(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 401 358**

(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 08017899 (9)**

(97) Fecha y número de publicación de la concesión europea: **12.12.2012 EP 2175454**

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

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.04.2013

(73) Titular/es:

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

(72) Inventor/es:

KORAICHI, NAJIB;
HOEKSEL, SEBASTIAAN y
BARRY, AGUIBOU MOUNTAGA

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

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

Campo técnico

La invención se refiere a tarjetas de memoria con protección de acceso. Más específicamente, la invención se refiere a un procedimiento y a un sistema para proporcionar acceso a datos almacenados en una tarjeta de memoria de este tipo.

Antecedentes de la invención

Las tarjetas de memoria son tarjetas de circuitos integrados (CI) que incluyen memoria no volátil y un controlador que controla la operación de la tarjeta de memoria. Tales tarjetas de memoria se pueden conectar temporalmente a dispositivos anfitrión, tales como, por ejemplo, ordenadores personales (PC), teléfonos celulares, asistentes digitales personales (PDA), cámaras digitales, reproductores de audio portátiles y otros dispositivos electrónicos anfitrión para almacenamiento de datos. Existe una pluralidad de estándares que especifican diferentes tipos de tarjetas de memoria, tales como, por ejemplo, tarjetas SD (Secure Digital), tarjetas CF (Compact Flash) y MMC (Multimedia Card). Un ejemplo adicional de una tarjeta de memoria, en el sentido en el que el término se usa en el presente documento, es un lápiz de memoria flash USB (Bus Universal en Serie).

Las tarjetas de memoria del tipo descrito anteriormente pueden proporcionar un mecanismo de seguridad para proteger datos de acceso no autorizados. Esto permite almacenar 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 protegidos para ciertas personas en algunas situaciones. Por ejemplo, el propietario de la tarjeta puede desear permitir a su médico leer datos médicos protegidos almacenados en la tarjeta de memoria o hacer disponibles fotos personales a un amigo.

El documento WO 2005/039218 desvela un procedimiento para proteger datos en un portador de datos, que se puede conectar a un dispositivo terminal. En base a condiciones de acceso un controlador juzga si el dispositivo terminal está autorizado o no a acceder a datos almacenados en el portador de datos. En una realización, un servidor de gestión proporciona las condiciones de acceso mediante una red de datos a la que se conecta el portador de datos mediante el dispositivo terminal. Además de la condición de acceso el servidor de gestión transmite una firma digital que se verifica en el portador de grabación antes de que se conceda el acceso a los datos protegidos en base a las condiciones de acceso.

Descripción de la invención

Es un objeto de la presente invención permitir a un propietario de una tarjeta de memoria hacer accesible a otra persona a los datos protegidos almacenados en la tarjeta de memoria.

El objeto se consigue mediante un procedimiento de acuerdo con la reivindicación 1 y mediante un sistema de acuerdo con la reivindicación 10. Se proporcionan realizaciones del procedimiento y del terminal en las reivindicaciones dependientes.

De acuerdo con un primer aspecto de la invención, se sugiere un procedimiento para proporcionar acceso a datos almacenados de manera segura en una tarjeta de memoria. El procedimiento comprende las siguientes etapas:

- recibir la tarjeta de memoria en un terminal;
- transmitir una solicitud para acceder a los datos mediante un enlace de comunicación desde el terminal al dispositivo;
- tras la recepción de la solicitud, enviar la primera información desde el dispositivo al terminal mediante el enlace de comunicación;
- recibir la primera información en el terminal y acceder a los datos usando la primera información.

De acuerdo con un segundo aspecto de la invención, se proporciona un terminal para acceder a datos de manera segura almacenados en una tarjeta de memoria. El terminal comprende:

- un medio de aceptación adaptado para recibir la tarjeta de memoria;
- un dispositivo de lectura adaptado para leer los datos de la tarjeta de memoria usando la primera información;
- un componente de envío adaptado para enviar una solicitud para acceder a los datos mediante un enlace de comunicación;
- un componente de recepción adaptado para recibir la primera información mediante el enlace de comunicación en respuesta a la solicitud.

La invención establece la idea de que se permite un acceso a la tarjeta de memoria insertada en un terminal por medio de un dispositivo que se puede comunicar con el terminal mediante un enlace de comunicación. El dispositivo puede ser un dispositivo del propietario de la tarjeta de modo que el propietario de la tarjeta puede controlar de manera remota el acceso a la tarjeta de memoria. En este punto, la expresión “de manera remota” no significa necesariamente que haya una gran distancia entre el dispositivo y el terminal sino que se puede controlar el acceso a la tarjeta de memoria desde fuera del terminal.

En una realización del procedimiento y del terminal, se envía la primera información al terminal en respuesta a una operación del usuario adquirida por medio de una interfaz de usuario del dispositivo. Esta realización tiene la ventaja que el propietario de la tarjeta puede dar directamente su consentimiento o rechazar su consentimiento a cada acceso individual a la tarjeta de memoria.

En una realización adicional del procedimiento y del terminal, el dispositivo es un dispositivo de comunicación móvil y el enlace de comunicación comprende una red de comunicación móvil. En particular, es una ventaja de esta realización que el propietario de la tarjeta pueda usar su dispositivo de comunicación móvil para desbloquear la tarjeta de memoria para que se acceda por medio del terminal. Por lo tanto, él puede usar un dispositivo que normalmente ya lleva para controlar el acceso a la tarjeta de memoria.

Una realización relacionada del procedimiento y del terminal comprende que el dispositivo de comunicación móvil comprende una tarjeta SIM que proporciona la primera información. Esta realización tiene la ventaja que la tarjeta SIM insertada en el dispositivo de comunicación móvil, que proporciona un entorno de seguridad para almacenar datos y realizar tareas, se puede usar para almacenar de manera segura la primera información y para proporcionar la información al terminal.

En una realización adicional del procedimiento y del terminal, se establece el enlace de comunicación desde el terminal al dispositivo usando la segunda información, leyéndose dicha segunda información desde la tarjeta de memoria por el terminal. En esta realización, el terminal puede establecer automáticamente un enlace de comunicación con el dispositivo de modo que no hay necesidad de proporcionar información para establecer la conexión de comunicación con el terminal mediante otro canal.

