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

DOMANDA NUMERO	**102006901439281**
Data Deposito	**04/08/2006**
Data Pubblicazione	**04/02/2008**

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
H	04	M		

Titolo

METODO PER LA REGISTRAZIONE NON RIPUDIABILE DI UNA TRASMISSIONE DIGITALE DI INFORMAZIONI E PER L'IDENTIFICAZIONE DEI PARTECIPANTI ALLA COMUNICAZIONE.

RM 2006 A 000426

Descrizione dell'invenzione avente per titolo:

" METODO PER LA REGISTRAZIONE NON RIPUDIABILE DI UNA TRASMISSIONE DIGITALE DI INFORMAZIONI E PER L'IDENTIFICAZIONE DEI PARTECIPANTI ALLA COMUNICAZIONE "

a nome della ditta KHAMSA ITALIA S.r.l.

a Milano

Inventori: MORO Federico; BOCCACCIA Lorenzo;

PIETROSANTI Fabio

DESCRIZIONE

SETTORE IN CUI SI ESPLICA IL TROVATO

L'invenzione fa riferimento in generale al settore della protezione dell'integrità della comunicazione così come pure al settore delle certificazioni e della crittografia applicati nelle reti di telecomunicazioni al fine di evitare intrusioni illegali nel corso della trasmissione. Più in particolare essa tratta di un metodo per l'identificazione delle credenziali dei partecipanti alla comunicazione ai fini della registrazione non ripudiabile della trasmissione digitale di informazioni.

STATO DELL'ARTE

Attualmente sono presenti sul mercato apparecchi e metodi per effettuare comunicazioni sicure tra due o più individui, ma nessuno di essi è stato sviluppato e pensato per offrire agli utilizzatori la massima sicurezza e semplicità di utilizzo. Inoltre

tutte queste tecniche basano l'identificazione della controparte su metodi insicuri per la natura stessa degli strumenti utilizzati: sebbene vengano utilizzate metodologie crittografiche sicure mutuate, ad esempio, dai sistemi di posta elettronica, la natura stessa degli apparati rende facile la sottrazione fisica della proprietà con tutte le chiavi annesse.

Oggetto della presente invenzione è un metodo e un dispositivo di comunicazione in tal modo programmato per raggiungere lo scopo prefissato di comunicazione e identificazione sicura.

E' ancora scopo della presente invenzione quello di fornire un metodo per l'identificazione delle credenziali dei partecipanti alla comunicazione ai fini anche della registrazione non ripudiabile della trasmissione digitale di informazioni, che impieghi mezzi e tecnologie note nell'ambito degli apparati e dei protocolli delle reti di telecomunicazioni al fine di operare con tecniche di colloquio affidabili e di immediata implementabilità.

Questi ed altri scopi che saranno chiari nel corso della descrizione sono ottenuti mediante un metodo per la registrazione non ripudiabile di una trasmissione digitale di informazioni e per l'identificazione dei partecipanti alla comunicazione secondo il principio enunciato nelle rivendicazioni allegate.

Grazie all'utilizzo di speciali protocolli e algoritmi crittografici, questo dispositivo e metodo permette di instaurare un canale sicuro sul quale comunicare e scambiarsi informazioni riservate, senza che nessuno possa intercettare il contenuto di tali

comunicazioni. Tali protocolli di comunicazione esistono allo stato dell'arte ma da soli non risolvono il problema dell'identificazione delle controparti. In aggiunta alla sicurezza crittografica della comunicazione, particolare attenzione è posta quindi sulla sicurezza dell'identificazione dei partecipanti alla comunicazione, fornendo meccanismi di identificazione biometrica di facile impiego e sistemi di memorizzazione non ripudiabile della conversazione in grado da fornire un adeguato complemento alla verifica dell'identità.

Allo stato dell'arte è possibile dunque stabilire una comunicazione sicura e non intercettabile nel caso tutti i partecipanti alla comunicazione dispongano di tutte le chiavi pubbliche degli altri, se e solo se queste chiavi pubbliche sono ottenute in modo sicuro. Questo pone il problema di fornire ai partecipanti la propria chiave in modo sicuro su un canale non sicuro, poiché prima dello scambio della chiave non si può essere certi ne che le controparti siano effettivamente i possessori dei certificati, ne che i certificati siano effettivamente quelli inviati dalle controparti, proprio in quanto il canale non è sicuro.

DESCRIZIONE

Secondo il trovato all'instaurazione della comunicazione viene creato un canale sicuro tramite un apposito protocollo che garantisca un associazione tra le chiavi pubbliche e le identità dei partecipanti.

Le chiavi pubbliche sono dunque distinte in due gruppi, sicure e

non sicure. Tutte le chiavi non note all'utente sono considerate insicure, e tutte le chiavi che vengono correttamente identificate e accettate dall'utente sono considerate sicure.

Se le chiavi pubbliche ricevute dalla controparte differiscono da quelle memorizzate in precedenti conversazioni con la controparte o non sono presenti nella memoria locale degli utenti sono considerate insicure e si procede alla mutua verifica delle identità.

Per le chiavi sicure si procede alla verifica dell'identità solo nel caso in cui l'utente lo richieda espressamente (nel caso la chiave ritorna a essere considerata insicura).

Per l'identificazione dell'utente e la verifica delle identità si attua il seguente protocollo.

Tramite una funzione matematica non invertibile (pura o procedurale) viene creato un identificativo della chiave crittografica pubblica del mittente, questo identificativo viene reso interpretabile da una persona e visualizzato al mittente in modo da permettere la realizzazione di una versione biometrica del medesimo. La versione biometria dell'identificativo viene inviata al destinatario. Questa versione può essere firmata con la chiave privata del mittente per una maggiore sicurezza.

Tale identificativo numerico nella sua versione biometrica viene interpretato dal destinatario e paragonato con l'identificativo calcolato sulla base del certificato pubblico ricevuto durante l'instaurazione del canale sicuro di comunicazione o della chiave con la quale è stato firmato. Se gli identificativi corrispondono, il

mittente è identificato e si ripete lo scambio di identificativi a ruoli invertiti.

In caso di verifica positiva di entrambe le chiavi le medesime vengono memorizzate e associate univocamente alla controparte della comunicazione, ottenendo un riscontro non ripudiabile dei certificati scambiati.

