(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 400 165**

(51) Int. CI.:

G11C 16/22 (2006.01)
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.10.2008 E 08017900 (5)**

(97) Fecha y número de publicación de la concesión europea: **12.12.2012 EP 2175455**

(54) Título: **Procedimiento para proporcionar un acceso controlado a una tarjeta de memoria y tarjeta de memoria**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.04.2013

(73) Titular/es:

VODAFONE HOLDING GMBH (100.0%)
MANNESMANNUFER 2
40213 DÜSSELDORF, DE

(72) Inventor/es:

KORAICHI, NAJIB y
HOEKSEL, SEBASTIAAN

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento para proporcionar un acceso controlado a una tarjeta de memoria y tarjeta de memoria

Campo técnico

La presente invención versa acerca de tarjetas de memoria con protección de acceso. Más específicamente, la invención versa acerca de un procedimiento para verificar el acceso a datos guardados de forma segura en tal tarjeta de memoria. Además, la invención versa acerca de una tarjeta de memoria para guardar datos de forma segura.

Antecedentes de la invención

Las tarjetas de memoria son tarjetas de circuitos integrados (IC) que incluyen memoria no volátil y un controlador que controla la operación de la tarjeta de memoria. Tales tarjetas de memoria puede estar conectadas temporalmente a dispositivos anfitriones, tales como, por ejemplo, ordenadores personales (PC), teléfonos celulares, agendas electrónicas (PDA), cámaras digitales, reproductores portátiles de audio y otros dispositivos electrónicos anfitriones para el almacenamiento de datos. Existe una pluralidad de estándares que especifican diferentes tipos de tarjetas de memoria, tales como, por ejemplo, las tarjetas SD (digitales seguras), las tarjetas CF (flash compacta) y MMC (tarjetas multimedia). Un ejemplo adicional de tarjeta de memoria, en el sentido del término usado en el presente documento, es un dispositivo de memoria flash USB (bus serie universal).

Las tarjetas de memoria del tipo descrito anteriormente pueden proporcionar un mecanismo de seguridad para proteger a los datos de un acceso no autorizado. Esto permite guardar datos sensibles en la tarjeta de memoria, tales como, por ejemplo, detalles bancarios del propietario de la tarjeta, datos médicos del propietario de la tarjeta y fotografías personales u otros datos personales.

El propietario de la tarjeta puede acceder a los datos usando una credencial, tal como, por ejemplo, una contraseña. Sin embargo, el usuario puede desear hacer accesibles los datos a otras personas en algunas situaciones. Por ejemplo, el propietario de la tarjeta puede desear permitir a su médico leer datos médicos protegidos guardados en la tarjeta de memoria o poner fotos personales a disposición de un amigo.

El documento WO 2005/039218 da a conocer un procedimiento para proteger datos en un soporte de datos que puede ser conectado a un dispositivo terminal. Con base en condiciones de acceso guardadas en el soporte de datos, una unidad discriminadora del soporte de datos juzga si el dispositivo terminal está o no autorizado a acceder a los datos guardados en el soporte de datos. en particular, las condiciones de acceso incluyen uno o más conjuntos de información de periodos, indicando cada información de periodo un periodo de tiempo disponible para que la persona correspondiente acceda a los datos. En conexión con estas condiciones de acceso, la unidad discriminadora extrae el periodo de tiempo disponible para el acceso y, además, adquiere la información de fecha de una unidad de gestión de fechas. Luego, la unidad discriminadora juzga si la hora actual indicada por la información de los datos está dentro del periodo de tiempo disponible para el acceso. La unidad de gestión de datos está asimismo incluida en el controlador del soporte de datos y gestiona la información de fechas que indica la fecha actual.

Descripción de la invención

Es un objeto de la presente invención permitir que el propietario de una tarjeta de memoria haga accesibles a otra persona los datos protegidos guardados en la tarjeta de memoria.

El objeto se logra mediante un procedimiento según la reivindicación 1 y por medio de una tarjeta de memoria según la reivindicación 9. En las reivindicaciones dependientes se dan realización del procedimiento y de la tarjeta de memoria.

Según un primer aspecto, la invención sugiere un procedimiento para proporcionar acceso a datos guardados de forma segura en una tarjeta de memoria. El procedimiento comprende las siguientes etapas:

- especificar una primera información temporal correspondiente a un periodo de tiempo y guardar la primera información temporal en la tarjeta de memoria;
- insertar la tarjeta de memoria en un terminal;
- determinar en una unidad de control incluida en la tarjeta de memoria si ha expirado el periodo de tiempo; y
- permitir que el terminal acceda a los datos hasta que se determine que el periodo de tiempo ha expirado.

Según un segundo aspecto, la invención sugiere una tarjeta de memoria para guardar datos de forma segura en la misma. La tarjeta de memoria está adaptada para recibir una primera información temporal correspondiente a un periodo de tiempo y para almacenar la primera información temporal. Y la tarjeta de memoria comprende una unidad de control configurada para determinar si ha expirado el periodo de tiempo y para permitir que un terminal acceda a los datos, a no ser que se determine que el periodo de tiempo ha expirado, mientras la tarjeta de memoria está insertada en el terminal.

La invención permite que el propietario de la tarjeta especifique una primera información temporal correspondiente a un periodo de tiempo en el que los datos protegidos guardados en la tarjeta de memoria pueden ser objeto de acceso por una persona por medio de un terminal. El propietario de la tarjeta puede especificar la primera información temporal antes de entregar la tarjeta de memoria a otra persona. Especificando una primera información temporal correspondiente a un periodo de tiempo adecuadamente breve, puede evitarse que terceras personas no autorizadas puedan acceder a los datos protegidos después de que la persona autorizada haya accedido a los datos. Así, el acceso a los datos protegidos puede limitarse de manera segura a personas seleccionadas.

