(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 409 931**

(51) Int. CI.:

H04M 3/533 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.02.2008 E 08709542 (8)**

(97) Fecha y número de publicación de la concesión europea: **06.03.2013 EP 2140672**

(54) Título: **Sistema y método de correo de voz seguro.**

(30) Prioridad:

27.02.2007 GB 0703798

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.06.2013

(73) Titular/es:

CELLCRYPT LIMITED (100.0%)
130 SHAFTSBURY AVENUE
LONDON W1D 5EU, GB

(72) Inventor/es:

POPPE, TOBIAS y
ROSINI, RODOLFO

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema y método de correo de voz seguro.

Campo de la Invención

La presente invención se refiere a un sistema para proporcionar un repositorio de correo de voz seguro y cifrado.

Antecedentes de la Invención

A menudo los sistemas telefónicos de empresa y también los sistemas telefónicos móviles ofrecen prestaciones de correo de voz para permitir la recepción de mensajes cuando un usuario no está disponible o está en otra línea. La mayoría de los sistemas telefónicos pueden ofrecer hoy en día alguna forma de correo de voz. En cada caso, el servicio de correo de voz se alberga normalmente en un sistema informático conectado a la red telefónica a la que se da servicio de manera que puede recibir llamadas a aparatos de teléfono configurados para reenviar llamadas al correo de voz o que no están disponibles y registrar mensajes en un repositorio.

Con el fin de ofrecer flexibilidad a los usuarios, los sistemas de correo de voz actuales permiten que los usuarios llamen al repositorio de correo de voz para recuperar sus mensajes. Los usuarios pueden asignar un número pin a su buzón de correo para limitar el acceso y muchos sistemas tienen un número pin predeterminado si no se asigna uno. Algunos sistemas no solicitarán un número pin si la persona que llama usa el aparato de teléfono asociado con el buzón de correo (a diferencia de cuando se llama desde un número diferente para recuperar sus mensajes).

Cada vez más, la seguridad de datos está convirtiéndose en un problema para todos. El teléfono todavía se considera un método de comunicación más seguro que el correo electrónico, por ejemplo. Como tal, pueden dejarse mensajes confidenciales por correo de voz que no se habrían comunicado necesariamente por correo electrónico.

Sin embargo, poco a poco resulta evidente que la seguridad que rodea a los sistemas de telecomunicaciones no es suficiente. La seguridad con respecto a sistemas de correo electrónico y similares ha aumentado durante los últimos años hasta el punto de que a menudo se requiere una autenticación fuerte para acceder a un buzón de correo electrónico. Sin embargo, los sistemas de correo de voz actuales están protegidos de una manera muy deficiente y los números pin pueden a menudo adivinarse o vulnerarse su protección mediante estrategias de fuerza bruta, permitiendo que cualquiera acceda al buzón de correo de un usuario. Además, podría interceptarse un mensaje de correo de voz durante la recuperación escuchando indiscretamente en la comunicación.

El documento US 6741705 da a conocer un sistema y un método para proteger mensajes de correo de voz. El documento US 5710816 da a conocer un método y un aparato para garantizar la recepción de mensajes de correo de voz.

Exposición de la Invención

Según un aspecto de la presente invención se proporciona un sistema según la reivindicación 1.

Cuando se solicita un mensaje de correo de voz, el mensaje se transmite en su forma cifrada al aparato de teléfono que entonces puede usar la clave privada asociada con el par de claves para descifrar el mensaje y emitirlo al usuario.

No es necesario que el sistema de correo de voz sea el sistema de correo de voz por defecto asignado por el proveedor de telecomunicaciones. El aparato de teléfono del receptor puede configurarse para reenviar llamadas de correo de voz a un proveedor de correo de voz alternativo.

El repositorio puede estar dispuesto para establecer dicho canal de comunicación segura con dicho sistema que realiza la llamada.

El repositorio puede comprender además al menos una clave de cifrado asociada con cada uno de una pluralidad de buzones de correo, estando cada uno de los buzones de correo asociado con un sistema receptor, estando el repositorio dispuesto para identificar el buzón de correo dependiendo del sistema receptor al que se llamó y usar dicha respectiva al menos una clave para el establecimiento de dicho canal de comunicación segura y/o para la comunicación con dicho sistema que realiza la llamada a través de dicho canal de comunicación segura.

El repositorio puede comprender además al menos una clave de cifrado asociada con cada uno de una pluralidad de buzones de correo, estando cada uno de los buzones de correo asociado con un sistema receptor, estando el repositorio dispuesto para identificar el buzón de correo al que se llamó dependiendo del sistema receptor al que se llamó y cifrar llamadas no cifradas en dicha forma cifrada durante o antes del registro usando dicha al menos una clave de cifrado.

La al menos una clave puede comprender una clave pública de un par de claves pública-privada.

