

ITALIAN PATENT OFFICE

Document No.

102011901929688A1

Publication Date

20120928

Applicant

IAMBOO S.R.L.

Title

METODO E APPARECCHIATURA PER L'AUTENTICAZIONE FORTE DI UN
UTENTE

5 DESCRIZIONE

Inoltre, l'invenzione riguarda una apparecchiatura che attua tale metodo.

L'introduzione di questo sistema, oltre ad interessare
25 le banche già esistenti, ha recentemente permesso la
nascita di banche totalmente on-line per le quali le

operazioni bancarie possono essere effettuate esclusivamente on-line.

La diffusione di questo tipo di tecnologia ha reso indispensabile lo sviluppo di sistemi di sicurezza sempre
5 più efficienti per garantire agli utenti di eseguire le operazioni bancarie in piena sicurezza.

I sistemi di sicurezza noti effettuano l'autenticazione dell'utente collegato in remoto alla banca per accertarne l'identità.

10 Tra i vari tipi di autenticazione quella in grado di assicurare il livello di sicurezza più elevato è nota con il termine di "autenticazione forte". Questo tipo di sistema è nella maggior parte dei casi un'autenticazione ad almeno due fattori, ossia una "password", o un "PIN" nota
15 all'utente, ed un oggetto posseduto dall'utente stesso, ad esempio una chiavetta OTP, o "token" ("gettone").

Una chiavetta OTP è un dispositivo elettronico, solitamente di dimensioni ridotte, che viene rilasciata ad esempio da un istituto di credito ai propri conto
20 correntisti. La chiavetta OTP genera un codice dinamico, ossia un codice che cambia periodicamente, o su richiesta dell'utente, che solitamente viene inoltrata premendo un tasto presente sul dispositivo stesso.

Tuttavia, le chiavette OTP comportano dei costi non
25 trascurabili per la loro gestione, approvvigionamento e distribuzione.

Un altro svantaggio è rappresentato dal fatto che un

utente che desidera accedere ad un'area riservata della banca on-line, ad esempio per predisporre una operazione bancaria, deve avere con sé la chiavetta. Inoltre, le chiavette OTP sono alimentate con batterie con una durata
5 limitata, al più di qualche anno. Una volta esaurita, la batteria deve essere sostituita, con notevoli disagi per l'utente soprattutto nel caso di operazioni bancarie urgenti. I sistemi di autenticazione prevedono l'uso di una password statica, ossia fissa, oppure dinamica, in quanto
10 cambia ad ogni nuovo utilizzo. Anche in questo caso, comunque, la password può essere "intercettata", ossia rubata da un utente malintenzionato.

In tal caso, sia che la password sia statica che dinamica, è necessario per l'utente richiedere una nuova
15 chiave al fornitore del servizio che dovrà anche provvedere a disabilitare la chiave rubata. Le "password dinamica", basta fare un accesso, o "riazzerare", il sistema per rendere inutilizzabile la chiave rubata.

Esistono anche sistemi di autenticazione che prevedono
20 l'autenticazione di un utente attraverso la SIM di un telefono cellulare.

Altri sistemi prevedono, invece, che l'utente effettui una chiamata al fornitore di un servizio, ad esempio chiamando un numero verde appositamente dedicato, per poter
25 accedere al servizio. L'autorizzazione ad accedere al servizio viene concessa dal sistema di autenticazione una volta effettuato il riconoscimento del numero di telefono

del chiamante.

Tuttavia, i numeri di telefono possono essere soggetti ad hackeraggio, quale "spoofing", alterazione, "impersonificazione". In particolare, è possibile
5 "ingannare" il sistema di autenticazione e far risultare una telefonata come effettuata da un determinato numero di telefono anche senza essere in possesso del terminale telefonico dell'utente associato a quel numero di telefono.

10 Sintesi dell'invenzione

È, quindi, scopo della presente invenzione fornire un metodo per l'autenticazione forte che sia in grado di superare i suddetti inconvenienti dei metodi noti.

È anche scopo della presente invenzione fornire una
15 apparecchiature per l'autenticazione forte che abbia i medesimi vantaggi.

Questi ed altri scopi sono raggiunti da un metodo per l'autenticazione forte di un utente, secondo l'invenzione, comprendente le fasi di:

- 20 - predisposizione di un terminale telefonico in corrispondenza di un utente, detto terminale telefonico essendo provvisto di un display di visualizzazione;
- interazione dell'utente con una pagina di
25 interfaccia di un computer tramite un dispositivo di interazione;

- inserimento di una pluralità di credenziali di autenticazione da parte dell'utente in detta pagina di interfaccia;

5 - invio da parte di detto computer di detta pluralità di credenziali di autenticazione ad una unità di gestione;

10 - elaborazione di detta pluralità di credenziali di autenticazione da parte di detta unità di gestione e generazione di un risultato, o esito, di detta elaborazione;

- autorizzazione/divieto a detto utente da parte dell'unità di gestione ad accedere ad un predeterminato servizio sulla base del risultato, o dell'esito di detta elaborazione;

15 la cui caratteristica principale è che detta elaborazione comprende le fasi di:

- esecuzione, da parte di detta unità di gestione, di una chiamata verso detto terminale telefonico, detta chiamata essendo associata ad un numero chiamante;

20 - visualizzazione di detto numero chiamante su detto display di detto terminale telefonico, detto numero chiamante coincidendo con, o contenendo, un codice di autorizzazione;

25 - introduzione da parte di detto utente di un codice in detta pagina di interfaccia, in particolare detto codice inserito corrispondendo a detto codice di autorizzazione;

- invio da parte di detto computer di detto codice inserito da detto utente a detta unità di gestione;
- verifica da parte di detta unità di gestione di una corrispondenza tra un codice inserito da detto utente in detta pagina di interfaccia e detto codice di autorizzazione coincidente con, o contenuto in numero chiamante, detta verifica generando detto risultato, o esito.

In particolare, la suddetta pluralità di credenziali di autenticazione inserite dall'utente nella pagina di interfaccia può comprendere almeno un recapito telefonico associato al terminale telefonico dell'utente.