Además, es una ventaja de la invención que pueda permitirse el acceso a los datos protegidos sin tener que proporcionar una credencial, tal como, por ejemplo, una contraseña. En particular, esto facilita el acceso a los datos a otra persona, dado que esta persona no tiene que recibir una credencial para desbloquear la tarjeta de memoria. Además, se garantiza que una persona no pueda acceder a los datos protegidos sin el permiso del propietario de la tarjeta cuando obtiene la tarjeta de memoria una segunda vez. Si se usó una credencial para proteger los datos, una persona, cuando obtiene la tarjeta de memoria una segunda vez, podría usar la credencial que ya recibió junto con la tarjeta en el pasado.

En una realización del procedimiento y el dispositivo, el terminal permite que la unidad de control se conecte con una unidad de reloj dispuesta externa a la tarjeta de memoria y que recupere de la unidad de reloj una segunda información temporal que especifique la hora actual, usándose dicha segunda información temporal para determinar si ha expirado el periodo de tiempo.

Esta realización tiene la ventaja de que la tarjeta de memoria no tiene que incluir una unidad de reloj, de modo que pueda reducirse la complejidad de la tarjeta de memoria.

En una realización adicional del procedimiento y el dispositivo, la unidad de reloj está comprendida en un servidor de red, y la unidad de control se conecta con el servidor de red por medio de una conexión de red proporcionada por el terminal para recuperar la segunda información temporal de la unidad de reloj.

Recuperar la segunda información temporal de un servidor de red tiene la ventaja de que puede usarse información temporal confidencial que se genera fuera de la esfera de influencia de la persona a la que se entrega la tarjeta de memoria. Esto reduce el riesgo de uso fraudulento de la tarjeta de memoria.

Sin embargo, la segunda información temporal recuperada del servidor de red puede ser manipulada indebidamente. Por ejemplo, la segunda información temporal puede ser manipulada durante su transmisión a la tarjeta de memoria o una solicitud de información temporal puede ser redirigida a otro servidor para proporcionar información temporal manipulada.

Para evitar que se manipule indebidamente la segunda información temporal, una realización del procedimiento y de la tarjeta de memoria comprende que la información temporal recuperada de la unidad de reloj comprenda información de autenticación, particularmente una firma digital, que sea verificada en la unidad de control.

En una realización adicional del procedimiento y del dispositivo, la primera información temporal especifica un punto en el tiempo y la unidad de control determina si ha expirado el periodo de tiempo con base en una diferencia horaria entre el punto especificado en el tiempo y la hora actual especificada en la segunda información temporal.

En esta realización el propietario de la tarjeta puede especificar ventajosamente un punto en el tiempo, es decir, una hora absoluta, hasta la que la tarjeta de memoria puede ser objeto de acceso por otra persona que use el terminal. Esto permite que el propietario de la tarjeta controle cuándo la otra persona accede a la tarjeta de memoria. Especificando un punto cercano en el tiempo, el propietario de la tarjeta puede evitar que una persona no autorizada pueda acceder a la tarjeta de memoria después de que la posesión de la tarjeta le sea transferida por la persona autorizada que recibió la tarjeta del propietario de la tarjeta.

En una realización relacionada del procedimiento y del dispositivo, la unidad de control recupera reiteradamente la segunda información temporal de la unidad de reloj mientras la tarjeta de memoria está insertada en el terminal y la unidad de control determina si ha expirado el periodo de tiempo cada vez después de que se haya recuperado la segunda información temporal.

Esto permite la implementación de un mecanismo de seguridad relativamente poco complejo en la tarjeta de memoria, en el que la unidad de control compara reiteradamente la hora actual recuperada con el punto en el tiempo especificado por el propietario de la tarjeta sin tener que llevar a cabo cálculos más complejos.

En una realización alternativa del procedimiento y del dispositivo, la unidad de control determina que el periodo de tiempo ha expirado cuando un contador de tiempos de la tarjeta de memoria indica que la diferencia de tiempo ha expirado, iniciándose dicho contador de tiempos después de que la tarjeta de memoria se haya insertado en el terminal.

Esta realización tiene la ventaja de que la segundo información temporal tiene que ser recuperada solo una vez. En particular, esto reduce el número de accesos al servidor horario de la red para que se reduzcan la carga del servidor y la carga de la red.

Una realización adicional del procedimiento y del dispositivo comprende que la primera información temporal especifique el periodo de tiempo.

Es una ventaja de esta realización que se proporcione una periodo de tiempo definido en el que una persona puede acceder a la tarjeta de memoria por medio del terminal con independencia del punto en el tiempo o de la hora absoluta en que la persona accede a la tarjeta. Así, la persona que accede a la tarjeta de memoria dispone de mayor flexibilidad al elegir el punto en el tiempo para el acceso a la tarjeta.

En una realización relacionada del procedimiento y del dispositivo, la unidad de control determina que el periodo de tiempo ha expirado cuando un contador de tiempos de la tarjeta de memoria indica que el periodo de tiempo ha expirado, iniciándose dicho contador de tiempos después de que la tarjeta de memoria se haya insertado en el terminal.

En una realización alternativa del procedimiento y del dispositivo, la unidad de control guarda la hora especificada en la segunda información temporal cuando recupera la segunda información por vez primera, la unidad de control recupera reiteradamente la segunda información temporal de la unidad de reloj, y la unidad de control determina si ha expirado el periodo de tiempo con base en una comparación del periodo de tiempo y una diferencia de tiempo entre la hora guardada y la hora actual especificada en la segunda información temporal recuperada la última vez.

Es una ventaja de esta realización que la determinación de si ha expirado el periodo de tiempo especificado por el propietario de la tarjeta se realice con base en la segunda información temporal recuperada de la unidad confidencial de reloj. Además, puede prescindirse de un contador de tiempos que se implemente en la tarjeta de memoria.

