



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 294 807**

51 Int. Cl.:
H04L 9/08 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Número de solicitud europea: **98108118 .5**

86 Fecha de presentación : **05.05.1998**

87 Número de publicación de la solicitud: **0877507**

87 Fecha de publicación de la solicitud: **11.11.1998**

54 Título: **Encriptación punto a punto.**

30 Prioridad: **05.05.1997 DE 197 18 583**

45 Fecha de publicación de la mención BOPI:
01.04.2008

45 Fecha de la publicación del folleto de la patente:
01.04.2008

73 Titular/es: **T-Mobile Deutschland GmbH**
Landgrabenweg 151
53227 Bonn, DE

72 Inventor/es: **Kaliner, Stefan**

74 Agente: **Isern Jara, Jorge**

ES 2 294 807 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Encriptación punto a punto.

5 El objeto del invento es una encriptación punto a punto, mejor dicho, un procedimiento para la generación y distribución de claves secretas para la encriptación punto a punto de informaciones de un enlace de comunicaciones en sistemas digitales de comunicaciones.

10 Bajo la denominación de encriptación punto a punto (End-to-end-encryption - ETEE) se entiende la posibilidad de intercambio uni- o bidireccional de informaciones (en especial idioma, pero también fax o datos), en forma codificada entre dos usuarios, dentro de un sistema digital de comunicaciones. En este caso, es característica la encriptación en el lugar del emisor y la decodificación sólo por el receptor de una información, no teniendo el canal de comunicación intermedio influencia alguna sobre la encriptación. Dentro de la cadena de transmisión digital no existe posibilidad alguna para la conversión de la información al texto claro original.

15 Los requerimientos en tiempo real especificados a procedimientos apropiados de encriptación, necesitan sin falta la aplicación de algoritmos de encriptación simétricos con claves secretas R idénticas en el emisor y en el receptor.

20 En ello, un problema fundamental es la generación de la clave ETEE secreta R y su transmisión segura a ambos usuarios de la comunicación. La demanda a formular básicamente al procedimiento criptográfico respecto de la seguridad por medio del mantenimiento en secreto de las claves, no por medio del mantenimiento en secreto de los procedimientos utilizados, conduce a los requerimientos siguientes:

1. Las claves ETEE deben poseer para cada sesión de comunicación un valor individual, no predecible
- 25 2. El valor inicial para la generación de la clave debe ser individual para cada usuario, es decir, los procedimientos conocidos que derivan las claves individuales de una clave maestra única no son apropiados.
3. En ningún momento debería aparecer una clave ETEE en texto claro fuera del entorno seguro o en otra forma
- 30 que permita el cálculo del valor original. Como entornos seguros son considerados solamente los dispositivos de comunicaciones emisores y receptores.

El documento US-A 5,481,613 expone un procedimiento para la generación y distribución de claves secretas para encriptación punto a punto de información de un enlace de comunicaciones entre dos usuarios (X;Y) de un sistema digital de comunicaciones que, para la encriptación punto a punto, utiliza un procedimiento de encriptación simétrico empleando una componente central del sistema de comunicaciones que controla determinados elementos de clave, y la clave secreta (R) necesaria para ello es intercambiada entre los usuarios mediante un procedimiento de encriptación asimétrico, generando uno de los dos usuarios la clave secreta (R), la encripta por medio de la parte pública de una clave privada del otro usuario y la transfiere por medio del sistema de comunicaciones al segundo usuario, decodificando el segundo usuario la cifra encriptada transmitida por medio de la parte secreta de su propia clave y obteniendo de esta forma la clave secreta (R), siendo los elementos de clave públicos (KPX, MX o KPY, MY) de cada usuario almacenados en la componente central del sistema de comunicaciones que, como consecuencia de una solicitud de encriptación del usuario (X), le son proporcionados los elementos de clave RSA públicos (KPY, MY) del otro usuario (X) por la componente central del sistema de comunicaciones, por medio de un canal independiente de datos o señales, que por parte del primer usuario (X) se genera y guarda como cifra aleatoria una clave secreta (R), y la clave (R), mediante el procedimiento RSA y utilizando los elementos de clave RSA públicos del segundo usuario (Y), se codifica a un valor (Z) y se transmite a través del sistema de comunicaciones al segundo usuario (Y), y que, por parte del segundo usuario (Y), el valor transmitido (Z) es decodificado a la clave (R) secreta, utilizando los elementos de clave RSA secretos (KSY, KY) del segundo usuario (Y) y almacenado.

