

<b>DOMANDA DI INVENZIONE NUMERO</b>	<b>102021000027632</b>
<b>Data Deposito</b>	<b>28/10/2021</b>
<b>Data Pubblicazione</b>	<b>28/04/2023</b>

Classifiche IPC

<b>Sezione</b>	<b>Classe</b>	<b>Sottoclasse</b>	<b>Gruppo</b>	<b>Sottogruppo</b>
G	06	F	21	31

<b>Sezione</b>	<b>Classe</b>	<b>Sottoclasse</b>	<b>Gruppo</b>	<b>Sottogruppo</b>
G	06	F	21	60

<b>Sezione</b>	<b>Classe</b>	<b>Sottoclasse</b>	<b>Gruppo</b>	<b>Sottogruppo</b>
H	04	L	9	40

Titolo

METODO E SISTEMA ELETTRONICO PER ABILITARE UNA OPERAZIONE A DISTANZA PER MEZZO DI UN COLLEGAMENTO PUNTO-PUNTO

## DESCRIZIONE

Annessa a domanda di brevetto per INVENZIONE INDUSTRIALE avente per titolo

### “METODO E SISTEMA ELETTRONICO PER ABILITARE UNA OPERAZIONE A DISTANZA PER MEZZO DI UN COLLEGAMENTO PUNTO-PUNTO”

A nome: FOOLFARM S.p.A.  
Via Filippo Corridoni, 6  
2012 MILANO (MI)  
Italia

\*\*\*\*\*

#### Campo tecnico dell'invenzione

La presente invenzione riguarda in generale il settore della identità digitale di un utente di un dispositivo elettronico mobile o di un personal computer.

5 Più in particolare, la presente invenzione riguarda un metodo e sistema elettronico per abilitare una operazione a distanza per mezzo dell'utilizzo di un collegamento sicuro di tipo punto-punto, come ad esempio una operazione di pagamento fra due soggetti.

#### Tecnica nota

10 E' nota la procedura di autenticazione in cui viene verificata l'identità di un soggetto che è stato identificato in una precedente fase di identificazione: nella fase di autenticazione viene verificato in tempo reale che il soggetto (utilizzando uno smartphone o un personal computer) che vuole utilizzare un determinato servizio sia effettivamente quello che ha dichiarato di essere 15 nella precedente fase di identificazione.

Il servizio può essere ad esempio l'accesso ad un conto corrente bancario, la sottoscrizione di un contratto a distanza, l'apertura di un conto corrente bancario.

15 E' noto l'utilizzo di procedure di autenticazione forte che utilizzano la combinazione di almeno due fattori di tipo diverso per aumentare il livello di

sicurezza con il quale viene identificato il soggetto, in particolare utilizzando un fattore noto al soggetto da identificare (ad esempio, una password) ed un fattore associato ad un oggetto fisico appartenente all'utente (ad esempio, la sua faccia).

5 Sono noti sistemi di pagamento digitali come ad esempio PayPal, Amazon Pay, Apple Pay o Satispay, che hanno il vantaggio di consentire di effettuare il pagamento di un bene o servizio acquistato online semplicemente cliccando su un pulsante che indica il pagamento per mezzo di uno dei sistemi sopra indicati, senza richiedere l'inserimento dei dati di una 10 carta di credito e sfruttando un account che è stato creato precedentemente dall'utente.

La Richiedente ha osservato che i sistemi di pagamento noti hanno i seguenti svantaggi:

- non garantiscono con sufficiente sicurezza che il destinatario del 15 pagamento sia corretto e/o che sia effettivamente quello che dichiara di essere;
- non consentono di abilitare un pagamento in denaro con un sufficiente livello di sicurezza.

#### **Breve sommario dell'invenzione**

20 La presente invenzione riguarda un metodo e sistema elettronico per abilitare una operazione a distanza per mezzo di un collegamento di tipo punto-punto come definiti nelle annesse rivendicazione 1 e 8 e da loro forme di realizzazione preferite descritte nelle rivendicazioni dipendenti da 2 a 6 e 9-11 .

25 La Richiedente ha percepito che il metodo e sistema elettronico di abilitazione dell'operazione a distanza in accordo con la presente invenzione hanno i seguenti vantaggi:

- aumentano la sicurezza che il destinatario dell'operazione a distanza (per esempio, un pagamento) sia corretto e/o sia effettivamente quello che 30 dichiara di essere;
- permettono di ottenere un livello di sicurezza medio-alto per un pagamento in denaro;

- rispettano la normativa EIDAS (Electronic Identification Authentication and Signature), Regolamento UE n.910/2014.

L'idea di base è quella di generare un identificativo operazione univoco che contiene informazioni indicative del tipo di operazione di collegamento punto-punto (per esempio, un comando di pagamento di denaro) fra un primo dispositivo elettronico associato ad un primo soggetto ed un secondo dispositivo elettronico di un secondo soggetto (oppure fra il primo dispositivo elettronico ed un punto vendita o un sito web di un negozio virtuale online) e contiene inoltre un identificativo utenti, poi condividere detto identificativo operazione univoco fra il primo dispositivo elettronico ed il secondo dispositivo elettronico (oppure condividerlo con il punto vendita o con il sito web del negozio virtuale online), quindi viene verificata l'identità digitale del soggetto che ha richiesto il pagamento per mezzo del primo dispositivo elettronico, poi viene verificata l'identità digitale del soggetto associato al secondo dispositivo elettronico (oppure è stata precedentemente certificata l'identità del punto vendita/sito web negozio virtuale) per mezzo di un sotto-sistema di autenticazione in modo da stabilire un collegamento sicuro di tipo punto-punto fra il primo dispositivo elettronico ed il secondo dispositivo elettronico (oppure fra il primo dispositivo elettronico ed il punto vendita/sito web del negozio virtuale),.

Forma oggetto della presente invenzione anche un supporto di memorizzazione non-transitorio leggibile da un elaboratore elettronico come definito nella annessa rivendicazione 7.

Forma oggetto della presente invenzione anche un programma per elaboratore elettronico comprendente porzioni di codice software atto ad eseguire i passi del metodo di autenticazione secondo le rivendicazioni 1-6, quando detto programma è eseguito su almeno un elaboratore elettronico.

#### **Breve descrizione dei disegni**

Ulteriori caratteristiche ed i vantaggi dell'invenzione risulteranno dalla descrizione che segue di una forma di realizzazione preferita e di sue varianti fornita a titolo esemplificativo con riferimento ai disegni allegati, in cui:

- la Figura 1 mostra uno schema a blocchi di un sistema elettronico per abilitare un pagamento per mezzo di un collegamento punto-punto secondo una prima forma di realizzazione dell'invenzione;
- la Figura 2 mostra più in dettaglio una parte del sistema elettronico della Figura 1;
- le Figure 3A-3B mostrano un andamento temporale dei messaggi scambiati fra i diversi componenti del sistema elettronico per abilitare il pagamento secondo la prima forma di realizzazione dell'invenzione;
- la Figura 4 mostra uno schema a blocchi di un sistema elettronico per abilitare un pagamento per mezzo di un collegamento punto-punto in base ad una seconda forma di realizzazione dell'invenzione;
- le Figure 5A-5B mostrano un andamento temporale dei messaggi scambiati fra i diversi componenti del sistema elettronico per abilitare il pagamento in base alla seconda forma di realizzazione dell'invenzione.

## 15 **Descrizione dettagliata dell'invenzione**

Si osservi che nella descrizione seguente blocchi, componenti o moduli identici o analoghi sono indicati nelle figure con gli stessi riferimenti numerici, anche se sono mostrati in differenti forme di realizzazione dell'invenzione.

20 Ai fini della spiegazione dell'invenzione si considera nelle Figure 1 e 3A-3B una operazione di pagamento di denaro e si considera nelle Figure 4 e 5A-5B il pagamento di un bene o servizio, ma più in generale l'invenzione può essere applicata anche ad altri tipi di operazioni, come ad esempio per:

- abilitare il trasferimento di un file digitale contenente informazioni importanti;
- abilitare lo scambio di documenti in formato digitale;
- abilitare un canale di comunicazione protetto fra due utenti collegati per mezzo di una rete di telecomunicazioni (per esempio, Internet);
- attivare una comunicazione tracciata fra un utente ed un dispositivo IoT.

Con riferimento alla Figura 1, viene mostrato un sistema elettronico 1 per abilitare un pagamento di denaro per mezzo di un collegamento punto-punto secondo una prima forma di realizzazione dell'invenzione.

In particolare, nelle Figure 1 e 3A-3B della prima forma di  
5 realizzazione si considera un pagamento che è un trasferimento di denaro fra due soggetti, in cui il trasferimento di denaro è richiesto da un primo soggetto 7-1 per mezzo di un primo dispositivo elettronico 8-1, mentre il pagamento viene ricevuto da un secondo soggetto 7-2 al quale appartiene un secondo dispositivo elettronico 8-2.

10 Più in generale, il pagamento può essere ad esempio uno fra i seguenti:

- un trasferimento di denaro fra due soggetti;
- un trasferimento di denaro fra un soggetto ed un punto vendita, ad esempio per l'acquisto di un bene (per esempio, un prodotto alimentare) o  
15 servizio (per esempio, una visita medica, un prodotto finanziario, una vacanza);
- un trasferimento di denaro fra un soggetto ed un negozio virtuale, per l'acquisto di un bene (ad esempio, un libro in formato digitale) o di un servizio (ad esempio, una visita medica, un prodotto finanziario, una vacanza, un file  
20 digitale da scaricare contenente informazioni importanti).

Il sistema elettronico 1 comprende un primo dispositivo elettronico 8-1, un secondo dispositivo elettronico 8-2, un primo sotto-sistema 10 di autenticazione, un secondo sotto-sistema 20 di condivisione messaggi, un primo dispositivo server di pagamento 9-1 ed un secondo dispositivo server  
25 di pagamento 9-2.

Il sotto-sistema di autenticazione 10 comprende una pluralità di dispositivi elettronici, i quali sono collegati per mezzo di una rete di telecomunicazioni a media-lunga distanza, ad esempio la rete Internet che utilizza il protocollo TCP/IP, con una architettura client-server ed utilizzo di  
30 Servizi Web ("Web Services").

Secondo la prima e seconda forma di realizzazione dell'invenzione, il sotto-sistema di autenticazione 10 ha la funzione di generare dinamicamente

(per mezzo di un dispositivo server 105 che verrà illustrato in seguito) un identificativo operazione univoco che contiene informazioni indicative del tipo di operazione di pagamento richiesta dal soggetto 7-1 e contiene un identificativo utenti che identifica gli utenti coinvolti nell'operazione di pagamento, ovvero i soggetti 7-1 e 7-2 nel caso di un comando di trasferimento di denaro fra di essi oppure il soggetto 7-1 ed un punto vendita 108 nel caso di un comando di pagamento di un bene o servizio.

Con il termine "identificativo operazione univoco generato dinamicamente" si intende che il valore dell'identificativo operazione cambia ad ogni richiesta di una nuova operazione di pagamento da parte del soggetto 7-1.

L'utilizzo dell'identificativo operazione univoco consente di rendere l'operazione di pagamento tracciata e verificabile, in quanto l'identificativo operazione univoco è sicuro perché contiene l'informazione del destinatario e quindi solo il destinatario corretto sarà in grado di identificarsi con successo, avviando quindi il tipo di operazione richiesta solo nel caso in cui sia stato effettuato con successo il riconoscimento dell'identità digitale di entrambe le parti (ovvero il soggetto 7-1 e il soggetto 7-2), come verrà spiegato più in dettaglio in seguito.

Per esempio, l'identificativo operazione univoco è un codice univoco associato ad un link web oppure contenuto in un codice a barre oppure in un codice QR, in cui detto codice contiene le informazioni indicative del tipo di operazione di pagamento richiesto e contiene l'identificativo degli utenti coinvolti nell'operazione di pagamento, come ad esempio un trasferimento di denaro fra due soggetti o il pagamento per l'acquisto di un bene o servizio.

Vantaggiosamente, viene effettuata una crittografia asimmetrica (ovvero che utilizza una chiave pubblica ed una privata) del valore generato dell'identificativo operazione per proteggere l'identificativo operazione trasmesso dal primo dispositivo elettronico 8-1 al secondo dispositivo elettronico 8-2: in questo modo il valore cifrato dell'identificativo operazione risulta anonimo, ovvero le informazioni contenute nell'identificativo operazione non possono essere interpretate da un essere umano in quanto

non sono in chiaro, mentre possono essere interpretate dal secondo dispositivo elettronico 8-2 in cui viene effettuata (per mezzo di una chiave pubblica) la decrittografia dell'identificativo operazione ricevuto.

Per esempio, nel caso di inserimento del codice identificativo 5 operazione all'interno di un sito web, il codice identificativo operazione viene rigenerato ogni volta che viene caricata la pagina web, consentendo un collegamento sicuro fra l'utente ed il servizio verso cui verrà effettuato il pagamento.

Inoltre secondo la prima e seconda forma di realizzazione, il sotto-10 sistema di autenticazione 10 ha l'ulteriore funzione di autenticare un soggetto 7-1 al quale appartiene il primo dispositivo elettronico 8-1, ovvero di verificare l'identità digitale del soggetto 7-1, per mezzo di un controllo biometrico di tipo vocale e/o facciale e/o oculare.

Inoltre secondo la prima forma di realizzazione, il sotto-sistema di 15 autenticazione 10 ha l'ulteriore funzione di autenticare un soggetto 7-2 al quale appartiene il secondo dispositivo elettronico 8-2, ovvero di verificare l'identità digitale del soggetto 7-2, per mezzo di un controllo biometrico di tipo vocale e/o facciale e/o oculare.

