SISTEMA E METODO DI RILEVAMENTO STRADALE

DESCRIZIONE

Campo tecnico dell'invenzione

La presente invenzione si riferisce ad un sistema e ad un metodo di ausilio alla gestione della mobilità per il rilevamento univoco e non ripudiabile del transito o della presenza di un utente e/o di un veicolo in corrispondenza di un tratto di rete stradale o di un varco di passaggio o di un'area di sosta. Il sistema funziona senza la necessità di stabilire una comunicazione bidirezionale tra dispositivi a lato-infrastruttura e dispositivi mobili dell'utente e/o del veicolo.

Background

Nel campo della mobilità veicolare, la gran parte dei sistemi per il rilevamento degli accessi e dei transiti implementati dalle autorità dei trasporti o dai gestori di sistemi o servizi di trasporto è basata sul riconoscimento dei veicoli. Spesso, tale riconoscimento prevede una associazione tra il veicolo rilevato ed una persona fisica, ad esempio il proprietario oppure un utente/viaggiatore del veicolo stesso. Tale associazione è generalmente gestita tramite la registrazione in una banca dati.

Esempi in tale senso sono i sistemi di controllo degli accessi, che sono basati sull'utilizzo di banche dati o liste di veicoli, ammessi o non ammessi all'accesso in determinate aree, essendo tale ammissibilità in realtà condizionata a caratteristiche di cui è titolare l'utente associato al veicolo, quali ad esempio la residenza.

Altri esempi sono servizi di concessione o limitazione dei permessi di sosta per residenti o per categorie particolari di persone (ad esempio portatori di handicap), nei quali avviene la pre-registrazione delle targhe delle vettura abilitate (in funzione dei diritti o delle caratteristiche della persona fisica o giuridica che registra la vettura e, spesso, in funzione dello stesso titolo di possesso della vettura). In altri casi, il veicolo è soggetto a tariffazione del transito (o della sosta) in funzione dell'identificazione del veicolo stesso; tale tariffa è addebitata ad una persona fisica (o giuridica) attraverso un meccanismo di associazione del veicolo.

Uno svantaggio della tecnica nota è che, nella maggior parte dei casi, l'associazione di persone (fisiche o giuridiche) ad un veicolo viene effettuata in maniera statica o quasi statica, ovvero non modificabile o modificabile con procedure che debbano essere

effettuate preventivamente ed off-line, con un non trascurabile anticipo rispetto al momento della fruizione del servizio.

Le cause di tali difficoltà risiedono principalmente nella necessità di procedere alla determinazione certa, univoca, non ripudiabile e non soggetta a inganni o truffe della identità della persona la cui titolarità di diritti viene trasferita al veicolo registrato.

Altro svantaggio della tecnica nota è quello di non potere facilmente, con un unico mezzo, identificare uno stesso viaggiatore anche quando egli non utilizzi un mezzo registrato per l'effettuazione dei propri spostamenti. Tale svantaggio si estende non solo all'utilizzo di mezzi non registrati ma anche all'utilizzo di modalità di trasporto collettive (servizi di bus, metropolitana, ecc.) o al semplice utilizzo della modalità pedonale. Ne risulta la difficoltà di gestire unitariamente e congruentemente politiche di gestione della mobilità multimodale che siano centrate sul viaggiatore e non sulle modalità di trasporto.

Ulteriore svantaggio della tecnica nota, da un punto di vista tecnologico, collegato al caso in cui l'identificazione dei veicoli avvenga tramite OBU (On Board Unit), è quello di necessitare di una comunicazione bidirezionale a corto-medio raggio tra la OBU sul veicolo e gli apparati di bordo-strada, per stabilire la quale è spesso necessario realizzare portali, canalizzazioni e regolazioni della velocità di transito.

Sommario dell'invenzione

Pertanto, il problema tecnico posto e risolto dalla presente invenzione è di fornire un sistema e un metodo, che consentano di ovviare agli inconvenienti sopra menzionati con riferimento alla tecnica nota.

Tale problema viene risolto da un sistema secondo la rivendicazione 1 ed un metodo secondo la rivendicazione 14.

Caratteristiche preferite della presente invenzione sono presenti nelle rivendicazioni dipendenti della stessa.

Vantaggiosamente, il sistema secondo la presente invenzione consente l'identificazione univoca e non ripudiabile di un viaggiatore in corrispondenza di una localizzazione nota (ad esempio un mezzo, un terminale, o un varco di accesso) ad un determinato istante di tempo, anche esso noto ed identificato in maniera univoca e non ripudiabile.

La presente invenzione consente inoltre un'identificazione univoca e non ripudiabile di

un'associazione tra un utente e un veicolo utilizzato dall'utente stesso per compiere uno spostamento, sia nel caso di veicolo proprio che nel caso di veicolo noleggiato a medio/breve termine e/o preso in car-sharing e/o semplicemente in prestito, con identificazione del luogo e del tempo in cui tale associazione viene rilevata.

Un ulteriore vantaggio è che il sistema secondo la presente invenzione prevede un controllo non ripudiabile degli accessi in corrispondenza di uno spazio predefinito prevenendo eventuali contestazioni da parte dell'utente utilizzatore del servizio.

Lo scopo della innovazione introdotta è quello di permettere la associazione rapida e non ripudiabile, con potenziale valore legale (ove utile), di utenti/viaggiatori a veicoli (anche non di loro proprietà), senza la necessità di mantenere registri e con la possibilità di determinare l'associazione in maniera temporanea e solo per il tempo necessario alla fruizione di un servizio o di un permesso di mobilità.

Il tutto avviene senza la necessità di una comunicazione bidirezionale tra dispositivi personali e/o di bordo-veicolo e dispositivi lato-infrastruttura, giacché l'invenzione rende sufficiente una comunicazione di tipo broadcast da parte dei dispositivi lato-infrastruttura.

Inoltre, l'invenzione proposta permette la conservazione da parte dell'utente della prova di passaggio/presenza dell'utente stesso ed eventualmente del veicolo, in modo che essa possa essere utilizzata per scopi successivi e/o possa essere inviata anche con ritardo alla centrale di controllo necessaria per la gestione del sistema.

Vantaggiosamente il trovato secondo l'invenzione consente di:

- abilitare una applicazione di politiche di controllo della mobilità stradale incentrata sulle persone e non sui mezzi (veicoli);
- rendere il più possibile trasparente al sistema di rilevamento i mezzi/veicoli di volta in volta utilizzati dagli utenti per il soddisfacimento della mobilità;
- rendere così il più possibile elastico ed estemporaneo per gli utenti l'utilizzo di un veicolo per la fruizione di diritti o permessi di mobilità di cui sono i reali beneficiari, non essendone beneficiari, nella maggior parte dei casi, i veicoli utilizzati;
- mantenere la possibilità di associare determinati e specifici permessi anche al veicolo, ad esempio nel caso di accesso o diniego al transito in funzione della classe di emissioni o della tipologia di motorizzazione (es.: Euro5, veicoli a zero-emissioni, ecc.);
- minimizzare l'impegno ed il costo per la manutenzione di registri di associazione utenti-veicoli (black-list, white-list, ecc.);

- massimizzare la robustezza della associazione tra veicoli e viaggiatori rispetto ad aspetti legali, compresa la certezza della associazione in termini di identificazione non ripudiabile del soggetto fisico e giuridico che effettua gli spostamenti;
- massimizzare il ricorso a soluzioni di certificazione della identità già disponibili e reperibili (firme digitali, firme digitali remote, ecc.);
- massimizzare la congruenza con strumenti digitali promossi a livello locale e nazionale della legislazione e dagli indirizzi correnti di digitalizzazione della pubblica amministrazione e dei rapporti tra istituzioni, cittadini ed imprese (ad esempio, Carte di Identità Elettroniche, Carte Nazionali dei Servizi, ecc.), soprattutto in considerazione del fatto che la gestione della mobilità, dei relativi permessi e delle relative tariffe è spesso direttamente in capo ad amministrazione pubbliche o, comunque, esercita per concessione o contratto di servizio stipulato con tali amministrazioni.