Se invece le chiavi pubbliche scambiate inizialmente corrispondono a quelle memorizzate, la comunicazione prosegue senza bisogno dei precedenti passaggi di autenticazione.

Una volta che le chiavi pubbliche sono autenticate possono venire utilizzate per firmare e/o cifrare la comunicazione tra le parti, ottenendo così un canale sicuro e non ripudiabile.

La registrazione avviene secondo il meccanismo descritto di seguito. Ciascun terminale può procedere indipendentemente dagli altri alla conservazione del flusso trasmesso e/o ricevuto, o in versione con flusso ricevuto e trasmesso conservati separatamente o nella loro versione miscelata.

I dispositivi che stanno registrando si accordano su un intrevallo temporale periodico di segmentazione del flusso registrato. Tali flussi vengono firmati digitalmente da ciuscun dispositivo e la firma scambiata tra i dispositivi coinvolti con detta frequenza.

Al solo fine di meglio chiarire l'invenzione e senza con ciò volerne limitare l'ambito ed i settori in cui essa può trovare applicazione, di seguito si descriveranno alcune realizzazioni specifiche.

DESCRIZIONE DI UN ESEMPIO DI REALIZZAZIONE PREFERITA

Entrando nel dettaglio procedurale viene fornito agli utenti un applicativo in grado di svolgere operazioni crittografiche che utilizzino chiavi asimmetriche per firmare o crittografare dati digitali e di utilizzare chiavi simmetriche per cifrare dati o flussi digitali. Tale applicativo prevede le fasi procedurali che seguono.

Durante la fase di installazione o a richiesta dell'utente esso genera un certificato digitale contenente i dati dell'utente e una coppia di chiavi asimmetriche.

Alternativamente il programma può essere distribuito con allegato un certificato già pronto all'utilizzo.

Dopo la generazione di ogni chiave pubblica o privata viene generato un identificativo univoco, detto "fingerprint", risultante da una funzione matematica non invertibile nota e presente in diverse varianti allo stato dell'arte, detta "funzione di hashing". A partire da ogni identificativo univoco viene generato un identificativo biometrico. Questo viene realizzato traducendo l'identificativo precedentemente ottenuto in una sequenza alfanumerica che ne rappresenti univocamente il valore, quindi visualizzando all'utente tale valore e infine memorizzando una rappresentazione biometrica dell'utente da associare a tale valore, sia essa una registrazione dell'utente che recita la sequenza alfanumèrica generata piuttosto che una foto dell'utente recante un cartello con iscritti i codici alfanumerici della sequenza stessa.

Questo identificativo può essere ulteriormente firmato con la chiave privata dell'utente per offrire un ulteriore meccanismo di sicurezza.

All'instaurazione della comunicazione si genera una chiave simmetrica valida solo per quella sessione di comunicazione da utilizzare per cifrare tutta la seguente comunicazione, in modo da proteggere i contenuti. Questa chiave può essere generata in modi diversi, tramite algoritmi di generazione di chiave in grado di proteggere la chiave da ascoltatori estranei alla comunicazioni, esistenti allo stato dell'arte, oppure generato dal chiamante utilizzando la chiave pubblica del destinatario (se disponibile) per inviarlo cifrato al destinatario stesso, oppure generata a partire da un segreto condiviso. La negoziazione della metodologia di generazione di questa prima chiave da utilizzare è a discrezione delle implentazioni. Se non viene utilizzata la metodologia di generazione e invio tramite chiave pubblica la chiave viene utilizzata solo temporaneamente per proteggere lo scambio di credenziali, non essendo le chiavi generate con altre metodologie in grado di garantire la sicurezza dei contenuti, e sostituita non appena i certificati delle controparti vengono identificati e considerati sicuri con una nuova chiave.

Sul canale vengono distribuite le chiavi pubbliche dei partecipanti da utilizzare, nel caso vengano verificate e considerate sicure, per generare la chiave di sessione definitiva da utilizzare durante la comunicazione. Queste chiavi possono opzionalmente includere

come allegato l'identificativo in formato biometrico della chiave stessa, per automatizzare il processo. Nella fase di instaurazione della connessione tutti i partecipanti hanno opzionalmente l'opportunità di rigenerare il proprio identificativo in formato biometrico (essendo l'identificativo alfanumerico stesso funzione della chiave utilizzata e quindi sempre identico per una data chiave)

La verifica della chiave pubblica consiste nei seguenti passi, che possono essere compiuti in contemporanea dai partecipanti della comunicazione, di cui verrà esplicato il processo dal punto di vista di un solo utente:

1) l'utente chiede a una controparte l'identificativo biometrico univoco della chiave pubblica, se non già distribuito allegato alla chiave pubblica.

2) Appena ricevuto, l'utente calcola l'identificativo della chiave pubblica della controparte a partire dalla chiave stessa, usando lo stesso algoritmo che la controparte ha utilizzato per la generazione dell'identificativo alfanumerico.

3) L'utente verifica che l'identificativo effettivamente corrisponda con l'identificativo biometrico.

Se la verifica ha successo, allora il certificato viene memorizzato come valido; se la verifica fallisce il certificato viene scartato e la comunicazione interrotta; opzionalmente in caso di incertezza si può utilizzare un meccanismo di ulteriore verifica interattiva che consiste nel generare in maniera casuale un identificativo

temporaneo, spedirlo alla controparte e aspettarne un corrispettivo biometrico.

Nel caso di una prima comunicazione tra le parti, successivamente alla verifica, le chiavi vengono memorizzate e associate univocamente alla controparte della comunicazione, ottenendo così un riscontro non ripudiabile delle chiavi scambiate, necessarie per le successive operazioni di verifica della comunicazione.

Nelle successive comunicazioni invece, se le chiavi pubbliche scambiate corrispondono a quelle memorizzate, la comunicazione prosegue senza bisogno dei vari passaggi di autenticazione e la generazione della chiave di sessione può essere effettuata direttamente dal chiamante utilizzando la metodologia dettagliata in precedenza, consistente nel cifrare la chiave di sessione con le chiavi pubbliche delle controparti e distribuirla alle medesime.