El sistema puede comprender además un sistema receptor, incluyendo el sistema receptor la clave privada del par

de claves pública-privada y estando dispuesto para obtener dicha forma cifrada de la llamada desde el repositorio y descifrar la llamada dependiendo de la clave privada.

El repositorio puede estar dispuesto, una vez finalizado el registro de una llamada, para transmitir dicha forma cifrada de dicha llamada al respectivo sistema receptor.

El repositorio puede estar dispuesto para transmitir dicha forma cifrada de dicha llamada al respectivo sistema receptor durante el registro.

El repositorio puede ser remoto con respecto al sistema de gestión de red de cualquier proveedor de telecomunicaciones y está dispuesto para recibir llamadas en nombre de sistemas receptores que operan en diferentes redes de telecomunicaciones.

El sistema puede comprender además una pluralidad de repositorios, estando dispuesto cada uno para recibir llamadas para un sistema receptor y transmitir dichas llamadas registradas en dicha forma cifrada entre los mismos a petición.

Según otro aspecto de la presente invención, se proporciona un método según la reivindicación 11.

El método puede comprender además:

almacenar al menos una clave de cifrado asociada con cada uno de una pluralidad de buzones de correo, estando cada uno de los buzones de correo asociado con un sistema receptor;
identificar el buzón de correo dependiendo del sistema receptor al que se llamó; y,
usar dicha respectiva al menos una clave para el establecimiento de dicho canal de comunicación segura y/o para la comunicación con dicho sistema que realiza la llamada a través de dicho canal de comunicación segura.

El método puede comprender además:

almacenar al menos una clave de cifrado asociada con cada uno de una pluralidad de buzones de correo, estando cada uno de los buzones de correo asociado con un sistema receptor;
identificar el buzón de correo al que se llamó dependiendo del sistema receptor al que se llamó; y, cifrar llamadas no cifradas en dicha forma cifrada durante o antes del registro usando dicha al menos una clave de cifrado.

El método puede comprender además, una vez finalizado el registro de una llamada, transmitir dicha forma cifrada de dicha llamada al sistema receptor.

El método puede comprender además transmitir dicha forma cifrada de dicha llamada al respectivo sistema receptor durante el registro.

Breve descripción de los dibujos

A continuación se describirán ejemplos de la presente invención con referencia a los dibujos adjuntos, en los que:

la figura 1 es un diagrama esquemático de un sistema de correo de voz seguro según un primer aspecto de la presente invención;
la figura 2 es el diagrama esquemático de la figura 1 que ilustra un modo preferido de funcionamiento;
la figura 3 es un diagrama esquemático de un sistema de correo de voz seguro según otro aspecto de la presente invención; y
la figura 4 es una ilustración de una visualización de pantalla según otro aspecto de la presente invención.

Descripción detallada

La figura 1 es un diagrama esquemático de un sistema de correo de voz seguro según una realización de la presente invención.

El sistema 5 de correo de voz seguro forma parte de una red de telefonía móvil. La red de telefonía móvil incluye una estación 40 de conmutación que está conectada a una red 30 telefónica pública conmutada (PSTN). Un repositorio 50 está conectado a través de una red 60 a la estación 40 de conmutación para almacenar mensajes de correo de voz.

Cuando un primer usuario desea comunicarse con un segundo usuario, el primer usuario usa su aparato 10 de teléfono y llama al número de teléfono asociado con el aparato 20 de teléfono del segundo usuario. Esta llamada se encamina a través de la PSTN 30 al centro 40 de conmutación. El centro 40 de conmutación determina si el aparato 20 de teléfono del segundo usuario está dentro del alcance y disponible.

Si el aparato 20 de teléfono del segundo usuario no está dentro del alcance o disponible (por ejemplo si el usuario estuviera en otra llamada o el aparato de teléfono estuviera configurado para reenviar todas las llamadas al correo de voz), el centro 40 de conmutación inicia un proceso de captura de mensaje de correo de voz que indica al usuario en el aparato 10 de teléfono que registre un mensaje de correo de voz.

El mensaje de correo de voz registrado se almacena en el repositorio 50. El mensaje registrado se almacena en una forma cifrada, realizándose el cifrado usando una clave pública desde un par de claves pública-privada asociadas con el aparato 20 de teléfono del segundo usuario.

Cuando el segundo usuario desea acceder a su correo de voz, usa el aparato 20 de teléfono para conectarse al sistema 5 de correo de voz. Al recibir la petición, el sistema 5 de correo de voz accede a los mensajes en el repositorio 50 y los carga en el aparato 20 de teléfono. El software en el aparato de teléfono usa la clave privada del par de claves pública-privada para descifrar el mensaje de modo que pueda emitirse al usuario a través del dispositivo 20.

La figura 2 es el diagrama esquemático de la figura 1 que ilustra un funcionamiento preferido del sistema de correo de voz seguro.

