(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 279 082**

(51) Int. Cl.:
G06F 1/00 (2006.01)
G07F 7/10 (2006.01)
H04Q 7/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **03292173 .6**
(86) Fecha de presentación : **03.09.2003**
(87) Número de publicación de la solicitud: **1513040**
(87) Fecha de publicación de la solicitud: **09.03.2005**

(54) Título: **Sistema y método para distribuir datos de acceso a contenidos.**

(45) Fecha de publicación de la mención BOPI:
16.08.2007

(45) Fecha de la publicación del folleto de la patente:
16.08.2007

(73) Titular/es: **FRANCE TELECOM**
6, place d'Alleray
75015 Paris, FR

(72) Inventor/es: **Ondet, Olivier;**
Gilbert, Henri;
Chauvaud, Pascal y
Milhau, Michel

(74) Agente: **Lehmann Novo, María Isabel**

DESCRIPCIÓN

Sistema y método para distribuir datos de acceso a contenidos.

Campo de la invención

La presente invención está relacionada también con sistemas y métodos para distribuir datos de acceso a contenidos a los usuarios, proporcionando los datos de acceso a contenidos datos de gestión de derechos que indican el derecho de un usuario a reproducir y/o copiar el contenido distribuido.

En algunas realizaciones, los datos de acceso a contenidos se distribuyen a través de una red de comunicaciones. La red de comunicaciones puede incluir una red de comunicaciones móviles.

Antecedentes de la invención

Con la creciente anchura de banda proporcionada por la mejora de la infraestructura de las comunicaciones móviles, a medida que las redes migran de redes 2G a 3G, hay un requisito de una instalación para distribuir contenidos digitales a usuarios de móviles, de manera que dé soporte a los derechos del proveedor de contenidos. Un ejemplo de contenidos puede ser un clip o una película de vídeo, que un usuario puede desear descargar para ver o copiar. Otros ejemplos incluyen contenidos multimedia, que pueden combinar audio, vídeo y datos interactivos.

Una preocupación creciente de los proveedores de contenidos es que se pierden ingresos a través de las copias pirata ilegales que se facilitan en formato digital del contenido y la disponibilidad de equipos, tales como ordenadores personales que pueden ser utilizados para generar fácilmente copias del contenido de alta calidad. Por tanto, aunque hay un requisito creciente para distribuir producciones de contenidos a los usuarios, también existe la preocupación de que la distribución de este contenido no debe dar lugar a la proliferación de copias y reproducciones no autorizadas. Se requiere por tanto una gestión y control de los derechos del contenido, que se denomina generalmente gestión de derechos digitales. La distribución de contenidos está normalmente asociada con una licencia, que determina las condiciones bajo las cuales qué reproducción del contenido se puede hacer y/o las condiciones bajo las cuales puede ser copiado el contenido. Por ejemplo, el contenido puede ser reproducido solamente una vez o puede ser reproducido muchas veces y copiado solamente una vez. Alternativamente, el contenido puede ser reproducido cualquier número de veces y puede ser copiado libremente.

La combinación de una demanda creciente de contenidos que deben ser entregados a usuarios de móviles en combinación con el requisito de gestionar los derechos de ese contenido requiere la cualidad de distribuir el contenido y gestionar los derechos del contenido una vez entregado.

En el documento US-B-6.466.671 se describe un receptor basado en tarjeta inteligente para señales radiodifundidas encriptadas. Las señales radiodifundidas son descodificadas bajo el control de un microprocesador provisto o de una tarjeta inteligente.

Sumario de la invención

De acuerdo con la presente invención, se proporciona un sistema para distribuir datos de acceso a contenidos a un usuario. Los datos de acceso a contenidos proporcionan datos de gestión de derechos que indican el derecho de un usuario a reproducir y/o copiar el contenido distribuido. El sistema comprende un dispositivo de aplicaciones que incluye un programa de aplicación que forma un reproductor confiable para recibir y reproducir y/o copiar el contenido, y un dispositivo de acceso por tarjeta inteligente que funciona accediendo a una tarjeta inteligente que está asociada unívocamente a un usuario. La tarjeta inteligente puede ser, por ejemplo, un Módulo de Identidad de Abonado (SIM). El sistema incluye un servidor confiable que funciona de manera que puede comunicar con seguridad los datos de acceso a la tarjeta inteligente, a través de una red de comunicaciones, encriptando los datos de acceso al contenido utilizando una primera clave (KC) de encriptación pre-almacenada en la tarjeta inteligente y conocida para el servidor confiable. La tarjeta inteligente funciona desencriptando los datos de acceso al contenido utilizando la primera clave (KC) de encriptación y almacenando los datos de acceso a contenidos en la tarjeta inteligente. El reproductor confiable funciona accediendo a los datos de gestión de derechos proporcionados con los datos de acceso a contenidos de la tarjeta inteligente, y reproduciendo y/o copiando el contenido de acuerdo con los datos de gestión de derechos. Al reproductor confiable se le permite acceso a los datos de acceso a contenidos en la tarjeta inteligente, solamente después de una autenticación mutua entre la tarjeta inteligente y el reproductor confiable.

En una realización, el contenido recibido por el dispositivo de aplicaciones ha sido encriptado utilizando una clave de encriptación de contenidos, los datos de acceso a contenidos incluyen la clave de contenidos para desencriptar el contenido. El sistema proporciona así una cualidad de distribuir el contenido y de gestionar los derechos en el contenido de una manera económica utilizando prestaciones de seguridad inherentes a la tarjeta inteligente. La eficiencia de costes proviene parcialmente de utilizar la encriptación de clave privada utilizando la tarjeta inteligente.

Los datos de acceso al contenido pueden incluir condiciones para el uso de datos de contenido. Los datos de acceso a contenidos pueden proporcionar por tanto datos digitales de gestión de derechos que indican, por ejemplo,

las condiciones para reproducir los datos de contenido y/o una indicación sobre si el contenido puede ser copiado y, si es así, el número de veces que puede ser copiado el contenido.

Realizaciones de la presente invención utilizan cualidades inherentes de las tarjetas inteligentes, que están asociadas unívocamente con un usuario particular. Las tarjetas inteligentes tales como la SIM o la USIM incluyen una clave pre-almacenada para efectuar comunicaciones seguras con una entidad a través de una red de comunicaciones. Una tarjeta inteligente incluye, por tanto, alguna disposición de equipo físico informático, lo cual restringe el acceso a partes de la memoria formada en la tarjeta inteligente. Por tanto, no se puede acceder a la clave almacenada dentro de la tarjeta inteligente a menos que se cumplan ciertas condiciones. Como resultado, la clave proporciona una instalación segura para comunicarse a través de la red.

Aunque el dispositivo de aplicaciones puede estar provisto de una instalación para comunicarse a través de una red, en algunas realizaciones el sistema incluye un dispositivo de red, el cual proporciona una instalación para comunicarse con seguridad con la red utilizando la clave de la tarjeta inteligente. El dispositivo de red incluye, por tanto, el dispositivo de acceso a la tarjeta inteligente. La tarjeta inteligente proporciona una instalación para recibir con seguridad los datos de acceso al contenido desde un servidor confiable, a través del dispositivo de red, estando encriptados los datos de acceso al contenido utilizando la primera clave pre-almacenada en la tarjeta inteligente. Los datos de acceso al contenido pueden ser comunicados al dispositivo de red que identifica las condiciones para la reproducción del contenido y/o que proporciona, por ejemplo, una segunda clave de encriptación de contenidos para desencriptar el contenido.

Realizaciones de la presente invención también incluyen una disposición para proporcionar una tercera clave de encriptación, que es compartida localmente entre el dispositivo de aplicaciones y el dispositivo de red. La tercera clave (KCP) de encriptación local es generada aleatoriamente por el dispositivo de aplicaciones y es encriptada utilizando una cuarta clave de encriptación por programa pre-almacenada en el reproductor confiable (cuarta clave (KP) de encriptación por programa) dentro del dispositivo de aplicaciones. La tercera clave local es comunicada entonces a través del dispositivo de red al servidor confiable. El servidor confiable y el dispositivo de red pueden entonces comunicar con seguridad la tercera clave local utilizando la primera clave de encriptación almacenada en la KC de la tarjeta inteligente. Una vez que el dispositivo de aplicaciones y el dispositivo de red tienen la tercera clave secreta local de encriptación, los datos de acceso al contenido pueden ser comunicados entre la tarjeta inteligente del dispositivo de red y el reproductor confiable del dispositivo de aplicaciones. Se proporciona por tanto una instalación económica para comunicaciones seguras que permite al dispositivo de red que se comunica con la red, ser independiente del dispositivo de aplicaciones para reproducir el contenido. El dispositivo de red y el dispositivo de aplicaciones pueden ser, por tanto, optimizados para implementar las funciones de comunicaciones por la red y de reproducción del contenido, respectivamente. Por ejemplo, el dispositivo de aplicaciones podría ser un Asistente Digital Personal (PDA) o un Ordenador Personal (PC), mientras que el dispositivo de red podría ser un radio-teléfono móvil. Como la comunicación segura se implementa utilizando la encriptación de clave privada, la seguridad se proporciona con un coste relativamente reducido en comparación con la encriptación de clave pública que requiere mayor potencia de proceso y por tanto mayor gasto.

En algunas realizaciones, el dispositivo de aplicaciones autentica la presencia de la tarjeta inteligente y/o copiada antes de determinar si el contenido puede ser reproducido. La autenticación puede incluir el intercambio de mensajes utilizando la tercera clave de encriptación local KCP, y determinando el estado actual de los datos digitales de gestión de derechos para determinar si se permite la reproducción del contenido.

En las reivindicaciones anexas, se definen diversos aspectos y características adicionales de la presente invención.

Breve descripción de los dibujos

Se describirán ahora realizaciones de la presente invención, solamente a modo de ejemplo, con referencia a los dibujos que se acompañan, en los que las partes similares están provistas de números de referencia correspondientes y en los que:

La figura 1 es un diagrama esquemático de bloques de un sistema para proporcionar servicios a un usuario utilizando un dispositivo de aplicaciones en el cual los datos sensibles son distribuidos a través de un dispositivo de red;

la figura 2 es un diagrama esquemático de bloques de un ejemplo de dispositivo de red y un ejemplo de dispositivo de aplicaciones, el cual aparece en la figura 1;

la figura 3 es un diagrama esquemático de bloques de otro ejemplo de dispositivo de aplicaciones que incorpora la capacidad de comunicaciones por red;

la figura 4 es un diagrama esquemático de bloques de una tarjeta inteligente;

la figura 5 es un diagrama de bloques de partes del sistema ilustrado en la figura 1 para ser utilizado en la distribución de datos sensibles;

la figura 6 es un diagrama de flujo que representa un proceso para establecer una clave local compartida entre una tarjeta inteligente del dispositivo de red y un programa de aplicaciones que se ejecuta en el dispositivo de aplicaciones ilustrado en la figura 1;

la figura 7 es un diagrama de flujo que ilustra un proceso para distribuir datos sensibles al programa de aplicaciones utilizando la tarjeta inteligente de la figura 6, incluyendo la autenticación mutua de la tarjeta inteligente y del programa de aplicaciones;

la figura 8 es un diagrama de flujo que ilustra el funcionamiento de la tarjeta inteligente y del programa de aplicaciones de la figura 6, cuando la tarjeta inteligente actúa como un servidor local;

la figura 9 es un diagrama esquemático de bloques que ilustra partes de un sistema que están configuradas para distribuir contenidos a un dispositivo de aplicaciones con datos de acceso a contenidos;

la figura 10 es un diagrama de flujo que ilustra un proceso para entregar datos de acceso a contenidos a un dispositivo de aplicaciones para su uso en el acceso a contenidos;

la figura 11 es un diagrama de flujo que ilustra un proceso para almacenar con seguridad datos actualizados de acceso a contenidos en una tarjeta inteligente ilustrada en la figura 9; y

la figura 12 es un diagrama de flujo que ilustra un proceso en el cual se efectúa la autenticación mutua entre una tarjeta inteligente y un reproductor confiable y se comprueban los datos de gestión de derechos antes de reproducir el contenido.