In particolare, la fase di esecuzione, da parte di detta unità di gestione, di una chiamata verso detto terminale telefonico viene realizzata componendo detto recapito telefonico inserito da detto utente in detta pagina di interfaccia insieme a dette credenziali di autenticazione.

In alternativa, la fase di esecuzione, da parte di detta unità di gestione, di una chiamata verso detto terminale telefonico viene realizzata componendo un recapito telefonico indicato da detto utente in una fase preliminare di registrazione dell'utente al servizio.

Preferibilmente, il codice di autorizzazione coincide col numero chiamante visualizzato sul display del terminale telefonico dell'utente.

In una possibile forma realizzativa, il codice di

autorizzazione è deducibile dal numero chiamante visualizzato sul display del terminale telefonico dell'utente.

In particolare, il codice di autorizzazione può
5 coincidere con una parte del numero chiamante visualizzato sul display del terminale telefonico dell'utente.

In particolare, il codice di autorizzazione può essere una predeterminata parte del numero chiamante visualizzato sul display dell'utente, ad esempio, le ultime n cifre del
10 numero chiamante, dove n può essere compreso tra 3 e 10. In alternativa, i caratteri del numero chiamante che coincidono con il codice di autorizzazione possono essere quelli che occupano una predeterminata posizione all'interno del numero chiamante, ad esempio la prima, la
15 terza e la settima posizione.

In particolare, il codice di autorizzazione e/o il numero chiamante può essere generato in maniera dinamica dall'unità di gestione, in modo tale da cambiare ad ogni nuova richiesta di accesso da parte dell'utente.

20 In una possibile forma realizzativa l'interazione dell'utente con la pagina di interfaccia avviene mediante una connessione internet. Più in dettaglio, la pagina di interfaccia è associata ad una predeterminata pagina web.

Vantaggiosamente, la connessione internet viene
25 effettuata tramite un dispositivo elettronico.

In particolare, l'unità di gestione può autorizzare/vietare una determinata operazione

dispositiva, ad esempio un servizio home banking, sulla base dell'esito di detta elaborazione.

In particolare, è prevista una fase preliminare di registrazione da parte dell'utente ad un predeterminato servizio, detta fase di registrazione comprendendo
5 l'indicazione di una pluralità di credenziali di autenticazione, ossia di dati personali, da parte dell'utente comprendente almeno un recapito telefonico associato a detto terminale telefonico.

10 Vantaggiosamente, la pluralità di credenziali di autenticazione comprende almeno uno dei seguenti dati personali:

- una Userid;
- una Password;
- 15 - un recapito telefonico associato a detto terminale telefonico;
- o una loro combinazione.

In particolare, il dispositivo elettronico comprendente attraverso il quale l'utente si collega alla
20 suddetta pagina web può essere scelto tra:

- un PC portatile;
- un notebook;
- un tablet;
- un telefono cellulare;
- 25 o una loro combinazione.

La fase di elaborazione può prevedere:

- una prima verifica della corrispondenza di

credenziali di autenticazione inserite dall'utente nella pagina di interfaccia con credenziali di autenticazione predeterminate, ad esempio password e userid indicate dall'utente durante una fase di registrazione ad un servizio, detta prima verifica generando un primo risultato, o esito;

- una seconda verifica avviata se il primo risultato, o esito, della prima verifica è positivo, ossia se le credenziali inserite corrispondono alle credenziali predeterminate, detta seconda verifica essendo atta a verificare una corrispondenza tra un codice di autorizzazione inserito nella pagina di interfaccia dall'utente ed il codice di autorizzazione trasmesso dall'unità di gestione al terminale telefonico.

In particolare, se il primo esito è negativo, l'unità di gestione nega l'accesso al servizio, se, invece, il primo esito è positivo, l'unità di gestione effettua la chiamata al terminale telefonico dell'utente e, quindi, avvia la seconda fase di verifica.

Secondo un altro aspetto dell'invenzione un'apparecchiatura per l'autenticazione forte di un utente comprende:

- un'unità di gestione atta ad elaborare una pluralità di credenziali di autenticazione di un utente e a generare un risultato, o esito, di tale elaborazione per autorizzare/vietare a detto utente un accesso ad un predeterminato servizio sulla base di

detto risultato, o esito, detta unità di gestione comprendendo mezzi di comunicazione telefonica ad un terminale telefonico di detto utente, detta chiamata essendo associata ad un numero chiamante atto ad essere visualizzato su un display di detto terminale telefonico, detto numero chiamante contenendo, o coincidendo con, detto codice di autorizzazione;

- un dispositivo di interazione di detto utente con detta unità di gestione, detto dispositivo di interazione comprendendo:

- mezzi di visualizzazione di una pagina di interfaccia;

- mezzi di inserimento di caratteri alfanumerici per l'inserimento di dette credenziali di autenticazione in detta pagina di interfaccia;

- mezzi di invio di dette credenziali di autenticazione a detta unità di gestione.

In particolare, l'unità di gestione verifica la corrispondenza delle credenziali di autenticazione con credenziali di autenticazione predeterminate comprendenti il codice di autorizzazione trasmesso al terminale telefonico dell'utente.

In particolare, l'unità centrale di gestione può comprendere:

- un server in collegamento con il dispositivo di interfaccia, detto server essendo atto a realizzare la verifica della corrispondenza tra la pluralità di

credenziali di autenticazione inserite nella pagina di interfaccia dall'utente con credenziali di autenticazione predeterminate memorizzate su un database presente sul server;

- 5 - un dispositivo ausiliario comprendente i suddetti mezzi per trasmettere il codice di autorizzazione al terminale telefonico dell'utente, detto dispositivo ausiliario essendo in collegamento con il server ed avviando l'esecuzione della chiamata al terminale
10 telefonico dell'utente su richiesta del server per trasmettere il codice di autorizzazione.

In una forma realizzativa prevista, ad ogni richiesta di accesso da parte dell'utente il dispositivo ausiliario genera un nuovo codice di autorizzazione ed effettua la
15 chiamata al terminale telefonico dell'utente.

In particolare, il dispositivo ausiliario effettua una chiamata al terminale telefonico dell'utente in modo tale da visualizzare sul display del terminale telefonico un numero chiamante contenente, o coincidente, con il codice
20 di autorizzazione.

