cioè sul marcatore del suo TAG RFID - e tale modifica rimane registrata all'interno del sistema remoto di gestione e controllo, fornendo quindi in ogni momento un codice identificativo unico per il prodotto e differente ogni volta. In questo modo il prodotto marcato sarà identificato da un codice differente ad ogni verifica e non esiste un solo singolo codice, clonabile, con il quale si possa riuscire a riprodurre in modo fraudolento il marcatore per applicarlo su un prodotto parallelo falso. Grazie all'intervento degli stessi utenti sui marcatori dei prodotti, sulla parte terminale della catena di distribuzione - ossia presso il punto vendita - i prodotti rimangono associati a marcatori univoci di cui è possibile tener traccia: ciò consente, per converso, di identificare immediatamente un eventuale marcatore clonato, così da metterlo subito fuori del circuito dei marcatori/prodotti autentici (dandone adeguata informazione all'utente/acquirente) e identificare il rivenditore che si è approvvigionato di prodotti paralleli senza dover svolgere alcuna attività investigativa in loco. Da un punto di vista operativo, il sistema può essere messo in opera mediante un marcatore con un solo codice variabile, preferibilmente composta da una parte fissa CF ed una parte dinamica CD, oppure con una coppia di codici di cui uno fisso CF ed uno variabile dinamicamente CD.

Vantaggiosamente, il CF permette di rilevare il caso in cui un CD venga sostituito con un CD esistente attribuito ad un altro prodotto, ed in caso di manomissione permette attraverso varie politiche di ripristinare il codice CD corretto. In tal caso il sistema prevede quindi l'utilizzo di una coppia di codici associati al prodotto: un codice fisso ed un codice dinamico. Considerato che in un determinato momento, ad un codice CF valido corrisponde uno ed un solo codice CD, è possibile rilevare e correggere eventuali manomissioni. Il fatto di usare la coppia CF+CD non implica necessariamente che il codice CF debba essere utilizzato per eseguire ogni verifica.

I codici CF possono essere rappresentati in vari modi, purché essi non siano alterabili dall'utente. A scopo esemplificativo: un codice a barre, un QR Code, un TAG NFC in sola lettura, il codice UID di un TAG, ecc.

Ulteriormente, entrambi i codici sono associati al prodotto durante il pro-

cesso produttivo o in una fase in cui se ne ha ancora il completo controllo, e sono parallelamente registrati all'interno di un database. Mentre il primo codice fisso CF non subisce modifiche nella vita del prodotto, il secondo codice dinamico CD viene modificato in relazione a controlli o aggiornamenti effettuati sul prodotto, ovvero sul marcatore del prodotto. Tale modifica rimane registrata all'interno del database remoto fornendo quindi in ogni momento un codice identificativo unico per il prodotto in maniera analoga al metodo precedente.

Ulteriormente, operando nella maniera descritta, il prodotto marcato viene identificato da un codice differente ad ogni verifica; in questo modo non esiste un codice univoco riproducibile con il quale si possa creare un clone del prodotto verificato. Quandunque venisse fatta una copia dell'assieme dei due codici CF+CD, in un determinato istante della vita del marcatore associato al prodotto, questa cesserebbe di essere riconosciuta valida alla successiva verifica sul marcatore associato al prodotto originale che, in virtù di tale verifica, verrebbe immediatamente modificato e tracciato nel database del sistema di gestione. Dipendendo la generazione del nuovo CD da un sistema remoto che genera ed associa il nuovo codice a quel prodotto ad ogni richiesta di verifica solamente quando sia andata a buon fine, non è possibile modificare parallelamente le eventuali copie create con il codice clonato. In tale maniera, ogni eventuale copia clonata del marcatore, verrebbe resa immediatamente riconoscibile come copia non originale.

Nel caso in cui venisse invece verificato il marcatore con il CD clonato associato ad un prodotto falso, automaticamente il codice dinamico CD sul marcatore originale smetterebbe di essere riconosciuto come valido: si avrebbe così la situazione in cui, a fronte di un campione/marcatore falsificato che viene riconosciuto come autentico, si otterrà come contropartita che il prodotto/marcatore originale viene riconosciuto come falso: questa situazione rende la clonazione economicamente non conveniente, perchè nella catena distributiva riesce a circolare un solo prodotto ritenuto "originale", mentre qualsiasi altro prodotto (clonato od originale che fosse all'inizio), viene escluso dal circuito dei prodotti genuini: il metodo impedisce così la reale possibilità di generazione seriale di copie. Risulta assolutamente impossibile creare più di una copia del singolo pezzo dell'assieme prodotto-marcatore originale e la produzione di una sola copia non risulta un processo vantaggioso.

È in tal modo dimostrato che il metodo secondo l'invenzione fornisce la migliore soluzione raggiungibile per mezzo di marcatori esogeni all'oggetto.