Descripción de las realizaciones de ejemplo

Red de ejemplo

La figura 1 proporciona un ejemplo de configuración en el cual se distribuyen datos a un dispositivo de aplicaciones a través de un dispositivo de red. En la figura 1, una red 1 incluye una cualidad por la cual se puede comunicar con un dispositivo ND de red, utilizando por ejemplo un enlace 2 de comunicaciones móviles. El enlace 2 de comunicaciones móviles se establece entre un nodo o estación base 3 y el dispositivo ND de red, de acuerdo con una interfaz estándar establecida. Si la red incluye una red radio UMTS de móviles, la interfaz de comunicaciones puede operar de acuerdo con el estándar de Red de Acceso Radio Terrestre Universal (UTRAN). La red 1 proporciona una prestación por la cual se comunican diversos tipos de datos a equipos conectados a la red. Por ejemplo, se puede disponer un servidor CS de contenidos para distribuir el contenido 4 a un dispositivo AD de aplicaciones. También se ilustra en la figura 1 un servidor confiable TS el cual, como se explicará en breve, proporciona la prestación de comunicar datos sensibles al dispositivo ND de red para su uso por el dispositivo AD de aplicaciones.

Se describirán ahora realizaciones de la presente invención con referencia a la configuración ilustrada en la figura 1, en la que un dispositivo ND de red está asociado operativamente con un dispositivo AD de aplicaciones. La configuración del dispositivo ND de red y del dispositivo AD de aplicaciones proporciona la cualidad de comunicar datos sensibles para su uso con programas de aplicaciones que se están ejecutando en el dispositivo de aplicaciones. En una realización de ejemplo, el contenido 4 es reproducido por el dispositivo AD de aplicaciones de acuerdo con datos de control de acceso, que pueden constituir, en una realización, un ejemplo de datos sensibles. Los datos de control de acceso pueden indicar condiciones para la reproducción y copia del contenido. Los datos de control de acceso pueden proporcionar también una clave para desencriptar el contenido, si el contenido ha sido encriptado antes de ser descargado en el dispositivo AD de aplicaciones. Aunque en la figura 1 el contenido puede ser descargado desde un servidor CS de contenidos, el contenido puede ser recibido por el dispositivo AD de aplicaciones a través de cualquier forma conveniente, por ejemplo a través de un portador de datos (tal como DVD, CD ROM) o por cualquier otro medio convencional conveniente y desde cualquier fuente. El dispositivo ND de red y el dispositivo AD de aplicaciones están ilustrados con más detalle en la figura 2.

Dispositivos de red y de aplicaciones

En la figura 2, el dispositivo ND de red se ilustra incluyendo una tarjeta inteligente 20 que está cargada en un dispositivo 22 de acceso de tarjetas inteligentes que forma parte del dispositivo de red. Un bus (vía de comunicaciones) 24 de acceso conecta el dispositivo de acceso de tarjetas inteligentes a un procesador 26 de datos para proporcionar acceso a la tarjeta inteligente 20. El procesador de datos está conectado a través del bus 28 de comunicaciones a una interfaz 30 de comunicaciones que funciona de acuerdo con un estándar de comunicaciones por red para comunicarse con la red 1, como se ilustra en la figura 1. Así, la interfaz 30 de comunicaciones puede operar, por ejemplo, de acuerdo con la interfaz de Red de Acceso Radio Terrestre Universal (UTRAN) utilizando la antena 32 para comunicarse a través del enlace 2 de comunicaciones, como se ilustra en la figura 1. La interfaz 30 de comunicaciones proporciona así la cualidad de conectar el dispositivo ND de red con la red 1.

El dispositivo ND de red incluye también una segunda interfaz 34 de comunicaciones conectada a través de un bus interno 36 al procesador 26 de datos, para formar un enlace de comunicaciones locales con un dispositivo AD de aplicaciones. En el dispositivo AD de aplicaciones está incluido una correspondiente interfaz 40 de comunicaciones

para comunicar datos entre el dispositivo ND de red y el dispositivo AD de aplicaciones. Un enlace de comunicaciones, representado por una flecha 42 de doble cabeza, está formado por la interfaz 34 de comunicaciones del dispositivo ND de red y la interfaz 40 de comunicaciones del dispositivo AD de aplicaciones. El enlace de comunicaciones proporciona la cualidad de comunicarse localmente entre el dispositivo AD de aplicaciones y el dispositivo ND de red. En algunas realizaciones, el enlace de comunicaciones puede estar formado mediante el funcionamiento de los interfaces 34, 40 de comunicaciones utilizando, por ejemplo, los estándares Bluetooth, RS232 ó IEEE802.3.

El dispositivo AD de aplicaciones incluye también un procesador 44 de datos que está configurado para ejecutar programas de aplicaciones que proporcionan servicios al usuario.

Aunque el dispositivo ND de red y el dispositivo AD de aplicaciones están ilustrados en las figuras 1 y 2 como dispositivos independientes, en otras realizaciones el dispositivo de aplicaciones y el dispositivo de red pueden estar formados físicamente como un mismo dispositivo. Un ejemplo de tales realizaciones está ilustrado en la figura 3.

En la figura 3, se dispone un dispositivo AD.1 de aplicaciones con una instalación para comunicarse con la red 1, utilizando una interfaz 30.1 de comunicaciones, que se corresponde sustancialmente con la interfaz de comunicaciones del dispositivo ND de red ilustrado en la figura 2. Para el dispositivo AD.1 de aplicaciones ilustrado en la figura 3, los procesadores 26, 44 de datos del dispositivo de aplicaciones y del dispositivo de red ilustrados en la figura 2, son sustituidos por el mismo procesador 26.1 de datos. El procesador 26.1 de datos ejecuta programas de aplicación y también controla la comunicación con la red 1 y los accesos a la tarjeta inteligente 20. El dispositivo AD.1 de aplicaciones podría ser un Asistente Digital Personal (PDA), un teléfono móvil o un dispositivo similar. El dispositivo ND de red ilustrado en la figura 2 podría ser implementado como un teléfono móvil o un PDA, mientras que el dispositivo AD de aplicaciones podría ser un ordenador personal (PC).

En las secciones siguientes se darán más explicaciones acerca del funcionamiento del dispositivo de aplicaciones y del dispositivo de red. Sin embargo, por facilidad de la explicación, se adoptará el sistema ilustrado en la figura 1, que incluye una red independiente y dispositivos de aplicaciones.

Tarjeta inteligente

La figura 4 ofrece un diagrama de bloques simplificado que ilustra la forma de una tarjeta inteligente típica. La tarjeta inteligente 20 se define generalmente como poseedora de ciertas prestaciones de proceso en combinación con una memoria y una interfaz. Como se ilustra en la figura 4, la tarjeta inteligente 20 incluye una memoria 50, conectada a un procesador 52 de datos a través de un canal 54 de interfaz. A la interfaz 54 de comunicaciones se accede a través del dispositivo 22 de acceso a la tarjeta inteligente (ilustrado en la figura 2), con el fin de leer datos de la memoria 50 y grabarlos en ella. Sin embargo, una de las características de las tarjetas inteligentes es que la interfaz 54 no tiene acceso directo a la memoria 50. Así, solamente el procesador 52 puede acceder a la memoria 50 y por tanto no todo es accesible a través de la interfaz 54. Típicamente, una tarjeta inteligente puede incluir datos tales como una clave KC de encriptación, que está pre-almacenada en una memoria 50. A la clave KC de encriptación no se puede acceder desde la interfaz 54, pero puede ser utilizada para encriptar datos alimentados a la tarjeta inteligente que pueden ser encriptados después por el procesador 52 de datos utilizando la clave KC pre-almacenada. Por tanto, la tarjeta inteligente se puede caracterizar generalmente como poseedora de limitaciones de equipo físico informático, lo cual restringe el acceso a la memoria 50, proporcionando así alguna seguridad a los datos almacenados en la tarjeta inteligente. Como será explicado en breve, la tarjeta inteligente proporciona la cualidad de almacenar datos sensibles y de desencriptar y encriptar datos que se han de comunicar hacia y desde la red y un programa de aplicaciones.

Un Módulo de Identidad del Abonado (SIM) es un ejemplo de tarjeta inteligente, siendo otro ejemplo un Módulo de Identidad de Abonado Universal (USIM), que son proporcionados por los proveedores de servicios de red y están unívocamente asociados con usuarios de una red de telecomunicaciones, tal como GSM o UMTS. Así, cuando se emite desde el proveedor de servicios de red a un usuario, la tarjeta inteligente está unívocamente asociada con ese usuario e incluye la clave KC de encriptación pre-almacenada para ser utilizada solamente con la tarjeta inteligente.

Comunicación segura entre el dispositivo de red y el dispositivo de aplicaciones

La figura 5 ofrece una ilustración de partes del sistema de la figura 1, que incluyen el dispositivo ND de red y el dispositivo AD de aplicaciones, e ilustra una configuración para establecer comunicaciones seguras entre la tarjeta inteligente del dispositivo de red y el programa de aplicaciones en el dispositivo de aplicaciones, y para efectuar la autenticación mutua. La figura 5 muestra también el servidor confiable TS de la figura 1, aunque los demás elementos de red que aparecen en la figura 1 no están representados en la figura 5 por razones de claridad.

Realizaciones de la presente invención proporcionan la cualidad de distribuir datos sensibles para ser utilizados por un dispositivo AD de aplicaciones utilizando características de seguridad inherentes a las tarjetas inteligentes que pueden ser emitidas a los usuarios por los proveedores de servicios de red para ser utilizadas con dispositivos de red. Una ventaja proporcionada por realizaciones de la presente invención es que se consigue a un coste comparativamente bajo una instalación para efectuar comunicaciones seguras entre un dispositivo de aplicaciones y un dispositivo de red, porque se puede utilizar la encriptación de clave privada en lugar de la encriptación de clave pública que requiere un aumento de la capacidad de proceso.

La figura 5 proporciona una ilustración de una instalación para efectuar una comunicación segura generando con seguridad una clave local exclusiva (KCP). La clave local se genera en el dispositivo AD de aplicaciones por medio de un programa de aplicaciones para ser comunicada al dispositivo de red. Se proporciona así una clave secreta compartida KCP para comunicar y autenticar acciones por el dispositivo AD de aplicaciones y el dispositivo ND de red. Utilizando la clave local compartida KCP, se puede utilizar la encriptación de clave privada para comunicarse entre el programa de aplicaciones y la tarjeta inteligente. Consecuentemente, la potencia de proceso de la tarjeta inteligente se puede mantener relativamente baja, manteniendo así una reducción de coste de la tarjeta inteligente con respecto al que sería requerido si se utilizase la encriptación de clave pública. La distribución de la clave privada y su generación serán explicadas ahora, con referencia a la figura 4, en combinación con un diagrama de flujo ilustrado en la figura 5.

En la figura 5, un programa 60 de aplicaciones que se ejecuta en el procesador 44 de datos del dispositivo AD de aplicaciones, incluye una clave privada KP que es exclusiva del programa de aplicaciones, pero que es también conocida por el servidor confiable TS. El programa 60 de aplicaciones está organizado para generar aleatoriamente una clave local compartida KCP para compartir su utilización entre el dispositivo AD de aplicaciones y el dispositivo ND de red. El procesador 44 de datos está configurado para encriptar la clave local KCP con la clave KP de encriptación del programa. La clave local KP(KCP) es comunicada después al servidor confiable. La comunicación puede ser efectuada por cualquier medio conveniente, tal como copiando la clave local encriptada KCP en un medio de almacenamiento y transportando físicamente el medio de almacenamiento al servidor confiable, o la comunicación puede ser efectuada a través del dispositivo de red comunicando la clave encriptada KCP a través del enlace local 42 que puede ser comunicada entonces a través del enlace 4 de red hacia el servidor confiable TS. Sin embargo, como generalización, la comunicación entre el dispositivo AD de aplicaciones y el servidor confiable TS se representa por medio de una flecha 62 de doble cabeza.

