MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA TUTELA DELLA PROPRIETA' INDUSTRIALE
UFFICIO ITALIANO BREVETTI E MARCHI

UIBM

DOMANDA NUMERO	102009901707308
Data Deposito	25/02/2009
Data Pubblicazione	25/08/2010

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F		

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	07	C		

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	07	F		

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	07	B		

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F		

Titolo

SISTEMA DI CONTROLLO PER LA GESTIONE DEGLI ACCESSI AD AREE RISERVATE

DESCRIZIONE dell'invenzione industriale dal titolo:
"Sistema di controllo per la gestione degli accessi ad aree riservate"
di: Giuseppe Asselle, nazionalità italiana, Via Don Orione 162, 12042 Bra (CN),
Inventori designati: Giuseppe ASSELLE.
Depositata il: 25 febbraio 2009

* * *

TESTO DELLA DESCRIZIONE

Campo dell'invenzione

La presente descrizione si riferisce alle tecniche di gestione degli accessi e più in particolare ad un sistema di controllo degli accessi ad aree riservate.

Descrizione della tecnica relativa

La presenza di un sistema di controllo degli accessi è richiesta in quelle situazioni nelle quali si vuole dare ad alcuni utenti, in base a certe regole, ad esempio dietro pagamento di un corrispettivo, il permesso di accedere ad una o più aree o strutture riservate.

Alcune possibili applicazioni sono qui di seguito indicate soltanto a titolo d'esempio non limitativo:

- accesso a strutture di intrattenimento (cinema, musei, parchi divertimento) in un comprensorio turistico,
- accesso agli impianti di risalita in un comprensorio sciistico,
- accesso a strutture sportive (piscine, palestre, saune),
- accesso alle camere di un albergo, e

- accesso ad ambienti virtuali (aree web riservate).

Esistono nella tecnica diverse soluzioni che permettono di gestire l'accesso ad aree riservate e condivise.

Un primo esempio è rappresentato dalla tipica biglietteria in cui un cliente acquista un biglietto d'ingresso che viene controllato e "validato" in modo che non possa essere riutilizzato, ad esempio strappandone una parte o imprimendovi sopra una data, all'ingresso della struttura di intrattenimento selezionata.

Una diversa soluzione è rappresentata dall'acquisto di un abbonamento che dà diritto all'accesso a diverse strutture di intrattenimento (ad esempio l'abbonamento musei di una città). In questo caso il cliente acquista un carnet di biglietti e poi in un secondo momento decide dove utilizzare questi biglietti all'interno di una gamma di strutture di intrattenimento disponibili. In questo caso il cliente paga l'abbonamento e l'importo viene distribuito in modo equo tra tutte le strutture aderenti, ma in questo modo le strutture che vengono visitate frequentemente sono penalizzate.

Scopo e sintesi dell'invenzione

Lo scopo della presente invenzione è quello di realizzare un sistema di controllo per la gestione degli accessi ad aree riservate che risulti semplice da realizzare, economico, e che garantisca allo stesso tempo la possibilità di avere un riconoscimento univoco dei singoli accessi ad ogni struttura di intrattenimento che fa parte del comprensorio gestito dal sistema di controllo.

Il sistema di controllo secondo la presente invenzione

garantisce al tempo stesso una elevata sicurezza, efficienza, funzionalità e versatilità.

In vista di raggiungere tale scopo l'invenzione ha per oggetto un sistema di controllo per la gestione degli accessi ad aree riservate avente le caratteristiche indicate nella rivendicazione 1, nonché un corrispondente procedimento.

Le rivendicazioni formano parte integrante dell'insegnamento relativo all'invenzione qui fornito.

Breve descrizione delle viste annesse

L'invenzione sarà ora descritta, a puro titolo di esempio non limitativo, con riferimento alle figure annesse, in cui:

- la figura 1 mostra un esempio di scenario di applicazione del sistema di controllo secondo la presente invenzione,
- la figura 2 mostra una porzione di una matrice dei simboli,
- la figura 3 mostra un esempio di codici di sicurezza,
- la figura 4 mostra le relazioni tra gli archivi del sistema di controllo,
- la figura 5 è un diagramma di flusso dei passi per la preparazione di un diritto d'accesso,
- la figura 6 è un diagramma di flusso dei passi relativi alla richiesta di accesso all'area riservata, e
- la figura 7 è un diagramma di flusso dei passi relativi ad una procedura di chiusura di una transazione.

Descrizione particolareggiata di forme di attuazione

Il sistema di controllo degli accessi secondo l'invenzione permette di gestire l'accesso alle aree riservate distribuendo dei permessi di accesso e verificando la validità di questi permessi al varco dell'area riservata.

Il sistema di controllo inoltre è configurato per generare diversi tipi di diritti di accesso che possono avere una validità temporale variabile (singolo accesso, accesso per un periodo di tempo limitato, accesso a tempo indeterminato).

La descrizione seguente è relativa al caso di accesso ad un'area fisica, ma è anche applicabile agli ambienti virtuali.

Per meglio comprendere la descrizione che segue, vengono preliminarmente fornite alcune definizioni di moduli o di entità che fanno parte del sistema di controllo accessi e che sono illustrati nelle figure 1, 2 e 3.

Un modulo gestore comprende, ad esempio, un'unità di elaborazione centrale 50 che si occupa dell'emissione e del controllo dei diritti di accesso 20.

Un utente 60 è ad esempio un soggetto utilizzatore di aree riservate 75 a cui il gestore 50 assegna un diritto di accesso 20.

Un modulo erogatore comprende, ad esempio, un'unità di elaborazione locale 70 posta all'ingresso di un'area riservata 75; l'erogatore è configurato per eseguire una verifica del diritto di accesso 20 per autorizzare l'accesso dell'utente 60, e per ricevere e trasmettere informazioni al gestore 50.