50 El documento mencionado publica el procedimiento arriba mencionado en la parte descriptiva general, en la que se aprecia el estado actual de la técnica respecto de este documento.

55 La componente central del sistema de comunicaciones que administra determinados elementos de clave se denomina en este documento Certification Authority System (CAS).

Consecuentemente, el nombrado CAS administra las claves públicas de ambas partes A y B, debiendo una parte que encripta (por ejemplo, la parte A) solicitar del CAS un certificado para poder disponer una encriptación sobre la base de este certificado y con la ayuda de una cifra aleatoria, utilizando la clave pública de la parte B.

60 Este sistema presupone que está dada una transferencia segura de la clave del CAS a la parte que debe encriptar. Ello podría ser el caso en grandes redes de ordenadores, en las que se basa el documento US-A-5,481,613. Allí se presupone una red de ordenadores ramificada ampliamente, en la que los diferentes usuarios (partes) forman dominios de seguridad y se basa en que una parte de un dominio de seguridad quiere ejecutar una operación de encriptación con una parte radicada en otro dominio de seguridad.

65 En este caso es problemático que la ruta de datos al CAS de una parte presupone un circuito de transmisión de datos seguro y que no puede ser comprometido.

Además, es desventajoso que en la red nombrada de ordenadores ampliamente ramificada, cada parte pueda iniciar con cualquier otra parte un proceso de encriptación, con el riesgo de que determinadas partes no estén habilitadas para procesos de encriptación de este tipo.

- 5 Por lo demás, el CAS allí mencionado sirve solamente para la distribución de las claves públicas (certificados), no controla, sin embargo, el tráfico de datos del modo de un servidor.

Con ello existe la desventaja de que la carga principal del trabajo de encriptación recae en los propios ordenadores del usuario y que allí no se encuentra un medio seguro.

10 Por este motivo, el invento tiene el objetivo de perfeccionar una componente central de un sistema de comunicaciones del tipo mencionado al comienzo, de forma que sea posible una selección (sujeta a pago) de diferentes usuarios en los que está dada una encriptación sencilla y segura.

- 15 Para lograr el objetivo, el invento está caracterizado por la enseñanza técnica de la reivindicación 1.

Una característica esencial del invento es que la componente central del sistema de comunicaciones está configurada como elemento sujeto a pago que, en consecuencia, puede ser llamada solamente mediando una solicitud de autorización del usuario respectivo. Consecuentemente, primero será procesada la solicitud de autorización del usuario, antes que esta componente sujeta a pago ponga a disposición las prestaciones de un servidor ETEE en el que se desarrolla, en lo esencial, el trabajo de encriptación.

De esta manera se propone una gestión sencilla en el servidor ETEE, y los usuarios reales ya no son cargados con trabajos preparatorios de este tipo.

25 Mediante la enseñanza técnica dada también se garantiza una encriptación segura, porque se dispone que esta encriptación se produzca en la tarjeta electrónica. Con ello se pone a disposición un medio que el usuario puede extraer fácilmente de un dispositivo y que, como se sabe, mantiene para el usuario una rutina de autenticación habitual. Con ello, la tarjeta electrónica se aprovecha doblemente, ya que mediante la solicitud de autorización del usuario se consulta de la manera habitual la rutina de autenticación almacenada en la tarjeta electrónica y, al mismo tiempo, se realiza la encriptación segura en la tarjeta electrónica.

Con ello resultan mecanismos de encriptación especialmente sencillos y controlables, producidos en un medio seguro (tarjeta electrónica).

35 En la patente EP 0 529 661 A2 se publica solamente una forma especial de encriptación, sin que se incluyan allí las características esenciales (elemento sujeto a pago con gestión en un servidor ETEE, solicitud de autorización y encriptación en la tarjeta electrónica).

- 40 Para conseguir el objetivo, el invento está caracterizado por las características de la reivindicación 1.