La clave local encriptada KC(KCP) es recibida entonces en el servidor confiable TS y es desencriptada utilizando la clave privada KP. El servidor confiable puede comunicar entonces la clave local KCP al dispositivo ND de red encriptando la clave local KCP mediante el uso de la clave KC de la tarjeta inteligente. Como la tarjeta inteligente tiene pre-almacenada la clave KC de tarjeta inteligente, la comunicación de la clave local KCP puede ser efectuada a través del enlace 2 de comunicaciones de red a la interfaz 30 de comunicaciones. La clave local KCP puede ser desencriptada en la tarjeta inteligente utilizando la clave KC de tarjeta inteligente y ser almacenada en la memoria 50 de la tarjeta inteligente. Por tanto, como resultado, la clave local KCP es conocida por la tarjeta inteligente del dispositivo ND de red y por el programa de aplicaciones en el dispositivo AD de aplicaciones, y además es exclusiva para el emparejamiento entre el programa de aplicaciones y la tarjeta inteligente en el dispositivo ND de red. Como resultado, cuando se requiere cualquier comunicación entre el dispositivo ND de red y el dispositivo AD de aplicaciones, la encriptación puede ser efectuada utilizando la clave KCP que puede ser utilizada también para autenticar la tarjeta inteligente, así como el propio programa 60 de aplicaciones.

Los pasos de proceso involucrados en la generación de la clave local KCP, compartida entre el dispositivo AD de aplicaciones y el dispositivo ND de red, están ilustrados en la figura 6 y se resumen de la manera siguiente:

S1: El programa confiable del dispositivo AD de aplicaciones genera una clave aleatoria exclusiva KCP y encripta la clave aleatoria utilizando una clave KP del programa que ha sido pre-almacenada en el programa confiable.

S2: La clave local encriptada KP(KCP) es comunicada al servidor confiable TS.

S3: El servidor confiable conoce la clave KP de encriptación utilizada por el programa de aplicaciones confiable y de esta manera puede desencriptar la clave local KCP.

S4: El servidor confiable encripta la clave local KCP con la clave KC de tarjeta inteligente que está almacenada en la tarjeta inteligente y asociada unívocamente con el usuario. El servidor confiable TS envía la clave local encriptada KC(KCP) al dispositivo ND de red a través del enlace 2 de comunicaciones de red.

S5: La tarjeta inteligente desencripta la clave local KCP utilizando la clave KC de tarjeta inteligente pre-almacenada dentro de la tarjeta inteligente 20 y almacena la clave local KCP dentro de la memoria de la tarjeta inteligente.

S6: La tarjeta inteligente y el programa de aplicaciones pueden entonces intercambiar datos con seguridad utilizando la clave exclusiva KCP.

Como la clave local KCP ha sido generada aleatoriamente por el programa 60 de aplicaciones, la clave KCP es exclusiva para la pareja de dispositivos de aplicaciones/red. La clave local KCP puede ser utilizada también para la autenticación tanto de la tarjeta inteligente por el programa de aplicaciones como del programa de aplicaciones por la tarjeta inteligente. El programa de aplicaciones, que es una entidad, que puede ser relativamente fácil de copiar, puede estar por tanto asociada operativamente de forma unívoca con una tarjeta inteligente, que es una entidad, que no puede ser copiada fácilmente.

Distribución y actualización de datos sensibles

Las partes del sistema ilustradas en la figura 5 pueden proporcionar la cualidad de comunicar datos sensibles con seguridad entre el programa de aplicaciones y la tarjeta inteligente con el fin de proporcionar un servicio a un usuario.

Ejemplos de datos sensibles podrían ser, por ejemplo, una licencia comprada para la reproducción de contenidos, información privada, detalles privados de contacto o una representación electrónica de datos de un valor monetario. Para el ejemplo de un valor monetario, se pueden proporcionar valores en dinero con el fin de permitir al usuario comprar un producto o servicio o llevar a cabo alguna transacción electrónica por la que se ofrece un valor monetario como intercambio por el servicio o producto. Otros ejemplos de datos sensibles son información privada o información de una póliza asociada por ejemplo con detalles de contacto que son confidenciales para un usuario. Estos son ejemplos de datos sensibles, que pueden ser cambiados por un programa de aplicaciones tras algún proceso de datos sensibles.

Haciendo referencia de nuevo a la figura 5, el servidor confiable, por ejemplo, puede almacenar o generar los datos sensibles que van a ser utilizados por el programa de aplicaciones que se ejecuta en el dispositivo AD de aplicaciones. Como la tarjeta inteligente incluye la clave KC exclusiva de la tarjeta inteligente asociada con el usuario, el servidor confiable TS puede encriptar los datos sensibles SD y comunicar los datos encriptados KC(SD) a la tarjeta inteligente en el dispositivo ND de red, utilizando el enlace 2 de comunicaciones de red, como se ha descrito anteriormente. Los datos sensibles encriptados KC(SD) son recibidos a través de la tarjeta inteligente utilizando el dispositivo 22 de acceso a tarjetas inteligentes y desencriptados para recuperar los datos sensibles que pueden ser entonces almacenados en la tarjeta inteligente 20.

Si el programa de aplicaciones del dispositivo de aplicaciones requiere acceso a los datos sensibles, se puede comunicar una petición de acceso a través del enlace local 42 que puede ser autenticada utilizando la clave local KCP, la cual puede ser verificada por la tarjeta inteligente 20 en el dispositivo de red. Los datos sensibles pueden ser entonces encriptados utilizando la clave local KCP en la tarjeta inteligente 20 y ser comunicados al dispositivo AD de aplicaciones, donde el programa de aplicaciones pude desencriptar los datos sensibles utilizando la clave local KCP.

El programa de aplicaciones puede confirmar también la presencia de la tarjeta inteligente que proporciona el servicio al usuario de acuerdo con el programa de aplicaciones. La autenticación y la presencia de la tarjeta inteligente pueden ser confirmadas intercambiando mensajes que utilicen la clave local compartida KCP, como ya se ha descrito.

Si el programa de aplicaciones cambia los datos sensibles de alguna manera, los datos sensibles pueden ser almacenados en la tarjeta inteligente 20 antes de ser actualizados por el servidor confiable. Sin embargo, con el fin de actualizar los datos sensibles en el servidor confiable TS, los datos sensibles deben ser comunicados a través del enlace de red al servidor confiable. Para el ejemplo de ilustración que se muestra en las figuras 1 y 5, la red forma una red radio de móviles y así el enlace 2 de comunicaciones puede no estar siempre disponible. Por tanto, el dispositivo ND de red puede no estar siempre en contacto con la red 1. En una situación en la cual el dispositivo de red no se pueda comunicar con la red, la tarjeta inteligente actúa como un almacén local para los datos sensibles. Como la propia tarjeta inteligente incluye provisiones de seguridad (explicadas anteriormente), los datos sensibles pueden ser almacenados con seguridad en la tarjeta inteligente de una manera tal que asocia unívocamente los datos sensibles con el usuario. Por tanto, por ejemplo, si los datos sensibles representan un valor monetario, que cambia como resultado de una transacción, los datos sensibles pueden ser actualizados entonces en la tarjeta inteligente para reflejar el cambio del valor. Los datos sensibles son actualizados entonces a través del enlace 2 de red cuando el enlace de red existe, proporcionando así una operación sustancialmente coherente del servicio al usuario como determina el programa de aplicaciones, esté o no el dispositivo de red en comunicación con la red. Esto es así cuando la red de móviles no está disponible, por ejemplo debido a falta de cobertura por radio, actuando entonces la tarjeta inteligente como un almacén local para el valor monetario actualizado.

En resumen, el funcionamiento de la realización de la invención ilustrada en la figura 5 se describe por medio de los diagramas de flujo ilustrados en la figura 7 y en la figura 8. El diagrama de flujo de la figura 7 ilustra el funcionamiento de la distribución de datos sensibles a la tarjeta inteligente, y el acceso del programa de aplicaciones a los datos sensibles de la tarjeta inteligente. La figura 8 ilustra el funcionamiento del programa de aplicaciones en el dispositivo de aplicaciones cuando se utiliza la tarjeta inteligente como servidor local.

El diagrama de flujo de la figura 7 se resume como sigue:

S10: El servidor confiable encripta los datos sensibles SD utilizando la clave KC de la tarjeta inteligente. El servidor confiable conoce la clave KC de la tarjeta inteligente. La clave KC de la tarjeta inteligente está pre-almacenada también en la tarjeta inteligente.

S11: El servidor confiable envía los datos sensibles encriptados KC(SD) al dispositivo de red.

S12: El dispositivo de red almacena los datos sensibles encriptados KC(SD) en la tarjeta inteligente, donde se desencriptan los datos utilizando la clave KC de la tarjeta inteligente.

S.13: La tarjeta inteligente desencripta entonces los datos sensibles, utilizando la clava KC de la tarjeta inteligente, para recuperar los datos sensibles. La desencriptación se realiza en la tarjeta inteligente y los datos sensibles son almacenados en la tarjeta inteligente.

S.14: Cuando el programa de aplicaciones que se ejecuta en el dispositivo de aplicaciones requiere el acceso a los datos sensibles para proporcionar un servicio al usuario, el programa de aplicaciones encripta una petición de datos sensibles utilizando la clave local compartida KCP, que ha sido establecida en la tarjeta inteligente.

S.15: Dentro de la tarjeta inteligente, la tarjeta inteligente determina si la petición del programa de aplicaciones es auténtica. La autenticación se realiza desencriptando la petición mediante el uso de la clave local KCP. Si se recupera correctamente una petición válida (de acuerdo con una forma predeterminada), entonces la petición se considera auténtica. Si la petición es auténtica, el proceso continúa en el paso S.19. En otro caso, el proceso continúa en el paso S.16.

S.16: Si falla la autenticación, el proceso termina y el servidor confiable es alertado del hecho de que se ha hecho un intento ilegal para acceder a los datos sensibles.

S.17: El programa de aplicaciones determina si la tarjeta inteligente es auténtica. Esto puede determinarse, por ejemplo, disponiendo la tarjeta inteligente para que responda al mensaje de petición enviado a ella, generando un mensaje de respuesta de acuerdo con un formato predeterminado y encriptando el mensaje mediante el uso de la clave local compartida KCP. Si tras desencriptar la respuesta el programa de aplicaciones recupera un mensaje de respuesta que tiene el formato correcto, se determina que la tarjeta inteligente es auténtica y el proceso continúa en el paso S.19. En otro caso, continúa en el paso S.18.

S.18: Si falla la autenticación, el proceso termina y el servidor confiable es alertado del hecho de se ha hecho un intento de utilizar una tarjeta inteligente incorrecta.

S.19: Si la tarjeta inteligente y el programa de aplicaciones han realizado con éxito una autenticación mutua, que puede ser indicada por un intercambio adicional de mensajes mutuos, la tarjeta inteligente encripta entonces los datos sensibles utilizando la clave local compartida.

S.20: El dispositivo de red envía entonces los datos sensibles encriptados al programa de aplicaciones a través de la interfaz local de comunicaciones.

Una de las ventajas proporcionadas por realizaciones de la invención, es que la tarjeta inteligente puede actuar como un servidor local cuando la red no está disponible para el programa de aplicaciones. Cualquier cambio en los datos sensibles puede ser almacenado en la tarjeta inteligente y actualizado en la red, cuando la red esté disponible. El funcionamiento del programa de aplicaciones y de la tarjeta inteligente cuando se utiliza la tarjeta inteligente como servidor local, como se ilustra en la figura 8, se resume como sigue:

S30: La tarjeta inteligente en el dispositivo de red comunica los datos sensibles al programa de aplicaciones cuando éste es requerido por el programa de aplicaciones que se ejecuta en el dispositivo de aplicaciones. El dispositivo de red encripta los datos sensibles utilizando la clave local compartida KCP antes de ser comunicada a través del enlace local 42.

S32: Después de que el programa de aplicaciones haya procesado los datos sensibles, proporcionando un servicio al usuario y posiblemente cambiando los datos sensibles, los datos sensibles son vueltos a comunicar al dispositivo de red por el dispositivo de aplicaciones. El dispositivo de aplicaciones encripta nuevamente los datos sensibles utilizando la clave local KCP, que es desencriptada dentro de la tarjeta inteligente 20 utilizando nuevamente la clave local compartida KCP. Los datos sensibles actualizados pueden ser mantenidos en la tarjeta inteligente de una forma segura y en asociación unívoca con el usuario. Así, de esta forma la tarjeta inteligente actúa como un repositorio para los datos sensibles. Los datos sensibles solamente pueden ser actualizados cuando el dispositivo de red está en contacto con la red. Por tanto, el almacenamiento de los datos sensibles en forma actualizada en la tarjeta inteligente mantiene una representación coherente de los datos sensibles, que pueden estar seguros en la tarjeta inteligente.