Preferibilmente, il dispositivo ausiliario genera il numero chiamante e/o il codice di autorizzazione in maniera dinamica, ossia in modo tale da risultare diverso ad ogni richiesta di accesso inoltrata da parte
25 dell'utente.

In una possibile forma realizzativa, il numero chiamante e/o il codice di autorizzazione può essere

selezionato tra una pluralità di numeri chiamanti e/o di codici di autorizzazione memorizzati nel dispositivo ausiliario.

In alternativa, il numero chiamante e/o il codice di
5 autorizzazione può essere generato in maniera casuale dal dispositivo ausiliario.

Descrizione dettagliata di alcune forme realizzative

Come illustrato nello schema a blocchi 100 di figura 1, un metodo per l'autenticazione forte di un utente,
10 secondo l'invenzione, comprende una fase iniziale di interazione dell'utente con una pagina di interfaccia tramite un dispositivo di interazione provvisto di un computer, o mezzi di elaborazione, blocco 101. L'utente procede, quindi, ad inserire nella pagina di interfaccia,
15 ad esempio mediante digitazione di tasti, o mediante un touch screen, una pluralità di credenziali di autenticazione e ad inviare la pluralità di credenziali di autenticazione ad una unità di gestione, blocco 102.

Segue una chiamata da parte dell'unità di gestione al
20 terminale telefonico dell'utente, blocco 103. In particolare, la chiamata è associata ad un numero chiamante che viene visualizzato sul display del terminale telefonico dell'utente. Più in dettaglio, il numero chiamante coincide, o contiene, un codice di
25 autorizzazione.

Questa fase, viene eseguita da mezzi di comunicazione

telefonica al terminale telefonico, ad esempio un telefono
cellulare 30. I mezzi per effettuare la chiamata possono
risiedere in un dispositivo ausiliario 40 (vedi figura 3 e
4) in collegamento con un server 20 nel quale è presente
5 un database all'interno del quale sono memorizzate le
credenziali di autenticazione degli utenti iscritti ad un
determinato servizio, ad esempio un servizio home banking
ed eventualmente un recapito telefonico associato
all'utente. In tal caso, quindi, l'unità di gestione 50
10 comprende il server 20 ed il dispositivo ausiliario 40.
Più in dettaglio, i mezzi per effettuare la chiamata, su
richiesta del server 20 effettuano la chiamata al
terminale telefonico 30.

Il metodo prevede, inoltre, una fase di verifica da
15 parte dell'unità di gestione, ed in particolare del server
20, della corrispondenza tra la pluralità di credenziali
di autenticazione con una pluralità di credenziali
predeterminate, in particolare registrate in una fase
preliminare dall'utente, e di un codice inserito nella
20 pagina di interfaccia ed inviato dall'utente con un codice
di autorizzazione inviato dai mezzi di comunicazione
telefonica al terminale telefonico dell'utente, blocco
104. Il server 20 effettua, in particolare, un matching
tra il codice inserito dall'utente nella pagina di
25 interfaccia ed inviato tramite il dispositivo di
interazione ed il codice di autorizzazione predeterminato.
In una forma realizzativa prevista, il codice di

autorizzazione può essere una parte, ad esempio le ultime n cifre del numero chiamante visualizzato sul display del terminale telefonico dell'utente. In particolare, n può essere compreso tra 3 e 10, ad esempio n=4.

5 La fase di verifica si conclude con la generazione di un risultato, o esito. Più precisamente, se l'esito della verifica è positivo, ossia se le credenziali di autenticazione ed il codice inserito dall'utente nella pagina di interfaccia coincidono con le credenziali di
10 autenticazione predeterminate, l'utente viene autorizzato ad accedere al servizio richiesto, o alla pagina riservata, blocco 110.

Se, invece, l'esito della verifica è negativo, ossia se le credenziali di autenticazione e/o il codice digitato
15 dall'utente nella pagina di interfaccia non coincidono con le credenziali di autenticazione predeterminate, l'accesso al servizio viene negato, blocco 105.

Nella variante del metodo illustrata in figura 2, è prevista una fase di inserimento nella pagina di
20 interfaccia da parte dell'utente di credenziali di autenticazione, quali userid e password, blocco 102a.

Segue, quindi, una verifica, o "matching", delle credenziali inserite nella pagina di interfaccia dall'utente con le credenziali predeterminate presenti nel
25 suddetto database, blocco 104a.

Se la verifica eseguita dal server 20, dà esito negativo, viene negato l'accesso al servizio, blocco 105.

Se, al contrario, la verifica dà esito positivo, il server 20 inoltra al dispositivo ausiliario una richiesta di effettuare una chiamata al terminale telefonico dell'utente, blocco 103.

5 L'utente, quindi visualizza il numero chiamante sul display del terminale telefonico, ed inserisce nella pagina di interfaccia il codice di autorizzazione inviandolo poi al server 20, blocco 102b.

Il server 20, quindi, inoltra il codice ricevuto
10 dall'utente 60 al dispositivo ausiliario 40 che provvede a verificarne la corrispondenza con il codice di autorizzazione e a fornire al server 20 un risultato, o esito di tale verifica. Se la verifica eseguita dal dispositivo ausiliario 40, dà esito negativo, il server 20
15 nega l'accesso al servizio, blocco 105.

Se, al contrario, la verifica dà esito positivo, il server 20 autorizza la fruizione del servizio all'utente, blocco 110.

In una variante prevista dall'invenzione e
20 schematicamente illustrata in figura 4, la verifica della corrispondenza del codice inserito nella pagina di interfaccia dall'utente con il codice di autorizzazione viene eseguita direttamente dal server 20.

In questo caso, è prevista una fase in cui il
25 dispositivo ausiliario 40 comunica al server 20 il codice di autorizzazione trasmesso al terminale telefonico 30 dell'utente 60 tramite la chiamata telefonica.

In una possibile forma realizzativa l'interazione dell'utente con la pagina di interfaccia avviene mediante una connessione internet. Più in dettaglio, la pagina di interfaccia è associata ad una predeterminata pagina web
5 alla quale l'utente 60 accede digitando un indirizzo web, o URL, ad esso associato su un dispositivo elettronico, quale un portatile, un PC, un notebook, un palmare, un tablet, uno smart-phone, ecc.