All'arrivo di un nuovo utente 60, il modulo gestore 50 come prima cosa assegna un codice identificativo, o codice

utente, che permette di identificare in modo univoco l'utente 60.

Quando l'utente 60 richiede un permesso per accedere ad un'area riservata 75, l'unità di elaborazione centrale 50, dopo aver verificato la possibilità di concedere il permesso, genera una transazione. Alla transazione viene assegnato un identificativo che la distingue in modo univoco rispetto alle altre transazioni e che la collega all'utente 60.

Il sistema di controllo comprende una serie di archivi in cui memorizza le informazioni relative agli utenti 60, agli erogatori 70 e alle transazioni.

Il sistema di controllo secondo l'invenzione comprende il modulo gestore 50 configurato per l'emissione e il controllo dei diritti di accesso 20 associati alle transazioni, e uno o più moduli erogatori 70, in cui ciascun modulo erogatore 70 è posto all'ingresso di un'area riservata 75 ed è configurato per eseguire una verifica del diritto di accesso 20. Il sistema di controllo è configurato per la gestione degli accessi degli utilizzatori 60 ad una pluralità di aree riservate 75 tramite l'impiego dei diritti d'accesso 20 emessi dal modulo gestore 50.

Inoltre, il modulo gestore 50 è configurato per eseguire una fase di abilitazione del diritto di accesso 20 associato alla transazione, trasmettendo informazioni sulla transazione agli erogatori 70.

Ciascun erogatore 70 è configurato per verificare la validità del diritto d'accesso presentato dall'utilizzatore 60, e autorizzare in base all'esito della verifica l'accesso alla corrispondente area riservata 75. Inoltre, ciascun erogatore 70 è configurato per notificare al

gestore 50, in un istante di tempo selezionabile, l'avvenuto accesso dell'utente 60 alla corrispondente area riservata 75.

Infine, il gestore 50 esegue, dietro ricezione della specifica notifica inviata dallo specifico erogatore 70, una successiva fase di chiusura della transazione. Per "specifica notifica" si intende una comunicazione all'interno della quale vi sono elementi che permettono di individuare in modo univoco l'erogatore 70 che genera e trasmette la notifica. In questo modo, si ottiene un riconoscimento univoco del singolo accesso alla singola area riservata 75 e il gestore 50 è in grado di contabilizzare dell'accesso assegnando all'erogatore 70 identificato dalla specifica notifica il corrispettivo associato alla transazione.

Scendendo maggiormente nei dettagli, in seguito alla creazione di una transazione, il gestore 50 genera una matrice dei simboli 10 che servirà per la generazione di un diritto d'accesso 20 e invia, nella fase di abilitazione, la matrice dei simboli 10 con il relativo codice identificativo della transazione a tutti gli erogatori 70. La matrice 10 viene inoltre memorizzata in un archivio presente sul gestore 50. Ogni transazione è abbinata ad una diversa matrice dei simboli 10, ed ogni matrice è diversa dalle altre matrici.

Un diritto d'accesso 20 è un codice o una chiave logica che permette all'utente 60 di farsi riconoscere in modo univoco e sicuro dall'erogatore 70 ed entrare nell'area riservata 75. Il diritto d'accesso 20 viene generato dal gestore 50, e una prima parte di esso, indicata con il riferimento 30, insieme all'identificativo della transazione vengono memorizzate su un dispositivo 65

(una carta magnetica riconfigurabile, un tag RFID, un badge, o un biglietto di ingresso) che viene poi consegnato all'utente 60.

Al fine di aumentare la sicurezza delle transazioni, i diritti d'accesso 20 vengono trasmessi in modo asimmetrico (ovvero vengono trasmesse informazioni diverse e complementari) al soggetto utilizzatore o utente 60 e agli erogatori 70. In particolare all'utente 60 viene trasmessa la prima porzione 30, mentre agli erogatori 70 viene trasmessa la seconda porzione 40 del diritto d'accesso 20 insieme all'intera matrice dei simboli 10.

Trasmettere agli erogatori 70 le informazioni sulla transazione dà a questi la possibilità di eseguire in modo autonomo ed indipendente una verifica della chiave 30 presentata dell'utente 60 anche in assenza del collegamento on-line con il gestore 50. In questo modo l'erogatore 70 autorizza l'accesso dell'utente 60 e contemporaneamente o in un momento successivo notifica al gestore 50 l'accesso alla corrispondente area riservata 75.

Su ogni varco posto all'ingresso di un'area riservata 75 è quindi presente un erogatore 70 che, per mezzo di un lettore 72, controlla la validità della porzione 30 del diritto d'accesso 20 fornita dall'utente 60.

Ad ogni transazione vengono assegnati codici diversi, ossia ogni transazione è univocamente distinguibile dalle altre perché ha una diversa matrice dei simboli 10 e un diverso diritto d'accesso 20 che sono generati appositamente per quella particolare transazione.

Questa variabilità consente di ottenere l'accessibilità attraverso controlli basati su codici che cambiano di volta in volta e di utente in utente ottenendo così un'elevata flessibilità. Questo inoltre garantisce una

maggiore sicurezza rispetto ai sistemi che eseguono controlli basati su codici permanenti impostati nell'erogatore presente sul varco.

Ogni utente 60 può utilizzare come identificativo un proprio dispositivo 65 (tag di identificazione, dispositivo RFID, badge, chiave USB, palmare, cellulare bluetooth) sul quale il gestore 50 carica l'identificativo della transazione e le informazioni contenute nella prima porzione 30 del diritto d'accesso 20. Queste informazioni sono necessarie al riconoscimento dell'utente 60 e della transazione. In alternativa, il gestore 50 può fornire all'utente 60 un dispositivo 65 su cui ha precedentemente caricato le medesime informazioni. Nel secondo caso, all'uscita dell'area riservata l'utente 60 restituisce il dispositivo 65 al gestore 50 il quale lo può riconfigurare e riutilizzare per altri utenti.