Una realización relacionada del procedimiento y del terminal proporciona que la segunda información comprende un MSISDN (Número de Red Digital de Servicios Integrados de Abonado Móvil) del dispositivo.

Para evitar la manipulación, es útil poder determinar que la solicitud para acceder a la tarjeta de memoria se origina realmente desde el terminal en el que la tarjeta de memoria está insertada. Por lo tanto, en una realización del procedimiento y del terminal, la solicitud para acceder a los datos incluye una firma digital de la tarjeta de memoria, verificándose dicha firma digital en el dispositivo, particularmente en la tarjeta SIM contenida en el dispositivo.

En una realización del procedimiento y del dispositivo, se almacenan los datos de manera encriptada en la tarjeta de memoria y la primera información comprende una clave criptográfica para desencriptar los datos.

En una realización adicional del procedimiento y del dispositivo, la tarjeta de memoria comprende una seguridad lógica que permite acceder a los datos después de que se haya verificado satisfactoriamente la primera información. Un mecanismo de seguridad de este tipo puede proteger los datos en lugar de la encriptación que se usa en la realización mencionada anteriormente. Sin embargo, también se puede proporcionar además de la encriptación para aumentar adicionalmente la seguridad.

Adicionalmente, en una realización del procedimiento y del terminal, la tarjeta de memoria comprende datos adicionales, que no son accesibles usando la primera información.

Es una ventaja, de esta realización, que se pueda conceder el acceso a datos seleccionados almacenados en la tarjeta de memoria, mientras que otros datos permanecen inaccesibles.

De acuerdo con un aspecto adicional de la invención, se proporciona un sistema para proporcionar acceso a una tarjeta de memoria. El sistema comprende el terminal del tipo descrito anteriormente y un dispositivo, comprendiendo dicho dispositivo un medio de autorización para proporcionar la primera información en respuesta a una recepción de la solicitud desde el terminal.

En una realización del sistema, el dispositivo comprende adicionalmente una interfaz de usuario acoplada al medio de autorización, adaptándose el medio de autorización para proporcionar la primera información en respuesta a una operación de usuario efectuada por medio de la interfaz de usuario.

Los aspectos de la invención anteriormente mencionados y otros serán también evidentes a partir de y se aclararán con referencia a las realizaciones descritas en lo sucesivo en el presente documento haciendo referencia a los dibujos.

Breve descripción de los dibujos

Se hará referencia a modo de ejemplo con los dibujos adjuntos en los que

La Figura 1 es un diagrama de bloques esquemático de un sistema para controlar acceso a datos protegidos almacenados en una tarjeta de memoria.

Descripción detallada de realizaciones de la invención

La Figura 1 representa esquemáticamente elementos de un sistema para controlar acceso a datos almacenados en una tarjeta 102 de memoria. En particular, la tarjeta 102 de memoria almacena datos sensibles del propietario de la tarjeta. En el sistema mostrado en la figura 1, el propietario de la tarjeta puede hacer accesibles tales datos a personas autorizadas, mientras que se evita que terceras partes no autorizadas accedan a los datos. En principio, los datos pueden ser cualquier dato que el propietario quiera compartir con personas seleccionadas. Por ejemplo, los datos son datos médicos del propietario de la tarjeta que el propietario de la tarjeta desea compartir únicamente con un médico. Otro ejemplo son detalles bancarios que el propietario de la tarjeta desea proporcionar únicamente a personas de confianza. En un ejemplo adicional más, se refiere a datos personales, tales como, por ejemplo, fotos personales, que el propietario de la tarjeta quiere compartir únicamente con amigos.

La tarjeta 102 de memoria comprende una memoria 104 y un microcontrolador 106 integrado en un alojamiento. El alojamiento puede ser suficientemente pequeño de modo que el propietario pueda llevar la tarjeta 102 de memoria fácilmente y que se pueda usar la tarjeta 102 de memoria en relación con lectores de tarjetas, que se integran en dispositivos pequeños, tales como, dispositivos de comunicación móvil. Preferentemente, se configura la tarjeta 102 de memoria de acuerdo con un formato estándar, y puede ser una tarjeta SD, una tarjeta CF, una tarjeta MMC o similares. 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 particularmente determinar el tamaño y forma de la tarjeta 102 de memoria, la configuración de sus contactos eléctricos y los protocolos de comunicación usados en la comunicación con la tarjeta 102 de memoria. El cumplimiento del estándar de la tarjeta 102 de memoria permite que se acceda a la tarjeta por medio de un dispositivo lector de tarjetas, que cumple de manera similar con el estándar.

La memoria 104 es un almacenamiento no volátil que se puede borrar y reprogramar eléctricamente. Particularmente, se puede configurar la memoria 104 como una unidad de almacenamiento de estado sólido, particularmente una memoria flash o una EEPROM (Memoria de Sólo Lectura Eléctricamente Programable y Borrable) no flash. Sin embargo, el experto en la materia entiende que en principio se puede usar cualquier tipo de dispositivo de memoria. La memoria 104 puede estar constituida por uno o más chips de memoria, que se disponen en el alojamiento de la tarjeta 102 de memoria. El microcontrolador 106 y la memoria 104 pueden residir en un solo chip en la tarjeta 102 de memoria, o el microcontrolador 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 se conecta la tarjeta 102 de memoria. En particular, el microcontrolador 106 implementa los protocolos de comunicación usados para el intercambio de datos entre la tarjeta 102 de memoria y un dispositivo conectado.

Al menos se protege la parte del contenido de datos de la memoria 104 que comprende los datos sensibles del propietario frente al acceso no autorizado, es decir la lectura y manipulación no autorizada de los datos protegidos. En una realización, el microcontrolador 106 también proporciona una seguridad lógica que controla acceso a los datos protegidos. Se permite o deniega cada intento de acceso a los datos protegidos almacenados en la memoria 104 mediante la unidad de autenticación. La seguridad lógica del microcontrolador 106 permite acceder a los datos únicamente después de que se ha proporcionado y verificado satisfactoriamente una credencial. La credencial puede ser, por ejemplo, un código personal, tal como una contraseña o un PIN (Número de Identificación Personal), o una firma digital. Como alternativa, se pueden almacenar los datos protegidos en la tarjeta 102 de memoria en una forma encriptada de modo que se tiene que usar una clave de desencriptación criptográfica para leer los datos. Sin embargo, comparado con la mera encriptación de los datos el control de acceso por medio del microcontrolador 106 particularmente tiene la ventaja que se puede evitar una manipulación de los datos no autorizada, cuando el microcontrolador 106 únicamente permite acceso de lectura a datos protegidos. Un acceso de escritura puede requerir una credencial adicional, que es únicamente conocida por el propietario de la tarjeta.

