(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 373 476**

(51) Int. CI.:
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08011848 .2**
(96) Fecha de presentación: **01.07.2008**
(97) Número de publicación de la solicitud: **2152033**
(97) Fecha de publicación de la solicitud: **10.02.2010**

(54) Título: **PROCEDIMIENTO Y DISPOSITIVO DE GENERACIÓN DE UNA CONTRASEÑA DEPENDIENTE DE LA HORA.**

(45) Fecha de publicación de la mención BOPI:
03.02.2012

(45) Fecha de la publicación del folleto de la patente:
03.02.2012

(73) Titular/es:
VODAFONE HOLDING GMBH
MANNESMANNUFER 2
40213 DÜSSELDORF, DE

(72) Inventor/es:
Moutarazak, Said y
Koraichi, Najib

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Procedimiento y dispositivo de generación de una contraseña dependiente de la hora

Campo técnico

La presente invención versa acerca de la generación de contraseñas dependientes de la hora, particularmente acerca de la generación de contraseñas de un solo uso sincronizadas con la hora. Más específicamente, la invención versa acerca de un procedimiento de generación de una contraseña dependiente de la hora en un dispositivo de comunicaciones móviles. La invención versa, además, acerca de un dispositivo para generar una contraseña dependiente de la hora en un dispositivo de comunicaciones móviles y acerca de un dispositivo de comunicaciones móviles que comprende el dispositivo.

Antecedentes de la invención

Las contraseñas estáticas convencionales corren el riesgo de que sean descubiertas por terceros no autorizados. La protección contra el acceso no autorizado a recursos restringidos puede mejorar con el uso de lo que se denomina contraseñas de un solo uso (OTP), que son válidas una sola vez. Un mecanismo de OTP, denominado a menudo OTP del tipo sincronizado con la hora, implica información horaria sincronizada para generar y validar las OTP. A intervalos temporales regulares, como, por ejemplo, cada minuto, un dispositivo de seguridad o una aplicación, denominada a menudo “testigo”, genera una nueva OTP a partir de la información horaria de ese momento y una nueva clave secreta asignada al usuario. Para validar la OTP, un puesto de autorización regenera la OTP en base a la clave secreta y a su propia información horaria usando el mismo algoritmo que el testigo y compara la contraseña autogenerada con la contraseña generada por el testigo.

En el entorno de la OTP descrito anteriormente, la información horaria usada en el testigo y la información horaria usada en la estación de autorización tienen que estar bien sincronizadas. Sin embargo, en los entornos de la OTP se permiten ciertas desviaciones, lo que significa que la estación de autorización acepta OTP generadas y basadas en información horaria que difiere de esa hora de la estación de autorización en una desviación temporal predefinida. Las desviaciones típicas permitidas pueden estar en el intervalo, por ejemplo, de uno o varios minutos.

El testigo puede ser un sistema de soporte físico cerrado resistente a alteraciones dedicado a la generación de OTP que guarde la clave secreta del usuario y que normalmente tiene un reloj incorporado para proporcionar información horaria. Como alternativa, el testigo puede estar configurado como lo que se denomina “testigo blando”, que es una aplicación de soporte lógico ejecutada en un procesador de uso general.

La solicitud de patente internacional WO 2007/126227 describe un dispositivo de comunicaciones móviles, como, por ejemplo, un teléfono móvil o una PDA (agenda electrónica) o similar, que tiene una interfaz para aceptar un chip de IC (IC: circuito integrado) para generar OTP del tipo sincronizado con la hora. El chip de IC guarda la clave secreta del usuario y comprende un módulo para generar las OTP. La información horaria es proporcionada por una estación base y recibida por la unidad procesadora de radiofrecuencia del dispositivo de comunicaciones móviles.

El chip de IC permite la implementación del testigo para generar OTP del tipo sincronizado con la hora en un dispositivo de comunicaciones móviles. Una señal horaria externa proporciona la información horaria para generar las OTP, de modo que puede evitarse un reloj especial para este fin. Sin embargo, la información horaria está disponible únicamente si el dispositivo de comunicaciones móviles está conectado a la estación base. Esto significa que la generación de OTP no es posible si el dispositivo de comunicaciones móviles no puede conectarse a la estación base.

En el dispositivo de comunicaciones móviles descrito en el documento WO 2007/062787 A1, la identidad, dependiente de la hora, del cliente se determina usando información horaria en un dispositivo de comunicaciones móviles, que está sincronizado con una información horaria en una red de comunicaciones móviles. Cuando el dispositivo de comunicaciones móviles está fuera de la cobertura de la red, se usa la información horaria local en el dispositivo de comunicaciones móviles junto con los cambios temporales objeto de seguimiento para calcular una identidad del cliente.

El dispositivo de comunicaciones móviles dado a conocer en el documento EP 1 833 219 A1 comprende una aplicación para calcular OTP usando la hora actual y un testigo numérico, que es proporcionado por medio de una red de comunicaciones móviles. In una operación fuera de la red, se usa un testigo numérico almacenado si no ha expirado.

Resumen de la invención

Es un objeto de la presente invención permitir la generación de OTP del tipo sincronizado con la hora en un dispositivo que tiene acceso a una señal horaria externa cuando el dispositivo no puede recibir la señal horaria externa.

El objeto se logra por medio de un procedimiento que comprende las características de la reivindicación 1 y por un dispositivo que comprende las características de la reivindicación 12. Las realizaciones del procedimiento y del dispositivo se dan en las reivindicaciones dependientes.