In particolare, nella prima forma di realizzazione il sotto-sistema di 20 autenticazione 10 è configurato per ricevere un messaggio indicativo di una richiesta di generare un identificativo di una operazione di pagamento, ed è configurato per generare un identificativo operazione univoco che contiene informazioni indicative del tipo di operazione di pagamento e contiene un identificativo utenti che identifica il soggetto 7-1 (che ha richiesto il 25 pagamento) ed il soggetto 7-2 (che riceve il pagamento).

Inoltre nella prima forma di realizzazione il sotto-sistema di autenticazione e 10 è configurato per trasmettere, verso il primo dispositivo elettronico 8-1, un messaggio che trasporta un valore di detto identificativo operazione univoco generato.

30 Inoltre nella prima forma di realizzazione il sotto-sistema di autenticazione e 10 è configurato per ricevere un messaggio di richiesta di verifica di una identità digitale del primo soggetto 7-1, quindi il sotto-sistema

di autenticazione 10 è configurato per effettuare una verifica positiva o negativa dell'identità digitale del primo soggetto 7-1.

Per esempio, l'identità digitale del primo soggetto 7-1 viene verificata per mezzo del sotto-sistema di autenticazione 10 realizzato come descritto 5 nella Figura 2 illustrata in seguito.

Inoltre nella prima forma di realizzazione il sotto-sistema di autenticazione 10 è configurato per trasmettere, verso il primo dispositivo elettronico 8-1, un messaggio di conferma di verifica positiva dell'identità digitale del primo soggetto 7-1, in caso in cui l'identità digitale del primo 10 soggetto 7-1 sia stata verificata con successo; alternativamente, il sotto-sistema di autenticazione 10 è configurato per trasmettere, verso il primo dispositivo elettronico 8-1, un messaggio di verifica negativa dell'identità digitale del primo soggetto 7-1, in caso di una verifica negativa dell'identità digitale del primo soggetto 7-1.

15 Inoltre nella prima forma di realizzazione il sotto-sistema di autenticazione 10 è configurato per ricevere un messaggio di richiesta di verifica dell'identità digitale del secondo soggetto 7-2, quindi il sotto-sistema di autenticazione 10 è configurato per effettuare una verifica positiva o negativa dell'identità digitale del secondo soggetto 7-2.

20 Per esempio, l'identità digitale del secondo soggetto 7-2 viene verificata per mezzo del sotto-sistema di autenticazione 10 realizzato come descritto nella Figura 2 illustrata in seguito.

Inoltre nella prima forma di realizzazione il sotto-sistema di autenticazione 10 è configurato per trasmettere, verso il secondo dispositivo elettronico 8-2, un messaggio di conferma di verifica positiva dell'identità digitale del secondo soggetto 7-2, nel caso in cui l'identità digitale del secondo soggetto 7-2 sia stata verificata con successo; alternativamente, il sotto-sistema di autenticazione 10 è configurato per trasmettere, verso il secondo dispositivo elettronico 8-2, un messaggio di verifica negativa 25 dell'identità digitale del secondo soggetto 7-2, in caso di una verifica negativa dell'identità digitale del secondo soggetto 7-2.

30

Il sotto-sistema di autenticazione 10 ha l'ulteriore funzione di abilitare il pagamento richiesto dal soggetto 7-1.

In particolare, nella prima forma di realizzazione il sotto-sistema di autenticazione 10 è configurato per ricevere un messaggio di richiesta di una 5 autorizzazione dell'operazione di pagamento, ed è configurato per generare una autorizzazione concessa o negata ad effettuare detta operazione di pagamento, in funzione rispettivamente della verifica positiva o negativa dell'identità digitale del secondo soggetto 7-2.

Inoltre nella prima forma di realizzazione il sotto-sistema di 10 autenticazione 10 è configurato per trasmettere, verso il primo dispositivo elettronico 8-1 e/o verso il secondo dispositivo elettronico 8-2, un messaggio indicativo di una conferma positiva o negativa ad un collegamento punto-punto fra il primo dispositivo elettronico 8-1 ed il secondo dispositivo elettronico 8-2, in funzione rispettivamente della autorizzazione concessa o 15 negata al trasferimento di denaro.

Nella seconda forma di realizzazione, il sotto-sistema di autenticazione 10 è configurato per ricevere un messaggio che trasporta un valore indicativo di un importo di denaro associato al pagamento del bene o servizio ed è configurato per generare una autorizzazione concessa o negata 20 ad effettuare detto pagamento del bene o servizio, in funzione rispettivamente di una verifica positiva o negativa dell'identità digitale del primo soggetto 7-1.

Inoltre nella seconda forma di realizzazione, il sotto-sistema di autenticazione 10 è configurato per trasmettere, verso il primo dispositivo elettronico 8-1, un messaggio indicativo di una conferma positiva o negativa ad un collegamento punto-punto fra il primo dispositivo elettronico 8-1 ed il punto vendita 108, in funzione rispettivamente di una autorizzazione concessa o negata al pagamento del bene o servizio.

Il primo dispositivo elettronico 8-1 può essere di tipo fisso (ad 30 esempio, un personal computer o un totem) oppure di tipo mobile (ad esempio, uno smartphone, un tablet oppure un computer portatile) ed appartiene al soggetto 7-1.

Ai fini della spiegazione dell'invenzione si considera in seguito per semplicità che il primo dispositivo elettronico 8-1 sia di tipo mobile, in particolare è uno smartphone sul quale è installata una particolare applicazione per eseguire una parte del metodo della prima, seconda e terza

5 forma di realizzazione dell'invenzione.

Il dispositivo elettronico 8-1 comprende un altoparlante, un microfono, una unità di elaborazione (per esempio, un micro-processore), un ricetrasmettitore di segnali a media-lunga distanza (per esempio, segnali senza fili di tipo radiomobile 2G/3G/4G/5G) e, preferibilmente, una

10 fotocamera ed un assistente vocale 2-1.

Preferibilmente, il dispositivo elettronico 8-1 comprende un assistente vocale 2-1 che ha la funzione di interpretare il linguaggio dell'uomo e di dialogare con esso.

L'assistente vocale 2-1 è una applicazione software (cioè un

15 programma software) eseguita per mezzo dell'unità di elaborazione del dispositivo elettronico 8-1, come ad esempio l'applicazione Google Assistant per smartphone o tablet che utilizzano il sistema operativo Android, oppure l'applicazione Siri per iPhone o iPad oppure l'Assistente vocale Cortana per Personal computer con sistema operativo Windows: in questo caso

20 l'assistente vocale 2-1 ed il dispositivo elettronico 8-1 sono realizzati in un unico componente elettronico (ad esempio, uno smartphone o iPhone o un Personal computer).

Alternativamente, l'assistente vocale può essere realizzato con un dispositivo elettronico dedicato separato dal dispositivo elettronico 8-1, come

25 ad esempio Google Home o Amazon Echo (o Echo dot) con Alexa.

In particolare, nella prima e seconda forma di realizzazione il primo dispositivo elettronico 8-1 è configurato per trasmettere, verso il sistema di autenticazione 10, un messaggio indicativo di una richiesta di generare un identificativo di una operazione di pagamento richiesta da un primo soggetto

30 7-1 associato al primo dispositivo elettronico 8-1.

Inoltre il primo dispositivo elettronico 8-1 è configurato per ricevere un messaggio che trasporta un valore di un identificativo operazione univoco

che contiene informazioni indicative del tipo di operazione di pagamento richiesta dal soggetto 7-1 e contiene un identificativo utenti che identifica i soggetti 7-1 e 7-2 coinvolti nell'operazione di pagamento, quindi il primo dispositivo elettronico 8-1 è configurato per trasmettere, verso il sistema di 5 autenticazione 10, un messaggio di richiesta di verifica di una identità digitale del primo soggetto 7-1.

Inoltre il primo dispositivo elettronico 8-1 è configurato per ricevere un messaggio di conferma di verifica positiva dell'identità digitale del primo soggetto 7-1 ed è configurato per generare una richiesta di condivisione 10 dell'identificativo operazione con il secondo dispositivo elettronico 8-2.

Inoltre il primo dispositivo elettronico 8-1 è configurato per trasmettere, verso il secondo dispositivo elettronico 8-2, un messaggio che trasporta un valore dell'identificativo operazione.

Infine il primo dispositivo elettronico 8-1 è configurato per ricevere un messaggio indicativo di una conferma positiva o negativa ad un collegamento punto-punto fra il primo dispositivo elettronico 8-1 ed il secondo dispositivo elettronico 8-2.

Il secondo dispositivo elettronico 8-2 può essere di tipo fisso (ad esempio, un personal computer o un totem) oppure di tipo mobile (ad esempio, uno smartphone, un tablet oppure un computer portatile) ed 20 appartiene al soggetto 7-2.

Le precedenti considerazioni relative al primo dispositivo elettronico 8-1 sono applicabili in modo analogo al secondo dispositivo elettronico 8-2, ovvero questo comprende un altoparlante, un microfono, una unità di 25 elaborazione (per esempio, un micro-processore), un ricetrasmettitore di segnali a media-lunga distanza (per esempio, segnali senza fili di tipo radiomobile 2G/3G/4G/5G) e, preferibilmente, una fotocamera ed un assistente vocale 2-2.

Ai fini della spiegazione dell'invenzione si considera in seguito per 30 semplicità che il secondo dispositivo elettronico 8-2 sia di tipo mobile, in particolare è uno smartphone sul quale è installata la particolare applicazione

per eseguire un'altra parte del metodo secondo la prima forma di realizzazione dell'invenzione.

In particolare, nella prima forma di realizzazione il secondo dispositivo elettronico 8-2 è configurato per ricevere il messaggio che trasporta il valore 5 dell'identificativo operazione ed è configurato per estrarre da questo le informazioni indicative del tipo di operazione di pagamento (ovvero trasferimento di denaro) ed estrarre il valore dell'identificativo utenti che identifica i soggetti 7-1 e 7-2, rilevando così che l'operazione di pagamento (trasferimento di denaro) è stata richiesta dal soggetto 7-1 (per mezzo del 10 primo dispositivo elettronico 8-1) verso il soggetto 7-2.

Inoltre nella prima forma di realizzazione il secondo dispositivo elettronico 8-2 è configurato per trasmettere, verso il sistema di autenticazione 10, un messaggio di richiesta di verifica dell'identità digitale del secondo soggetto 7-2 associato al secondo dispositivo elettronico 8-2.

15 Inoltre nella prima forma di realizzazione il secondo dispositivo elettronico 8-2 è configurato per ricevere un messaggio di conferma di verifica positiva dell'identità digitale del secondo soggetto 7-2 ed è configurato per trasmettere, verso il sistema di autenticazione 10, un messaggio di richiesta dell'autorizzazione dell'operazione di pagamento.

20 Infine il secondo dispositivo elettronico 8-2 è configurato per ricevere un messaggio indicativo di una conferma positiva o negativa ad un collegamento punto-punto fra il primo dispositivo elettronico 8-1 ed il secondo dispositivo elettronico 8-2.

25 Secondo la prima forma di realizzazione, il sotto-sistema di condivisione messaggi 20 è collegato con il primo dispositivo elettronico 8-1 e con il secondo dispositivo elettronico 8-2, per mezzo di una rete di telecomunicazioni a media-lunga distanza (per esempio, la rete Internet oppure una rete radiomobile).

30 Nella prima forma di realizzazione, il sotto-sistema di condivisione messaggi 20 ha la funzione di inoltrare, dal primo dispositivo elettronico 8-1 al secondo dispositivo elettronico 8-2, un messaggio che trasporta l'identificativo operazione univoco che contiene un comando di pagamento o

trasferimento di denaro e contiene un identificativo utenti che identifica i soggetti 7-1 e 7-2 coinvolti nell'operazione di pagamento.

Il sotto-sistema di condivisione messaggi 20 è quindi separato dal sotto-sistema di autenticazione 10, ovvero è esterno ad esso.

5 Per esempio, il sotto-sistema di condivisione messaggi 20 è implementato con un messaggio di posta elettronica, un messaggio WhatsApp, un breve messaggio di testo (SMS) o altri sistemi di scambio messaggi.

10 Il primo dispositivo server di pagamento 9-1 è un gateway di pagamento che è posizionato presso una banca o una istituzione finanziaria che gestisce sistemi di pagamento ed ha la funzione di gestire il pagamento richiesto dal primo soggetto 7-1; in particolare, il primo dispositivo server di pagamento 9-1 gestisce un conto corrente che appartiene al primo soggetto 7-1.

15 Il primo dispositivo server di pagamento 9-1 è quindi un dispositivo elettronico che comprende un ricetrasmettitore di segnali a media-lunga distanza per scambiare dati con il sotto-sistema di autenticazione 10 e per scambiare dati direttamente con il secondo dispositivo server di pagamento 9-2.

20 Il secondo dispositivo server di pagamento 9-2 è un gateway di pagamento che è posizionato presso una banca o una istituzione finanziaria che gestisce sistemi di pagamento ed ha la funzione di gestire il pagamento verso il secondo soggetto 7-2 (prima forma di realizzazione) o il pagamento nel luogo in cui è posizionato il punto vendita 108 (seconda forma di realizzazione); in particolare, il secondo dispositivo server di pagamento 9-2 gestisce un conto corrente che appartiene al secondo soggetto 7-2, oppure gestisce un conto corrente che è associato al punto vendita 108.

30 Il secondo dispositivo server di pagamento 9-2 è quindi un dispositivo elettronico che comprende un ricetrasmettitore di segnali a media-lunga distanza per scambiare dati con il sotto-sistema di autenticazione 10 e per scambiare dati direttamente con il primo dispositivo server di pagamento 9-1.

Con riferimento alla Figura 2, viene mostrato più in dettaglio il sotto-sistema di autenticazione 10.

Il sotto-sistema di autenticazione 10 può essere ad esempio implementato come descritto nella domanda di brevetto PCT avente numero 5 di deposito PCT/IB2021/055428 depositata il 21 giugno 2021 a nome della stessa Richiedente.