S34: Si el dispositivo de red es conectable a la red, entonces:

S36: Los datos sensibles SD son actualizados comunicando los datos sensibles actualmente almacenados desde la tarjeta inteligente hacia el servidor confiable. Los datos sensibles son encriptados utilizando la clave KC de la tarjeta inteligente dentro de la tarjeta inteligente, y son correspondientemente desencriptados dentro del servidor confiable.

S38: Si el dispositivo de red no es conectable a la red, los datos sensibles se mantienen solamente en la tarjeta inteligente.

Distribución de datos de gestión de derechos y contenidos

Se describirá ahora otra realización de ejemplo de la presente invención, en asociación con la provisión de una cualidad para distribuir contenidos a un usuario. Como se ilustra en la figura 1, el contenido puede ser descargado a un dispositivo de aplicaciones desde un servidor de contenidos donde se almacenan los contenidos. Como se mencionó anteriormente, la forma por la cual se puede distribuir el contenido no está limitada a la descarga desde un servidor, sino que puede ser distribuido, por ejemplo, sobre un medio apropiado tal como un CD ROM o un DVD o similar.

La figura 9 proporciona una ilustración de una realización de la presente invención que está configurada para distribuir contenidos con seguridad y para gestionar los derechos de esos contenidos. En la figura 8, se distribuye un CD ROM 70 a un dispositivo 72 de aplicaciones. El dispositivo 72 de aplicaciones incluye una presentación visual 74 para observar el contenido, que en el presente ejemplo de aplicación incluye material de vídeo. Por tanto, como se

ilustra con la flecha 76, el contenido se distribuye desde el CD ROM al dispositivo de aplicaciones para la reproducción en el dispositivo de aplicaciones. Sin embargo, con el fin de controlar la distribución y la copia, el contenido es encriptado utilizando una clave KS de encriptación denominada en la descripción siguiente como clave de encriptación de contenidos.

Como ya se ha explicado anteriormente, una clave local compartida KCP ha sido ya establecida entre el dispositivo 72 de aplicaciones y un dispositivo 80 de red. El dispositivo de red y el dispositivo de aplicaciones ilustrados en la figura 9 se corresponden sustancialmente con el dispositivo de red y el dispositivo de aplicaciones ilustrados en las figuras 1, 2 y 4, y por tanto, solamente se explicarán las diferencias entre estas implementaciones alternativas.

De acuerdo con una realización de la invención, si el usuario desea observar el contenido recibido desde el CD ROM 70, se debe obtener una licencia para la reproducción y/o permiso de copia del contenido, ya sea mediante compra o como intercambio de condiciones apropiadas. Con este fin, un reproductor confiable 94 envía una petición de la clave de contenidos desde el servidor confiable TS. El reproductor confiable 94 representa un ejemplo de un programa de aplicaciones y así se corresponde sustancialmente con el programa de aplicaciones de la realización ilustrada mostrada en la figura 5. La petición de la clave de contenidos podría ser enviada desde el dispositivo 80 de red, que nuevamente podría ser encriptada utilizando la clave KC de la tarjeta inteligente. Como respuesta a la petición para reproducir el contenido, el servidor confiable genera datos de acceso a contenidos, que son encriptados utilizando la clave KC de tarjeta inteligente que es conocida por el servidor confiable. Los datos de acceso a contenidos encriptados son comunicados entonces, a través del enlace 2 de red, al dispositivo ND.2 de red y son desencriptados dentro de la tarjeta inteligente 92 utilizando la clave KC de encriptación de la tarjeta inteligente pre-almacenada.

Con el fin de reproducir el contenido, el reproductor confiable 94 requiere la clave KS de contenidos. Los datos de acceso a contenidos incluyen la clave KS de contenidos que puede ser proporcionada bajo las condiciones para reproducir y/o copiar el contenido.

Como respuesta a una orden de reproducción iniciada por un usuario para requerir la reproducción del contenido por el reproductor confiable, el reproductor confiable extrae los datos de acceso a contenidos desde la tarjeta inteligente 92, accediendo al dispositivo ND.2 de red a través del enlace 42 de comunicaciones. La petición es autenticada utilizando la clave local KCP de manera que como respuesta a la petición, el dispositivo ND.2 de red reproduce los datos de acceso al contenido una vez que éstos han sido encriptados dentro de la tarjeta inteligente utilizando la clave compartida KCP. Los datos de acceso a contenidos encriptados pueden ser entonces comunicados al reproductor confiable 94 y desencriptados para recuperar los datos de acceso a contenidos. Como se ha mencionado anteriormente, los datos de acceso a contenidos pueden incluir no solamente la clave KS de encriptación de contenidos que permite desencriptar el contenido, sino también las condiciones para reproducir el contenido y/o copiar el contenido en la forma denominada generalmente como datos de gestión de derechos.

Una vez que el contenido ha sido desencriptado y reproducido, los datos de acceso a contenidos pueden ser actualizados y devueltos al dispositivo de red y ser almacenados en la tarjeta inteligente. Por tanto, la tarjeta inteligente puede ser utilizada como repositorio para los datos seguros de acceso a contenidos que pueden ser actualizados por la red en el servidor confiable cuando el dispositivo de red está conectado a la red, como se ha explicado con referencia a la realización anterior.

De acuerdo con la realización de la presente invención ilustrada en la figura 9, se puede comprar una licencia para reproducción de un elemento de contenido particular con seguridad utilizando la naturaleza segura de la tarjeta inteligente. El dispositivo AD.2 de aplicaciones confirma la presencia de la tarjeta inteligente y autentica la tarjeta inteligente antes de que se pueda reproducir el contenido. Como resultado, se proporciona una configuración mejorada de distribución de contenidos que reduce la probabilidad de que el contenido sea reproducido ilegalmente y/o copiado de una manera que esté fuera del control del distribuidor.

En la figura 10 se proporciona el funcionamiento del dispositivo de aplicaciones y del dispositivo de red para reproducir el contenido encriptado, que puede ser resumido como sigue:

S40: El contenido digital, que ha sido encriptado, es cargado en el dispositivo de aplicaciones. El contenido ha sido encriptado utilizando una clave KS de encriptación de contenidos.

S41: Los datos de acceso al contenido que incluyen los datos de gestión de derechos que proporcionan los derechos de reproducción y las condiciones de copia, e incluyen la clave KS, son encriptados por el servidor confiable utilizando la clave KC de encriptación de tarjeta inteligente. Los datos de acceso a contenidos pueden incluir otros tipos de datos e información.

S42: El servidor confiable comunica los datos de acceso a contenidos encriptados al dispositivo ND.2 de red.

S43: El dispositivo de red alimenta los datos de acceso a contenidos encriptados a la tarjeta inteligente, donde son desencriptados utilizando la clave KC de tarjeta inteligente.

S44: Los datos de acceso a contenidos son almacenados en la tarjeta inteligente.

S45: La tarjeta inteligente encripta los datos de acceso a contenidos que incluyen los datos de gestión de derechos y la clave KS de desencriptación utilizando la clave local compartida KCP.

S46: El dispositivo de red envía los datos de acceso a contenidos encriptados al dispositivo de aplicaciones.

S47: El reproductor confiable del dispositivo de aplicaciones desencripta los datos de acceso a contenidos para recuperar los datos de gestión de derechos y la clave KS de contenidos.

S48: El reproductor confiable puede desencriptar entonces el contenido utilizando la clave KS de contenidos, que es reproducido por la pantalla 74 de reproducción.

Una vez que el contenido ha sido reproducido por el dispositivo de aplicaciones, se puede requerir que se actualicen los datos de gestión de derechos para reflejar el hecho de que los datos han sido reproducidos. Consecuentemente, el funcionamiento del dispositivo de aplicaciones y del dispositivo de red se resume en la figura 11, que es una continuación desde el nodo "A" que aparece en la figura 10.

S50: Tras reproducir el contenido, el reproductor confiable determina si los datos de derechos digitales necesitan ser actualizados.

S51: Si los datos de gestión de derechos no necesitan ser actualizados, los datos de gestión de derechos actualizados serán encriptados utilizando la clave local KCP.

S52: Los datos de gestión de derechos encriptados son comunicados a la tarjeta inteligente en el dispositivo ND.2 de red.

S53: El dispositivo de la tarjeta inteligente desencripta los datos de gestión de derechos y almacena los datos de gestión de derechos en la tarjeta inteligente.

S54: El dispositivo de red comunica entonces los datos de gestión de derechos actualizados al servidor confiable con seguridad, encriptando los datos de derechos actualizados con la clave KC de la tarjeta inteligente.

En resumen, la distribución de contenidos y la gestión de los derechos en el contenido se efectúan por medio del servidor confiable en combinación con la tarjeta inteligente que está asociada unívocamente con un usuario. Utilizando las características de seguridad inherentes a la tarjeta inteligente, los datos de acceso a contenidos pueden ser comunicados con seguridad al usuario en la tarjeta inteligente. Además, disponiendo la generación de una clave local (KCP) y compartiéndola entre el reproductor confiable (programa de aplicaciones) del dispositivo de aplicaciones y la tarjeta inteligente del dispositivo de red, los datos de acceso a contenidos pueden ser comunicados al reproductor confiable y después ser actualizados en el dispositivo de red para su almacenamiento seguro en la tarjeta inteligente.

Seguridad reforzada de reproducción

Con el fin de reforzar la seguridad de la reproducción del contenido y la gestión y ejecución de los derechos en el contenido, se proporciona la provisión de una seguridad reforzada de los contenidos. Las provisiones de seguridad reforzada se proporcionan organizando el reproductor confiable del dispositivo de aplicaciones para que identifique si está presente la tarjeta inteligente dentro del dispositivo de red, antes de que se desencripte y se reproduzca el contenido. Además, el servidor confiable puede autenticar la tarjeta inteligente antes de bien reproducir el contenido, o de copiar el contenido, o efectuar, de hecho, cualquier otra acción. Un diagrama de flujo que representa un proceso para reproducir el contenido, como se ejecuta por el dispositivo de aplicaciones ilustrado en la figura 9, está ilustrado en la figura 12 y se resume como sigue:

S60: El usuario activa un modo de reproducción con el efecto de que el reproductor confiable (programa de aplicaciones) está configurado para reproducir el contenido, el cual ha sido cargado en el dispositivo de aplicaciones.

S61: El servidor confiable (programa de aplicaciones) genera entonces un mensaje de petición, indicando que el reproductor confiable desea reproducir el contenido. El reproductor confiable encripta el mensaje de la petición utilizando la clave local compartida KCP.

S.62: El servidor confiable comunica entonces la petición encriptada a la tarjeta inteligente del dispositivo de red.

S.63: La tarjeta inteligente determina después si la petición recibida del programa de aplicaciones es auténtica. La autenticidad puede ser determinada desencriptando el mensaje de petición encriptado utilizando la clave local compartida KCP. Si se recupera un mensaje de acuerdo con un formato correcto (de acuerdo con el estándar preestablecido), el mensaje queda autenticado. Si la petición es auténtica, el proceso continúa en el paso S.64, en otro caso el proceso continúa en el paso S.80 a través del nodo A.

S.64: La tarjeta inteligente examina entonces los datos de gestión de derechos que forman parte de los datos de acceso a contenidos, para determinar si el programa de aplicaciones tiene el derecho a reproducir o copiar el contenido.

Si el programa de aplicaciones tiene el derecho a reproducir el contenido, el proceso continúa en el paso S.66, pasando el proceso en otro caso al paso S.80 a través del nodo A.

S.68: En paralelo, como parte de la autenticación mutua, el programa de aplicaciones determina si la tarjeta inteligente está presente en el dispositivo de red. Si la tarjeta inteligente está presente, el proceso continúa en el paso S.70, pasando el proceso en otro caso al paso S.80 a través del nodo A.

S.70: El programa de aplicaciones determina entonces si la tarjeta inteligente que está presente es la tarjeta inteligente correcta. Esto puede ser determinado de varias maneras. Por ejemplo, la tarjeta inteligente puede enviar un mensaje como respuesta al mensaje de petición para reproducir el mensaje de contenidos. Para algunas realizaciones, el mensaje de respuesta puede ser los datos de acceso a contenidos encriptados, como se ha explicado en el paso S.66.