En esta realización, el dispositivo 15 del primer usuario incluye un sistema 100 de comunicación segura.

Cuando el sistema 40 de conmutación se conecta al aparato 15 de teléfono del primer usuario, inicia una consulta para determinar si existe un sistema de comunicación segura. En este caso, puesto que sí existe un sistema 120 de este tipo, el primer aparato 15 de teléfono proporciona una respuesta de confirmación y se negocia un canal 70 de comunicación segura entre el dispositivo 15 del primer usuario y el segundo dispositivo 20. De esta manera, las comunicaciones a través de la PSTN 30 (u otra red puesto que no es necesario que las realizaciones de la presente invención operen a través de una PSTN) se cifran y también son seguras.

En uso, cuando está estableciéndose una sesión de comunicación, el sistema 100 de comunicación comprueba si el dispositivo 20 del segundo usuario soporta comunicaciones seguras. En este escenario, el dispositivo 20 al que se llamó incluye un sistema 110 de comunicación segura compatible. Durante la negociación para el establecimiento de la llamada, los respectivos sistemas 100, 110 de comunicaciones seguras establecen una conexión 70 de datos (usando preferiblemente una conexión basada en protocolo de Internet (IP)), realizan un intercambio de claves e interceptan a continuación comunicaciones de voz y las digitalizan, las encapsulan por paquetes y las cifran antes de transmitirlas a través de una conexión de datos. En la recepción, el dispositivo 20 del segundo usuario realiza las etapas en sentido inverso y emite la voz al usuario remoto.

Opcionalmente puede usarse una conexión de datos de GSM directa en lugar de IP. Se usa una conexión de datos de GSM de HSCSD para reducir la latencia.

Preferiblemente se usa el códec ITU-T G.722.2 para el procesamiento de voz.

Los sistemas 100, 110 de comunicaciones pueden usar sistemas de cifrado redundantes para una sesión, autenticación y/o intercambio de claves. Realizaciones preferidas usan dos algoritmos fuertes al mismo tiempo en serie. La combinación preserva la seguridad de comunicación en caso de que se descubra en el futuro que un algoritmo es débil.

Para el cifrado de una sesión: pueden usarse AES y RC4 con 256 bits. Para la autenticación: pueden usarse RSA y DSA con 4096 bits. Para el intercambio de claves: puede usarse Diffie-Hellman con 4096 bits.

Preferiblemente, las claves de sesión se borran de los teléfonos móviles tanto de origen como de recepción una vez concluida la comunicación. De esta manera, no pueden descifrarse comunicaciones anteriores aunque se extraiga el material de clave privada de los teléfonos móviles. Las claves de sesión sólo se almacenan en el teléfono móvil, sólo en la memoria y sólo durante la duración de la comunicación segura.

Los números aleatorios usados para la generación de claves se toman de una fuente segura si está disponible. Puesto que la mayoría de teléfonos móviles no ofrecen una fuente de este tipo, puede usarse una fuente remota tal como un servidor 120 de SMS para proporcionar una semilla de números aleatorios por SMS 125. De esta manera, para cada sesión de comunicación se solicitó a través de SMS la primera semilla para un generador de números pseudoaleatorios local.

Preferiblemente, el sistema de comunicación puede instalarse simplemente en un teléfono móvil desde una fuente remota. Preferiblemente, la instalación no requiere gestión de claves. Puede usarse gestión de claves “en las que se confía por primera vez” de manera similar a en SSH. Realizar y recibir una llamada telefónica preferiblemente no será diferente de una llamada telefónica tradicional con respecto a la calidad de voz y a la latencia.

La identidad de un usuario está ligada a la EMSI, IMSI y/o al número de teléfono.

Cada paquete de GSM se cifra preferiblemente por separado. Se ignora cualquier paquete de GSM que no llega a tiempo o se pierde durante la transmisión. Se cree que los paquetes de GSM perdidos no representan un problema de seguridad o calidad.

En el caso en el que el dispositivo 20 del segundo usuario está disponible para establecer el canal 70 de comunicación segura pero no está disponible para recibir realmente la llamada (por ejemplo el receptor puede estar en otra llamada o el dispositivo puede estar configurado para remitir directamente al correo de voz), se produce un intercambio de claves y un establecimiento del canal 70 de comunicación segura como antes. Sin embargo, una vez establecido el canal, el dispositivo 20 del segundo usuario activa el sistema 40 de conmutación para desviar la llamada al correo de voz.

El sistema 40 de conmutación encamina la llamada al repositorio 50 donde se reproduce el saludo grabado previamente o convencional del usuario en el dispositivo 15 del primer usuario. Después se recibe el mensaje de correo de voz del dispositivo 15 del primer usuario en la forma cifrada y encapsulada por paquetes. Los datos se almacenan en el repositorio 50 según se reciben. Preferiblemente, el repositorio captura los datos en el dispositivo del primer usuario y metadatos sobre la llamada (por ejemplo identificador/número de teléfono del dispositivo del primer usuario, fecha y hora del mensaje) y almacena los datos vinculados a los paquetes almacenados de datos de correo de voz.

