(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 955 478**

(51) Int. CI.:

H04L 9/40 (2012.01)
H04W 4/14 (2009.01)
H04L 67/12 (2012.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04W 12/033 (2011.01)
H04W 12/041 (2011.01)
H04L 51/04 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.12.2017 PCT/FR2017/053867**

(87) Fecha y número de publicación internacional: **19.07.2018 WO18130761**

(96) Fecha de presentación y número de la solicitud europea: **29.12.2017 E 17832313 (5)**

(97) Fecha y número de publicación de la concesión europea: **28.06.2023 EP 3568964**

(54) Título: **Método de transmisión de una información digital cifrada de extremo a extremo y sistema que implementa dicho método**

(30) Prioridad:

10.01.2017 FR 1750212

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.12.2023

(73) Titular/es:

WALLIX (100.0%)
250 Bis Rue du Faubourg Saint-Honoré
75008 Paris, FR

(72) Inventor/es:

BINSZTOK, HENRI

(74) Agente/Representante:

DEL VALLE VALIENTE, Sonia

DESCRIPCIÓN

Método de transmisión de una información digital cifrada de extremo a extremo y sistema que implementa dicho método

Campo de la invención

La presente invención se refiere al campo de la protección de las comunicaciones electrónicas asíncronas en redes informáticas, sobre todo, aunque no de forma limitativa, la red de internet o las redes privadas virtuales.

La información, por ejemplo, datos digitales producidos por objetos conectados, máquinas de fax, o mensajes de texto, archivos digitales, se transmiten gracias a un conjunto normalizado de protocolos de transferencia de datos, que permite la elaboración de aplicaciones y de servicios diversos, como la publicación de datos, correo electrónico, mensajería instantánea, ‘‘peer-to-peer’’, etc.

Las soluciones más protegidas utilizan técnicas de cifrado de extremo a extremo (‘‘End-to-end encryption’’ en inglés). Cuando se envía un mensaje a un destinatario, este está cifrado por el usuario, en el equipo informático del emisor, según soluciones que garantizan que solo el receptor pueda descifrar la misiva. El servidor por el que transite la conversación sirve únicamente para transmitir, sin intentar en ningún caso decodificarlo. En este caso, los usuarios pueden comunicarse entre ellos sin intermediarios.

En vez de enviarse en forma de texto, el mensaje se codifica en forma de cifras, y es necesaria una clave para descifrarlo. Las claves son efímeras y desaparecen cuando el mensaje ha sido descifrado por el usuario. Por ello, ni los piratas, ni los ciberdelincuentes, ni incluso los empleados del operador del servicio, pueden leer los mensajes. Como ejemplo, el servicio de mensajería WhatsApp (nombre comercial) propone una solución de cifrado de extremo a extremo.

Estado de la técnica

Se conoce en el estado de la técnica la solicitud de patente WO2014175830, que describe un método para tratar un paquete de datos procedente de un primer dispositivo informático a un segundo dispositivo informático para permitir una comunicación de cifrado de extremo a extremo

El paquete de datos comprende un mensaje cifrado con ayuda de una primera clave de cifrado para formar un mensaje cifrado, datos de identificación del segundo dispositivo informático cifrados con ayuda de una segunda clave de cifrado, para formar datos de identificación cifrados, y la primera y segunda claves de cifrado, cifradas.

El método según esta solución conocida consiste en descifrar la segunda clave de cifrado cifrada, descifrar les datos de identificación cifrados con ayuda de la segunda clave de cifrado descifrada, y transmitir el paquete de datos según los datos de identificación descifrados, estando diseñados el mensaje cifrado y la primera clave de cifrado para que no puedan ser descifradas por el servidor, con el fin de permitir una comunicación de cifrado de extremo a extremo entre el primer y segundo dispositivos informáticos.

La solicitud de patente WO2012067847 describe también sistemas y métodos que permiten un cifrado de extremo a extremo. Según una realización, un método de registro de dispositivo comprende las etapas siguientes:

- una aplicación ejecutada por un procesador informático recibe de un usuario una contraseña de usuario;
- mediante el procesador informático, la aplicación combina la contraseña de usuario y una extensión de la contraseña;
- mediante el procesador informático, la aplicación trata de forma criptográfica la combinación de contraseña del usuario y de extensión de la contraseña, lo que permite obtener información pública criptográfica. La información pública criptográfica se suministra a un servidor. Sin embargo, la contraseña del usuario no es suministrada por el servidor.

Se conoce también la patente EP1536601, que hace referencia a un método de cifrado de extremo a extremo de correos electrónicos enviados de un emisor a un destinatario, que comprende las etapas siguientes:

a) el emisor solicita a un sistema de cifrado un certificado correspondiente a dicho destinatario,

b) el sistema de cifrado reenvía a dicho emisor un primer certificado correspondiente a dicho destinatario, el emisor con su software de correo electrónico envía un correo electrónico saliente a dicho destinatario, cifrado con dicho certificado,

c) dicho correo electrónico es enviado por dicho sistema de cifrado.

El sistema de cifrado descifra el correo electrónico utilizando una clave privada correspondiente al certificado, y el sistema de cifrado facilita el contenido de dicho correo electrónico a dicho destinatario.

