(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 268 296**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **03292168 .6**
(86) Fecha de presentación : **03.09.2003**
(87) Número de publicación de la solicitud: **1513113**
(87) Fecha de publicación de la solicitud: **09.03.2005**

(54) Título: **Sistema y método para proporcionar comunicaciones seguras basadas en tarjetas inteligentes.**

(45) Fecha de publicación de la mención BOPI:
16.03.2007

(45) Fecha de la publicación del folleto de la patente:
16.03.2007

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

(72) Inventor/es: **Ondet, Olivier y**
Gilbert, Henri

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

DESCRIPCIÓN

Sistema y método para proporcionar comunicaciones seguras basadas en tarjetas inteligentes.

Campo de la invención

La presente invención se relaciona con sistemas para proporcionar servicios seguros a los usuarios a través de una red de comunicaciones.

En algunas realizaciones la red de comunicaciones es una red de radio móvil.

Antecedentes de la invención

Con el desarrollo de los servicios móviles facilitados por un mejoramiento en la infraestructura móvil, como la migración de las redes existentes de redes de tipo 2G a 3G, existe una demanda creciente del mejoramiento de la seguridad de los datos. Aunque los servicios para los usuarios de los móviles pueden ser concebidos para incluir los servicios que no solicitan la comunicación de datos sensibles, los datos sensibles pueden ser solicitados para muchas aplicaciones que proporcionan servicios a los usuarios. Por ejemplo, los datos sensibles pueden representar valores monetarios, que pueden usarse para comprar artículos de manera electrónica usando un dispositivo de comunicación móvil. Otro ejemplo de datos sensibles pudiera ser, por ejemplo, un perfil de datos personales del usuario o una política privada que incluye una lista de contactos, que son confidenciales para el usuario.

Existe por lo tanto un requerimiento creciente de una facilidad para distribuir de manera segura datos sensibles de manera eficiente y efectiva en cuanto a costo. En particular, pero no exclusivamente, es deseable distribuir tales datos sensibles a los dispositivos de comunicaciones móviles para su uso en proporcionar servicios móviles a los usuarios.

Sumario de la invención

De acuerdo a la presente invención es proporcionado un sistema para proporcionar servicios seguros a un usuario a través de una red de comunicaciones. El sistema comprende un dispositivo de aplicaciones que incluye un procesador de datos operable para proporcionar un servicio a un usuario de acuerdo con un programa de aplicaciones que solicita datos sensibles. El sistema incluye un dispositivo de acceso a la tarjeta inteligente para acceder a una tarjeta inteligente únicamente asociada con el usuario, la tarjeta inteligente incluyendo una primera clave de codificación prealmacenada, y una interfase de comunicaciones para comunicar los datos a través de la red de comunicaciones. Un servidor confiable es operable para comunicar los datos sensibles a la tarjeta inteligente de manera segura a través de la red de comunicaciones codificando los datos sensibles usando la primera clave de codificación. Los datos sensibles son descodificados y almacenados en la tarjeta inteligente. El programa de aplicaciones es operable para acceder a los datos sensibles en la tarjeta inteligente solamente a continuación de una autenticación mutua exitosa entre la tarjeta inteligente y el programa de aplicaciones.

Este programa de aplicaciones puede acceder a los datos sensibles para realizar una función particular, o para procesar los datos, por ejemplo para cambiar el valor de los datos, tal como reducir el valor de los datos a continuación de una acción. Por ejemplo, si los datos sensibles representan un valor monetario, el valor puede ser reducido a continuación de una transacción.

La autenticación mutua entre la tarjeta inteligente y el programa de aplicaciones puede incluir un intercambio de mensajes entre el programa de aplicaciones y la tarjeta inteligente, siendo los mensajes codificados usando una segunda clave de codificación local (KCP) compartida entre la tarjeta inteligente y el programa de aplicaciones. En algunas realizaciones la clave puede ser generada de manera aleatoria. La segunda clave de codificación local es comunicada a la tarjeta inteligente a través del servidor confiable. La segunda clave de codificación local puede ser por lo tanto usada para autenticar la tarjeta inteligente, y la tarjeta inteligente puede autenticar el programa de aplicaciones antes que el programa de aplicaciones pueda acceder a los datos sensibles.