El repositorio no contiene preferiblemente la(s) clave(s) necesaria(s) para descifrar los datos recibidos a través del canal de comunicaciones seguras y por tanto no tiene más opción que registrarlos en la forma segura según se reciben. Por tanto, incluso aunque el repositorio se vea comprometido, los propios datos todavía son seguros.

En una realización preferida, se usa un cifrado de claves pública/privada y el repositorio contiene copias de la(s) clave(s) pública(s) del segundo dispositivo. De esta manera, si el segundo dispositivo no está disponible (por ejemplo si estuviera apagado) para establecer el canal 70 de comunicación segura, el repositorio puede actuar como *proxy* con respecto al segundo dispositivo y establecer el canal 70 de comunicaciones seguras para su uso posterior para recibir un mensaje de correo de voz. De hecho, el repositorio 50 puede actuar como *proxy* incluso aunque el segundo dispositivo 20 esté disponible puesto que puede considerarse más eficaz para que el segundo dispositivo pase inmediatamente peticiones de conexión destinadas al correo de voz al repositorio para su tratamiento en lugar de tener que gestionar la sobrecarga de intercambio de claves, etc. Incluso cuando el segundo dispositivo 20 sí participa en el establecimiento del canal 70 de comunicaciones seguras, todavía se prefiere que el repositorio contenga copias de la(s) clave(s) pública(s) del dispositivo de modo que pueda cifrar el saludo de correo de voz saliente y comunicar cualquier opción de manera segura al primer dispositivo 15.

La figura 3 es un diagrama esquemático de un sistema de correo de voz seguro según otra realización de la presente invención.

En esta realización, el aparato 20 de teléfono del segundo usuario está configurado para reenviar correos de voz a un sistema 80 de correo de voz alternativo que no está vinculado o asociado con el centro 40 de conmutación del proveedor de comunicaciones.

El sistema 80 de correo de voz alternativo está situado de manera remota con respecto al centro 40 de conmutación. Cuando el centro 40 de conmutación intenta reenviar a la primera persona que llama al correo de voz, se identifica la dirección de reenvío alternativa y se conecta el primer aparato 15 de teléfono (a través de un canal 70 seguro si el aparato 15 de teléfono puede hacerlo) al sistema 80 de correo de voz alternativo. El canal 70 seguro puede establecerse tal como se comentó anteriormente (es decir o bien mediante el segundo dispositivo 20 y luego redirigirse o bien, preferiblemente, directamente usando el sistema 80 de correo de voz alternativo copias de las claves de cifrado públicas del segundo dispositivo).

Preferiblemente, si el sistema 80 de correo de voz alternativo es remoto con respecto a la red o sistemas del operador de telecomunicaciones que da servicio al segundo aparato 20 de teléfono, se establece un canal de comunicación segura entre el segundo aparato 20 de teléfono y el sistema 80 de correo de voz alternativo siempre que se transmita correo de voz al aparato 20 de teléfono. De esta manera, no sólo el propio correo de voz está cifrado, sino también el tráfico de comunicación, lo que proporciona redundancia y seguridad adicional.

La figura 4 es una ilustración de una visualización de pantalla según una realización adicional de la presente invención.

En esta realización, se proporciona una interfaz 100 al usuario del aparato 20 de teléfono asociado con el buzón de correo en el sistema (50 u 80) de correo de voz seguro. Cuando se reciben correos de voz y se almacenan en el repositorio 50, 80, se envía una notificación al aparato 20 de teléfono y se visualiza en la interfaz 100 de usuario. Preferiblemente, se visualizan el número de teléfono de la persona que llama, la hora y la fecha y la duración del mensaje. La interfaz permite preferiblemente que el usuario seleccione mensajes para su descarga, reproducción, almacenamiento o eliminación. Se apreciará que aunque el sistema de correo de voz seguro de la presente

invención puede funcionar de la misma manera que los sistemas de correos de voz convencionales a los que se accede y se emiten correos de voz de manera secuencial, enviando una notificación al dispositivo de usuario, puede proporcionarse acceso aleatorio a correos de voz, lo que mejorará sustancialmente la experiencia de usuario. Adicionalmente, los correos de voz pueden descargarse en el aparato 20 de teléfono para permitir que el usuario los escuche cuando le venga bien y la persona que llama y la longitud del correo de voz pueden proporcionar al usuario en el aparato 20 de teléfono una indicación de cuánto tiempo tardará en obtener los mensajes. Opcionalmente, pueden enviarse los propios mensajes cifrados al aparato 20 de teléfono en lugar de una notificación. De esta manera, el usuario no tendrá que esperar durante el proceso de descarga pero se requerirá que el aparato 20 de teléfono tenga una mayor capacidad de almacenamiento.