In particolare, il sotto-sistema di autenticazione 10 può essere realizzato come illustrato nella Figura 3 oppure nella Figura 5 della sopra indicata domanda di brevetto PCT, utilizzando un dispositivo server operativo 10 105, un primo dispositivo server di autenticazione 56, un secondo dispositivo server di autenticazione 106, un elaboratore elettronico di linguaggio umano 3 ed una applicazione 4 di erogazione servizi a pagamento: per mezzo di questi dispositivi viene verificata l'identità digitale dei soggetti 7-1, 7-2 utilizzando una autenticazione biometrica di tipo vocale (oppure 15 vocale/facciale, oppure vocale/facciale/oculare) che effettua il confronto fra un profilo vocale campione (oppure un profilo vocale/facciale campione, oppure un profilo vocale/facciale campione +codice oculare campione) generato in tempo reale ed un profilo vocale di riferimento (oppure un profilo 20 vocale/facciale di riferimento, oppure un profilo vocale/facciale di riferimento +codice oculare di riferimento) che è stato memorizzato in precedenza in condizioni di sicurezza in una procedura di profilazione, in cui il profilo vocale di riferimento (oppure il profilo vocale/facciale di riferimento, oppure il profilo vocale/facciale di riferimento +codice oculare di riferimento) è stato suddiviso 25 in due (o più) porzioni memorizzate nel primo e secondo dispositivo server di autenticazione 56, 106 (e in eventuali ulteriori dispositivi server di autenticazione).

Nel caso in cui il sotto-sistema di autenticazione 10 sia tale da effettuare l'autenticazione del soggetto 7-1 per mezzo di un controllo biometrico, il soggetto 7-1 è stato identificato in una precedente procedura di 30 profilazione in una condizione di sicurezza, in cui sono stati acquisiti dati personali del soggetto, come ad esempio il suo nome, cognome, numero di telefono, carta di identità ed in cui è stato generato un profilo vocale di

riferimento (oppure il profilo vocale/facciale di riferimento, oppure il profilo vocale/facciale di riferimento+ profilo oculare di riferimento) del soggetto 7-1.

Con il termine “profilo vocale di riferimento” si intende un profilo di riferimento della identità digitale del soggetto 7-1 associato alla traccia audio digitale di riferimento della voce del soggetto 7-1, in cui detta traccia audio digitale di riferimento è stata precedentemente acquisita dal soggetto 7-1 e memorizzata in una procedura di profilazione ed in condizioni di sicurezza, ed in cui detto profilo vocale di riferimento è stato memorizzato in uno o più dispositivi del sotto-sistema di abilitazione 10: il profilo vocale di riferimento è stato quindi verificato in precedenza ed è considerato attendibile.

Vantaggiosamente, in aggiunta al segnale vocale del soggetto 7-1, nella procedura di profilazione viene acquisita una o più immagini rappresentative della faccia del soggetto 7-1, generando così un “profilo vocale/facciale di riferimento” che è una combinazione della traccia audio digitale di riferimento con dati biometrici associati alla faccia del soggetto 7-1, in cui detto profilo vocale/facciale di riferimento è stato precedentemente acquisito e memorizzato nella procedura di profilazione in condizioni di sicurezza, ed in cui detto profilo vocale/facciale di riferimento è stato memorizzato in uno o più dispositivi del sotto-sistema di abilitazione 10; per esempio, nella procedura di profilazione viene acquisita una registrazione video in cui viene inquadrata almeno la faccia del soggetto 7-1 e questo pronuncia ad alta voce una frase definita, generando così il profilo vocale/facciale di riferimento.

Con il termine “codice oculare di riferimento” si intende un codice univoco che viene generato in funzione di almeno un parametro biometrico degli occhi del soggetto 7-1, per mezzo di un opportuno algoritmo che prende in ingresso uno o più parametri associati agli occhi del soggetto 7-1, in cui detto codice oculare di riferimento è stato precedentemente acquisito e memorizzato nella procedura di profilazione in condizioni di sicurezza.

Pertanto con il termine “profilo vocale/facciale di riferimento+ codice oculare di riferimento” si intendono dati associati ad una combinazione della traccia audio digitale di riferimento della voce del soggetto 7-1, di dati

biometrici associati alla faccia del soggetto 7-1 e di uno o più parametri biometrici degli occhi del soggetto 7-1 (ad esempio, colore dell'iride, colore della sclera, colore della cornea, diametro degli occhi, distanza della pupilla dall'angolo interno dell'occhio, distanza della pupilla dall'angolo esterno dell'occhio, dimensione e forma delle sopracciglia).

Con il termine "profilo vocale campione" si intende un profilo campione della identità digitale del soggetto 7-1 associato alla traccia audio digitale campione della voce del soggetto 7-1, in cui detta traccia audio digitale campione viene generata per mezzo della conversione da analogico a digitale della voce del soggetto 7-1 acquisita in tempo reale (cioè durante la prima fase di abilitazione pagamento che verrà illustrata in seguito) per mezzo del microfono integrato nel dispositivo elettronico 8-1.

Con il termine "profilo vocale/facciale campione" si intendono dati associati ad una combinazione della traccia audio digitale campione della voce del soggetto 7-1 e di dati biometrici associati alla faccia del soggetto 7-1, questi ultimi generati per mezzo di una immagine della faccia del soggetto 7-1 acquisita in tempo reale (cioè durante la prima fase di abilitazione pagamento che verrà illustrata in seguito) per mezzo di una fotocamera integrata nel dispositivo elettronico 8-1.

Con il termine "codice oculare campione" si intende un codice univoco che viene generato in tempo reale (cioè durante la prima fase di abilitazione pagamento che verrà illustrata in seguito) in funzione di almeno un parametro biometrico degli occhi del soggetto 7-1, per mezzo di un opportuno algoritmo che prende in ingresso uno o più parametri associati agli occhi del soggetto 7-1.

Pertanto con il termine "profilo vocale/facciale campione+ codice oculare campione" si intendono dati associati ad una combinazione della traccia audio digitale campione della voce del soggetto 7-1, di dati biometrici associati alla faccia del soggetto 7-1 e di uno o più parametri biometrici degli occhi del soggetto 7-1 (ad esempio, colore dell'iride, colore della sclera, colore della cornea, diametro degli occhi, distanza della pupilla dall'angolo

interno dell'occhio, distanza della pupilla dall'angolo esterno dell'occhio, dimensione e forma delle sopracciglia).

Per maggiori dettagli relativamente alla verifica della identità digitale di un soggetto si faccia riferimento alla domanda di brevetto 5 PCT/IB2021/055428, che si considera incorporata all'interno della presente descrizione.

Per maggiori dettagli relativamente alla generazione di un codice oculare campione/di riferimento si faccia riferimento alla domanda di brevetto Italiano num. 102021000011753 depositata il 7 maggio 2021 a nome della 10 stessa Richiedente, che si considera incorporata all'interno della presente descrizione.

Con riferimento alle Figure 3A-3B, viene mostrato un andamento temporale dei messaggi scambiati fra i diversi componenti del sistema elettronico di abilitazione pagamento 1 secondo la prima forma di 15 realizzazione dell'invenzione.

Le Figure 3A-3B mostrano quindi come viene implementato il metodo di abilitazione pagamento secondo la prima forma di realizzazione dell'invenzione, per mezzo di opportuni programmi software eseguiti su rispettive unità di elaborazione del primo dispositivo elettronico 8-1, del 20 secondo dispositivo elettronico 8-2, dei dispositivi elettronici che formano il sotto-sistema di autenticazione 10 e dei dispositivi elettronici del sotto-sistema di condivisione messaggi 20.

E' possibile osservare che sono presenti due fasi temporali:

- una prima fase di abilitazione pagamento compresa fra l'istante iniziale t0 e l'istante t19, in cui viene effettuata l'identificazione del soggetto 7-1 per mezzo della verifica della sua identità digitale, poi viene effettuata una condivisione dell'identificativo operazione univoco che contiene un comando di trasferimento di denaro ed un identificativo utenti che identifica gli utenti coinvolti nell'operazione di pagamento, ed infine viene effettuata 30 l'identificazione del soggetto 7-2 per mezzo della verifica della sua identità digitale;

- una successiva seconda fase di pagamento effettivo compresa fra l'istante t20 e l'istante t33, in cui viene eseguito il trasferimento di denaro fra un conto corrente del soggetto 7-1 ed un conto corrente del soggetto 7-2.

Nella prima fase il sotto-sistema di autenticazione 10 ha quindi la 5 funzione di gestire l'autenticazione dei soggetti 7-1, 7-2 e di generare il valore dell'identificativo operazione, mentre nella seconda fase ha l'ulteriore funzione di gestire il pagamento effettivo relativo al trasferimento di denaro: pertanto verrà utilizzato in seguito il termine "sotto-sistema di autenticazione e gestione pagamento 10" per indicare la doppia funzione effettuata dal 10 sotto-sistema 10.

Per semplicità si suppone che il dispositivo elettronico 8-1 sia uno smartphone dotato di una fotocamera integrata frontale 2 e che il servizio richiesto sia il trasferimento di un importo definito di denaro dal conto corrente bancario del soggetto 7-1 al conto corrente bancario del soggetto 15 7-2.

Si suppone inoltre che il sotto-sistema di condivisione messaggi 20 sia implementato per mezzo dell'applicazione software per smartphone WhatsApp.

All'istante iniziale t0 il soggetto 7-1 avvia una opportuna applicazione 20 software sul suo smartphone 8-1 ed inizia la prima fase di abilitazione pagamento: l'unità di elaborazione dello smartphone 8-1 genera (ad esempio in seguito al tocco di una icona rappresentata sullo schermo tattile dello smartphone 8-1) una richiesta di generazione di un identificativo di un comando di trasferimento di denaro dal soggetto 7-1 al soggetto 7-2.

25 Successivamente, il ricetrasmettitore senza fili a media-lunga distanza dello smartphone 8-1 trasmette, verso il sotto-sistema di autenticazione e gestione pagamento 10, un messaggio che trasporta una richiesta di generazione dell'identificativo del comando di trasferimento di denaro.

All'istante t1 (successivo a t0) il sotto-sistema di autenticazione e 30 gestione pagamento 10 riceve detto messaggio della richiesta di generazione dell'identificativo del comando di trasferimento di denaro e quindi viene generato, per mezzo del dispositivo server 105 del sotto-sistema di

autenticazione e gestione pagamento 10, un identificativo operazione univoco che contiene informazioni indicative di un comando di trasferimento di denaro e contiene un identificativo utenti che identifica i soggetti 7-1 e 7-2 coinvolti nell'operazione di trasferimento di denaro: il valore dell'identificativo operazione generato viene quindi memorizzato in una memoria associata al dispositivo server 105, in cui la memoria può essere interna al dispositivo server 105 oppure può essere collegata esternamente ad esso.

5 All'istante t2 (successivo a t1) il sotto-sistema di autenticazione e gestione pagamento 10 trasmette, verso lo smartphone 8-1, un messaggio 10 che trasporta il valore di detto identificativo operazione generato.

All'istante t3 (successivo a t2) il ricetrasmettitore dello smartphone 8-1 riceve il messaggio che trasporta il valore dell'identificativo operazione, quindi detto messaggio viene inoltrato all'unità di elaborazione dello smartphone 8-1.

15 All'istante t4 (successivo a t3) l'unità di elaborazione dello smartphone 8-1 genera una richiesta di verifica della identità digitale del soggetto 7-1 e la inoltra al ricetrasmettitore senza fili dello smartphone 8-1, quindi il ricetrasmettitore senza fili dello smartphone 8-1 trasmette, verso il sotto-sistema di autenticazione e gestione pagamento 10, un messaggio indicativo 20 di una richiesta di verifica dell'identità digitale del soggetto 7-1.

All'istante t5 (successivo a t4) il sotto-sistema di autenticazione e gestione pagamento 10 riceve il messaggio indicativo della richiesta di verifica dell'identità digitale del soggetto 7-1 e viene effettuata, per mezzo del sotto-sistema di autenticazione e gestione pagamento 10, una verifica 25 positiva dell'identità digitale del soggetto 7-1.

Per esempio, la verifica dell'identità digitale del soggetto 7-1 viene effettuata per mezzo del controllo di un profilo biometrico vocale del soggetto 7-1, effettuando un confronto fra un profilo vocale campione del soggetto 7-1 generato in tempo reale ed un profilo vocale di riferimento del soggetto 7-1 30 generato in una precedente fase di profilazione in condizioni di sicurezza, in cui il profilo vocale di riferimento è stato memorizzato in parte in una memoria associata al dispositivo server 56 ed in parte in una memoria

associata al dispositivo server 106, in cui detto confronto può essere effettuato nel dispositivo server 105 oppure nello smartphone 8-1, come descritto in dettaglio rispettivamente nella Figura 3 o nella Figura 5 della domanda di brevetto PCT/IB2021/055428.

5 All'istante t6 (successivo a t5) il sotto-sistema di autenticazione e gestione pagamento 10 trasmette, verso lo smartphone 8-1, un messaggio di conferma della verifica positiva dell'identità digitale del soggetto 7-1.

10 All'istante t7 (successivo a t6) il ricetrasmettitore senza fili dello smartphone 8-1 riceve il messaggio di conferma della verifica positiva dell'identità digitale del soggetto 7-1, quindi detto messaggio di conferma viene inoltrato all'unità di elaborazione dello smartphone 8-1.

15 All'istante t8 (successivo a t7) l'unità di elaborazione dello smartphone 8-1 genera una richiesta di condivisione con il secondo smartphone 8-2 (e quindi con il secondo soggetto 7-2) dell'identificativo operazione che contiene il comando di trasferimento di denaro e l'identificativo utenti che identifica i soggetti 7-1 e 7-2, quindi all'istante t9 (successivo a t8) il ricetrasmettitore senza fili dello smartphone 8-1 trasmette, verso il secondo smartphone 8-2 attraverso il sotto-sistema di condivisione messaggi 20, un messaggio WhatsApp che trasporta il valore dell'identificativo operazione contenente il comando di trasferimento di denaro e l'identificativo utenti che identifica i soggetti 7-1 e 7-2.