Al singolo utente 60 è consentito richiedere uno o più diritti di accesso 20 da utilizzare, a sua libera scelta, nelle aree o strutture controllate dal sistema di controllo accessi.

Più nel dettaglio, il diritto d'accesso 20 è un codice che viene generato scegliendo in modo arbitrario un certo numero di elementi o caselle a partire dalla matrice dei simboli 10 abbinata a quella particolare transazione. Inoltre, il diritto d'accesso 20 è un codice composto da tre campi, indicati con i riferimenti 22, 23 e 24. I campi 22, 23 e 24 contengono rispettivamente le coordinate della colonna, le coordinate della riga, e il contenuto delle caselle selezionate a partire dalla matrice dei simboli 10.

Il gestore 50 genera anche una coppia di chiavi 30, 40 suddividendo le informazioni presenti nel diritto d'accesso 20 e consegna le chiavi all'utente 60 e agli erogatori 70.

In particolare all'utente 60 viene fornita la prima chiave 30 (anche detta codice di sblocco) che comprende i campi 22 e 23 che contengono le coordinate delle caselle della matrice dei simboli 10 che compongono il diritto d'accesso 20. Invece, agli erogatori 70 viene fornita la seconda chiave 40 (detta codice random) che comprende il campo 24 in cui sono memorizzati i contenuti delle corrispondenti caselle che compongono il diritto d'accesso 20.

Il set di chiavi utilizzate dal sistema di controllo degli accessi si divide quindi in due parti. Una parte è assegnata agli erogatori 70 ed è costituita dalla matrice dei simboli 10 e dalla seconda chiave 40 (codice random), e l'altra parte è assegnata all'utente 60 ed è costituita dalla prima chiave 30 (codice di sblocco). Naturalmente, si possono invertire gli abbinamenti tra i soggetti e le chiavi, ed in particolare si può decidere di assegnare la chiave 40 all'utente e la chiave 30 (sempre insieme alla matrice dei simboli 10) agli erogatori 70. Quindi sia l'utente 60 che gli erogatori 70 non sono in possesso del diritto d'accesso 20 completo, ma ne hanno soltanto una rispettiva porzione. In questo modo la sicurezza aumenta notevolmente in quanto per ottenere l'accesso ci deve essere una corretta ricombinazione delle informazioni.

Ogni erogatore 70 dispone della seconda chiave 40 da abbinare alla prima chiave 30 presentata da un utente 60 ed inoltre dispone della matrice dei simboli 10. In particolare, partendo dalla prima chiave 30 (codice di sblocco) fornita dall'utente 60 e che contiene le coordinate delle caselle, lo specifico erogatore 70 legge i contenuti delle caselle della matrice dei simboli 10 indirizzate dalle coordinate e confronta tali contenuti con

la seconda chiave 40 (codice random) a sua disposizione.

L'erogatore 70 è quindi in grado di verificare in modo autonomo e indipendente l'autenticità del diritto d'accesso ricostruito, senza la necessità di avere un'interazione con l'unità di elaborazione centrale del gestore 50.

Se il confronto dà esito positivo l'erogatore autorizza l'ingresso dell'utente 60 nell'area riservata 75. In un momento successivo, o contestualmente all'ingresso dell'utente 60, l'erogatore 70 è nella condizione di poter notificare al gestore 50 l'avvenuta transazione.

Il gestore 50 riceve dall'erogatore 70, assieme alla specifica notifica dell'avvenuta transazione, anche la coppia di chiavi logiche 30 e 40 e può quindi verificare l'autenticità del diritto di accesso ricostruito. Se anche questa seconda verifica dà esito positivo, il gestore 50 procede a registrare l'accesso dell'utente 60 e ad attivare le conseguenti azioni (ad esempio accredito del corrispettivo del diritto di accesso; contabilizzazioni; monitoraggi statistici; giro fondi) tra cui anche la chiusura della transazione.

Nella complessa struttura considerata, si identificano principalmente due esigenze. Da un lato si ha la necessità di gestire in modo comune l'assegnazione dei diritti di accesso 20, dall'altro si deve accertare in quale area riservata 75 il singolo diritto di accesso 20 è stato utilizzato dall'utente 60.

L'interesse di ogni erogatore 70 è quello di vedersi riconoscere l'accesso effettuato dall'utente 60, mentre l'interesse del gestore 50 è quello di monitorare che l'accesso segnalato da ogni singolo erogatore 70 corrisponda ad un diritto di accesso 20 autentico.

Infine, l'interesse dell'utente 60 è quello di

disporre di un diritto di accesso 20 che gli permetta di accedere all'area riservata 75 cui intende accedere.

Per poter soddisfare tutti questi interessi il sistema di controllo, basandosi sulla generazione di codici incrociati, genera un set di chiavi logiche 20, 30 e 40 grazie alle quali:

- l'utente 60 può accedere all'area riservata 75 solo se fornisce una chiave logica 30 valida;

- l'erogatore 70 può verificare l'autenticità della chiave 30 dell'utente 60 abbinandola con la chiave logica 40 e accertandosi che nella matrice dei simboli 10 il contenuto delle caselle sia identico al contenuto delle corrispondenti caselle che formano il diritto d'accesso ricostruito abbinando la chiave 30 con la chiave 40; e

- l'erogatore 70 non può notificare al gestore 50 un accesso senza fornire l'esatto abbinamento delle due chiavi, la sua chiave 40 e quella dell'utente 30.