Per maggiore sicurezza, prima dell'instaurazione della connessione il chiamante può richiedere di ripetere lo scambio di credenziali biometriche, indipendentemente dal fatto di aver precedentemente memorizzato la chiave della controparte.

Come ulteriore misura di sicurezza, lo scambio di identificativi biometrici può avvenire anche in maniera interattiva durante o all'inizio della comunicazione. In questo caso si può richiedere di identificare in maniera biometrica la chiave di sessione corrente, come garanzia che la chiave sia quella effettivamente in utilizzo dalle controparti.

In questo modo si ottiene il risultato di associare in maniera univoca le chiavi utilizzate per rendere sicura la comunicazione ai destinatari stessi della comunicazione.

Durante la comunicazione tra le parti tutti i dispositivi coinvolti registrano il contenuto del flusso telematico. Questo può essere fatto in diversi modi: ciascun apparato può o memorizzare il flusso delle controparti, o memorizzare tutti i flussi uniti mantenendoli separati.

Alla fine della comunicazione o a intervalli determinati ciascun dispositivo firma la parte di comunicazione generata e invia l'hash ottenuto alle controparti, utilizzando eventualmente un apposito algoritmo di scambio per le firme digitali che garantisca che i dispositivi ottengano le firme contemporaneamente.

Tale processo utilizza le chiavi private dei partecipanti per generare le firme utilizzando protocolli esistenti allo stato dell'arte. La memorizzazione delle firme da parte di tutti i partecipanti alla comunicazione garantisce che chiunque possa dimostrare la presenza della controparte alla discussione utilizzando la firma, la chiave pubblica fornita e l'identificativo biometrico associato.

In tale modo si è ottenuto il risultato di ottenere una comunicazione non ripudiabile.

Di seguito si descriveranno alcune realizzazioni specifiche con riferimento alle Figure allegate al solo scopo esemplificativo e senza con ciò volerne limitare l'ambito ed i settori in cui essa può

Avv. C. FIAMMENGHI N° 29
Dott. D. DOMENIGHETTI - FIAMMENGHI N° 27
Via Quattro Fontane, 31 - ROMA

trovare applicazione, tali figure fanno rispettivamente riferimento a:

Fig. 1 è un diagramma temporale delle fasi esecutive di una telefonata verso destinatario di cui non si conosce il certificato

Fig. 2 è un diagramma temporale delle fasi esecutive di una telefonata verso destinatario di cui non si conosce il certificato con rifiuto dell'identificativo biometrico.

Fig. 3 è un diagramma temporale delle fasi esecutive di una telefonata verso destinatario di cui si conosce il certificato.

Fig. 4 è un diagramma temporale delle fasi esecutive di una telefonata verso destinatario di cui si conosce il certificato con richiesta di rivalidazione dell'impronta biometria.

In questi esempi la sequenza di operazioni viene descritta solo per la verifica d'identità da parte del chiamante e si presuppone la presenza di due soli partecipanti alla comunicazione. Il ricevente effettua prima della creazione del canale di comunicazione vero e proprio e contemporaneamente al chiamante una verifica analoga a quella del chiamante, che avviene subordinata all'accettazione dell'identificativo da parte del chiamante, in maniera indipendente rispetto alla procedura utilizzata fra quelle proposte dal chiamante: il ricevente effettuerà una procedura di verifica adeguata alle condizioni del proprio telefono e allo stato dei propri certificati memorizzati.

Figura 1 : Telefonata verso destinatario di cui non si conosce il certificato:

1. Il chiamante "a" attiva il programma e sceglie il destinatario "e", da rubrica o componendo il numero.

2. Il telefono "b" contatta il telefono "d" e stabiliscono una chiave di sessione. In questo caso data l'assenza di certificati viene utilizzato un protocollo per la generazione di chiavi di sessione, esistente allo stato dell'arte. In alternativa la chiave di sessione può essere ottenuta a partire da un segreto condiviso dalle due parti della telefonata, o tramite protocolli alternativi equivalenti.

3. Il telefono "b" contatta il telefono "d" del destinatario e ottiene il certificato.

4. Il telefono "b" controlla tramite servizio "c" (che può essere la memoria del telefono piuttosto che un servizio di verifica certificati esterno) se il certificato è presente nella rubrica con il dato identificativo.

5. In questo caso il servizio "c" comunica al telefono "b" che il certificato non è conosciuto.

6. Il telefono "b" contatta il telefono "d" e richiede al telefono di fornire un identificativo biometrico.

7. Il telefono "d" richiede all'utente "e" una versione biometrica dell'identificativo numerico del certificato.

8. L'utente "e" fornisce al telefono l'identificativo biometrico.

9. Il telefono "e" fornisce al telefono "b" l'identificativo biometrico del certificato.

10. Il telefono "b" mostra all'utente "a" l'identificativo biometrico del certificato.

11. L'utente "a" in questo caso decide di accettare l'identificativo biometrico ricevuto.

12. Il telefono "b" spedisce il certificato al servizio di deposito "c".

13. Il deposito "c " conferma la ricezione del certificato.

14. Il telefono "b" comunica al telefono "d" che l'autenticazione è stata accettata.

X. La procedura di riconoscimento viene effettuata a parti invertite.

15. I telefoni avvisano i rispettivi utenti che la comunicazione è sicura e può incominciare. Poiché in questo caso la chiave di sessione iniziale è stata generata in maniera insicura, il chiamante rigenera una nuova chiave di sessione e la invia crittografata con la chiave pubblica del chiamato alla controparte.

Figura 2: verso destinatario di cui non si conosce il certificato, con rifiuto dell'impronta biometrica:

1. Il chiamante “a” attiva il programma e sceglie il destinatario “e”da rubrica o componendo il numero.

2. Il telefono “b” contatta il telefono "d" e stabiliscono una chiave di sessione. In questo caso data l'assenza di certificati viene utilizzato un protocollo per la generazione di chiavi di sessione, esistente allo stato dell'arte. In alternativa la chiave di sessione può essere ottenuta a partire da un segreto condiviso dalle due parti della telefonata, o tramite protocolli alternativi equivalenti.

3. Il telefono ”b” contatta il telefono “d” del destinatario e ottiene

il certificato.

4. Il telefono “b” controlla tramite servizio “c” (che può essere la memoria del telefono piuttosto che un servizio di verifica certificati esterno) se il certificato è presente nella rubrica con il dato identificativo.

