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

DOMANDA NUMERO	**102007901577190**
Data Deposito	**26/11/2007**
Data Pubblicazione	**26/05/2009**

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
H	04	L		

Titolo

METODO DI AUTENTICAZIONE PER UTENTI APPARTENENTI AD ORGANIZZAZIONI DIVERSE SENZA DUPLICAZIONE DELLE CREDENZIALI

Descrizione dell'Invenzione Industriale dal titolo: **-CSP001-**

"METODO DI AUTENTICAZIONE PER UTENTI APPARTENENTI AD ORGANIZZAZIONI DIVERSE SENZA DUPLICAZIONE DELLE CREDENZIALI"

di CSP – Innovazione nelle ICT Scarl, di nazionalità italiana, con sede in Torino, Via Livorno 60, ed elettivamente domiciliata, ai fini del presente incarico, presso i Mandatari Ing. Marco CAMOLESE (Iscr. Albo No. 882BM), Ing. Antonio DI BERNARDO (Iscr. Albo No. 1163BM), Ing. Andrea GRIMALDO (Iscr. Albo No. 1160BM) e Dott. Giancarlo REPOSIO (Iscr. Albo No. 1168BM), c/o Metroconsult S.r.l., Via Sestriere, 100 - 10060 None (TO).

Inventori designati:

Andrea GHITTINO, Via Frejus, 35 Torino 10139

Stefano ANNESE, Via Chambery, 91/13 Torino 10142

Roberto BORRI, Via Torino 110, Nole 10076

Sergio Sagliocco, Via Bodina 41, Cuneo 12100

Depositata il No.

RIASSUNTO

La presente invenzione si riferisce ad un metodo per permettere ad un utente di accedere ad Internet. Un utente effettua una richiesta di accesso ad Internet attraverso un gateway di una prima Organizzazione e fornisce a quest'ultimo alcune credenziali di autenticazione presso una seconda Organizzazione. Le credenziali fornite contengono almeno una informazione relativa alla seconda Organizzazione.

La prima Organizzazione contatta la seconda Organizzazione al fine di autenticare l'utente e permettergli l'accesso ad Internet. La seconda

Organizzazione rilascia all'utente l'autorizzazione ad accedere ad Internet. Secondo l'invenzione, a seguito della richiesta di accesso il gateway redirige l'utente verso una pagina web della seconda Organizzazione, e a questo punto l'utente fornisce alla seconda Organizzazione, attraverso la pagina web, ulteriori credenziali di autenticazione necessarie ad identificarlo.

DESCRIZIONE

La presente invenzione si riferisce ad un metodo per permettere ad un utente di accedere ad Internet secondo il preambolo della rivendicazione 1.

In particolare, l'invenzione è diretta ad incrementare le possibilità di un utente di accedere ad Internet.

Internet è ormai diventato uno strumento di lavoro indispensabile per molte persone e, tramite le reti wireless (es. WLAN) un utente può accedere ad Internet anche al di fuori dell'ufficio.

Ad esempio negli aeroporti, nelle stazioni ferroviarie, e nelle biblioteche sono previsti Hot Spot, ossia dei punti di accesso dove un utente può collegarsi ad Internet attraverso un gateway.

Solitamente, all'interno di un Hot Spot di una data Organizzazione l'accesso al servizio è consentito solamente agli utenti che hanno un account valido registrato presso la data Organizzazione.

Un utente di una data Organizzazione non può quindi accedere ad Internet in aree non coperte dalla suddetta Organizzazione per mancanza di interesse della stessa o per guasti alle infrastrutture.

Per ovviare a questi problemi, sono state concepite diverse soluzioni che permettono ad un utente di una prima Organizzazione di accedere ad

Internet attraverso punti di accesso di una seconda Organizzazione.

Alcune di queste soluzioni prevedono di intervenire sul client dell'utente con configurazioni a volte complesse e dipendenti dalla piattaforma utilizzata.

Altre soluzioni, preferibili dal punto di vista della semplicità di utilizzo e di configurazione del client utente, intervengono solamente a livello di gateway reindirizzando gli utenti che non rientrano nell'elenco degli utenti autorizzati all'accesso, verso l'Authentication Server di una diversa Organizzazione.

Una di queste ultime soluzioni è nota dal brevetto US 5,898,780, il quale rende noto un metodo ed un apparato per permettere ad un utente di accedere ad Internet da una località remota utilizzando un Internet Service Provider (ISP) locale con il quale non ha alcun account. L'utente si registra nel sistema dell'ISP locale utilizzando le credenziali (nome utente e password) dell'account che l'utente ha presso l'ISP remoto.