20 All'istante t11 (successivo a t9) il secondo smartphone 8-2 del secondo soggetto 7-2 riceve, per mezzo di un ricetrasmettitore senza fili a media-lunga distanza, il messaggio WhatsApp che trasporta il valore dell'identificativo operazione contenente il comando di trasferimento di denaro e contenente l'identificativo utenti che identifica i soggetti 7-1 e 7-2, quindi detto messaggio WhatsApp viene inoltrato all'unità di elaborazione dello smartphone 8-2.

25 Successivamente l'unità di elaborazione dello smartphone 8-2 decodifica il valore dell'identificativo operazione effettuando una decrittografia dell'identificativo operazione, quindi estrae da questo le informazioni che indicano che si tratta del comando di trasferimento di

denaro e rileva che il trasferimento di denaro è dal soggetto 7-1 al soggetto 7-2.

In altre parole, l'unità di elaborazione dello smartphone 8-2 rileva che l'identificativo operazione è stato trasmesso dallo smartphone 8-1 del 5 soggetto 7-1 (identificato in precedenza) allo smartphone 8-2 del soggetto 7-2 (che non è stato invece ancora identificato) e che il comando di trasferimento di denaro è dal soggetto 7-1 verso il soggetto 8-2: in questo modo lo smartphone 8-2 rileva che il soggetto 7-1 ha richiesto (per mezzo del suo smartphone 8-1) un trasferimento di denaro al soggetto 7-2 al quale 10 appartiene lo smartphone 8-2, ovvero è stata associata al soggetto 7-1 la richiesta di trasferimento di denaro verso il soggetto 7-2.

Successivamente l'unità di elaborazione dello smartphone 8-2 genera una richiesta di verifica dell'identità digitale del soggetto 7-2 e inoltra detta richiesta al ricetrasmettitore senza fili dello smartphone 8-2.

15 All'istante t12 (successivo a t11) il ricetrasmettitore senza fili dello smartphone 8-2 trasmette, verso il sotto-sistema di autenticazione e gestione pagamento 10, un messaggio che trasporta detta richiesta di verifica dell'identità digitale del soggetto 7-2.

20 All'istante t13 (successivo a t12) il sotto-sistema di autenticazione e gestione pagamento 10 riceve il messaggio che trasporta detta richiesta di verifica della identità digitale del soggetto 7-2 e viene effettuata, per mezzo del sotto-sistema di autenticazione e gestione pagamento 10, una verifica positiva dell'identità digitale del soggetto 7-2.

25 La verifica dell'identità digitale del soggetto 7-2 viene effettuata analogamente a quella sopra indicata del soggetto 7-1, alla quale si rimanda per maggiori dettagli.

All'istante t14 (successivo a t13) il sotto-sistema di autenticazione e gestione pagamento 10 trasmette, verso lo smartphone 8-2, un messaggio di conferma della verifica positiva dell'identità digitale del soggetto 7-2.

30 All'istante t15 (successivo a t14) il ricetrasmettitore senza fili dello smartphone 8-2 riceve il messaggio indicativo della conferma della verifica

positiva dell'identità digitale del soggetto 7-2, quindi detto messaggio viene inoltrato all'unità di elaborazione dello smartphone 8-2.

Successivamente l'unità di elaborazione dello smartphone 8-2 genera una richiesta di autorizzazione al trasferimento di denaro dal soggetto 7-1 al soggetto 7-2 e inoltra detta richiesta di autorizzazione al ricetrasmettitore senza fili dello smartphone 8-2.

Successivamente il ricetrasmettitore senza fili dello smartphone 8-2 trasmette, verso il sotto-sistema di autenticazione e gestione pagamento 10, un messaggio di richiesta di una autorizzazione al trasferimento di denaro dal soggetto 7-1 al soggetto 7-2.

All'istante t16 (successivo a t15) il sotto-sistema di autenticazione e gestione pagamento 10 riceve il messaggio che trasporta detta richiesta di autorizzazione al trasferimento di denaro e viene concessa l'autorizzazione al trasferimento di denaro fra il soggetto 7-1 identificato in precedenza ed il soggetto 7-2 anch'esso identificato in precedenza: infatti è stato stabilito con successo un collegamento punto-punto sicuro fra il primo smartphone 8-1 del soggetto 7-1 e il secondo smartphone 8-2 del soggetto 7-2, in quanto è stata precedentemente verificata con successo sia l'identità digitale del soggetto 7-1, sia l'identità digitale del soggetto 7-2, ed inoltre il soggetto 7-2 ha di fatto certificato la sua identità e confermato che è lui la persona abilitata a ricevere il trasferimento di denaro.

All'istante t17 (successivo a t16) il sotto-sistema di autenticazione e gestione pagamento 10 trasmette, verso lo smartphone 8-1 e verso lo smartphone 8-2, un rispettivo messaggio indicativo di una conferma positiva ad un collegamento punto-punto fra lo smartphone 8-1 e lo smartphone 8-2, che quindi sono fra di loro collegati direttamente in modo sicuro.

All'istante t18 (successivo a t17) lo smartphone 8-1 riceve detto messaggio indicativo della conferma positiva al collegamento punto-punto e analogamente all'istante t19 (successivo a t17) lo smartphone 8-2 riceve detto messaggio indicativo della conferma positiva al collegamento punto-punto.

All'istante t20 inizia la seconda fase, in cui viene effettuato il trasferimento di denaro per mezzo del controllo effettuato dal sotto-sistema di autenticazione e gestione pagamento 10.

In particolare, all'istante t20 il sotto-sistema di autenticazione e  
5 gestione pagamento 10 (che nella prima fase di abilitazione pagamento ha ricevuto l'informazione relativa al tipo di operazione di trasferimento di denaro fra il soggetto 7-1 ed il soggetto 7-2 ed ha effettuato con successo la verifica dell'identità digitale dei due soggetti 7-1, 7-2) trasmette, verso il secondo dispositivo server di pagamento 9-2, un messaggio indicativo di una  
10 richiesta di informazioni del conto corrente bancario del soggetto 7-2.

All'istante t21 (successivo a t20) il ricetrasmettitore del secondo dispositivo server di pagamento 9-2 riceve detto messaggio indicativo della richiesta di informazioni del conto corrente bancario del soggetto 7-2 e inoltra il messaggio all'unità di elaborazione del secondo dispositivo server di  
15 pagamento 9-2, quindi l'unità di elaborazione del secondo dispositivo server di pagamento 9-2 riceve dati indicativi del conto corrente bancario del soggetto 7-2, come ad esempio il numero del suo conto corrente bancario; successivamente l'unità di elaborazione del secondo dispositivo server di pagamento 9-2 inoltra i dati indicativi del conto corrente bancario del  
20 soggetto 7-2 al ricetrasmettitore del secondo dispositivo server di pagamento 9-2, il quale trasmette (verso il sotto-sistema di autenticazione e gestione pagamento 10) un messaggio che trasporta detti dati indicativi del conto corrente bancario del soggetto 7-2.

All'istante t23 (successivo a t21) il sotto-sistema di autenticazione e  
25 gestione pagamento 10 riceve il messaggio che trasporta detti dati indicativi del conto corrente bancario del soggetto 7-2, quindi all'istante t24 (successivo a t23) il sotto-sistema di autenticazione e gestione pagamento 10 trasmette, dal dispositivo server 105 verso il primo dispositivo server di pagamento 9-1, un messaggio indicativo di una richiesta di trasferimento di  
30 denaro dal conto corrente del soggetto 7-1 al conto corrente del soggetto 7-2, in cui detto messaggio comprende anche i dati indicativi del conto corrente bancario del soggetto 7-2.

All'istante t25 (successivo a t24) il ricetrasmettitore del primo dispositivo server di pagamento 9-1 riceve il messaggio indicativo della richiesta di trasferimento di denaro e inoltra detto messaggio all'unità di elaborazione del primo dispositivo server di pagamento 9-1, quindi l'unità di elaborazione del primo dispositivo server di pagamento 9-1 riceve i dati indicativi del conto corrente bancario del soggetto 7-1.

Successivamente l'unità di elaborazione del primo dispositivo server di pagamento 9-1 inoltra i dati indicativi del conto corrente bancario del soggetto 7-1 al ricetrasmettitore, il quale trasmette (verso il secondo dispositivo server di pagamento 9-2) un messaggio che trasporta detti dati indicativi del conto corrente bancario del soggetto 7-1.

All'istante t27 (successivo a t25) il ricetrasmettitore del secondo dispositivo server di pagamento 9-2 riceve detto messaggio che trasporta i dati indicativi del conto corrente bancario del soggetto 7-1, i quali vengono inoltrati all'unità di elaborazione del secondo dispositivo server di pagamento 9-2.

Successivamente, l'unità di elaborazione del secondo dispositivo server di pagamento 9-2 genera un messaggio indicativo di una conferma di avvenuto trasferimento di denaro dal conto corrente bancario del soggetto 7-1 al conto corrente bancario del soggetto 7-2 ed inoltra detto messaggio al ricetrasmettitore del secondo dispositivo server di pagamento 9-2, il quale trasmette verso il primo dispositivo server di pagamento 9-1 detto messaggio indicativo di una conferma di avvenuto trasferimento di denaro.

All'istante t29 (successivo a t27) il ricetrasmettitore del primo dispositivo server di pagamento 9-1 riceve detto messaggio indicativo della conferma di avvenuto trasferimento di denaro, quindi detto messaggio viene inoltrato verso il sotto-sistema di autenticazione e gestione pagamento 10.

All'istante t30 (successivo a t29) il sotto-sistema di autenticazione e gestione pagamento 10 riceve detto messaggio indicativo della conferma di avvenuto trasferimento di denaro, quindi all'istante t31 (successivo a t30) il sotto-sistema di autenticazione e gestione pagamento 10 trasmette, verso lo

smartphone 8-1 e verso lo smartphone 8-2, un rispettivo messaggio indicativo di una conferma di avvenuto trasferimento di denaro.

All'istante t32 (successivo a t31) lo smartphone 8-1 riceve detto messaggio indicativo della conferma di avvenuto trasferimento di denaro e 5 analogamente all'istante t33 (successivo a t31) lo smartphone 8-2 riceve detto messaggio indicativo della conferma di avvenuto trasferimento di denaro.

Si osservi che in Figura 3A è stato mostrato che prima viene effettuato il riconoscimento dell'identità del soggetto 7-1 e successivamente viene 10 effettuata la generazione e condivisione dell'identificativo operazione, ma è anche possibile il contrario, ovvero prima viene effettuata la generazione e condivisione dell'identificativo operazione e successivamente viene effettuato il riconoscimento della identità del soggetto 7-1.

Con riferimento alla Figura 4, viene mostrato un sistema elettronico 15 101 per abilitare un pagamento di denaro per mezzo di un collegamento punto-punto in base ad una seconda forma di realizzazione dell'invenzione.

Nella seconda forma di realizzazione il soggetto 7-1 effettua il pagamento di un bene presso un punto vendita 108, utilizzando nuovamente un collegamento punto-punto con il punto vendita.

20 Con il termine "punto vendita" 108 si intende una postazione (ad esempio, una cassa) presso un luogo fisico (ad esempio, un negozio, un supermercato) in cui sono presenti dei prodotti in vendita (per esempio, prodotti alimentari) che possono essere acquistati dal soggetto 7-1 che si reca nel punto vendita 108, effettuando il pagamento presso una cassa 25 all'interno del punto vendita 108 per mezzo di una cassiera 107 o per mezzo di una cassa automatizzata che non richiede la presenza della cassiera.

Il sistema elettronico di abilitazione pagamento 101 della seconda forma di realizzazione di Figura 4 differisce pertanto dal sistema elettronico di abilitazione pagamento 1 della prima forma di realizzazione della Figura 1 30 per il fatto che è presente un punto vendita 108 al posto del secondo dispositivo elettronico 8-2 e per il fatto che è presente una cassiera 107 al posto del secondo soggetto 7-2.

Inoltre il sistema elettronico di abilitazione pagamento 101 differisce dal sistema elettronico di abilitazione pagamento 1 per il fatto che l'identità del punto vendita 108 è stata verificata con successo in una fase di registrazione precedente a quella in cui viene effettuata l'operazione di pagamento da parte del soggetto 7-1, pertanto durante la prima fase di abilitazione pagamento non viene effettuata la verifica dell'identità digitale del punto vendita 108 che si ritiene attendibile e quindi l'identificativo operazione generato viene utilizzato per identificare l'identità del soggetto 7-1 e per associare a lui una richiesta di pagamento.

Il secondo dispositivo server di pagamento 109 della seconda forma di realizzazione ha una funzione simile al secondo dispositivo server di pagamento 9-2 della prima forma di realizzazione, ovvero il secondo dispositivo server di pagamento 109 è un gateway di pagamento che è posizionato presso una banca o una istituzione finanziaria che gestisce sistemi di pagamento ed ha la funzione di gestire il pagamento verso il secondo punto vendita 108; in particolare, il secondo dispositivo server di pagamento 109 gestisce un conto corrente che appartiene al punto vendita 108.

Il punto vendita 108 è dotato di un opportuno lettore o di una applicazione software in grado di acquisire (ad esempio con una scansione ottica) una rappresentazione grafica o testuale contenente l'identificativo operazione che contiene il comando di pagamento di un bene o servizio e contiene l'identificativo utenti che identifica il soggetto 7-1 ed il punto vendita 108, in cui la rappresentazione grafica contenente l'identificativo è ad esempio un codice a barre oppure un codice QR (Quick Response).