5. In questo caso il servizio “c” comunica al telefono “b” che il certificato non è conosciuto.

6. Il telefono “b” contatta il telefono "d" e richiede al telefono un identificativo biometrico.

7. Il telefono “d” richiede all’utente “e” una versione biometria dell’ identificativo numerico del certificato.

8. L’utente “e” fornisce al telefono l’identificativo biometrico.

9. Il telefono “d” fornisce al telefono “b” l’identificativo biometrico del certificato.

10.Il telefono “b” mostra all’utente “a” l’identificativo biometrico del certificato.

11. L'utente "a" in questo caso decide di rifiutare l’identificativo biometrico ricevuto.

12. Il telefono “b” chiude la connessione immediatamente.

Fig 3: Telefonata verso destinatario di cui si conosce il certificato:

1. Il chiamante "a" attiva il programma e sceglie il destinatario “e”, da rubrica o componendo il numero.

2. Poiché il numero era già stato verificato, il telefono "d" reperisce tramite servizio “c” (che può essere la memoria del telefono piuttosto che un servizio di verifica certificati esterno) il

certificato corrispondente al destinatario.

3. Il servizio comunica al telefono il certificato.

4. Il telefono "b" chiede all'utente "a" se accettare il certificato

5. L'utente "a" riconosce il certificato.

6. Il telefono "b" comunica al telefono "d" l'accettazione del certificato e invia una chiave di sessione randomica crittografata con la chiave pubblica della controparte. (Se la controparte avesse cambiato il certificato, non potendo accettare la chiave di sessione chiederebbe al chiamante una chiave di sessione generata con un altro dei meccanismi disponibili e fornirebbe al chiamante il nuovo certificato, ripetendo la procedura di identificazione biometrica).

X. La procedura di riconoscimento viene effettuata a parti invertite.

7. I telefoni avvisano i rispettivi utenti che la comunicazione è sicura e può incominciare.

Fig 4; Telefonata verso destinatario di cui si conosce il certificato, con richiesta di rivalidazione dell'impronta biometrica:

1. Il chiamante "a" attiva il programma e sceglie il destinatario "e", da rubrica o componendo il numero.

2. Poiché il numero era già stato verificato, il telefono "b" reperisce tramite servizio "c" (che può essere la memoria del telefono piuttosto che un servizio di verifica certificati esterno) il certificato corrispondente al destinatario.

3. Il servizio comunica al telefono il certificato.

4. Il telefono "b" chiede all'utente "a" se accettare il certificato.

5. L'utente "a" non riconosce il certificato.

6. Il telefono "b" contatta il telefono "d" e stabiliscono una chiave di sessione. In questo caso poiché non viene riconosciuto il certificato viene utilizzato un protocollo per la generazione di chiavi di sessione, esistente allo stato dell'arte. In alternativa la chiave di sessione può essere ottenuta a partire da un segreto condiviso dalle due parti della telefonata, o tramite protocolli alternativi equivalenti.

7. Il telefono "b" contatta il telefono "d" e richiede un nuovo identificativo biometrico.

8. Il telefono "d" richiede all'utente "e" una versione biometrica dell'identificativo numerico del certificato.

9. L'utente "e" fornisce al telefono l'identificativo biometrico.

10. Il telefono "e" fornisce al telefono "b" l'identificativo biometrico del certificato.

11. Il telefono "b" mostra all'utente "a" l'identificativo biometrico del certificato.

12. L'utente "a" in questo caso decide di accettare l'identificativo biometrico ricevuto.

13. Il telefono "b" spedisce il certificato al servizio di deposito "c".

14. Il servizio "c" conferma la ricezione del certificato.

15. Il telefono "b" comunica al telefono "d" che l'autenticazione è stata accettata.

X La procedura di riconoscimento viene effettuata a parti invertite.

16. I telefoni avvisano i rispettivi utenti che la comunicazione è sicura e può incominciare. Poiché in questo caso la chiave di sessione iniziale è stata generata in maniera insicura, il chiamante rigenera una nuova chiave di sessione e la invia crittografata con la chiave pubblica del chiamato alla controparte.

RIVENDICAZIONI

1. Metodo per l'identificazione dei partecipanti alla comunicazione caratterizzato dal fatto di impiegare protocolli crittografici per il riscontro della integrità e della correttezza dello scambio di informazioni su canale digitale, basati su verifica biometrica bidirezionale e l'acquisizione delle credenziali da parte di ciascun partecipante alla comunicazione, garantendo che la presenza della controparte possa essere autenticata per mezzo della firma, della chiave pubblica fornita e dell'identificativo biometrico associato.

2. Metodo per la registrazione non ripudiabile di una trasmissione digitale di informazioni in base alla rivendicazione 1, caratterizzato dal fatto di impiegare protocolli crittografici per il riscontro della integrità e della correttezza dello scambio di informazioni su canale digitale, basati su verifica bidirezionale e sullo scambio e la verifica preliminare di chiavi crittografiche asimmetriche tramite le quali far proseguire la conversazioni con protocolli di cifratura standard, l'acquisizione delle credenziali da parte di ciascun partecipante alla comunicazione, garantendo che la presenza della controparte possa essere autenticata per mezzo della firma, della chiave pubblica fornita e dell'identificativo associato.

3. Metodo per la registrazione non ripudiabile di una trasmissione digitale di informazioni e per l'identificazione dei partecipanti alla comunicazione secondo ciascuna delle rivendicazioni precedenti caratterizzato dal fatto che

I - durante la fase di inizializzazione vengano generati o allegati un certificato digitale contenente i dati dell'utente e una coppia di chiavi asimmetriche,

II - dopo la generazione di ogni chiave pubblica o privata sia fornito un identificativo univoco, risultante da una funzione matematica nota, di hashing, non invertibile, ricavando da ogni identificativo univoco un identificativo biometrico mediante:

a - traduzione dell'identificativo precedentemente ottenuto, in una sequenza alfanumerica che ne rappresenti univocamente il valore,

b - visualizzazione all'utente di tale valore, e infine

c - memorizzazione di una rappresentazione biometrica dell'utente da associare a detto valore;