Según un primer aspecto de la invención, se propone un procedimiento del tipo descrito anteriormente que comprende las siguientes etapas:

– comprobar si el dispositivo de seguridad tiene acceso a una señal horaria externa;

– solicitar a un usuario del dispositivo de seguridad que introduzca información horaria si se determina que el dispositivo de seguridad no tiene ningún acceso a la señal horaria externa; y

– generar una contraseña dependiente de la hora usando la información horaria introducida en respuesta a la solicitud.

Según un segundo aspecto, la invención propone un dispositivo para generar una contraseña dependiente de la hora usando información horaria. El dispositivo comprende:

– un medio de comprobación para comprobar si es accesible una señal horaria externa;

– un medio para solicitar a un usuario que introduzca información horaria si el medio de comprobación determina que la señal horaria externa no es accesible; y

– un medio de cálculo para generar una contraseña dependiente de la hora usando la información horaria introducida en respuesta a la solicitud.

La invención tiene la ventaja de que puede generarse una contraseña dependiente de la hora en ausencia de la señal horaria externa. Esto se logra permitiendo que el usuario del dispositivo de seguridad especifique la información horaria necesaria para generar una contraseña dependiente de la hora si no se recibe ninguna señal horaria externa en el dispositivo de comunicaciones móviles.

Permitiendo que el usuario introduzca la información horaria, la invención contradice la opinión habitual de que el mecanismo para generar la información horaria necesaria para calcular contraseñas dependientes de la hora es un componente sensible de la generación de contraseñas que tiene que ser protegido contra el acceso del usuario. En particular, se ha descubierto que la posibilidad de generar una contraseña dependiente de la hora en base a la información horaria proporcionada por el usuario es muy útil para salvar una ausencia temporal de una señal horaria externa.

Sin embargo, si la señal horaria externa puede ser recibida en el dispositivo de seguridad, puede usarse la señal horaria para generar la contraseña dependiente de la hora. Esto tiene la ventaja de que se reduce el riesgo de un uso indebido fraudulento.

Por lo tanto, en una realización del procedimiento y el dispositivo, la contraseña dependiente de la hora se genera usando la señal horaria externa si se determina que el dispositivo de seguridad tiene acceso a la señal horaria externa.

La información horaria usada para generar la contraseña dependiente de la hora tiene que estar sincronizada con la información horaria usada por la estación de autorización. Sin embargo, el usuario puede estar en una zona horaria diferente a la zona horaria en la que está situada la estación de autorización. En este caso, si el usuario ha introducido su hora local, la contraseña generada sería inválida debido a la diferencia horaria con respecto a la ubicación de la estación de autorización.

Por lo tanto, en una realización del procedimiento y el dispositivo, se solicita del usuario que especifique una zona horaria a la que se refiere la información horaria introducida, la información horaria introducida por el usuario es convertida a la zona horaria de un puesto de autorización para validar la contraseña y se genera la contraseña dependiente de la hora usando la información horaria convertida.

En una realización adicional del procedimiento y el dispositivo, se solicita del usuario que introduzca un código de autenticación y la información horaria introducida se usa únicamente para generar una contraseña dependiente de la hora si se ha validado con éxito el código de autenticación.

Esto evita que terceros que no dispongan del código de autenticación generen una contraseña y hagan un uso fraudulento de ella. En particular, se impide que terceros no autorizados generen y usen una contraseña que sea válida en un punto futuro en el tiempo.

Además, una realización del procedimiento y del dispositivo comprende las etapas de:

– almacenar la información horaria introducida;

– determinar que el dispositivo de seguridad tiene acceso a la señal horaria externa;

– comprobar si la información horaria introducida se refiere a un punto futuro en el tiempo con respecto a la señal horaria externa recibida en ese momento; e

– iniciar una rutina de alarma si la información horaria introducida se refiere a un punto futuro en el tiempo con respecto a la señal horaria externa recibida en ese momento.

Esto proporciona seguridad contra un ataque basado en la generación antes mencionada de una contraseña que sea válida en un punto futuro en el tiempo.

Para evitar que un atacante obtenga acceso no autorizado usando tal contraseña, en una realización del procedimiento y el dispositivo, la contraseña generada usando la información horaria introducida es marcada como inválida en la estación de autorización en respuesta al inicio de la rutina de alarma.

En una realización adicional del procedimiento y el dispositivo, se solicita que el usuario introduzca una clave secreta asignada al usuario y la contraseña dependiente de la hora se genera usando la clave secreta introducida por el usuario.

Además, en una realización del procedimiento y el dispositivo, la contraseña dependiente de la hora generada es mostrada en el dispositivo de seguridad y/o la contraseña dependiente de la hora es transmitida desde el dispositivo de seguridad al puesto de autorización por medio de una red de datos a la cual está conectado el dispositivo de seguridad.

En una realización del procedimiento, un dispositivo de comunicaciones móviles comprende el dispositivo de seguridad.

Usar un dispositivo de comunicaciones móviles que comprende un dispositivo de seguridad para la generación de la contraseña dependiente de la hora aumenta la comodidad del usuario, dado que un usuario que porte normalmente un dispositivo de comunicaciones móviles no precisa un dispositivo adicional para generar la contraseña dependiente de la hora.