In particolare, nella seconda forma di realizzazione il primo dispositivo elettronico 8-1 è configurato per ricevere il messaggio di conferma e generare da questo una richiesta di condivisione dell'identificativo operazione con un punto vendita 108, è configurato per visualizzare , sul suo schermo, dati che contengono l'identificativo operazione contenente il comando di pagamento e l'identificativo utenti che identifica il soggetto 7-1 ed il punto vendita 108, ed è configurato per ricevere un messaggio indicativo di una

conferma positiva o negativa ad un collegamento punto-punto fra il primo dispositivo elettronico 8-1 ed il punto vendita 108.

Inoltre nella seconda forma di realizzazione il punto vendita 108 è configurato per acquisire, per mezzo di un lettore ottico, detti dati visualizzati 5 contenenti l'identificativo operazione che contiene il comando di pagamento e l'identificativo utenti, è configurato per estrarre dai dati visualizzati il valore dell'identificativo operazione e rilevare che il pagamento è stato richiesto dal primo soggetto 7-1 verso il punto vendita 108, ed è configurato per trasmettere, verso il sotto-sistema di autenticazione e gestione pagamento 10, 10 un messaggio che trasporta un valore indicativo di un importo di denaro associato al pagamento del bene o servizio.

Inoltre nella seconda forma di realizzazione il sotto-sistema di autenticazione e gestione pagamento 10 è configurato per ricevere detto messaggio e generare da questo una autorizzazione concessa ad effettuare 15 detto pagamento del bene o servizio, ed è configurato per trasmettere, verso il primo dispositivo elettronico 8-1, un messaggio indicativo di una conferma positiva ad un collegamento punto-punto fra il primo dispositivo elettronico 8-1 ed il punto vendita 108.

Con riferimento alle Figure 5A-5B, viene mostrato un andamento 20 temporale dei messaggi scambiati fra i diversi componenti del sistema elettronico di abilitazione pagamento 101 in base alla seconda forma di realizzazione dell'invenzione.

Le Figure 5A-5B mostrano quindi come viene implementato il metodo 25 di abilitazione pagamento in base alla seconda forma di realizzazione dell'invenzione.

E' possibile osservare che sono presenti due fasi temporali:

- una prima fase di abilitazione pagamento compresa fra l'istante iniziale t0 e l'istante t119, in cui viene effettuata l'identificazione del soggetto 7-1 per mezzo della verifica della sua identità digitale e viene effettuata una 30 generazione e condivisione dell'identificativo operazione contenente un comando di pagamento di denaro e contenente un identificativo utenti che

identifica gli utenti coinvolti nell'operazione di pagamento, ovvero il soggetto 7-1 ed il punto vendita 108;

- una successiva seconda fase di pagamento effettivo compresa fra l'istante t200 e l'istante t303, in cui viene eseguito il pagamento di denaro di 5 un bene o servizio.

Il funzionamento fra gli istanti t0 e t8 della Figura 5A è uguale a quello illustrato in precedenza per la Figura 3A, con la differenza che vengono generati e visualizzati, sullo schermo dello smartphone 8-1, dati in forma grafica o testuale che contengono un identificativo operazione contenente un 10 comando di pagamento di denaro (invece del comando di trasferimento di denaro) e contenente un identificativo utenti che identifica il soggetto 7-1 ed il punto vendita 108 (invece dei soggetti 7-1 e 7-2).

Si suppone che i dati visualizzati (che contengono l'identificativo operazione del comando di pagamento di denaro e l'identificativo utenti) 15 siano rappresentati con un codice a barre, che il punto vendita 108 sia una cassa di un negozio di generi alimentari in cui è presente una cassiera 107 dotata di un lettore ottico di codici a barre e che il soggetto 7-1 voglia pagare un prodotto alimentare presso la cassa 108.

All'istante t109 (successivo a t8) sullo schermo dello smartphone 8-1 20 vengono visualizzati dati (ad esempio, un codice a barre) che contengono l'identificativo operazione contenente il comando di pagamento di denaro e l'identificativo utenti che identifica il soggetto 7-1 ed il punto vendita 108.

All'istante t110 (successivo a t109) la cassiera 107 effettua la 25 scansione del codice a barre visualizzato sullo schermo per mezzo di un lettore ottico collegato con la cassa 108, quindi viene acquisito il codice a barre contenente l'identificativo operazione, viene estratto da questo (per mezzo di una unità di elaborazione del lettore ottico o della cassa) il valore dell'identificativo operazione che contiene il comando di pagamento di denaro e contiene l'identificativo utenti che identifica il soggetto 7-1 ed il 30 punto vendita 108. Viene quindi rilevato (per mezzo della scansione del codice a barre) che l'identificativo operazione è stato trasmesso dallo smartphone 8-1 del soggetto 7-1 e che il comando di pagamento è dal

soggetto 7-1 verso il punto vendita 108: in questo modo la cassa 108 rileva che il soggetto 7-1 ha richiesto (per mezzo del suo smartphone 8-1) un pagamento di denaro verso la cassa 108, ovvero è stata associata al soggetto 7-1 la richiesta di pagamento verso il punto vendita 108.

5 All'istante t114 (successivo a t110) la cassa 108 trasmette, verso il sotto-sistema di autenticazione e gestione pagamento 10, un messaggio che trasporta un valore indicativo dell'importo di denaro associato al pagamento di un bene o servizio richiesto dal soggetto 7-1, che nel caso considerato è il pagamento di un prodotto alimentare.

10 All'istante t116 (successivo a t114) il sotto-sistema di autenticazione e gestione pagamento 10 riceve il messaggio che trasporta detto valore indicativo dell'importo di denaro associato al pagamento richiesto e viene concessa l'autorizzazione al pagamento del bene o servizio, che nel caso considerato è il pagamento di un prodotto alimentare: infatti è stato stabilito 15 con successo un collegamento punto-punto sicuro fra lo smartphone 8-1 del soggetto 7-1 e la cassa 108, in quanto è stata precedentemente verificata con successo l'identità digitale del soggetto 7-1 ed inoltre è stata precedentemente associata la richiesta di pagamento al soggetto 7-1 dello smartphone 8-1 .

20 All'istante t117 (successivo a t116) il sotto-sistema di autenticazione e gestione pagamento 10 trasmette, verso lo smartphone 8-1 e verso la cassa 108, un rispettivo messaggio indicativo di una conferma positiva ad un collegamento punto-punto fra lo smartphone 8-1 e la cassa 108, che quindi sono fra di loro collegati direttamente in modo sicuro.

25 All'istante t118 (successivo a t117) lo smartphone 8-1 riceve detto messaggio indicativo della conferma positiva al collegamento punto-punto e analogamente all'istante t119 (successivo a t117) la cassa 108 riceve detto messaggio indicativo della conferma positiva al collegamento punto-punto.

Il funzionamento della seconda fase fra gli istanti t200 e t303 della 30 Figura 5B è analoga a quella illustrata in precedenza fra gli istanti t20 e t33 della Figura 3B, con la differenza che è presente la cassa 108 al posto del secondo smartphone 8-2 e che il secondo dispositivo server di pagamento 9-

2 è la banca in cui è stato aperto un conto corrente bancario del negozio in cui è posizionata la cassa 108.

Vantaggiosamente, viene effettuata una crittografia asimmetrica del valore generato dell'identificativo operazione per proteggere l'identificativo operazione visualizzato sullo schermo del dispositivo elettronico 8-1: in questo modo il valore cifrato dell'identificativo operazione risulta anonimo, ovvero le informazioni contenute nell'identificativo operazione non possono essere interpretate da un essere umano che osserva lo schermo del dispositivo elettronico 8-1 in quanto non sono in chiaro, mentre possono essere interpretate dal lettore ottico e/o dal punto vendita 108 in cui viene effettuata (per mezzo di una chiave pubblica) la decrittografia dell'identificativo operazione acquisito.

Secondo una terza forma di realizzazione dell'invenzione (non mostrata nelle Figure), il punto vendita 108 è sostituito da un sito web di un negozio virtuale online di commercio elettronico al quale si collega il soggetto 7-1, utilizzando il suo dispositivo elettronico 8-1.

L'identità del negozio virtuale è stata verificata con successo in una fase di registrazione precedente a quella in cui viene effettuata l'operazione di pagamento online da parte del soggetto 7-1, pertanto durante la prima fase di abilitazione pagamento non viene effettuata la verifica dell'identità digitale del negozio virtuale che si ritiene attendibile e quindi l'identificativo operazione generato viene utilizzato per identificare l'identità soltanto del soggetto 7-1 e per associare a lui la richiesta di pagamento online.

In questo caso la seconda forma di realizzazione viene modificata in modo che all'istante t109 il ricetrasmettitore a media-lunga distanza del dispositivo elettronico 8-1 trasmette, verso il sito web del negozio virtuale, un pacchetto dati (per esempio, su rete Internet con protocollo TCP/IP) che trasporta l'identificativo operazione che contiene il comando di pagamento di un bene o servizio richiesto dal soggetto 7-1 e contiene l'identificativo utenti che identifica il primo soggetto 7-1 ed il sito web.

All'istante t110 il sito web del negozio virtuale riceve detto pacchetto dati, estraе (dal pacchetto dati) il valore dell'identificativo operazione e poi

estrae (dal valore dell'identificativo operazione) il comando di pagamento di un bene o servizio e l'identificativo utenti che identifica il primo soggetto 7-1 ed il sito web.

All'istante t114 il sito web del negozio virtuale trasmette, verso il sottosistema di autenticazione e gestione pagamento 10, un pacchetto dati che trasporta un valore indicativo dell'importo di denaro associato al pagamento richiesto del bene o servizio.

Il funzionamento dall'istante t116 prosegue analogamente a quanto illustrato in precedenza per la seconda forma di realizzazione.

10

#### IL MANDATARIO

Ing. Giancarlo PENZA  
(Albo iscr. n. 1335 B)

## RIVENDICAZIONI

1. Metodo realizzato mediante almeno un elaboratore elettronico per abilitare una operazione a distanza per mezzo di un collegamento punto-punto, il metodo comprendente i passi di:
  - 5 a) trasmettere (t0), da un primo dispositivo elettronico (8-1) ad un sistema elettronico di autenticazione (10), un primo messaggio indicativo di una richiesta di generare un identificativo di una operazione di collegamento punto-punto fra un primo soggetto (7-1) associato al primo dispositivo elettronico (8-1) ed un secondo soggetto (7-2) associato ad un secondo dispositivo elettronico (8-2);
    - 10 b) ricevere (t1), al sistema di autenticazione (10), il primo messaggio e generare (t2) da questo un identificativo operazione univoco che contiene informazioni indicative del tipo di operazione di collegamento punto-punto e contiene un identificativo utenti che identifica il primo soggetto (7-1) ed il secondo soggetto (7-2) coinvolti nell'operazione di collegamento punto-punto;
    - 15 c) trasmettere (t2), dal sistema di autenticazione (10) verso il primo dispositivo elettronico (8-1), un secondo messaggio che trasporta un valore di detto identificativo operazione generato;
  - 20 d) ricevere (t3), al primo dispositivo elettronico (8-1), il secondo messaggio e trasmettere (t4) da questo, verso il sistema di autenticazione (10), un terzo messaggio di richiesta di verifica di una identità digitale di un primo soggetto (7-1);
    - 25 e) ricevere (t5), al sistema di autenticazione (10), il terzo messaggio di richiesta e verificare (t5) con successo, per mezzo del sistema di autenticazione (10), l'identità digitale del primo soggetto;
    - f) trasmettere (t6), dal sistema di autenticazione (10) verso il primo dispositivo elettronico (8-1), un quarto messaggio di conferma di verifica positiva dell'identità digitale del primo soggetto (7-1);
  - 30 g) ricevere (t7), al primo dispositivo elettronico (8-1), il quarto messaggio di conferma e generare (t8) da questo una richiesta di condivisione dell'identificativo operazione con il secondo dispositivo elettronico (8-2);

associato ad un secondo soggetto (7-2);

h) trasmettere (t9), dal primo dispositivo elettronico (8-1) verso il secondo dispositivo elettronico (8-2) per mezzo di un sotto-sistema di condivisione messaggi (20), un quinto messaggio che trasporta un valore dell'identificativo operazione;

i) ricevere (t11), al secondo dispositivo elettronico (8-2), il quinto messaggio che trasporta il valore dell'identificativo operazione, estrarre da questo le informazioni indicative del tipo di operazione di collegamento punto-punto e l'identificativo utenti che identifica il primo soggetto (7-1) ed il secondo soggetto (7-2), e rilevare che l'operazione di collegamento punto-punto è stata richiesta dal primo soggetto (7-1) verso il secondo soggetto (7-2);

j) trasmettere (t12), dal secondo dispositivo elettronico (8-2) verso il sistema di autenticazione (10), un sesto messaggio di richiesta di verifica di una identità digitale del secondo soggetto (7-2) associato al secondo dispositivo elettronico (8-2);

k) ricevere (t13), al sistema di autenticazione (10), il sesto messaggio di richiesta e verificare con successo, per mezzo del sistema di autenticazione (10), l'identità digitale del secondo soggetto;

l) trasmettere (t14), dal sistema di autenticazione (10) verso il secondo dispositivo elettronico (8-2), un settimo messaggio di conferma di verifica positiva dell'identità digitale del secondo soggetto (7-2);

m) ricevere (t15), al secondo dispositivo elettronico (8-2), il settimo messaggio di conferma e trasmettere da questo, verso il sistema di autenticazione (10), un ottavo messaggio di richiesta di una autorizzazione di detta operazione di collegamento punto-punto;

n) ricevere (t16), al sistema di autenticazione (10), l'ottavo messaggio di richiesta e generare da questo una autorizzazione concessa ad effettuare detta operazione di collegamento punto-punto;

o) trasmettere, dal sistema di autenticazione (10) verso il primo dispositivo elettronico (8-1) e/o verso il secondo dispositivo elettronico (8-2), un nono messaggio indicativo di una conferma positiva all'operazione di

collegamento punto-punto fra il primo dispositivo elettronico (8-1) ed il secondo dispositivo elettronico (8-2).