Breve descrizione dei disegni

Ulteriori caratteristiche e vantaggi del sistema e metodo secondo l'invenzione risulteranno comunque meglio evidenti dalla descrizione dettagliata che segue di preferite forme di esecuzione della stessa, data a titolo di esempio ed illustrata nei disegni annessi, nei quali:

Fig. 1 è una vista schematica che rappresenta le interazioni in un sistema secondo una prima forma di esecuzione dell'invenzione;

Fig. 2 è una vista schematica che rappresenta le interazioni in un sistema concordemente ad una seconda forma di esecuzione dell'invenzione; e

Fig. 3 è una vista schematica che rappresenta le interazioni in un sistema secondo una terza forma di esecuzione dell'invenzione.

Descrizione di forme di esecuzione preferite

A puro scopo esemplificativo e non esaustivo, si fornirà qui di seguito una possibile modalità di messa in opera del sistema e metodo dell'invenzione.

Come rappresentato in fig. 1, il sistema si basa su marcatore 1, da applicarsi ad un prodotto, una infrastruttura informatica 2, che agisce da sistema remoto di gestione e controllo, e da un dispositivo informatico personale 3 in grado di comunicare col marcatore in lettura/scrittura e con l'infrastruttura informatica per lo scambio di dati.

In particolare, il marcatore 1 è in forma di un TAG RFID, per la precisione un TAG con tecnologia NFC che richiede una maggiore prossimità tra dispositivo di lettura/scrittura e TAG. Il marcatore 1 deve essere preferibilmente applicato sul prodotto di interesse con una modalità che renda evidenti eventuali manomissioni o rimozioni (tamper evident), così da rendere sostanzialmente univoca l'associazione tra marcatore 1 ed il relativo prodotto da proteggere rispetto alla contraffazione. L'infrastruttura informatica 2, come rappresentato in fig. 1, si compone essenzialmente di un server di comunicazione con una rete accessibile da remoto, per esempio la rete Internet, su cui risiede un database proprietario la cui gestione è affidata ad un ente certificatore, tipicamente (ma non necessariamente) terzo rispetto ai produttori di beni "consumer", ai soggetti coinvolti nella catena distributiva ed agli acquirenti. Il dispositivo informatico personale 3 possiede un'unità di comunicazione con l'infrastruttura informatica 2 ed una unità di lettura/scrittura del marcatore 1; esso è costituito tipicamente da uno smartphone o tablet o altro supporto informatico dotato di dette unità di comunicazione e lettura/scrittura e di un sistema operativo su cui sono installabili applicazioni

software.

Sul dispositivo informatico personale 3 è installata un'applicazione APP che è in grado di scambiare dati con l'infrastruttura informatica 2 e di leggere/scrivere dati da e su detto TAG NFC 1 mediante detta unità di lettura/scrittura.

Sul TAG NFC 1 è registrato, con modalità di per sé note nel settore degli RFID, almeno un codice variabile, eventualmente con una parte fissa CF ed una parte variabile dinamicamente CD, oppure un primo codice fisso CF ed un secondo codice variabile dinamicamente CD.

Si può anche realizzare il sistema utilizzando un codice composto da una parte fissa CF, che corrisponde allo stesso codice associato alla tipologia di prodotto ed al produttore, e da una parte variabile dinamicamente CD che sia un semplice codice casuale generato dal sistema remoto (con il vincolo di non poter mai assegnare un codice già in precedenza assegnato). I due codici del marcatore possono essere entrambi memorizzati nel medesimo TAG oppure possono essere di natura eterogenea: per esempio il codice fisso CF può essere un codice a barre applicato all'etichetta di prodotto ovvero un codice registrato nella memoria di un TAG READ-ONLY, mentre il codice variabile CD è registrato all'interno di un TAG riscrivibile in una determinata fase del processo di produzione (o di distribuzione o di vendita).

I dati relativi al prodotto (ad es nome del prodotto, proprietario, CF, CD,...) sono registrati all'interno del database messo in opera nel server dell'infrastruttura informatica 2, opportunamente protetto dagli accessi ed in cui è mantenuta la correlazione fra il codice variabile CD e gli altri dati dello specifico prodotto ovvero fra il codice fisso CF ed i dati ovvero fra il codice fisso CF ed il codice variabile CD ovvero tutte le correlazioni indicate.

Poichè il codice variabile dinamicamente CD viene modificato ad ogni verifica dell'assieme dei due codici CD+CF conclusa con esito positivo, parallelamente i dati del database vengono conformemente modificati. Preferibilmente nel database non viene semplicemente modificato il singolo record relativo a quel prodotto con il nuovo codice variabile CD, ma viene conservata tutta la sequenza di codici variabili CD utilizzata con quel corrispondente codice fisso CF e gli ulteriori dati aggiuntivi del marcatore, in un rispettivo numero di record; la sequenza temporale dei vari record permette di tener traccia della vita del marcatore e del prodotto ad esso associato, così da poter ricostruire anche - nel caso si indivi-

duassero dei tentativi di clonazione, a seguito di una mancata verifica di autenticità un codice variabile CD - la catena distributiva ed il rivenditore coinvolti nella circolazione del prodotto contraffatto.

