(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 392 707**

(51) Int. CI.:

G06F 21/00 (2006.01)
G07F 17/16 (2006.01)
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02799789 .9**
(96) Fecha de presentación: **06.12.2002**
(97) Número de publicación de la solicitud: **1451784**
(97) Fecha de publicación de la solicitud: **01.09.2004**

(54) Título: **Sistema de control de acceso a una red, y procedimiento de control de acceso correspondiente**

(30) Prioridad:

10.12.2001 FR 0115912

(45) Fecha de publicación de la mención BOPI:

13.12.2012

(45) Fecha de la publicación del folleto de la patente:

13.12.2012

(73) Titular/es:

MORPHO (100.0%)
LE PONANT DE PARIS, 27 RUE LEBLANC
75015 PARIS, FR

(72) Inventor/es:

CHABANNE, HERVÉ

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema de control de acceso a una red, y procedimiento de control de acceso correspondiente

La presente invención se refiere a un sistema de control de acceso a una red tal como una red informática del tipo de la Internet, una red de comunicación o, más generalmente, una red de transferencia de datos. Semejante sistema se conoce por el documento GB-A-2.329.499.

Existen sistemas de control de acceso a una red semejante que comprenden terminales provistos de un lector de tarjeta de circuito integrado, así como de medios de conexión a la red, y tarjetas de circuito integrado configuradas para cooperar con el lector. El administrador de la red suministra a cada usuario autorizado un terminal y una tarjeta de circuito integrado que contiene códigos de identificación y datos personales relativos al usuario. Cuando las informaciones transitan por la red en la forma de señales que pueden ser igualmente captadas por usuarios no autorizados, se conoce la práctica de cifrar o entremezclar las señales antes de su emisión por la red, y de memorizar en el circuito integrado tarjetas de claves que permiten la reconstrucción de la señal cifrada o entremezclada, utilizables por los terminales de los usuarios autorizados a descifrar la señal. Sin embargo, existe el riesgo de que un falsificador se haga con la tarjeta de circuito integrado de uno de los usuarios autorizados y consiga extraer las claves. El falsificador puede entonces fabricar tarjetas falsas utilizando estas claves para permitir que terceros no autorizados por el administrador de la red accedan a las informaciones disponibles en la red.

Es un propósito de la invención aportar un sistema de control de acceso a una red que ofrezca más seguridad.

A este efecto, se ha concebido, de acuerdo con la invención, un sistema de control de acceso de una red tal y como se define en la reivindicación 1.

De forma ventajosa, la función que se ha de activar comprende una autentificación de la tarjeta a partir de al menos una información personalizada contenida en el circuito integrado de la tarjeta, y, de preferencia, la función que se ha de activar comprende un tratamiento de una señal procedente de la red, que comprende, ventajosamente, un desciframiento de esta señal por medio de una clave incorporada en el módulo de información cifrada.

Así, pues, el tratamiento de la señal y, por tanto, el acceso a las informaciones es precedido de una autentificación de la tarjeta, de tal forma que este tratamiento únicamente es efectuado si la tarjeta recibida dentro del lector es auténtica.

La invención tiene, igualmente, como propósito un procedimiento de control de acceso a una red por medio de un sistema análogo, tal y como se define en la reivindicación 5.

Otras características y ventajas de la invención se pondrán de manifiesto por la lectura de la descripción que sigue de un modo de puesta en práctica particular y no limitativo de la invención.

Se hará referencia a la figura única que se acompaña, la cual representa un esquema por bloques de un sistema de control de acceso de acuerdo con la invención.

El sistema de control de acceso de conformidad con la invención está destinado, en particular, a utilizarse en una red 1 gestionada por un administrador y por la que circulan señales cifradas o entremezcladas que representan informaciones o datos a los que pueden acceder usuarios de la red mediante una autorización del administrador de la red. El sistema de control de acceso tiene, por tanto, como propósito garantizar que solo los usuarios autorizados tienen acceso a las informaciones.

El sistema de control de acceso comprende unos terminales 2 (de los que solo uno es visible en la figura) dispuestos en el domicilio de cada usuario y una tarjeta de circuito integrado 3, distribuida a cada usuario. Claves de desciframiento de las señales cifradas transitan por la red 1, y datos personales del usuario son memorizados en el circuito integrado de la tarjeta de circuito 3 (estas claves están destinadas a ser utilizadas para reconstituir las señales cifradas o entremezcladas, de tal manera que se hagan aprovechables las informaciones representadas por estas señales, por ejemplo, mediante una operación de desciframiento y/o de eliminación del entremezclado).