2. Metodo di abilitazione operazione a distanza secondo la rivendicazione 1, in cui:

- 5 - nel passo a) l'operazione di collegamento punto-punto è una operazione di trasferimento di denaro fra un conto corrente associato al primo soggetto ed un conto corrente associato al secondo soggetto;
- nel passo i) viene rilevato che l'operazione è un trasferimento di denaro dal conto corrente del primo soggetto al conto corrente del secondo soggetto;
- nel passo m) l'ottavo messaggio è una richiesta di autorizzazione al trasferimento di denaro dal conto corrente del primo soggetto al conto corrente del secondo soggetto;
- nel passo n) viene generata l'autorizzazione concessa al trasferimento di denaro dal conto corrente del primo soggetto al conto corrente del secondo soggetto.

3. Metodo di abilitazione operazione a distanza secondo le rivendicazioni 1 o 2, in cui il secondo dispositivo elettronico è un punto vendita (108) di un negozio e l'operazione collegamento punto-punto è un pagamento di un bene o servizio presso il punto vendita,

il metodo comprendente, al posto dei passi g)-o), i passi di:

- g1) ricevere (t7), al primo dispositivo elettronico (8-1), il quarto messaggio di conferma e generare (t8) da questo una richiesta di condivisione dell'identificativo operazione con un punto vendita (108);
- 25 h1) visualizzare (t109), su uno schermo del primo dispositivo elettronico (8-1), dati che contengono l'identificativo operazione contenente un comando di pagamento e l'identificativo utenti che identifica il soggetto (7-1) ed il punto vendita (108);
- i1) acquisire (t110), al punto vendita (108) per mezzo di un lettore ottico, 30 detti dati visualizzati contenenti l'identificativo operazione che contiene il comando di pagamento e l'identificativo utenti, estrarre dai dati visualizzati il valore dell'identificativo operazione e rilevare che il pagamento è stato

richiesto dal primo soggetto (7-1) verso il punto vendita (108);

j1) trasmettere (t114), dal punto vendita (108) al sotto-sistema di autenticazione (10), un messaggio che trasporta un valore indicativo di un importo di denaro associato al pagamento del bene o servizio;

5 k1) ricevere (t116), al sotto-sistema di autenticazione (10), detto messaggio e generare da questo una autorizzazione concessa ad effettuare detto pagamento del bene o servizio;

l1) trasmettere, dal sistema di autenticazione (10) verso il primo dispositivo elettronico (8-1), un messaggio indicativo di una conferma

10 positiva ad un collegamento punto-punto fra il primo dispositivo elettronico (8-1) ed il punto vendita (108).

4. Metodo di abilitazione operazione a distanza secondo le rivendicazioni 1 o 2, in cui il secondo dispositivo elettronico è un negozio virtuale avente un sito web per acquisti online di un bene o servizio e l'operazione è un

15 pagamento online di un bene o servizio,

il metodo comprendente, al posto dei passi g)-o), i passi di:

g2) ricevere (t7), al primo dispositivo elettronico (8-1), il quarto messaggio di conferma e generare (t8) da questo una richiesta di condivisione dell'identificativo operazione con il sito web del negozio virtuale;

20 h2) trasmettere, dal primo dispositivo elettronico (8-1) verso il sito web attraverso una rete di telecomunicazioni, un pacchetto dati che trasporta l'identificativo operazione contenente un comando di pagamento di un bene o servizio e l'identificativo utenti che identifica il primo soggetto (7-1) ed il sito web;

25 i2) ricevere, al sito web, detto pacchetto dati, estrarre da questo un valore dell'identificativo operazione, estrarre da questo il comando di pagamento e l'identificativo utenti e rilevare che il pagamento è stato richiesto dal primo soggetto (7-1) verso il sito web;

j2) trasmettere, dal sito web del negozio virtuale al sistema di autenticazione (10), un messaggio che trasporta un valore indicativo di un importo di denaro associato al pagamento del bene o servizio;

k2) ricevere, al sistema di autenticazione (10), detto messaggio e

generare da questo una autorizzazione concessa ad effettuare detto pagamento del bene o servizio;

l2) trasmettere, dal sistema di autenticazione (10) verso il primo dispositivo elettronico (8-1), un messaggio indicativo di una conferma

5 positiva ad un collegamento punto-punto fra il primo dispositivo elettronico (8-1) ed il sito web del negozio virtuale.

5. Metodo di abilitazione operazione a distanza secondo la rivendicazione 1, in cui l'identificativo operazione è un link web.

6. Metodo di abilitazione operazione a distanza secondo una qualunque

10 delle precedenti rivendicazioni, in cui il primo dispositivo elettronico è un dispositivo mobile, selezionato fra uno smartphone, un tablet, un iPhone, un iPad.

7. Supporto di memorizzazione non-transitorio leggibile da un elaboratore elettronico avente un programma comprendente porzioni di

15 codice software atto ad eseguire i passi del metodo secondo le rivendicazioni 1-6, quando detto programma è eseguito su almeno un elaboratore elettronico.

8. Sistema elettronico per abilitare una operazione a distanza per mezzo di un collegamento punto-punto, il sistema comprendente un primo

20 dispositivo elettronico (8-1), un secondo dispositivo elettronico (8-2), un sotto-sistema di autenticazione (10) collegato con il primo e secondo dispositivo elettronico, un sotto-sistema di condivisione messaggi (20) per collegare fra di loro il primo dispositivo elettronico (8-1) con il secondo dispositivo elettronico (8-2) attraverso una rete di telecomunicazioni a media-  
25 lunga distanza (20),

in cui il primo dispositivo elettronico (8-1) è configurato per:

- trasmettere (t0), verso il sotto-sistema di autenticazione (10), un primo messaggio indicativo di una richiesta di generare un identificativo di una operazione di collegamento punto-punto fra un primo soggetto (7-1)

30 associato al primo dispositivo elettronico (8-1) ed un secondo soggetto (7-2) associato al secondo dispositivo elettronico (8-2);

- ricevere (t3) un secondo messaggio che trasporta un valore di un

identificativo operazione univoco che contiene informazioni indicative del tipo di operazione di collegamento punto-punto e contiene un identificativo utenti che identifica il primo soggetto (7-1) ed un secondo soggetto (7-2) coinvolti nell'operazione di collegamento punto-punto, e trasmettere (t4) da questo,

5 verso il sotto-sistema di autenticazione (10), un terzo messaggio di richiesta di verifica di una identità digitale di un primo soggetto (7-1);

- ricevere (t7) un quarto messaggio di conferma di verifica positiva dell'identità digitale del primo soggetto e generare (t8) da questo una richiesta di condivisione dell'identificativo univoco con un secondo dispositivo

10 elettronico (8-2);

- trasmettere (t9), verso il secondo dispositivo elettronico (8-2), un quinto messaggio che trasporta un valore dell'identificativo operazione;

- ricevere (t18) un sesto messaggio indicativo di una conferma positiva o negativa ad un collegamento punto-punto fra il primo dispositivo elettronico

15 (8-1) ed il secondo dispositivo elettronico (8-2);

in cui il sotto-sistema di autenticazione (10) è configurato per:

- ricevere (t1) il primo messaggio e generare (t2) da questo detto identificativo operazione univoco che contiene informazioni indicative del tipo di operazione di collegamento punto-punto e contiene l'identificativo utenti

20 che identifica il primo soggetto (7-1) ed il secondo soggetto (7-2) coinvolti nell'operazione di collegamento punto-punto;

- trasmettere (t2), verso il primo dispositivo elettronico (8-1), il secondo messaggio che trasporta il valore di detto identificativo operazione generato;

- ricevere (t5) il terzo messaggio di richiesta e verificare (t5) con

25 successo, per mezzo del sotto-sistema di autenticazione (10), l'identità digitale del primo soggetto;

- trasmettere (t6), verso il primo dispositivo elettronico (8-1), il quarto messaggio di conferma di verifica positiva dell'identità digitale del primo soggetto (7-1);

30 - ricevere (t13) un settimo messaggio di richiesta di verifica di una identità digitale di un secondo soggetto (7-2) e verificare con successo, per mezzo del sotto-sistema di autenticazione (10), l'identità digitale del secondo

soggetto;

- trasmettere (t14), verso il secondo dispositivo elettronico (8-2), un ottavo messaggio di conferma di verifica positiva dell'identità digitale del secondo soggetto (7-2);
- 5 - ricevere (t16) un nono messaggio di richiesta di una autorizzazione di detta operazione collegamento punto-punto e generare da questo una autorizzazione concessa ad effettuare detta operazione di collegamento punto-punto;
- trasmettere (t17), verso il primo dispositivo elettronico (8-1) e/o verso il 10 secondo dispositivo elettronico (8-2), il sesto messaggio indicativo della conferma positiva o negativa al collegamento punto-punto fra il primo dispositivo elettronico (8-1) ed il secondo dispositivo elettronico (8-2); in cui il sotto-sistema di condivisione messaggi (20) è configurato per inoltrare, dal primo dispositivo elettronico (8-1) verso il secondo dispositivo 15 elettronico (8-2), il quinto messaggio che trasporta un valore di detto identificativo operazione;
- ed in cui il secondo dispositivo elettronico (8-2) è configurato per:
  - ricevere (t11) il quinto messaggio che trasporta il valore dell'identificativo operazione, estrarre da questo le informazioni indicative del 20 tipo operazione di collegamento punto-punto e l'identificativo utenti che identifica il primo soggetto (7-1) ed il secondo soggetto (7-2), e rilevare che l'operazione di collegamento punto-punto è stata richiesta dal primo soggetto (7-1) verso il secondo soggetto (7-2);
  - trasmettere (t12), verso il sotto-sistema di autenticazione (10), il 25 settimo messaggio di richiesta di verifica dell'identità digitale del secondo soggetto (7-2) associato al secondo dispositivo elettronico (8-2);
  - ricevere (t15) l'ottavo messaggio di conferma e trasmettere da questo, verso il sotto-sistema di autenticazione (10), il nono messaggio di richiesta dell'autorizzazione di detta operazione di collegamento punto-punto;
  - 30 - ricevere (t19) il sesto messaggio indicativo della conferma positiva o negativa ad un collegamento punto-punto fra il primo dispositivo elettronico (8-1) ed il secondo dispositivo elettronico (8-2).

9. Sistema elettronico secondo la rivendicazione 8, in cui l'operazione di collegamento punto-punto è una operazione di trasferimento di denaro fra un conto corrente associato al primo soggetto ed un conto corrente associato al secondo soggetto,
- 5 in cui il secondo dispositivo elettronico (8-2) è ulteriormente configurato per:
  - rilevare che l'operazione è un trasferimento di denaro dal conto corrente del primo soggetto al conto corrente del secondo soggetto;
  - trasmettere l'ottavo messaggio di richiesta di una autorizzazione al trasferimento di denaro dal conto corrente del primo soggetto al conto 10 corrente del secondo soggetto;in cui il sistema di autenticazione è ulteriormente configurato per generare da questo una autorizzazione concessa al trasferimento di denaro dal conto corrente del primo soggetto al conto corrente del secondo soggetto.
10. Sistema elettronico secondo la rivendicazione 8, in cui il secondo dispositivo elettronico è un punto vendita (108) di un negozio e l'operazione di collegamento punto-punto è un pagamento di un bene o servizio presso il punto vendita,
  - 15 in cui il primo dispositivo elettronico (8-1) è configurato per:
    - ricevere (t7) il quarto messaggio di conferma e generare (t8) da questo una richiesta di condivisione dell'identificativo operazione con un punto vendita (108);
    - visualizzare (t109), sul suo schermo, dati che contengono l'identificativo operazione contenente il comando di pagamento e l'identificativo utenti che identifica il soggetto (7-1) ed il punto vendita (108);
  - 20 25 - ricevere un messaggio indicativo di una conferma positiva o negativa ad un collegamento punto-punto fra il primo dispositivo elettronico (8-1) ed il punto vendita (108);ed in cui il punto vendita (108) è configurato per:
  - 30 acquisire (t110), per mezzo di un lettore ottico, detti dati visualizzati contenenti l'identificativo operazione che contiene il comando di pagamento e l'identificativo utenti, estrarre dai dati visualizzati il valore dell'identificativo operazione e rilevare che il pagamento è stato richiesto dal primo soggetto

(7-1) verso il punto vendita (108);

- trasmettere (t114), verso il sotto-sistema di autenticazione (10), un messaggio che trasporta un valore indicativo di un importo di denaro associato al pagamento del bene o servizio;

5 ed in cui il sotto-sistema di autenticazione (10) è configurato per:

- ricevere (t116) detto messaggio e generare da questo una autorizzazione concessa ad effettuare detto pagamento del bene o servizio;

- trasmettere, verso il primo dispositivo elettronico (8-1), detto messaggio indicativo di una conferma positiva o negativa ad un

10 collegamento punto-punto fra il primo dispositivo elettronico (8-1) ed il punto vendita (108).

11. Sistema elettronico secondo la rivendicazione 8, in cui il secondo dispositivo elettronico è un negozio virtuale avente un sito web per acquisti online di un bene o servizio e l'operazione di pagamento è un pagamento

15 online di un bene o servizio,

in cui il primo dispositivo elettronico (8-1) è configurato per:

- ricevere (t7) il quarto messaggio di conferma e generare (t8) da questo una richiesta di condivisione dell'identificativo operazione con il sito web;

20 - trasmettere, dal primo dispositivo elettronico (8-1) verso il sito web attraverso una rete di telecomunicazioni, un pacchetto dati che trasporta l'identificativo operazione contenente un comando di pagamento di un bene o servizio e l'identificativo utenti che identifica il primo soggetto (7-1) ed il sito web;

25 - ricevere un messaggio indicativo di una conferma positiva o negativa ad un collegamento punto-punto fra il primo dispositivo elettronico (8-1) ed il sito web;

ed in cui il sito web è configurato per:

30 - ricevere detto pacchetto dati, estrarre da questo un valore dell'identificativo operazione, estrarre da questo il comando di pagamento e l'identificativo utenti e rilevare che il pagamento è stato richiesto dal primo soggetto (7-1) verso il sito web;

- trasmettere, verso il sotto-sistema di autenticazione (10), un messaggio che trasporta un valore indicativo di un importo di denaro associato al pagamento del bene o servizio;  
ed in cui il sotto-sistema di autenticazione (10) è configurato per:
  - 5 - ricevere (t116) detto messaggio e generare da questo una autorizzazione concessa ad effettuare detto pagamento del bene o servizio;
  - trasmettere, verso il primo dispositivo elettronico (8-1), detto messaggio indicativo della conferma positiva o negativa al collegamento punto-punto fra il primo dispositivo elettronico (8-1) ed il sito web.