Según un aspecto adicional de la invención, se proporciona un sistema, comprendiendo el sistema una tarjeta de memoria del tipo antes descrito y comprendiendo, además, un terminal para recibir la tarjeta de memoria.

Los aspectos mencionados anteriormente y otros aspectos de la invención también serán evidentes a partir de las realizaciones descritas en lo que sigue, y esclarecidos con respecto a las mismas, haciendo referencia a los dibujos.

Breve descripción de los dibujos

Ahora se hará referencia, a título de ejemplo, a los dibujos adjuntos, en los que la Fig. 1 es un diagrama esquemático de bloques de un sistema para el control del acceso a datos protegidos guardados en una tarjeta de memoria.

Descripción detallada de realizaciones de la invención

La Figura 1 representa esquemáticamente elementos de un sistema para el control del acceso a datos protegidos guardados en una tarjeta 102 de memoria. En particular, la tarjeta 102 de memoria guarda datos sensibles del propietario de la tarjeta. En el sistema mostrado en la Figura 1, el propietario puede hacer accesibles tales datos a personas autorizadas mientras que se impide que terceras personas no autorizadas accedan a los datos. En principio, los datos pueden ser datos cualesquiera que el propietario quieran compartir con personas seleccionadas. Por ejemplo, los datos son datos médicos del propietario, que el propietario quiere compartir únicamente con un médico. Otro ejemplo son detalles bancarios que el propietario que proporcionar únicamente a personas dignas de confianza. En otro ejemplo adicional, los datos personales se refieren, por ejemplo, a fotos personales que el propietario quiere compartir únicamente con amigos.

La tarjeta 102 de memoria comprende una memoria 104 y un microcontrolador 106 integrados en un alojamiento. El alojamiento puede ser lo bastante pequeño como para que el propietario pueda transportar la tarjeta 102 de memoria fácilmente y para que la tarjeta 102 de memoria también pueda ser usada en conexión con lectores de tarjetas que estén integrados en dispositivos pequeños, tales como, por ejemplo, dispositivos de comunicaciones móviles. Preferentemente, la tarjeta 102 de memoria está configurada según un formato estándar y puede ser una tarjeta SD, una tarjeta CF, una MMC o similar. Otro ejemplo de un formato de tarjeta de memoria en el sentido de esta divulgación es un dispositivo de memoria flash USB. El formato estándar puede especificar en particular el tamaño y la forma de la tarjeta 102 de memoria, la configuración de sus contactos eléctricos y los protocolos de comunicaciones usados en la comunicación con la tarjeta 102 de memoria. La conformidad de la tarjeta 102 de memoria con el estándar permite que la tarjeta sea objeto de acceso por medio de un dispositivo lector de tarjetas que, asimismo, es conforme con el estándar.

La memoria 104 es un almacenamiento no volátil que puede ser borrada y reprogramado eléctricamente. En particular, la memoria 104 puede ser configurada como una unidad de almacenamiento de estado sólido, particularmente una memoria flash o una EEPROM (memoria de solo lectura programable borrable eléctricamente) no flash. Sin embargo, la persona experta en la técnica entiende que, en principio, puede usarse cualquier tipo de dispositivo de memoria. La memoria 104 puede estar constituida por uno o más chips de memoria, que están

dispuestos en el alojamiento de la tarjeta 102 de memoria. El microcontrolador 106 y la memoria 104 pueden residir en un único chip dentro de la tarjeta 102 de memoria o el controlador puede ser un chip separado conectado a la memoria 104.

El microcontrolador 106 proporciona funcionalidad para acceder a la memoria 104 por medio de dispositivos a los que está conectada la tarjeta 102 de memoria. En particular, el microcontrolador 106 implementa los protocolos de comunicaciones usados para el intercambio de datos entre la tarjeta 102 de memoria y un dispositivo conectado.

Al menos la parte del contenido de los datos de la memoria 104 que comprende los datos sensibles del propietario está protegida contra el acceso no autorizado, es decir, la lectura no autorizada, el borrado y la manipulación de los datos protegidos. Para proteger los datos, el microcontrolador 106 proporciona una unidad de control que controla el almacenamiento de datos en la memoria 104 y la recuperación de datos de la misma. Cada tentativa de acceder a los datos protegidos guardados en la memoria 104 es permitida o denegada por la unidad de control. Preferentemente, la unidad de control se implementa como un programa de soporte lógico que se ejecuta en el microcontrolador 106 de la tarjeta 102 de memoria.

Además de los datos protegidos, pueden guardarse en la tarjeta 102 de memoria datos adicionales que no estén protegidos en particular. En relación con los datos protegidos, puede proporcionarse opcionalmente una gestión de grupos. Esto quiere decir que en la tarjeta 102 de memoria se guardan grupos de datos protegidos, pudiendo configurarse diferentes autoridades de acceso para los grupos. Los grupos pueden guardarse en áreas diferentes de la memoria 104 o los ficheros de datos contenidos en los diferentes grupos pueden ser identificados de otra manera. Los grupos se gestionan en la unidad de control. La gestión de grupos permite guardar en la misma tarjeta 102 de memoria datos que el propietario quiere compartir con diferentes personas. Por ejemplo, el propietario puede guardar en la misma tarjeta 102 de memoria datos de salud para compartir con su médico y datos para compartir con sus amigos.