Un server dell'ISP locale riconosce che le credenziali inserite dall'utente contengono un'informazione che permette di identificare il server dell'ISP locale ed indirizza una query a quest'ultimo al fine di autorizzare l'utente ad accedere ad Internet attraverso l'ISP locale.

Questa soluzione presenta tuttavia lo svantaggio che dati sensibili dell'utente (nome utente e password) vengono fornite al server dell'ISP locale, il che le rende soggette ad attacchi di sniffing.

Una soluzione che utilizza una filosofia opposta rispetto a quella nota dal brevetto US 5,898,780, è stata utilizzata dall'università di Trento e pubblicizzata con il nome di Uni-fy.

Questa soluzione prevede che il client utente esegua una richiesta DHCP al gateway dell'università che gli assegna così un indirizzo IP.

Il gateway è provvisto di alcune regole di firewall, ognuna delle quali prevede due possibili azioni a seconda che i pacchetti dati provengano da un utente che rientra, o meno, in una lista di utenti autorizzati.

Nel caso in cui l'utente non sia tra quelli autorizzati, allora i pacchetti dati vengono indirizzati verso un gatekeeper che si occupa dell'autorizzazione. Secondo un metodo del tipo "*captive portal*", l'utente non autorizzato viene indirizzato verso una pagina web locale dove può selezionare l'Organizzazione da cui farsi autorizzare.

A questo punto il client utente viene messo in comunicazione con l'Organizzazione selezionata e vengono eseguite le procedure di autenticazione secondo i protocolli richiesti dall'Organizzazione.

Secondo questa soluzione, le apparecchiature della rete dell'Università di Trento non possono e non devono in alcun modo venire a conoscenza di dati sensibili dell'utente, i quali sono trasmessi tutti direttamente all'Organizzazione selezionata.

In caso di autenticazione, l'Organizzazione selezionata trasmette una richiesta di autorizzazione al gatekeeper dell'università, il quale cambia lo stato dell'utente da non autorizzato ad autorizzato, consentendogli così l'accesso ad Internet.

Questa soluzione presenta lo svantaggio che il riconoscimento dell'utente connesso (ad esempio per motivi di sicurezza o di fatturazione) non è agevole e richiede di legare lo pseudonimo dell'utente all'identità dell'utente registrata presso l'Organizzazione autenticante remota.

Inoltre questa soluzione presenta notevoli limiti di scalabilità del sistema in quanto la selezione manuale dell'Organizzazione da cui farsi autenticare presuppone che il gateway dell'università conosca tutte le Organizzazioni autenticatrici e che sia costantemente aggiornato di eventuali cambiamenti nelle procedure di autenticazione a livello di singola Organizzazione autenticatrice.

Al crescere del numero delle organizzazioni conduttrici, la complessità di gestione del sistema dell'università cresce considerevolmente.

La presente invenzione ha come scopo primario quello di superare gli inconvenienti dell'arte nota presentando un metodo alternativo per permettere ad un utente di accedere ad Internet attraverso un gateway di un'Organizzazione presso la quale non è inizialmente accreditato.

Questo scopo è raggiunto mediante un metodo incorporante le caratteristiche delle rivendicazioni allegate, le quali formano parte integrante della presente descrizione.

L'idea alla base della presente invenzione consiste generalmente nel separare gli istanti di tempo (e i destinatari) in cui sono fornite le credenziali di autenticazione.

Più precisamente, l'idea consiste nel fatto che quando l'utente si connette al gateway di una prima Organizzazione ed effettua una richiesta di accesso ad Internet, questo fornisce una parte delle credenziali necessarie per l'accreditamento presso una seconda Organizzazione. Ad esempio, l'utente può fornire un nome utente e un identificativo della seconda Organizzazione.

Il gateway che riceve tale richiesta e che non riconosce l'utente come

utente autorizzato, redirige l'utente verso una pagina web della seconda Organizzazione per l'accreditamento.

A questo punto, l'utente fornisce alla seconda Organizzazione, attraverso la suddetta pagina web, ulteriori credenziali necessarie ad identificarlo presso la seconda Organizzazione, così che quest'ultima possa verificare l'identità dell'utente ed autorizzarlo a navigare in Internet.

Questa soluzione offre diversi vantaggi.

In primo luogo, l'utente è identificabile dalla prima Organizzazione mediante le credenziali fornite in fase di richiesta di accesso ad Internet e quindi questo semplifica l'identificazione dell'utente in caso di sicurezza pubblica o per esigenze di fatturazione; ciò nonostante, la prima Organizzazione non possiede tutte le credenziali dell'utente, il che rende la soluzione piuttosto robusta ad attacchi di sniffing.