10

**IL MANDATARIO**

Ing. Giancarlo PENZA  
(Albo iscr. n. 1335 B)

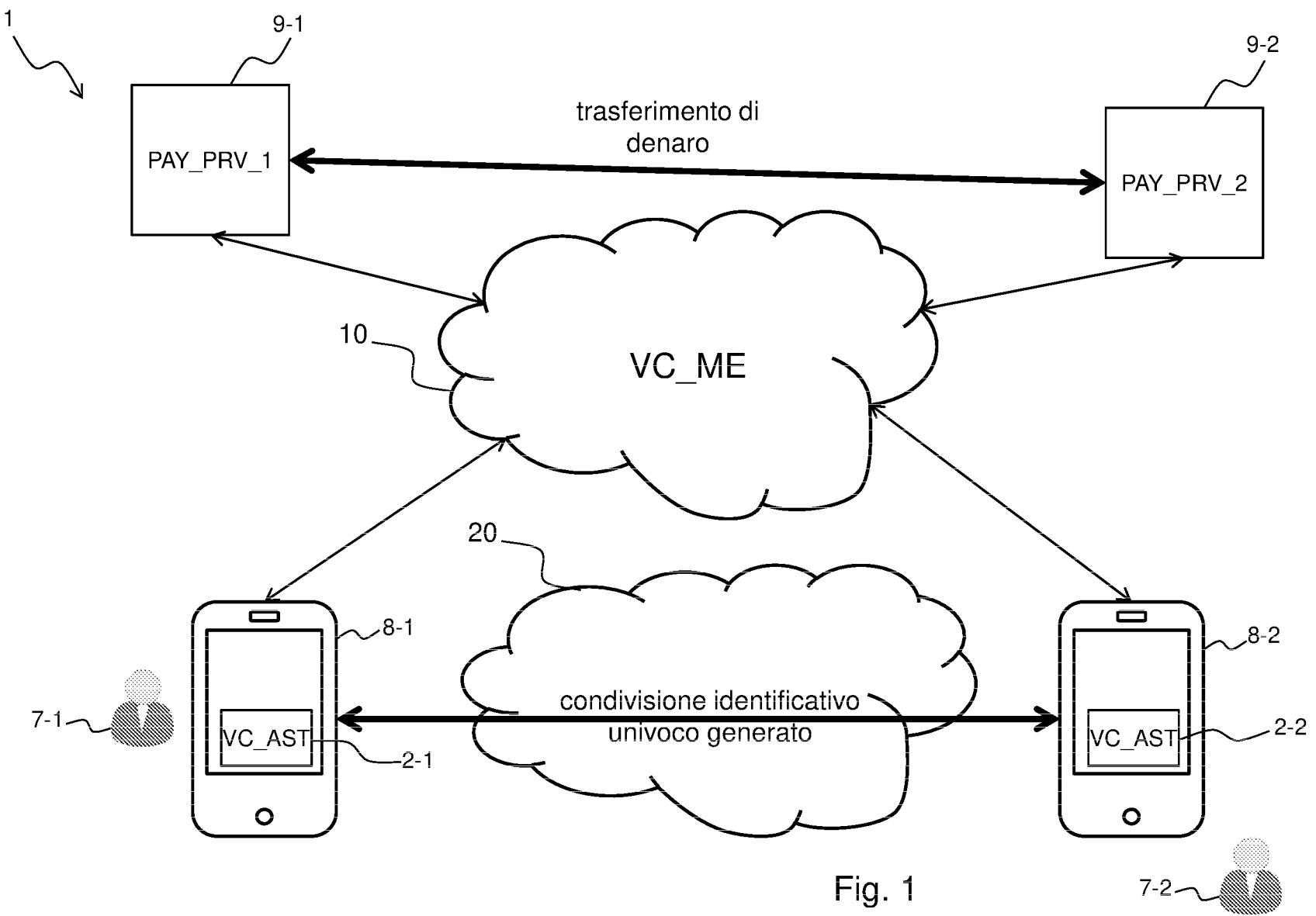


Fig. 1

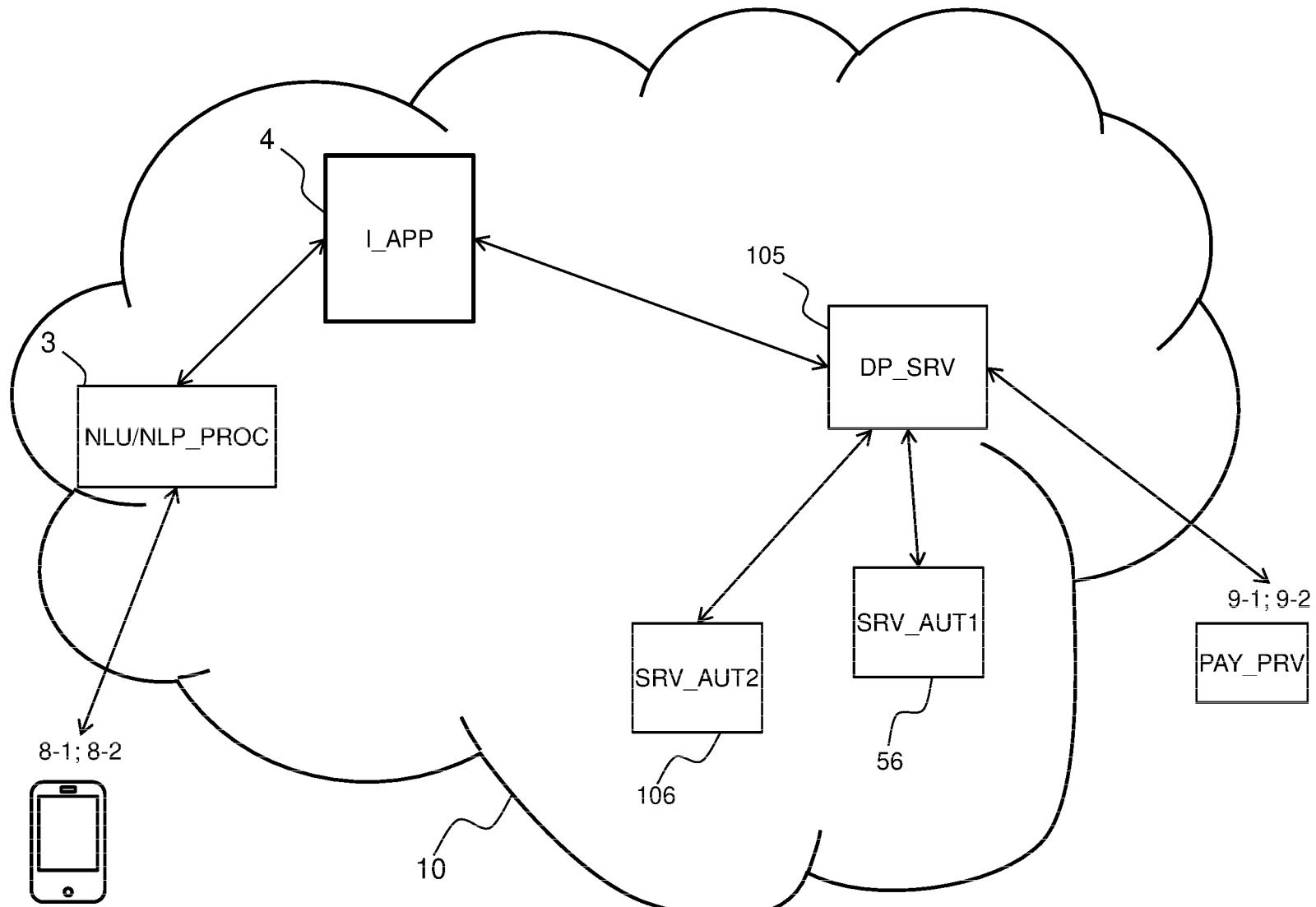


Fig. 2

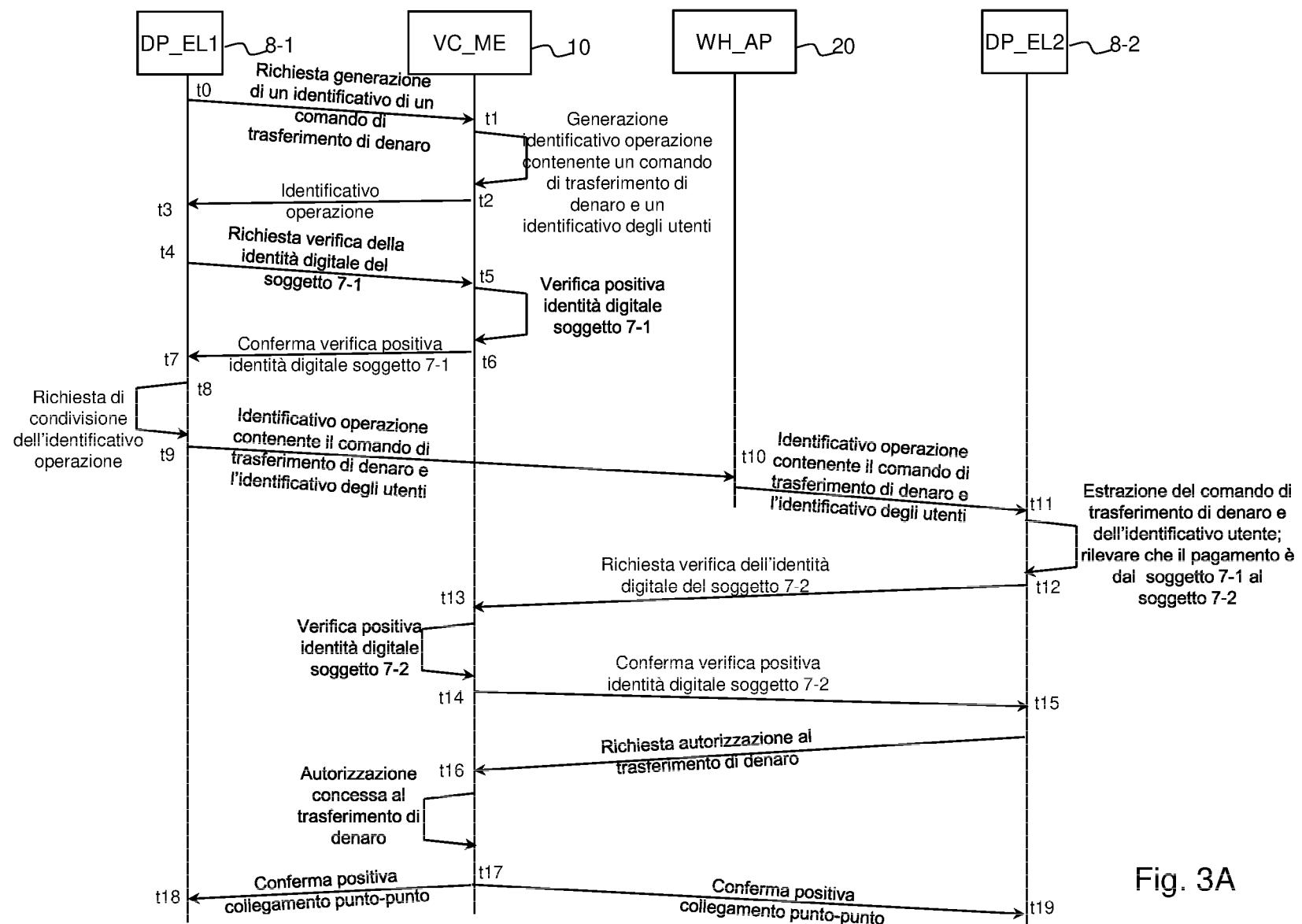