III- all'instaurazione della comunicazione sia generata una chiave simmetrica valida solo per una sessione di comunicazione da utilizzare per cifrare tutta la comunicazione seguente, in modo da proteggerne i contenuti;

IV- sul canale vengano distribuite le chiavi pubbliche dei partecipanti da impiegare, se verificate, per generare la chiave di sessione definitiva da utilizzare durante la comunicazione, potendo queste chiavi includere opzionalmente come allegato l'identificativo in formato biometrico della chiave stessa,

V- sia eseguita la verifica della chiave pubblica attraverso le seguenti fasi:

a) l'utente chiede a una controparte l'identificativo univoco della chiave pubblica, se non già distribuito allegato alla chiave

Avv. C. FIAMMENGHI N° 29
Dott. D. DOMENICHETTI - FIAMMENGHI N° 27
Via Quattro Fontane, 31 - ROMA

pubblica,

b) il chiamante calcola l'identificativo della chiave pubblica del ricevente a partire dalla chiave stessa, usando lo stesso algoritmo che la controparte ha utilizzato per la generazione dell'identificativo alfanumerico,

c) l'utente verifica che l'identificativo effettivamente corrisponda con l'identificativo biometrico,

c-1) se la verifica ha successo, allora il certificato viene memorizzato come valido;

c-2) se la verifica fallisce il certificato viene scartato e la comunicazione interrotta;

c-3) opzionalmente in caso di incertezza viene utilizzato un meccanismo di ulteriore verifica interattiva che consiste nel generare in maniera casuale un identificativo temporaneo, spedirlo alla controparte e aspettarne un corrispettivo biometrico,

VI-a nel caso di una prima comunicazione tra le parti, successivamente alla verifica, le chiavi vengano memorizzate e associate univocamente alla controparte della comunicazione, ottenendo così un riscontro non ripudiabile delle chiavi, scambiate, necessarie per le successive operazioni di verifica della comunicazione,

VI-b nelle successive comunicazioni in condizioni di corrispondenza tra le chiavi pubbliche scambiate e quelle memorizzate, la comunicazione prosegua senza bisogno dei vari passaggi di autenticazione e la generazione della chiave di

sessione sia effettuata direttamente dal chiamante, cifrando la chiave di sessione con le chiavi pubbliche delle controparti e distribuendola alle medesime,

VII- durante la comunicazione tra le parti tutti i dispositivi coinvolti registrino il contenuto del flusso telematico,

VIII- alla fine della comunicazione o a intervalli determinati ciascun dispositivo firmi la parte di comunicazione generata e la invii alle controparti, utilizzando eventualmente un algoritmo di scambio, per le firme digitali, che garantisca che i dispositivi ottengano le firme contemporaneamente.

4. Metodo per la registrazione non ripudiabile di una trasmissione digitale di informazioni e per l'identificazione dei partecipanti alla comunicazione secondo ciascuna delle rivendicazioni precedenti caratterizzato dal fatto che dopo la generazione di ciascuna chiave pubblica o privata fornendo l'identificativo univoco, ed il corrispondente identificativo biometrico, quest'ultimo venga ancora ulteriormente firmato con la chiave privata dell'utente per offrire un ulteriore meccanismo di sicurezza.

5. Metodo per la registrazione non ripudiabile di una trasmissione digitale di informazioni e per l'identificazione dei partecipanti alla comunicazione secondo ciascuna delle rivendicazioni precedenti caratterizzato dal fatto che nella fase di instaurazione della comunicazione la chiave simmetrica da utilizzare per cifrare la comunicazione seguente, sia generata tramite i soliti algoritmi di generazione di chiave in grado di proteggere la chiave da ascolta-

Avv. C. FIAMMENGHI N° 29
Dott. D. DOMENIGHETTI - FIAMMENGHI N° 27
Via Quattro Fontane, 31 - ROMA

tori estranei alla comunicazioni.

6. Metodo per la registrazione non ripudiabile di una trasmissione digitale di informazioni e per l'identificazione dei partecipanti alla comunicazione secondo ciascuna delle rivendicazioni precedenti caratterizzato dal fatto che nella fase di instaurazione della comunicazione la chiave simmetrica da utilizzare per cifrare la comunicazione che segue, sia generata dal chiamante utilizzando la chiave pubblica del destinatario con l'invio cifrato al destinatario stesso.

7. Metodo per la registrazione non ripudiabile di una trasmissione digitale di informazioni e per l'identificazione dei partecipanti alla comunicazione secondo ciascuna delle rivendicazioni precedenti caratterizzato dal fatto che in seguito alla distribuzione delle chiavi pubbliche dei partecipanti da utilizzare, se verificate, per generare la chiave di sessione definitiva, tutti i partecipanti abbiano, opzionalmente, l'opportunità di rigenerare il proprio identificativo in formato biometrico, essendo l'identificativo alfanumerico funzione della chiave utilizzata e quindi sempre identico per una data chiave.

8. Metodo per la registrazione non ripudiabile di una trasmissione digitale di informazioni e per l'identificazione dei partecipanti alla comunicazione secondo ciascuna delle rivendicazioni precedenti caratterizzato dal fatto che nelle comunicazioni successive alla prima, seppur in condizioni di corrispondenza tra le chiavi pubbliche scambiate e quelle memorizzate, prima dell'instaura-

Avv. C. FIAMMENGHI N° 29
Dott. D. DOMENGHETTI - FIAMMENGHI N° 27
Via Quattro Fontane, 31 - ROMA

zione della connessione il chiamante possa richiedere di ripetere lo scambio di credenziali biometriche, indipendentemente dal fatto di aver precedentemente memorizzato la chiave della controparte.

9. Metodo per la registrazione non ripudiabile di una trasmissione digitale di informazioni e per l'identificazione dei partecipanti alla comunicazione secondo ciascuna delle rivendicazioni precedenti caratterizzato dal fatto che come ulteriore misura di sicurezza, lo scambio di identificativi biometrici avvenga anche in maniera interattiva durante o all'inizio delle comunicazioni successive, richiedendo di identificare in maniera biometrica la chiave di sessione corrente, come garanzia che la chiave sia quella effettivamente in utilizzo dalle controparti.

10. Metodo sicuro, secondo ciascuna delle rivendicazioni precedenti, di generazione di identificativi di chiavi crittografiche interpretabile da persone e/o umanamente intelligibili.