Cada terminal 2 comprende medios informáticos de mando 4 que comprenden, de forma conocida en sí misma, un microprocesador y una memoria. La memoria contiene un programa de mando 5 que el microprocesador está destinado a ejecutar para garantizar el funcionamiento del terminal 2.

Los medios informáticos de mando 4 están conectados a unos medios de conexión 6 a la red 1. La conexión se realiza por cable.

Los medios informáticos de mando 4 están, además, conectados a un lector 7 destinado a recibir la tarjeta de circuito integrado 3.

De acuerdo con la invención, la memoria de los medios informáticos de mando 4 contiene unos módulos de activación 8, 9, 10 cifrados, destinados a activar al menos una función del terminal 2, y un módulo de desciframiento 11 de los módulos de activación 8, 9, 10 cifrados. Por módulo se entiende un módulo informático, es decir, un

subprograma (o una parte de programa) destinado a ser llamado por el programa de mando 5 para ser ejecutado por el microprocesador de los medios informáticos de mando 4.

El módulo de activación 8 se ha dispuesto para descifrar una señal procedente de la red 1 por medio de una clave de desciframiento contenida en el módulo de activación 8.

El módulo de activación 9 está dispuesto para efectuar una autentificación de la tarjeta de circuito integrado 3 en función de uno de los datos personales contenidos en esta.

El módulo de activación 10 se ha dispuesto para ejecutar una autentificación tal como la que se ha descrito anteriormente en esta memoria, así como un tratamiento de la señal proveniente de la red 1. Este tratamiento consiste, por ejemplo, en efectuar una modificación predeterminada de una característica de la señal.

El módulo de activación 9 cifrado es, aquí, registrado en la memoria de los medios informáticos de mando 4 en el momento de la fabricación del terminal 2, en tanto que los módulos de activación 8 y 10 cifrados han sido cargados a distancia, o telecargados, en la memoria a través de la red 1.

En su modo de funcionamiento clásico o convencional, las señales cifradas o entremezcladas que transitan por la red 1 son reconstituidas por el programa de mando 5 utilizando una clave calculada a partir de las claves contenidas en el circuito integrado de la tarjeta de circuito integrado 3. Las informaciones contenidas en la señal son, entonces, accesibles sin el desciframiento de uno de los módulos 8, 9, 10.

En un primer modo de funcionamiento asegurado de conformidad con la invención, la señal es sometida, previamente a su emisión, a un primer cifrado o entremezclado como en el modo de funcionamiento convencional, tras lo cual al menos una parte de esta señal es sometida a un segundo cifrado. Antes de la emisión de la señal cifrada, el administrador de la red 1 envía por la red 1 la clave de desciframiento del módulo de activación 8 cifrado. La clave de desciframiento del módulo de activación 8 cifrado es entonces transmitida, a través de los medios de conexión 6 y el programa de mando 5, al módulo de desciframiento 11, el cual descifra entonces el módulo de activación 8 cifrado. El módulo de activación 8 descifrado es entonces cargado en una memoria viva del terminal 2, y el microprocesador de los medios informáticos de mando 4 ejecuta el módulo de activación 8 descifrado con el fin de romper el segundo cifrado de la señal procedente de la red 1 por medio de la clave de desciframiento incorporada en el módulo de activación 8. El primer cifrado o entremezclado se le rompe de la misma manera que en el modo de funcionamiento convencional. Tras su utilización, el módulo de activación 8 descifrado es borrado de la memoria viva del terminal.

En un segundo modo de funcionamiento asegurado de conformidad con la invención, el administrador emite por la red 1, previamente a la emisión de la señal, una clave de desciframiento del módulo de activación 9 que es transmitida al módulo de desciframiento 11 con el fin de que este descifre el módulo de activación 9. El módulo de activación 9, una vez descifrado, es ejecutado por el microprocesador y efectúa una autentificación de la tarjeta de circuito integrado 3 en función de las informaciones personales contenidas en esta. Si la tarjeta de circuito integrado 3 es auténtica, la señal es reconstituida de acuerdo con un modo de funcionamiento convencional. Si la tarjeta de circuito integrado 3 no es auténtica, la señal no es reconstituida. El acceso a las informaciones contenidas en la señal está, por tanto, condicionado por el resultado de la autentificación de la tarjeta de circuito integrado 3.