Puesto que los mensajes de correo de voz están cifrados, podrán transportarse por Internet puesto que hay un menor riesgo en cuanto a seguridad. Una posibilidad para mover mensajes de correo de voz sería si el usuario del segundo aparato 20 de teléfono se encontrase en itinerancia entre redes. Podría transmitirse un mensaje de correo de voz a un almacén local en la última red conocida usada por el aparato 20 de teléfono en lugar de requerir que siempre se envíe a través de la red doméstica del usuario.

En una realización, pueden implementarse repositorios de correos de voz en alguna forma o jerarquía o topología de igual a igual y disponerse para que distribuyan claves públicas entre los mismos para proporcionar redundancia, proporcionar iteración y también permitir la selección del repositorio más cercano a la persona que llama para reducir la sobrecarga de la red. En tales disposiciones, puede identificarse un repositorio como repositorio doméstico para un dispositivo de usuario y pueden transferirse correos de voz recibidos en otros repositorios a, o sincronizarse con, el repositorio doméstico. Un repositorio no doméstico que recibe un correo de voz puede indicar su disponibilidad al repositorio doméstico y transmitirlo al repositorio doméstico si no se solicita por el dispositivo o repositorio doméstico dentro de un periodo predeterminado de tiempo.

Aunque los pares de claves pública/privada se mencionan como implementación preferida para el cifrado, se apreciará existen que otros sistemas de cifrado que serían igualmente aplicables. Por ejemplo, los pares de claves pública-privada podrían usarse para negociar una clave de sesión simétrica usada sólo para ese mensaje. Preferiblemente, el par de claves pública/privada se genera en el aparato 20 de teléfono del usuario. Pueden vincularse opcionalmente con un parámetro específico del aparato de teléfono tal como el identificador único IMEI. La clave pública podría compartirse entre proveedores de telecomunicaciones y quienes proporcionan el servicio de correo de voz cifrado seguro sin temor a vulnerar la seguridad del sistema de correo de voz seguro. Preferiblemente, aparatos de teléfono compatibles pueden descargar una aplicación de software para permitir el uso de un sistema de correo de voz cifrado. Cuando la aplicación se ejecuta por primera vez, se crean los pares de claves pública y privada y la clave pública se transmite después al sistema de correo de voz seguro para su uso en la creación de los correos de voz cifrados seguros.

REIVINDICACIONES

1. Sistema que incluye un repositorio (50) de correo de voz seguro y un sistema (20) receptor, estando el repositorio dispuesto para recibir llamadas para el sistema receptor y registrar dichas llamadas en una forma cifrada, en el que la forma cifrada puede descifrarse mediante una clave asociada con un aparato de teléfono del sistema receptor, estando el sistema **caracterizado porque** está dispuesto, a petición, para proporcionar la forma cifrada de la llamada al sistema receptor,
en el que el repositorio está dispuesto para recibir llamadas en la forma cifrada a través de un canal de comunicación segura y para registrar dichas llamadas en dicha forma cifrada, estableciéndose el canal de comunicación segura entre un sistema que realiza la llamada y el sistema receptor, siendo el sistema receptor remoto con respecto al repositorio, el estando el repositorio dispuesto para recibir una transferencia del canal de comunicación segura desde el sistema receptor para recibir dicho correo de voz.

2. Sistema según la reivindicación 1, en el que el repositorio está dispuesto para establecer dicho canal de comunicación segura con dicho sistema que realiza la llamada cuando dicho sistema receptor no está disponible.

3. Sistema según la reivindicación 1 ó 2, en el que el repositorio comprende además al menos una clave de cifrado asociada con cada uno de una pluralidad de buzones de correo, estando cada uno de los buzones de correo asociado con un sistema receptor, estando el repositorio dispuesto para identificar el buzón de correo dependiendo del sistema receptor al que se llamó y usar dicha respectiva al menos una clave para el establecimiento de dicho canal de comunicación segura y/o para la comunicación con dicho sistema que realiza la llamada a través de dicho canal de comunicación segura.

4. Sistema según la reivindicación 1, en el que el repositorio comprende además al menos una clave de cifrado asociada con cada uno de una pluralidad de buzones de correo, estando cada uno de los buzones de correo asociado con un sistema receptor, estando el repositorio dispuesto para identificar el buzón de correo al que se llamó dependiendo del sistema receptor al que se llamó y cifrar llamadas no cifradas en dicha forma cifrada durante o antes del registro usando dicha al menos una clave de cifrado.

5. Sistema según la reivindicación 3 ó 4, en el que la al menos una clave comprende una clave pública de un par de claves pública-privada.

6. Sistema según la reivindicación 5, que comprende además un sistema receptor, incluyendo el sistema receptor la clave privada del par de claves pública-privada y estando dispuesto para obtener dicha forma cifrada de la llamada desde el repositorio y descifrar la llamada dependiendo de la clave privada.