11. Metodo sicuro, secondo ciascuna delle rivendicazioni precedenti, di generazione di identificativi biometrici a partire da identificativi numerici.

12. Metodo secondo ciascuna delle rivendicazioni precedenti, che consenta la verifica del possessore di una chiave crittografica

13. Metodo secondo ciascuna delle rivendicazioni precedenti, che consenta la verifica del possessore di una chiave crittografica mediante un identificativo biometrico.

14. Metodo secondo ciascuna delle rivendicazioni precedenti, che consenta la verifica di una chiave di sessione o chiave simmetrica

che utilizzi identificativi biometrici.

15. Dispositivo per l'implementazione a livello di programma software dei metodi secondo le rivendicazioni 10 e 11.

16. Dispositivo per l'implementazione a livello di programma software dei metodi secondo le rivendicazioni 10 e 11 per l'identificazione sicura delle identità degli attori di una comunicazione.

17. Dispositivo per l'implementazione a livello di programma software dell'utilizzo delle chiavi pubbliche sicure secondo la rivendicazioni 13 per la creazione di un canale di comunicazione sicuro tra gli attori di una comunicazione.

18. Dispositivo per l'implementazione a livello di programma software dei metodi secondo le rivendicazioni 10 e 11, utilizzando i metodi secondo le rivendicazioni 13 e 14 per creare una comunicazione sicura tale da impedire a terze parti di intercettarne il contenuto.

19. Dispositivo per l'implementazione a livello di programma software dei metodi secondo le rivendicazioni 10 e 11, utilizzando i metodi delle rivendicazioni 13 e 14 per creare una comunicazione sicura tale da garantire l'identità del chiamante

20. Dispositivo per l'implementazione a livello di programma software dei metodi secondo le rivendicazioni 10, 11, 12, 13, 14, 15 e 16 che necessita solo di una semplice installazione del programma.

21. Dispositivo per l'implementazione a livello di programma

Avv. C. FIAMMENGHI N° 29
Dott. D. DOMENIGHETTI - FIAMMENGHI N° 27
Via Quattro Fontane, 31 - ROMA

software dei metodi secondo la rivendicazioni 16 che permette di effettuare comunicazioni sicure con una semplice installazione del relativo programma.

22. Metodo crittografico secondo ciascuna delle rivendicazioni precedenti, per firmare le registrazioni.

23. Metodo secondo ciascuna delle rivendicazioni precedenti, per garantire la privacy in una comunicazione.

24. Metodo secondo ciascuna delle rivendicazioni precedenti, per garantire la certezza della identità delle parti coinvolte in una comunicazione.

25. Metodo per la creazione e distribuzione di pacchetti comunicativi digitali secondo ciascuna delle rivendicazioni precedenti, tale da garantire l'identicità del pacchetto su tutti i dispositivi partecipanti alla comunicazione.

26. Metodo per la firma digitale di pacchetti comunicativi digitali generati secondo la rivendicazione 22, tale da garantire la interoperabilità delle operazioni di verifica.

27. Metodo secondo le rivendicazioni 22, 23 e 24 per la firma contemporanea delle comunicazioni che permetta a tutti i partecipanti di avere una versione non ripudiabile della medesima, grazie alle funzioni di firma crittografica delle registrazioni ed alla garanzia di privacy della comunicazione stessa.

Avv. C. FIAMMENGHI N° 29
Dott. D. DOMENIGHETTI - FIAMMENGHI N° 27
Via Quattro Fontane, 31 - ROMA
MIRELLA EREDIA (N° 184)