En un tercer modo de funcionamiento asegurado de conformidad con la invención, el administrador emite por la red 1, previamente a la emisión de la señal, una clave de desciframiento del módulo de activación 10 que es transmitida al módulo de desciframiento 11 a través de los medios de conexión 7 y el programa de mando 5 para que el módulo de desciframiento 11 realice un desciframiento del módulo de activación 10. El módulo de activación 10, una vez descifrado, es ejecutado por el microprocesador y efectúa una autentificación de la tarjeta de circuito integrado 3 a partir de las informaciones personales contenidas en esta. Si la tarjeta de circuito integrado 3 es auténtica, el módulo de activación 10 efectúa el tratamiento de la señal y la señal es reconstituida de conformidad con el modo de funcionamiento convencional. Si la tarjeta de circuito integrado 3 no es auténtica, la señal no es tratada. El acceso a las informaciones contenidas en la señal está aquí, por tanto, aún condicionado por el resultado de la autentificación de la tarjeta de circuito integrado 3.

Es posible en todo momento cargar a distancia, o telecargar, otros módulos de activación cifrados en la memoria de los medios informáticos de mando 4.

Por supuesto, la invención no está limitada al modo de realización que se ha descrito y pueden aportársele variantes de realización sin apartarse del ámbito de la invención, tal y como se define por las reivindicaciones.

En particular, la invención es aplicable a cualquier red de transferencia de datos, en particular por cable, por vía hertziana o por satélite (los medios de conexión comprenden entonces una antena de recepción), y utilizable en asociación con cualquier tipo de terminal conectado a una red y, en particular, los terminales de pago. La invención es, más particularmente, aplicable y de interés cuando no hay camino de retorno del terminal hacia la red.

La transmisión de la clave puede realizarse con un cierto retardo (por ejemplo, de algunas horas a algunos días) o inmediatamente antes del uso de la función.

El número de módulos de activación puede ser distinto de tres y la estructura de estos puede ser diferente de la descrita, por ejemplo, para que estos activen o ejecuten más de dos funciones del terminal 2. El módulo de activación puede igualmente ejercer una función permanente de asegurar la continuidad de recepción o de tratamiento de las señales, una función que afecta a un modo normal de funcionamiento del terminal, tal como una función de detención del terminal 2 en caso de fracaso en la autentificación de la tarjeta, o aportar una modificación a una etapa de funcionamiento del terminal (por ejemplo, una corrección del programa de mando).

De la misma manera, la arquitectura del terminal 2 puede ser diferente de la descrita. Los medios informáticos de mando pueden, por ejemplo, comprender tantos módulos de desciframiento como módulos de activación cifrados, estando estos cifrados según algoritmos diferentes.

Los módulos de activación cifrados pueden ser memorizados en cualquier tipo de memoria, como memorias muertas o memorias vivas. Lo mismo es válido para los módulos de activación una vez descifrados.

Los módulos de activación cifrados pueden, igualmente, ser implantados en la tarjeta de circuito integrado (ya sea en el momento de la fabricación, ya sea por carga ulterior en el circuito integrado de la tarjeta), en lugar de ser implantados en el terminal.

Como variante, el módulo informático es memorizado en un soporte adicional de informaciones apto para cooperar con un órgano de lectura correspondiente del terminal. Este soporte adicional de informaciones puede ser, por ejemplo, una tarjeta del tipo de PCMCIA [Asociación Internacional de Tarjetas de Memoria de Computadoras Personales –“Personal Computer Memory Card International Association”].

REIVINDICACIONES

1.- Un sistema de control de acceso a una red (1), que comprende al menos un terminal (2) provisto de un lector (7) de tarjeta de circuito integrado y de medios de conexión (6) a la red, y al menos una tarjeta de circuito integrado (3), configurada para cooperar con el lector, estando el sistema caracterizado por que comprende una memoria que contiene al menos un módulo informático (8, 9, 10) cifrado de activación de al menos una función del terminal, un medio de desciframiento (11) del módulo informático por medio de una clave, y un medio de transmisión (6, 5) de la clave por medio de desciframiento a través de la red, y por que la función que se ha de activar comprende una autentificación de la tarjeta (3) a partir de al menos una información personalizada contenida en el circuito integrado de la tarjeta.

2.- Un sistema de control de acceso de acuerdo con la reivindicación 1, caracterizado por que la función que se ha de activar comprende un tratamiento de una señal proveniente de la red (1).

3.- Un sistema de acuerdo con la reivindicación 2, caracterizado por que el tratamiento comprende un desciframiento de una señal proveniente de la red (1) por medio de una clave incorporada en el módulo informático cifrado.