El mensaje de respuesta desde la tarjeta inteligente es encriptado utilizando la clave local compartida KCP. Si al desencriptar la respuesta recibida desde la tarjeta inteligente utilizando la clave local compartida KCP se obtiene un mensaje de respuesta correcto, entonces se determina que la tarjeta inteligente es auténtica. Si el programa de aplicaciones determina que la tarjeta inteligente es auténtica, el proceso continúa en el paso S.66, continuando el proceso en otro caso en el paso S.80 a través del nodo A.

S.66: La tarjeta inteligente encripta entonces los datos de acceso a contenidos utilizando la clave local compartida KCP y comunica los datos de acceso a contenidos encriptados al programa de aplicaciones.

S-72: El programa de aplicaciones desencripta los datos de acceso a contenidos y obtiene los datos de gestión de derechos.

S.76: El programa de aplicaciones determina entonces si los datos de gestión de derechos permiten la reproducción y/o copia que hayan sido requeridos. Si los datos de gestión de derechos permiten la reproducción, el proceso continúa en el paso S.78 y se reproduce el contenido, pasando el proceso en otro caso al paso S.80.

S.78: Se reproduce el contenido y/o se copia de acuerdo con la petición.

S.80: En el paso S.80 no se reproduce el contenido, y se alerta al servidor confiable del intento de reproducir el contenido de una manera que puede ser contraria a los deseos del distribuidor.

En algunas realizaciones, el dispositivo de aplicaciones puede requerir los datos sensibles desde el servidor confiable de acuerdo con el funcionamiento del programa de aplicaciones. Con el fin de autenticar la petición de datos sensibles, el programa de aplicaciones puede incluir la clave KP del programa, que es conocida por el servidor confiable. Además, si se comunica la petición al servidor confiable a través del dispositivo de red, con la petición se puede comunicar entonces un número de identidad de línea de abonado que está pre-almacenado en la tarjeta inteligente (SIM), para verificar que la petición de datos sensibles es auténtica.

En las reivindicaciones anexas se definen diversos aspectos y características de la presente invención.

Se pueden hacer diversas modificaciones a las realizaciones que se han descrito aquí anteriormente, sin salir del alcance de la presente invención. Por ejemplo, aunque las realizaciones descritas contemplan un dispositivo de aplicaciones independiente para el dispositivo de red independiente conectado a través de un enlace local de comunicaciones, se apreciará que en otras realizaciones los dispositivos de red y de aplicaciones pueden estar combinados en un solo dispositivo. Para tal realización no habrá requisito de un enlace local de comunicaciones o, alternativamente, el enlace local de comunicaciones podría representar un canal de comunicaciones cableadas por equipo físico informático entre diferentes dispositivos. Correspondientemente, el programa de aplicaciones y el procesador de datos del dispositivo de red pueden ser el mismo procesador de datos que ejecuta el equipo lógico informático. En este caso, el enlace de comunicaciones entre el dispositivo de aplicaciones y el dispositivo de red sería un enlace interno dentro de la estructura de un programa de aplicaciones.

REIVINDICACIONES

1. Un sistema para distribuir datos de acceso a contenidos a un usuario, proporcionando los datos de acceso a contenidos unos datos de gestión de derechos que indican un derecho del usuario para reproducir y/o copiar el contenido distribuido, comprendiendo el sistema:

un dispositivo (AD) de aplicaciones que incluye un programa (60) de aplicaciones que forma un reproductor confiable (44) para recibir y reproducir y/o copiar el contenido,

un dispositivo (22) de acceso a tarjetas inteligentes que funciona accediendo a una tarjeta inteligente (20),

un servidor confiable (TS) que funciona comunicando con seguridad los datos de acceso a contenidos a la tarjeta inteligente (20) a través de una red de comunicaciones encriptando los datos de acceso a contenidos mediante el uso de una primera clave (KC) de encriptación pre-almacenada en la tarjeta inteligente (20) y conocida por el servidor confiable (TS),

una tarjeta inteligente (20) que está asociada unívocamente con el usuario y que funciona desencriptando los datos de acceso a contenidos encriptados utilizando la primera clave (KC) de encriptación y almacenando los datos de acceso a contenidos en la tarjeta inteligente (20);

en el que el reproductor confiable es operable:

para acceder a los datos de gestión de derechos proporcionados con los datos de acceso a contenidos en la tarjeta inteligente (20), y

para reproducir y/o copiar el contenido de acuerdo con los datos de gestión de derechos;

caracterizado porque el reproductor confiable (44) tiene permitido el acceso a los datos de acceso a contenidos en la tarjeta inteligente, solamente cuando sigue a una autenticación mutua entre la tarjeta inteligente (20) y el reproductor confiable (44).

2. Un sistema según la reivindicación 1, en el que el contenido distribuido ha sido encriptado utilizando una segunda clave (KS) de encriptación de contenidos, incluyendo los datos de acceso a contenidos la segunda clave (KS) de encriptación de contenidos, pudiendo funcionar el reproductor confiable (44):

para recuperar la segunda clave (KS) de encriptación de contenidos a partir de los datos de acceso a contenidos de la tarjeta inteligente (20), y

para desencriptar el contenido utilizando la segunda clave (KS) de encriptación de contenidos proporcionada con los datos de acceso a contenidos, de acuerdo con si la reproducción y/o copia del contenido está permitida por los datos de gestión de derechos.

3. Un sistema como se reivindica en la reivindicación 1 o 2, donde los datos de gestión de derechos incluyen una indicación del número de veces que puede ser reproducido el contenido, pudiendo funcionar el reproductor confiable (44) de manera que actualiza los datos de gestión de derechos de acuerdo con la reproducción del contenido, y almacena los datos de gestión de derechos en la tarjeta inteligente (20).

4. Un sistema según la reivindicación 1, 2 o 3, en el que la autenticación mutua incluye un intercambio de mensajes entre el reproductor confiable (44) y la tarjeta inteligente (20), siendo encriptados los mensajes mediante la utilización de una tercera clave local (KCP) de encriptación compartida entre la tarjeta inteligente (20) y el reproductor confiable (44).

5. Un sistema según la reivindicación 4, en el que el reproductor confiable (44) es operable:

para generar la tercera clave local (KCP) de encriptación,

para encriptar la tercera clave local (KCP) de encriptación utilizando una cuarta clave (KP) de encriptación de programa que forma parte del reproductor confiable (44), y

para comunicar la tercera clave local encriptada (KCP) de encriptación al servidor confiable (TS);

y el servidor confiable (TS) es operable:

para encriptar la tercera clave local (KCP) de encriptación con la primera clave (KC) de encriptación de la tarjeta inteligente, y

para comunicar la tercera clave local encriptada (KCP) de encriptación a la tarjeta inteligente (20) a través de la red de comunicaciones, pudiendo funcionar la tarjeta inteligente (20) de manera que desencripta la tercera clave local (KCP) de encriptación utilizando la primera clave (KC) de encriptación.

6. Un sistema según cualquiera de las reivindicaciones 4 o 5, que comprende un dispositivo (ND) de red para comunicarse con la red de comunicaciones, incluyendo el dispositivo (ND) de red el dispositivo (22) de acceso a tarjetas inteligentes que funciona para acceder a la tarjeta inteligente (20), una interfaz (30) de comunicaciones para comunicar datos con seguridad a través de la red de comunicaciones, utilizando la primera clave (KC) de encriptación, y una interfaz local (34) de comunicaciones para comunicar datos con el dispositivo (AD) de aplicaciones, incluyendo el dispositivo (AD) de aplicaciones una correspondiente interfaz local (40) para comunicarse con el dispositivo (ND) de red, pudiendo funcionar la tarjeta inteligente (20) del dispositivo de red y el reproductor confiable (44) del dispositivo (AD) de aplicaciones de manera que efectúan una comunicación segura de los datos de acceso a contenidos a través de los interfaces locales de comunicaciones, utilizando la tercera clave local (KCP) de encriptación compartida entre el dispositivo (AD) de aplicaciones y el dispositivo (ND) de red.

7. Un sistema según cualquier reivindicación precedente, donde la red de comunicaciones incluye una red radio de telecomunicaciones móviles, incluyendo la interfaz de comunicaciones del dispositivo de red un dispositivo de comunicaciones radio de móviles para comunicarse a través de la red radio de móviles.

8. Un sistema según la reivindicación 7, en el que la tarjeta inteligente (20) es un módulo de identidad de abonado para la red radio de móviles, que proporciona la primera clave (KC) de encriptación pre-almacenada y un número de identidad de línea de abonado.

9. Un sistema según la reivindicación 8 cuando la reivindicación 7 depende de la reivindicación 5, en el que el dispositivo (AD) de aplicaciones es operable solicitando los datos de acceso a contenidos desde el servidor confiable (TS), incluyendo la solicitud el número de identidad de la línea de abonado desde la tarjeta inteligente (20), encriptado con la cuarta clave (KP) de encriptación de programa, pudiendo funcionar el servidor confiable (TS) de manera que comunica datos seguros a la tarjeta inteligente (20) si la cuarta clave (KP) de encriptación de programa y el número de identidad de línea de abonado están autenticados.

10. Un sistema según cualquier reivindicación precedente, donde el reproductor confiable (44) es operable de manera que confirma la presencia de la tarjeta inteligente (20) en el dispositivo (22) de acceso de tarjetas inteligentes, antes de reproducir el contenido.

11. Un sistema según la reivindicación 10, donde el reproductor confiable (44) funciona de manera que confirma la presencia de la tarjeta inteligente (20) intercambiando mensajes encriptados, que utilizan la tercera clave local (KCP) de encriptación, con la tarjeta inteligente (20).

12. Un método para distribuir los datos de acceso a contenidos a un usuario, proporcionando los datos de acceso a contenidos datos de gestión de derechos que indican un derecho del usuario para reproducir y/o copiar el contenido distribuido, comprendiendo el método:

recibir el contenido en un programa (60) de aplicaciones que forma un reproductor confiable (44) para recibir y reproducir y/o copiar el contenido,

acceder a una tarjeta inteligente (20) que está unívocamente asociada con el usuario,

encriptar los datos de acceso a contenidos utilizando una primera clave (KC) de encriptación pre-almacenada en la tarjeta inteligente (20) y conocida por el servidor confiable (TS),

comunicar con seguridad los datos de acceso a contenidos encriptados desde el servidor confiable (TS) a la tarjeta inteligente (20), a través de una red de comunicaciones,

desencriptar los datos de acceso a contenidos encriptados utilizando la primera clave (KC) de encriptación, y

almacenar los datos de acceso a contenidos en la tarjeta inteligente (20);

caracterizado porque:

se autentican mutuamente la tarjeta inteligente (20) y el reproductor confiable (44),

se accede a los datos de gestión de derechos proporcionados con los datos de acceso a contenidos en la tarjeta inteligente (20), utilizando el reproductor confiable (44), estando permitido el acceso a los datos de acceso a contenidos de la tarjeta inteligente (20), solamente si la autenticación mutua entre la tarjeta inteligente (20) y el reproductor confiable (44) ha tenido éxito, y

reproducir y/o copiar el contenido utilizando el reproductor confiable (44) de acuerdo con los datos de gestión de derechos.

13. Un método como se reivindica en la reivindicación 12, en el que el contenido distribuido ha sido encriptado utilizando una segunda clave (KS) de encriptación de contenidos, incluyendo los datos de acceso a contenidos la segunda clave (KS) de encriptación de contenidos, comprendiendo el método:

recuperar la segunda clave (KS) de encriptación de contenidos a partir de los datos de acceso a contenidos accedidos desde la tarjeta inteligente (20), y

desencriptar el contenido utilizando la segunda clave (KS) de encriptación de contenidos proporcionada con los datos de acceso a contenidos, de acuerdo con si la reproducción y/o copia del contenido está permitida por los datos de gestión de derechos.

14. Un método según la reivindicación 12 o 13, en el que los datos de gestión de derechos incluyen una indicación del número de veces que se puede reproducir el contenido, comprendiendo el método:

actualizar los datos de gestión de derechos de acuerdo con una reproducción del contenido, y

almacenar los datos de gestión de derechos actualizados en la tarjeta inteligente (20).