Fig. 3A

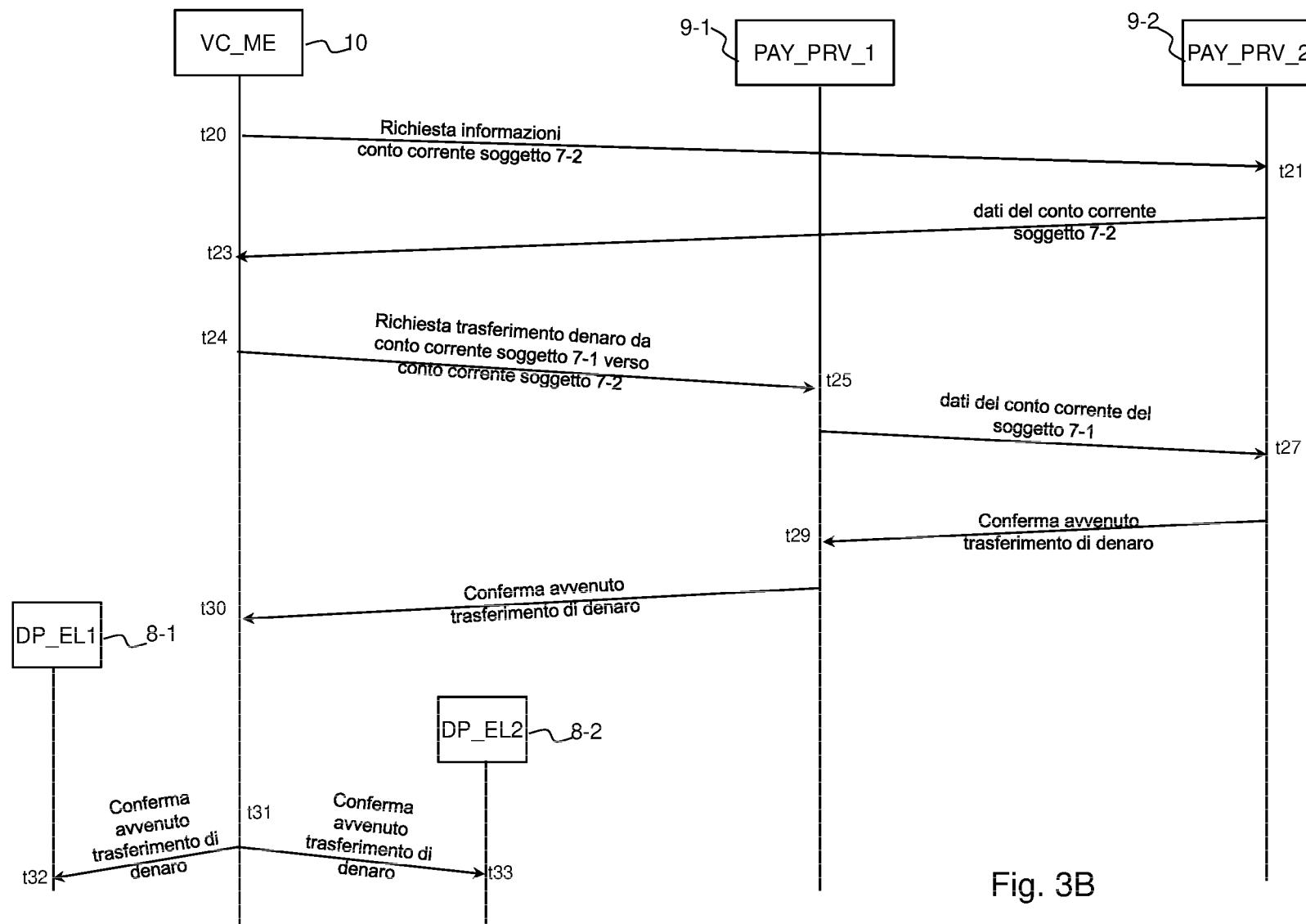


Fig. 3B

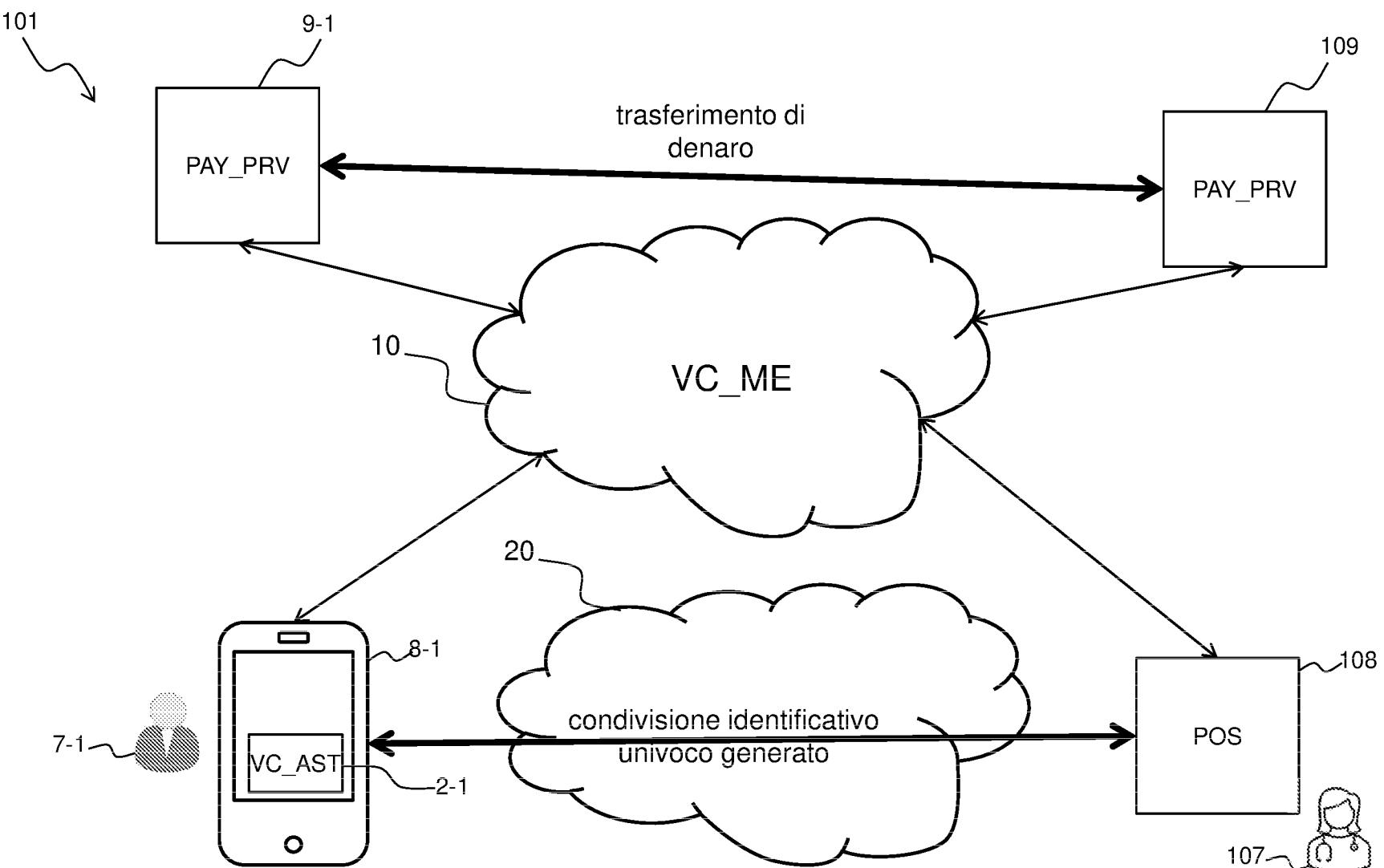


Fig. 4

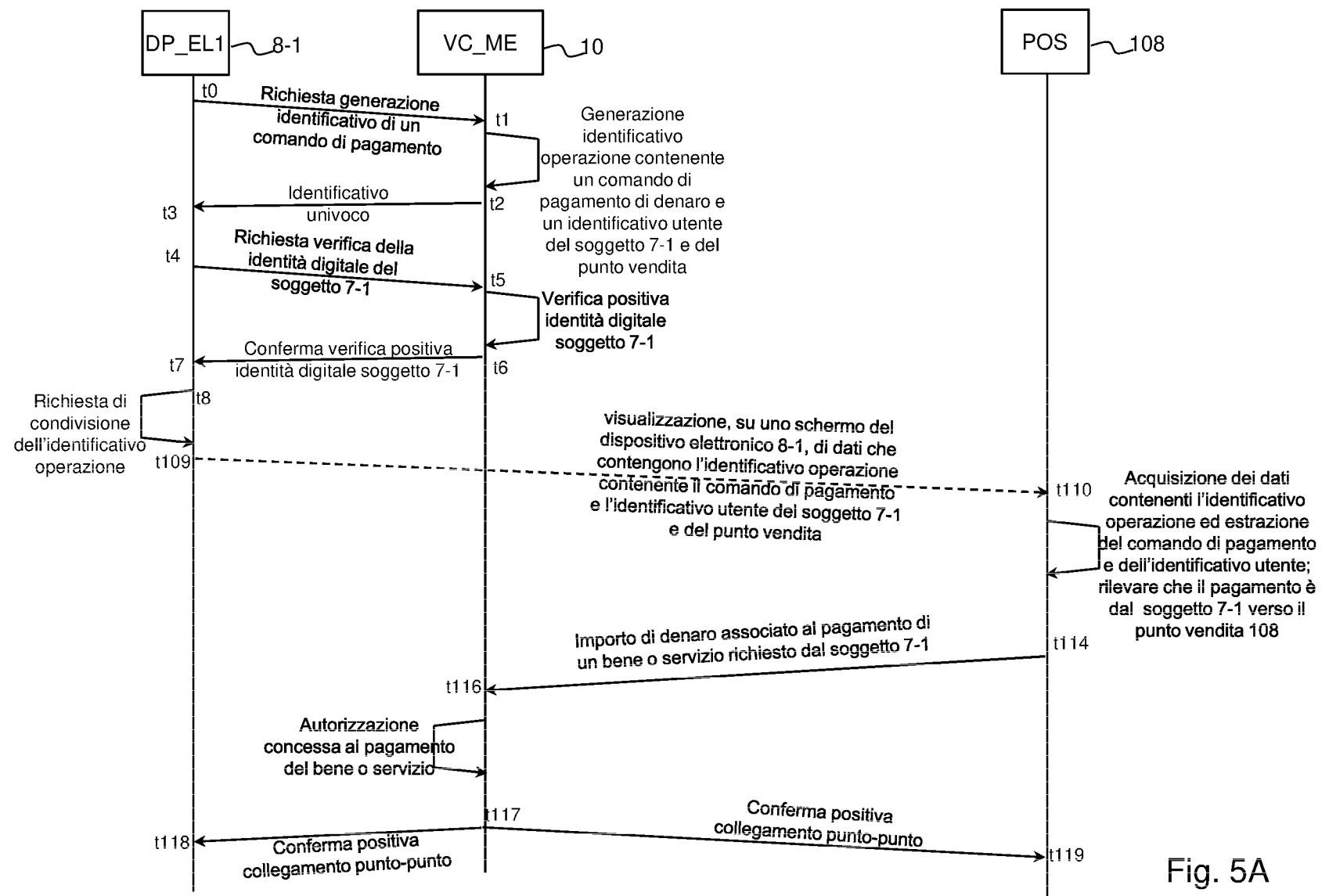


Fig. 5A

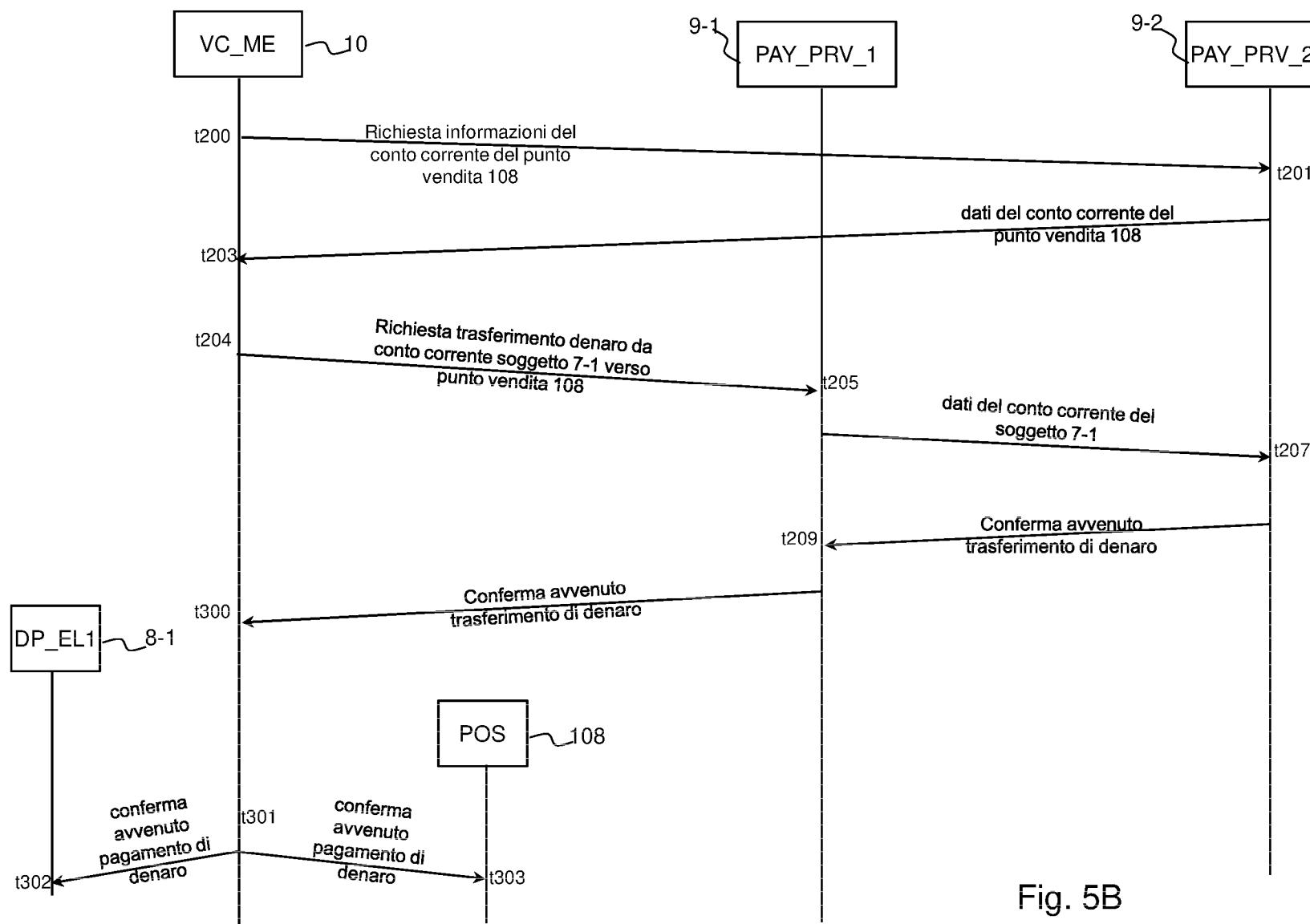


Fig. 5B