7. Sistema según la reivindicación 6, en el que el repositorio está dispuesto, una vez finalizado el registro de una llamada, para transmitir dicha forma cifrada de dicha llamada al respectivo sistema receptor.

8. Sistema según la reivindicación 6, en el que el repositorio está dispuesto para transmitir dicha forma cifrada de dicha llamada al respectivo sistema receptor durante el registro.

9. Sistema según cualquier reivindicación anterior, en el que el repositorio es remoto con respecto al sistema de gestión de red de cualquier proveedor de telecomunicaciones y está dispuesto para recibir llamadas en nombre de sistemas receptores que operan en diferentes redes de telecomunicaciones.

10. Sistema según cualquier reivindicación anterior, que comprende además una pluralidad de repositorios, estando dispuesto cada uno para recibir llamadas para un sistema receptor y transmitir dichas llamadas registradas en dicha forma cifrada entre los mismos a petición.

11. Método para operar un repositorio de correo de voz seguro **caracterizado por**:

establecer un canal de comunicación segura para una llamada entre un sistema (10) de llamada y un sistema (20) receptor,
transferir el canal de comunicación segura desde el sistema receptor a un repositorio (50) remoto con respecto al sistema receptor para recibir una llamada de correo de voz;
recibir dicha llamada de correo de voz en una forma cifrada y encapsulada por paquetes en el repositorio;
registrar dichas llamadas en dicha forma cifrada y encapsulada por paquetes en el repositorio; y, proporcionar, a petición, la forma cifrada de la llamada al sistema receptor, en el que
la forma cifrada puede descifrarse mediante una clave asociada con un aparato de teléfono del sistema receptor.