El emisor solicita un certificado correspondiente a dicho destinatario a un sistema de cifrado en dicha red privada, el sistema de cifrado reenvía a dicho emisor un primer certificado pro forma correspondiente a dicho destinatario, siendo generado o encontrado el certificado pro forma por el sistema de cifrado para el destinatario, y utilizado únicamente entre el emisor (1) y el sistema de cifrado, el emisor envía un correo electrónico con su cliente, correo electrónico que sale hacia dicho destinatario cifrado con dicho certificado pro forma, transmitiéndose dicho correo electrónico a través de dicho sistema de cifrado, descifrando dicho sistema de cifrado dicho correo electrónico utilizando una clave privada correspondiente a dicho certificado, facilitando dicho sistema de cifrado el contenido de dicho correo electrónico a dicho destinatario.

También se conoce en el estado de la técnica la patente de Estados Unidos US-7.240.366, que describe un método de autenticación de extremo a extremo basado en los certificados de clave pública, combinado con el Session Initiation Protocol (SIP, por sus siglas en inglés) para permitir, a un nodo de SIP que reciba un mensaje de solicitud de SIP, la autenticación del expedidor de la solicitud. El mensaje de solicitud de SIP se envía con una firma digital generada con una clave privada del expedidor, y puede incluir un certificado del expedidor. El mensaje de solicitud de SIP puede estar también cifrado con una clave pública del destinatario. Después de haber recibido la solicitud de SIP, el nodo receptor de SIP obtiene un certificado del expedidor, y autentifica al expedidor basándose en la firma digital.

La firma digital puede estar incluida en un encabezado de autorización de la solicitud de SIP, o en un cuerpo de mensaje en varias partes construido según la norma S/MIME.

La solicitud de patente US-20100189260 describe una solución de gestión de derechos atribuidos a una sesión de comunicación y a los componentes relacionados con la solicitud del usuario. A los participantes autorizados a participar en la sesión se les proporcionan herramientas de acceso, tales como las claves de descifrado. Las restricciones basadas en los derechos de conversación otorgados se extienden para preservar los registros y los documentos asociados de la sesión de comunicación.

Inconveniente de la técnica anterior

Las soluciones de la técnica anterior permiten transmisiones de datos o mensajes cifrados de extremo a extremo, únicamente entre un emisor, previamente registrado en una plataforma transaccional, y un destinatario, también previamente registrado en una plataforma transaccional.

Cuando un emisor desea enviar un mensaje o datos a un destinatario que no esté registrado aún, debe enviarle primero un mensaje no cifrado invitándolo a registrarse en la plataforma transaccional.

Durante este tiempo, el emisor debe conservar el mensaje en la memoria de su equipo informático, vigilar la recepción de una notificación de inscripción del destinatario, y activar el proceso de transmisión del mensaje o de los datos cifrados de extremo a extremo con el destinatario recién inscrito.

La intercepción del mensaje de invitación enviado por el emisor puede ser interceptado, y producir, por tanto, un fallo de seguridad.

Por otra parte, si se produce un retraso prolongado entre el envío de la invitación y la notificación del registro del emisor, el mensaje o los datos pueden perderse o alterarse.

En cualquier caso, las soluciones de la técnica anterior requieren mecanismos de sincronización entre el equipo informático del emisor, el del destinatario, y la plataforma transaccional.

En particular, en la solución propuesta por la solicitud de patente US-20100189260 (Figura 3), los usuarios ya son conocidos por la plataforma, que no permite la comunicación con un destinatario desconocido por la plataforma.

Las soluciones de la técnica anterior presentan, por otra parte, un fallo de seguridad conocido con el nombre de "ataque del hombre del medio" (en inglés, ‘‘man-in-the-middle attack’’), que es un ataque que tiene el objetivo de interceptar las comunicaciones entre dos partes, sin que ninguna de ellas pueda sospechar que el canal de comunicación entre ellas está comprometido.

Solución aportada por la invención

La invención está definida por las reivindicaciones independientes. Las realizaciones particulares se definen en las reivindicaciones dependientes.

Descripción detallada de un ejemplo no limitativo de la invención

La presente invención se comprenderá mejor tras la lectura de la siguiente descripción, haciendo referencia a un ejemplo no limitativo de realización ilustrado por los dibujos adjuntos, en donde:

- la Figura 1 muestra una vista esquemática de la arquitectura material de un sistema para la realización de la invención
- la Figura 2 muestra el diagrama de intercambios de datos entre Alice y Bob
- la Figura 3 muestra el diagrama funcional de la etapa de registro temporal del mensaje de Alice
- la Figura 4 muestra el diagrama de generación de información a partir de la contraseña elegida por Bob
- la Figura 5 muestra el diagrama funcional de la etapa de re-cifrado del mensaje por Alice
- la Figura 6 muestra el diagrama funcional de la etapa de recuperación del mensaje por Bob

Arquitectura material

La Figura 1 muestra una vista esquemática de la arquitectura material, en una situación simplificada relativa a los intercambios entre únicamente dos usuarios.