De acuerdo a las realizaciones de la presente invención la tarjeta inteligente la cual puede ser, por ejemplo, un Módulo de Identidad del Abonado (SIM) o un Módulo de Identidad del Abonado Universal (USIM) proporciona una facilidad para comunicar datos de manera segura entre un servidor confiable conectado a la red y a la misma tarjeta inteligente. Como tal la tarjeta inteligente proporciona un lugar de depósito para los datos sensibles para el acceso por un programa de aplicaciones proporcionando un servicio al usuario el cual utiliza los datos sensibles. Sin embargo, el acceso a los datos sensibles es solamente permitido a continuación de la autenticación por el programa de aplicaciones de que la tarjeta inteligente está asociada únicamente con un usuario y la autenticación por la tarjeta inteligente de que al programa de aplicaciones se le permite el acceso a los datos sensibles.

Los datos sensibles pueden ser almacenados de manera segura y actualizados en la tarjeta inteligente tanto si la comunicación es a través de una red disponible o no. Por ejemplo, si la red de comunicaciones es una red de comunicaciones de radio móvil entonces si el dispositivo de red entra en un área donde no existe cobertura para radio entonces el servidor confiable puede no estar accesible. Sin embargo, utilizando las facilidades de seguridad de la tarjeta inteligente los datos sensibles pueden ser almacenados de manera segura en la tarjeta inteligente. El programa de aplicaciones puede desear actualizar los datos sensibles a continuación de los servicios proporcionados al usuario.

Los datos sensibles pueden ser accedidos en la tarjeta inteligente como si la tarjeta inteligente estuviera actuando como un servidor confiable local proporcionando un almacenamiento seguro para los datos sensibles.

Asociando un programa de aplicaciones, el cual es relativamente fácil de copiar o clonar, con una tarjeta inteligente la cual es única y por lo tanto no puede ser clonada, una combinación segura para proporcionar servicios a los usuarios es formada.

El dispositivo de aplicaciones pueden ser por ejemplo un Asistente Personal Digital (PDA) o un teléfono inteligente u otro dispositivo similar, el cual está provisto con una facilidad para comunicarse con una red de comunicaciones. Sin embargo, en algunas realizaciones el dispositivo de aplicaciones puede proporcionar el servicio al usuario de acuerdo al programa de aplicación que corre en el dispositivo, con un dispositivo de red siendo proporcionado para comunicarse con la red. Por lo tanto el dispositivo de red puede incluir el dispositivo de acceso a la tarjeta inteligente, así como la interfase de comunicaciones para comunicar los datos de manera segura a través de la red de comunicaciones usando la primera clave de codificación (tarjeta inteligente). El dispositivo de red puede también incluir una interfase de comunicación local para la comunicación de los datos con el dispositivo de aplicaciones. El dispositivo de aplicaciones puede incluir una interfase de comunicación local correspondiente para la comunicación con el dispositivo de red. El dispositivo de red y el dispositivo de aplicaciones son operables para efectuar la comunicación segura de los datos sensibles a través de las interfases de comunicación locales usando la segunda clave de codificación local (KCP). La segunda clave por lo tanto proporciona una facilidad para comunicar los datos de manera segura entre el dispositivo de aplicaciones y el dispositivo de red usando la codificación de clave privada. Una ventaja es proporcionada usando la segunda clave de codificación local debido a que la codificación de clave privada puede ser utilizada requiriendo una energía de procesamiento relativamente baja en comparación con la codificación de clave pública. El costo para la implementación de la autenticación y comunicación segura puede ser por lo tanto relativamente bajo.

Varios aspectos adicionales y características de la presente invención que han sido realizados están definidos en las reivindicaciones anexadas.