Para acceder a los datos protegidos guardados en la tarjeta 102 de memoria se usa una unidad lectora 108 de tarjetas, que está acoplada a un terminal 110 de la persona que quiere acceder a los datos protegidos. La unidad lectora 108 de tarjetas puede estar integrada en el terminal 110, tal como se representa en la Figura 1, o la unidad lectora 108 de tarjetas puede ser una unidad separada conectada al terminal 110. Mediante una interfaz adecuada, el terminal 110 se conecta a una red 112 de comunicaciones, que conecta el terminal 110 a un servidor horario 116. Preferentemente, la red 112 de comunicaciones es Internet. Sin embargo, la red 112 de comunicaciones también puede ser configurada como otra red que permita un intercambio entre el terminal 110 y el servidor horario 116, tal como, por ejemplo, una red de comunicaciones móviles. Además, puede haber otras redes, no mostradas en la Figura 1, que conecten el terminal 110 a la red 112 de comunicaciones. Si la red 112 de comunicaciones es Internet, el terminal 110 puede conectarse a la misma mediante, por ejemplo, una red de comunicaciones móviles. El terminal 110 puede ser un ordenador personal u otro dispositivo estacionario, incluyendo un terminal estacionario dedicado. Asimismo, es posible que el terminal 110 esté configurado como un dispositivo de mano, que puede ser un dispositivo dedicado o un dispositivo de uso general, tal como, por ejemplo, un dispositivo de comunicaciones móviles.

El servidor horario 116 incluye una unidad de reloj, que mide la hora absoluta actual. Preferentemente, la unidad de reloj proporciona una precisión elevada, con solo pequeñas desviaciones de la hora correcta. Además, el servidor horario 116 está preferentemente protegido, a través de medios adecuados, de ser manipulado indebidamente.

El propietario de la tarjeta 102 de memoria también dispone de un dispositivo 114 que comprende una unidad lectora 118 de tarjetas para recibir la tarjeta 102 de memoria. El dispositivo 114 es utilizado para preparar la tarjeta 102 de memoria antes de que pueda ser objeto de acceso por medio del terminal 110. Por lo tanto, el dispositivo 114 es, preferentemente, un dispositivo portátil que pueda ser transportado por el usuario fácilmente. Para permitir que el propietario de la tarjeta opere el dispositivo 114, este comprende una unidad 120 de visualización, tal como, por ejemplo, un monitor, y una unidad 122 de entrada, tal como, por ejemplo, un teclado. La operación del dispositivo 114 está controlada por medio de un microprocesador 124. El microprocesador 124 está acoplado a la unidad lectora 118 de tarjetas, a la unidad 120 de visualización y a la unidad 122 de entrada. Además, el microprocesador 124 está acoplado a una unidad 126 de memoria para guardar programas de soporte lógico que se ejecutan en el microprocesador 124 y para guardar datos adicionales usados en la operación del dispositivo 114. El dispositivo 114 puede ser un dispositivo dedicado a las funciones descritas en el presente documento. Sin embargo, se prefiere usar un dispositivo 114 que el propietario de la tarjeta ya suela llevar, de modo que no tenga que transportar un dispositivo adicional. Un ejemplo de un dispositivo 114 que puede ser utilizado dentro del ámbito de la invención y que ya es transportado por el propietario de la tarjeta es un dispositivo de comunicaciones móviles, tal como, por ejemplo, un teléfono celular, una PDA o similares.

Cuando el propietario de la tarjeta 102 de memoria desea hacer sus datos protegidos accesibles al usuario del terminal 110, inserta la tarjeta 102 de memoria en la unidad lectora 118 de tarjetas de su dispositivo 114. El dispositivo 114 proporciona una función que permite al usuario especificar un punto en el tiempo hasta el que han de hacerse accesibles los datos protegidos guardados en la tarjeta 102 de memoria. Como alternativa, el propietario de la tarjeta puede especificar un periodo de tiempo durante el que han de hacerse accesibles los datos protegidos

guardados en la tarjeta 102 de memoria. Con esta alternativa, el punto en el tiempo hasta el que han de hacerse accesibles los datos protegidos se calcula a partir del periodo de tiempo especificado usando la hora actual, que está disponible en el dispositivo 114. Debería hacerse notar que el periodo de tiempo que especifica el propietario de la tarjeta se calcula comenzado en el momento en que es introducido en el dispositivo 114.

En una realización, la función para especificar el punto en el tiempo se implementa en forma de una aplicación de soporte lógico que se ejecuta en el microprocesador del dispositivo 114. El usuario puede especificar el punto en el tiempo o el periodo de tiempo usando la unidad 122 de entrada y la aplicación puede proporcionar una interfaz gráfica de usuario en la unidad 120 de visualización para permitir una operación fácil y cómoda. En otra realización, la función es proporcionada por la propia tarjeta 102 de memoria. Aquí, la tarjeta 102 de memoria puede comprender un servidor web que permite que la tarjeta 102 de memoria proporcione páginas electrónicas que pueda ser objeto de acceso por medio de un navegador de red. Para implementar el servidor web en la tarjeta 102 de memoria, puede usarse la tecnología denominada servidor web de tarjeta inteligente (SCWS). Esta tecnología, que permite integrar servidores web en tarjetas inteligentes, puede adaptarse a la tarjeta 102 de memoria, que es una tarjeta inteligente particular. La comunicación entre la tarjeta 102 de memoria y el dispositivo 114 puede usar uno de los soportes ofrecidos por la tecnología SWCS, es decir, el protocolo T=0 con una capa de interfaz BIP (protocolo independiente del soporte) o el TCP/IP (protocolo de control de transmisiones/protocolo de Internet) usando una interfaz USB, describiéndose en particular las tarjetas inteligentes de interfaz USB, estandarizadas recientemente, en ISO 7816-12. Para permitir que el propietario de la tarjeta especifique el punto en el tiempo hasta el que es accesible la tarjeta 102 de memoria, el servidor web de la tarjeta 102 de memoria puede proporcionar una página web que sea objeto de acceso por medio de un soporte lógico de navegación del dispositivo 114. La página electrónica puede mostrarse en la unidad 120 de visualización y el usuario puede introducir el punto en el tiempo o el periodo de tiempo hasta el punto en el tiempo usando la unidad 122 de entrada del dispositivo 114. Si el usuario especifica un periodo de tiempo, la unidad de control puede calcular el punto en el tiempo con base en la hora actual, que puede ser proporcionada por el reloj del dispositivo 114.