En una realización del procedimiento y el dispositivo, la señal horaria externa puede ser proporcionada por la red de comunicaciones a la que puede estar conectado el dispositivo de seguridad: Por lo tanto, comprobar en esta realización si el dispositivo de seguridad tiene acceso a la señal horaria externa comprende la comprobación de si el dispositivo de seguridad está conectado a una red de comunicaciones que proporcione la señal horaria externa.

Proporcionar la señal horaria externa en la red de comunicaciones tiene la ventaja de que no se precisa ningún equipo adicional para acceder a la señal horaria si un dispositivo de comunicaciones móviles comprende el dispositivo de seguridad, dado que el dispositivo de comunicaciones móviles normalmente tiene todos los componentes para conectarse con una red de comunicaciones.

En una realización de la invención, el dispositivo es una tarjeta inteligente que puede ser conectada a un dispositivo de comunicaciones móviles.

Es una ventaja de esta realización que el dispositivo pueda ser proporcionado fácilmente al usuario en forma de tarjeta inteligente, que es conectable a su dispositivo de comunicaciones móviles. El uso de un dispositivo de comunicaciones móviles para generar la contraseña dependiente de la hora es especialmente conveniente para el usuario, debido a las razones descritas anteriormente. Una ventaja adicional de esta realización es que el mecanismo de seguridad de la tarjeta inteligente impide el uso fraudulento del dispositivo.

En la comunicación móvil se usan las tarjetas inteligentes para identificar y autenticar a un usuario ante una red de comunicaciones móviles. Ventajosamente, tales tarjetas inteligentes también puede alojar al dispositivo según la invención. Por lo tanto, en una realización de la invención, la tarjeta inteligente comprende un módulo de identificación del abonado para identificar y/o autenticar a un usuario ante una red de comunicaciones móviles.

Además, la invención proporciona un programa de ordenador que comprende porciones de código de soporte lógico para llevar a cabo un procedimiento del tipo descrito en lo que antecede cuando se ejecuta el programa de ordenador en un procesador.

Además, la invención propone un dispositivo de comunicaciones móviles capaz de comprender un dispositivo del tipo anterior.

Estos y otros aspectos de la invención resultarán evidentes y serán esclarecidos con referencia referencia a las realizaciones descritas en lo sucesivo en el presente documento haciendo referencia a los dibujos adjuntos.

Breve descripción de los dibujos

En los dibujos,

la Fig. 1 es un diagrama esquemático de bloques que muestra un dispositivo de comunicaciones móviles para generar OTP del tipo de sincronización horaria, y

la Fig. 2 es un diagrama esquemático de flujo que ilustra un procedimiento para proporcionar información para generar las OTP del tipo de sincronización horaria.

Descripción detallada de las realizaciones de la invención

La Figura 1 muestra un dispositivo 101 de comunicaciones móviles que puede ser conectado a una red 102 de comunicaciones móviles (PLMN: Red Pública de Radiotelefonía Móvil), que puede ser configurada, por ejemplo, según el estándar GSM o el UMTS (GSM: Sistema Global para Comunicaciones Móviles; UMTS: Sistema Universal de Telecomunicaciones Móviles). Para conectar el dispositivo 101 de comunicaciones móviles a la PLMN 102, el dispositivo 101 de comunicaciones móviles comprende una interfaz 103 de radio. La interfaz 103 de radio está acoplada a un procesador principal 104 para controlar la operación del dispositivo 101 de comunicaciones móviles. Para interactuar con el usuario móvil, el dispositivo 101 de comunicaciones móviles comprende un componente 105 de entrada y un componente 106 de visualización, estando acoplados ambos con el procesador principal 104. Las aplicaciones son ejecutadas por el procesador principal 104 y los datos de referencia son almacenados en un componente 107 de memoria al que tiene acceso el procesador principal 104.

El dispositivo 101 de comunicaciones móviles interactúa con una tarjeta inteligente 108, que está insertada en una unidad lectora 114 de tarjetas del dispositivo 101 de comunicaciones móviles. La tarjeta inteligente 108 incluye un microprocesador 109 y una memoria 110 y comprende un módulo de identificación del abonado asignado al usuario del dispositivo 101 de comunicaciones móviles. En particular, el módulo de identificación del abonado incluye información para identificar y autenticar al usuario móvil ante la PLMN 102 y proporciona funcionalidad para acceder a servicios de la PLMN 102. El módulo de identificación del abonado puede ser configurado según el tipo de la PLMN 102. Si la PLMN 102 es una red GSM o UMTS, el módulo de identificación del abonado es un módulo de identidad de abonado (SIM) según el estándar GSM o un módulo universal de identidad de abonado (USIM) según el estándar UMTS.

El usuario móvil tiene la autorización de acceder a un recurso restringido. En una realización, el recurso puede ser una aplicación web o un servicio web alojado en un servidor 113 de red que está conectado a una red 112 de datos. El acceso al recurso es controlador por un puesto 111 de autorización, que deniega el acceso al recurso a no ser que el usuario se identifique y se autentique con éxito. El servidor 113 de red puede comprender la estación 111 de autorización, o la estación 111 de autorización puede residir en otro servidor de red. En la realización representada en la Figura 2, el servidor 113 de red está conectado a la red 112 de datos a través de la estación 111 de autorización. Sin embargo, son posibles otras arquitecturas de red.

La estación 111 de autorización efectúa la autorización del usuario usando OTP sincronizadas con la hora. Esto garantiza un nivel de seguridad relativamente elevado del control de acceso. Así, la aplicación web puede ser, por ejemplo, una aplicación de pago, que tiene que estar protegida de manera eficientemente contra un acceso no autorizado por parte de terceros.