In una particolare forma realizzativa prevista ed
10 illustrata schematicamente in figura 5, il dispositivo di interfaccia 10 attraverso il quale l'utente si collega al server 20 può essere un computer 10 di un bancomat 70 collegato tramite rete telematica al server 20 stesso.

La descrizione di cui sopra di una forma
15 realizzativa specifica è in grado di mostrare l'invenzione dal punto di vista concettuale in modo che altri, utilizzando la tecnica nota, potranno modificare e/o adattare in varie applicazioni tale forma realizzativa specifica senza ulteriori ricerche e senza
20 allontanarsi dal concetto inventivo, e, quindi, si intende che tali adattamenti e modifiche saranno considerabili come equivalenti della forma realizzativa specifica. I mezzi e i materiali per realizzare le varie funzioni descritte potranno essere di varia natura senza
25 per questo uscire dall'ambito dell'invenzione. Si intende che le espressioni o la terminologia utilizzate hanno scopo puramente descrittivo e per questo non limitativo.

RIVENDICAZIONI

1. Metodo per l'autenticazione forte di un utente comprendente le fasi di:

- predisposizione di un terminale telefonico in
5 corrispondenza di un utente, detto terminale telefonico essendo provvisto di un display di visualizzazione;

- interazione di detto utente con una pagina di interfaccia tramite un dispositivo di interazione;

10 - inserimento di una pluralità di credenziali di autenticazione da parte di detto utente in detta pagina di interfaccia;

- invio di detta pluralità di credenziali di autenticazione ad una unità di gestione;

15 - elaborazione, da parte di detta unità di gestione, di detta pluralità di credenziali di autenticazione e generazione di un risultato, o esito, di detta elaborazione;

20 - autorizzazione/divieto a detto utente da parte di detta unità di gestione ad accedere ad un predeterminato servizio sulla base di detto risultato, o esito di detta elaborazione;

caratterizzato dal fatto che detta elaborazione comprende le fasi di:

25 - esecuzione, da parte di detta unità di gestione, di una chiamata verso detto terminale telefonico, detta

chiamata essendo associata ad un numero chiamante;

- visualizzazione di detto numero chiamante su detto display di detto terminale telefonico, detto numero chiamante coincidendo, o contenendo, un codice di autorizzazione;

- verifica da parte di detta unità di gestione della corrispondenza tra un codice inserito da detto utente in detta pagina di interfaccia e detto codice di autorizzazione, detta verifica generando detto risultato, o esito.

2. Metodo, secondo la rivendicazione 1, in cui detto numero chiamante e/o detto codice di autorizzazione viene generato in maniera dinamica da detta unità di gestione, per cui detto numero chiamante e/o detto codice di autorizzazione è diverso ad ogni nuova richiesta di accesso da parte di detto utente.

3. Metodo, secondo la rivendicazione 1, in cui detta pagina di interfaccia è una pagina web, detta interazione di detto utente con detta pagina di interfaccia essendo realizzata attraverso un collegamento internet a detta pagina web.

4. Metodo, secondo la rivendicazione 1, in cui è prevista una fase preliminare di registrazione da parte di detto utente ad un predeterminato servizio, detta fase di registrazione prevedendo l'indicazione da parte di detto utente di una pluralità di credenziali di

autenticazione ed un recapito telefonico associato a detto utente.

5. Metodo, secondo la rivendicazione 1, in cui detta fase di elaborazione prevede le fasi di:

5 - una prima verifica della corrispondenza di
credenziali di autenticazione inserite da detto utente
in detta pagina di interfaccia con credenziali di
autenticazione predeterminate, detta prima verifica
generando un primo risultato, o esito;

10 - una seconda verifica avviata se detto primo
risultato, o esito, di detta prima verifica è
positivo, ossia se dette credenziali inserite
corrispondono a dette credenziali predeterminate,
detta seconda verifica essendo atta a verificare una
15 corrispondenza tra un codice di autorizzazione
inserito in detta pagina di interfaccia da detto
utente e detto codice di autorizzazione contenuto in,
o coincidente con, detto numero chiamante di detta
chiamata effettuata da detta unità di gestione a detto
20 terminale telefonico di detto utente.

6. Apparecchiatura per l'autenticazione forte di un
utente **caratterizzata dal fatto** di comprendere:

 - un'unità di gestione atta ad elaborare una
pluralità di credenziali di autenticazione di un
25 utente e a generare un risultato, o esito, di tale
elaborazione per autorizzare/vietare a detto utente un
accesso ad un predeterminato servizio sulla base di

detto risultato, o esito, detta unità di gestione comprendendo mezzi di comunicazione telefonica atti ad effettuare una chiamata ad un terminale telefonico di detto utente, detta chiamata essendo associata ad un numero chiamante atto ad essere visualizzato su un display di visualizzazione di detto terminale telefonico di detto utente, detto numero chiamante contenendo, o coincidendo con, un codice di autorizzazione, detta unità di gestione essendo atta a verificare la corrispondenza tra un codice inserito in detta pagina di interfaccia da detto utente e detto codice di autorizzazione, generando detto risultato, o esito;

- un dispositivo di interazione di detto utente con detta unità di gestione, detto dispositivo di interazione comprendendo:

- mezzi di visualizzazione di una pagina di interfaccia;

- mezzi di inserimento di caratteri alfanumerici per l'inserimento di dette credenziali di autenticazione in detta pagina di interfaccia;

- mezzi di invio di dette credenziali di autenticazione a detta unità di gestione.

7. Apparecchiatura, secondo la rivendicazione 6, in cui detta unità centrale di gestione comprende:

- un server in collegamento con detto dispositivo di interfaccia, detto server essendo atto a realizzare

una verifica di corrispondenza tra detta pluralità di
credenziali di autenticazione inserite in detta pagina
di interfaccia da detto utente con credenziali di
autenticazione predeterminate memorizzate su un
5 database presente in detto server;

- un dispositivo ausiliario in collegamento con detto
server, detto dispositivo ausiliario comprendendo
detti mezzi di comunicazione telefonica atti ad
effettuare detta chiamata associata a detto numero
10 chiamante a detto terminale telefonico di detto utente
su richiesta di detto server.