Además de los datos protegidos, se puede almacenar en la tarjeta 102 de memoria datos adicionales que no se aseguran particularmente. En relación con los datos protegidos, se puede proporcionar opcionalmente una gestión de grupos. Esto significa que se almacenan diferentes grupos de datos protegidos en la tarjeta 102 de memoria, donde se puede configurar diferentes autorizaciones de acceso para los grupos. Esto se puede conseguir asignando diferentes credenciales a los grupos o encriptando los datos de diferentes grupos de tal manera que se puedan desencriptar con diferentes claves de desencriptación. La gestión de grupos permite almacenar en la misma tarjeta 102 de memoria datos que el propietario quiere compartir con diferentes personas. Por ejemplo, el propietario puede almacenar datos sanitarios para compartir con su médico o médica y datos para compartir con amigos en la misma tarjeta 102 de memoria.

Para acceder a los datos protegidos almacenados en la tarjeta 102 de memoria, se usa una unidad 108 lectora de tarjetas, que se acopla a un terminal 110 de la persona que quiere acceder a los datos protegidos. El terminal 110 se conecta a una red 112 de comunicación, que preferentemente es una red de comunicación móvil, que también se supone en lo sucesivo. Particularmente, se puede configurar la red 112 de comunicación móvil de acuerdo con el estándar GSM (Sistema Global para Comunicaciones Móviles) o de acuerdo con el estándar UMTS (Sistema de

Telecomunicaciones Móviles Universal). Sin embargo, la red 212 de comunicación móvil puede, de manera similar, adoptar otra tecnología de comunicaciones móvil.

Se puede integrar la unidad 108 lectora de tarjetas en el terminal 110 como se representa en la figura 1, o la unidad 108 lectora de tarjetas puede ser una unidad separada conectada al terminal 110. En una realización, el terminal 110 puede ser un dispositivo de comunicación móvil, tal como, por ejemplo un teléfono móvil, un asistente de datos personal (PDA) o similares. Tales dispositivos a menudo tienen una unidad 108 lectora de tarjetas para aceptar tarjetas de memoria de ciertos formatos estándar, tales como los formatos anteriormente mencionados.

El propietario de la tarjeta 102 de memoria también dispone de un dispositivo 114, que es conectable con la red 112 de comunicación móvil. El dispositivo 114 del propietario puede ser, de manera similar, un dispositivo de comunicación móvil, tal como un teléfono móvil, un PDA o similares. Opcionalmente, el dispositivo 114 de comunicación móvil del propietario de la tarjeta de memoria tiene una unidad lectora de tarjetas para aceptar la tarjeta 102 de memoria. Esto permite al propietario de la tarjeta usar la tarjeta 102 de memoria junto con su dispositivo 114 de comunicación móvil para almacenar y acceder a datos personales. Adicionalmente, el propietario de la tarjeta puede tener la tarjeta 102 de memoria insertada en su dispositivo 114 de comunicación móvil durante el uso normal del dispositivo 114 de comunicación móvil. En este caso, el propietario de la tarjeta tiene la tarjeta 102 de memoria a su disposición en el momento que lleva su dispositivo 114 de comunicación móvil.

Para conectarse a la red 112 de comunicación móvil el terminal 110 y el dispositivo 114 de comunicación móvil del propietario de la tarjeta comprenden una tarjeta inteligente 116, 118, que proporciona un servicio para identificar y/o autenticar los usuarios de los dispositivos 110, 114 en la red 112 de comunicación móvil. Si la red 112 de comunicación móvil es una red GSM, se configura cada una de las tarjetas inteligentes 116, 118 como una tarjeta SIM (Módulo de Identidad de Abonado) de acuerdo con el estándar GSM que comprende una aplicación SIM, que proporciona el servicio de identificación y autenticación. Si la red 112 de comunicación móvil es una red UMTS, se configura cada una de las tarjetas inteligentes 116, 118 como una UICC (Tarjeta Universal de Circuito Integrado) que comprende una aplicación USIM (módulo de Identificación de Abonado Universal) que proporciona el servicio de identificación y autenticación. La aplicación SIM o USIM comprende un código de software que se almacena en la memoria de las tarjetas inteligentes 116, 118 y se ejecuta por medio del microprocesador.

A continuación, se denominan las tarjetas inteligentes 116, 118 como tarjetas SIM. Sin embargo, el término tarjeta SIM, como se usa en el presente documento, debe entenderse como que incluye también tarjetas inteligentes 116, 118 que comprenden aplicaciones USIM o aplicaciones correspondientes que proporcionan funciones de autenticación y/o identificación en relación con una red 112 de comunicación móvil.

Además de los componentes ya descritos, el terminal 110 y el dispositivo 114 de comunicación móvil particularmente pueden comprender un módulo de radio, que se usa para conectar los dispositivos 110, 114 a la red 112 de comunicación móvil mediante red de acceso de radio. Los dispositivos 110, 114 se pueden manejar usando una unidad de entrada, tal como, por ejemplo, un teclado numérico y una unidad de visualización, tal como, por ejemplo, un monitor. Se pueden conectar los componentes de cada dispositivo 110, 114 a un microprocesador, que controla la operación de los dispositivos 110, 114. El microprocesador ejecuta programas de software que se almacenan en una unidad de memoria del dispositivo 110, 114.

Cuando el propietario de la tarjeta 102 de memoria desea hacer accesibles sus datos protegidos al usuario del terminal 110, él traspasa la tarjeta 102 de memoria al usuario del terminal 110, y el usuario inserta la tarjeta 102 de memoria en la unidad 108 lectora de tarjetas del terminal 110. Como se ha descrito anteriormente, el usuario del terminal 110 puede ser un médico que necesita datos sanitarios almacenados de manera segura en la tarjeta 102 de memoria, o el usuario del terminal 110 puede ser alguien a quien el propietario de la tarjeta quiere hacer accesibles datos personales.