El propietario de la tarjeta puede iniciar el procedimiento de especificación del punto en el tiempo o el periodo de tiempo arrancando la correspondiente aplicación de soporte lógico. Esto puede hacerse cuando el propietario de la tarjeta se propone entregar la tarjeta 102 de memoria para la lectura de los datos en el futuro cercano y cuando sabe cuánto tiempo precisa el aceptante para leer los datos protegidos. Normalmente, el usuario puede especificar el punto en el tiempo o el periodo de tiempo en las dependencias del aceptante inmediatamente antes de que entregue la tarjeta 102 de memoria al aceptante. Así, es ventajoso que el dispositivo 114 sea portátil.

Una vez que el propietario de la tarjeta haya especificado el punto en el tiempo o que se haya calculado el punto en el tiempo a partir del periodo de tiempo especificado por el propietario de la tarjeta, la unidad de control comprueba la autorización del propietario de la tarjeta. Con este fin, el dispositivo 114 remite una credencial a la tarjeta 102 de memoria. A continuación, la unidad de control verifica la credencial. La credencial puede incluir un nombre de usuario y/o una contraseña secreta o un PIN (número de identificación personal). La credencial puede pasarse a la unidad de control de la tarjeta 102 de memoria junto con el punto en el tiempo o el periodo de tiempo. La credencial es introducida por el propietario de la tarjeta o la credencial es guardada de forma segura en el dispositivo 114 y remitida a la tarjeta 102 de memoria junto con el punto en el tiempo o el periodo de tiempo. Si la credencial no puede ser verificada con éxito, la unidad de control no permite guardar el punto en el tiempo en la tarjeta 102 de memoria. Tras haber verificado con éxito la credencial, la unidad de control guarda de forma segura en la tarjeta 102 de memoria el punto en el tiempo especificado por el propietario de la tarjeta o calculado a partir del periodo de tiempo especificado por el propietario de la tarjeta.

Para permitir que el propietario de la tarjeta acceda a los datos protegidos sin poner un límite de tiempo, puede hacerse que la unidad de control también permita el acceso a los datos protegidos con base en una verificación de la credencial con éxito.

Después de que el punto en el tiempo o el periodo de tiempo se hayan guardado en la tarjeta 102 de memoria, el propietario de la tarjeta entrega la tarjeta 102 de memoria al aceptante. El propietario de la tarjeta puede ser informado sobre el almacenamiento con éxito del punto en el tiempo presentado un correspondiente mensaje, que se genera en la unidad de control, en la unidad 120 de visualización de su dispositivo 114. Tal la recepción de la tarjeta 102 de memoria, el aceptante inserta la tarjeta 102 de memoria en la unidad lectora 108 de tarjetas del terminal 110.

Antes de que la unidad de control permita al terminal 110 acceder a los datos protegidos guardados en la memoria 104 de la tarjeta 102 de memoria, la unidad de control recupera información temporal del servidor horario 116. La información para establecer una conexión con el servidor horario 116, tal como la dirección de red del servidor horario 116, está guardada de forma segura en la tarjeta 102 de memoria. El intercambio de datos entre la unidad de control y el servidor horario 116 puede basarse en HTTP (protocolo de transferencia de hipertextos). En una realización puede establecerse una conexión “continua” entre la tarjeta 102 de memoria y el servidor horario 116 a través del terminal 110 usando HTTP. Esto quiere decir que puede prescindirse de una conversión de protocolo de la solicitud de la unidad de control para proporcionar información temporal y de la respuesta del servidor horario 116.

La información temporal proporcionada por el servidor horario 116 especifica la hora actual tal como está medida en el servidor horario 116. Además, la información temporal está protegida criptográficamente de tal manera que un destinatario pueda verificar que la información se origina en el servidor horario 116 y que la información temporal no fue modificada durante su transmisión al destinatario. Para lograr esto, la información temporal es cifrada usando una clave de cifrado secreta del servidor horario 116. Como alternativa, la información temporal incluye una firma digital del servidor horario 116, es decir, un valor de comprobación que se deriva del contenido de la información y cifrado usando la clave secreta del servidor horario 116. La clave secreta de cifrado es parte de un par asimétrico de claves que, además, incluye una clave pública de descifrado para descifrar los datos que han sido cifrados usando la clave secreta de cifrado. La clave pública de descifrado del servidor horario 116 se guarda de manera segura en la tarjeta 102 de memoria. El almacenamiento seguro evita que la clave sea sustituida por otra clave. Como alternativa a la utilización del par asimétrico de claves, es igualmente posible utilizar un cifrado simétrico con una clave para el cifrado y el descifrado que se comparte entre el servidor horario 116 y la tarjeta 102 de memoria.

Cuando la tarjeta 102 de memoria recibe la información temporal, la unidad de control verifica la autenticidad de la información temporal. Con este fin, la unidad de control descifra la información temporal o la firma digital con la calve pública de cifrado verificando la autenticidad y la integridad de la información temporal. Si se usa una firma digital, la unidad de control descifra el valor de comprobación, confirmando con ello que la información temporal se origina en el servidor horario 116. Acto seguido, la unidad de control de la hora compara el valor de comprobación con un valor de comprobación autogenerado y determina que la información temporal está inalterada si coinciden ambos valores de comprobación.