L'innovazione è anche in grado di permettere applicazioni al contesto della mobilità pubblica/collettiva. Infatti, l'innovazione è in grado di rilevare in maniera univoca e non ripudiabile la presenza di un viaggiatore in un determinato luogo predefinito ed ad una determinata ora (es.: stazionamento o fermata di trasporto collettivo, mezzo di trasporto collettivo, piattaforma di accesso ad un servizio metropolitano, ecc.). In tale modo è possibile abilitare sistemi di accredito ed addebito di tariffe di trasporto (e più in generale di servizio di mobilità) alternative al possesso di un titolo di viaggio o di servizio, anche gestibili su piattaforme remote e/o centralizzate.

Tale opportunità permette, tra l'altro, la gestione innovativa della mobilità multimodale, basata sulla eventuale contabilizzazione, anche trasferibile da un modo di trasporto all'altro, della aliquota e delle caratteristiche di spostamento effettuate con il sistema di trasporto privato e con il sistema di trasporto pubblico/collettivo.

Caratteristiche salienti dell'invenzione sono quelle di permettere il rilievo di passeggeri e/o veicoli anche senza la predisposizione di varchi di accesso o corsie o canalizzazioni particolari e stabilendo tra i mezzi di rilievo ed i mezzi a bordo vettura (o i mezzi personali del viaggiatore) una comunicazione unidirezionale e non bidirezionale.

Altri vantaggi e caratteristiche, nonché le modalità di impiego, della presente

invenzione risulteranno evidenti dalla seguente descrizione dettagliata di alcune forme di realizzazione, presentate a scopo esemplificativo e non limitativo.

Descrizione breve delle figure

Verrà fatto riferimento alle figure dei disegni allegati, in cui:

- la Figura 1 mostra una prima forma di realizzazione preferita del sistema secondo la presente invenzione, detta di “massima dematerializzazione”;
- la Figura 2 mostra una seconda forma di realizzazione preferita del sistema secondo la presente invenzione, detta a “automazione semplice”;
- la Figura 3 mostra una terza forma di realizzazione preferita del sistema secondo la presente invenzione, detta a “automazione totale”;
- la Figura 4 mostra un diagramma schematico della struttura di un messaggio generato da un dispositivo;
- la Figura 5 mostra un diagramma a blocchi schematico dell’architettura logica di un componente del sistema di Figura 1 e 2;
- la Figura 6 mostra un diagramma a blocchi schematico dell’architettura logica di un componente del sistema di Figura 2 e 3.

Descrizione dettagliata di forme di realizzazione preferite

Con riferimento inizialmente alla figura 1, il sistema secondo una prima forma di realizzazione preferita dell’invenzione è complessivamente denotato con 10.

Il sistema 10 per il rilevamento del transito o della presenza di un utente e/o di un veicolo in corrispondenza di una rete stradale, di un varco di passaggio o di un’area di sosta, comprende almeno un dispositivo marcatore “lato-infrastruttura” 1, posizionato o posizionabile in corrispondenza di una determinata localizzazione nota. Il sistema 10 prevede inoltre almeno un dispositivo di identificazione “lato-utente” 2, mobile con l’utente che effettua lo spostamento.

Il dispositivo di rilevamento “lato-infrastruttura” 1 presenta primi mezzi di elaborazione per la generazione di primi dati crittografati atti a rendere univoca e non ripudiabile

l'identificazione del dispositivo stesso e primi mezzi trasmittenti per la trasmissione dei primi dati crittografati generati.

Vantaggiosamente, il dispositivo di identificazione "lato-utente" 2 presenta mezzi riceventi atti a ricevere i primi dati crittografati, ad esempio un messaggio, e mezzi di interfaccia per l'acquisizione di dati identificativi dell'utente e/o del veicolo. In tutte le forme realizzative inoltre il dispositivo "lato-utente" 2 comprende secondi mezzi di elaborazione per la generazione di secondi dati crittografati, consistenti in un ulteriore messaggio, includente il primo, atto a rendere univoci e non ripudiabili i dati identificativi acquisiti e secondi mezzi trasmittenti per la trasmissione dei secondi dati crittografati ad una centrale operativa remota.

La centrale operativa remota indicata come (OC) nelle Figure 1 e 2 comprende mezzi per la decrittografazione dei primi e secondi dati crittografati e quindi per la verifica dei dati identificativi del dispositivo marcatore, dell'utente e/o del veicolo in maniera tale da rilevare in maniera univoca e non ripudiabile il transito o la presenza dell'utente e/o del veicolo in prossimità di un determinato dispositivo marcatore, anche esso univocamente e non ripudiabilmente identificato.

Nel presente esempio, i primi mezzi di elaborazione comprendono dispositivi di tipo "embedded". In particolare, il dispositivo marcatore lato-infrastruttura 1 è realizzato come soluzione embedded costituita da opportuni microchip, schede di memoria, schede integrate, schede e porte di comunicazione, antenne, circuitazioni elettriche, sistemi di alimentazione, logiche e procedure, tutte orientate alla automatizzazione della generazione, gestione e trasmissione di messaggi crittografati, opportunamente codificati e strutturati, finalizzati ad essere ricevuti da veicoli e/o utenti transitanti o stazionanti nel raggio di trasmissione del dispositivo stesso. I messaggi sono finalizzati a testimoniare in maniera univocamente identificata e non ripudiabile il transito o lo stazionamento dei veicoli e/o dei viaggiatori nel raggio di azione del dispositivo stesso. Allo scopo, il dispositivo marcatore 1 realizza al suo interno la gestione di una smart-card (od altra opportuna ed equivalente soluzione) idonea a implementare un meccanismo di firma digitale basato su crittografia asimmetrica. Inoltre, il dispositivo è a conoscenza della chiave di cifratura pubblica di un apposito dispositivo remoto di tipo embedded di verifica, dislocato presso la centrale operativa OC (server-side).

Il dispositivo marcatore lato-infrastruttura 1, realizza in tecnologia embedded le

funzioni di:

- generazione automatica di un messaggio, secondo opportuni contenuti specificati nel seguito;

- firma digitale del messaggio, congruentemente con tecniche a crittografia asimmetrica e generazione dell'impronta di messaggio (digest) con algoritmo di Hash, secondo la modalità:

  - generazione della impronta del messaggio (digest) con algoritmo di Hash, implementato in modalità embedded; l'algoritmo è di tipo SHA-256, il dispositivo marcatore 1 è realizzato in maniera che il firmware sia aggiornabile in seguito per l'utilizzo di algoritmi per la generazione del digest più avanzati (es.: SHA-512, oppure algoritmi a 1024 bit);
  - crittografia del digest utilizzando la chiave privata di cifratura del dispositivo marcatore lato-infrastruttura 1 stesso;
  - crittografia del messaggio in chiaro e del digest crittografato, utilizzando la chiave pubblica del dispositivo remoto di verifica presso la centrale operativa OC;

- il messaggio crittografato finale ottenuto, unitamente all'indirizzo del dispositivo remoto di verifica presso la centrale operativa OC ed alla chiave crittografica pubblica di detto dispositivo remoto, viene trasmesso dal dispositivo marcatore 1 con continuità, in modalità tale da potere essere ricevuto da qualsiasi dispositivo ricevente passante nel raggio di azione. La trasmissione avviene:

  - con tecnologie basata su specifica ZigBee (o XBee) e protocollo 802.15.4;
  - in contemporanea od in alternativa alla precedente, in modalità WiFi con protocollo 802.11a/b/g/n e successive evoluzioni (o, in alternativa, con protocollo 802.11p);
  - in contemporanea o in alternativa alla precedente, in modalità Bluetooth.