El terminal 110 comprende un componente de acceso, para acceder a los datos protegidos almacenados en la tarjeta 102 de memoria. Preferentemente, se configura el componente de acceso como una aplicación de software que comprende un código de software, que se almacena y ejecuta en el terminal 110. En una realización, se hace funcionar la aplicación de software en el microprocesador del terminal 110. En una realización adicional, se almacena y ejecuta la aplicación de software en la tarjeta 116 SIM del terminal 110. Esto tiene la ventaja de que se ejecuta la aplicación de software en un entorno seguro, lo que ya se proporciona en el terminal 110 mediante la tarjeta SIM. Adicionalmente, se puede preinstalar la aplicación de software - que tiene una fuerte relación con la red 112 de comunicación móvil - en la tarjeta SIM de modo que se proporciona junto con la tarjeta SIM por el operador de red móvil.

Cuando se inserta la tarjeta 102 de memoria en la unidad 108 lectora de tarjetas del terminal 110, el componente de acceso del terminal 110 reconoce que la tarjeta 102 de memoria tiene datos protegidos almacenados en la misma, que se pueden acceder usando una credencial que se verifica en la tarjeta 102 de memoria o usando una clave de desencriptación para desencriptar los datos. Se proporciona la credencial o la clave de desencriptación mediante el dispositivo 114 de comunicación móvil del propietario de la tarjeta 102 de memoria tras la solicitud. Se genera la solicitud en el componente de acceso del terminal 110 después de que se haya insertado la tarjeta 102 de memoria en el módulo 108 de lector de tarjetas.

Si se almacenan múltiples grupos de datos protegidos en la tarjeta 102 de memoria, la solicitud incluye información que especifica el grupo a acceder. En una realización, se puede identificar el grupo automáticamente mediante el componente de acceso. Esto requiere que los datos pertenezcan a un grupo de múltiples grupos predeterminados, que se asignan a códigos de identificación predeterminados. Adicionalmente, en principio, se especifica el grupo para el que el usuario del terminal 110 tiene autorización de acceso a datos de configuración del componente de acceso permitiendo de esta manera al componente de acceso identificar ese grupo. Esta realización es particularmente ventajosa, si hay uno o más grupos predeterminados de personas u organizaciones, tales como, por ejemplo, médicos. En este caso, se podrían expedir tarjetas 116 SIM especiales a las personas u organizaciones predeterminadas, y tales tarjetas 116 SIM podrían incluir funcionalidad para acceder a un grupo de datos asignados al grupo de personas u organizaciones.

En otra realización, el componente de acceso presenta los grupos existentes en la tarjeta 102 de memoria en la unidad de visualización del terminal 110 y el usuario del terminal 110 usa la unidad de entrada del terminal 110 para seleccionar el grupo al que quiere acceder.

La solicitud generada mediante el componente de acceso se direcciona al dispositivo 114 de comunicación móvil del propietario de la tarjeta. Preferentemente, esto se hace usando el MSISDN del propietario de la tarjeta, que identifica únicamente la suscripción del propietario de la tarjeta en la red 112 de comunicación móvil. Preferentemente, se almacena el MSISDN en la tarjeta 102 de memoria y se lee desde la tarjeta 102 de memoria mediante el componente de acceso. Sin embargo, de manera similar es posible que el usuario del terminal 110 introduzca el MSISDN manualmente usando la unidad de entrada.

En una realización, la tarjeta 102 de memoria firma digitalmente la solicitud antes de que se envíe al dispositivo 114 de comunicación móvil del propietario de la tarjeta. Con este fin, la tarjeta 102 de memoria proporciona una aplicación adecuada, que se ejecuta en el microcontrolador 106 de la tarjeta 102 de memoria. Se encripta la firma digital usando una clave criptográfica privada, que es parte de un par de claves asimétricas asignadas a la tarjeta 102 de memoria y que se almacenan de manera segura en la tarjeta 102 de memoria. La clave pública correspondiente del par de claves se almacena en el dispositivo 114 de comunicación móvil del propietario de la tarjeta y se usa para verificar la firma digital incluida en la solicitud.

Después de haber generado la solicitud y - si es aplicable - se ha añadido la firma digital opcional, el componente de acceso ordena al terminal 110 enviar la solicitud al dispositivo 114 de comunicación móvil del propietario de la tarjeta 102 de memoria mediante la red 112 de comunicación móvil.

La comunicación entre el terminal 110 y el dispositivo 114 de comunicación móvil se puede basar en cualquier servicio portador proporcionado en la red 112 de comunicación móvil. Particularmente, se puede usar un servicio portador para datos no de habla, tales como SMS (Servicio de Mensajes Cortos), USSD (servicio suplementario de datos no estructurados), CSD (datos por conmutación de circuitos), HSCSD (datos por conmutación de circuitos a alta velocidad) o GPRS (sistema general de paquetes de radio). Sin embargo, se puede proporcionar de manera similar para intercambiar información en la forma de datos de habla usando un servicio portador correspondiente de la red 112 de comunicación móvil.

Cuando se recibe la solicitud en el dispositivo 114 de comunicación móvil, se reenvía en el dispositivo 114 de comunicación móvil a un componente de autorización. Preferentemente, se configura también el componente de autorización como una aplicación de software que se almacena y ejecuta en el dispositivo 114 de comunicación móvil. Particularmente, se puede ejecutar la aplicación de software en el microprocesador del dispositivo 114 de comunicación móvil. Como alternativa, la tarjeta 118 SIM insertada en el dispositivo 114 de comunicación móvil puede proporcionar el componente de autorización. Esto significa que se almacena y ejecuta la correspondiente aplicación de software en la tarjeta 118 SIM. En particular, esta realización tiene de nuevo la ventaja que la tarjeta 118 SIM ya proporciona un entorno seguro para hacer correr la aplicación y que se puede proporcionar la aplicación mediante el operador de red móvil junto con la tarjeta 118 SIM.