Los usuarios se denominan Alice y Bob, y cada uno de ellos utiliza uno o varios equipos informáticos conectados respectivamente (1, 11; 2, 12). Puede tratarse, por ejemplo, de un ordenador conectado, o de una tableta, o de un teléfono de tipo “Smartphone”.

Cuando se trata de un ordenador, es necesario que este disponga de recursos informáticos para acceder a una red, por ejemplo, internet, y un navegador web habitual.

En el caso de una tableta o de un teléfono, el equipo comprende también recursos tales como un navegador o una aplicación móvil que asegure la conexión a una plataforma remota.

El sistema según la invención pone en marcha, opcionalmente, un proxy (3), que distribuye la carga del servicio a uno o varios servidores (4, 13, 14), que pueden ser locales o remotos en la “nube”, que ejecutan una interfaz de programación interactiva (API).

Los servidores (4, 13, 14) están asociados a uno o varios equipos (5, 15, 16) de gestión de bases de datos, que pueden ser locales o remotos en la “nube”.

La comunicación entre los distintos equipos utiliza una capa de transporte habitual, por ejemplo, TCP/IP o Lora, y una capa de comunicación estándar, por ejemplo, http o https.

El proxy (3) y los servidores (4, 13, 14), así como los equipos (5, 15, 16) de gestión de bases de datos, forman una plataforma (20) de intercambios seguros.

Diagrama de intercambios

La iniciadora de los intercambios es Alice, que desea transmitir a Bob un mensaje en forma segura a través de una plataforma, entendiéndose que Bob no dispone de acceso a la plataforma (20) de intercambios.

Alice compone localmente, en uno de sus equipos (1, 11) un mensaje digital (21) con un editor cualquiera, por ejemplo, una aplicación de mensajería adaptada a la plataforma (20) y, por tanto, cliente de los API (4, 13, 14), y lo registra localmente en la memoria intermedia de uno de sus equipos (1,11).

A continuación, Alice introduce un identificador público (22) del destinatario Bob, por ejemplo, una dirección de mensajería de Bob o un número de teléfono móvil, en la aplicación ejecutada en su equipo de trabajo (1, 11).

Esta aplicación controla la apertura de una sesión de comunicación con su identificador. La aplicación ordena seguidamente la emisión de una consulta a través de la plataforma (20) para la capa de transporte, y a través de esta sesión y, para la capa de comunicación, a través del *token* de sesión (o mecanismo equivalente), de identificación de Bob, en forma de un mensaje que comprende al menos el identificador de Bob.

La plataforma (20) compara el identificador (22) transmitido por Alice, con la lista de los identificadores de los titulares de una cuenta, mediante una etapa (23) de verificación.

Si Bob es desconocido, es decir, que no dispone de una cuenta en la plataforma (20), la plataforma genera una cuenta temporal asociada al identificador de Bob transmitido por Alice.

Esta cuenta temporal se traduce en:

- la creación de une entrada dedicada a Bob, en la base de la base (5, 15, 16) de datos
- el envío por la plataforma (20), de un mensaje a Bob, que contiene:
- un mensaje (25) de texto de información a Bob, de la existencia de un mensaje procedente de Alice
- un enlace a una interfaz (26) de creación por Bob, de una contraseña, por ejemplo, en forma de código JavaScript y HTML.

Esta interfaz (26) de creación se ejecuta inmediatamente o en diferido en el equipo (2) de Bob, localmente y sin comunicación de la cadena (27) de caracteres creada por Bob en la plataforma (20), ni en los equipos (1, 11) de Alice y, de forma más general, en ningún equipo presente en la red.

A continuación, la plataforma (20) transmite a Alice un mensaje de validación. El envío de este mensaje significa que:

- la plataforma (20) ha creado una cuenta temporal asignada a Bob
- la plataforma (20) ha transmitido a Bob el mensaje (25) que contiene el enlace que le permite, en el momento que elija, proceder a la etapa de introducción de un contraseña en la interfaz (26).

Registro temporal del mensaje de Alice

La Figura 3 muestra el diagrama funcional de la etapa de registro temporal del mensaje de Alice.

La recepción del mensaje desencadena automáticamente las operaciones siguientes:

- la aplicación cliente de Alice ordena el cifrado del mensaje (21) con la clave pública (19) de Alice, transmitida por la plataforma (20) a partir de la información registrada en la base (5, 15, 16) de datos, y que corresponde a su cuenta. Esta clave pública es transmitida, por ejemplo, en el mensaje o en el proceso de apertura de la sesión. Puede también almacenarse localmente en el equipo (1, 11) de Alice, por ejemplo, en la memoria caché de una aplicación móvil. Esta etapa acaba con un mensaje cifrado (42) que contiene metadatos generalmente no cifrados, en concreto, un identificador del destinatario Bob.
- a continuación, este mensaje cifrado (42) se transmite mediante una transmisión (102) a la plataforma (20), y se registra, por ejemplo:
- en la base (5, 15, 16) de datos de la plataforma (20)
- en un buzón de mensajería tercero asociado a Alice
- en una plataforma Cloud...