Il gestore 50 comprende un'unità di elaborazione munita di software firmware dedicato:

- alla generazione della matrice dei simboli 10,

- alla generazione del set di chiavi 20, 30, 40;

- all'abbinamento delle chiavi 30, 40 con gli identificativi del singolo diritto di accesso 20 (aggiornamento degli archivi);

- alla comunicazione con l'utente 60 e con gli erogatori 70;

- al controllo delle specifiche notifiche di accesso inviate dagli erogatori 70; e

- all'attivazione di procedure collegate per la contabilizzazione dell'accesso.

Ciascun erogatore 70 comprende un'unità di elaborazione in grado di:

- comunicare con il gestore 50 e con l'utente 60 o con il dispositivo 65;

- memorizzare la matrice dei simboli 10,

- memorizzare le chiavi 30, 40; e

- verificare l'autenticità di una chiave 30 abbinandola alla chiave 40 e confrontando il risultato dell'abbinamento con la matrice 10.

L'utente 60 viene dotato del supporto fisico/logico 65 in grado di ricevere dall'unità di elaborazione centrale 50 e trasmettere allo specifico erogatore 70 la chiave logica 30.

Nel caso in cui la chiave 30 destinata all'utente 60 venga trasmessa sotto forma di messaggio wireless (sms, bluetooth) su un apparato mobile (telefono cellulare o palmare) gli erogatori 70 saranno muniti di interfaccia di comunicazione compatibile con gli stessi. Viceversa se la chiave 30 viene fornita all'utente 60 sotto forma di TAG RFID agli erogatori 70 saranno associati lettori *(transceiver)* dotati di un'antenna. Esistono inoltre altre possibili varianti che prevedono di fornire all'utente 60 la chiave 30 su supporto cartaceo come codice in chiaro (tipo PIN) o codice a barre; in questo caso gli erogatori 70 saranno muniti di tastiera accessibile all'utente 60 o di lettore di codici a barre.

In base al livello di inviolabilità che si intende garantire al sistema il gestore 50:

- sceglie la dimensione della matrice dei simboli 10 variando di conseguenza il numero di simboli presenti nella matrice stessa, e

- sceglie la complessità del set di chiavi 20, 30, e 40 andando ad agire sulla dimensione dei codici utilizzati.

Infatti, aumentando la dimensione della matrice dei

simboli 10 e/o l'ampiezza del diritto d'accesso 20 (e di conseguenza della prima chiave 30 e della seconda chiave 40) diminuisce la probabilità di successo di un tentativo di violazione del sistema.

Nel seguito viene descritta, con riferimento alle figure 2 e 3, una forma di realizzazione scelta tra le possibili impostazioni e i possibili livelli di sicurezza adottabili. Si sottolinea il fatto che la matrice può essere costruita con ogni tipo di carattere, numero o simbolo.

La figura 2 mostra una porzione della matrice dei simboli 10 che risulta troppo estesa per essere completamente illustrata in una singola figura.

La matrice 10 dei simboli qui descritta a scopo puramente illustrativo ha le seguenti caratteristiche:

- è una matrice quadrata (numero delle colonne uguale al numero delle righe, e pari a 52),

- il contenuto di ogni casella è una lettera dell'alfabeto (distinguendo tra carattere minuscolo e maiuscolo), e

- il numero complessivo delle caselle è dato dal numero delle colonne moltiplicato per il numero delle righe, (ovvero è 52 * 52 = 2704).

Le colonne vengono indicizzate nel seguente modo: la prima colonna è identificata con la lettera maiuscola "A"; le colonne seguenti sono indicizzate ognuna con le lettere maiuscole dell'alfabeto sino alla "Z" (26a colonna); a seguire l'indice della 27a colonna è la lettera minuscola "a", e le altre colonne sono indicizzate ognuna con le seguenti lettere minuscole dell'alfabeto sino alla "z" (52a colonna).

Le righe vengono invece indicizzate con un indice

numerico che va da 1 a 52.

Vengono ora indicati i passi seguiti per la creazione della matrice dei simboli 10:

- ognuna delle 52 lettere (maiuscole e minuscole) che rappresenta l'indice delle colonne viene assegnata, con modalità casuale, a 52 caselle sparse nella tabella, e
- si ripete tale assegnazione per ciascuna delle restanti lettere (ad ogni lettera vengono quindi assegnate 52 caselle della matrice) andando man mano ad esaurire tutte le caselle della matrice.

La figura 3 mostra un esempio di generazione delle chiavi 30 e 40 a partire da un diritto d'accesso 20 generato a partire dalla matrice della figura 2.

Il gestore 50, dopo aver creato la matrice dei simboli 10 (vedere figura 2), seleziona con modalità casuale una pluralità di caselle, nell'esempio di figura 2 seleziona in particolare 12 caselle che formano il diritto di accesso 20.

Il gestore 50 genera la prima chiave 30, detta anche codice di sblocco, e la assegna all'utente 60. Il codice di sblocco è costituito dai campi 22 e 23 del diritto di accesso 20 e contiene le coordinate delle caselle selezionate.

Il gestore 50 genera anche la seconda chiave 40, detta anche codice random, che comprende il campo 24 del diritto di accesso 20 e contiene i contenuti delle caselle selezionate. Il gestore 50 assegna la chiave 40 agli erogatori 70, assieme alla matrice dei simboli 10.

La probabilità che estranei riescano ad indovinare il diritto di accesso 20 dipende dalla dimensione della matrice dei simboli 10 e dal numero di caselle che compongono il diritto di accesso 20 (e di conseguenza anche

il codice random 40 e il codice di sblocco 30).