La verifica di originalità viene effettuata, ad esempio, utilizzando uno smartphone in cui sia installato un software applicativo APP che interagisce con i codici fisso e variabile contenuti nel TAG RFID 1 e comunica con il database dell'infrastruttura informatica 2 attraverso protocolli di trasmissione dati sicuri.

Secondo una prima forma di esecuzione dell'invenzione (fig. 1), il software applicativo sul dispositivo 3 provvede ad effettuare una procedura di scambio dati che prevede una memorizzazione del nuovo codice identificativo all'esito positivo della verifica. Ossia, l'applicativo provvede inizialmente (i) ad interrogare il marcatore (con tecniche di per sè note) per (ii) ottenere il codice identificativo ID presente sul marcatore (il singolo codice memorizzato nel TAG RFID, oppure i due codici memorizzati nel TAG RFID, oppure ancora i codici eterogenei in parte nel TAG ed in parte visibili esternamente in forma di QR Code o codice a barre, per esempio) e (iii) lo comunica al database dell'infrastruttura di certificazione 2, verificandone la validità. Se la verifica sul database fornisce esito favorevole, ossia la composizione corrente del codice identificativo corrisponde a quanto memorizzato nel database, l'infrastruttura informatica 2 provvede a generare un nuovo codice identificativo ID1 - o meglio, la sua parte variabile dinamicamente CD1 - che associa nel database ai dati del rispettivo prodotto e lo trasmette (iv) all'applicazione del dispositivo 3 affinché (v) venga ritrasmesso al marcatore ed ivi memorizzato al posto del precedente. Se la procedura si conclude regolarmente, con la memorizzazione del nuovo codice identificativo ID1 nel TAG RFID 1, si determina (vi) un messaggio di buon fine ACK - per esempio a seguito di una serie di letture sequenziali del marcatore, finchè non si rilevi che il codice vecchio CD sia stato effettivamente sostituito con quello nuovo CD1 - che chiude la procedura di scambio dati.

Secondo una forma di esecuzione alternativa (fig. 2), la procedura di scambio dati prevede una memorizzazione del nuovo codice identificativo come operazione preliminare. Ossia, l'applicazione sul dispositivo 3 provvede inizialmente (i) a richiedere all'infrastruttura informatica 2 di generare ed associare un nuovo codice identificativo ID1 - o meglio, la sua parte variabile dinamicamente CD1 - a quel prodotto e poi (ii) inviarlo al dispositivo 3 che procede poi (iii) a trasmetterlo al marcatore per memorizzarlo, al posto del precedente codice identi-

cattivo ID che (iv) viene trasmesso indietro al dispositivo 3. Dopo conferma che la memorizzazione del nuovo codice ID1 è andata a buon fine, l'applicazione del dispositivo 3 provvede (v) a comunicare il codice identificativo ID, che aveva trovato residente sul marcatore 1, al database dell'infrastruttura di certificazione 2 per verificarne la validità. Se la verifica sul database fornisce esito favorevole, ossia la composizione corrente del codice identificativo corrisponde a quanto memorizzato nel database, l'infrastruttura 2 completa l'associazione del nuovo codice ID1 col prodotto e restituisce (vi) al dispositivo 3 un messaggio di buon fine che chiude la procedura di scambio dati.

Questa seconda forma di esecuzione presenta il pregio di limitare la finestra temporale che rimane aperta per lo scambio di dati con il TAG RFID, poichè la lettura e la memorizzazione dei nuovi dati avvengono in rapida sequenza: ciò è vantaggioso per evitare scambi irregolari di informazioni nelle frazioni di secondo in cui l'utente avvicina il proprio dispositivo mobile al marcatore del prodotto. Viceversa, la prima forma di esecuzione presenta una finestra temporale più ampia - perchè tra la lettura e la memorizzazione/scrittura del TAG avviene l'interrogazione del sistema informatico 2 e la generazione del nuovo codice - ma ha il pregio di generare un nuovo codice (con ciò che ne consegue in termini di risorse impiegate) solo nei casi in cui la verifica di validità sia andata a buon fine.

Secondo una terza forma di esecuzione alternativa rappresentata in fig. 3, il processo avviene in maniera del tutto simile alla prima forma di esecuzione descritta, sino al punto (vi) in cui viene determinato un messaggio di buon fine (ACK) dal marcatore 1. A questo punto però, a differenza della prima forma di esecuzione, il dispositivo informatico portatile 3 invia a sua volta (vii) un messaggio di riscontro (di buon o cattivo fine dell'operazione di scrittura nel marcatore 1) all'infrastruttura 2, la quale risponde (viii) con l'esito conclusivo dell'operazione con un messaggio di buona o cattiva fine che chiude lo scambio dati.