Por otra parte, la plataforma registra en la base (5, 15, 16) de datos de la plataforma (20) los metadatos (43) que contengan, en concreto, la dirección de almacenamiento del mensaje, por ejemplo, en forma de dirección URL.

Opcionalmente, el equipo (1, 11) de Alice genera una clave (44) aleatoria de cifrado , que permite el cifrado simétrico del mensaje (42). Esta clave aleatoria (44) está a su vez cifrada de forma asimétrica con la clave pública (19) de Alice, de modo que permita a Alice descifrar, a continuación, la clave aleatoria (44) con su propia clave privada.

Generación de información pública y privada de Bob

Esta etapa es asíncrona con respecto al proceso de intercambio. Se produce en un momento cualquiera tras la recepción de la notificación del mensaje (25) y del enlace asociado.

La Figura 4 muestra los detalles del procedimiento de creación de la información pública y privada de Bob.

La contraseña (27) puede ser introducida por Bob mediante un teclado físico o virtual. También puede ser generada por un equipo de tipo generador de códigos.

Esta contraseña (27) es objeto de un tratamiento por la interfaz (26) de creación, para generar:

- un resumen criptográfico (28) (en inglés, "hash") mediante la aplicación de un algoritmo criptográfico conocido

- opcionalmente, uno o varios números aleatorios (29)

- una pareja de claves pública (30) y privada (31).

A partir del código ejecutado a partir de la interfaz (26) de creación, Bob crea una cadena (27) de caracteres que constituye una contraseña.

La interfaz (26) de creación genera, en el ejemplo descrito, un número aleatorio (29).

La interfaz (26) de creación ordena el cálculo de tres secuencias digitales:

- un resumen criptográfico (28) opcional, mediante la aplicación de un tratamiento de tipo Sha512, por ejemplo, a la secuencia (27) de caracteres, después de la aplicación eventual de un algoritmo de salado a esta secuencia (27)

- una pareja de claves pública y privada (30, 31), respectivamente, mediante la aplicación de un tratamiento, por ejemplo, PBKDF2, a una combinación del número aleatorio (29) y la contraseña (27).

El resultado de estas operaciones lleva a:

- datos secretos, que no serán retransmitidos por Bob a terceros: se trata de la contraseña (27) y de la clave privada (31)

- datos públicos, que se transmiten a la plataforma (20), y se registran en la cuenta de Bob: la función resumen (28), el número aleatorio (29) y la clave pública (30).

Re-cifrado del mensaje por Alice

Una vez que Alice haya transmitido a la plataforma (20) el mensaje cifrado (42), como se mencionó en referencia a la Figura 3, y que Bob haya procedido, de forma asíncrona, a la introducción de una contraseña, como se mencionó en referencia a la Figura 4, se reúnen las condiciones de finalización de intercambio entre Alice, que dispone ya de una cuenta, y Bob, que no dispone de una cuenta en el momento de la emisión del mensaje (21).

La Figura 5 muestra el diagrama funcional de la etapa de re-cifrado del mensaje por Alice.

En un modo de ejecución automático, cuando un equipo (1, 11) de Alice se conecta a la plataforma (20), la plataforma (20) ordena una etapa de re-cifrado (52) del mensaje (42) en un equipo (1, 11) de Alice, y no en la plataforma (20).

Si fuese necesario, por ejemplo, cuando el equipo (1, 11) no disponga de una memoria caché, esta operación prevé la transmisión (103) mediante la plataforma (20) al equipo conectado (1, 11) de Alice, de:

- la clave pública (30) de Bob

- los metadatos (43) asociados al mensaje cifrado (42)

- opcionalmente, el mensaje cifrado (42) en el equipo conectado (1, 11) de Alice.

Primera alternativa

Según una primera alternativa, la plataforma (20) transmite a Alice la totalidad del mensaje cifrado (42), y Alice descifra este mensaje con su clave privada, y después lo re-cifra con la clave pública (30) de Bob que acaba de recibir de la plataforma (20).

El mensaje original (21), inicialmente cifrado con la clave pública de Alice (19) para dar lugar a un mensaje (42) cifrado transitorio, está en ese momento disponible en una nueva forma cifrada (45) con la clave pública de Bob.

El mensaje (42) se elimina de la plataforma (20), y se sustituye por el mensaje cifrado (45).

Esta variante requiere un procesamiento intenso para mensajes grandes.

Segunda alternativa

Según otra alternativa, la plataforma (20) transmite a Alice únicamente la clave aleatoria (44). Alice descifra esta clave aleatoria (44) con su clave privada, y vuelve a cifrar la clave aleatoria (44) así descifrada, con la clave pública (30) de Bob que acaba de recibir de la plataforma (20).

En este caso, el mensaje cifrado (42) se conserva, solo los metadatos (43) asociados se actualizan en la plataforma, gracias a una solicitud automática de Alice.

Esta variante permite simplificar el procesamiento de mensajes de gran volumen.

Recuperación del mensaje por Bob

La Figura 6 muestra el diagrama funcional de la etapa de recuperación del mensaje por Bob.

Después de esta operación de re-cifrado, la plataforma (20) envía a Bob un mensaje digital que comprende una notificación textual o automática que le permite recuperar el mensaje cifrado de Alice.