In secondo luogo la soluzione è facilmente scalabile, in quanto nuove Organizzazioni possono essere aggiunte alla federazione semplicemente aggiungendo un sistema informatico (in particolare un nodo di rete ed un server) in grado di svolgere le funzioni del metodo secondo l'invenzione.

Vantaggiosamente, le credenziali che l'utente fornisce alla prima Organizzazione sono fornite attraverso una pagina web di benvenuto e contengono uno *username* nel formato *nome@realm*, in cui il *realm* rappresenta il nome a dominio della seconda Organizzazione.

In base al *realm* introdotto ogni gateway è in grado di individuare il server di autenticazione dell'Organizzazione di appartenenza dell'utente, vuoi tramite una richiesta al DNS, vuoi tramite confronto con una lista memorizzata a livello di singolo gateway, contenente un elenco dei server

di autenticazione delle Organizzazioni appartenenti alla federazione.

Vantaggiosamente, per garantire l'autenticazione delle comunicazioni tra i gateway e i server di autenticazione di Organizzazioni diverse, i messaggi di segnalazione sono firmati e preferibilmente cifrati utilizzando un algoritmo di crittografia asimmetrica, come quello utilizzato da PGP® (Pretty Good Privacy), che utilizza chiavi pubbliche e chiavi private.

Vantaggiosamente, per semplificare la gestione dello scambio delle chiavi in caso di aggiunta (o di rimozione di nuove Organizzazioni), è stato introdotto nell'architettura un server per la gestione delle chiavi.

Ogni volta che viene aggiunta una nuova Organizzazione, la chiave pubblica del suo server di autenticazione viene pubblicata su questo server; i gateway delle varie Organizzazioni, periodicamente, lo contattano attraverso un protocollo di comunicazione sicura (ad es. via HTTPS) per aggiornare il proprio elenco delle chiavi.

Il mantenere un elenco di chiavi a livello di gateway, fa si che un eventuale malfunzionamento del server di gestione delle chiavi non comprometta il servizio, ma, nel caso peggiore, ritardi di alcune ore l'inserimento di un nuovo server di autenticazione nel sistema.

Il server per la gestione delle chiavi è autenticato da tutti i gateway delle varie Organizzazioni attraverso la sua chiave pubblica, presente sugli stessi, e non permette ad esterni di inserire la propria Organizzazione in modo non autorizzato.

Ulteriori scopi e vantaggi della presente invenzione appariranno maggiormente chiari dalla descrizione che segue e dai disegni annessi, forniti a puro titolo esemplificativo e non limitativo in cui:

- la fig. 1 mostra una federazione di Organizzazioni che permettono l'accesso ad Internet ad utenti di una qualsiasi delle Organizzazioni;

- la fig. 2 mostra schematicamente la procedura che permetta ad un utente di una prima Organizzazione, di accedere ad Internet attraverso un punto di accesso di una seconda Organizzazione;

Con riferimento alla figura 1 viene mostrata una federazione di Organizzazioni (E1, E2, E3) collegate alla rete Internet 1.

Ai fini della presente descrizione, con Organizzazione si vuole indicare un qualsiasi soggetto in grado di permettere ad un utente un accesso ad Internet, oppure che gestisca un sistema strutturato di gestione degli utenti

Nell'esempio di figura 1, le Organizzazioni E1 ed E2 sono provviste di un sistema informatico, in particolare di un nodo di rete, comprendente un gateway GW, un server di autenticazione AS ed una base di dati DB contenente informazioni necessarie per autenticare gli utenti dell'Organizzazione.

Il gateway GW svolge tutte le funzioni di firewall e di filtro del traffico non autorizzato, mentre il server di autenticazione AS verifica le credenziali utente su una base dati DB (database MySQL, LDAP o file di password) o tramite protocollo standard quale ad esempio RADIUS.

Nell'esempio di figura 1, l'Organizzazione E2 è dotato di un access point 3 attraverso il quale offre un accesso wireless agli utenti.

L'Organizzazione E1 è dotata di uno switch 4, collegato al gateway GW, per permettere un accesso via cavo agli utenti.

L' Organizzazione E3 è invece un Internet Service Provider ISP sprovvisto di una propria rete di accesso, ma dotato di propri utenti.

Questa Organizzazione è dotata di un server di autenticazione AS e di un database DB come nel caso delle Organizzazioni E1 ed E2; il server di autenticazione AS è collegato ad internet attraverso un router RT che, a differenza del gateway GW delle organizzazioni E1 ed E2, non è in grado di svolgere le funzioni di reindirizzamento degli utenti che verranno di seguito descritte.