- il raggio di azione del dispositivo marcatore 1 è regolabile intervenendo, anche in modalità remota, sul firmware in un intervallo inferiore ai 100 metri, nel funzionamento ordinario tale intervallo è compreso tra 1 metro e 30 metri;

- la generazione di un nuovo messaggio da parte del dispositivo marcatore lato-infrastruttura 1 è aggiornata con una frequenza (fr) variabile (e settabile intervenendo,

anche in modalità remota, sul firmware) tra 5Hz ed uno ogni 120 secondi; ad ogni aggiornamento viene modificata una parte del contenuto informativo, con particolare riferimento al periodo temporale di generazione del messaggio;

- può essere richiesto al dispositivo marcatore lato-infrastruttura 1 l'aggiornamento del messaggio anche attraverso l'invio dall'esterno di un opportuno segnale di trigger; qualsiasi messaggio, appena generato o aggiornato, viene immediatamente trasmesso con continuità in modo da potere essere ricevuto da qualsiasi dispositivo ricevente nel raggio di azione.

La struttura di un messaggio generato dal dispositivo marcatore "lato-infrastruttura" 1, ovvero di un esempio realizzativo dei suddetti primi dati crittografati, è mostrata in Figura 4. Per quanto concerne le modalità di confezionamento e trasporto del messaggio, si fa riferimento alla tecnica nota ed in particolare al protocollo TCP-IP. Con riferimento alla Figura 4, la marca temporale (*timestamp*) del messaggio che varia con una frequenza f_r, comprende:

- il giorno, mese ed anno (ggmmaaaa) di generazione del messaggio;

- l'ora, i minuti ed i secondi (hhmmss) dell'orario di generazione del messaggio;

- i millisecondi (mmm) dell'orario di generazione del messaggio, generalmente questa quantità non è utile dal punto di vista applicativo e viene posta pari a valore nullo (000).

Il corpo del messaggio è, una volta data la localizzazione e la funzione del dispositivo marcatore lato-infrastruttura 1 all'interno del sistema di gestione e controllo della mobilità, fisso. Esso si compone di informazioni che per la maggior parte vengono predisposte in fabbrica o settate in fase di installazione in loco del dispositivo (ed eventualmente successivamente aggiornate, attraverso interventi remoti o locali, protetti ed autorizzati, sul firmware del dispositivo), ad esempio:

- TP_Device = Tipologia del dispositivo; ad esempio, "Dispositivo marcatore Lato-infrastruttura";
- ID_Device = Identificativo Univoco del dispositivo marcatore; ad esempio, "RS_XXX";
- MAC_ZigBee = MAC Address della scheda di comunicazione ZigBee (o XBee) installata nel dispositivo marcatore lato-infrastruttura 1;

- MAC_WiFi = MAC Address della scheda di comunicazione 802.11a/b/g/n e successive evoluzioni (o 802.11p) installata nel dispositivo marcatore lato-infrastruttura 1;
- MAC_BT = MAC Address della scheda di comunicazione Bluetooth installata nel dispositivo marcatore lato-infrastruttura 1;
- Localizzazione = Descrittivo della localizzazione del dispositivo; ad esempio, “Ingresso ZTL Centro Antico, varco 12”;
- LAT = Latitudine della localizzazione del dispositivo marcatore;
- LONG = Longitudine della localizzazione del dispositivo marcatore;
- Servizio = Tipologia di servizio cui il dispositivo marcatore è dedicato; ad esempio “identificazione veicoli in ingresso ZTL”;
- Altri campi opzionali.

Il dispositivo marcatore “lato-infrastruttura” è, inoltre, equipaggiato con le seguenti porte di comunicazione con dispositivo esterni:

- Porta di comunicazione seriale RS232;
- Porta di ingresso per segnali di trigger/sincronizzazione (hanno effetto sulla frequenza di aggiornamento del messaggio, che può essere sincronizzata con altri dispositivi esterni e/o gestita “ad evento”);
- Porta di ingresso USB veloce per acquisizione immagini bitmap e vettoriali compresse (file di medio/piccole dimensioni);
- Porta di ingresso (RJ45) e scheda di interfaccia di rete per acquisizione pacchetti dati in protocollo TCP/IP e scambio dati bidirezionale LAN/WAN;
- Porte di Input/output di tipo analogico; e/o
- Porte di Input/output di tipo digitale.

In particolare, il dispositivo marcatore “lato-infrastruttura” 1 è contenuto in un involucro (*case*) con grado di protezione almeno IP65 ed è installabile all’aperto ed in una qualsiasi delle seguenti posizioni:

- Sopra la strada (o area per il passaggio dei veicoli o area di ingresso a

stazionamenti, sosta, fermate, terminali, ecc.);

- A lato-strada (o area per il passaggio dei veicoli o area di ingresso a stazionamenti, sosta, fermate, terminali, ecc.);
- Nelle immediate adiacenze della strada (o area per il passaggio dei veicoli o area di ingresso a stazionamenti, sosta, fermate, terminali, ecc.).

Vantaggiosamente, non sono necessarie particolari cautele in termini di installazione. E' importante solo che la trasmissione sia ricevibile ove, a seconda della applicazione di controllo/gestione della mobilità da implementare, è necessario distribuire il messaggio. Ove il messaggio raggiunga e sia acquisito anche da dispositivi riceventi non interessati alla applicazione o non sotto l'influenza del dispositivo marcatore lato-infrastruttura 1 che lo ha emesso, non si genera alcuna eccezione di funzionamento, il messaggio può essere ignorato e la non-gestione dell'evento è facilmente governabile via software. È comunque il caso di limitare in maniera appropriata, allo scopo di tenere sotto controllo il traffico di rete ed il carico di elaborazione complessivo del sistema, la potenza del segnale di trasmissione, in tale modo il minore numero possibile di dispositivi riceventi non interessati riceve inutilmente il messaggio.

Il dispositivo marcatore lato-infrastruttura 1 è alimentabile sia da rete elettrica che da sistemi ad energie rinnovabili e batterie di accumulo/tamponamento. Ciò è permesso dalle limitate esigenze energetiche del dispositivo, le maggiori delle quali legate alla trasmissione dei messaggi in modalità wireless.

La scelta degli specifici componenti del sistema permette di ridurre al minimo i consumi energetici, come permesso dalla specifica ZigBee (XBee) di implementazione dello standard 802.15.4 e dallo standard Bluetooth, entrambi a richieste energetiche basse o medio-basse. Il funzionamento a basso consumo, può essere favorito degradando via software la modalità di trasmissione, disabilitando la trasmissione 802.11x (WiFi). Il dispositivo marcatore lato-infrastruttura 1, ove installato e funzionante, è preferibilmente associato a segnalazioni opportune per gli utenti, ad esempio cartellonistica stradale atta a notificare il passaggio in una area sottoposta a politiche di controllo/gestione della mobilità ed atte a indicare la necessità di tenere accesi ed attivi i dispositivi necessari per la applicazione implementata (tipicamente smartphone o altro dispositivi personale di comunicazione e, per alcune forme realizzative descritte di seguito, un dispositivo processore 3 specifico personale).

In figura 5 è mostrato il diagramma schematico dell'architettura logica del dispositivo

marcatore “lato-infrastruttura” 1 secondo la forma di realizzazione preferita della presente invenzione.

Preferibilmente, anche i secondi mezzi di elaborazione comprendono dispositivi di tipo “embedded”. Nella prima forma di realizzazione preferita, come schematizzata in figura 1, il dispositivo di identificazione “lato-utente” comprende uno smartphone e/o un tablet 2 (anche indicato nel seguito come *dispositivo di comunicazione personale*).

Come sarà meglio descritto nel seguito, nella prima forma di realizzazione, l’utente e/o il veicolo potrà/potranno essere identificato/i unicamente tramite l’utilizzo di una applicazione gestita da uno smartphone e/o un tablet 2.

In una seconda forma di realizzazione preferita, come schematizzata in figura 2, il dispositivo di identificazione “lato-utente” 20 comprende inoltre un dispositivo processore 3 (indicato nel seguito come *DSP - Dispositivo Specifico Personale*) atto a processare dati digitali, associato o associabile in maniera univoca allo smartphone e/o tablet 2.