De forma alternativa, la aplicación de Bob interroga periódicamente a la plataforma (20) para comprobar la disponibilidad de nuevos mensajes, o bien Bob se conecta manualmente a la plataforma (20) para comprobar si hay disponibles nuevos mensajes.

En el momento de la conexión, el equipo informático (2, 12) de Bob ejecuta un tratamiento similar al ilustrado en la Figura 5, a partir de la contraseña (27) que había creado inicialmente, y del número aleatorio (29) inicialmente registrado en la plataforma (20).

Esto permite a Bob, por una parte, volver a generar la clave pública (30) y la clave privada (31) que nunca se ha almacenado y que nunca transita por la red.

A continuación, Bob puede recuperar los metadatos cifrados (43) y, por otra parte, el mensaje cifrado (42 o 45, según la variante), y proceder a su descifrado con su clave privada (31).

Para los intercambios siguientes, las dos partes disponen de una cuenta en la plataforma (20) que le permita comunicar en modo cifrado de extremo a extremo.

Arquitectura funcional de un objeto conectado

En caso de que los intercambios se hagan no entre dos personas que dispongan de un equipo informático, sino entre objetos conectados, o un objeto conectado y una persona, el objeto conectado presenta una arquitectura de la que la Figura 6 muestra un ejemplo.

El objeto conectado comprende de forma conocida un calculador (300) asociado a un circuito (301) de comunicaciones de red.

Comprende una zona de memoria (302) no volátil en la que hay registrada al menos una secuencia digital correspondiente a la contraseña (27). Opcionalmente, la memoria (302) no volátil puede contener también una segunda secuencia digital correspondiente al número aleatorio (29).

REIVINDICACIONES

1. Método de transmisión de una información digital cifrada de extremo a extremo, entre un emisor registrado en una plataforma transaccional (20), y al menos un destinatario cualquiera, que comprende las etapas siguientes:

•selección en el equipo informático (1, 11) del emisor, de una información digital y de un identificador digital de dicho destinatario,
•cifrado temporal de dicha información digital mediante la ejecución de una aplicación de cifrado local en el equipo informático (1, 11) del emisor, con una clave del emisor,
•transmisión por el equipo informático del emisor, de dicha información digital cifrada y de dicho identificador del destinatario, a la plataforma transaccional (20),
•transmisión por la plataforma transaccional (20) al equipo informático (2, 12) de dicho destinatario, de un mensaje digital de invitación que comprende un vínculo cuya activación por dicho destinatario controla:

o la ejecución de una aplicación de creación en el equipo informático (2, 12) de dicho destinatario, de al menos una pareja de claves de cifrado de dicho destinatario,
o la transmisión de al menos una clave pública de dicho destinatario así creada por el equipo informático (2, 12) de dicho destinatario, a dicha plataforma transaccional (20), y su registro en dicha plataforma en relación con el identificador de dicho destinatario,

•transmisión a dicho equipo informático de dicho destinatario, mediante el equipo informático (1, 11) del emisor, de dicha información digital cifrada con la clave pública de dicho destinatario, opcionalmente, a través de la plataforma transaccional (20),
•descifrado mediante el equipo informático de dicho destinatario, de dicha información con la clave privada del destinatario, en donde la clave del emisor es la clave pública del emisor, y en donde el método comprende, además, las etapas siguientes, después del registro de la al menos una clave pública, y antes de la etapa de transmisión a dicho equipo informático de dicho destinatario, de dicha información digital cifrada con la clave pública de dicho destinatario:
•una notificación por dicha plataforma transaccional (20) al equipo informático (1, 11) del emisor, de un mensaje digital que permite la recuperación y el registro en una memoria temporal en el equipo informático del emisor de dicha clave pública de dicho destinatario, así como de la información digital cifrada con la clave del emisor,
•el descifrado, en el equipo informático (1, 11) del emisor, de dicha información digital cifrada con la clave del emisor, y el cifrado de dicha información digital con la clave pública de dicho destinatario, método en el que la generación de la al menos pareja de claves de cifrado comprende una etapa de tratamiento criptográfico aplicado a una combinación formada por una contraseña elegida por el destinatario y un valor elegido para la ocasión, transmitido por dicha plataforma transaccional a dicho equipo informático de dicho destinatario, comprendiendo el método, cuando se aplica a un grupo formado por una pluralidad de destinatarios:
•una etapa de introducción de claves de cifrado intermedias únicas para cada información digital,
•accediendo cada destinatario a dicha información digital, mediante el descifrado con sus claves personales de dichas claves intermedias,
•etapas de recálculo de claves intermedias, en caso de modificación de dicho grupo de destinatarios.

2. Método de transmisión de una información digital cifrada de extremo a extremo según la reivindicación 1, en donde la aplicación de cifrado está constituida por una aplicación web transmitida por dicha plataforma informática al equipo informático del emisor, en forma de código fuente ejecutable por un navegador con JavaScript.

3. Método de transmisión de una información digital cifrada de extremo a extremo según la reivindicación 1, en donde la aplicación de cifrado está constituida por una aplicación móvil previamente instalada en el equipo informático del emisor.