Nel caso illustrato nella figura 3 sono state scelte con modalità arbitraria 12 caselle all'interno della matrice 10 di figura 2. Le 12 caselle vanno a formare il codice o diritto di accesso 20. Il numero di codici di accesso 20 ottenibili scegliendo 12 caselle in modo casuale è dato dalle combinazioni di 12 caselle a partire dal numero di elementi della matrice che in questo caso è di 2704.

Un così elevato numero di possibili combinazioni rende sostanzialmente impossibile indovinare il diritto di accesso 20 anche conoscendo la matrice dei simboli 10 o una delle due chiavi 30 o 40.

Si considera ora il caso in cui il tentativo di indovinare uno dei codici sia effettuato da uno dei soggetti che utilizza il sistema di accesso.

Al fine di creare una tutela reciproca si pone una soglia minima di caselle (ad esempio 7 su 12) che devono essere corrispondenti a quelle del codice originale affinché il diritto d'accesso ricostruito sia ritenuto valido dal gestore 50. Questo serve per creare un livello di difficoltà equilibrato tra utente e erogatore nella possibilità di violazione del sistema.

Infatti, gli utilizzatori del sistema di accesso sono l'utente 60 e gli erogatori 70 che, al fine di concludere una transazione, garantendosi l'uno la prestazione dell'altro, si impegnano a scambiarsi i codici nel momento della richiesta di transito dell'utente 60 attraverso il varco dello specifico erogatore 70. La prestazione dello specifico erogatore 70 (consenso all'ingresso dell'utente 60 nella propria area riservata 75) avviene solo dopo che l'utente 60 comunica all'erogatore 70 la prima chiave 30 o

codice di sblocco; solo così l'erogatore 70 in questione può verificare, utilizzando la matrice dei simboli 10 e la chiave 40 di cui dispone, l'autenticità del codice di sblocco 30 e avere la garanzia che la prestazione dell'utente 60 venga a lui corrisposta dal gestore 50 (pagamento del corrispettivo; registrazione dell'accesso, contabilizzazione, monitoraggio statistico).

Si consideri ora il caso in cui un erogatore 70 cerchi di indovinare il codice di sblocco 30 (assegnato all'utente 60 dal gestore 50) per ricomporre il diritto di accesso 20 ed ottenere così una prestazione a suo favore, senza tuttavia aver ricevuto alcuna richiesta di accesso dall'utente 60.

In questo caso l'erogatore 70 dispone della matrice dei simboli 10 e conosce, grazie al codice random 40, il contenuto delle 12 caselle del diritto di accesso 20 ma non ne conosce le coordinate all'interno della matrice dei simboli 10. Le possibili combinazioni delle coordinate delle 12 caselle corrispondono alle combinazioni di 12 elementi a partire da 52 simboli (infatti ciascun elemento della matrice 10 è ripetuto, in questo esempio illustrato, esattamente 52 volte).

Qualora, ad esempio, delle 12 caselle sia sufficiente indovinarne 7, in questo caso le possibili combinazioni corrispondono a:

52*52*52*52*52*52*52 = 1.028.071.702.528

Anche in questo caso un così elevato numero di possibili combinazioni rende sostanzialmente impossibile indovinare il diritto di accesso 20 da parte dell'erogatore 70, pur in presenza di una soglia minima di elementi che devono essere corrispondenti di 7 su 12.

Si consideri ora il caso in cui l'utente 60 voglia

cercare di variare il proprio codice di sblocco 30 senza indicarlo all'erogatore 70, per far sì che con il codice di sblocco 30 variato l'erogatore 70 non riesca ad ottenere dal gestore 50 la prestazione a suo favore. In questo caso, quindi, l'utente 60 cerca di comunicare all'erogatore 70, nel momento della richiesta di accesso, un codice errato ma che superi il controllo che l'erogatore 70 fa confrontando il codice di sblocco 30 fornito dall'utente 60 con il codice random 40 e la matrice dei simboli 10 a sua disposizione.

Per riuscire in questo l'utente 60 deve fornire all'erogatore 70 un codice di sblocco contraffatto che, con una o più coordinate diverse rispetto al codice di sblocco autentico 30, riporti comunque le coordinate di caselle della matrice 10 dei simboli che hanno lo stesso contenuto delle caselle indicizzate dal codice di sblocco autentico 30.

Se così non fosse l'erogatore 70 si accorgerebbe della non autenticità del codice di sblocco contraffatto e non autorizzerebbe l'accesso dell'utente 60.

Le probabilità che l'utente 60 riesca a sostituire una coordinata del codice di sblocco 30 con un'altra coordinata che contenga la stessa lettera sono pari a 51/2703. Infatti, all'interno della matrice dei simboli 10, vi sono altre 51 caselle con lo stesso contenuto di una certa coordinata; complessivamente la matrice dei simboli 10 contiene 2704 caselle, escludendo quella interessata ne rimangono 2703. Si tratta all'incirca di due possibilità su cento che l'utente 60 riesca a modificare il codice di sblocco 30 senza farsi scoprire dall'erogatore 70.

Rispetto alle situazioni precedenti si tratta, quindi, di una possibilità concreta di violazione; ma solo nel caso

in cui sia previsto che il gestore 50 consideri autentico il diritto di accesso ricostruito se questo è fornito esatto dall'erogatore 70 per tutte e 12 le caselle che lo compongono.

Se, come già in precedenza, il diritto di accesso 20 è ritenuto autentico anche solo con 7 caselle esatte delle 12 complessive, quindi, per impedire l'autenticazione del diritto di accesso 20 all'erogatore 70, all'utente serve contraffare con successo almeno 6 coordinate.

Per rendere nullo il diritto di accesso l'utente deve riuscire a variare 6 caselle e in questo caso l'erogatore notifica meno di 7 caselle giuste al gestore.