Come sarà descritto meglio in seguito con riferimento alle modalità di funzionamento del sistema nelle sue forme di realizzazione preferite, il dispositivo processore 3 comprende ulteriori mezzi riceventi atti a ricevere i suddetti primi dati crittografati.

In particolare, i primi dati crittografati sono inviati sotto forma di messaggi dai dispositivi marcatori lato-infrastruttura 1 e vengono ricevuti dai veicoli/viaggiatori transitati o stazionanti nel raggio di trasmissione dei dispositivi stessi.

Come sarà meglio descritto nel seguito con riferimento alle specifiche forme di realizzazione preferite, la ricezione può avvenire da parte di un dispositivo di comunicazione personale 2 (smartphone/tablet o similare) sul quale sia attiva la applicazione di fruizione del servizio di controllo della mobilità implementata, oppure da un DSP 3, a sua volta associato con un dispositivo di comunicazione personale 2 sul quale sia attiva la applicazione. In particolare, il dispositivo di comunicazione personale 2 può ricevere il messaggio dal dispositivo marcatore lato-infrastruttura 1 mediante Bluetooth o WiFi (802.11.abgn/p). Preferibilmente, il DSP 3 riceve il messaggio dal

dispositivo lato-infrastruttura 1 mediante 802.15.4 (ZegBee o XBee), oppure 802.11p. Nel caso la ricezione del messaggio avvenga sia tramite DSP 3 che tramite il dispositivo di comunicazione personale 2 ad esso associato, il DSP 3 prevale sul dispositivo di comunicazione 2 come sarà dettagliato meglio a seguire.

In particolare, nella prima forma di realizzazione preferita (*cosiddetta modalità di massima dematerializzazione*), che prevede l'utilizzo esclusivo dei dispositivi di comunicazione 2 come dispositivo "lato-utente", uno o più degli smartphone/tablet 2 (o similari) presenti a bordo del veicolo ricevono il messaggio dal dispositivo lato-infrastruttura 1. Tra questi, uno è quello che accrediterà l'utente/viaggiatore che intende usufruire del servizio o permesso di mobilità gestito dal dispositivo lato-infrastruttura. Su indicazioni della apposita applicazione e guidato in maniera da rendere l'operazione pratica ed estremamente rapida, l'utente sarà invitato ad accreditarsi (eventualmente insieme al veicolo digitato o rilevato) quale effettivo titolare del permesso o titolo di transito/viaggio, nonché ad accreditarsi quale fruitore del servizio di mobilità gestito dal dispositivo lato-infrastruttura. A tale scopo, l'utente utilizzerà il dispositivo personale di comunicazione 2 per digitare quanto richiesto e per utilizzare la propria firma digitale remota, preferibilmente implementate tramite OTP (One-Time Password) gestita attraverso token. In particolare, la applicazione sul dispositivo personale di comunicazione 2 provvederà a formare un messaggio, ovvero un esempio realizzativo dei suddetti secondi dati crittografati, contenente:

- una marca temporale (*timestamp*), a sua volta articolata in:
  - giorno, mese ed anno (ggmmaaaa) di generazione del messaggio;
  - ora, minuti ed secondi (hhmmss) dell'orario di generazione del messaggio;
  - millisecondi (mmm) dell'orario di generazione del messaggio, generalmente questa quantità non è utile dal punto di vista applicativo e viene posta pari a valore nullo (000).
- un corpo del messaggio, a sua volta articolato in:
  - identificativo dell'utente/viaggiatore;
  - campo a valore convenzionale (es.: 0000) che identifica il fatto non sia utilizzato un DPS 3 (*cosiddetta modalità di massima dematerializzazione*);
  - numero di targa del veicolo, come asseverato dall'utente/viaggiatore;

- indicazione dell'impiego di *massima dematerializzazione* (es.: variabile intera a valore 0);

- un allegato al messaggio consistente nel messaggio crittografato ricevuto dal dispositivo marcatore lato-infrastruttura 1.

L'operazione di firma consiste ad esempio nel produrre il digest del precedente messaggio, nel crittografare tale digest con la chiave privata collegata alla firma digitale remota dell'utente/viaggiatore, nel crittografare messaggio e digest con la chiave pubblica del dispositivo remoto di verifica presso la centrale operativa OC. Il messaggio crittografato ottenuto viene spedito il prima possibile dal dispositivo personale di comunicazione (smartphone/tablet o similare) verso il dispositivo remoto di verifica presso la centrale operativa OC utilizzando le tecnologie ed i provider di comunicazione fruibili sul dispositivo personale di comunicazione ed un canale di trasmissione certificata (es.: provider di PEC – posta elettronica certificata). Eventuali ritardi in tale trasmissione, ad esempio dovuti a momentanea assenza del segnale di comunicazione, possono essere gestiti a livello procedurale con comportamenti di ravvedimento operoso da parte dei viaggiatori/utenti, ad esempio prima che la procedura lato-server collegata al dispositivo remoto di verifica presso la centrale operativa OC ed i meccanismi di controllo e sanzionatori siano giunti a livello di emissione della notifica di sanzione. Il ravvedimento operoso è reso possibile dalla applicazione gestita dal dispositivo personale di comunicazione, che conserva tutti i messaggi che non sia stata in grado di spedire al dispositivo remoto di verifica presso la centrale operativa OC (e/o per la cui spedizione non abbia ricevuto conferma di recapito, come sarà descritto meglio nel seguito).

Nella seconda (*cosiddetta modalità automatizzata semplice)* e nella terza (*cosiddetta modalità automatizzata totale*) forma di realizzazione preferita, che prevedono l'utilizzo del dispositivo processore 3 DSP in associazione con un dispositivo di comunicazione 2, il messaggio dal dispositivo marcatore lato-infrastruttura 1 viene ricevuto dal DSP 3, contemporaneamente, qualsiasi dispositivo smartphone/tablet (o similare) che riceva il messaggio deve essere utilizzato, in tale forma realizzativa, in maniera da ignorare quanto ricevuto.

Preferibilmente, il dispositivo processore DSP 3 ha le seguenti caratteristiche:

- è di dimensioni e peso ridotti (minori di uno smartphone);
- è alimentato autonomamente con una batteria sostituibile di piccole dimensioni, di durata prolungata, ricaricabile; la batteria può essere ricaricata via porta USB, a sua volta alimentata da PC/notebook, alimentatore esterno, accumulatore portatile di energia;
- allo scopo di salvaguardare la durata della batteria, è dotato di un sistema di accensione/spegnimento attivato dall'utente (bottone); l'accessione è segnalata da un led di colore rosso;
- è in grado di associarsi ad uno smartphone/tablet (o similare) in modalità Bluetooth; la associazione è guidata dalla applicazione residente sullo smartphone/tablet, la corretta associazione con il dispositivo è segnalata dal colore verde di un led di accensione;
- prevede mezzi di interfaccia, ad esempio almeno due terminali per la lettura di smartcard e/o la lettura di token USB con funzione equivalente, allo scopo di gestire l'identificazione personale ed eventualmente del veicolo, come sarà descritto meglio nel seguito; un ulteriore led assume i colori rosso, giallo e verde a seconda che: i) non sia stata possibile la corretta lettura di credenziale identificativa (né personale né del veicolo); ii) sia stata possibile la corretta lettura della sola credenziale identificativa della persona (modalità di automazione semplice); iii) sia stata possibile la lettura sia delle credenziali della persona sia di quelle del veicolo (modalità di automazione totale);
- è in grado di comunicare secondo lo standard 802.15.4 e la specifica ZigBee (o XBee).

Ad esempio, in Figura 6 è mostrato uno schema della architettura logica preferita del dispositivo personale 3.