Questo terzo metodo permette di eliminare una vulnerabilità presente nel caso in cui si dovesse interrompere accidentalmente la procedura (per esempio per un guasto dell'unità di scrittura o del marcatore) tra le fasi (iv) e (v) della prima forma di esecuzione, nel qual caso si otterrebbe una situazione inconsistente tra le informazioni mantenute all'interno del marcatore 1 e le informazioni contenute all'interno dell'infrastruttura 2.

In ogni caso, l'esito della verifica viene mostrato all'utente sul dispositivo

informatico portatile 3, unitamente ad altre informazioni sul prodotto (per esempio tipologia, qualità, modalità di uso, prezzo suggerito ed altro) che siano sufficientemente interessanti per l'utente tanto da indurlo ad avvicinare il proprio dispositivo al marcatore ed eseguire il processo di verifica, a prescindere dalla conclusione di un atto di acquisto. E' infatti vantaggioso per la robustezza del sistema, che vengano effettuate una o più operazioni di verifica sul marcatore del prodotto, così che il codice identificativo univoco venga modificato e tracciato sul database dell'infrastruttura informatica 2 e si annullino sostanzialmente le possibilità di clonazione del marcatore.

Operativamente, il metodo anticontraffazione secondo l'invenzione ha il seguente funzionamento.

In fase di produzione, i prodotti originali vengono associati, in modalità che rendano evidenti eventuali manomissioni, a rispettivi marcatori dotati di un codice univoco ID del tipo descritto sopra. Contemporaneamente, nel database dell'infrastruttura informatica 2 i dati di ciascun prodotto originale (quale tipologia, colore, taglia ed altro) vengono memorizzati in relazione al codice identificativo ID del marcatore.

Si fornisce agli utenti un software applicativo APP, da installare in un dispositivo informatico personale, che è in grado di leggere/scrivere da e sul marcatore, nonché di comunicare da remoto con l'infrastruttura informatica di gestione e controllo 2.

Il codice identificativo del marcatore, o meglio la sua parte variabile dinamicamente, viene quindi modificato nel tempo ad ogni operazione di verifica, condotta lungo la filiera di distribuzione e/o dagli utenti/acquirenti finali mediante il software applicativo APP, in modo da renderlo di fatto irriproducibile. Ad ogni operazione di verifica, infatti, il codice univoco ID viene sostituito da un nuovo codice univoco ID1 generato casualmente o con altri criteri di fatto imprevedibili (per esempio connessi alle credenziali del dispositivo informatico personale che si collega alla infrastruttura informatica 2). Il codice univoco modificato ID1 viene memorizzato nel database e viene considerato il nuovo codice autentico.

Ad ogni operazione di verifica, il codice univoco letto nel marcatore viene confrontato con l'ultimo memorizzato come autentico nel database e, se il confronto fornisce un esito favorevole, viene fornita all'utente un'informazione di verifica di validità andata a buon fine. Nella stessa operazione di verifica vengono fornite all'utente anche altre informazioni utili sul prodotto.

Se il confronto fornisce un esito non favorevole, ossia non vi è corrispondenza tra il codice univoco appena letto dal marcatore e quello memorizzato come autentico nel database, all'utente viene fornita un'informazione corrispondente e viene generato un segnale di allerta nell'infrastruttura informatica di gestione e verifica 2. A seguito di questo evento, è possibile risalire al rivenditore che si trova in possesso del prodotto ritenuto falso, tramite informazioni che l'utente ha scelto deliberatamente di fornire tramite il software applicativo APP (per esempio sfruttando modalità compensative) oppure tramite tracciatura dei codici prodotto effettuata dal produttore.

Come si comprende dalla descrizione riportata sopra, con il sistema e metodo secondo l'invenzione si conseguono perfettamente gli scopi esposti nelle premesse.

Il metodo anticontraffazione è infatti configurabile a bassissimo costo, utilizzando TAG RFID riscrivibili (ma senza capacità di calcolo) di costo modesto, una infrastruttura informatica standard ed un dispositivo di verifica nella disponibilità degli utenti. Sfruttando poi le operazioni di verifica degli utenti, si rende di fatto irriproducibile il codice identificativo univoco dei marcatori proprio in corrispondenza della parte terminale della linea di distribuzione, ciò che rende possibile individuare i rivenditori coinvolti nell'acquisto di prodotti paralleli senza necessità di sgradevoli operazioni investigative.

Con il sistema secondo l'invenzione la probabilità di individuare casualmente il codice corretto, per ogni momento temporale della vita del prodotto, si riduce ad un valore prossimo allo zero; di conseguenza la possibilità di generare una serie di copie del codice variabile CD che siano verificabili con esito positivo risulta impossibile, rimanendo ciascun codice variabile CD valido unicamente sino alla successiva verifica effettuata con esito positivo ed essendo impossibile clonare di conseguenza il nuovo codice sulle eventuali copie create.