In questo caso la probabilità che l'utente 60 riesca, senza essere scoperto, a contraffare 6 caselle del codice di sblocco 30 corrisponde a:

(51/2703)* (51/2703)* (51/2703)* (51/2703)* (51/2703)* (51/2703) = 0,00000000004

ossia a circa 4 possibilità su 100.000.000.000.

In conclusione al fine di rendere sostanzialmente impossibile violare e/o contraffare i codici su cui si basa il sistema di controllo una delle impostazioni più efficaci è quella non solo di adottare una matrice dei simboli 10 sufficientemente ampia, ma prevedere anche un diritto di accesso 20 con un numero di caselle complessivo superiore al numero di caselle dello stesso richieste per l'autenticazione. Solo così si rende sostanzialmente impossibile per l'utente 60 quanto per l'erogatore 70 violare il sistema.

Viene ora descritta l'interazione del gestore 50 con gli erogatori 70.

- prima fase di abilitazione: assegnazione dei diritti di accesso 20; gli erogatori 70 sono in contatto con il

gestore 50 dal quale ricevono progressivamente o al quale possono richiedere direttamente i dati relativi ai diritti di accesso 20 assegnati agli utenti 60; i dati che ciascun erogatore 70 può conoscere sono l'identificativo della singola transazione, l'identificativo del singolo diritto di accesso 20, la relativa matrice dei simboli 10 e la relativa seconda chiave o codice random 40;

- seconda fase: richiesta di accesso; quando l'utente 60 raggiunge uno specifico erogatore 70 si fa riconoscere comunicando la prima chiave o codice di sblocco 30 (generato e trasmessogli dal gestore 50); verificata l'autenticità del codice di sblocco 30, grazie all'abbinamento con la seconda chiave o codice random 40 e al confronto con la matrice dei simboli 10, l'erogatore 70 autorizza l'ingresso dell'utente 60 nella propria area riservata 75;

- terza fase: notifica di accesso; autorizzato l'accesso all'utente 60 lo specifico erogatore 70 notifica al gestore 50 il diritto di accesso ricostruito (abbinamento del codice di sblocco 30 e del codice random 40);

- quarta fase: chiusura della transazione; ricevuto e verificato il diritto di accesso ricostruito il gestore 50 registra l'avvenuto accesso ed esegue le azioni previste (accredito del corrispettivo del diritto di accesso; contabilizzazioni; monitoraggi statistici; giro fondi; ecc).

L'interazione dell'utente 60 con lo specifico erogatore 70 prevede una fase di identificazione dell'utente; giunto all'erogatore 70 l'utente 60 accede all'area riservata 75 della struttura facendosi riconoscere al varco dell'area stessa; il riconoscimento avviene

comunicando al lettore dei diritti 72 dello specifico erogatore 70 il codice di sblocco 30, che identifica l'utente 60 in modo univoco ed identifica in modo univoco anche lo specifico diritto di accesso 20. L'erogatore 70, dopo aver identificato l'utente 60, autorizza l'accesso alla corrispondente area 75.

Con riferimento alla figura 4 vengono descritti gli archivi presenti nel sistema di controllo.

L'archivio generale 92 ha memorizzati al suo interno i codici identificativi degli utilizzatori del sistema, ovvero degli utenti e degli erogatori.

Esiste poi un archivio 80 dei codici degli erogatori in cui per ogni erogatore 70 vengono memorizzate in un record le relative informazioni (codice erogatore, campo anagrafica e campo ubicazione).

All'arrivo di un utente 60 viene creato un nuovo record nell'archivio 82 dei codici utenti. Nel record vengono memorizzate le informazioni codice utente, campo anagrafica, e campo indirizzo.

L'archivio 84 dei diritti d'accesso comprende record formati da un campo numero diritto d'accesso, un campo data, un campo corrispettivo e un campo codice utente. Il campo " utente" permette di mettere in relazione l'archivio 84 dei diritti d'accesso e l'archivio 82 dei codici utenti.

Per ogni transazione viene aggiunto un nuovo record all'archivio 86 degli identificativi delle transazioni. Ciascun record comprende un campo numero transazione, un campo numero diritto d'accesso, e un campo data. Anche in questo caso il campo "numero diritto d'accesso" mette in relazione l'archivio 84 con l'archivio 86.

L'archivio 88 delle matrici dei simboli prevede un record per ogni nuova matrice generata. Il record contiene

un campo numero matrice, un campo numero transazione, e un campo che contiene la matrice vera e propria. Il campo "numero transazione" mette in relazione l'archivio 88 delle matrici dei simboli con l'archivio 86 degli identificativi delle transazioni.

Infine l'archivio 90 dei codici di accesso contiene un record per ogni diritto d'accesso emesso dal gestore 50. in questo caso si ha un campo numero matrice, un campo codice random e un campo codice di sblocco.

Con riferimento alla figura 5 viene ora descritto un diagramma di flusso dei passi per la preparazione del diritto d'accesso 20.

In un passo 100 il gestore 50 elabora un ordine di assegnazione di un diritto d'accesso 20. Nel successivo passo 102 avviene l'identificazione dell'utente, e nel passo 104 avviene l'assegnazione di un identificativo al diritto d'accesso. Ad esempio un identificativo del diritto d'accesso può contenere le seguenti informazioni: codice utente, data, numero progressivo.

In un passo 106 avviene quindi la preparazione dei codici del sistema di controllo e nel passo 108 avviene l'assegnazione di un identificativo ad una transazione. Ad esempio un identificativo di una transazione può contenere il codice utente e il numero progressivo.

Nel passo 110 avviene la generazione della matrice dei simboli 10 e dei relativi diritti di accesso 20, codice di sblocco 30 e codice random 40.