Chiaramente il router RT può essere sostituito da un gateway GW, anche se alcune funzioni non sarebbero utilizzate.

Sempre con riferimento all'esempio qui di seguito descritto con riferimento alle figure 1 e 2, l'utente 2 è un utente autorizzato (ossia appartiene al dominio) dell'Organizzazione E1 ed effettua una richiesta web all'Organizzazione E2 presso la quale non è autenticato.

Questa situazione potrebbe ad esempio verificarsi quando un utente dell'Organizzazione E1 (ad esempio un dipendente dell'azienda ALFA), si trova all'aeroporto o in prossimità di un'altra Organizzazione (ad esempio l'azienda BETA) e desidera accedere ad Internet utilizzando le infrastrutture dell'aeroporto o dell'azienda BETA.

Quando l'utente 2 verifica la presenza di un Hot Spot dell'Organizzazione E2, effettua una richiesta DHCP in seguito alla quale gli viene assegnato un indirizzo IP.

A questo punto l'utente 2 può inoltrare una richiesta di accesso ad Internet.

Il gateway GW intercetta la richiesta e re-dirige il client ad una pagina di benvenuto su cui l'utente inserisce una parte delle credenziali necessarie per autenticarsi presso l'Organizzazione E1.

Secondo l'invenzione, le credenziali fornite all'Organizzazione E2 contengono almeno una informazione relativa all' Organizzazione presso la quale l'utente desidera essere autenticato, nell'esempio qui descritto l'Organizzazione E1.

Preferibilmente queste credenziali sono costituite dal nome utente dell'utente 2 e dal nome a dominio dell'Organizzazione E1 che deve autenticare l'utente 2.

Nome utente e nome a dominio possono essere inseriti in campi separati o essere ricavati automaticamente dal gateway nel caso i cui all'utente 2 sia richiesto di inserire un account nel formato *nome@realm*, in cui 'nome' è il nome utente dell'utente 2 e *realm* rappresenta il nome a dominio dell'Organizzazione E1.

Utilizzando le credenziali fornite dall'utente, l'Organizzazione E2 è quindi in grado di mettersi in contatto con l'Organizzazione E1 per fare autenticare l'utente 2.

L'indirizzo IP del server di autenticazione dell'Organizzazione E1 viene determinato attraverso una gerarchia di regole qui di seguito riportate.

In prima istanza, il *gateway* GW dell'Organizzazione E2 antepone al *realm* un nome scelto a priori (ad esempio: `authserv`) ed effettua una richiesta al DNS per conoscere l'indirizzo IP del server di autenticazione AS di origine dell'utente (ossia dell'Organizzazione 1).

Ad esempio, per l'utente `mario.rossi@organizzazione1.it`, il gateway GW cercherà sul DNS l'IP di `authserv.organizzazione1.it`.

Il nome che viene anteposto al *realm* è scelto uguale per tutti i server di

autenticazione delle organizzazioni che fanno parte di una stessa federazione, in modo da permettere una formulazione semplice della query che il gateway deve inoltrare al DNS.

In caso di risposta positiva da parte del DNS, il gateway GW redirigerà l'utente 2 al server di autenticazione dell'Organizzazione E2; se tale ricerca non da esito positivo, si passa alla regola successiva.

Quest'ultima prevede di ricercare l'indirizzo IP del server di autenticazione AS dell'Organizzazione E1 in una base di dati locale dell'Organizzazione E2.

Secondo l'invenzione, i gateway GW delle diverse Organizzazioni dispongono ognuno di una lista di domini e degli indirizzi IP dei corrispettivi server di autenticazione, in una base dati locale.

Tale lista viene aggiornata con cadenza periodica da un server centrale predefinito, preferibilmente comune a tutte le Organizzazioni federate.

Se anche la ricerca in tale base dati non desse esito positivo, il *gateway* che ha ricevuto la richiesta web passa all'ultima regola, la quale prevede di redirigere l'utente ad un server di autenticazione di default, configurato in fase di installazione del gateway.

Quest'ultima regola sostanzialmente permette di riconoscere, quale informazione relativa ad un'Organizzazione prefissata, l'assenza di informazioni indicate esplicitamente dall'utente in fase di richiesta di accesso ad Internet.

In altre parole, se l'utente 2 fornisce come uniche credenziali al gateway GW il proprio nome senza indicazione del dominio dell'Organizzazione 1 presso cui autenticarsi, allora il gateway interpreta

questa informazione come la volontà di autenticarsi presso un'Organizzazione di default.

Individuato il server di autenticazione, il gateway redirige il client sul server di autenticazione e l'utente per autenticarsi inserisce la propria *password*, ricadendo in una fase di autenticazione di tipo standard, come ad esempio prevista dai sistemi di tipo 'Captive Portal' come il sistema NoCat.

