Title

A call management system

Technical Field

The invention concerns a call management system for accessing a call bridging service to make a call.

Background of the Invention

Call back services are available to users from anywhere in the world. A touch tone (DTMF) phone and a call back account on a phone network are required. The mechanism of a call back involves the user calling a pre-allocated telephone number (often referred to as a DDI number), and then receiving a call back call on their registered call back number. Once the user receives the call back call, they pick up the phone and are able to make an outbound call. Call back is suitable for locations where there are no available direct access numbers to a particular country for direct calling, or where charges applied are excessive.

Phone calls are made using a call back service with a touchtone phone or mobile phone by contacting the call back service either through the Internet or by dialing a special "trigger" number and hanging up after one ring. Within seconds, a call is received from the system (the "call back"). After answering this call, instructions to dial the destination number are provided. When the call is finished, the user hangs up or presses # on the keypad to place another call.

Call back works on any line that can receive an incoming call. Many mobile phone providers do not charge airtime for calls received, and thus in addition to saving on long distance charges, airtime charges are also eliminated since call back service calls are perceived by the telecommunications operator as incoming only calls.

Call back services can also be used with a fax machine by picking up the handset and calling the trigger number and hanging up. When it calls back, the user picks up the handset, dials the destination number and then presses the send button once to hear the fax tone.

However, with call back services, there are numerous issues. Some of the issues are related to accounting problems as the owner of the DDI number may refuse to pay for the call. In addition, call back services are typically not legal in countries that have a monopoly on the telecommunications industry.

Summary of the Invention

In a first preferred aspect, there is provided a call management system for accessing a call bridging service, the system comprising:

a private signing key to validate the identity of a user;

a token provided to the validated user for accessing the service, the token being associated with predetermined conditions; and

a service module to initiate the service by connecting a call bridging call to the user with an outbound call to a predetermined destination;

wherein the use of the private signing key represents non-repudiated access of the service by the user.

The system may further comprise a token management system to manage the allocation and revocation of tokens to validated users.

The system may further comprise a web server to receive a public signing key from the user via the Internet.

The system may further comprise an application server to execute the service module.

The system may further comprise a database to store user details of the users.

The system may further comprise directory services to store contact details of the users.

The predetermined conditions may be call duration limitation, calling number restriction or calling country restriction.

The private signing key may be part of a PKI key pair or issued by a trusted party.

The private signing key may be stored in a USB storage device of the user. The USB storage device may be a keychain storage device, for example, a USB memory key.

In a second aspect, there is provided a method for accessing a call bridging service, the method comprising:

validating the identity of a user using a private signing key;

providing the validated user with a token to access the service, the token being associated with predetermined conditions; and

initiating the service by connecting a call bridging call to the user with an outbound call to a predetermined destination;

wherein the use of the private signing key represents non-repudiated access of the service by the user.

In a third aspect, there is provided a software client for accessing a call bridging service, the client comprising:

a validation module to receive a private signing key to validate the identity of a user;

a token receiver to receive a token provided to the validated user for accessing the service, the token being associated with predetermined conditions; and

a client service module to collect the phone number of the user for a call bridging call and the phone number of a predetermined destination for an outbound call;

wherein the use of the private signing key represents non-repudiated access of the service by the user.

In a fourth aspect, there is provided a call bridge server for accessing a call bridging service, the server comprising:

a token generator to provide a token to a validated user for accessing the service, the token being associated with predetermined conditions, and the identity of the user being validated by a private signing key; and

a service module to initiate the service by connecting a call bridging call to the user with an outbound call to a predetermined destination;

wherein the use of the private signing key represents non-repudiated access of the service by the user.

Brief Description of the Drawings

An example of the invention will now be described with reference to the accompanying drawings, in which:

Figure 1 is a system architecture diagram of the call management system;
Figure 2 is a block diagram at the client end of the call management system;
Figure 3 is a block diagram at the server end of the call management system;
Figure 4 is a first roadmap diagram for users of the call management system;
Figure 5 is a second roadmap diagram for users of the call management system;
Figure 6 is a diagram of a data message communicated in the call management system; and
Figure 7 is an activity diagram of communication between the client and server in the call management system.