Para generar OTP sincronizadas con la hora, el dispositivo 101 de comunicaciones móviles comprende una aplicación de OTP. La aplicación de OTP puede estar residente en el terminal móvil y ser ejecutada en el procesador principal 104 del dispositivo 101 de comunicaciones móviles. En una realización diferente, la aplicación de OTP puede estar residente en la tarjeta inteligente 108 que incluye el módulo de identificación del abonado. En esta realización, la aplicación de OTP está almacenada en la memoria 110 y es ejecutada en el microprocesador 109 de la tarjeta inteligente 108. Esto tiene la ventaja de que la aplicación de OTP está protegida contra el acceso no autorizado por medio del mecanismo de seguridad de la tarjeta inteligente 108. En realizaciones adicionales, puede estar conectado al terminal móvil un chip de OTP que incluye la aplicación de OTP.

El dispositivo 101 de comunicaciones móviles puede estar conectado a la red 112 de datos por medio de una tecnología de acceso, como, por ejemplo, una conexión WLAN. En la Figura 1, esto se ilustra esquemáticamente por medio de la flecha 115. En esta arquitectura, el usuario móvil puede acceder al servidor 113 de red usando el dispositivo 101 de comunicaciones móviles y las OTP generadas en el dispositivo 101 de comunicaciones móviles puede ser transmitidas electrónicamente desde el dispositivo 101 de comunicaciones móviles al puesto 111 de autorización. Además, la PLMN 102 puede estar acoplada a la red 112 de datos, de modo que el dispositivo 101 de comunicaciones móviles pueda estar conectado a la red de datos a través de la PLMN 102 si está dado de alta en la PLMN 102.

En otra realización, el usuario móvil acceder al servidor 113 de red usando un dispositivo adicional conectado a la red 112 de datos, tal como, por ejemplo, un ordenador personal. En este caso, la aplicación de OTP da salida a contraseñas generadas en el dispositivo 101 de comunicaciones móviles. El usuario lee la contraseña generada en

el componente 106 de visualización del dispositivo 101 de comunicaciones móviles e introduce la contraseña en el dispositivo usado para acceder al servidor 113 de la red.

La aplicación de OTP proporciona una interfaz gráfica de usuario en el componente 106 de visualización del dispositivo 101 de comunicaciones móviles para representar salidas al usuario y para presentar solicitudes de entrada al usuario. Además, la aplicación de OTP está configurada para recibir entradas del usuario desde el componente 105 de entrada del dispositivo 101 de comunicaciones móviles. Si la aplicación de OTP reside en la tarjeta inteligente 108, la aplicación de OTP puede acceder a las funcionalidades del dispositivo 101 de comunicaciones móviles usando instrucciones del Juego de Herramientas SIM que, en general, resulta conocido para un experto en la técnica.

Para generar OTP sincronizadas con la hora, se implementa un algoritmo en la aplicación de OTP que se usa para calcular OTP en base a la información horaria y una clave secreta asignada al usuario. La clave secreta puede ser, por ejemplo, un número de identificación personal (PIN). La clave secreta puede ser introducida por el usuario cuando arranca la aplicación de OTP o cuando el usuario solicita la generación de una contraseña. De forma similar, es posible que la clave secreta esté almacenada de forma segura en el dispositivo 101 de comunicaciones móviles, en particular en la tarjeta inteligente 108. En esta realización, la generación de una contraseña puede resultar posible después de que un código de autorización introducido por el usuario haya sido validado con éxito por la aplicación de OTP. El código de autorización puede ser otro PIN y difiere de la clave secreta asignada al usuario porque la clave secreta se usa para calcular las contraseñas, mientras que el código de autorización se usa para desbloquear la generación de contraseñas. Proteger una aplicación de OTP con un código de autorización para desbloquear la generación de contraseñas tiene la ventaja de que un atacante tiene que usar el dispositivo 101 de comunicaciones móviles para generar las contraseñas del usuario, dado que la clave secreta está protegida contra el acceso dentro del dispositivo 101 de comunicaciones móviles.

Para validar la contraseña generada por la aplicación de OTP, la estación 111 de autorización recalcula las contraseñas usando la clave secreta del usuario, que también está almacenada en la estación 111 de autorización, y su propia información horaria. La información horaria usada por la aplicación de OTP y la información horaria presente en la estación 111 de autorización tienen que estar sincronizadas con la suficiente precisión. Normalmente, la estación 111 de autorización permite la generación de contraseñas calculadas usando una información horaria con una desviación predeterminada con respecto a la información horaria presente y la estación 111 de autorización. Con este fin, la estación 111 de autorización determina que la contraseña es válida si se calcula usando un instante de un intervalo temporal predeterminado en torno a la hora actual de la estación 111 de autorización. El intervalo temporal puede estar entre 1 y 15 minutos, preferentemente entre 2 y 4 minutos.