Ulteriormente, risulta possibile correlare in maniera univoca un oggetto con il relativo proprietario. Nel momento in cui viene identificata univocamente la proprietà di un oggetto, risulta anche possibile associare ad esso informazioni personali che possano essere utili eventualmente ad altre persone o che possono essere utilizzate nei più disparati usi. È possibile ad esempio aggiungere del testo ad un messaggio di verifica risultante dal controllo, es: "se ritrovate questo oggetto chiamate il numero xxx-xxxxx. Ricompensa".

Il concetto di proprietario risulta funzionale: ad esempio se una persona

ritrovasse l'oggetto, a meno di non rimuovere il marcatore e quindi manomettere il marchio di originalità, risulterebbe possedere un oggetto originale ma non di sua proprietà.

Con i marcatori può essere incentivato anche un uso sociale dei TAG, che va ben oltre il semplice controllo di originalità, ma che può esporre a potenziali complesse dinamiche sociali online e non.

Una possibile applicazione del sistema è anche quella di fornire un'alternativa alle prove d'acquisto.

Ancora, capita spesso che ad alcuni prodotti, esempio alimentari o medicinali, venga riciclata la data di scadenza ad esempio attaccando un'etichetta sopra all'originale. Vantaggiosamente, con il sistema proposto, se l'azienda decide che il proprio prodotto possiede una data di scadenza, è possibile avvertire l'acquirente - previa registrazione presso l'infrastruttura informatica - quando quello specifico prodotto è giunto a scadenza.

Ulteriormente, con questo sistema, riuscendo a certificare l'effettiva proprietà di un oggetto attribuendola ad una persona o società, è vantaggiosamente possibile fornire un servizio di garanzia per gli acquisti online tra privati o negozi e privati, certificando che tale persona o società possiede realmente il prodotto che dichiara di vendere, e che tale prodotto è originale e non una contraffazione. Vantaggiosamente ciò può aiutare a combattere il fenomeno delle truffe relative alla vendita di beni online.

Infine, si noti che il sistema dell'invenzione risponde puntualmente ai requisiti di robustezza:

1. Verificabilità: in qualunque momento, interrogando il database dell'infrastruttura remota di gestione e controllo 2, utilizzando la coppia CF+CD è possibile verificare tutto il flusso produttivo ed ulteriormente il flusso distributivo del prodotto;

2. Non generabilità: l'impossibilità di generare un codice corretto da parte di un "malintenzionato" è sostanzialmente legata alla possibilità di assimilare la codifica ad una generazione pseudo-casuale ed alla gestione dei codici tramite database remoto. Ossia non è possibile generare un codice valido senza inserirne il valore nell'infrastruttura remota di gestione e controllo 2; parallelamente, generare casualmente un codice che sia riconoscibile come valido ha una possibilità di riuscita prossima allo zero (dipendente dalla lunghezza del codice);

3. Non replicabilità: mentre il codice fisso CF definisce in maniera univoca

il prodotto, il codice variabile CD associato al codice fisso CF risulta ai fini della generazione un codice casuale: la possibilità di individuare casualmente un simile codice risulta talmente bassa da poter definire l'evento praticamente impossibile. Qualora un codice esistente venisse copiato su un diverso marcatore, la validità di tale codice cesserebbe di esistere alla successiva verifica o variazione di stato del prodotto: la copia prodotta non risulterebbe quindi più una copia valida e verificabile del codice, rendendo *de facto* il codice associato al prodotto non duplicabile.

4. *Verificabilità delle manomissioni*: essendo l'insieme di codice fisso CF e codice variabile CD un codice assimilabile ad un codice casuale, l'eventuale manomissione del codice variabile CD genererebbe un codice non presente nel database dei codici validi e la sua assenza nel database verifica quindi la manomissione del marcatore.

S'intende comunque che l'invenzione non è limitata alle particolari configurazioni illustrate sopra, che costituiscono solo degli esempi non limitativi della portata dell'invenzione, ma che numerose varianti sono possibili, tutte alla portata di un tecnico del ramo, senza per questo uscire dall'ambito dell'invenzione stessa.