La logica integrata (*embedded*) nel dispositivo 3 implementa il seguente meccanismo:

- il DSP 3 riceve dal dispositivo marcatore lato-infrastruttura 1 il messaggio cifrato strutturato, già descritto nel paragrafo precedente;

- il DPS 3 richiede ad una smart-card 4/5 identificativa dell'utente/viaggiatore (eventualmente inserita in un token USB) i dati di identificazione riportati del certificato

pubblico di identificazione;

- nella seconda forma realizzativa preferita (*modalità automatizzata semplice*), come mostrata in Figura 2, ove la applicazione di gestione della domanda implementata prevede l'utilizzo di un veicolo, il DPS 3 richiede allo smartphone (o tablet/iPhone/iPad, o similare) cui è associato il numero di targa del veicolo da associare, digitata in precedenza sotto la responsabilità dell'utente/viaggiatore;

- nella terza forma di realizzazione preferita (*modalità automatizzata totale*), come mostrata in Figura 3, il DPS 3 richiede ad una smart-card 5 identificativa del veicolo (eventualmente inserita in un token USB) i dati di identificazione (es.: numero di targa);

- sia nella seconda che nella terza forma di realizzazione preferita, il DPS 3 genera un nuovo messaggio contenente:

  - una marca temporale (timestamp), a sua volta articolata in:
    - giorno, mese ed anno (ggmmaaaa) di generazione del messaggio;
    - ora, minuti ed secondi (hhmmss) dell'orario di generazione del messaggio;
    - millisecondi (mmm) dell'orario di generazione del messaggio, generalmente questa quantità non è utile dal punto di vista applicativo e viene posta pari a valore nullo (000).
  - un corpo del messaggio comprendente:
    - dati identificativi dell'utente/viaggiatore;
    - dati identificativi del DPS;
    - dati identificativi del numero di targa del veicolo (ove applicabile);
    - indicazione dell'impiego di automazione totale (variabile intera a valore 2) o semplice (variabile intera a valore 1).
  - un allegato al messaggio consistente nel messaggio crittografato ricevuto dal dispositivo marcatore lato-infrastruttura 1.

- il DPS 3 genera l'impronta del nuovo messaggio (digest) con algoritmo di Hash di tipo SHA-256 (con firmware aggiornabile per l'utilizzo di algoritmi più avanzati, ad esempio SHA-512 oppure a 1024 bit);

- nella seconda forma realizzativa preferita (*modalità automatizzata semplice*) il DPS 3

crittografa con la chiave privata dell'utente/viaggiatore il digest del nuovo messaggio generato, ottenendo così sia il nuovo messaggio generato (comprensivo di quello crittografato ricevuto dal dispositivo marcatore lato-infrastruttura 1) che il digest cifrato del nuovo messaggio generato;

- nella terza forma realizzativa preferita (*cosiddetta modalità automatizzata totale*) il DPS 3 crittografa con la chiave privata del veicolo il digest del nuovo messaggio generato, a sua volta questo digest cifrato viene ulteriormente cifrato con la chiave privata dell'utente/viaggiatore; in tale modo si ottengono sia il nuovo messaggio generato (comprensivo di quello crittografato ricevuto dal dispositivo marcatore lato-infrastruttura 1) che il digest del nuovo messaggio cifrato dapprima con la chiave privata utente/viaggiatore e successivamente con la chiave privata del veicolo;

- in tutti i casi:

  - il DPS 3 crittografa i 2 oggetti ottenuti al passo precedente con la chiave pubblica del dispositivo remoto di verifica presso la centrale operativa OC;
  - il DPS 3 inoltra il messaggio crittografato finale così ottenuto allo smartphone/tablet cui è associato;
  - lo smartphone/tablet 2 associato inoltra, appena possibile, il messaggio finale al dispositivo remoto di verifica presso la centrale operativa OC, utilizzando le tecnologie ed i provider di comunicazione fruibili sul dispositivo personale di comunicazione ed un canale di trasmissione certificata (es.: provider di PEC – posta elettronica certificata).

In particolare, sia nella seconda che nella terza forma di realizzazione descritte sopra, prima dell'utilizzo, il DSP 3 deve essere associato allo smartphone 2 dell'utilizzatore. Preferibilmente, l'associazione avviene in maniera guidata, utilizzando la tecnologia Bluetooth. Durante la procedura di associazione viene controllata la possibilità di leggere i certificati (quello personale ed eventualmente quello del veicolo) e ne viene testata la validità. In caso affermativo per entrambi i certificati (e per entrambe le smart-card – o token USB - inserite dall'utilizzatore) il software dà autorizzazione a procedere in modalità totalmente automatica (confermata dalla accensione di apposito led verde sul DSP 3). In caso di presenza o corretta lettura solo del certificato personale, il software chiede l'immissione della targa del veicolo e autorizza alla modalità automatizzata semplice (confermata dall' accensione di apposito led giallo sul

DSP 3).

In caso di assenza o di non validità o non corretta lettura della certificazione di identità sia del veicolo che personale, il software non autorizza l'accesso al servizio e sul DSP 3 si accende apposito led rosso. In tal caso, se l'utente/viaggiatore è in possesso di una firma elettronica remota, sarà possibile l'utilizzo del sistema nella sua prima forma di realizzazione descritta sopra *(modalità di massima dematerializzazione)*.

Preferibilmente, tutte le forme di realizzazione descritte prevedono l'utilizzo di un supporto di memorizzazione sicura per effettuare l'autenticazione dell'utente e/o del veicolo.

Ad esempio, nella prima forma di realizzazione è previsto l'utilizzo di un token per la gestione di una password temporanea (OTP – One time Password) associata alla firma digitale remota ed atto a consentire l'identificazione dell'utente tramite l'inserimento della password temporanea nella applicazione gestita dallo smartphone e/o tablet.

Come suddetto, nella seconda forma di realizzazione descritta sopra è previsto l'utilizzo di una smart card 4 per l'identificazione dell'utente. Nella terza forma di realizzazione è inoltre previsto l'utilizzo di una ulteriore smart card 5 per l'identificazione del veicolo, tali smart-card sono lette direttamente dal DSP 3 oppure lette dal DSP 3 per il tramite di token USB in cui una e/o l'altra delle smart-card sia inserita.

Come suddetto, il sistema di rilevamento secondo la presente invenzione comprende una centrale operativa remota OC che riceve messaggi criptati inviati dagli smartphone/tablet degli utenti/viaggiatori che usufruiscono del servizio. I messaggi ricevuti vengono sottoposti ad un processo di decriptaggio come descritto di seguito:

- utilizzo della chiave privata del dispositivo remoto di verifica presso la OC per decriptare il messaggio; in questo modo si ottengono sia il messaggio in chiaro generato dal DSP 3 (*nelle modalità automatizzate, sia semplice che totale*) o dallo smartphone/tablet 2 (*nella modalità di massima dematerializzazione*), comprensivo del messaggio crittato ricevuto dal dispositivo marcatore lato-infrastruttura 1, che il digest crittato di tale messaggio;

- il digest crittato viene decriptato con la chiave pubblica dell'utente/viaggiatore (come desunto dal messaggio in chiaro), nel caso di messaggio generato da un DSP con

procedura di automazione totale (il campo apposito del messaggio in chiaro permette di desumere in quale caso si sia), occorre decrittare ulteriormente il digest utilizzando la chiave pubblica del veicolo;

- viene rigenerato il digest del messaggio in chiaro generato dal dispositivo “lato utente (DSP 3 o smartphone/iPhone 2) e confrontato con il digest trasmesso e decriptato per verificare l’integrità del messaggio; inoltre, grazie al buon fine delle procedure di decriptaggio, è certificata la identità del utente/viaggiatore; infine, nel caso di modalità totalmente automatizzata la identità del veicolo (sempre rilevante) è certificata dal buon esito del secondo decriptaggio effettuato, mentre nel caso di modalità ad automazione semplice, la identità del veicolo (ove rilevante) è attestata, in maniera la cui integrità è stata verificata, dall’utente/viaggiatore stesso;

- si procede a decriptare con chiave privata del dispositivo remoto di verifica presso la OC il messaggio generato dal dispositivo marcatore lato-infrastruttura; in tale maniera si ottiene:

  - un messaggio in chiaro generato dal dispositivo marcatore lato-infrastruttura;
  - il digest del messaggio precedente, cifrato con la chiave privata del dispositivo marcatore lato-infrastruttura;

- si procede a decrittare il digest ed a confrontarlo con il ricalcolo dello stesso a partire dal messaggio in chiaro, in tale modo si certifica:

  - l’integrità del messaggio generato dal dispositivo marcatore lato-infrastruttura;
  - l’effettiva paternità del messaggio da parte del dispositivo marcatore stesso.