En una realización adicional, la tarjeta 102 de memoria puede incluir una firma digital de la tarjeta 102 de memoria en las solicitudes enviadas al servidor horario 116, que puede ser devuelta junto con la información temporal. El firma digital puede ser generada usando una clave secreta asignada a la tarjeta 102 de memoria y, cuando recibe la información temporal, la tarjeta de memoria puede verificar la signatura digital usando la clave secreta o una clave de descifrado asignada a la clave secreta. Cuando se verifica con éxito la firma digital, se garantiza que la información temporal se origina en el servidor horario al que se ha enviado la ciudad. La verificación de la firma digital puede formar parte de la verificación de la autenticidad de la información temporal.

Si no puede verificarse con éxito la autenticidad de la información temporal, la unidad de control niega el acceso a los datos protegidos guardados en la tarjeta 102 de memoria. Una vez que se ha validado con éxito la autenticidad y la integridad de la información temporal, la unidad de control compara la información temporal con el punto en el tiempo que fue especificada por el propietario de la tarjeta y que está guardada en la tarjeta 102 de memoria. Si este punto en el tiempo sigue al punto en el tiempo especificado en la información temporal recibida del servidor horario 116, la unidad de control permite el acceso a los datos protegidos guardados en la tarjeta 102 de memoria por medio del terminal 110.

Una vez que se ha permitido que la unidad de control acceda a los datos protegidos, determina cuándo se alcanza el punto en el tiempo especificado por el propietario de la tarjeta. Si se determina que se alcanza el punto en el tiempo, la unidad de control vuelve a bloquear los datos protegidos; es decir, la unidad control impide cualquier acceso ulterior a los datos. Los datos protegidos están bloqueados incluso cuando la tarjeta 102 de memoria sigue insertada en el lector 108 de tarjetas del terminal 110.

Para determinar cuándo se alcanza el punto en el tiempo almacenado, la unidad de control puede recuperar reiteradamente información temporal. En particular, la unidad de control puede recuperar la información temporal a intervalos de tiempo predeterminados regulares que no son demasiado largos para que el usuario del terminal 110 no tenga acceso a la información protegida significativamente después del punto en el tiempo almacenado. Cada vez que la unidad de control recupera del servidor horario 116 información temporal, compara el momento especificado en la información temporal con el punto en el tiempo almacenado y desbloquea los datos protegidos cuando el punto en el tiempo almacenado ya no está en el futuro con respecto a la hora actual, según está especificada en la información temporal recuperada del servidor horario 116. La unidad de control también puede bloquear los datos protegidos si la información temporal recibida del servidor horario 116 no puede ser verificada con éxito. Y, preferentemente, la unidad de control también bloquea los datos protegidos si no puede recuperarse del servidor horario 116 información temporal, dado que, en este caso, la unidad de control es incapaz de determinar si se ha alcanzado el punto en el tiempo especificado por el propietario de la tarjeta.

En una realización adicional, la unidad de control solo recupera información temporal del servidor horario 116 una vez, después de que la tarjeta 102 de memoria haya sido insertada en el terminal 110, y calcula una diferencia entre la hora indicada por el servidor horario 116 y el punto en el tiempo especificado por el propietario de la tarjeta. Acto seguido, la unidad de control iniciar un contador de tiempos. Cuando se ha alcanzado el valor del contador correspondiente a la diferencia calculada de tiempo, la unidad de control determina que ha expirado el periodo de tiempo correspondiente a la diferencia calculada y vuelve a bloquear los datos protegidos contra el acceso desde el exterior de la tarjeta 102 de memoria.

Preferentemente, la información temporal proporcionada por el servidor horario 116 y recibida en la tarjeta 102 de memoria se guarda en la tarjeta 102 de memoria. Cada vez que la unidad de control recibe nueva información

temporal del servidor horario 116, comprueba si la nueva información temporal especifica un momento posterior a la información temporal recibida antes. Si no es así, se ha recibido información temporal manipulada y se bloquean los datos protegidos. Este procedimiento resulta particularmente útil si la unidad de control recupera reiteradamente información temporal del servidor horario 116 para determinar si los datos protegidos han de volver a bloquearse. Sin embargo, también puede permitirse que la unidad de control compare la información temporal de un intervalo de acceso con la información temporal recuperada en el siguiente intervalo de acceso para detectar un fraude, lo que también es posible cuando la unidad de control recupera información temporal solo para un instante durante el intervalo de acceso. Aquí, la expresión intervalo de acceso se refiere a un intervalo de tiempo contiguo en el que se permite el acceso a los datos protegidos y que se inicia especificando un punto en el tiempo hasta el que son accesibles los datos protegidos.

Realizaciones adicionales de la invención difieren de las realizaciones descritas anteriormente porque el propietario de la tarjeta especifica un periodo de tiempo para acceder a la tarjeta 102 de memoria en vez de o además de un punto absoluto en el tiempo hasta el que la tarjeta 102 de memoria puede ser objeto de acceso. Aquí, la unidad de control guarda la información temporal que recupera del servidor horario 116 cuando la tarjeta 102 de memoria ha sido insertada en el terminal 110. Mientras la tarjeta 102 de memoria está insertada en el terminal 110, la unidad de control puede volver a recuperar reiteradamente información temporal del servidor horario 116. Cada vez que la unidad de control recupera información temporal del servidor horario 116, compara la hora especificada en la información temporal con la hora almacenada y vuelve a bloquear los datos protegidos cuando la diferencia entre estas horas supera el periodo de tiempo especificado por el usuario. En otros respectos, el mecanismo de seguridad puede ser el mismo que en las realizaciones descritas anteriormente. En particular, la unidad de control puede bloquear la memoria 104 si no puede recuperarse información temporal alguna del servidor horario 116, si no puede autenticarse con éxito la información temporal recibida y si la información temporal recibida del servidor horario 116 especifica una hora anterior o igual que la información temporal recibida anteriormente.