RIVENDICAZIONI

1. Sistema anticontraffazione per prodotti consumer comprendente almeno un marcatore (1) da associare, in modalità da rendere evidente manomissione, ad un relativo prodotto e dotato di almeno un codice identificativo (ID),

un'infrastruttura informatica remota di gestione e controllo (2) dotata di un database in cui detto codice identificativo (ID) è memorizzato in relazione a dati identificativi di detto prodotto, ed

almeno un apparato di interfaccia fra detto marcatore (1) e detta infrastruttura informatica remota di gestione e controllo (2), caratterizzato da ciò che detto marcatore (1) comprende almeno un TAG RFID/NFC di tipo riscrivibile,

detto codice identificativo (ID) comprende almeno una parte variabile dinamicamente (CD) che viene modificata a seguito di un accesso in lettura a fini di verifica, e che

detto apparato di interfaccia è un dispositivo informatico personale (3) provvisto di un'unità di lettura/scrittura di TAG RFID/NFC mediante interfaccia wireless di prossimità e di una unità di comunicazione con una rete di trasmissione dati verso detta infrastruttura informatica remota (2),

su detto dispositivo informatico personale (3) essendo installato un software applicativo (APP) che provvede a trasferire dati da e per detto marcatore (1) tramite detta interfaccia wireless di prossimità e da e per detta infrastruttura informatica remota (2) mediante detta unità di comunicazione, e provvede a fornire una prima informazione di verifica, a seguito di confronto fra detto codice identificativo (ID) letto dal marcatore (1) e detto database, unitamente ad una seconda informazione di prodotto.

2. Sistema anticontraffazione come in 1, caratterizzato dal fatto che detta parte variabile dinamicamente (CD) del codice identificativo (ID) viene modificata a seguito di un accesso in lettura a fini di verifica solo a seguito di un esito favorevole di detta verifica.

3. Sistema anticontraffazione come in 1, caratterizzato dal fatto che detta parte variabile dinamicamente (CD) del codice identificativo (ID) viene modificata

in un nuovo codice identificativo (ID1) contestualmente ad un accesso in lettura a fini di verifica di detto codice identificativo (ID).

4. Sistema anticontraffazione come in 1, 2 o 3, in cui detto codice identificativo è composto da una parte fissa (CF) ed una parte variabile dinamicamente (CD).

5. Sistema anticontraffazione come in 1, 2 o, secondo una o più rivendicazioni precedenti, caratterizzato dal fatto che una parte del codice variabile dinamicamente (CD) rimane immutata durante la vita del prodotto.

6. Sistema anticontraffazione come in una qualsiasi delle rivendicazioni precedenti, in cui in detta infrastruttura informatica remota (2) si conserva traccia di una correlazione univoca dei dati di un prodotto con i dati di un proprietario.

7. Sistema anticontraffazione come in una qualsiasi delle rivendicazioni precedenti, in cui in detta infrastruttura informatica remota (2) sono conservate univocamente informazioni di prodotto in relazione a detto codice identificativo (ID).

8. Metodo anticontraffazione per prodotti consumer comprendente almeno un sistema come in una qualsiasi delle rivendicazioni precedenti in cui

un marcatore (1) comprendente almeno un TAG RFID/NFC di tipo riscrivibile viene dotato di almeno un codice identificativo univoco (ID) e viene associato, in modalità da rendere evidente manomissione, ad un relativo prodotto,

in un'infrastruttura informatica remota di gestione e controllo (2) dotata di un database, viene memorizzato detto codice identificativo univoco (ID) in relazione a dati identificativi di detto prodotto,

caratterizzato da ciò che

almeno una parte variabile dinamicamente (CD) di detto codice identificativo univoco (ID) viene modificata a seguito di un accesso in lettura a fini di verifica a detto marcatore (1) mediante un dispositivo informatico personale (3) provvisto di un'unità di lettura/scrittura di TAG RFID/NFC mediante interfaccia wireless di prossimità,

detto dispositivo informatico personale (3) scambiando prime informazioni di verifica e seconde informazioni di prodotto con detta infrastruttura informatica remota (2) mediante una unità di comunicazione con una rete di trasmissione dati,

detto dispositivo informatico personale (3) ricevendo inoltre dati generati

da detta infrastruttura informatica remota (2) per detta modifica di detta parte variabile dinamicamente (CD), ed in cui

detto dispositivo informatico personale (3) fornisce su un display dette prime informazioni di verifica e dette seconde informazioni di prodotto, le informazioni di verifica essendo tracciate anche in detto database dell'infrastruttura informatica remota (2).

9. Metodo come in 8, in cui viene preliminarmente letto detto codice identificativo univoco (ID) dal marcatore (1) e comunicato a detta infrastruttura informatica remota (2) per una verifica di validità, tramite confronto con dati memorizzati in detto database, e successivamente, ad esito positivo di detta verifica di validità, viene modificata detta parte variabile dinamicamente (CD) di detto codice identificativo univoco (ID) mediante rispettivi dati di modifica generati da detta infrastruttura informatica remota (2) e trasmessi a detto dispositivo informatico personale (3).

10. Metodo come in 8, in cui dati di modifica di detta parte variabile dinamicamente (CD) vengono preliminarmente generati da detta infrastruttura informatica remota (2) e trasmessi a detto dispositivo informatico personale (3), detta parte variabile dinamicamente (CD) di detto codice identificativo univoco (ID) venendo modificata contestualmente alla lettura a fini di verifica del marcatore (1) prima della successiva comunicazione del codice identificativo univoco (ID) a detta infrastruttura informatica remota (2) per una verifica di validità tramite confronto con dati memorizzati in detto database.