15. Un método según la reivindicación 14, en el que la autenticación mutua incluye:

encriptar mensajes utilizando una tercera clave local (KCP) de encriptación, compartida entre la tarjeta inteligente (20) y el reproductor confiable (44),

intercambiar los mensajes entre el reproductor confiable (44) y la tarjeta inteligente (20), y

desencriptar los mensajes utilizando la tercera clave local (KCP) de encriptación, estando autenticados mutuamente la tarjeta inteligente (20) y el reproductor confiable (44) si los mensajes se han recuperado correctamente.

16. Un método según la reivindicación 15, comprendiendo el método:

generar la tercera clave local (KCP) de encriptación,

encriptar la tercera clave local (KCP) de encriptación utilizando una cuarta clave (KP) de encriptación de programas que forma parte del reproductor confiable (44),

comunicar la tercera clave encriptada (KCP) de encriptación al servidor confiable (TS),

encriptar la tercera clave (KCP) de encriptación con la primera clave (KC) de encriptación conocida por el servidor confiable (TS),

comunicar la tercera clave local encriptada (KCP) de encriptación a la tarjeta inteligente (20) a través de la red de comunicaciones, y

desencriptar la tercera clave local (KCP) de encriptación utilizando la primera clave (KC) de encriptación de la tarjeta inteligente (20).

17. Un método según la reivindicación 16, en el que la tarjeta inteligente (20) es un módulo de identidad de abonado, que proporciona la primera clave (KC) de encriptación pre-almacenada e incluye un número de identidad de línea de abonado.

18. Un método según la reivindicación 17, que comprende:

comunicar una petición de datos seguros desde el servidor confiable (TS), incluyendo la petición el número de identidad de la línea de abonado desde la tarjeta inteligente (20), encriptado con la cuarta clave (KP) del programa,

autenticar el número de identidad de línea de abonado y la cuarta clave (KP) del programa,

comunicar los datos seguros a la tarjeta inteligente (20) si la cuarta clave del programa y el número de identidad de la línea de abonado son auténticos.

19. Un método según cualquiera de las reivindicaciones 13 a 18, que comprende confirmar la presencia de la tarjeta inteligente antes de reproducir el contenido, intercambiando la tercera clave local (KCP) de encriptación con la tarjeta inteligente (20).

20. Un dispositivo (AD) de aplicaciones que ejecuta un programa (60) de aplicaciones que forma un reproductor confiable (44), para recibir y reproducir y/o copiar el contenido de acuerdo con los datos de acceso a contenidos, proporcionando los datos de acceso a contenidos datos de gestión de derechos que indican un derecho del usuario a reproducir y/o copiar contenidos distribuidos, comprendiendo el dispositivo (AD) de aplicaciones:

un dispositivo (22) de acceso de tarjetas inteligentes que funciona accediendo a una tarjeta inteligente (20) que está asociada unívocamente con el usuario, pudiendo ser operada la tarjeta inteligente (20) de manera que recibe los datos de acceso a contenidos desde un servidor confiable (TS) a través de una red de comunicaciones, habiendo sido encriptados los datos de acceso a contenidos utilizando una primera clave (KC) de encriptación pre-almacenada en la tarjeta inteligente (20),

una tarjeta inteligente (20) que opera desencriptando los datos de acceso a contenidos utilizando la primera clave (KC) de encriptación y almacenando los datos de acceso a contenidos en la tarjeta inteligente (20);

en el que el reproductor confiable (44) es operable:

para acceder a los datos de gestión de derechos proporcionados con los datos de acceso a contenidos recibidos en la tarjeta inteligente (20), y

para reproducir y/o copiar el contenido de acuerdo con los datos de gestión de derechos;

caracterizado porque el reproductor confiable (44) tiene permitido el acceso a los datos de acceso a contenidos de la tarjeta inteligente (20), solamente si sigue a una autenticación mutua entre la tarjeta inteligente (20) y el reproductor confiable (44).

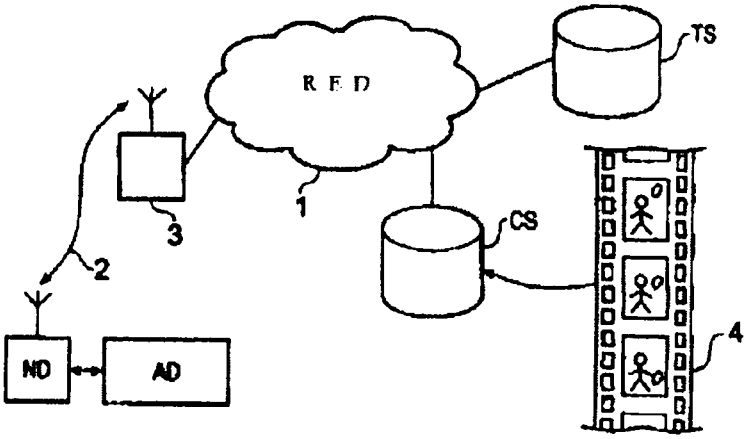

Fig. 1

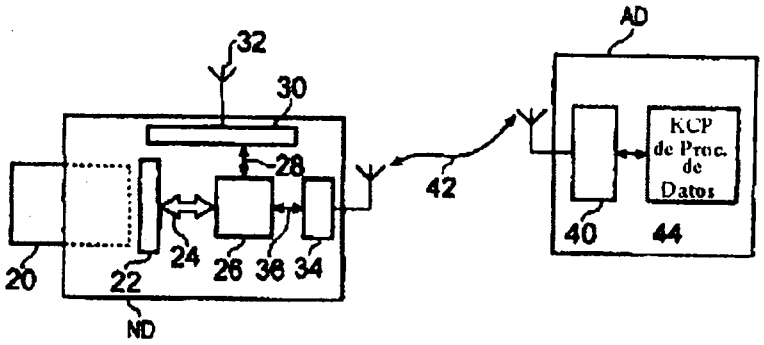

Fig. 2

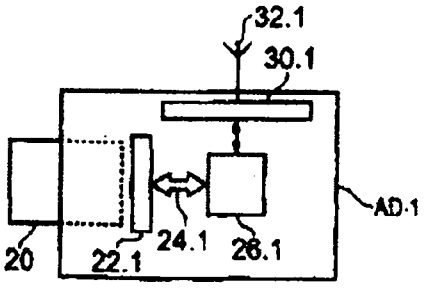

Fig. 3

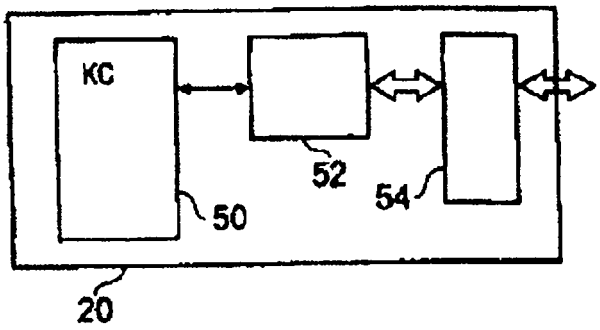
KC
52
54
50
20

Fig. 4

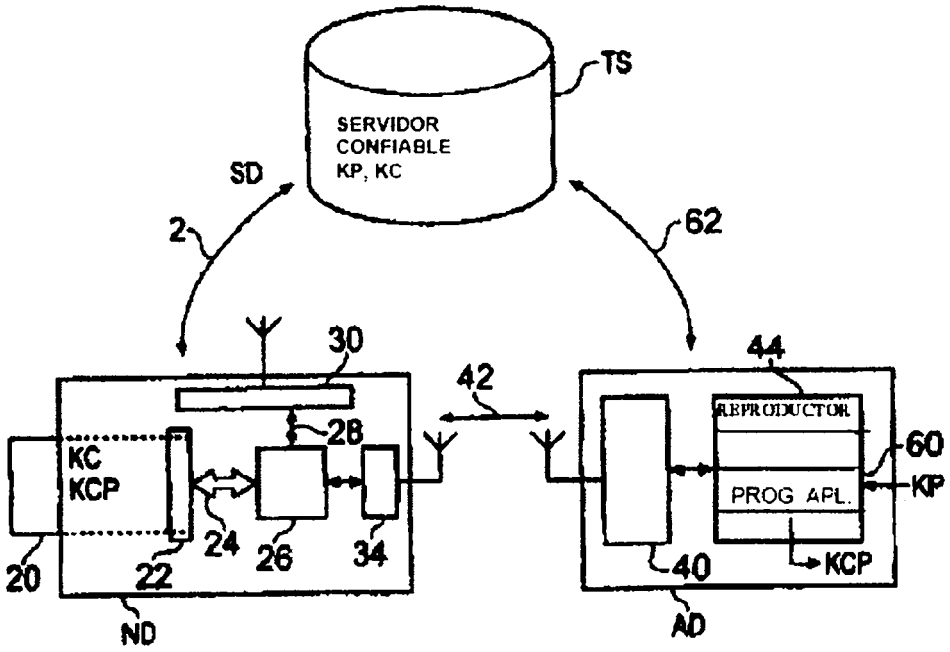
TS
SERVIDOR
CONFIABLE
KP, KC
SD
2
62
30
42
44
28
KC
KCP
REPRODUCTOR
60
KP
PROG APL.
KCP
24
26
34
20
22
40
ND
AD

Fig. 5

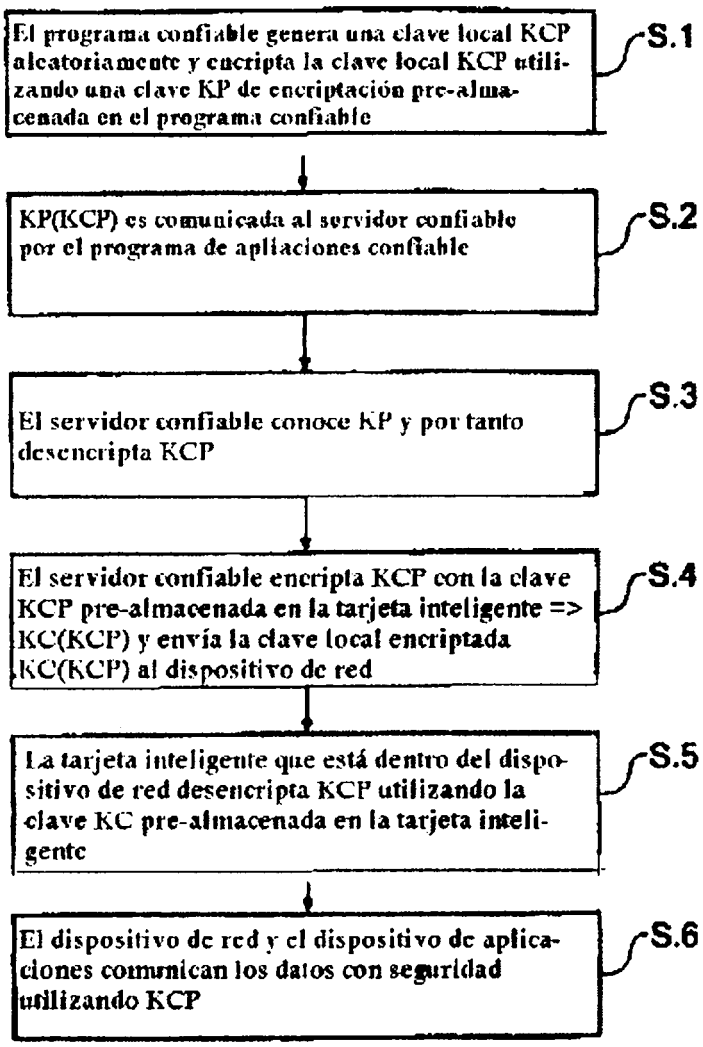
El programa confiable genera una clave local KCP aleatoriamente y encripta la clave local KCP utilizando una clave KP de encriptación pre-almacenada en el programa confiable
S.1
KP(KCP) es comunicada al servidor confiable por el programa de apliaciones confiable
S.2
El servidor confiable conoce KP y por tanto desencripta KCP
S.3
El servidor confiable encripta KCP con la clave KCP pre-almacenada en la tarjeta inteligente => KC(KCP) y envía la clave local encriptada KC(KCP) al dispositivo de red
S.4
La tarjeta inteligente que está dentro del dispositivo de red desencripta KCP utilizando la clave KC pre-almacenada en la tarjeta inteligente
S.5
El dispositivo de red y el dispositivo de aplicaciones comunican los datos con seguridad utilizando KCP
S.6