La aplicación de OTP recupera de la PLMN 102 la información horaria necesaria para generar las OTP sincronizadas con la hora. Para este fin, la PLMN 102 incluye un servicio suplementario que proporciona una señal horaria. Se puede acceder al servicio usando instrucciones USSD (USSD: Datos No Estructurados de Servicio Suplementario) que son, en general, conocidas para un experto en la técnica en su conjunto. Sin embargo, recuperar la información horaria de la PLMN 102 requiere que el dispositivo 101 de comunicaciones móviles esté conectado a la PLMN 102. Esto no siempre es verdad, dado que puede ocurrir que el dispositivo 101 de comunicaciones móviles esté, por ejemplo, fuera de cobertura de la PLMN 102. Por lo tanto, la aplicación OTP solicita que el usuario introduzca información horaria en el dispositivo 101 de comunicaciones móviles en el caso de que no pueda recibirse de la PLMN 102 ninguna información horaria.

En una realización, se implementa para este fin en la aplicación de OTP un procedimiento representado esquemáticamente en la Figura 2. Una vez que el usuario ha introducido su clave secreta o su código de autorización en la etapa 201, la aplicación de OTP envía una instrucción para recuperar la información horaria de la PLMN 102 en la etapa 202. Se pasa la instrucción a la interfaz 103 de radio del dispositivo 101 de comunicaciones móviles, que transmite la instrucción a la PLMN 102 si el dispositivo 101 de comunicaciones móviles está conectado a la PLMN 102. Después de haber pasado la instrucción a la interfaz 103 de radio, la aplicación de OTP comprueba si se da respuesta a la instrucción dentro de un intervalo temporal predeterminado en la etapa 203. Esto significa que la aplicación de OTP comprueba si se recibe la señal horaria durante el intervalo temporal. Si se recibe a tiempo la señal horaria, la aplicación de OTP calcula una contraseña en base a la información horaria recibida y la clave secreta del usuario en la etapa 204.

Si la aplicación de OTP determina en la etapa 203 que no se ha recibido ninguna información horaria de la PLMN 102 en el intervalo temporal predeterminado, la aplicación de OTP comprueba si el dispositivo 101 de comunicaciones móviles está conectado a la PLMN 102 en la etapa 205. Esto puede efectuarse comprobando si el dispositivo de comunicaciones móviles recibe una señal predeterminada de datos emitida en la PLMN 102, como, por ejemplo, una señal que identifique a la PLMN 102. Si se determina en la etapa 205 que el dispositivo 101 de comunicaciones móviles está dado de alta en la PLMN 102, la aplicación de OTP vuelve, preferentemente, a la etapa 202 y vuelve a enviar la instrucción para recuperar la información horaria. Sin embargo, si se determina en la etapa 205 que el dispositivo 101 de comunicaciones móviles no está conectado a la PLMN 102, la aplicación de OTP solicita al usuario que introduzca información horaria en el dispositivo 101 de comunicaciones móviles.

Después de haber recibido la entrada del usuario, la aplicación de OTP calcula una contraseña usando la información horaria especificada por el usuario en la etapa 204.

Para solicitar al usuario que introduzca la información horaria, la interfaz de usuario de la aplicación de OTP presentada en el componente 106 de visualización del dispositivo de comunicaciones móviles puede proporcionar un campo de entrada, que puede ser cumplimentado por el usuario usando el componente 105 de entrada del dispositivo 101 de comunicaciones móviles. El usuario puede recibir la información horaria de cualquier fuente disponible. Esta puede ser, por ejemplo, su reloj de pulsera o un reloj público en las inmediaciones de su posición.

Para que la contraseña calculada sea válida, la contraseña tiene que ser calculada usando la información horaria presente en la estación 111 de autorización. En particular, esto significa que la información horaria usada para el cálculo debería referirse a la misma zona horaria que la información horaria de la estación 111 de autorización. Por lo tanto, en una realización, se pide al usuario que introduzca una información horaria referente a la zona horaria de la estación 111 de autorización en la etapa 206. Esto requiere conocimiento de la zona horaria de la estación 111 de autorización y sobre la diferencia horaria entre esta zona horaria y la zona horaria actual del usuario.

En otra realización, se solicita del usuario que introduzca su hora local y que especifique su zona horaria actual. Para la especificación de la zona horaria puede presentarse al usuario una lista de las zonas horarias existentes, de modo que el usuario pueda especificar su zona horaria eligiéndola de la lista. Usando la información horaria introducida por el usuario y la información sobre la zona horaria a la que se refiere la información horaria, la aplicación de OTP calcula la hora local de la estación 111 de autorización y usa esta hora calculada para generar la contraseña en la etapa 204.

Para impedir que un atacante use el dispositivo 101 de comunicaciones móviles para generar una contraseña que sea válida en el futuro introduciendo información horaria relativa a un punto futuro en el tiempo, la introducción de la información horaria por el usuario puede ser protegida por un código de autorización. Esto significa que la aplicación de OTP solicita que el usuario introduzca el código de autorización además de la información horaria. El código de autorización también está almacenado de forma segura en el dispositivo 101 de comunicaciones móviles, particularmente en la tarjeta inteligente 108. En esta realización, la aplicación de OTP valida el código de autorización antes de generar una contraseña usando la información temporal dada por el usuario.

Además, en una realización, la aplicación de OTP almacena, al menos, la información horaria cuando calcula y da salida a una contraseña en base a la información horaria especificada por el usuario. En particular, la información horaria puede ser almacenada de forma segura en la tarjeta inteligente 108. Después de haber guardado la información horaria, la aplicación de OTP monitoriza si el dispositivo 101 de comunicaciones móviles vuelve a conectarse a la PLMN 102. Esto puede realizarse enviando instrucciones para recuperar la información horaria de la PLMN 102 o comprobando, a intervalos temporales regulares, si el dispositivo 101 de comunicaciones móviles recibe una señal predeterminada de datos emitida en la PLMN 102. De nuevo, esta señal de datos puede ser una señal que identifique a la PLMN 102 que es emitida en la PLMN a intervalos temporales regulares.