4.- Un sistema de acuerdo con la reivindicación 1, caracterizado por que la función que se ha de activar afecta a un modo normal de funcionamiento del terminal.

5.- Un procedimiento de control de acceso a una red (1) por medio de un sistema que comprende un terminal (2), provisto de un lector (7) de tarjeta de circuito integrado y de medios de conexión (6) a una red, y al menos una tarjeta de circuito integrado (3), caracterizado por que comprende las etapas de:

- registrar en una memoria del sistema al menos un módulo informático (8, 9, 10) cifrado de activación de al menos una función del terminal,

- transmitir a través de la red una clave a un medio de desciframiento (11) incorporado al sistema,

- descifrar el módulo informático con el fin de activar la función del terminal,

y por que la función que se ha de activar comprende una autentificación de la tarjeta (3) a partir de al menos una información personalizada contenida en el circuito integrado de la tarjeta.

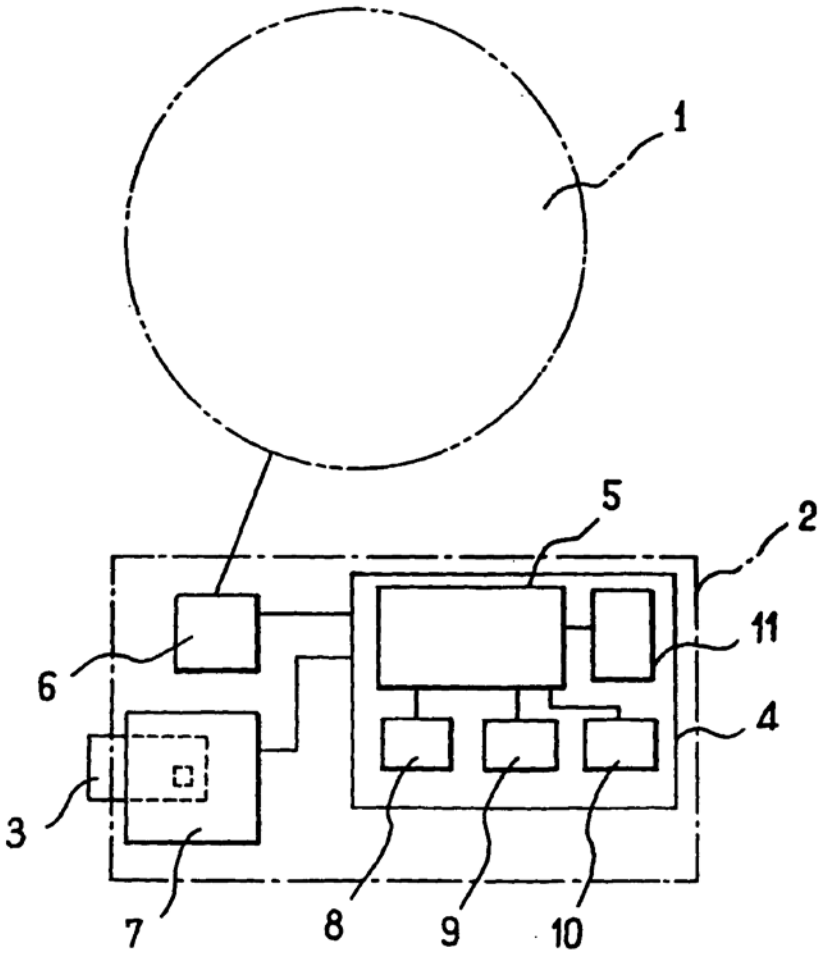
6.- Un procedimiento de acuerdo con la reivindicación 5, caracterizado por que el módulo informático (8, 9, 10) es cargado a distancia, o telecargado, en la memoria a través de la red (1).

7.- Un procedimiento de acuerdo con la reivindicación 5, caracterizado por que el módulo informático (8, 9, 10) es registrado en la memoria previamente a la utilización del sistema.

8.- Un procedimiento de acuerdo con la reivindicación 5, caracterizado por que el módulo informático es memorizado en un soporte adicional de informaciones apto para cooperar con un órgano de lectura correspondiente del terminal.

9.- Un procedimiento de acuerdo con una cualquiera de las reivindicaciones 5 a 8, caracterizado por que la transmisión de la clave a través de la red se realiza inmediatamente antes de una utilización de la función.

10.- Un procedimiento de acuerdo con una cualquiera de las reivindicaciones 5 a 9, caracterizado por que el módulo informático, una vez descifrado, es registrado en una memoria viva del terminal para ser ejecutado.


1
5
2
11
6
4
3
7
8
9
10