Fig. 6

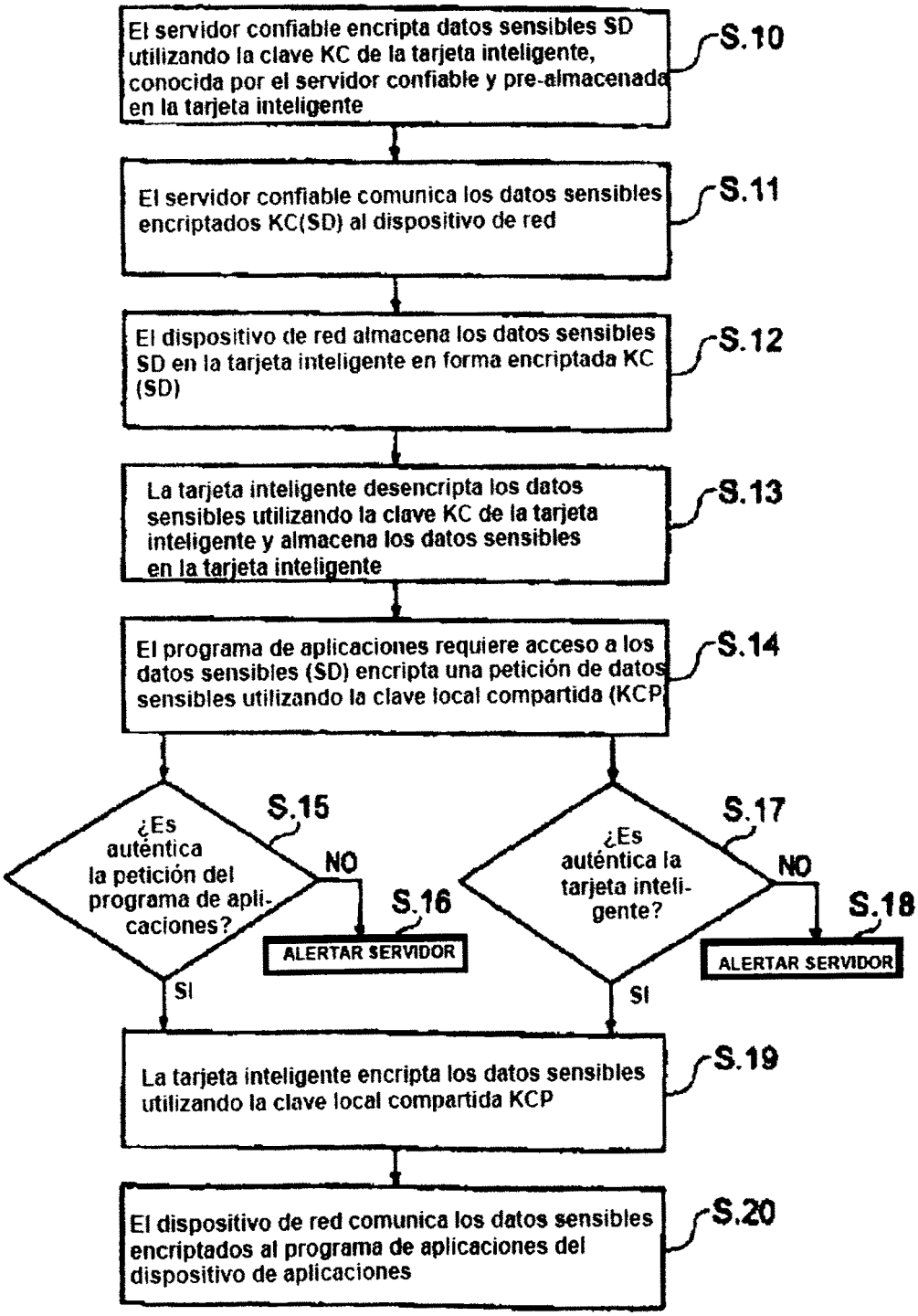
El servidor confiable encripta datos sensibles SD utilizando la clave KC de la tarjeta inteligente, conocida por el servidor confiable y pre-almacenada en la tarjeta inteligente
S.10
El servidor confiable comunica los datos sensibles encriptados KC(SD) al dispositivo de red
S.11
El dispositivo de red almacena los datos sensibles SD en la tarjeta inteligente en forma encriptada KC (SD)
S.12
La tarjeta inteligente desencripta los datos sensibles utilizando la clave KC de la tarjeta inteligente y almacena los datos sensibles en la tarjeta inteligente
S.13
El programa de aplicaciones requiere acceso a los datos sensibles (SD) encripta una petición de datos sensibles utilizando la clave local compartida (KCP
S.14
¿Es auténtica la petición del programa de aplicaciones?
S.15
NO
S.16
ALERTAR SERVIDOR
SI
¿Es auténtica la tarjeta inteligente?
S.17
NO
S.18
ALERTAR SERVIDOR
SI
La tarjeta inteligente encripta los datos sensibles utilizando la clave local compartida KCP
S.19
El dispositivo de red comunica los datos sensibles encriptados al programa de aplicaciones del dispositivo de aplicaciones
S.20

Fig. 7

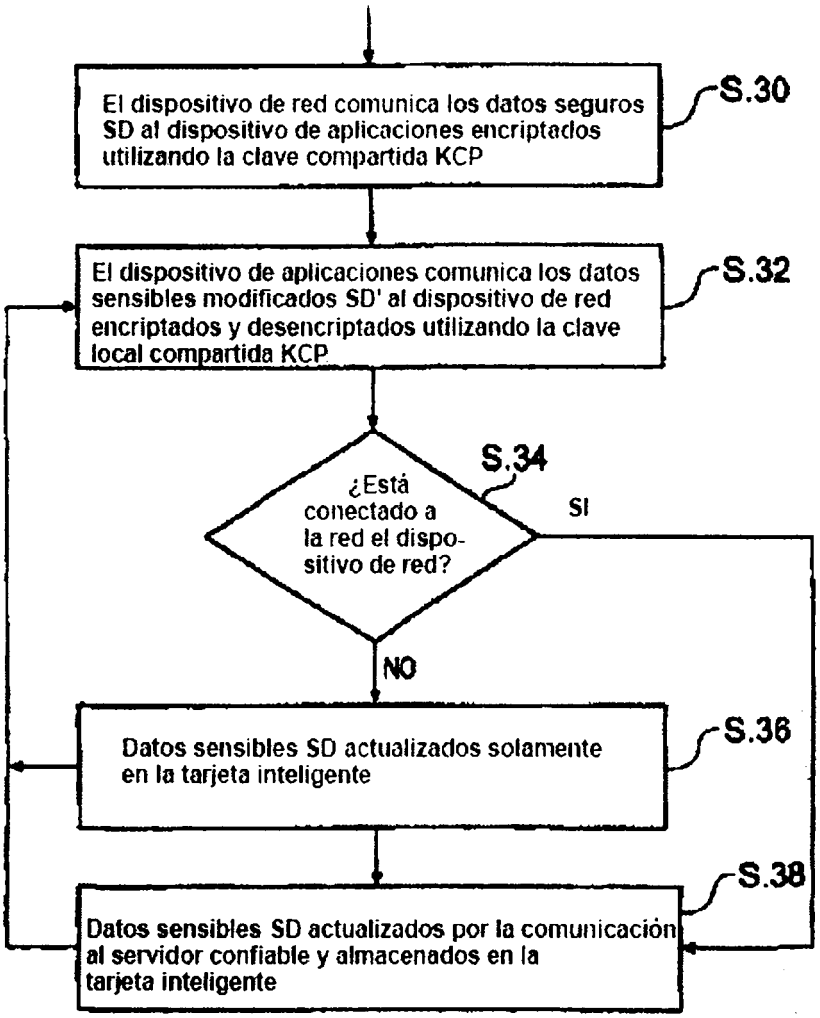
El dispositivo de red comunica los datos seguros SD al dispositivo de aplicaciones encriptados utilizando la clave compartida KCP
S.30
El dispositivo de aplicaciones comunica los datos sensibles modificados SD' al dispositivo de red encriptados y desencriptados utilizando la clave local compartida KCP
S.32
¿Está conectado a la red el dispositivo de red?
S.34
SI
NO
Datos sensibles SD actualizados solamente en la tarjeta inteligente
S.36
Datos sensibles SD actualizados por la comunicación al servidor confiable y almacenados en la tarjeta inteligente
S.38

Fig. 8

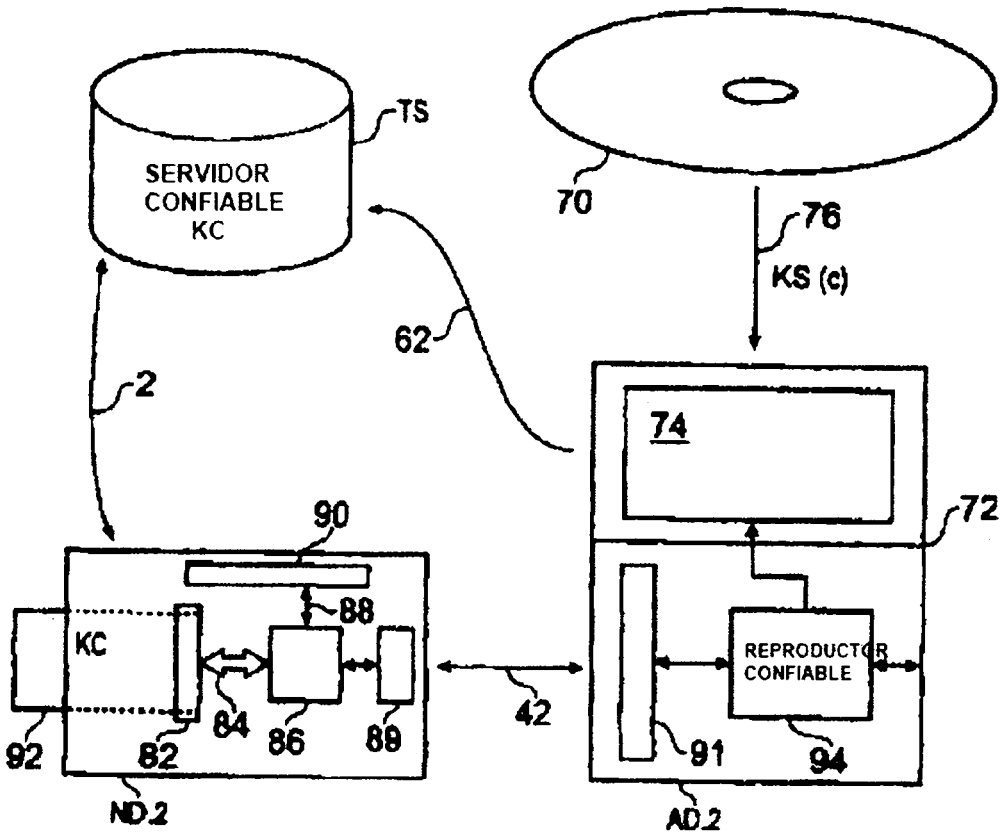
SERVIDOR
CONFIABLE
KC
TS
70
76
KS (c)
62
2
74
72
90
88
KC
REPRODUCTOR
CONFIABLE
42
92
82
84
86
89
91
94
ND.2
AD.2