En otra realización adicional en la que el usuario especifica un periodo de tiempo para acceder a la tarjeta 102 de memoria en vez de o además de un punto absoluto en el tiempo hasta el que la tarjeta 102 de memoria puede ser objeto de acceso, la unidad de control utiliza un contador de tiempos de la tarjeta 102 de memoria para determinar si ha expirado el periodo de tiempo. El contador de tiempos se inicia una vez que se ha insertado en el terminal 110 la tarjeta 102 de memoria. Cuando se ha alcanzado el valor del contador correspondiente al periodo de tiempo especificado, la unidad de control determina que ha expirado el periodo de tiempo y vuelve a bloquear los datos protegidos contra el acceso desde el exterior de la tarjeta 102 de memoria.

Si el periodo de tiempo es especificado además de un punto absoluto en el tiempo hasta el que la tarjeta 102 de memoria puede ser objeto de acceso, la unidad de control bloquea los datos protegidos si se ha alcanzado el punto en el tiempo o si ha expirado el periodo de tiempo, dependiendo de qué evento ocurra primero. Esto significa que los datos protegidos quedan bloqueados cuando se alcanza el punto en el tiempo aun en el caso de que el periodo de tiempo no haya expirado todavía. Además, los datos protegidos se bloquean cuando ha expirado el periodo de tiempo si todavía no se ha alcanzado el punto en el tiempo.

Tal como se ha descrito anteriormente, la tarjeta 102 de memoria puede proporcionar una gestión de grupos. Si el propietario de la tarjeta quiere hacer accesibles únicamente uno o más grupos seleccionados de datos, puede especificar tales grupos junto con el punto en el tiempo hasta el que los datos se hacen accesibles o junto con el periodo de tiempo para acceder a los datos. Los grupos especificados se memorizan en la unidad de control y la unidad de control no permite el acceso a otros grupos de datos protegidos cuando la tarjeta 102 de memoria se inserta en la unidad lectora 108 de tarjetas del terminal 110.

Además, aparte de los mecanismos de seguridad descritos anteriormente, puede proporcionarse un mecanismo adicional de seguridad para proteger los datos de la tarjeta 102 de memoria. Por ejemplo, permitir el acceso a los datos protegidos puede requerir, además, que se introduzca en el terminal 110 una contraseña u otra credencial y que sea verificada por la unidad de control. La contraseña o la credencial pueden ser proporcionadas al usuario del terminal 110 por el propietario de la tarjeta. En este contexto, el límite temporal para acceder a los datos impide al usuario del terminal 110 acceder a los datos en un grado mayor que el deseado por el propietario de la tarjeta. En particular, el usuario del terminal 110 no puede acceder a los datos protegidos sin el permiso del propietario de la tarjeta cuando obtiene la tarjeta 102 de memoria una segunda vez después de haber recibido anteriormente la credencial junto con la tarjeta 102 de memoria.

Aunque la invención ha sido ilustrada y descrita con detalle en los dibujos y en la descripción precedente, tal ilustración y tal descripción han de ser consideradas ilustrativas o ejemplares y no restrictivas; la invención no está limitada a las realizaciones dadas a conocer. En la puesta en práctica de la invención reivindicada, a partir de un estudio de los dibujos, la divulgación y las reivindicaciones adjuntas, los expertos en la técnica pueden entender y efectuar otras variaciones de las realizaciones dadas a conocer.

En las reivindicaciones, la palabra “comprende” no excluye otros elementos u otras 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. El mero hecho de que se enumeren ciertas medidas en

reivindicaciones dependientes mutuamente diferentes no indica que no pueda usarse con ventaja una combinación de estas medidas.

No debería interpretarse que cualquier signo de referencia en las reivindicaciones limite el alcance.

REIVINDICACIONES

1. Un procedimiento para proporcionar acceso a datos guardados de forma segura en una tarjeta (102) de memoria que comprende las siguientes etapas:

- especificar una primera información temporal correspondiente a un periodo de tiempo y guardar la primera información temporal en la tarjeta (102) de memoria;
- insertar la tarjeta (102) de memoria en un terminal (110);
- determinar en una unidad de control incluida en la tarjeta (102) de memoria si ha expirado el periodo de tiempo; y
- permitir que el terminal (110) acceda a los datos hasta que se determine que el periodo de tiempo ha expirado

caracterizado porque el terminal (110) permite que la unidad de control se conecte con un servidor (116) de red por medio de una conexión de red proporcionada por el terminal (110) y recupere de una unidad de reloj comprendida en el servidor (116) de red una segunda información temporal que especifica la hora actual, usándose dicha segunda información temporal para determinar si ha expirado el periodo de tiempo.

2. El procedimiento según la reivindicación 1 en el que la información temporal recuperada de la unidad de reloj comprende información de autenticación, particularmente una firma digital, que es verificada en la unidad de control.

3. El procedimiento según las reivindicaciones 1 o 2 en el que la primera información temporal especifica un punto en el tiempo y en el que la unidad de control determina si ha expirado el periodo de tiempo con base en una diferencia horaria entre el punto especificado en el tiempo y la hora actual especificada en la segunda información temporal.

4. El procedimiento según la reivindicación 3 en el que la unidad de control recupera reiteradamente la segunda información temporal de la unidad de reloj mientras la tarjeta (102) de memoria está insertada en el terminal (110) y en el que la unidad de control determina si ha expirado el periodo de tiempo cada vez después de que se haya recuperado la segunda información temporal.

5. El procedimiento según la reivindicación 3 en el que la unidad de control determina que el periodo de tiempo ha expirado cuando un contador de tiempos de la tarjeta (102) de memoria indica que la diferencia de tiempo ha expirado, iniciándose el contador después de que la tarjeta (102) de memoria se haya insertado en el terminal (110).

6. El procedimiento según las reivindicaciones 1 o 2 en el que la primera información temporal especifica el periodo de tiempo.