Se la verifica di username e password va a buon fine, il server di autenticazione trasmette al client dell'utente 2 un messaggio di autorizzazione che viene rediretto al gateway GW.

Quest'ultimo inserisce le necessarie regole di firewall in modo da fornire i servizi previsti dal profilo dell'utente, redirigendo quest'ultimo sulla pagina web inizialmente richiesta.

La procedura qui sopra descritta è esemplificata in figura 2, dove sono riportate le comunicazioni tra il client dell'utente 2, il gateway dell'Organizzazione E2, il server di autenticazione dell'Organizzazione E1 e la base di dati dell'Organizzazione E1 ove sono riposte le identità degli utenti autorizzati presso l'Organizzazione E1.

Con riferimento alla figura 2:

- il client invia una richiesta web, ad es. http://www.google.it (sequenza c1),
- il gateway intercetta la richiesta e redirige il client su un portale di autenticazione (sequenza c2),
- il client invia le proprie credenziali, ad esempio lo *username* (sequenza c3),
- il gateway redirige il client sul portale del server di

autenticazione (sequenza c4),

- l'utente inserisce la *password* (sequenza c5),
- il server di autenticazione verifica le credenziali dell'utente (*username* e *password*) confrontandole con quelle contenute in una base di dati, ad esempio tramite protocollo RADIUS (sequenza c6),
- l'utente viene autorizzato (sequenza c7),
- il server di autenticazione invia al client un messaggio di apertura del firewall e conferma di avvenuta autenticazione (sequenza c8),
- il client inoltra il messaggio ricevuto al gateway per l'apertura del firewall (sequenza c9),
- il gateway redirige il client sul sito richiesto http://www.google.it (sequenza c10).
- Il client accede ad Internet al sito richiesto http://www.google.it (sequenza c11).

Questo tipo di architettura permette una scalabilità assoluta del sistema.

Per estendere il sistema, infatti, è sufficiente installare un gateway GW presso la nuova Organizzazione EX e registrare il server di autenticazione, che gestirà gli utenti appartenenti al nuovo dominio (es. organizzazioneX.it), sul DNS; per quanto detto sopra, la registrazione nel DNS deve essere effettuata nel formato precedentemente descritto, ad esempio authserv.organizzazioneX.it.

Vantaggiosamente, per evitare che un sistema si sostituisca ad un server di autenticazione, cercando di autenticare utenti non registrati, la comunicazione tra il server di autenticazione ed il gateway viene firmata, in

particolare la comunicazione viene firmata e preferibilmente cifrata utilizzando una crittografia asimmetrica del tipo a chiave pubblica/chiave privata.

Preferibilmente, nel caso in cui i messaggi siano solamente firmati, il messaggio viene lasciato in chiaro, ma viene allegato un hash calcolato con la chiave privata, che verificato con quella pubblica, garantisce che il messaggio è quello originale creato dal possessore della chiave privata

I messaggi così scambiati vengono quindi firmati e preferibilmente cifrati tramite una chiave (privata nel caso di firma, e pubblica nel caso di cifratura), ottenuta ad esempio mediante il software PGP.

Ogni gateway GW possiede l'elenco delle chiavi pubbliche dei server di autenticazione AS delle Organizzazioni federate, in modo da poter verificare che non ci sia un falso authentication server che tenti di effettuare lo *sniffing* delle autenticazioni.

Affinché il sistema rimanga aggiornato senza limitarne la scalabilità, si utilizza un server di gestione delle chiavi (indicato con KS in figura 1) su cui è presente un *repository* delle chiavi (ad esempio PGP) pubbliche appartenenti ai server di autenticazione riconosciuti dal sistema.

L'aggiunta di una nuova Organizzazione comporta quindi l'inserimento in questa lista della chiave del server di autenticazione AS che gestisce il nuovo dominio.

Ogni gateway possiede una copia dell'elenco delle chiavi e, per fare in modo che il sistema rimanga aggiornato, il metodo secondo l'invenzione prevede che i gateway, periodicamente, consultino il server di gestione delle chiavi KS prelevando l'elenco delle chiavi.

Quando viene aggiunto al sistema un nuovo server di autenticazione, si avrà quindi un primo periodo di transitorio, in cui gli utenti della nuova Organizzazione non potranno utilizzare le proprie credenziali in roaming preso gli altri domini del sistema; tale periodo durerà fino a quando non avverrà l'aggiornamento delle copie locali delle chiavi in tutti i gateway.