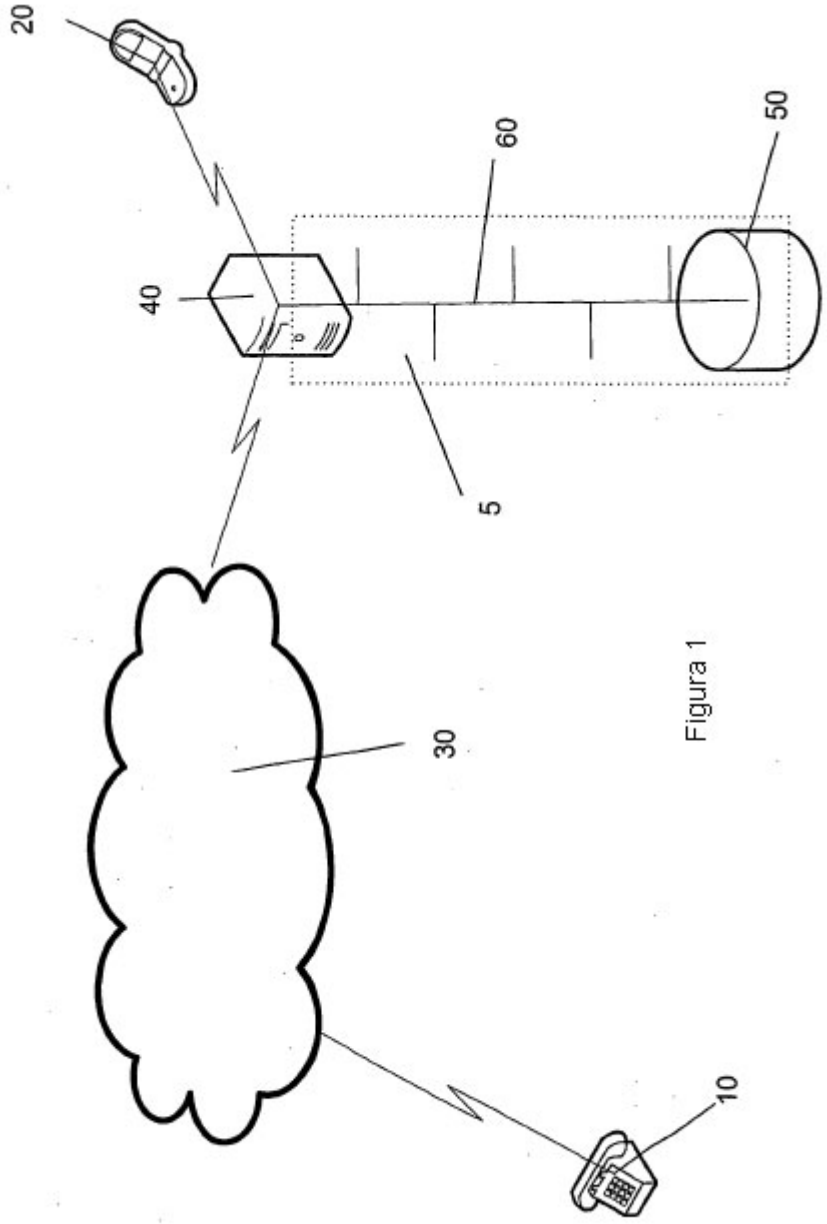

Figura 1

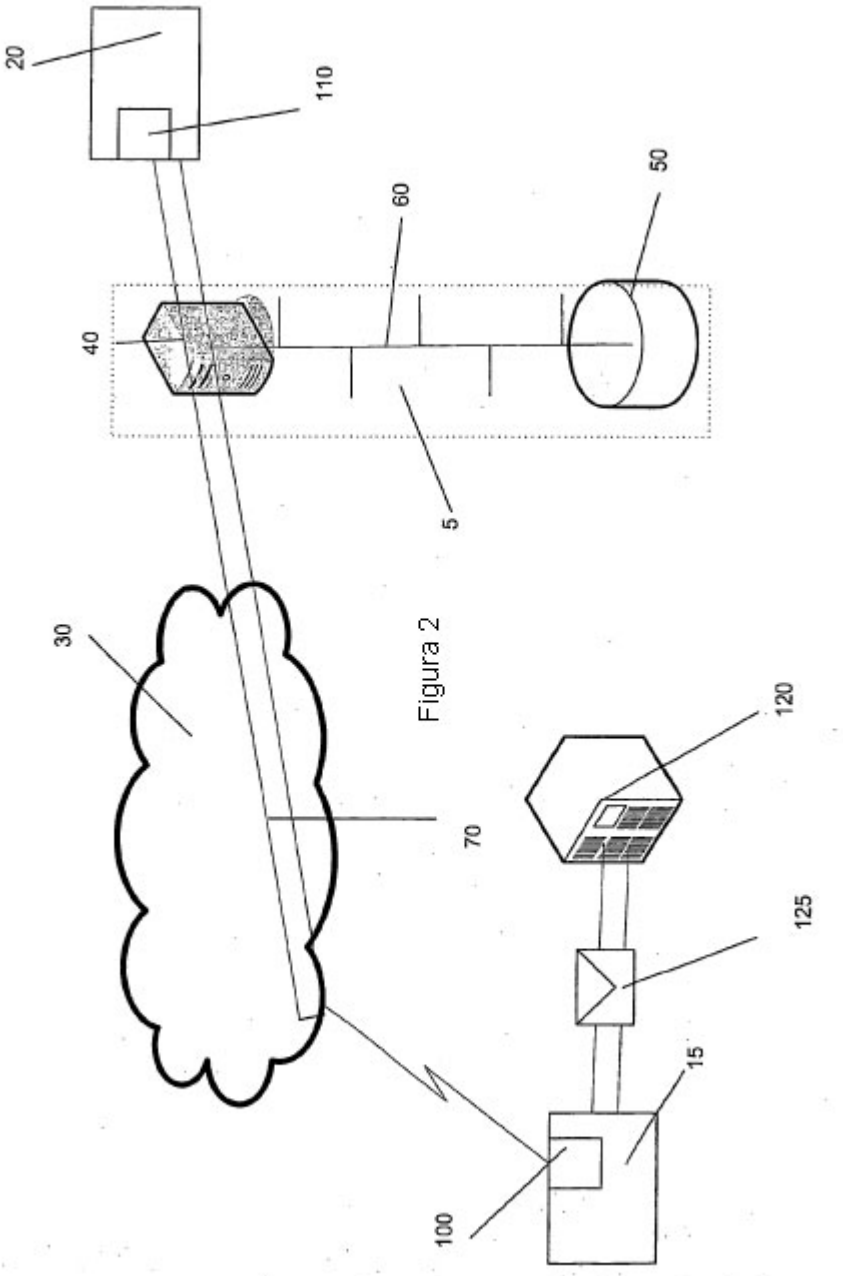

Figura 2

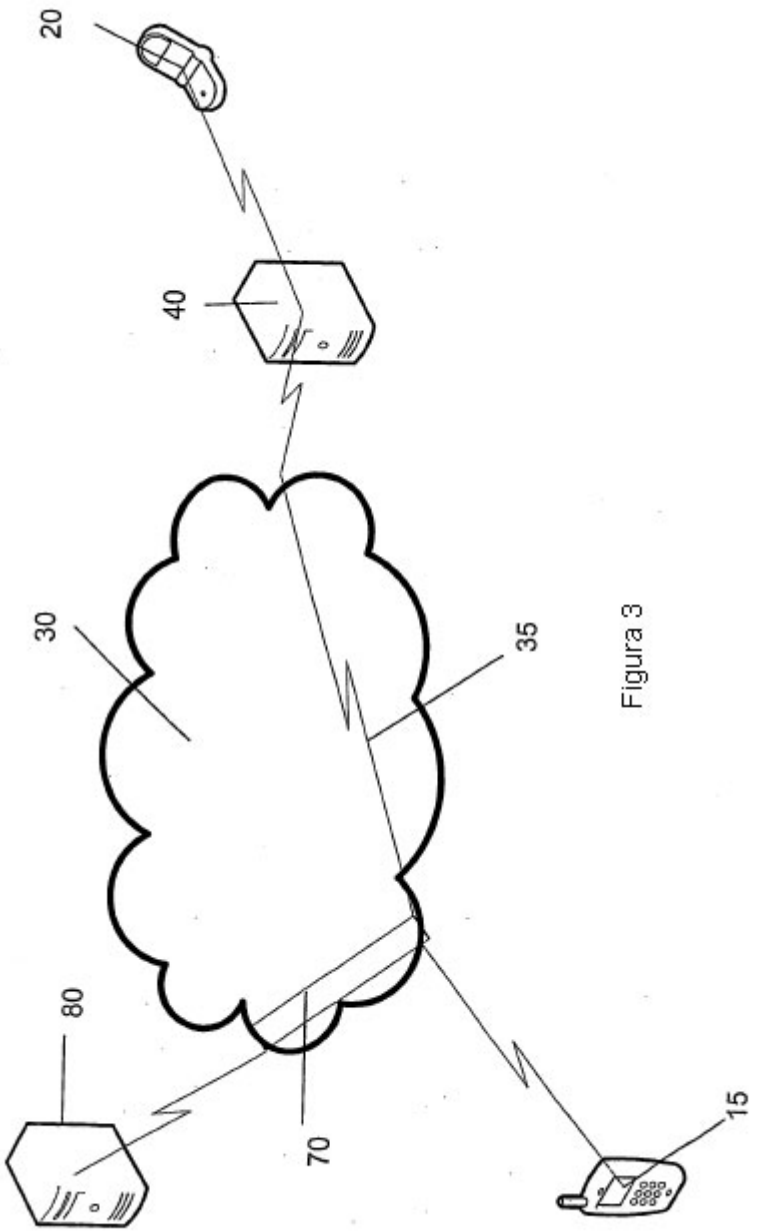

Figura 3

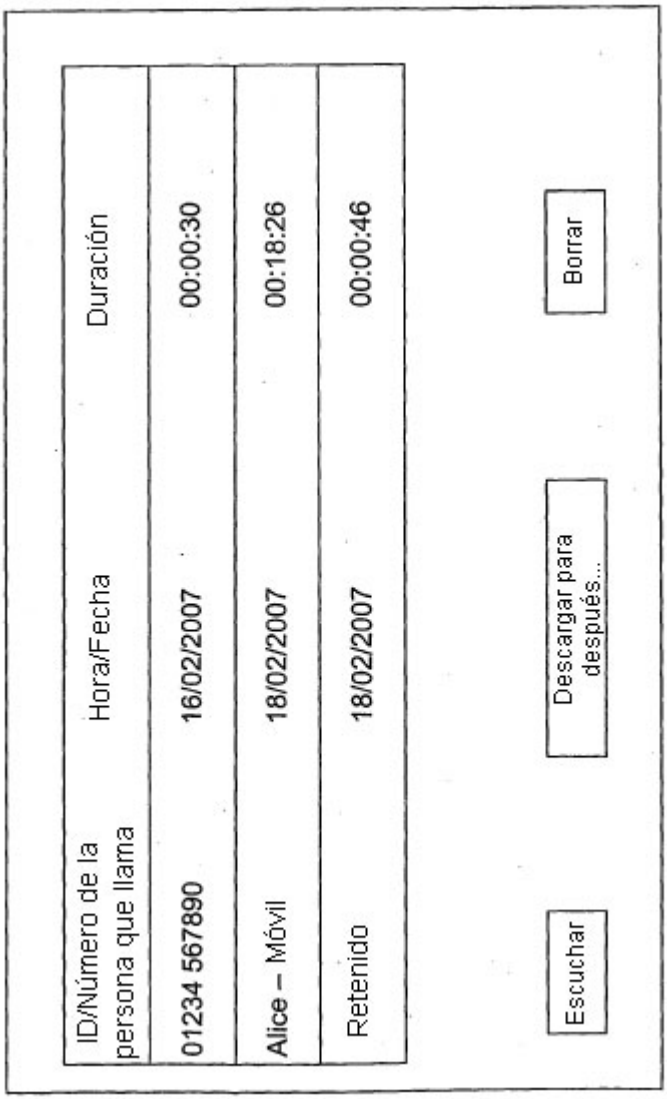
ID/Número de la persona que llama
Hora/Fecha
Duración
01234 567890
16/02/2007
00:00:30
Alice – Móvil
18/02/2007
00:18:26
Retenido
18/02/2007
00:00:46
Escuchar
Descargar para después...
Borrar

Fig. 4