- ne consegue la certificazione del luogo e del tempo di passaggio del veicolo e/o del viaggiatore per la zona di influenza del dispositivo marcatore lato-infrastruttura.

Ad ogni messaggio ricevuto il server presso la centrale remota OC risponde, verso il dispositivo personale mobile smartphone/tablet che ha spedito il messaggio, con una notifica di ricezione. Il sistema di messaggistica tra centrale remota OC e dispositivo personale smartphone/tablet è certificato, ad esempio essendo basato su PEC (Posta Elettronica Certificata). In alternativa, può essere implementata una soluzione di

certificazione associata al sistema messo a punto che comprende un messaggio firmato elettronicamente (in maniera da assicurare l'integrità della ricevuta stessa) con la chiave privata del dispositivo di verifica d'autenticità e cifrato con la chiave pubblica del DSP che ha generato il messaggio spedito (*modalità automatizzata*) o con la chiave pubblica del viaggiatore/utente che ha utilizzato la firma digitale remota (*modalità a massima dematerializzazione*).

Tutti i messaggi trasmessi da viaggiatori/utenti (o dai relativi DSP) vengono gestiti in un database "lato-server" in corrispondenza della centrale operativa remota OC con una chiave primaria costituita da:

(i) una marca temporale (timestamp) del messaggio generato dal dispositivo marcatore lato-infrastruttura (e/o da un dispositivo di controllo, come sarà meglio descritto nel seguito);

(ii) identificativo del dispositivo lato-infrastruttura (e/o di controllo);

(iii) identificativo del viaggiatore che ha firmato elettronicamente il messaggio;

(iv) targa identificativa del veicolo (se pertinente).

Eventuali violazioni della precedente chiave primaria rilevano potenziali tentativi di infrazione delle regole di utilizzo del sistema o di malfunzionamenti dello stesso.

In funzione della applicazione di controllo e gestione della mobilità cui sono destinati i dispositivi marcatori lato-infrastruttura (o di controllo, come descritto nel seguito), la catena di messaggi ricevuti (in un lasso di tempo predefinito) e riferiti ad uno stesso viaggiatore viene processata in modo da ricostruire la posizione del viaggiatore stesso rispetto alla applicazione di controllo e gestione.

Vantaggiosamente, il trovato secondo la presente invenzione comprende inoltre un dispositivo di controllo 8, comprende ancora ulteriori mezzi di elaborazione per la generazione di dati di controllo crittografati.

In corrispondenza di varchi di accesso ed egresso ad aree/zone/strade/infrastrutture sottoposte a politiche di controllo della mobilità sono posizionabili, come già descritto, dispositivi marcatori lato-infrastruttura 1 che generano e trasmettono messaggi ai viaggiatori ed ai veicoli transitanti nel raggio di azione. In corrispondenza di essi sono implementabili, ove rilevanti, soluzioni di controllo delle targhe dei veicoli transitanti.

In una forma di realizzazione preferita, mostrata nelle figure 1 e 2, il dispositivo di controllo 8 è configurato per essere posizionato o posizionabile in corrispondenza di un dispositivo marcatore “lato-infrastruttura” 1. Esso comprende una telecamera per il riconoscimento automatico delle targhe dei veicoli, collegata, assieme al dispositivo marcatore lato-infrastruttura 1, con una centralina che trasmette alla centrale operativa remota OC. La centralina contiene anche essa un sistema embedded finalizzato alla automatizzazione della procedura descritta di seguito.

La telecamera 8 di lettura delle targhe ed il dispositivo marcatore lato-infrastruttura 1 vengono sincronizzati attraverso un apposito segnale di trigger, generato dalla centralina cui entrambi sono collegati. Il segnale di trigger ha una frequenza fr liberamente settabile aggiornando il software della centralina, anche da remoto; esemplificativamente, la frequenza potrebbe essere fr = 10 secondi. Il segnale di trigger determina l’aggiornamento del messaggio generato dal dispositivo marcatore lato-infrastruttura collegato (in particolare del time-stamp), e la generazione di una nuova crittografia. Il messaggio crittografato viene trasmesso a tutti i veicoli/viaggiatori nel raggio di azione. Lo stesso segnale determina l’inizio di un nuovo periodo di registrazione di tutte le targhe lette dalla telecamera e, quindi, l’inizio di generazione di un nuovo insieme di targhe ed il termine di generazione dell’insieme temporalmente precedente. Per ogni targa contenuta in un insieme terminato, si genera un messaggio opportunamente strutturato, firmato e crittografato a cura della centralina preposta al controllo. La centralina si comporta alla stregua di un DSP in modalità di automazione semplice; essa assume sia il ruolo di DSP che il ruolo di utente/viaggiatore del sistema. La comunicazione verso la centrale operativa remota OC di decrittografia dei messaggi avviene, ad esempio, tramite SIM M2M. Preferibilmente quindi, per ogni targa letta, la centralina preposta al controllo genera un nuovo messaggio contenente:

- una marca temporale (timestamp), a sua volta articolata in:
  - giorno, mese ed anno (ggmmaaaa) di generazione del messaggio;
  - ora, minuti e secondi (hhmmss) dell’orario di generazione del messaggio;
  - millisecondi (mmm) dell’orario di generazione del messaggio, generalmente questa quantità non è utile dal punto di vista applicativo e viene posta pari a valore nullo (000).
- un corpo del messaggio, ad esempio articolato in:

- campo a valore convenzionalmente nullo (es.: 0000), caratterizzante il fatto che è ignoto al dispositivo di controllo l'identità dell'utente/viaggiatore a bordo della vettura identificata;
- proprio codice identificativo (es.: CTRL_00234);
- numero di targa del veicolo (letto dalla telecamera);
- indicazione di un codice di operazione, variabile intera posta al valore 3, caratterizzante una operazione di controllo ad un varco;

- un allegato, contenente sia il messaggio crittografato del dispositivo lato-infrastruttura che la foto associata dal lettore di targhe all'atto della lettura e riconoscimento della stessa;

- la centralina genera l'impronta del nuovo messaggio (digest) ad esempio con algoritmo di Hash, implementato in modalità embedded; l'algoritmo è preferibilmente di tipo SHA-256, la centralina è realizzata in maniera che il firmware sia aggiornabile per l'utilizzo di algoritmi per la generazione del digest più avanzati (es.: SHA-512, oppure algoritmi a 1024 bit);

- la centralina crittografa con la propria chiave privata il nuovo messaggio generato; in tale modo si ottengono sia il nuovo messaggio generato (con allegato quello crittografato ricevuto dal dispositivo lato-infrastruttura) che il digest cifrato con la chiave privata della centralina;

- la centralina crittografa con la chiave pubblica del dispositivo di verifica presso la centrale operativa remota OC il messaggio generato ed il digest cifrato ottenuti al passo precedente e inoltra, ad esempio tramite SIM M2M, il messaggio crittografato risultante alla centrale operativa remota stessa.

Preferibilmente, nella centrale avviene un processo di decodifica dei messaggi inviati. Si applica un procedimento del tutto simile a quello utilizzato per i messaggi inviati da dispositivi di tipo DSP 3 con modalità ad automazione semplice; in luogo della chiave pubblica dell'utente/viaggiatore viene utilizzata la chiave pubblica della centralina preposta al controllo. Ad esempio, una volta de-crittografato il messaggio, a questo viene associata la chiave di ricerca formata dal timestamp del messaggio lato-infrastruttura e dalla targa del veicolo identificata; con tale chiave di ricerca viene interrogato il database che archivia i messaggi ricevuti dai dispositivi personali di

comunicazione degli utenti; la ricerca avviene nella sotto-parte della chiave primaria di detto database consistente nel timestamp e nella targa, notando che in condizioni normali dovrebbe esservi un solo record per ogni coppia timestamp+targa. Il messaggio trovato applicando la ricerca viene marcato come “verificato”. Se la ricerca non dà risultato, si apre una procedura di potenziale infrazione (a carico del proprietario) per il veicolo la cui targa è stata identificata e trasmessa dalla centralina di controllo, giacché è presumibile che il veicolo sia passato per il varco di accesso/egresso senza farsi riconoscere.