4. Método de transmisión de una información digital cifrada de extremo a extremo según la reivindicación 1, en donde al menos una aplicación de cifrado está constituida por una aplicación móvil descargable, para su instalación en el equipo informático del destinatario, y en donde dicho mensaje digital de invitación contiene un mecanismo que controla dicha descarga.

5. Método de transmisión de una información digital cifrada de extremo a extremo según la reivindicación 1, aplicado a un grupo de información digital, comprendiendo el método:

•una etapa de introducción de claves de cifrado intermedias únicas para cada información digital,
•cada destinatario accede al conjunto de dicho grupo de información digital, mediante el descifrado con sus claves personales de dichas claves intermedias.

6. Método de transmisión de una información digital cifrada de extremo a extremo según la reivindicación 1, en donde al menos uno de dichos equipos informáticos está constituido por un objeto conectado.

7. Método de transmisión de una información digital cifrada de extremo a extremo según la reivindicación 6, en donde la generación de las claves de cifrado comprende una etapa de tratamiento criptográfico aplicado a una combinación formada por una información única secreta, registrada en el objeto conectado en el momento de su fabricación, y un valor elegido para la ocasión, transmitido por dicha plataforma transaccional.

8. Método de transmisión de una información digital cifrada de extremo a extremo según la reivindicación 1, para un servicio de mensajería.

9. Método de transmisión de una información digital cifrada de extremo a extremo según la reivindicación 1, para un servicio de compartición de datos.

10. Método de transmisión de una información digital cifrada de extremo a extremo según la reivindicación 1, para un servicio de comunicación multimedia en tiempo real.

11. Método de transmisión de una información digital cifrada de extremo a extremo según la reivindicación 1, para un servicio de comunicación de información digital con un objeto conectado.

12. Método de transmisión de una información digital cifrada de extremo a extremo según la reivindicación 1, para un servicio de comunicación de información digital con un equipo médico conectado.

13. Sistema que comprende un objeto conectado que incluye una información única y secreta, registrada en el momento de su fabricación, un procesador para la ejecución de aplicaciones registradas en una memoria local, y medios para la comunicación con una plataforma transaccional, **caracterizado porque** una de dichas aplicaciones registradas puede ejecutar los tratamientos del equipo informático del destinatario, propios del método según la reivindicación 1, generándose la al menos un par de claves de cifrado del destinatario, a partir de la información única y secreta, comprendiendo también el sistema la plataforma transaccional y un equipo informático de un emisor para la realización del método según la reivindicación 1.

14. Sistema según la reivindicación anterior, en donde el objeto conectado comprende, además, un calculador (300) asociado a un circuito (301) de comunicación de red y una zona de memoria (302) no volátil, en donde se registra al menos una secuencia digital correspondiente a la contraseña (27).