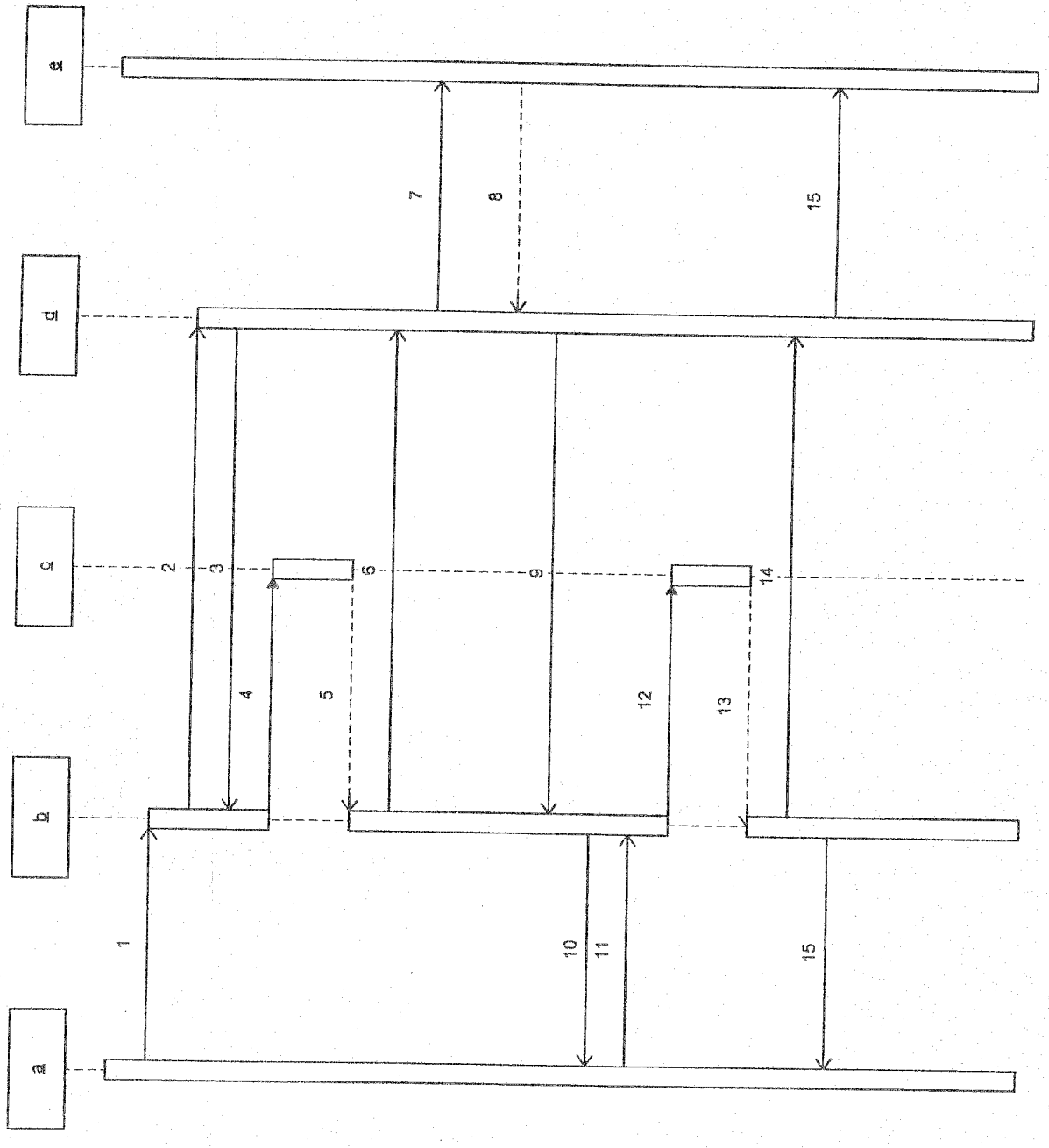

FIG. 1

Avv. C. FIAMMENGHI N° 29
Dott. D. DOMENICHETTI-FIAMMENGHI N° 27
Via Quattro Fontane, 31 - ROMA
MIRELLA EREDIA (N° 184)

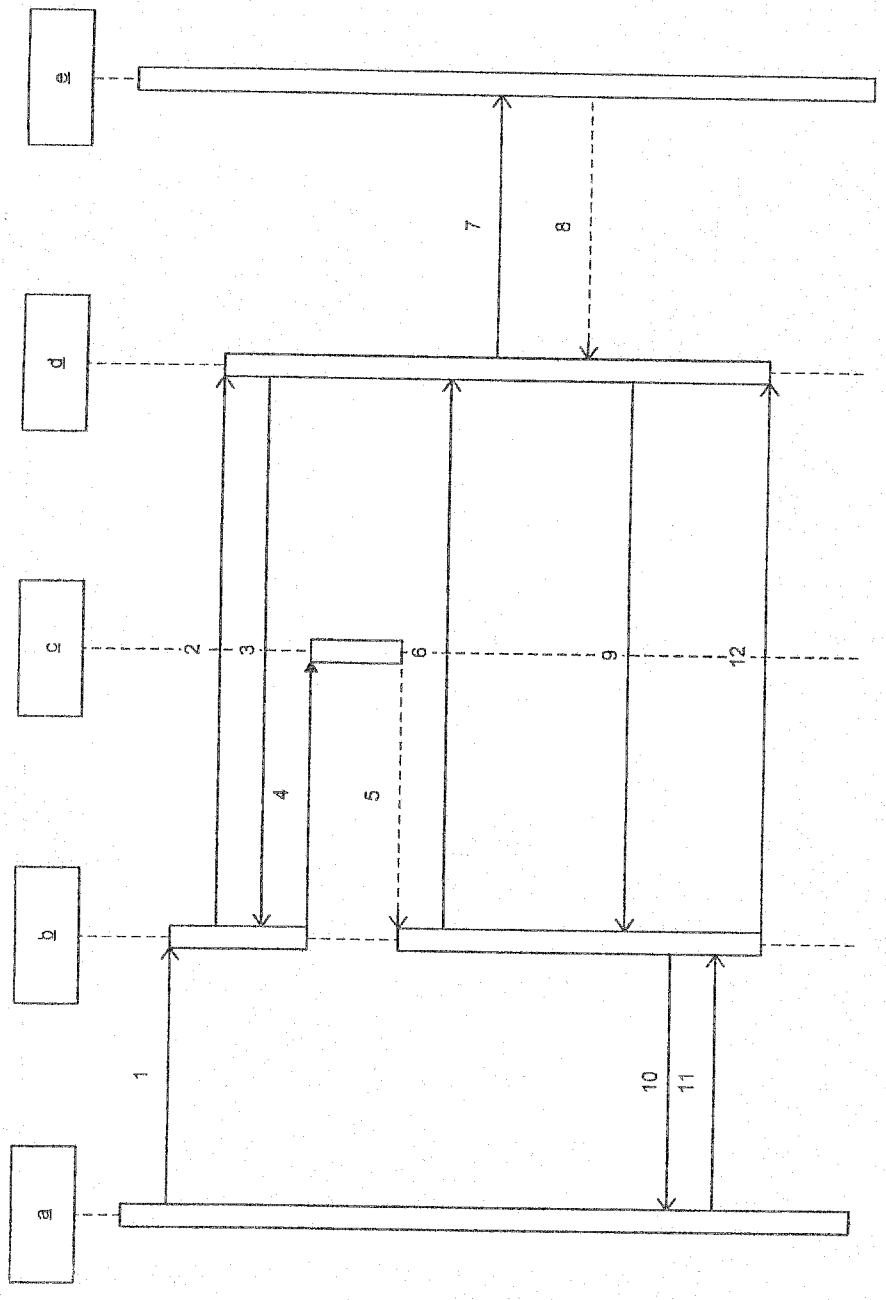

FIG. 2

Avv. C. FIAMMENGHI N° 29
Dott. D. DOMENIGHETTI-FIAMMENGHI N° 27
Via Quattro Fontane, 31 - ROMA