In particolare, se la ricerca consegna più di un risultato, occorre procedere con una verifica più dettagliata ed affidata ad un addetto al controllo, giacché una delle identità veicolari registrate potrebbe essere falsa.

Il una ulteriore forma di realizzazione non mostrata nelle figure, il dispositivo di controllo 80 è un dispositivo portatile. Il controllo viene effettuato anche in questo caso tramite riconoscimento automatico della targa dei veicoli. La lettura viene effettuata tramite dispositivo portatile 80 operato da un addetto al controllo. Il dispositivo è costituito ad esempio dalla integrazione funzionale di un dispositivo portatile di lettura e riconoscimento automatico targhe del tipo noto con un dispositivo portatile simile ad un DSP 3 (Dispositivo Specifico Personale) e ricavato per adattamento da esso. Il dispositivo portatile 80 si pone in ricezione (802.14.5 – ZigBee o XBee) con i dispositivi marcatori lato-infrastruttura 1 dell’area di stazionamento/sosta ed acquisisce il messaggio lato-infrastruttura valido al momento del riconoscimento del numero di targa. Il messaggio lato-infrastruttura e la targa riconosciuta vengono confezionati in un nuovo messaggio; a tale scopo il dispositivo portatile di controllo funziona in modo del tutto analogo ad un DSP 3 in modalità ad automazione totale, inoltre, l’addetto all’utilizzo del dispositivo portatile assume il ruolo assunto nella modalità ad automazione totale dall’utente/viaggiatore. Si noti che il dispositivo portatile di controllo 80 utilizza le capacità di comunicazione verso la centrale operativa remota offerta da un dispositivo di comunicazione personale dell’addetto al controllo, similmente a come il DSP utilizza il dispositivo personale di comunicazione del viaggiatore. Ricapitolando, per ogni targa riconosciuta (e per il messaggio di dispositivo lato-infrastruttura valido in quel momento), il dispositivo portatile di controllo:

- genera un nuovo messaggio comprendente:
    - una marca temporale (timestamp), a sua volta articolata in:

- giorno, mese ed anno (ggmmaaaa) di generazione del messaggio;
- ora, minuti e secondi (hhmmss) dell'orario di generazione del messaggio;
- millisecondi (mmm) dell'orario di generazione del messaggio, generalmente questa quantità non è utile dal punto di vista applicativo e viene posta pari a valore nullo (000).

- un corpo del messaggio, ad esempio articolato in:
  - identificativo dell'addetto incaricato dell'utilizzo del dispositivo portatile di controllo;
  - proprio codice identificativo (es.: PORTCTRL_010234);
  - numero di targa del veicolo (letto dal dispositivo di riconoscimento automatico targhe);
  - indicazione di un codice di operazione, variabile intera posta al valore 4, caratterizzante una operazione di controllo con dispositivo portatile;
- un allegato, composto sia dal messaggio crittografato ricevuto dal dispositivo marcatore lato-infrastruttura che dalla fotografia del veicolo a cui è stata riconosciuta la targa;

- il dispositivo portatile di controllo genera l'impronta del nuovo messaggio (digest) ad esempio con algoritmo di Hash, in particolare implementato in modalità embedded; l'algoritmo è di tipo SHA-256, la centralina è realizzata in maniera che il firmware sia aggiornabile per l'utilizzo di algoritmi per la generazione del digest più avanzati (es.: SHA-512, oppure algoritmi a 1024 bit);

- il dispositivo portatile di controllo crittografa con la propria chiave privata il nuovo messaggio generato, che viene poi nuovamente crittografato utilizzando la chiave privata dell'operatore addetto all'utilizzo del dispositivo portatile; in tale modo si ottengono sia il nuovo messaggio generato (con allego quello crittografato ricevuto dal dispositivo lato-infrastruttura) che il digest cifrato con la chiave privata della dispositivo portatile di controllo e la chiave privata dell'addetto all'utilizzo del dispositivo;

- il dispositivo portatile di controllo, infine, crittografa il messaggio generato ed il digest cifrato ottenuti al passo precedente con la chiave pubblica del dispositivo di verifica presso la centrale operativa remota OC ed inoltra, tramite un ulteriore dispositivo

personale di comunicazione dell'addetto al controllo (ad esempio uno smartphone/iPhone/iPad/tablet, ecc), il messaggio crittografato risultante centrale remota OC.

Preferibilmente, nella centrale operativa remota OC avviene un processo di decodifica dei messaggi inviati dai dispositivi portatili di controllo. Si applica un procedimento del tutto simile a quello utilizzato per i messaggi inviati da dispositivi di tipo DSP 3 con modalità ad automazione totale; in luogo della chiave pubblica dell'utente/viaggiatore viene utilizzata la chiave pubblica dell'addetto all'utilizzo del dispositivo portatile di controllo ed in luogo della chiave privata del DSP si utilizza quella del dispositivo portatile di controllo stesso. Al messaggio, una volta completamente de-crittografato, viene associata la chiave di ricerca formata dal time-stamp del messaggio distribuito dal dispositivo marcatore lato-infrastruttura e dalla targa del veicolo identificato dal dispositivo portatile di controllo; con tale chiave di ricerca viene interrogato il database che archivia i messaggi ricevuti dai dispositivi personali di comunicazione degli utenti; la ricerca avviene nella sotto-parte della chiave primaria di detto database consistente nel time-stamp e nella targa. Il messaggio trovato applicando la ricerca viene marcato come "verificato". Se la ricerca non dà risultato, si apre una procedura di potenziale infrazione (a carico del proprietario) per il veicolo la cui targa è stata identificata e trasmessa dalla centralina di controllo, giacché è presumibile che il veicolo stia stazionando nell'area sottoposta a controllo senza essersi fatto rilevare e riconoscere. Se la ricerca produce più di un risultato, quelli non associati con dispositivi lato-infrastruttura localizzati nello stesso luogo del dispositivo portatile di controllo sono da sottoporre a procedura di verifica di infrazione.

Vantaggiosamente, tutte le forme realizzative del presente trovato consentono una identificazione certificata (univoca e non ripudiabile) del passaggio di un viaggiatore in corrispondenza di un determinato spazio infrastrutturale (sezione/varco stradale, fermata di trasporto, stazionamento, banchina, terminale, varco di accesso a servizio, ecc.) o dello stazionamento in un'area di sosta, nonché la realizzazione, ove pertinente, di associazioni estemporanee certificate (univoche e non ripudiabili) veicolo/viaggiatore e la loro contestualizzazione rispetto all'accesso e/o utilizzo di servizi/permessi di mobilità.

In tutti i casi è inoltre previsto che i dispositivi marcatori lato-infrastruttura comunichino unidirezionalmente, inoltrando messaggi verso dispositivi di comunicazione personali

degli utenti/viaggiatori nel loro raggio di azione (tipicamente dispositivi smartphone/tablet o similari) e integrandosi con sistemi di identificazione elettronica in dotazione agli utenti/viaggiatori del tipo FD (Firma Digitale) e/o del tipo CIE (Carta di Identità Elettronica) e/o CNS (Carta Nazionale dei Servizi). Attraverso l'identificazione certificata e non ripudiabile ottenibile con FD, CIE o CNS, è possibile associare alle applicazioni di mobilità gestite dal sistema anche metodi di tariffazione (e più in generale di pagamento) basati su wallet elettronico o su altra forma di pagamento.