Si la aplicación de OTP determina que el dispositivo 101 de comunicaciones móviles vuelve a conectarse a la PLMN 102, la aplicación de OTP comprueba si la información horaria usada para calcular la contraseña se refiere a un punto futuro en el tiempo. Si esto es así, se pone en marcha una rutina de alarma, dado que, en este caso, un atacante podría haber generado la contraseña para un uso fraudulento en el futuro. Para la comprobación mencionada, la aplicación de OTP compara la información horaria recuperada en ese momento de la PLMN 102 y la información horaria almacenada. Si se determina que la información horaria almacenada se refería al futuro en relación con la información horaria recibida en ese momento, la aplicación de OTP pone en marcha la rutina de alarma.

La rutina de alarma puede comprender informar al usuario que se ha generado una contraseña para un punto futuro en el tiempo. Si el usuario juzga que la contraseña podría haber sido generada para un uso fraudulento, puede informar a la estación 111 de autorización. En otra realización, la aplicación de OTP puede informar a la estación 111 de autorización automáticamente. Con este fin, la aplicación de OTP puede generar un mensaje correspondiente que especifique la información horaria en cuestión y si la aplicación de OTP puede controlar el dispositivo 101 de comunicaciones móviles para transmitir el mensaje a la estación 111 de autorización. El mensaje puede ser transmitido a la estación 111 de autorización a través de la PLMN 102 o a través de otra conexión de datos entre el dispositivo 101 de comunicaciones móviles y la estación 111 de autorización.

Después de que haya sido informada del posible uso indebido, la estación 111 de autorización puede emprender acciones para evitar un acceso no autorizado al servidor 113 de red usando la contraseña en cuestión. Esto puede realizarse bloqueando el acceso al servidor 113 de red con esta contraseña. En particular, la contraseña generada para el punto futuro en el tiempo puede ser marcada como inválida, de modo que la contraseña no pueda ser usada como autorización para acceder al servidor 113 de red.

Aunque la invención ha sido ilustrada y descrita con detalle en los dibujos y la descripción precedente, tal ilustración y tal descripción deben ser consideradas ilustrativas o ejemplares y no restrictivas; la invención no está limitada a las realizaciones dadas a conocer. En particular, la invención no está limitada a la descarga de una aplicación o código

de programa a una tarjeta inteligente 106. Un experto en la técnica reconoce que pueden descargarse a la tarjeta inteligente 106 otros datos de la misma manera que se ha descrito anteriormente en conexión con la descarga de un código de programa de una aplicación. En la puesta en práctica de la invención reivindicada, a partir de un estudio de los dibujos, la revelación y las reivindicaciones adjuntas, los expertos en la técnica pueden entender y efectuar otras variaciones a las realizaciones dadas a conocer.

En las reivindicaciones, la palabra “comprende” no excluye otros elementos ni etapas y el artículo indefinido “un” o “una” no excluye una pluralidad. Un único procesador u otra unidad pueden cumplir las funciones de varios elementos enumerados en las reivindicaciones. Un programa de ordenador puede ser almacenado/distribuido sobre un medio adecuado, como uno medio de almacenamiento óptico o un medio en estado sólido suministrado junto con otro soporte físico o como parte del mismo, pero también puede ser distribuido de otras formas, como a través de Internet o de otros sistemas de telecomunicaciones alámbricos o inalámbricos. No debe interpretarse que cualquier signo de referencia en las reivindicaciones limite el alcance.

REIVINDICACIONES

1. Un procedimiento para generar una contraseña dependiente de la hora en un dispositivo (101; 108) de seguridad usando información horaria, comprendiendo el procedimiento la comprobación de si el dispositivo de seguridad tiene acceso a una señal horaria externa, **caracterizado porque** el procedimiento comprende, además, las etapas de:

- solicitar a un usuario del dispositivo de seguridad que introduzca información horaria si se determina que el dispositivo de seguridad no tiene ningún acceso a la señal horaria externa; y
- generar una contraseña dependiente de la hora usando la información horaria introducida en respuesta a la solicitud.

2. El procedimiento según la reivindicación 1 en el que la contraseña dependiente de la hora se genera usando la señal horaria externa si se determina que el dispositivo (101; 108) de seguridad no tiene ningún acceso a la señal horaria externa.

3. El procedimiento según una de las reivindicaciones precedentes en el que se solicita que el usuario especifique una zona horaria a la que se refiere la información horaria introducida, en el que la información horaria introducida por el usuario es convertida a la zona horaria de un puesto (111) de autorización para validar la contraseña y en el que la contraseña dependiente de la hora se genera usando la información horaria convertida.

4. El procedimiento según una de las reivindicaciones precedentes en el que se solicita que el usuario introduzca un código de autenticación y en el que la información horaria introducida se usa únicamente para generar una contraseña dependiente de la hora si el código de autenticación ha sido validado con éxito.

5. El procedimiento según una de las reivindicaciones precedentes que, además, comprende las etapas de:

- almacenar la información horaria introducida;
- determinar que el dispositivo (101; 108) de seguridad tiene acceso a la señal horaria externa;
- comprobar si la información horaria introducida se refiere a un punto futuro en el tiempo con respecto a la señal horaria externa recibida en ese momento; e
- iniciar una rutina de alarma si la información horaria introducida se refiere a un punto futuro en el tiempo con respecto a la señal horaria externa recibida en ese momento.