Fig. 9

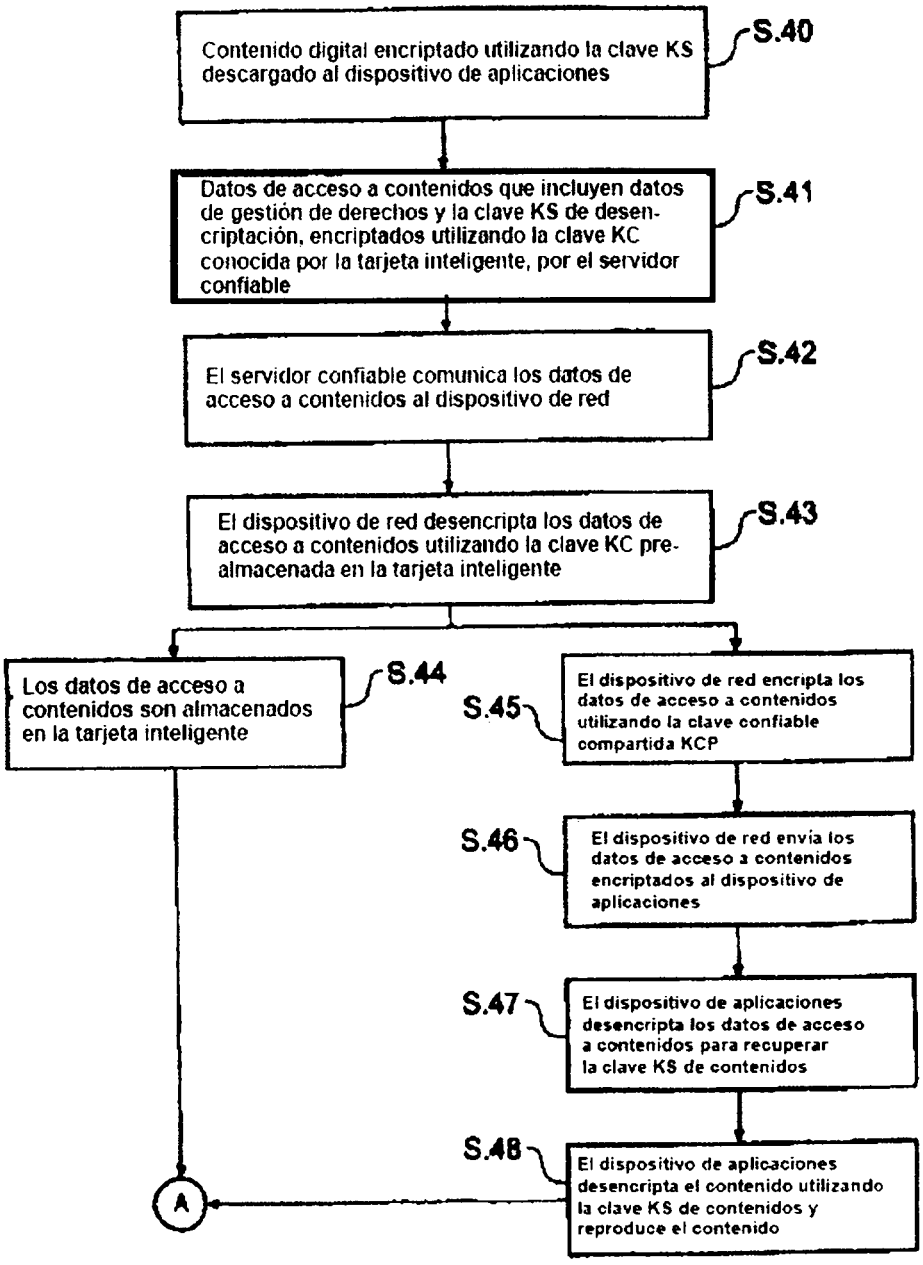
Contenido digital encriptado utilizando la clave KS descargado al dispositivo de aplicaciones
S.40
Datos de acceso a contenidos que incluyen datos de gestión de derechos y la clave KS de desencriptación, encriptados utilizando la clave KC conocida por la tarjeta inteligente, por el servidor confiable
S.41
El servidor confiable comunica los datos de acceso a contenidos al dispositivo de red
S.42
El dispositivo de red desencripta los datos de acceso a contenidos utilizando la clave KC prealmacenada en la tarjeta inteligente
S.43
Los datos de acceso a contenidos son almacenados en la tarjeta inteligente
S.44
S.45
El dispositivo de red encripta los datos de acceso a contenidos utilizando la clave confiable compartida KCP
S.46
El dispositivo de red envía los datos de acceso a contenidos encriptados al dispositivo de aplicaciones
S.47
El dispositivo de aplicaciones desencripta los datos de acceso a contenidos para recuperar la clave KS de contenidos
S.48
El dispositivo de aplicaciones desencripta el contenido utilizando la clave KS de contenidos y reproduce el contenido
A

Fig. 10

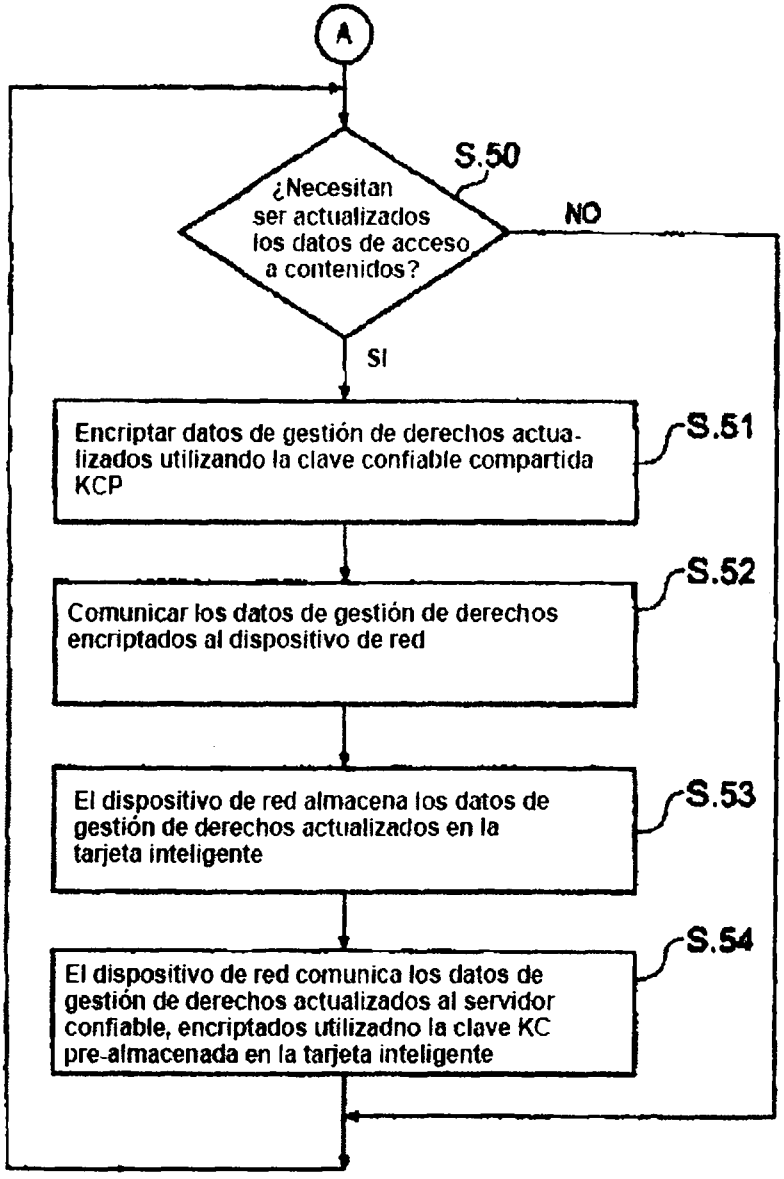
A
S.50
¿Necesitan ser actualizados los datos de acceso a contenidos?
NO
SI
Encriptar datos de gestión de derechos actualizados utilizando la clave confiable compartida KCP
S.51
Comunicar los datos de gestión de derechos encriptados al dispositivo de red
S.52
El dispositivo de red almacena los datos de gestión de derechos actualizados en la tarjeta inteligente
S.53
El dispositivo de red comunica los datos de gestión de derechos actualizados al servidor confiable, encriptados utilizadno la clave KC pre-almacenada en la tarjeta inteligente
S.54

Fig. 11

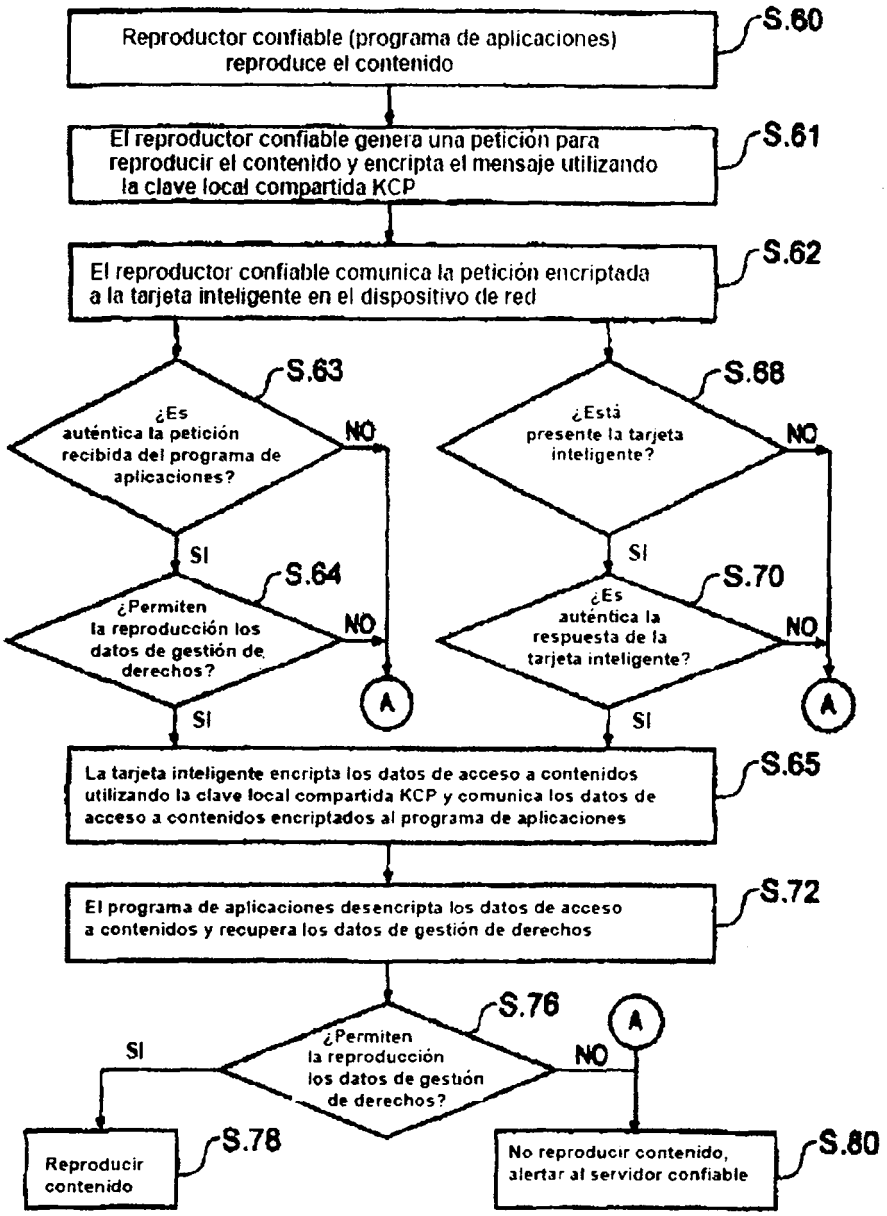
Reproductor confiable (programa de aplicaciones) reproduce el contenido
S.60
El reproductor confiable genera una petición para reproducir el contenido y encripta el mensaje utilizando la clave local compartida KCP
S.61
El reproductor confiable comunica la petición encriptada a la tarjeta inteligente en el dispositivo de red
S.62
S.63
¿Es auténtica la petición recibida del programa de aplicaciones?
NO
SI
S.64
¿Permiten la reproducción los datos de gestión de derechos?
NO
SI
A
S.68
¿Está presente la tarjeta inteligente?
NO
SI
S.70
¿Es auténtica la respuesta de la tarjeta inteligente?
NO
SI
A
La tarjeta inteligente encripta los datos de acceso a contenidos utilizando la clave local compartida KCP y comunica los datos de acceso a contenidos encriptados al programa de aplicaciones
S.65
El programa de aplicaciones desencripta los datos de acceso a contenidos y recupera los datos de gestión de derechos
S.72
S.76
¿Permiten la reproducción los datos de gestión de derechos?
SI
NO
A
Reproducir contenido
S.78
No reproducir contenido, alertar al servidor confiable
S.80

Fig. 12