Perfeccionamientos favorables y variantes del invento resultan de las sub-reivindicaciones.

45 El presente concepto cumple los requerimientos respecto de seguridad e individualidad, sin que el sistema de comunicaciones mismo tenga conocimiento respecto de las claves secretas (R). Sin embargo, al mismo tiempo al sistema le incumbe la inicialización de la transmisión de claves y, con ello, el control respecto de la aplicación de la encriptación punto a punto. Para el caso en que el procedimiento está configurado como un servicio adicional pago, la autorización puede otorgarse en función de determinadas propiedades de la relación de usuarios. Al mismo tiempo, los usuarios no son cargados con el almacenamiento y gestión de elementos de clave de sus contrapartes de la comunicación.

50 El procedimiento utiliza una generación descentralizada de la clave ETEE R por parte del usuario X solicitante de la ETEE. La clave secreta R es transmitida en forma encriptada al usuario Y por medio de procedimientos RSA conocidos (procedimiento según Rivest, Shamir y Adleman) utilizando los elementos de clave RSA públicos del usuario Y, reencriptada allí mediante los elementos de clave RSA secretos del usuario Y, estando ahora a disposición en ambos lados para la encriptación de la información. Antes, los elementos de clave RSA públicos del usuario Y fueron puestos a disposición del usuario X por una componente central del sistema de comunicaciones (servidor ETEE). Todos los cálculos para generar y transmitir la clave ETEE, así como el almacenamiento de los elementos de clave RSA secretos, se realizan en una componente segura (por ejemplo, tarjeta electrónica) del lado de los usuarios.

60 A continuación, el invento se explica en detalle sobre la base de dibujos que representan solamente una ruta de realización. En este caso, de los dibujos y de su descripción resultan otras características esenciales y ventajas del invento.

- 65 La figura 1 muestra en forma esquematizada el principio básico de una comunicación encriptada entre dos usuarios X e Y;

La figura 2 muestra en forma esquematizada un procedimiento de encriptación según el invento.

ES 2 294 807 T3

La figura 1 representa en forma esquematizada y en general el principio básico de una comunicación encriptada simétrica entre dos usuarios X e Y. Ambos usuarios X e Y disponen por parte de los equipos terminales de una clave R secreta, que puede utilizarse en ambos lados tanto para la encriptación (Encryption) como para la decodificación (Decryption) de los datos transmitidos por medio de una red/sistema de comunicaciones.

Con ello, es problemático que la clave secreta deba ser conocida por ambos usuarios y solamente por ellos. Con sólo dos usuarios ello es posible sin problemas, porque las partes pueden, por ejemplo, ponerse de acuerdo antes respecto de una clave. Sin embargo, con una pluralidad de usuarios ello ya no es posible. En especial, cuando por motivos de seguridad se cambia continuamente la clave secreta.

Aquí interviene el invento. Según la figura 2, el usuario X quiere proteger mediante una encriptación punto a punto (ETEE) una comunicación existente o a establecer con el usuario Y.

Cada usuario X o Y dispone de un equipo terminal con una componente segura 4 ó 5, por ejemplo una tarjeta electrónica en la que están almacenados los datos individuales de usuario y los elementos de clave RSA secretos individuales K_{SX} , M_X o bien K_{SY} , M_Y .

Los elementos de clave RSA públicos K_{PX} , M_X o bien K_{PY} , M_Y , etc. de cada usuario están almacenados en una componente central 3 del sistema de comunicaciones 1 y accesible a cualquier usuario habilitado.

Por medio de un canal independiente de datos o de señalización 2 (por ejemplo Short Message Service en redes GSM), el usuario X envía a una componente central 3 (por ejemplo Servidor ETEE) del sistema de comunicaciones 1 una solicitud de encriptación (ETEE-request) respectiva.

En la componente central 3 del sistema de comunicaciones se verifica el derecho del usuario X para la encriptación y, en caso de aceptación, el sistema contesta con los elementos de clave RSA secretos, es decir, la clave RSA pública K_{PY} y el módulo M_Y del usuario Y. El usuario X transfiere los datos recibidos a su componente segura 4.

La componente segura 4 genera ahora una clave ETEE R como cifra aleatoria y la encripta con K_{PY} y M_Y a un valor Z. La clave R se almacena por el lado X para su aplicación en la comunicación siguiente.