7. El procedimiento según la reivindicación 6 en el que la unidad de control determina que el periodo de tiempo ha expirado cuando un contador de tiempos de la tarjeta (102) de memoria indica que el periodo de tiempo ha expirado, iniciándose el contador después de que la tarjeta (102) de memoria se haya insertado en el terminal (110).

8. El procedimiento según la reivindicación 6 en el que la unidad de control guarda la hora especificada en la segunda información temporal cuando recupera la segunda información por vez primera, en el que la unidad de control recupera reiteradamente la segunda información temporal de la unidad de reloj, y en el que la unidad de control determina si ha expirado el periodo de tiempo con base en una comparación del periodo de tiempo y una diferencia de tiempo entre la hora guardada y la hora actual especificada en la segunda información temporal recuperada la última vez.

9. Una tarjeta (102) de memoria para guardar datos de forma segura en la misma, en la que la tarjeta (102) de memoria:

- está adaptada para recibir una primera información temporal correspondiente a un periodo de tiempo y para almacenar la primera información temporal y
- comprende una unidad de control configurada para determinar si ha expirado el periodo de tiempo y para permitir que un terminal (110) acceda a los datos hasta que se determine que el periodo de tiempo ha expirado, mientras la tarjeta (102) de memoria está insertada en el terminal (110),

caracterizada porque la unidad de control está adaptada para conectarse con un servidor (116) de red por medio de una conexión de red proporcionada por el terminal (110), mientras la tarjeta (102) de memoria está insertada en el terminal (110), y recuperar de una unidad de reloj comprendida en el servidor de red una segunda información temporal que especifica la hora actual, usándose dicha segunda información temporal para determinar si ha expirado el periodo de tiempo.

10. Un sistema que comprende una tarjeta (102) de memoria según la reivindicación 9 y que, además, comprende un terminal (110) para recibir la tarjeta (102) de memoria.

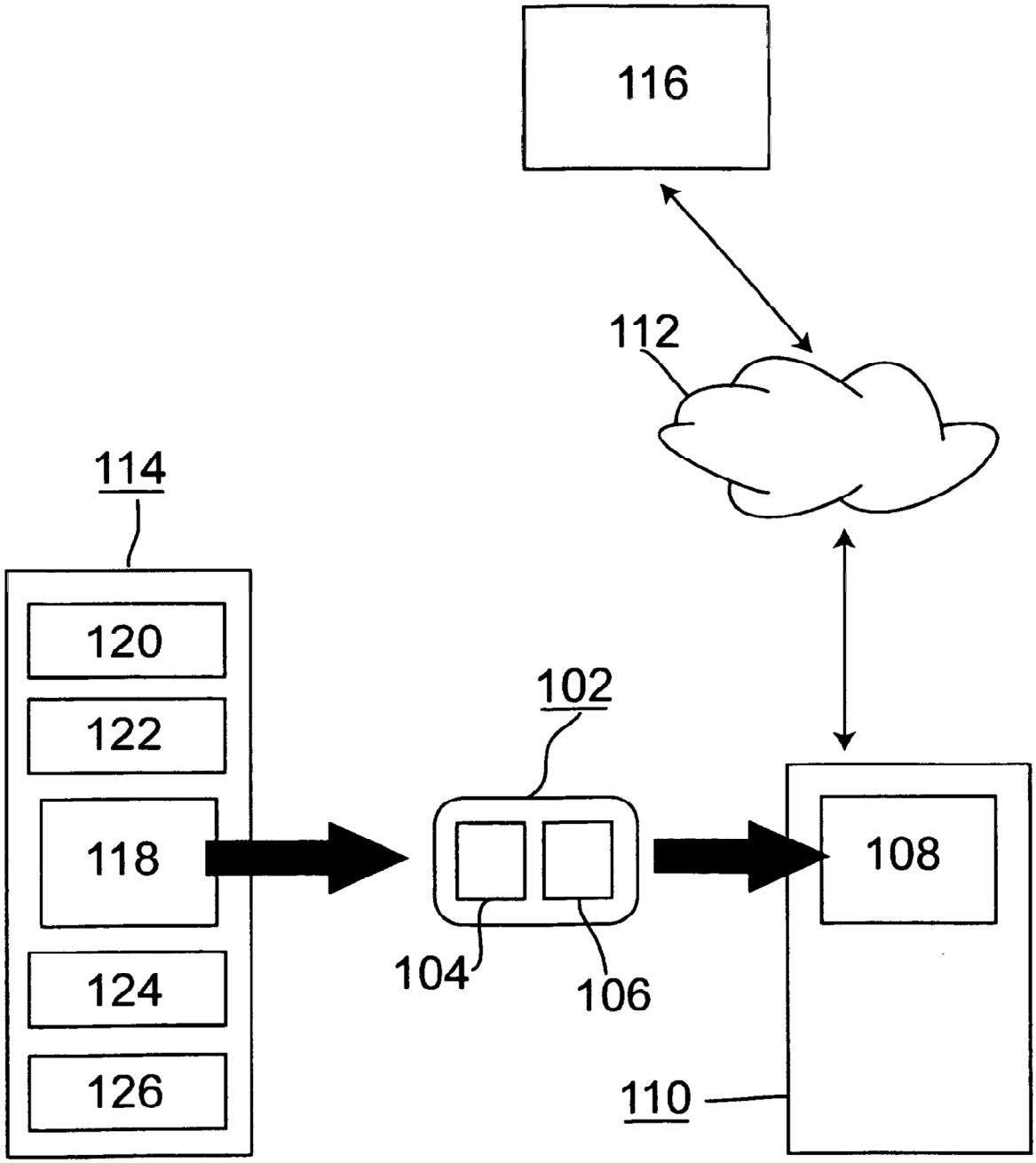

Fig. 1