8. Apparecchiatura, secondo la rivendicazione 7, in cui
ad ogni richiesta di accesso a detto servizio da parte
di detto utente detto dispositivo ausiliario genera un
15 nuovo codice di autorizzazione ed effettua detta
chiamata a detto terminale telefonico di detto utente,
detta chiamata essendo associata ad un numero
chiamante atto ad essere visualizzato su un display di
detto terminale telefonico, detto codice di
20 autorizzazione essendo contenuto in, o coincidendo
con, detto numero chiamante.

9. Apparecchiatura, secondo la rivendicazione 8, in cui
detto codice di autorizzazione comprende:
- un numero chiamante selezionato tra una pluralità
25 di numeri chiamanti memorizzati in detto dispositivo
ausiliario.

10. Apparecchiatura, secondo la rivendicazione 8, in cui detto codice di autorizzazione comprende:

- un numero chiamante generato in maniera dinamica da detto dispositivo ausiliario, in modo tale che detto
5 numero chiamante e/o detto codice di autorizzazione è diverso per ciascuna richiesta di accesso da parte di detto utente.

p.p. IAMBOO S.r.l.

CLAIMS

1. Method for strong authentication of a user comprising the steps of:

- 5 - prearranging a telephone at a user, said telephone having a visualization display;
- interaction of said user with an interface page on a computer terminal by an interaction device;
- entering by said user a plurality of authentication credentials in said interface page;
- 10 - sending by said computer terminal said plurality of authentication credentials to an operation unit;
- controlling, by said operation unit, said plurality of authentication credentials and generating a result, or outcome, of said controlling step;
- 15 - authorizing/denying said user by said operation unit to approach a predetermined service on the basis of said result, or outcome of said controlling step;
- characterised in that** said controlling step comprises:
 - 20 - executing, by said operation unit, a phone call towards said telephone, said phone call associated with a calling number;
 - displaying said calling number on said display of said telephone, said calling number coinciding with, or containing, an authorization code;
 - 25 - entering by said user a code in said interface page;

- sending by said computer terminal said authorisation code to said operation unit;

- verifying by said operation unit a correspondence between said code entered by said user in said interface page and said authorization code coinciding with, or contained in said calling number, said check generating said result, or outcome.

5

10

2. Method, according to claim 1, wherein said calling number and/or said authorization code is generated in a dynamic way from said operation unit, such that said calling number and/or said authorization code is different at each request for access by said user.

15

3. Method, according to claim 1, wherein said interface page is a web page, said interaction of said user with said interface page being carried out through a Internet connection to said web page.

20

4. Method, according to claim 1, wherein a preliminary registration step by said user to a predetermined service is provided, said registration step providing entering by said user a plurality of authentication credentials and a telephone address associated with said user.

25

5. Method, according to claim 1, wherein said controlling provides the steps of:
- a first check of authentication credentials entered by said user in said interface page with registered

authentication credentials, said first check generating a first result, or outcome;

- a second check started if said first result, or outcome, of said first check is positive, i.e. if said

5 authentication credentials entered correspond to said registered authentication credentials, said second check adapted to test a correspondence between a authorization code entered in said interface page by said user and said authorization code contained in, or
10 coinciding with, said calling number of said phone call made by said operation unit to said telephone of said user.

6. Apparatus for strong authentication of a user **characterised in that** it comprises:

15 - an operation unit for evaluating a plurality of authentication credentials of a user and for generating a result, or outcome, of this evaluating for authorizing/denying to said user an access to a predetermined service on the basis of said result, or
20 outcome, said operation unit comprising a phone communication means adapted to make a phone call one to a telephone of said user, said phone call associated with a calling number that is adapted to be displayed on a visualization display of said telephone
25 of said user, said calling number containing, or coinciding with, an authorization code, said operation

unit adapted to test the correspondence between a code entered in said interface page by said user and said authorization code, in order to generate said result, or outcome;

5 - an interaction device of said user with said operation unit, said interaction device comprising:

 - a means for displaying an interface page;

 - a means for entering alphanumeric characters for entering said authentication credentials in said
10 interface page;

 - a means for sending said authentication credentials to said operation unit.

7. Apparatus, according to claim 6, wherein said central operation unit comprises:

15 - a server in connection with said interface device, said server adapted to provide a checking correspondence between said plurality of authentication credentials put in said interface page by said user with authentication predetermined
20 credentials registered on a database present in said server;

 - an auxiliary device in connection with said server, said auxiliary device comprising said phone communication means that is adapted to make said phone
25 call associated with said calling number to said telephone of said user on request by said server.

8. Apparatus, according to claim 7, wherein at each request for said service by said user said auxiliary device generates an authorization code and carries out said phone call to said telephone of said user, said
5 phone call associated with a calling number that is adapted to be displayed on a display of said telephone, said authorization code contained in, or coinciding with, said calling number.
9. Apparatus, according to claim 8, wherein said
10 authorization code comprises a calling number selected among a plurality of calling numbers recorded in said auxiliary device,
10. Apparatus, according to claim 8, wherein said authorization code comprises a calling number
15 generated in a dynamic way by said auxiliary device, such that said calling number and/or said authorization code is different for each request for access by said user.