Si se firma la solicitud digitalmente mediante la tarjeta 102 de memoria, el componente de autorización verifica la firma digital después de haber recibido la solicitud. Con el fin de verificar la firma digital, se almacena la clave pública asignada a la tarjeta 102 de memoria en el dispositivo 114 de comunicación móvil. Si se proporciona el componente de autorización mediante la tarjeta 118 SIM, se puede almacenar también la clave pública en la tarjeta 118 SIM. Si no se puede verificar satisfactoriamente la firma digital, no se responde la solicitud. En particular, esto significa que la credencial o la clave, que es necesaria para acceder a los datos protegidos en la tarjeta 102 de memoria, no se transmite al terminal 110. Adicionalmente, se puede informar al propietario de la tarjeta acerca de la firma digital inválida presentado información correspondiente en la unidad de visualización del dispositivo 114 de comunicación móvil. Éste informa al propietario de la tarjeta que posiblemente una persona no autorizada intenta acceder a los datos protegidos almacenados en la tarjeta 102 de memoria.

Si se ha verificado satisfactoriamente la firma digital, el componente de autorización preferentemente informa al propietario de la tarjeta acerca de la solicitud. Esto se puede hacer presentando información correspondiente en la unidad de visualización del dispositivo 114 de comunicación móvil. La información puede incluir el MSISDN del terminal 110 desde el que se origina la solicitud. Si existen múltiples grupos de datos protegidos, la información

presentada también especifica el grupo al que se desea el acceso. Cuando se presenta la información, se da al propietario de la tarjeta la oportunidad de dar su consentimiento a la solicitud, es decir permitir acceso a los datos protegidos almacenados en la tarjeta 102 de memoria, o rechazar la solicitud. Para dar su consentimiento a la solicitud, el usuario puede manejar la unidad de entrada del dispositivo 114 de comunicación móvil de una manera predeterminada. Por ejemplo, el usuario puede manejar una tecla predeterminada, si se configura la unidad de entrada como un teclado numérico. Si el usuario quiere rechazar la solicitud, él maneja el dispositivo de entrada de una manera prescrita diferente.

El componente de autorización puede no contestar la solicitud a menos que el usuario de su consentimiento en un intervalo de tiempo predeterminado. Después de que el intervalo de tiempo haya transcurrido, se retira la información de la unidad de visualización. Si el componente de autorización determina que el usuario ha dado su consentimiento en el intervalo de tiempo, genera una respuesta a la solicitud. La respuesta incluye la credencial, que es necesaria para acceder a los datos protegidos, o la clave de desencriptación para desencriptar los datos. Si se almacenan múltiples grupos de datos protegidos en la tarjeta 102 de memoria, el componente de autorización identifica el grupo al que se desea acceso usando la información correspondiente en la solicitud y determina la credencial o la clave criptográfica asignada a este grupo e incluye la credencial o la clave en la respuesta.

Después de haber generado la respuesta que incluye la credencial o la clave necesaria, el componente de autorización controla el dispositivo 114 de comunicación móvil para enviar la respuesta al terminal 110 mediante la red 112 de comunicación móvil. Con este fin, la respuesta se direcciona, en particular, usando el MSISDN del terminal 110, que se incluyó en la solicitud.

En el terminal 110 se procesa la respuesta a la solicitud mediante el componente de acceso. En particular, el componente de acceso reconoce la credencial o la clave para acceder a los datos protegidos en la tarjeta 102 de memoria y extrae esta información a partir de la respuesta. Si se proporciona una credencial, el componente de acceso reenvía la credencial extraída a la tarjeta 102 de memoria. La seguridad lógica de la tarjeta 102 de memoria verifica la credencial, y si la credencial se ha verificado satisfactoriamente, la seguridad lógica permite al terminal 110 o a una aplicación del terminal 110 acceder a los datos protegidos. Como se ha mencionado anteriormente, se puede restringir el acceso permitido a un acceso de lectura, o se puede permitir también manipular datos por medio del terminal 110. Si la respuesta a la solicitud incluye una clave de desencriptación, se usa la clave de desencriptación en el terminal 110 para desencriptar los datos o se reenvía la clave de desencriptación a la tarjeta 102 de memoria y se usa mediante el microcontrolador 106 de la tarjeta 102 de memoria para desencriptar los datos y hacerlos accesibles al terminal 110 o a una aplicación ejecutada en el terminal 110.

Para aumentar la seguridad en el sistema descrito anteriormente, se puede proporcionar que la respuesta a la solicitud del terminal se asegure criptográficamente. Con este fin, se puede usar encriptación asimétrica. En este punto, el componente de autorización puede encriptar la respuesta a la solicitud antes de enviarla al terminal 110. Para encriptar la respuesta se puede usar la clave pública de la tarjeta 102 de memoria. Cuando se recibe la respuesta en el terminal 110, se pasa a la tarjeta 102 de memoria que desencripta la respuesta usando su clave secreta, antes de que se procese la respuesta en el componente de acceso. En otra realización, la unidad de autorización firma digitalmente la respuesta a la solicitud usando una clave secreta asignada a la unidad de autorización. En este caso, la tarjeta 102 de memoria verifica la firma digital usando una clave pública del componente de autorización. La clave pública se almacena de manera segura en la tarjeta 102 de memoria. Esto significa que no se puede sustituir por otra clave pública.

Debe observarse que no se usa clave criptográfica del terminal 110 en el mecanismo descrito anteriormente de modo que no es necesaria una clave de intercambio entre el dispositivo 114 de comunicación móvil y el terminal 110. Por lo tanto se puede acceder a la tarjeta 102 de memoria por medio del terminal 110 ad hoc sin la necesidad de preparar intercambio de datos.

Adicionalmente, el propietario de la tarjeta puede querer restringir la autorización de una persona de acceso a los datos protegidos en la tarjeta hasta un periodo de tiempo limitado o hasta un número de accesos definido. Con este fin, después de que haya transcurrido el periodo de tiempo se puede usar una nueva credencial o se pueden encriptar los datos usando otra clave criptográfica. Esto evita que el usuario del terminal 110 almacene la credencial o clave recibidas después de que haya transcurrido el periodo de tiempo.