Figura 1

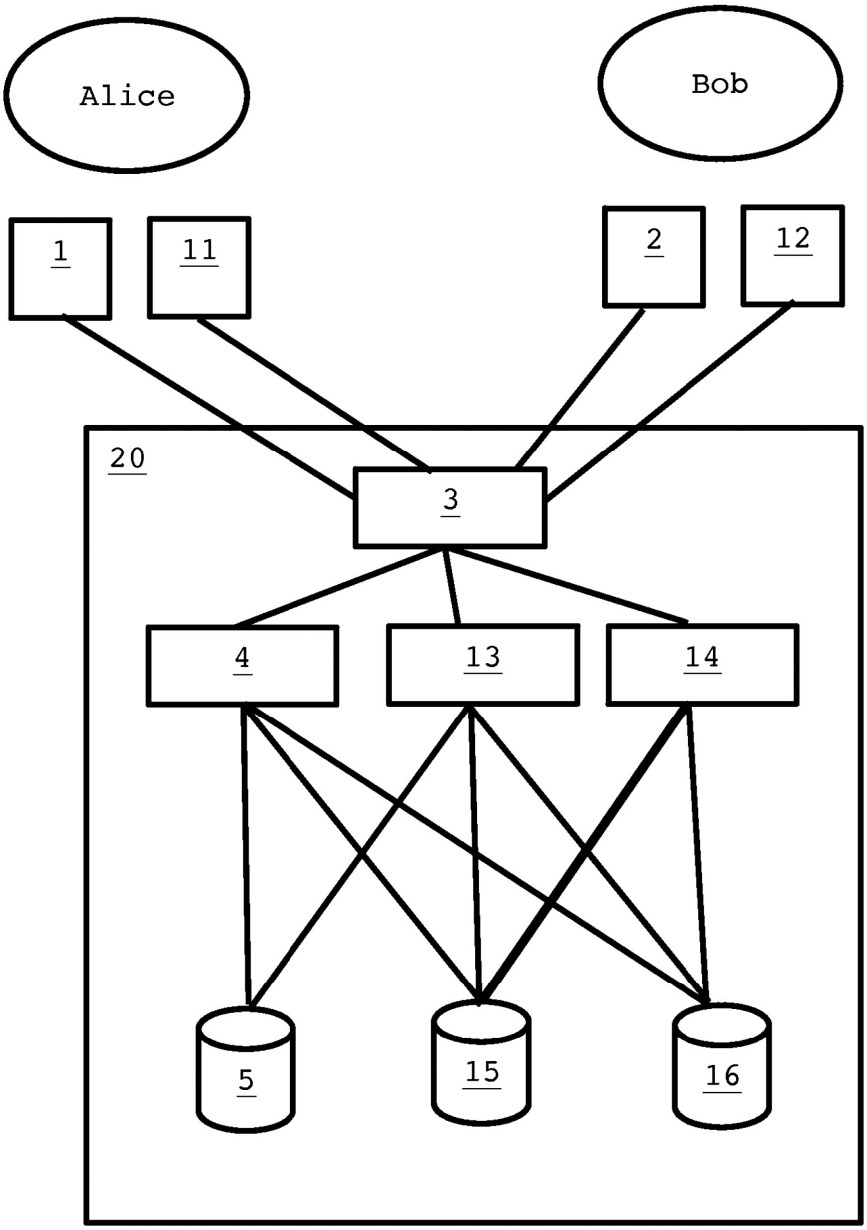

Figura 2

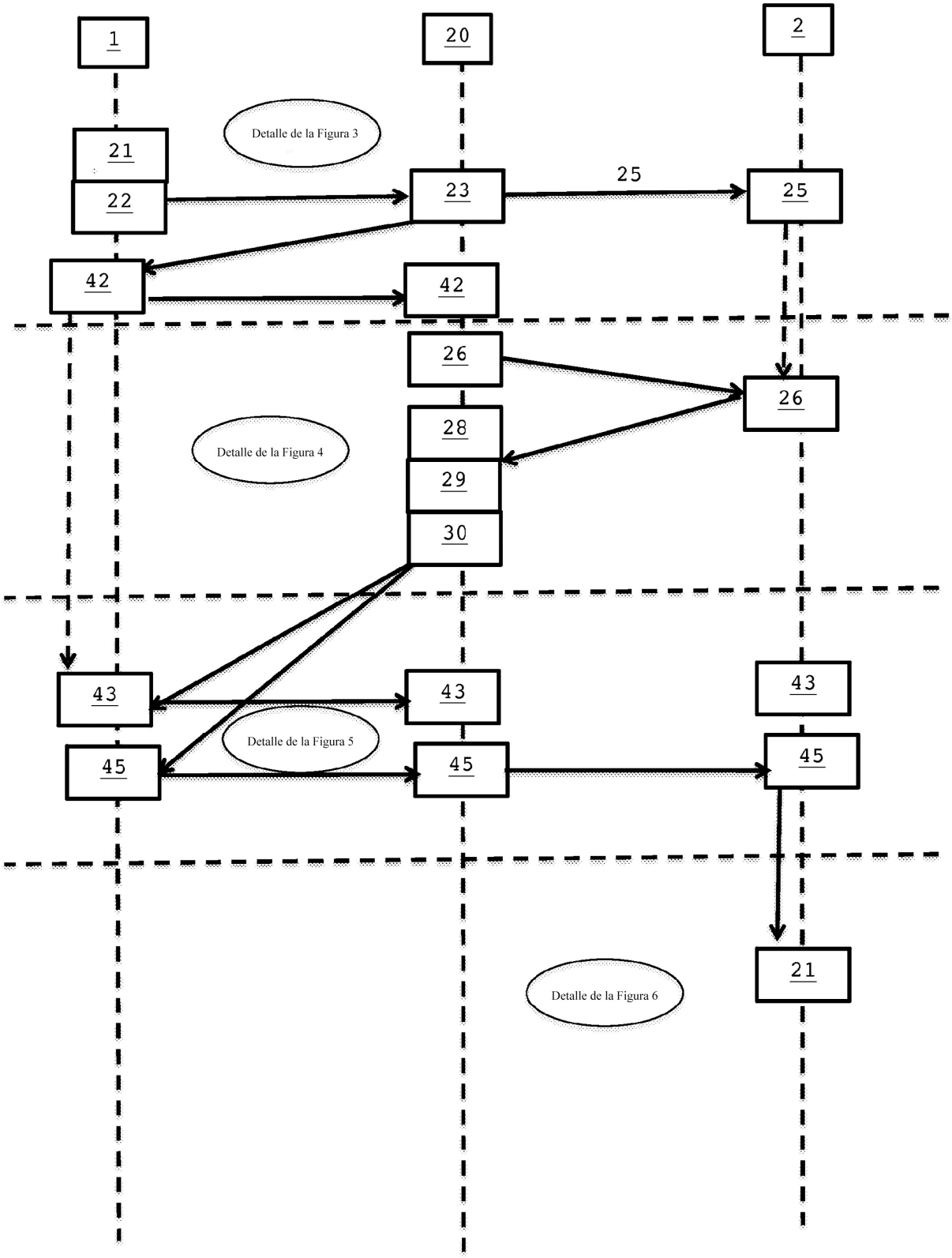
1
20
2
Detalle de la Figura 3
21
22
23
25
25
42
42
26
26
28
Detalle de la Figura 4
29
30
43
43
43
Detalle de la Figura 5
45
45
45
21
Detalle de la Figura 6