Fig. 1

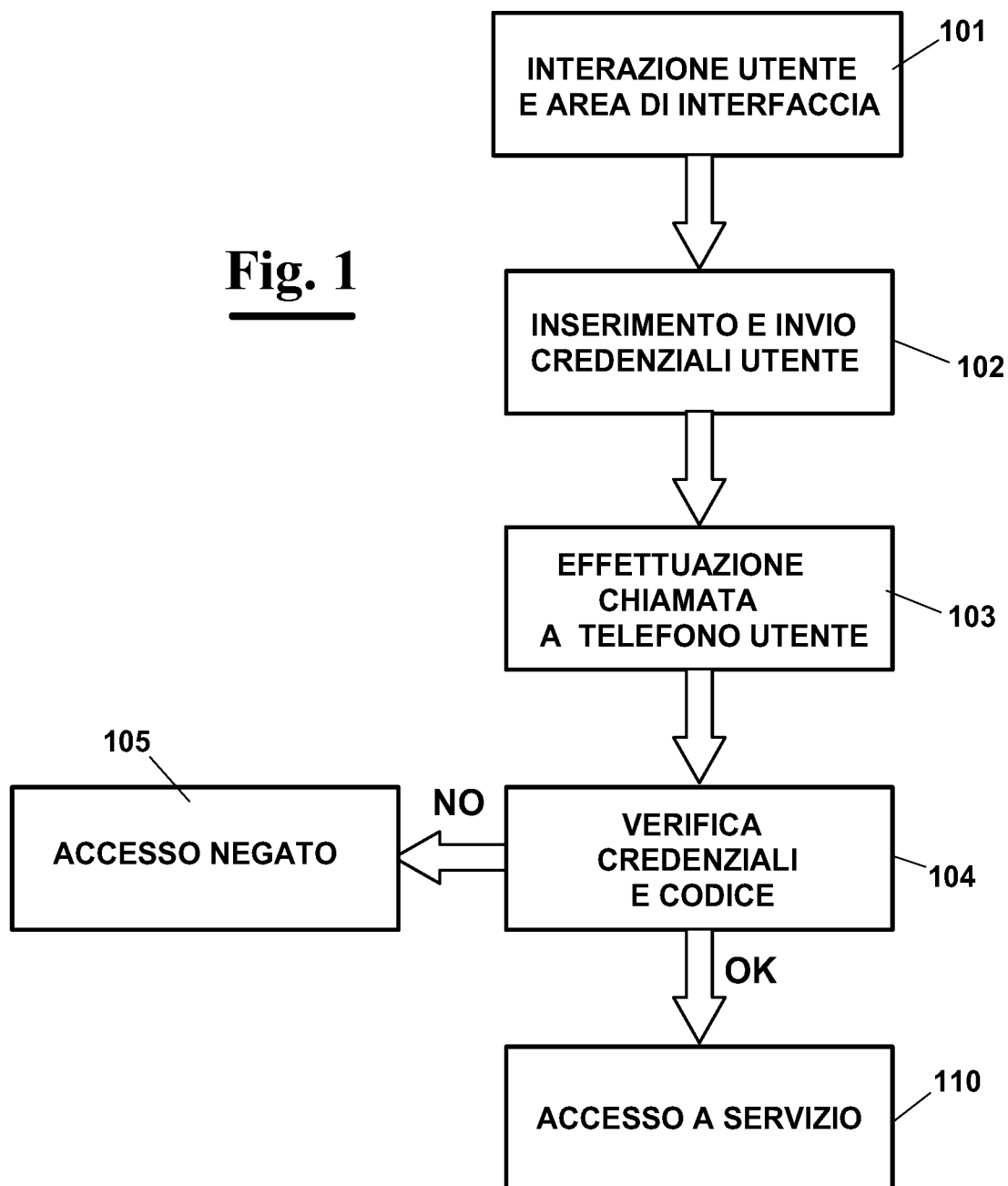
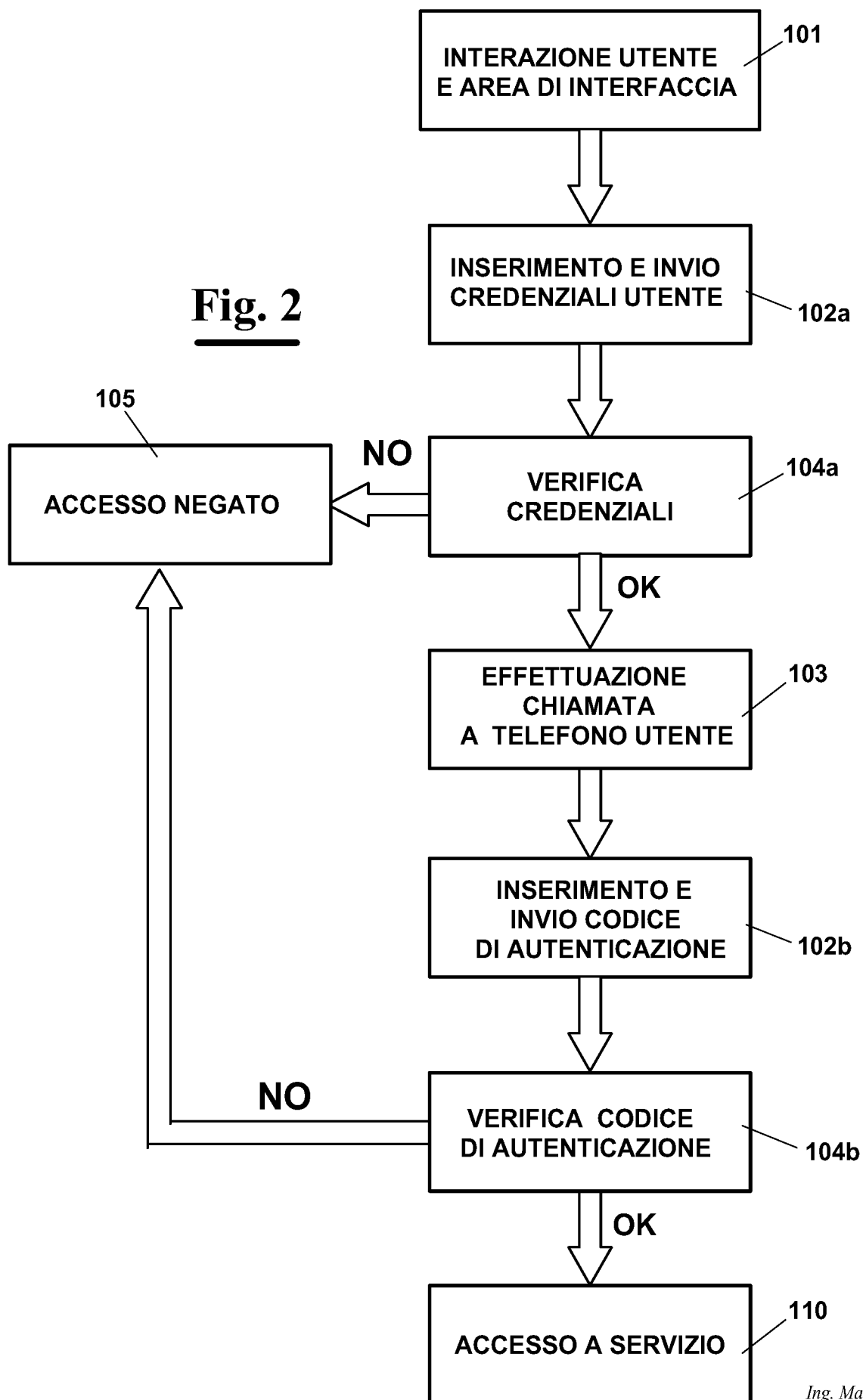