$R = \text{RAND}$

$$Z = \text{RSA} | K_{PY}, M_Y (R)$$

El valor Z se transmite a través de un canal de datos 6 del sistema de comunicaciones 1 al usuario Y y allí se transfiere a su componente segura 5.

La componente segura 5 decodifica el valor Z con su clave RSA secreta K_{SY} y el módulo M_Y y obtiene la clave secreta R. La clave R es almacenada en el lado Y.

$$R = \text{RSA} | K_{SY}, M_Y (Z)$$

Ahora, ambos lados X e Y tienen a su disposición claves ETEE R idénticas.

O sea, puede realizarse una encriptación y decodificación simétrica de la información intercambiada por medio de la red de comunicaciones 1.

No es necesario un aseguramiento especial de las claves R, debido a que sólo existen en los dispositivos del lado emisor y receptor (equipos terminales) y, además, pierden su validez inmediatamente después del fin de la comunicación ETEE. Cualquier otra comunicación ETEE sería realizada con nuevas claves.

De igual manera, no son críticos los elementos de clave RSA públicos en el servidor ETEE ni su ruta de transmisión al usuario X. En este caso se puede prescindir de precauciones contra espionaje.

Leyenda del dibujo

R clave secreta

X usuario X

Y Usuario Y

Z Magnitud encriptada

ES 2 294 807 T3

	1	Sistema de comunicaciones
	2	Canal de datos
5	3	Componente central
	4	Componente segura
	5	Componente segura
10	6	Canal de datos

15

20

25

30

35

40

45

50

55

60

65

REIVINDICACIONES

1. Procedimiento para la generación y distribución de claves secretas para la encriptación punto a punto de información de un enlace de comunicaciones entre dos usuarios (X;Y) de un sistema digital de comunicaciones que, para la encriptación punto a punto, utiliza un procedimiento de encriptación simétrico empleando una componente central del sistema de comunicaciones que controla determinados elementos de clave, y la clave secreta (R) necesaria para ello es intercambiada entre los usuarios mediante un procedimiento de encriptación asimétrico, generando uno de los dos usuarios la clave secreta (R), la encripta por medio de la parte pública de una clave privada del otro usuario y la transfiere por medio del sistema de comunicaciones al segundo usuario, decodificando el segundo usuario la cifra encriptada transmitida por medio de la parte secreta de su propia clave y obteniendo de esta forma la clave secreta (R), siendo los elementos de clave públicos (KPX, MX o KPY, MY) de cada usuario almacenados en la componente central (3) del sistema de comunicaciones (1) como un servicio adicional de pago (5.3, línea 2), realizándose en el componente central del sistema de comunicaciones una verificación para determinar si el usuario está autorizado a realizar una solicitud de encriptación, de manera que, como resultado de la solicitud de encriptación del usuario (X), por medio del canal de datos o de señalización (2) independiente del enlace de comunicación, los elementos de clave RSA públicos (KPY, MY) del otro usuario (Y) están a disposición del primer usuario (X) desde la componente central (3) del sistema de comunicaciones, que una clave secreta (R) es generada por parte del primer usuario (X) como una cifra aleatoria y almacenada, y la clave (R) es encriptada a un valor Z por medio del procedimiento RSA utilizando los elementos de clave RSA públicos (KPY, KY) del segundo usuario (Y) y transmitidos a través del sistema de comunicaciones al segundo usuario (Y), y que el valor (Z) transmitido es decodificado a la clave secreta (R) por el segundo usuario (Y) utilizando los elementos de clave RSA secretos (KSY, KY) del segundo usuario (Y) y almacenados, y que los cálculos para generar y transmitir la clave secreta (R) y el almacenamiento de los elementos de clave RSA secretos tenga lugar exclusivamente en una tarjeta electrónica segura en el equipo terminal del lado de los usuarios.

2. Procedimiento según la reivindicación 1, **caracterizado** porque la encriptación y la decodificación del valor (R) se realiza según un procedimiento de encriptación RSA.

3. Procedimiento según una de las reivindicaciones 1 a 2, **caracterizado** porque la clave secreta (R) generada pierde su validez al fin de cada enlace encriptado.