Figura 3

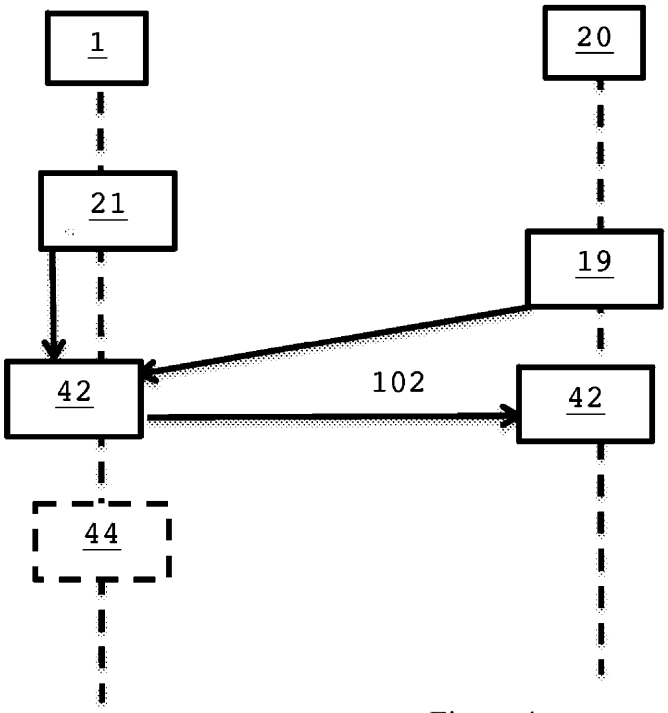

Figura 4

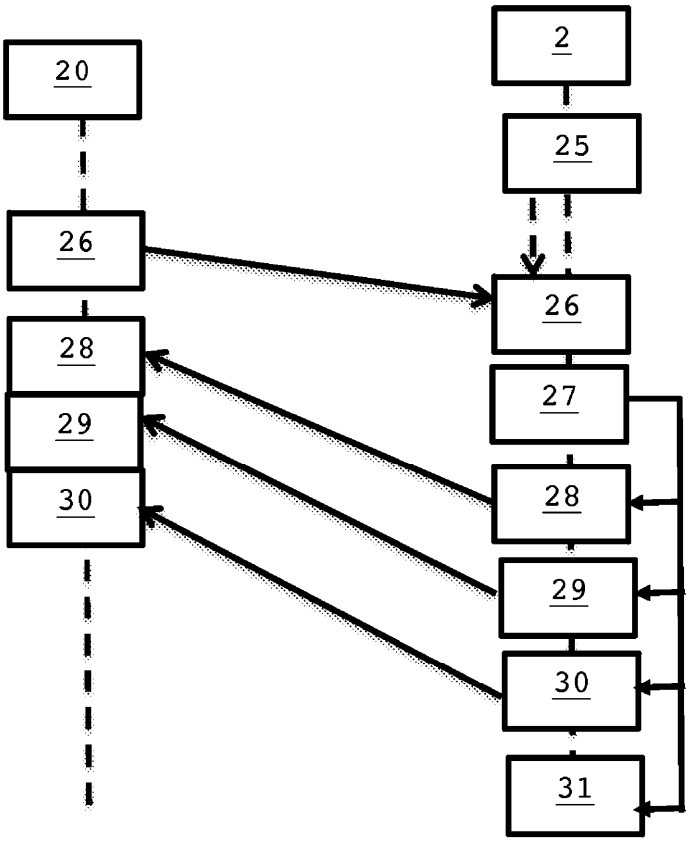

Figura 5

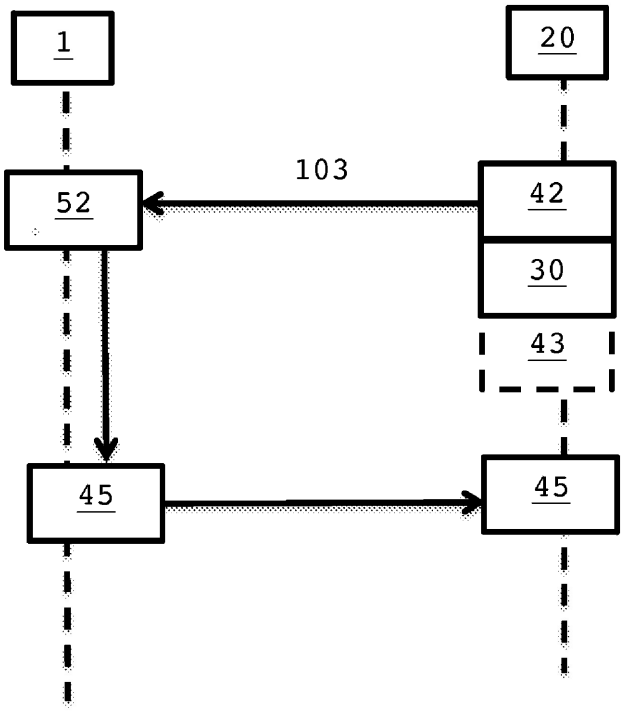

Figura 6