Fig. 2



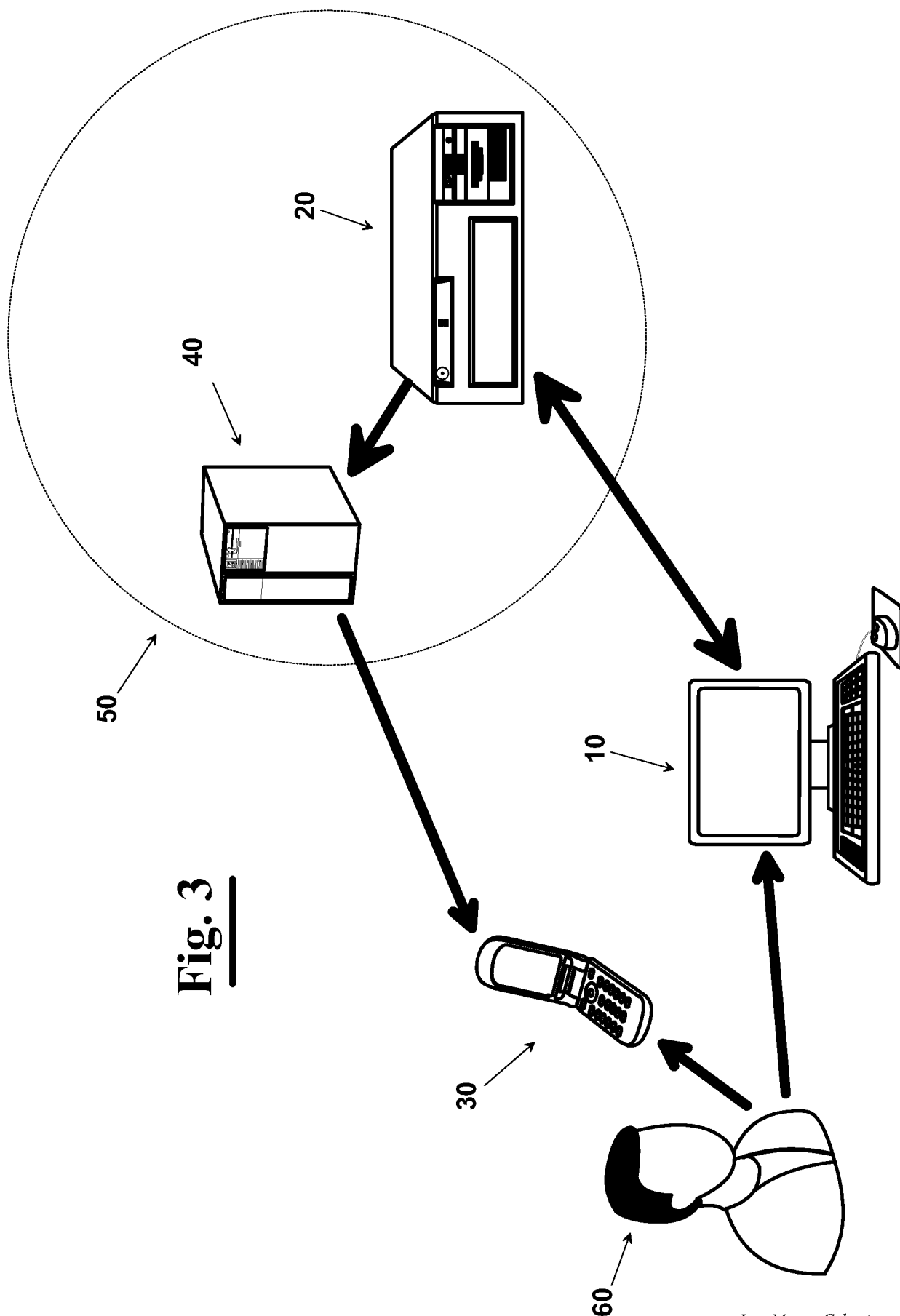


Fig. 3