Tale disservizio è quindi limitato e legato solo all'installazione di nuove Organizzazioni, non al mantenimento della rete.

Poiché ogni gateway possiede copia dell'elenco delle chiavi pubbliche dei server di autenticazione di tutte le Organizzazioni, in caso di un malfunzionamento o guasto del server di gestione delle chiavi KS, il sistema continua a funzionare.

Il sistema così concepito permette di gestire la fatturazione del traffico effettuato dagli utenti delle diverse Organizzazioni poiché ogni gateway attraverso cui avviene l'accesso ad Internet possiede e deve mantenere all'interno di appositi log le informazioni sugli orari di collegamento di ciascun utente; tale informazione contiene sia il nome dell'utente sia l'Organizzazione di appartenenza e permette la corretta fatturazione del traffico.

Il meccanismo così descritto presuppone delle politiche di fiducia tra le Organizzazioni; nel caso sia necessario un meccanismo di controllo, è preferibile l'introduzione di un server centrale che riceva da tutti le informazioni sui collegamenti degli utenti in modo da verificare quelle memorizzate in ciascun gateway.

E' chiaro che l'esempio di realizzazione sopra descritto deve intendersi in modo non limitativo dell'invenzione e che molte varianti possono essere

apportate al sistema senza per questo fuoriuscire dall'ambito di protezione dell'invenzione quale risulta dalle rivendicazioni allegate.

Ad esempio il gateway, il server di autenticazione e la base di dati per l'autenticazione (es. la base di dati SQL), possono essere implementate da una stessa macchina, o essere distribuiti su un numero maggiore di macchine.

Ancora, i metodi di cifratura delle comunicazioni tra server di autenticazione e gateway o tra server di autenticazione e client possono essere di qualsiasi tipo noto.

* * * * * * * * *

RIVENDICAZIONI

1. Metodo per permettere ad un utente di accedere ad Internet,

in cui un utente effettua una richiesta di accesso ad Internet attraverso un gateway di una prima Organizzazione, detta richiesta prevedendo che detto utente fornisca a detta prima Organizzazione delle prime credenziali di autenticazione presso una seconda Organizzazione, dette credenziali contenendo almeno una informazione relativa a detta seconda Organizzazione, ed

in cui detta prima Organizzazione contatta detta seconda Organizzazione al fine di autenticare detto utente e permettergli l'accesso ad Internet, ed

in cui detta seconda Organizzazione rilascia a detto utente l'autorizzazione ad accedere ad Internet,

caratterizzato dal fatto che a seguito di detta richiesta di accesso detto gateway redirige detto utente verso una pagina web di detta seconda Organizzazione, e dal fatto che detto utente fornisce a detta seconda Organizzazione, attraverso detta pagina web, seconde credenziali di autenticazione necessarie ad identificare detto utente presso detta seconda Organizzazione.

2. Metodo secondo la rivendicazione 1, in cui dette prime credenziali di autenticazione comprendono un nome utente espresso nel formato nome@realm, dove 'nome' identifica l'utente e realm identifica detta seconda Organizzazione.

3. Metodo secondo la rivendicazione 1 o 2, in cui dette seconde credenziali comprendono una password.

4. Metodo secondo una qualsiasi delle rivendicazioni precedenti, in cui detta richiesta di accesso ad Internet comprende una prima fase di assegnazione di un indirizzo IP a detto utente ed una seconda fase in cui detto gateway indirizza detto utente verso una pagina web locale di benvenuto dove detto utente inserisce dette prime credenziali.

5. Metodo secondo una qualsiasi delle rivendicazioni da 1 a 4, in cui se detto gateway non è in grado individuare un server di autenticazione di detta seconda Organizzazione, allora detto gateway trasmette dette prime credenziali ad un server di autenticazione di default.

6. Metodo secondo una qualsiasi delle rivendicazioni da 1 a 4, in cui detto gateway trasmette dette prime credenziali ad un server di autenticazione di detta seconda Organizzazione.

7. Metodo secondo la rivendicazione 6, in cui detto gateway determina l'indirizzo di detto server di autenticazione mediante una query ad un DNS.

8. Metodo secondo la rivendicazione 6 o 7, in cui detto gateway accede ad una lista di Organizzazioni e determina l'indirizzo di detto server di autenticazione mediante confronto tra detta lista e dette prime credenziali.

9. Metodo secondo una qualsiasi delle rivendicazioni da 5 a 8, in cui la comunicazione tra detto gateway e detto server di autenticazione è firmata.

10. Metodo secondo una qualsiasi delle rivendicazioni da 5 a 9, in cui la comunicazione tra detto gateway e detto server di autenticazione è cifrata.