Detailed Description of the Drawings

The drawings and the following discussion are intended to provide a brief, general description of a suitable computing environment in which the present invention may be implemented. Although not required, the invention will be described in the general context of computer-executable instructions, such as program modules, being executed by a personal computer. Generally, program modules include routines, programs, characters, components, data structures, that perform particular tasks or implement particular abstract data types. As those skilled in the art will appreciate, the invention may be practiced with other computer system configurations, including hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

Referring to the drawings, there is provided a call management system 10 for accessing a call bridging service 20. The system 10 is a client 11/server 12 system. The system 10 comprises: a private signing key that is part of a PKI key pair or is issued by a trusted party. The private signing key validates the identity of a user. Preferably, the private signing key is stored in a USB memory key 13. Public-key infrastructure (PKI) is the combination of software, encryption technologies, and services that protects the security of communication between the client 11 and the server 12 over the Internet. PKI integrates digital certificates, public-key cryptography, and certificate authorities into a network security architecture. PKI

encompasses the issuance of digital certificates to individual users and servers; end-user enrollment software; integration with corporate certificate directories; tools for managing, renewing, and revoking certificates; and related services and support. PKI also support non-repudiation. That is, the digital certificates validate the identity of users, and makes it feasibly impossible to later repudiate a digitally "signed" transaction, for example, use of the service 20. The use of the private signing key represents non-repudiated access of the service 20 by the user.

Once the user has been validated, a token (not shown) is allocated to the user for accessing the service 20. The token has predetermined conditions and confers limited rights and certain restrictions on the user using the service 20. For example, the predetermined conditions include call duration limits, calling number restriction or calling country restriction. A service module (not shown) is executed on an application server 17 to initiate the service 20 by connecting a call bridging call to the user with an outbound call to a predetermined destination. Once connected, the call bridging call is handled by a voice gateway 19.

The system 10 further comprises a token management system 14 to manage the allocation and revocation of tokens to validated users. A public signing key of the PKI key pair can be entered by the user via the Internet on a web site 16. User details of the user is retrieved from a database 18. Directory services 15 also store contact details of the user.

The system 10 can provide reporting functions such as retrieving Call Data Records (CDR) 30. Records can be filtered according to each individual user or monthly records may be reviewed. Other back-end services include user management 40, password recovery 50 and client software updates 60.

In a typical scenario, the user executes client software on their computer 11. The user inserts their USB memory key 13 with the private signing key into their computer 11. The software reads the USB memory key 13 to retrieve the private signing key. Validation of the user's identity occurs by communicating the public signing key with the server 12. Once the user is validated, the server 12 responds by associating the user with a token. All subsequent communication from the client 11 requires use of the token, otherwise the service 20 cannot be accessed by the user. The software transmits the phone number of the call bridging call to the user and the phone number of the outbound call to the server 12. Alternatively, the

phone number of the call bridging call does not need to be transmitted if one is already recorded for the user. A call is made, for example, from Singapore, outward to the phone number of the call bridging call to the user. Once the user picks up the call bridging call on their phone, the service 20 is operational. The service 20 terminates once the user hangs up the call.

The client 11 internally maintains a data structure for communicating data messages 70 to the server 12, as graphically depicted in Figure 6. The header portion 71 is used to identify the versioning of the data structure and any relevant information related to the key that is used to protect the data and program. The key 72 is either a symmetric key or private key-public key pair. The data structure of the header 71, code segment 73 and data segment 74 is:

Header	
Magic	A fixed value to identify the Header
Salt	Initialization vector for the encryption algorithm
Encrypted Key	Password-protected key for decrypting data/code
HMAC	Data-integrity check

Code Segment	
Encrypted Executable Code	Executable code of application in encrypted form
HMAC	Data Integrity Check

Data Segment	
Encrypted data	Application data information in encrypted form
HMAC	Data Integrity Check

In other embodiments, there may be more than one data segment.

Referring to Figure 7, when a user initiates 80 a connection to the call management server 12, the client 11 transmits a data message 70. The data message 70 contains data relating to the type of device, key information and the encrypted value of the client random (a random number, for example 64 bits).

This communication protocol requires unique information relating to the hardware device during negotiation between the client 11 and the server 11. This unique information is derived from the type of device the client 11 is installed on. The protocol provides an anti-copying mechanism to hinder unauthorised copying of the client 11 to other devices. If the client 11 is copied to another device, the hardware identity will change. If the server 11 detects that the hardware identity has changed, it will determine that the client 11 is an unauthorised copied and thus will not communicate with the unauthorised client 11.