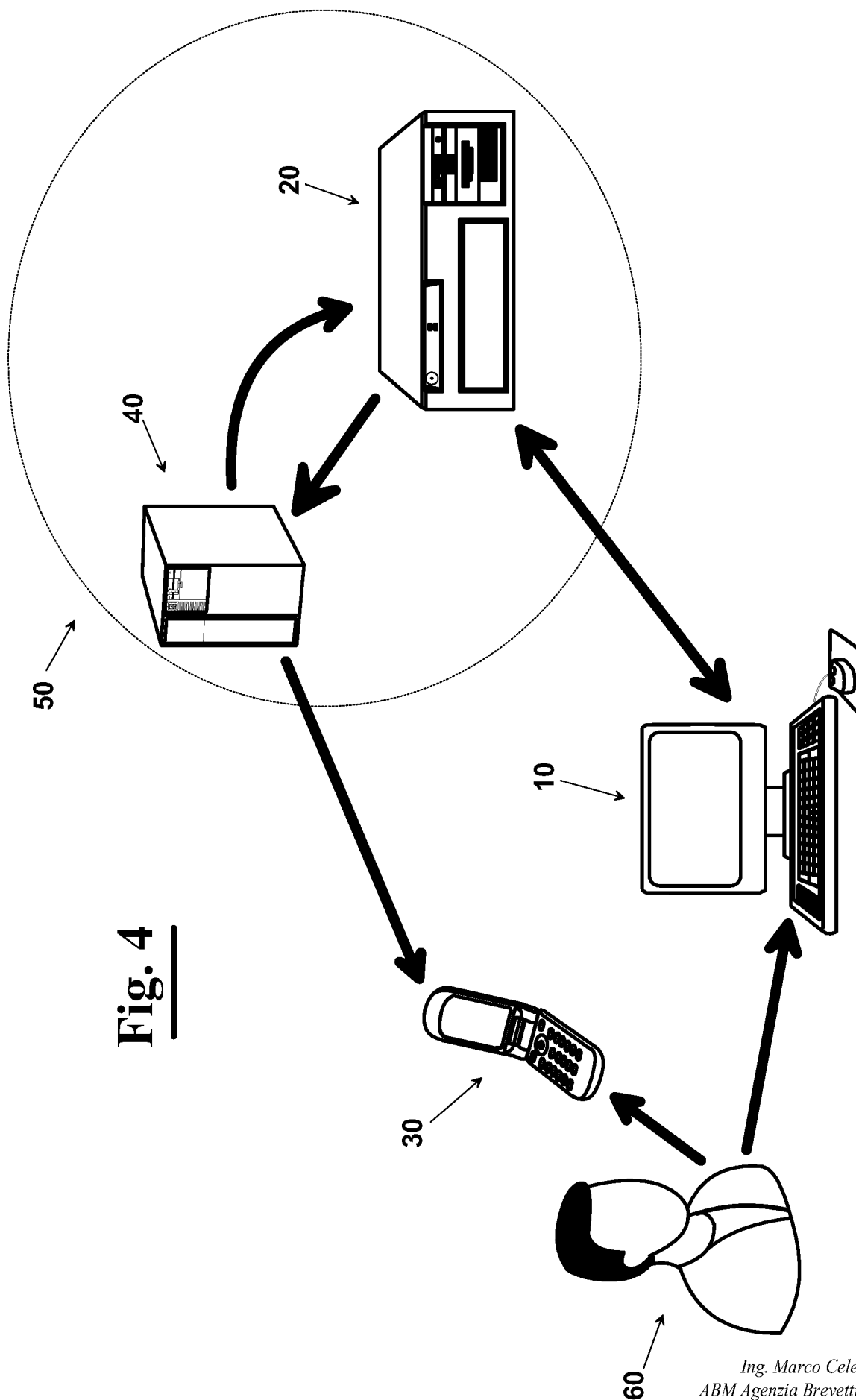


Fig. 4

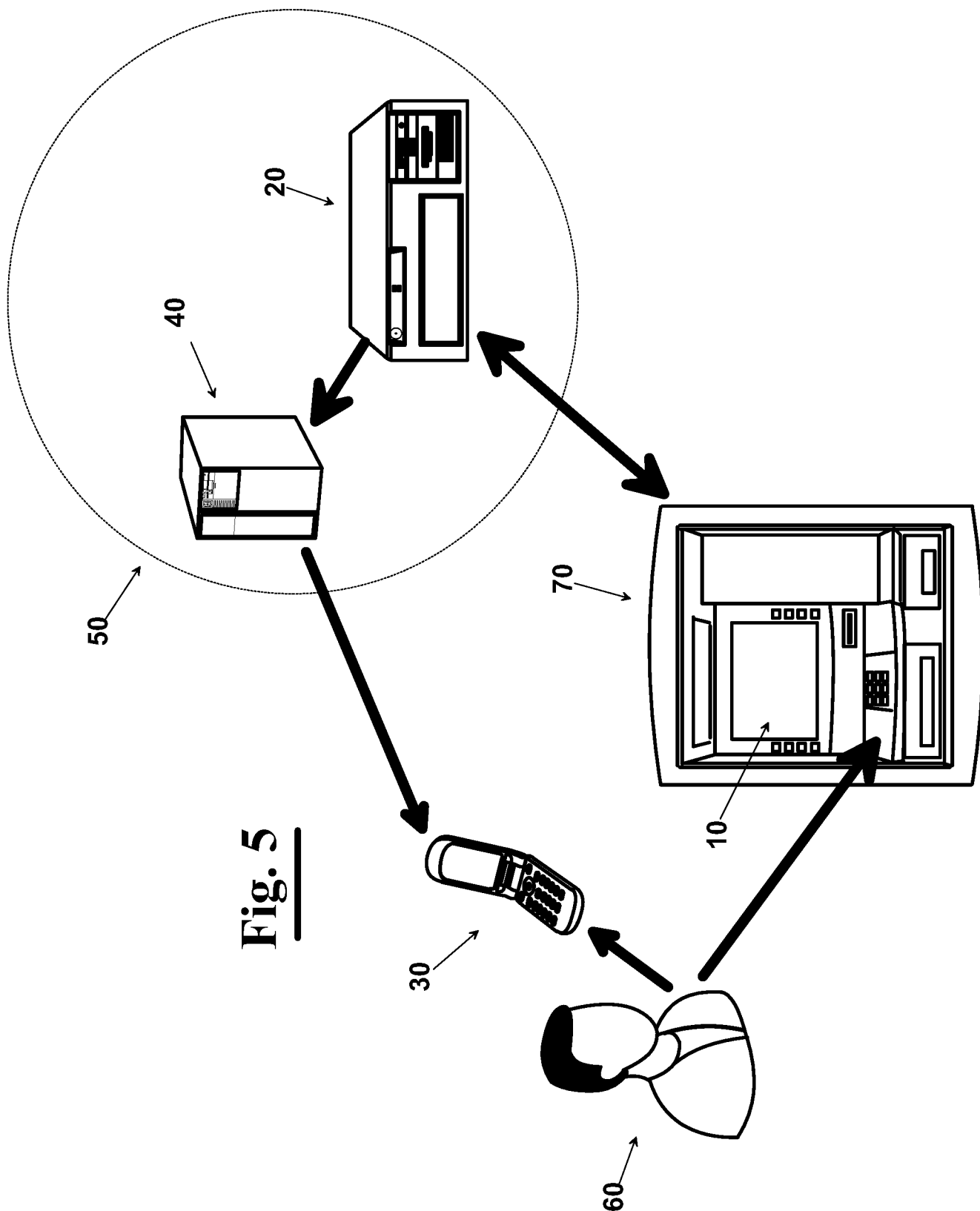


Fig. 5