In seguito, nel passo 112 viene eseguito l'abbinamento tra:

- identificativo del diritto d'accesso (primo campo dell'archivio 84),
- identificativo della transazione (primo campo

dell'archivio 86),

- matrice dei simboli 10,
- diritto di accesso 20,
- codice di sblocco 30, e
- codice random 40.

Infine, in un passo 114 avviene la trasmissione degli identificativi e dei codici all'erogatore 70 e all'utente 60. In particolare l'erogatore 70 riceve:

- l'identificativo del diritto d'accesso,
- l'identificativo della transazione,
- la matrice dei simboli 10, e
- il codice random 40.

L'utente invece riceve

- l'identificativo del diritto d'accesso,
- l'identificativo della transazione, e
- il codice di sblocco 30.

Con riferimento alla figura 6 viene ora descritto il diagramma di flusso dei passi relativi alla richiesta di accesso all'area riservata.

In un passo 120 l'utente 60 si presenta ad uno degli erogatori 70, e nel passo 122 l'utente 60 comunica all'erogatore 70 l'identificativo del diritto d'accesso, l'identificativo della transazione, e il codice di sblocco 30.

In seguito, nel passo 124 l'erogatore 70 recupera dalla memoria locale o dall'archivio centrale 92 i dati della specifica matrice dei simboli 10.

Nel successivo passo 126 l'erogatore 70 abbina il codice di sblocco 30 al codice ramdom 40 e ottiene il diritto di accesso ricostruito. Inoltre, in un passo 128 l'erogatore 70 verifica se le caselle del diritto di accesso 20 così ricomposto corrispondono nel contenuto alle

caselle della matrice dei simboli 10. Nel passo 130 si controlla se c'è corrispondenza tra le caselle: in caso negativo in un passo 132 l'erogatore 70 rifiuta l'accesso, in caso positivo in un passo 134 l'erogatore autorizza l'accesso dell'utente e trasmette al gestore 50 in un passo 136 le seguenti informazioni:

- identificativo del diritto d'accesso,
- identificativo della transazione,
- codice di accesso 20, e
- notifica dell'accesso.

Con riferimento alla figura 7 viene ora descritta la procedura di chiusura della transazione ad opera del gestore 50.

In un passo 140 il gestore 50 riceve dall'erogatore 70 i dati dell'accesso (quelli inviati nel passo 136) e il gestore 50 verifica che il diritto di accesso trasmesso dall'erogatore 70 corrisponda (rispettando la soglia minima prestabilita) al diritto d'accesso 20 originario; il gestore 50 in un passo 142 registra l'accesso. Infine, nel seguente passo 144 il gestore 50 attua le altre eventuali azioni (pagamenti, accrediti, monitoraggi statistici).

Il sistema di controllo secondo la presente invenzione può essere utilizzato anche per la gestione degli accessi ad aree logiche o virtuali, ad esempio l'accesso tramite identificativo (nome utente) e chiave di accesso (password) in un sito web per la distribuzione di contenuti multimediali, documenti, autorizzazioni o certificazioni.

Naturalmente, i particolari di realizzazione e le forme di attuazione potranno essere ampiamente variati rispetto a quanto descritto ed illustrato senza per questo uscire dall'ambito di protezione della presente invenzione, così come definito dalle rivendicazioni annesse.

RIVENDICAZIONI

1. Sistema di controllo per la gestione degli accessi di utilizzatori (60) ad una pluralità di aree riservate (75) tramite l'impiego di diritti d'accesso (20) comprendente:

- almeno un modulo gestore, comprendente un'unità di elaborazione centrale (50), configurata per l'emissione e il controllo di un diritto di accesso (20) associato ad una transazione, e

- uno o più moduli erogatori, comprendenti ciascuno un'unità di elaborazione locale (70), in cui ciascun modulo erogatore è posto all'ingresso di un'area riservata (75) ed è configurato per eseguire una verifica del diritto di accesso (20),

caratterizzato dal fatto che

- detto modulo gestore (50) è configurato per eseguire una fase di abilitazione del diritto di accesso (20) associato alla transazione trasmettendo informazioni (10, 40) su detta transazione alle unità di elaborazione locali (70),

- il modulo erogatore (70) è configurato per verificare la validità del diritto d'accesso (30) presentato dall'utilizzatore (60), e autorizzare in base all'esito di detta verifica l'accesso alla corrispondente area riservata (75), inviando una notifica specifica del modulo erogatore (70) al modulo gestore (50) in un istante di tempo selezionabile per notificare l'avvenuto accesso, e

- detto modulo gestore (50) è inoltre configurato per eseguire, dietro ricezione di detta specifica notifica una fase di controllo di dati della transazione e una successiva fase di chiusura della transazione per ottenere un riconoscimento univoco del singolo accesso alla singola

area riservata (75).

2. Sistema di controllo per la gestione degli accessi ad aree riservate (75) secondo la rivendicazione 1, caratterizzato dal fatto che detto modulo gestore (50) è configurato per emettere diritti d'accesso (20) con una validità temporale variabile.

3. Sistema di controllo per la gestione degli accessi ad aree riservate (75) secondo una qualsiasi delle precedenti rivendicazioni, caratterizzato dal fatto che detto modulo gestore (50) comprende mezzi di memorizzazione per memorizzare archivi (80, 82, 84, 86, 88, 90, 92) in cui sono contenute informazioni relative a:

- utilizzatori (60),
- erogatori (70)
- diritti d'accesso (20), e
- transazioni.