The type of device may include a mobile phone, client application or token-based solution. The key information may include the public key of the client 11 or other key information that provides sufficient information for encrypting the client random using an E_1 encryption function. The encrypted value of the client random is further protected by a checksum H_1 based on the Keyed-Hashing Message Authentication (HMAC) algorithm. The server 12 receives the key information and attempts to decrypt the client random. The server 12 determines whether the decryption is successful or not based on the HMAC validity check. This check is also proves the authenticity of the client 11.

When the server 12 has successfully validated the client random, it generates its own server random 81, and then encrypts the server random. The encrypted value is also HMAC protected to ensure data integrity. The client 11 validates the encrypted value and if successfully validated, the client 11 generates a session key based on the information from the client random and the server random. The client random and the server random are only known to the client 11 and the server 12. The encryption key is derived from this information. The client 11 encrypts the phone number to call and phone number to callback and transmits 82 this information to the server 12.

Although a call bridging service has been described it is envisaged that a call back service is possible where there is a point of presence in the country of operations of the service provider.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the scope or spirit of the invention as broadly described.

The present embodiments are, therefore, to be considered in all respects illustrative and not restrictive.

WE CLAIM:

1. A call management system for accessing a call bridging service, the system comprising:

a private signing key to validate the identity of a user;

a token provided to the validated user for accessing the service, the token being associated with predetermined conditions; and

a service module to initiate the service by connecting a call bridging call to the user with an outbound call to a predetermined destination;

wherein the use of the private signing key represents non-repudiated access of the service by the user.

2. The system according to claim 1, further comprising a token management system to manage the allocation and revocation of tokens to validated users.

3. The system according to claim 1, further comprising a web server to receive a public signing key from the user via the Internet.

4. The system according to claim 1, further comprising an application server to execute the service module.

5. The system according to claim 1, further comprising a database to store user details of the user.

6. The system according to claim 1, further comprising a directory service to store contact details of the user.

7. The system according to claim 1, wherein the predetermined conditions include call duration limitation, calling number restriction or calling country restriction.

8. The system according to claim 1, wherein the private signing key is part of a PKI key pair or issued by a trusted party.

9. The system according to claim 1, wherein the private signing key is stored in a USB storage device of the user.

10. The system according to claim 9, wherein the USB storage device is a keychain storage device.

11. The system according to claim 10, wherein the keychain storage device is a USB memory key.

12. The system according to claim 4, wherein the system is a client/server system.

13. The system according to claim 12, wherein the client negotiates with the server, where the client transmits data relating to the type of hardware device the client is installed on, key information for encrypting a client random using an encryption function and encrypted value of the client random.

14. The system according to claim 13, wherein the encrypted value of the client random is protected by a checksum based on the Keyed-Hashing Message Authentication (HMAC) algorithm.

15. The system according to claim 14, wherein the server decrypts the client random and authenticates the client by performing a HMAC validity check against the decrypted client random.

16. The system according to claim 15, further comprising an anti-copying mechanism to deny use of the service if the client is copied to an unauthorised hardware device.

17. The system according to claim 16, wherein the unauthorised hardware device is detected by the server by inspecting the transmitted data relating to the type of hardware device by the client.

18. A method for accessing a call bridging service, the method comprising:

validating the identity of a user using a private signing key;

providing the validated user with a token to access the service, the token being associated with predetermined conditions; and

initiating the service by connecting a call bridging call to the user with an outbound call to a predetermined destination;

wherein the use of the private signing key represents non-repudiated access of the service by the user.

19. A software client for accessing a call bridging service, the client comprising:

a validation module to receive a private signing key to validate the identity of a user;

a token receiver to receive a token provided to the validated user for accessing the service, the token being associated with predetermined conditions; and

a client service module to collect the phone number of the user for a call bridging call and the phone number of a predetermined destination for an outbound call;

wherein the use of the private signing key represents non-repudiated access of the service by the user.

20. A call bridge server for accessing a call bridging service, the server comprising:

a token generator to provide a token to a validated user for accessing the service, the token being associated with predetermined conditions, and the identity of the user being validated by a private signing key; and

a service module to initiate the service by connecting a call bridging call to the user with an outbound call to a predetermined destination;

wherein the use of the private signing key represents non-repudiated access of the service by the user.