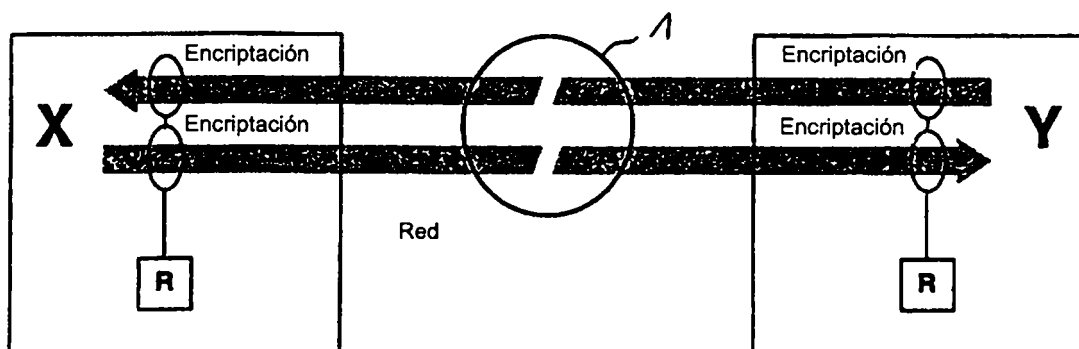


Abb. 1

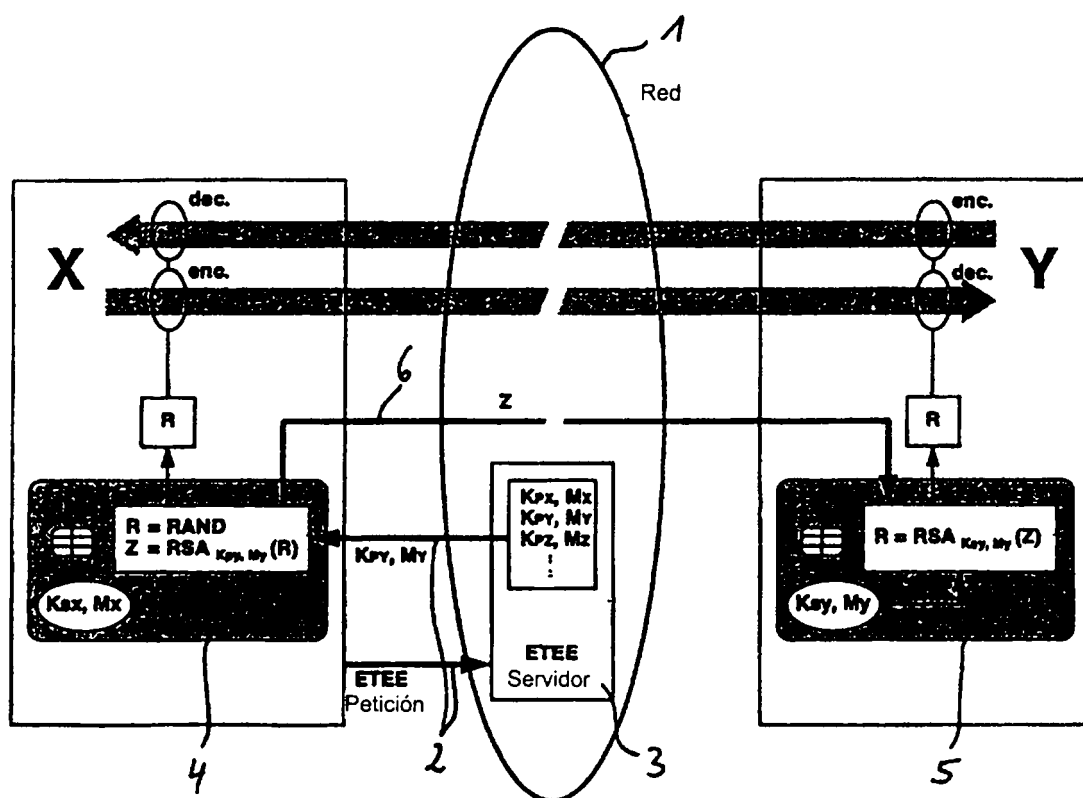


Abb. 2