6. El procedimiento según la reivindicación 5 en el que la contraseña generada usando la información horaria introducida es marcada como inválida en la estación (111) de autorización en respuesta al inicio de la rutina de alarma.

7. El procedimiento según una de las reivindicaciones precedentes en el que se solicita que el usuario introduzca una clave secreta asignada al usuario y en el que la contraseña dependiente de la hora se genera usando la clave secreta introducida por el usuario.

8. El procedimiento según una de las reivindicaciones precedentes en el que la contraseña dependiente de la hora generada se muestra en el dispositivo (101; 108) de seguridad y/o en el que la contraseña dependiente de la hora es transmitida desde el dispositivo (101; 108) de seguridad al puesto (111) de autorización por medio de una red de datos a la cual está conectado el dispositivo (101; 108) de seguridad.

9. El procedimiento según una de las reivindicaciones precedentes en el que un dispositivo (101) de comunicaciones móviles comprende el dispositivo (101; 108) de seguridad.

10. El procedimiento según una de las reivindicaciones precedentes en el que la comprobación de si el dispositivo (101; 108) de seguridad tiene acceso a la señal horaria externa comprende la comprobación de si el dispositivo (101; 108) de seguridad está conectado a una red (102) de comunicaciones que proporcione la señal horaria externa.

11. Un programa de ordenador que comprende porciones de código de soporte lógico para llevar a cabo un procedimiento según una de las reivindicaciones precedentes cuando el programa de ordenador es ejecutado en un procesador (104; 109).

12. Un dispositivo (101; 108) para generar una contraseña dependiente de la hora usando información horaria que comprende un medio de comprobación para comprobar si es accesible una señal horaria externa, **caracterizado porque** el dispositivo comprende, además:

- un medio para solicitar a un usuario que introduzca información horaria si el medio de comprobación determina que la señal horaria externa no es accesible; y

- un medio de cálculo para generar una contraseña dependiente de la hora usando la información horaria introducida en respuesta a la solicitud.

13. Un dispositivo (101; 108) según la reivindicación 12 en el que el dispositivo es una tarjeta inteligente (108) que puede ser conectada a un dispositivo (101) de comunicaciones móviles.

14. Un dispositivo (101; 108) según la reivindicación 13 en el que la tarjeta inteligente (108) comprende un módulo de identificación del abonado para identificar y/o autenticar a un usuario antes una red (102) de comunicaciones móviles.

15. Un dispositivo (101) de comunicaciones móviles que comprende un dispositivo (101; 108) según una de las reivindicaciones 12 a 14.