MIRELLA EREDIA (N° 184)
Mirella Eredia

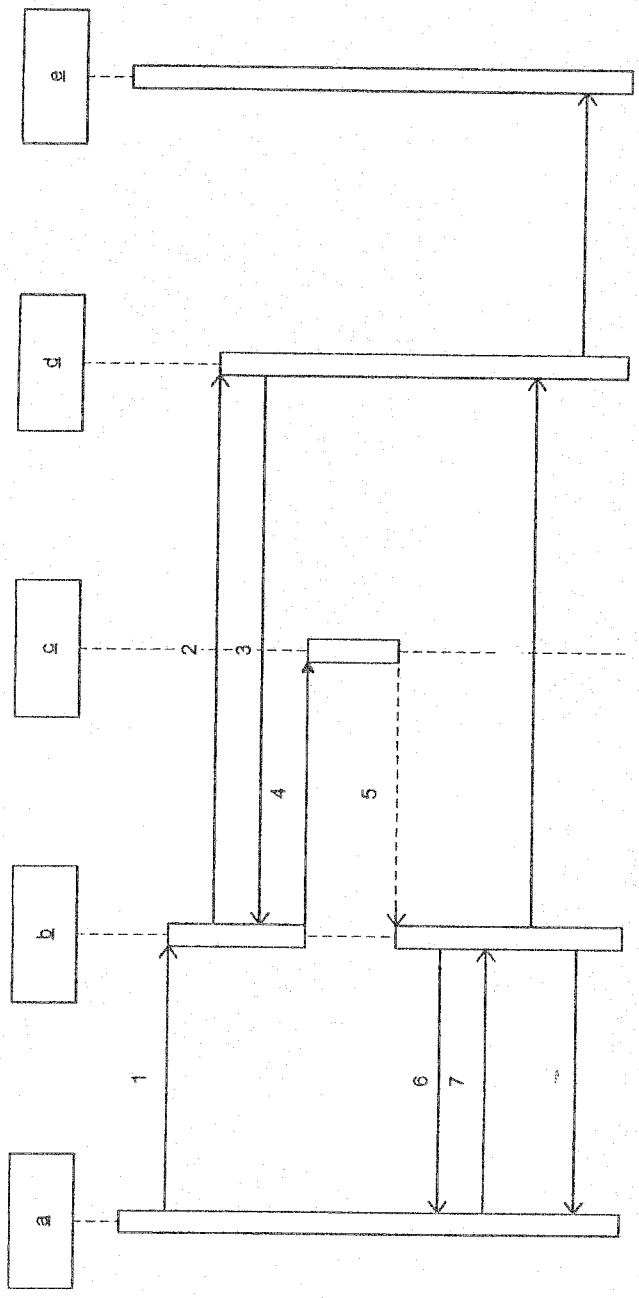

FIG. 3

Avv. C. FIAMMENGHI N° 29
Dott. D. DOMENIGHETTI-FIAMMENGHI N° 27
Via Quattro Fontane, 31 - ROMA

MIRELLA EREDIA (N° 184)

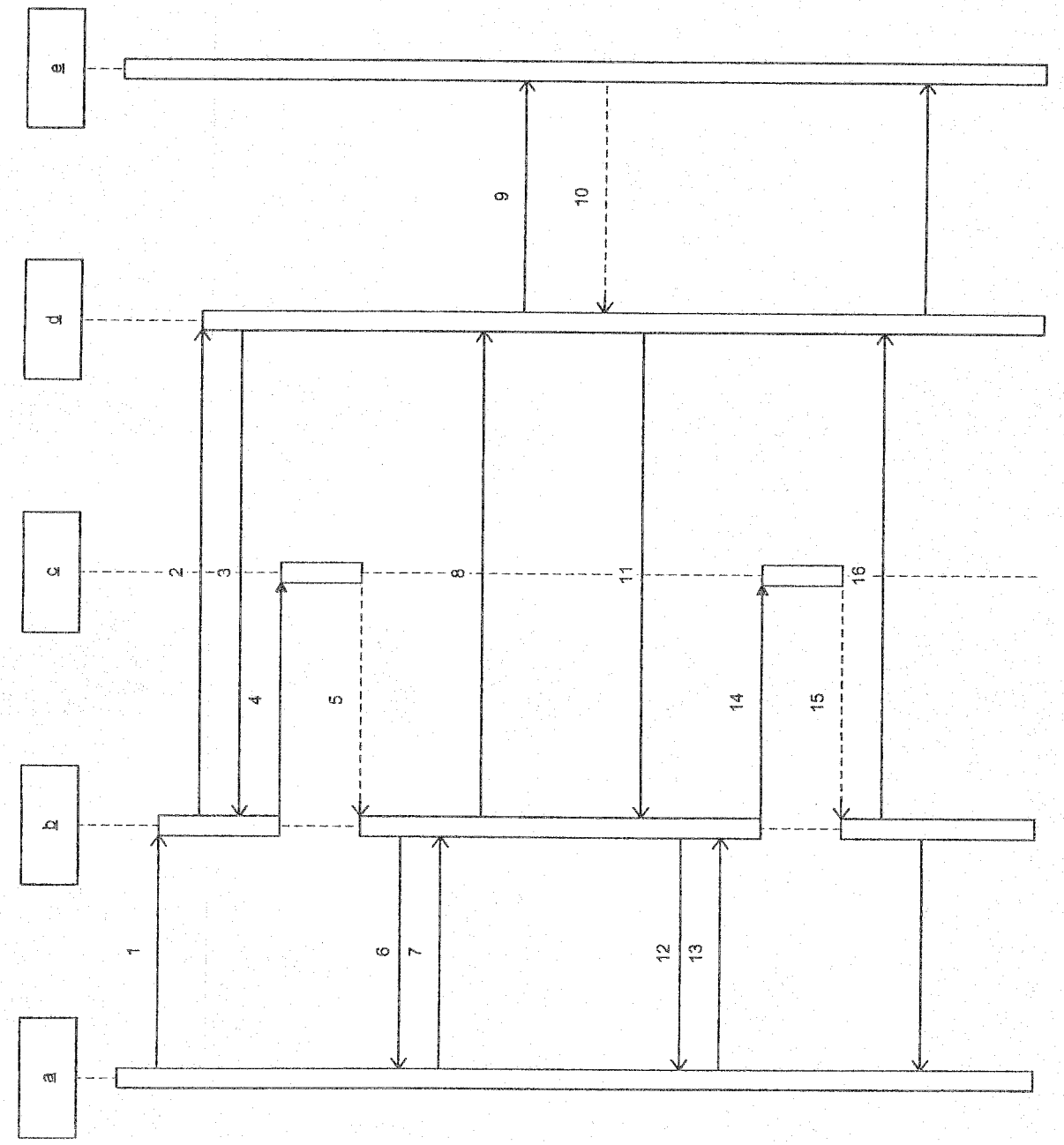

FIG. 4

Avv. C. FIAMMENGHI N° 29
Dott. D. DOMENIGHETTI-FIAMMENGHI N° 27
Via Quattro Fontane, 31 - ROMA
MIRELLA EREDIA (N° 184)