Breve descripción de los dibujos

Las realizaciones de la presente invención serán ahora descritas a modo de ejemplo solamente con referencia a los dibujos acompañantes donde las partes están provistas con números de referencia correspondientes y en los cuales:

La Figura 1 es un diagrama en bloque esquemático de un sistema para proporcionar servicios a un usuario usando un dispositivo de aplicaciones en los cuales los datos sensibles son distribuidos a través de un dispositivo de red;

La Figura 2 es un diagrama en bloque esquemático de un dispositivo de red ejemplo y un dispositivo de aplicaciones ejemplo, los cuales aparecen en la Figura 1;

La Figura 3 es un diagrama en bloque esquemático de otro dispositivo de aplicaciones ejemplo que incorpora una capacidad de comunicaciones de red;

La Figura 4 es un diagrama en bloque esquemático de una tarjeta inteligente;

La Figura 5 es un diagrama en bloque de las partes del sistema mostrado en la Figura 1 para su uso en distribuir datos sensibles;

La Figura 6 es un diagrama de flujo que representa un proceso para establecer una clave local compartida entre una tarjeta inteligente en el dispositivo de red y un programa de aplicaciones que corre en el dispositivo de aplicaciones mostrado en la Figura 1;

La Figura 7 es un diagrama de flujo que ilustra un proceso para distribuir datos sensibles al programa de aplicaciones usando la tarjeta inteligente de la Figura 6, incluyendo la autenticación mutua de la tarjeta inteligente y el programa de aplicaciones;

La Figura 8 es un diagrama de flujo que ilustra una operación 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 en bloque esquemático que muestra las partes de un sistema las cuales están dispuestas para distribuir contenido a un dispositivo de aplicaciones con datos de acceso a contenido;

La Figura 10 es un diagrama de flujo que ilustra un proceso para entregar datos de acceso a contenido a un dispositivo de aplicaciones para usar en el acceso a contenido;

La Figura 11 es un diagrama de flujo que ilustra para almacenar de manera segura datos de acceso a contenido actualizados en una tarjeta inteligente mostrada en la Figura 9; y

La Figura 12 es un diagrama de flujo que ilustra un proceso en el cual la autenticación mutua entre una tarjeta inteligente y un jugador confiable es realizada y los datos de administración de derechos son chequeados antes que el contenido sea reproducido.

Descripción de las realizaciones ejemplos

Red Ejemplo

La Figura 1 proporciona un arreglo ejemplo en el cual los datos son distribuidos a un dispositivo de aplicaciones a través de un dispositivo de red. En la Figura 1 una red 1 incluye una facilidad para comunicarse con un dispositivo de red ND usando por ejemplo un enlace de comunicaciones móviles 2. El enlace de comunicaciones móviles 2 es establecido entre un nodo o estación base 3 y el dispositivo de red ND de acuerdo con un estándar de interfase establecido. Si la red incluye una red de radio móvil de UMTS, entonces la interfase de comunicaciones puede operar de acuerdo con el estándar de Red de Acceso de Radio Terrestre Universal (UTRAN). La red 1 proporciona una facilidad para comunicar varios tipos de datos a equipamiento conectado a la red. Por ejemplo, un servidor de contenido CS puede ser provisto para distribuir el contenido 4 a un dispositivo de aplicaciones AD. También mostrado en la Figura 1 está un servidor confiable TS el cual, como será explicado en breve, proporciona una facilidad para comunicar datos sensibles al dispositivo de red ND para su uso por le dispositivo de aplicaciones AD.

Las realizaciones de la presente invención serán ahora descritas con referencia a los arreglos mostrados en la Figura 1 donde un dispositivo de red ND está operativamente asociado con un dispositivo de aplicaciones AD. El arreglo del dispositivo de red ND y el dispositivo de aplicaciones AD proporciona una facilidad para comunicar datos sensibles para su uso en programas de aplicaciones que son ejecutados en el dispositivo de aplicaciones. En una realización ejemplo, el contenido 4 es reproducido por el dispositivo de aplicaciones AD de acuerdo con los datos de control de acceso, los cuales pueden formar, en una realización, un ejemplo de datos sensibles. Los datos de control de acceso pueden indicar las condiciones para la reproducción y copia del contenido. Los datos de control de acceso pueden también proporcionar una clave para descodificar el contenido, si el contenido ha sido codificado antes de ser descargado en el dispositivo de aplicaciones AD. Aunque en la Figura 1 el contenido puede ser descargado desde un servidor de contenido CS, el contenido puede ser recibido por el dispositivo de aplicaciones AD a través de cualquier forma conveniente tal como a través de un portador de datos (por ejemplo DVD, CD ROM) o cualquier otro medio convencional y de cualquier fuente. El dispositivo de red ND y el dispositivo de aplicaciones AD son mostrados en más detalle en la Figura 2.