11. Metodo come in 9 o 10, una volta completata la modifica di detta parte variabile dinamicamente (CD) di detto codice identificativo univoco (ID), viene generato un segnale di buone fine (ACK) che viene ritrasmesso indietro da detto dispositivo informatico personale (3) a detta infrastruttura informatica remota (2) per una conclusione del processo di verifica.

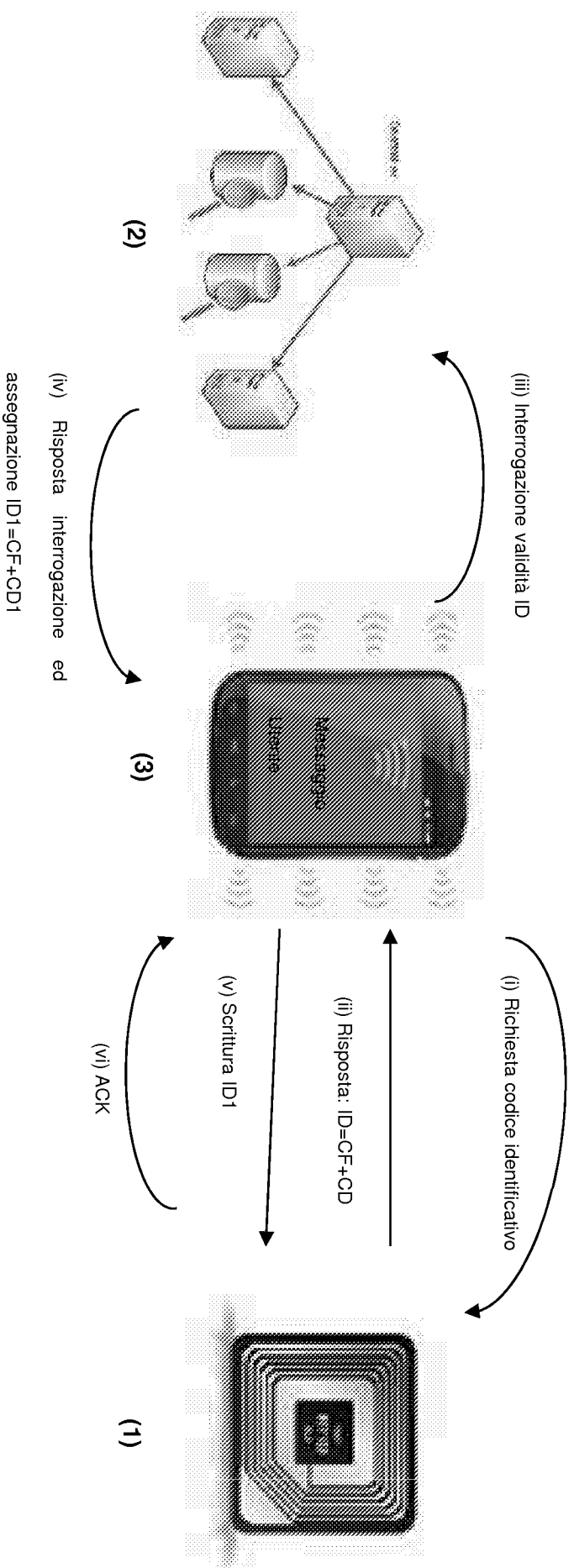


Fig. 1

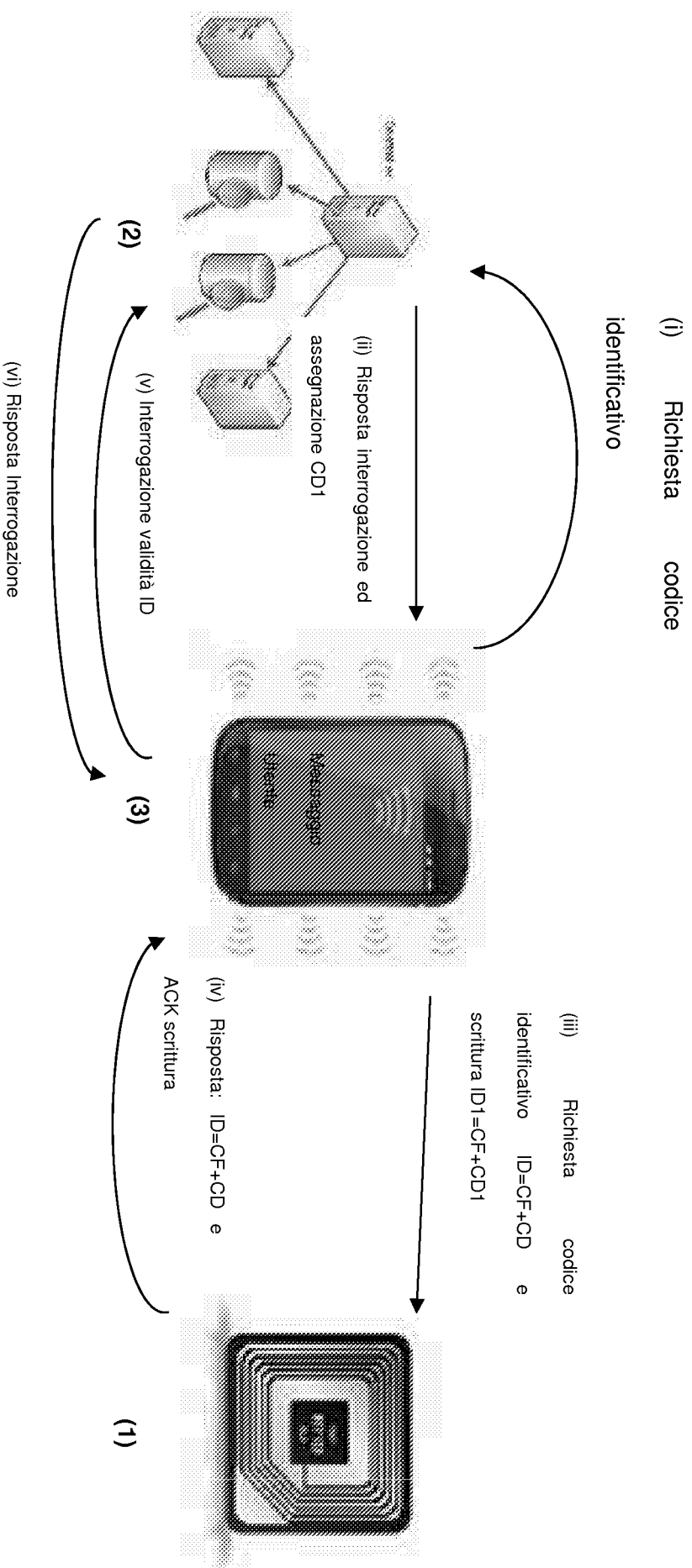


Fig. 2

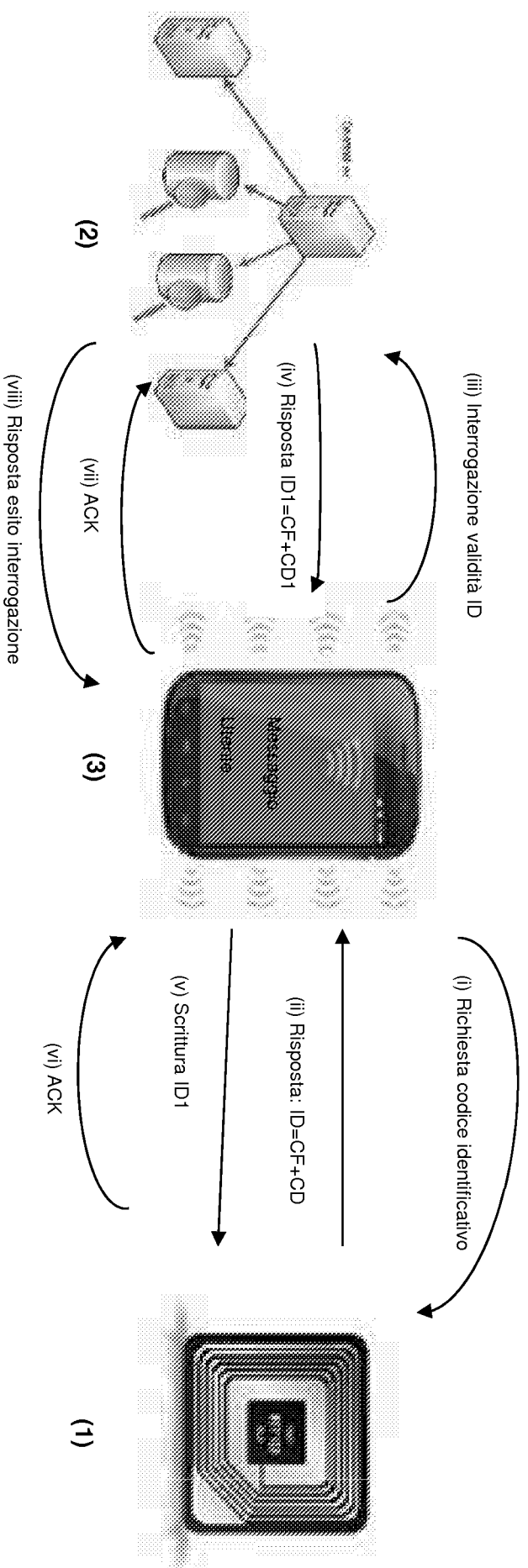


Fig. 3