En una realización, se puede generar una nueva credencial en el dispositivo 114 de comunicación móvil del propietario de la tarjeta, particularmente en la tarjeta 118 SIM del propietario de la tarjeta, y la tarjeta 118 SIM puede proporcionar una funcionalidad para instalar la nueva credencial en la tarjeta 102 de memoria cuando se conecta la tarjeta 102 de memoria al dispositivo 114 de comunicación móvil. En este punto, la seguridad lógica de la tarjeta 102 de memoria puede no permitir la instalación a menos que se proporcione una credencial adicional, que se conoce únicamente por el propietario de la tarjeta. De manera similar, el dispositivo 114 de comunicación móvil, particularmente la tarjeta 118 SIM, puede proporcionar una funcionalidad para desencriptar los datos y encriptarlos usando una nueva clave.

En realizaciones adicionales, la respuesta del dispositivo 114 a la solicitud puede comprender información de tiempo además de la credencial o en lugar de la credencial. La información de tiempo puede especificar un punto en el

tiempo, es decir un tiempo absoluto, hasta el que se puede acceder a los datos protegidos almacenados en la tarjeta 102 de memoria por medio del terminal 110. Se puede introducir la información de tiempo por el propietario de la tarjeta cuando maneja el dispositivo 114 para dar su consentimiento para el acceso a los datos protegidos.

Antes de que la tarjeta 102 de memoria permita al terminal 110 acceder a los datos protegidos almacenados en la memoria 104, recibe información de tiempo desde una unidad de reloj. Preferentemente, se incluye la unidad de reloj en un servidor de tiempo, que se conecta al terminal 110 mediante la red 112 de comunicación. La información para establecer una conexión al servidor 116 de tiempo, tal como la dirección de red del servidor 116 de tiempo, se almacena de manera segura en la tarjeta 102 de memoria. El intercambio de datos entre la tarjeta 102 de memoria y el servidor de tiempo se puede basar en el HTPP (protocolo de transferencia hipertexto). En una realización, puede haber una conexión “continua” entre la tarjeta 102 de memoria y el servidor 116 de tiempo mediante el terminal 110 usando el HTTP. Esto significa, que se puede prescindir de una conversión de protocolo de la solicitud de la tarjeta 102 de memoria para proporcionar información de tiempo y de la respuesta del servidor 116 de tiempo. En otra realización, se incluye la información de tiempo generada por una unidad de reloj contenida en el dispositivo 114 de comunicación móvil del propietario de la tarjeta en respuesta a la solicitud del terminal 110.

La información de tiempo proporcionada por la unidad de reloj especifica el tiempo actual como medido en la unidad de reloj. Adicionalmente, se asegura criptográficamente la información de tiempo de tal manera que un receptor puede verificar que se origina la información de tiempo desde la unidad de reloj y que no se modificó la información de tiempo durante la transmisión al receptor.

Si se proporciona la información de tiempo mediante el dispositivo 114 de comunicación móvil en la respuesta a la solicitud, se puede asegurar de la misma manera que la propia solicitud.

Si se recupera la información de tiempo desde un servidor de tiempo, se encripta la información de tiempo usando una clave de encriptación secreta del servidor de tiempo. Como una alternativa la información de tiempo incluye una firma digital del servidor, es decir, valor de comprobación, que se obtiene del contenido de la información y se encripta usando la clave secreta de la unidad de reloj. La clave de encriptación secreta es parte de un par de claves asimétricas que incluyen adicionalmente una clave de desencriptación pública para desencriptar datos, que se han encriptado usando la clave de encriptación secreta. La clave de desencriptación pública de la unidad de reloj se almacena de manera segura en la tarjeta 102 de memoria. El almacenamiento seguro evita que se sustituya la clave por otra clave. Como una alternativa a la utilización del par de claves asimétricas, es posible, de manera similar, utilizar encriptación simétrica con una clave para encriptación y desencriptación que se comparte entre la unidad de reloj y la tarjeta 102 de memoria. Cuando la tarjeta 102 de memoria recibe la información de tiempo, verifica la autenticidad de la información de tiempo. Con este fin, la tarjeta 102 de memoria desencripta la información de tiempo o la firma digital con la clave de desencriptación pública, verificando de esta manera la autenticidad e integridad de la información de tiempo. Si se usa una firma digital, la tarjeta 102 de memoria desencripta el valor de comprobación confirmando de esta manera que se origina la información de tiempo desde la unidad de reloj. A continuación, la tarjeta 102 de memoria compara el valor de comprobación con un valor de comprobación auto-generado y determina que la información de tiempo está inalterada, si coinciden ambos valores de comprobación.

Si no se puede verificar satisfactoriamente la autenticidad de la información de tiempo, la tarjeta 102 de memoria deniega el acceso a los datos protegidos almacenados en la tarjeta 102 de memoria. Después de que se han validado satisfactoriamente la autenticidad e integridad de la información de tiempo, la tarjeta 102 de memoria compara la información de tiempo con el punto en el tiempo que se especificó por el propietario de la tarjeta. Si este punto en el tiempo sigue al punto en el tiempo especificado en la información de tiempo recibida desde el servidor de tiempo o la unidad de reloj del dispositivo 114 de comunicación móvil, la tarjeta 102 de memoria permite acceder a los datos protegidos almacenados en la tarjeta 102 de memoria por medio del terminal 110.

Para determinar cuándo se alcanza el punto almacenado en el tiempo, la tarjeta 102 de memoria puede determinar una diferencia entre el tiempo indicado mediante la unidad de reloj y el punto en el tiempo especificado por el propietario de la tarjeta. A continuación, la tarjeta 102 de memoria inicia un contador de tiempo interno. Cuando se ha alcanzado un valor de contador que corresponde con la diferencia de tiempo calculada, la tarjeta 102 de memoria determina que ha transcurrido el periodo de tiempo que corresponde a la diferencia calculada y bloquea los datos protegidos de nuevo contra acceso desde fuera de la tarjeta 102 de memoria.