Ricapitolando, a seconda delle modalità di funzionamento previste per il sistema può essere o meno necessario integrare nel meccanismo di utilizzo complessivo ulteriori dispositivi. Le modalità di funzionamento preferite, come descritte sopra sono:

i) *modalità di massima dematerializzazione.*

In tale caso l'utente del sistema interagisce con lo stesso esclusivamente tramite smartphone/tablet o similari ed il sistema identificativo certificato da utilizzare da parte dell'utente è preferibilmente la Firma Digitale nella sua variante Remota (sono da considerare a disposizione dell'utente i dispositivi per la fruizione della firma remota, tipicamente quelli eventualmente necessari per la gestione delle OTP – One-Time-Password).

In tale modalità è richiesta una interazione personale nella certificazione di identità che non può essere automatizzata (ancorché previo consenso e pre-autorizzazione specifica dell'interessato).

ii) *modalità automatizzata semplice.*

In tal caso è necessario che il viaggiatore/utente utilizzi anche un Dispositivo Specifico Personale 3 (DSP), oltre ad uno smartphone/tablet o similare. La certificazione di identità avviene con sistema automatico (ancorché dopo preventivo accesso ed autorizzazione ad operare da parte del viaggiatore/utente), eventualmente anche con veicolo viaggiante ad alta velocità (es.: 150 Km/h). I sistemi di firma digitale preferibilmente utilizzati da parte dell'utente/viaggiatore sono quelli su smart-card o su token USB (non è possibile utilizzare la firma digitale remota) oppure CIE o CNS. Il DSP deve essere preventivamente associato con il dispositivo personale di comunicazione dell'utente/viaggiatore; se rilevante, in tale operazione l'utente/viaggiatore digita a sistema (applicazione su smartphone/tablet o similare) anche il numero di targa del veicolo eventualmente utilizzato e, associando il

dispositivo tramite una apposito procedura guidata, concede, tramite identificazione con username e password, il proprio consenso alla associazione veicolo/viaggiatore e si assume le responsabilità e gli oneri da tale associazione derivanti.

iii) *modalità con automazione totale*.

Tale modalità è utile solo ove necessaria l'associazione veicolo/viaggiatore, non è necessaria per la sola identificazione del viaggiatore;

a. mentre nella modalità automatizzata semplice la associazione avviene in maniera gestita dal sistema ma con (pre)indicazione da parte del viaggiatore/utente della targa del veicolo che intende associare, nella modalità ad automazione totale il DSP legge anche una seconda smart-card (o token USB) contenente la chiave privata ed il certificato pubblico del veicolo;

b. in alternativa al precedente punto a), il DPS può permettere un collegamento wireless o cabalato ai sistemi di bordo del veicolo ove questi siano in grado di rilasciare un identificativo del veicolo certificato col meccanismo della crittografia asimmetrica (soltanto a fini di esempio si fa riferimento nella presente descrizione al progetto EVITA, realizzazione del Vehicular Hardware Security Module, full-mode).

La coppia di chiavi pubblico-privata ed il meccanismo di utilizzo presente sul DSP relativamente al veicolo (precedente punto a), oppure eventuali meccanismi proprietari del veicolo (precedente punto b) permettono la identificazione automatica e non ripudiabile del veicolo; il responsabile di tale identificazione è, comunque, il responsabile della smart-card personale (FD, CIE, CNS) gestita dal DSP.

Durante il funzionamento del sistema di gestione della mobilità sono possibili delle verifiche a campione sulla corretta identificazione del veicolo, nelle ipotesi di cui al precedente punto a, nel caso in cui la smart-card del veicolo sia stata utilizzata su un veicolo diverso da quello per la quale sia stata emessa, il proprietario della smart-card personale risponde di una infrazione alle regole.

A titolo esclusivamente esemplificativo, finalizzato alla dimostrazione della utilità dell'invenzione, si illustra una delle possibili applicazioni.

I viaggiatori/utenti del sistema di trasporto di un dato territorio sono possessori di permessi di sosta che possono essere spesi per lo stazionamento in zone di sosta specificamente riservate (parcheggi Dedalo). Tali zone di sosta possono essere sia di

tipo off-street che di tipo on-street. In entrambi i casi, la zona della città dove tali parcheggi sono posti è delimitata da un cordone in cui sono identificabili un numero finito di varchi di accesso e di varchi di uscita (egresso). Eventualmente, gli stalli di sosta potrebbero essere dislocati all'interno di una Zona a Traffico Limitato (ZTL), i permessi di sosta comprendono il permesso di accesso alla ZTL. I viaggiatori/utenti possono usufruire dei loro permessi di sosta associandoli estemporaneamente a qualsiasi veicolo desiderino, anche non di loro proprietà, non preventivamente comunicato. Ai varchi di accesso ed egresso alla ZTL sono collocati dei dispositivi marcatori lato-infrastruttura; analogamente, gli stalli di sosta sono coperti da ulteriori dispositivi marcatori lato-infrastruttura. L'utente/viaggiatore utilizza un DSP, in modalità completamente automatizzata, ed una firma elettronica che lo identifica in maniera univoca e non ripudiabile. Prima di approcciarsi alla ZTL, l'utente/viaggiatore associa il suo DSP ad uno smartphone (anche non necessariamente il proprio) sul quale è attiva la applicazione di gestione client-side del sistema di controllo della mobilità. All'entrata nella ZTL, per uno qualsiasi dei suoi varchi, avviene la trasmissione (dallo smartphone) al sistema remoto di centrale OC; tale trasmissione attesta l'ingresso (con data ed ora) alla ZTL di un dato veicolo, estemporaneamente associato ai permessi di sosta disponibili per l'utente/viaggiatore. Da quel momento la centrale inizia a conteggiare un tempo tipico di raggiungimento degli stalli di sosta disponibili; entro tale lasso di tempo non vengono decrementati permessi di sosta; dopo tale lasso di tempo, i permessi di sosta vengono decrementati, se il viaggiatore non è stato rilevato all'interno di un'area di sosta, ad una velocità molto elevata. Al raggiungimento degli stalli di sosta riservati il DSP intercetta il messaggio del dispositivo marcatore lato-infrastruttura che copre l'area stessa e lo inoltra in centrale remota debitamente firmato. Il primo di tali messaggi giunti in centrali attesta il raggiungimento degli stalli di sosta da parte dell'utente/viaggiatore e del veicolo ad esso associato, ne consegue il decremento a velocità ordinaria dei permessi di sosta a disposizione. I messaggi del dispositivo marcatore lato-infrastruttura a bordo dell'area di sosta continuano ad essere inoltrati con frequenza fissa e vengono mantenuti in archivio in centrale sia il primo che l'ultimo arrivato. Quando non giungono più messaggi per il veicolo/utente e dal dispositivo lato-infrastruttura della area di sosta, viene contato il termine della sosta e l'inizio dello spostamento per allontanarsi dalla ZTL. Viene concesso un tempo prestabilito di allontanamento in cui non vengono scalati permessi di sosta e, al temine di questo, vengono decrementati permessi con velocità molto elevata, a meno che il veicolo e l'utente/viaggiatore siano smarcati in uscita dalla ZTL da un dispositivo lato-infrastruttura.

È il caso di notare che è opportuno installare centraline di controllo per l'erogazione di eventuali sanzioni in corrispondenza dei varchi di ingresso alla ZTL (dove sono in genere già collocate telecamere per la lettura ed il riconoscimento delle targhe). In tale modo si evita l'ingresso di veicoli che non facciano riconoscere a bordo la presenza di utenti/viaggiatori in possesso di permessi di sosta. Non è necessario utilizzare dispositivi di controllo portatili all'interno delle aree di sosta, giacché il meccanismo di decremento dei permessi invoglia gli utenti a farsi riconoscere. Similmente, non è necessario installare strumenti di controllo finalizzati alla sanzione ai varchi di uscita dalle ZTL, sempre per effetto del meccanismo di decremento dei permessi di sosta.

La presente invenzione è stata fin qui descritta con riferimento a forme preferite di realizzazione. È da intendersi che possano esistere altre forme di realizzazione che afferiscono al medesimo nucleo inventivo, come definito dall'ambito di protezione delle rivendicazioni qui di seguito riportate.