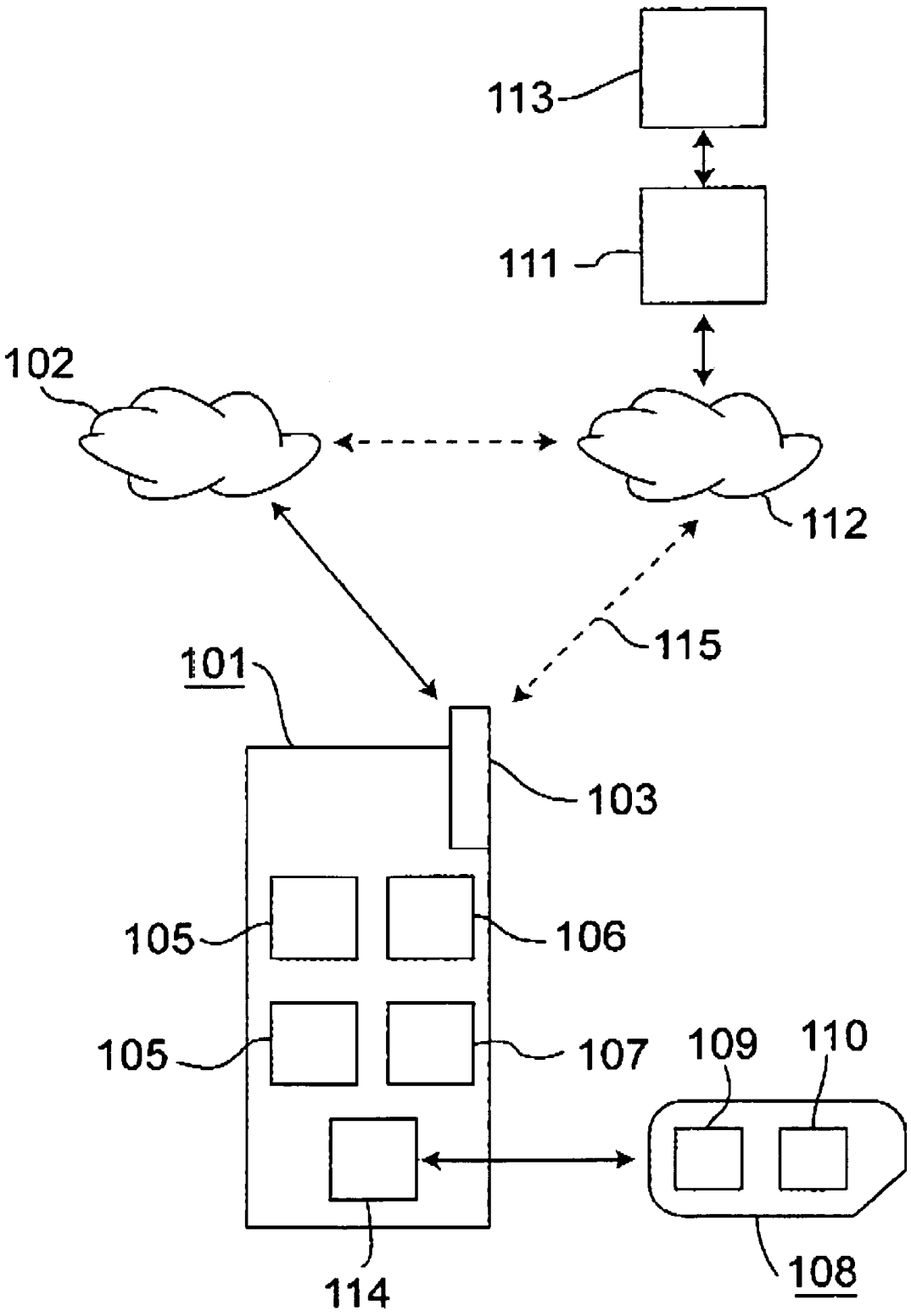

Fig. 1

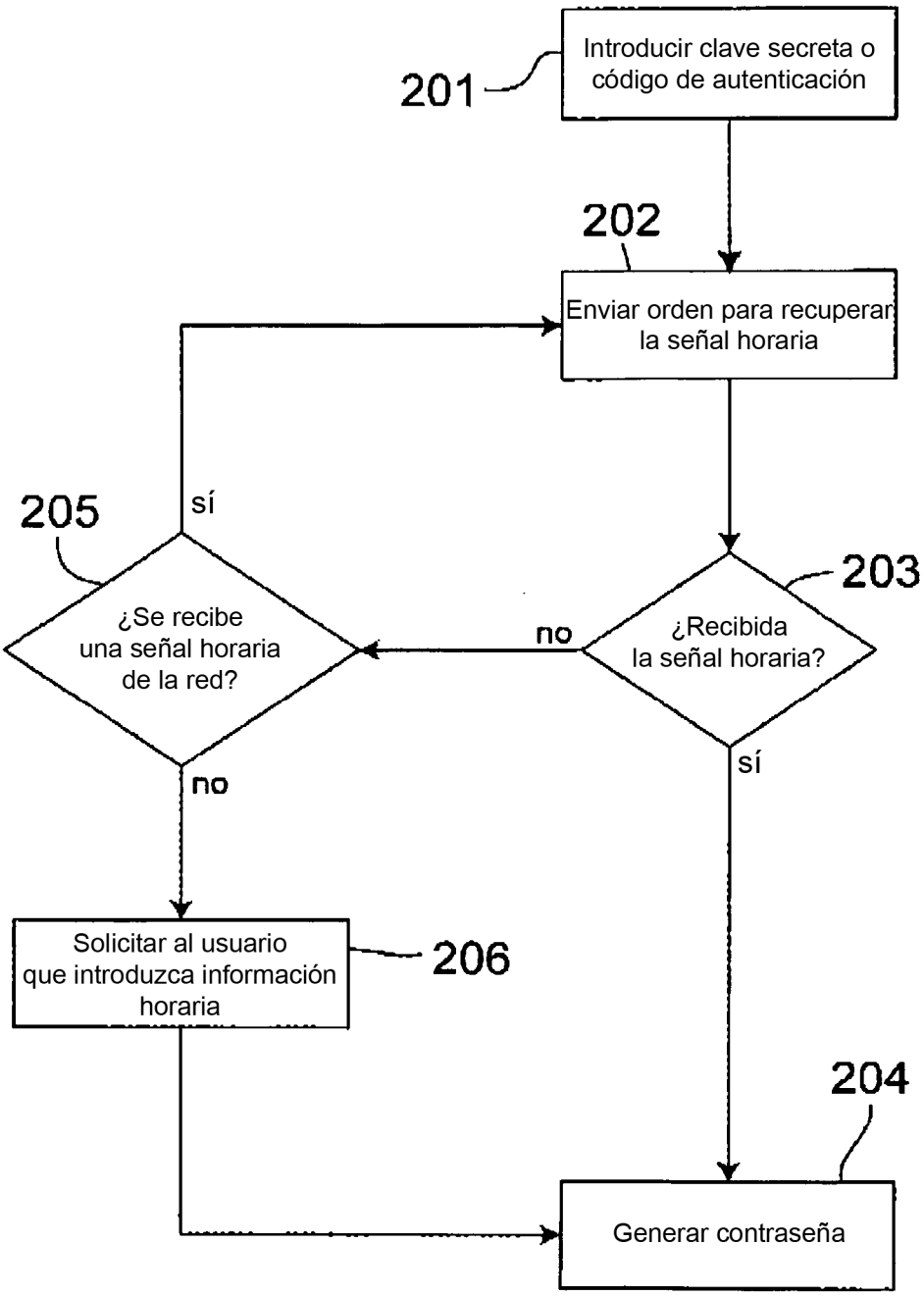
201
Introducir clave secreta o código de autenticación
202
Enviar orden para recuperar la señal horaria
203
¿Recibida la señal horaria?
no
sí
205
¿Se recibe una señal horaria de la red?
sí
no
206
Solicitar al usuario que introduzca información horaria
204
Generar contraseña

Fig. 2