En otra realización, la tarjeta 102 de memoria puede recuperar repetidamente información de tiempo desde el servidor de tiempo. En particular, la tarjeta 102 de memoria puede recuperar la información de tiempo en intervalos de tiempo predeterminados regulares, que no son demasiado largos de modo que el usuario del terminal 110 no tenga acceso a la información protegida significativamente después del punto almacenado en el tiempo. Cada vez que la tarjeta 102 de memoria recupera información de tiempo desde el servidor de tiempo, compara el tiempo especificado en la información de tiempo con el punto en el tiempo especificado por el propietario de la tarjeta y desbloquea los datos protegidos cuando el punto en el tiempo especificado por el propietario de la tarjeta ya no es en el futuro relativo al tiempo actual como se especifica en la información de tiempo recuperada desde el servidor de tiempo. La tarjeta 102 de memoria puede también bloquear los datos protegidos, si no se puede verificar satisfactoriamente la información de tiempo recibida desde el servidor de tiempo. Y la tarjeta de memoria preferentemente también bloquea los datos protegidos, si no se puede recuperar información de tiempo desde el

servidor de tiempo, puesto que en este caso, la tarjeta de memoria no puede determinar, si se ha alcanzado el punto de tiempo especificado por el propietario de la tarjeta.

Realizaciones adicionales se diferencian de las realizaciones descritas anteriormente en que el propietario de la tarjeta especifica un periodo de tiempo para acceder a la tarjeta 102 de memoria en lugar de un punto absoluto en el tiempo hasta el que se pueda acceder a la tarjeta 102 de memoria.

En estas realizaciones, se puede usar de manera similar un servidor de tiempo. En este punto, la tarjeta 102 de memoria puede almacenar la información de tiempo que recupera del servidor de tiempo cuando la tarjeta de memoria recupera la información de tiempo por primera vez. A continuación, la tarjeta de memoria puede de nuevo recuperar repetidamente información de tiempo desde el servidor 116 de tiempo. Cada vez que la unidad de memoria recupera información de tiempo desde el servidor 116 de tiempo, compara el tiempo especificado en la información de tiempo con el tiempo almacenado y bloquea los datos protegidos de nuevo cuando la diferencia entre estos tiempos excede el periodo de tiempo especificado por el usuario. En otros aspectos, el mecanismo de seguridad puede ser el mismo que en las realizaciones descritas anteriormente. En particular, la tarjeta 102 de memoria puede bloquear los datos protegidos, si no se puede recuperar información de tiempo desde el servidor de tiempo, si no se puede autenticar satisfactoriamente la información de tiempo recuperada y si la información de tiempo recibida del servidor 116 de tiempo especifica un tiempo anterior que la información de tiempo recibida antes.

En una realización adicional, en la que el usuario especifica un periodo de tiempo para acceder a la tarjeta 102 de memoria en lugar de un punto absoluto en el tiempo hasta el que se pueda acceder a la tarjeta 102 de memoria, la tarjeta 102 de memoria utiliza un contador de tiempo interno para determinar si ha transcurrido el periodo de tiempo. Se inicia el contador de tiempo, después de que se recibe la respuesta del dispositivo 114 de comunicación móvil en el terminal 110. Cuando se ha alcanzado un valor de contador que corresponde al periodo de tiempo especificado, la tarjeta 102 de memoria determina que ha transcurrido el periodo de tiempo y bloquea los datos protegidos de nuevo contra acceso desde fuera de la tarjeta 102 de memoria.

Las realizaciones descritas anteriormente permiten al propietario de la tarjeta especificar un punto en el tiempo hasta el que se pueda acceder a los datos protegidos almacenados en la tarjeta 102 de memoria por otra persona por medio de un terminal 110 o un periodo de tiempo para acceder a los datos. El propietario de la tarjeta puede especificar el punto en el tiempo o el periodo de tiempo antes de traspasar la tarjeta 102 de memoria a otra persona. Especificando un corto periodo de tiempo adecuado, en el que la otra persona pueda acceder a los datos protegidos, se puede evitar que terceras partes no autorizadas puedan acceder a los datos protegidos. Por lo tanto, se puede delimitar el acceso a los datos protegidos a personas seleccionadas de una manera segura.

Mientras que la invención se ha ilustrado y descrito en detalle en los dibujos y la descripción anterior, se han de considerar tal ilustración y descripción ilustrativas o ejemplares y no restrictivas; la invención no está limitada a las realizaciones desveladas.

Por ejemplo, es posible manejar la invención en una realización en la que la no se configura la red 112 de comunicación como red 112 de comunicación móvil sino como otra red de comunicación adecuada para conectar el dispositivo 114 del propietario de la tarjeta 102 de memoria y del terminal 110.

Se pueden entender y efectuar otras variaciones de las realizaciones desveladas por los expertos en la materia en la práctica de la invención reivindicada, a partir de un estudio de los dibujos, la divulgación y las reivindicaciones adjuntas.

En las reivindicaciones, las palabras “que comprende” no excluye otros elementos o etapas, y el artículo indefinido “un” o “una” no excluye una pluralidad. Un solo procesador u otra unidad puede cumplir las funciones de varios elementos descritos en las reivindicaciones. El mero hecho de que se describan ciertas medidas en las reivindicaciones dependientes mutuamente diferentes no indica que no se pueda usar una combinación de estas medidas con ventaja.

Cualquier signo de referencia en las reivindicaciones no se debe interpretar como que limita el alcance.

REIVINDICACIONES

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

- recibir la tarjeta (102) de memoria en un terminal (110);
- transmitir una solicitud para acceder a los datos mediante un enlace de comunicación desde el terminal (110) al dispositivo (114);
- tras la recepción de la solicitud, enviar la primera información desde el dispositivo (114) al terminal (110) mediante el enlace de comunicación;
- recibir la primera información en el terminal (110) y acceder a los datos usando la primera información,

caracterizado porque se envía la primera información al terminal (110) en respuesta a una operación de usuario efectuada por medio de una interfaz de usuario del dispositivo (114).

2. El procedimiento de acuerdo con la reivindicación 1, en el que el dispositivo (114) es un dispositivo de comunicación móvil y el enlace de comunicación comprende una red (112) de comunicación móvil.

3. El procedimiento de acuerdo con la reivindicación 1 o 2, en el que el dispositivo (114) de comunicación móvil comprende una tarjeta (118) SIM que proporciona la primera información.

4. El procedimiento de acuerdo con una de las reivindicaciones precedentes, en el que se establece el enlace de comunicación desde el terminal (110) al dispositivo (114) usando la segunda información, leyéndose dicha segunda información desde la tarjeta (102) de memoria mediante el terminal (110).