11. Metodo secondo la rivendicazione 10, in cui la comunicazione tra detto gateway e detto server di autenticazione è cifrata mediante codifica a chiave pubblica/chiave privata.

12. Metodo secondo la rivendicazione 11, in cui un server di gestione delle chiavi mantiene un elenco delle chiavi pubbliche di una pluralità di server di autenticazione di una corrispondente pluralità di Organizzazioni.

13. Metodo secondo la rivendicazione 12, in cui i gateway di detta pluralità di Organizzazioni si connettono periodicamente a detto server di gestione delle chiavi e memorizzano a livello locale detto elenco delle chiavi pubbliche.

14. Sistema informatico atto ad implementare il metodo secondo una qualsiasi delle rivendicazioni da 1 a 13.

15. Programma per elaboratore atto ad essere memorizzato entro aree di memoria di detto elaboratore e contenente porzioni di codice atte a eseguire il metodo secondo una qualsiasi delle rivendicazioni da 1 a 13 quando eseguite da detto elaboratore.

* * * * * *

CSP – Innovazione nelle ICT Scarl

p.i. Ing. Marco Camolese

(No Iscr. Albo 882BM)

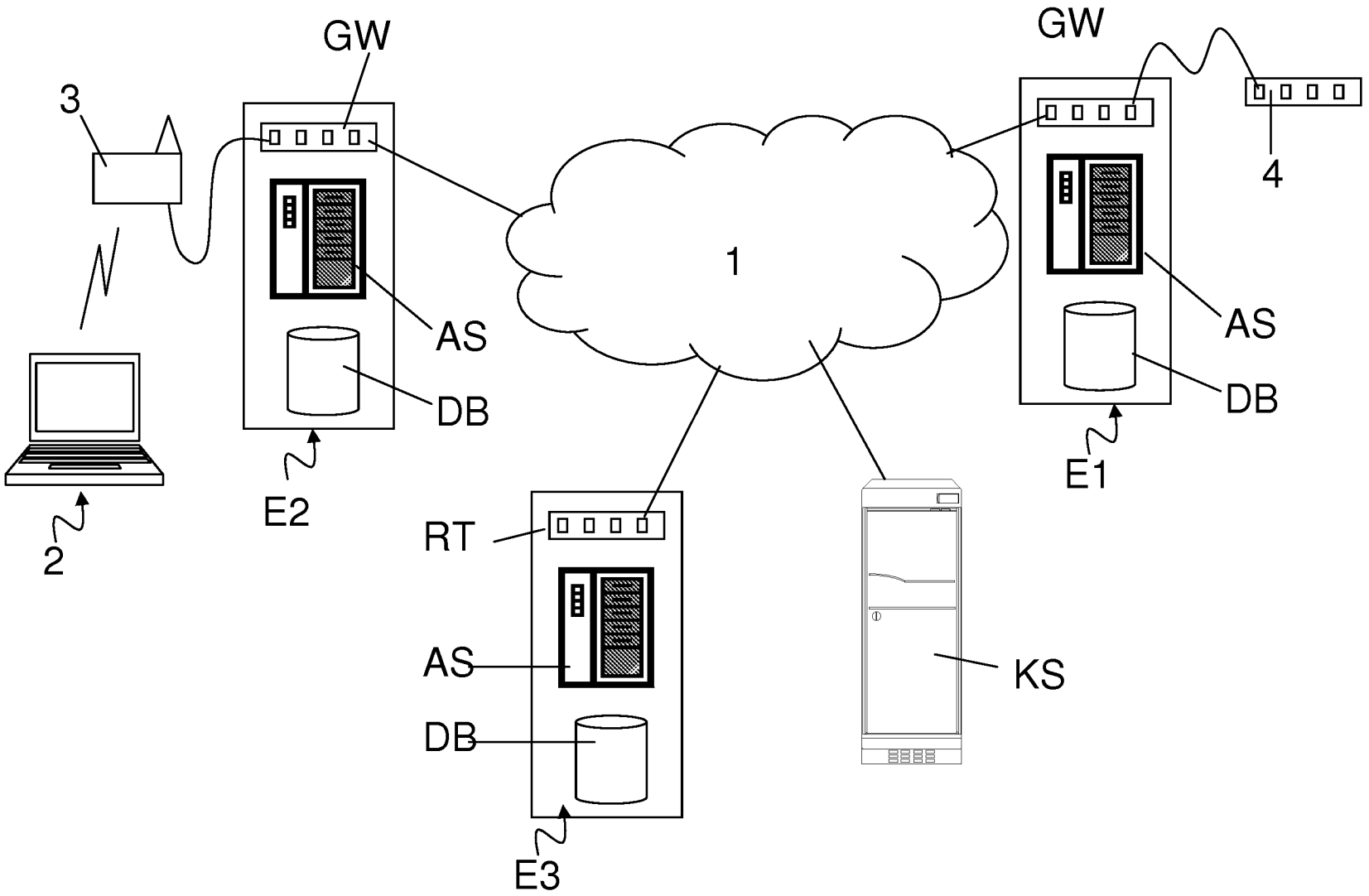

Fig. 1

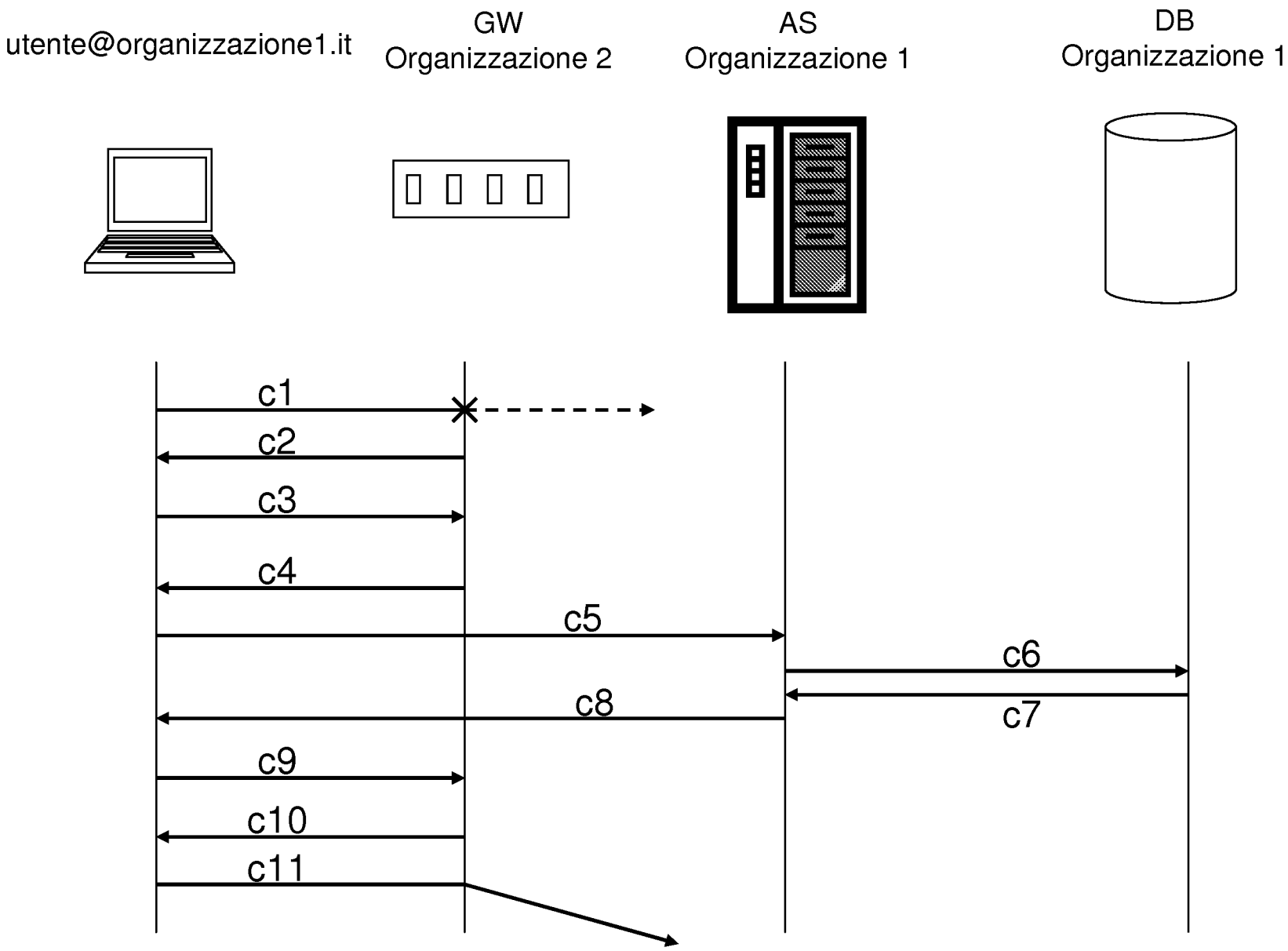
utente@organizzazione1.it
GW
Organizzazione 2
AS
Organizzazione 1
DB
Organizzazione 1
c1
c2
c3
c4
c5
c6
c7
c8
c9
c10
c11

Fig. 2