4. Sistema di controllo per la gestione degli accessi ad aree riservate (75) secondo una qualsiasi delle precedenti rivendicazioni, caratterizzato dal fatto che detta unità di elaborazione centrale (50) del modulo gestore è configurata per:

- generare una matrice dei simboli (10) utilizzata per la creazione del diritto d'accesso (20),
- generare una coppia di chiavi d'accesso (30, 40) a partire dal diritto d'accesso (20) suddividendo le informazioni in esso contenute (22, 23, 24), e
- assegnare una prima chiave (30) all'utilizzatore (60), e
- trasmettere, durante la suddetta fase di abilitazione, la matrice dei simboli (10) e una seconda chiave (40) ai moduli erogatori (70).

5. Sistema di controllo per la gestione degli accessi

ad aree riservate (75) secondo la rivendicazione 4, caratterizzato dal fatto che detta unità di elaborazione locale (70) del modulo erogatore è configurata per:

- ricostruire il diritto d'accesso (30, 40) tramite la prima chiave (30) fornita dall'utilizzatore (60) e la seconda chiave (40) a sua disposizione,

- confrontare le informazioni del diritto d'accesso (30, 40) ricostruito con la matrice dei simboli (10),

- verificare in modo autonomo, ovvero anche in assenza di collegamento on-line con il gestore (50), l'autenticità del diritto d'accesso ricostruito (30, 40),

- se il confronto ha dato esito positivo autorizzare l'accesso dell'utilizzatore (60), e

- notificare all'unità di elaborazione centrale (50) l'accesso dell'utilizzatore (60) alla corrispondente area riservata (75).

6. Sistema di controllo per la gestione degli accessi ad aree riservate (75) secondo la rivendicazione 5, caratterizzato dal fatto che la suddetta unità di elaborazione centrale (50) è inoltre configurata per:

- ricevere dal modulo erogatore (70) la specifica notifica dell'accesso e il relativo diritto d'accesso ricostruito (30, 40),

- accertare, nella fase di controllo, l'autenticità del diritto d'accesso ricostruito (30, 40) confrontandolo con il diritto d'accesso (20) originario, e

- in caso di esito positivo eseguire la suddetta fase di chiusura che prevede la contabilizzazione dell'accesso assegnando al modulo erogatore (70) il corrispettivo associato alla transazione.

7. Sistema di controllo per la gestione degli accessi ad aree riservate (75) secondo una qualsiasi delle

rivendicazioni 4 a 6, caratterizzato dal fatto che detto modulo gestore (50) è configurato per fornire ad ogni utilizzatore (60) un dispositivo (65) su cui ha precedentemente memorizzato:

- l'identificativo dell'utilizzatore (60),
- l'identificativo della transazione, e
- la prima chiave (30).

8. Sistema di controllo per la gestione degli accessi ad aree riservate (75) secondo la rivendicazione 7, caratterizzato dal fatto che ciascun modulo erogatore (70) comprende un lettore (72) per controllare la validità delle informazioni (30) fornite dal dispositivo (65) dell'utilizzatore (60).

9. Sistema di controllo per la gestione degli accessi ad aree riservate (75) secondo la rivendicazione 8, caratterizzato dal fatto che detto modulo gestore (50) è configurato per generare il diritto d'accesso (20) scegliendo in modo arbitrario un certo numero di caselle a partire dalla matrice dei simboli (10) associata alla suddetta transazione.

10. Sistema di controllo per la gestione degli accessi ad aree riservate (75) secondo la rivendicazione 9, caratterizzato dal fatto che detto modulo gestore (50) è configurato per generare il diritto d'accesso (20) utilizzando tre campi (22, 23 e 24) che contengono rispettivamente le coordinate della colonna (22), le coordinate della riga (23), e il contenuto (24) delle caselle selezionate a partire dalla suddetta matrice dei simboli (10).

11. Sistema di controllo per la gestione degli accessi ad aree riservate (75) secondo la rivendicazione 10, caratterizzato dal fatto che detto modulo gestore (50) è

configurato per generare la prima chiave (30) selezionando i primi due campi (22, 23) del diritto d'accesso (20) e la seconda chiave (40) selezionando il terzo campo (24) del diritto d'accesso (20).

12. Sistema di controllo per la gestione degli accessi ad aree riservate (75) secondo la rivendicazione 11, caratterizzato dal fatto che il livello di inviolabilità definito dal modulo gestore (50) dipende:

- dalla dimensione della matrice dei simboli (10), e
- dalla complessità o dimensione del set di chiavi (20, 30, 40).

13. Sistema di controllo per la gestione degli accessi ad aree riservate (75) secondo la rivendicazione 12, caratterizzato dal fatto che al fine di creare una tutela reciproca tra l'utilizzatore (60) e l'erogatore (70), detto modulo gestore (50) crea un livello di difficoltà equilibrato nella possibilità di violazione del sistema ponendo una soglia minima sul numero di caselle che nel diritto d'accesso ricostruito (30, 40) devono trovare corrispondenza con quelle del diritto d'accesso originario (20) affinché il diritto d'accesso ricostruito (30, 40) sia ritenuto valido.

14. Sistema di controllo per la gestione degli accessi ad aree riservate (75) secondo una qualsiasi delle rivendicazioni 4 a 13, caratterizzato dal fatto che la matrice dei simboli (10) ha le seguenti caratteristiche:

- è una matrice quadrata di ordine N,
- il contenuto di ogni casella è un carattere, un numero o un simbolo,
- le righe e le colonne vengono indicizzate con un ordine prestabilito dei caratteri, numeri o simboli adottati,

- ognuno dei caratteri, numeri o simboli adottati per gli indici delle colonne e/o delle righe viene assegnato, con modalità casuale, ad un numero N di caselle sparse nella matrice dei simboli (10).

15. Procedimento di controllo per la gestione degli accessi di utilizzatori (60) ad una pluralità di aree riservate (75) caratterizzato dal fatto di comprendere le operazioni implementate dal sistema secondo una o più delle rivendicazioni 1 a 14.