5. El procedimiento de acuerdo con la reivindicación 5-4, en el que la segunda información comprende un Número de Red Digital de Servicios Integrados de Abonado Móvil, MSISDN, del dispositivo (114).

6. El procedimiento de acuerdo con una de las reivindicación precedentes, en el que la solicitud para acceder a los datos incluye una firma digital de la tarjeta (102) de memoria, verificándose dicha firma digital en el dispositivo (114), particularmente en la tarjeta (118) SIM.

7. El procedimiento de acuerdo con una de las reivindicaciones precedentes, en el que se almacenan los datos de manera encriptada en la tarjeta (102) de memoria y la primera información comprende una clave criptográfica para desencriptar los datos.

8. El procedimiento de acuerdo con una de las reivindicaciones precedentes, en el que la tarjeta (102) de memoria comprende una seguridad lógica que permite acceder a los datos después de haber verificado satisfactoriamente la primera información.

9. El procedimiento de acuerdo con una de las reivindicaciones precedentes, en el que la tarjeta (102) de memoria comprende datos adicionales, que no son accesibles usando la primera información.

10. Un sistema que comprende un terminal (110) para acceder a datos almacenados en una tarjeta (102) de memoria, comprendiendo el terminal

- un medio (108) de aceptación adaptado para recibir la tarjeta (102) de memoria;
- un dispositivo de lectura adaptado para leer los datos desde la tarjeta (102) de memoria usando la primera información;
- un componente de envío adaptado para enviar una solicitud para acceder a los datos mediante un enlace de comunicación;
- un componente de recepción adaptado para recibir la primera información mediante el enlace de comunicación en respuesta a la solicitud;

comprendiendo el sistema adicionalmente un dispositivo, comprendiendo dicho dispositivo un medio de autorización para proporcionar la primera información en respuesta a una recepción de la solicitud en el dispositivo (114),

caracterizado porque el dispositivo (114) comprende adicionalmente una interfaz de usuario acoplada al medio de autorización, adaptándose el medio de autorización para proporcionar la primera información en respuesta a una operación de usuario adquirida por medio de la interfaz de usuario.

11. El sistema de acuerdo con la reivindicación 10, en el que el dispositivo (114) es un dispositivo de comunicación móvil y el enlace de comunicación incluye una red de comunicación móvil.

12. El sistema de acuerdo con la reivindicación 10 u 11, que comprende una tarjeta SIM que incluye el medio de autorización.

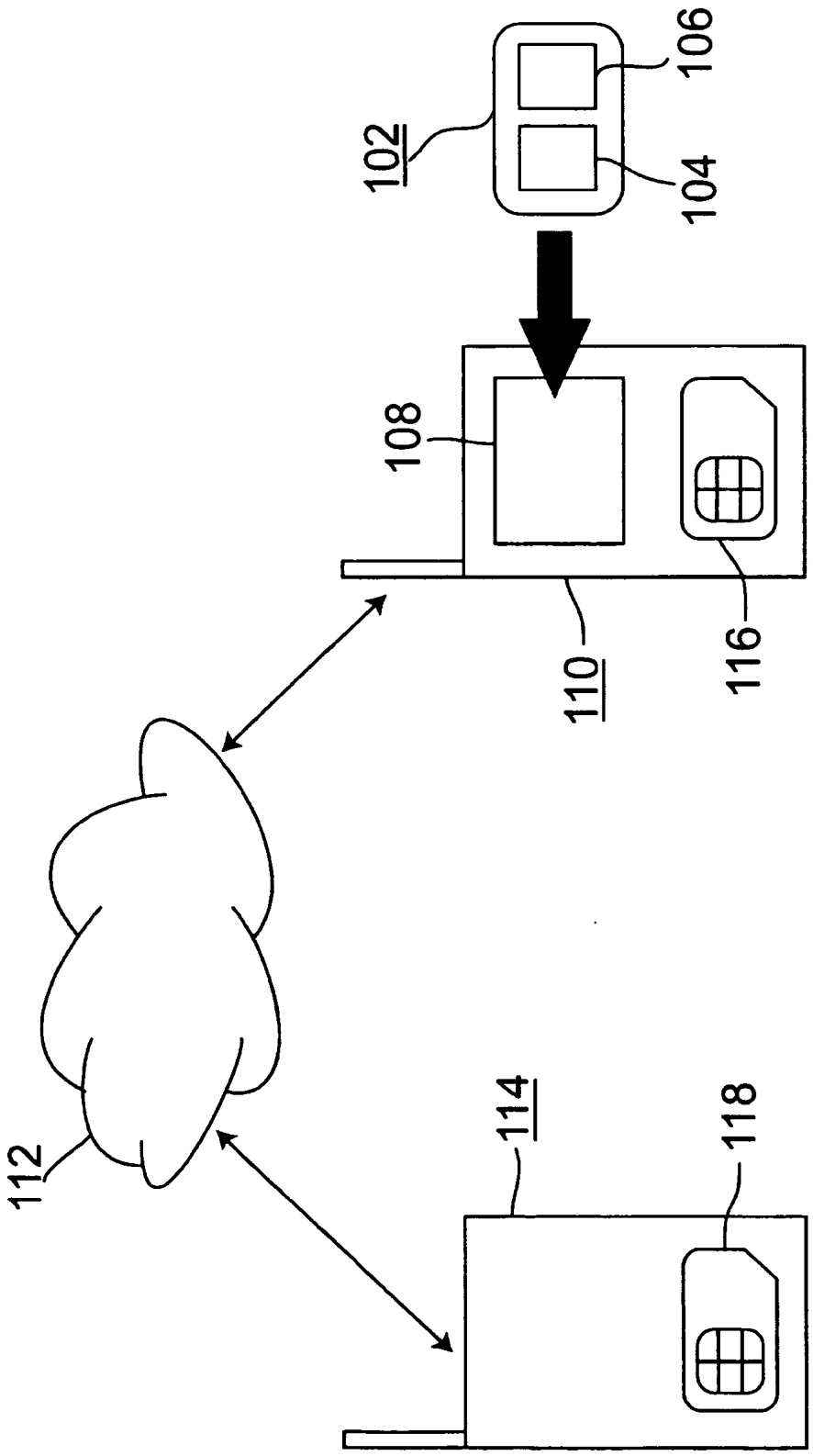

Fig. 1