Dispositivos de Red y de Aplicaciones

En la Figura 2 el dispositivo de red ND es mostrado incluyendo una tarjeta inteligente 20 la cual es cargada en un dispositivo de acceso a la tarjeta inteligente 22 que forma parte del dispositivo de red. Un bus de acceso 24 conecta el dispositivo de acceso a la tarjeta inteligente a un procesador de datos 26 para proporcionar el acceso a la tarjeta inteligente 20. El procesador de datos está conectado a través de un bus de comunicaciones 28 a una interfase de comunicaciones 30 la cual es operable de acuerdo con un estándar de comunicaciones en red para comunicarse con la red 1 como es mostrado en la Figura 1. Así la interfase de comunicaciones 30, por ejemplo, puede operar de acuerdo con la interfase de la Red de Acceso de Radio Terrestre Universal (UTRAN) utilizando la antena 32 para comunicarse a través del enlace de comunicaciones 2 como es mostrado en la Figura 1. La interfase de comunicaciones 30 de esta manera proporciona una facilidad para conectar el dispositivo de red ND con la red 1.

El dispositivo de red ND también incluye una segunda interfase de comunicaciones 34 conectada a través de un bus interno 36 al procesador de datos 26, para formar un enlace de comunicaciones local con un dispositivo de aplicaciones AD. Una interfase de comunicaciones correspondiente 40 está incluida en el dispositivo de aplicaciones AD para comunicar los datos entre el dispositivo de red ND y el dispositivo de aplicaciones AD. Un enlace de comunicaciones representado por una flecha de doble cabeza 42 está formado por la interfase de comunicaciones 34 en el dispositivo de red ND y la interfase de comunicaciones 40 en el dispositivo de aplicaciones AD. El enlace de comunicaciones proporciona una facilidad para comunicarse localmente entre el dispositivo de aplicaciones AD y el dispositivo de red ND. En algunas realizaciones el enlace de comunicaciones puede ser formado por la operación de las interfases de comunicaciones 34, 40 usando, por ejemplo, los estándares Bluetooth, RS232 o IEEE802.3.

El dispositivo de aplicaciones AD también incluye un procesador de datos 44 el cual está dispuesto para ejecutar programas de aplicaciones para proporcionar servicios a un usuario.

Aunque el dispositivo de red ND y el dispositivo de aplicaciones AD son mostrados en las Figuras 1 y 2 como dispositivos separados, en otras realizaciones el dispositivo de aplicaciones y el dispositivo y el dispositivo de red pueden estar físicamente formados como el mismo dispositivo. Un ejemplo de tales realizaciones es mostrado en la Figura 3.

En la Figura 3 un dispositivo de aplicaciones AD.1 está provisto con una facilidad para comunicarse con la red 1, usando una interfase de comunicaciones 30.1, que se corresponde de manera sustancial con la interfase de comunicaciones del dispositivo de red ND mostrado en la Figura 2. Para el dispositivo de aplicaciones AD.1 mostrado en la Figura 3 los procesadores de datos 26, 44 en el dispositivo de aplicaciones y el dispositivo de red mostrados en la Figura 2, son remplazados por el mismo procesador de datos 26.1. El procesador de datos 26.1 ejecuta los programas

de aplicaciones y también controla la comunicación con la red 1 y accede a la tarjeta inteligente 20. El dispositivo de aplicaciones AD.1 pudiera ser un Asistente Personal Digital (PDA), un teléfono móvil o dispositivo similar. El dispositivo de red ND mostrado en la Figura 2 pudiera también ser implementado como un teléfono móvil o un PDA, donde el dispositivo de aplicaciones AD pudiera ser una computadora personal (PC).

Más será explicado a cerca de la operación del dispositivo de aplicaciones y el dispositivo de red en las siguientes secciones. Sin embargo, para facilitar la explicación, el sistema ilustrado en la Figura 1, que incluye dispositivos de red, y de aplicaciones separados será adoptado.

Tarjeta Inteligente

La Figura 4 proporciona un diagrama en bloque simplificado ilustrando la forma de una tarjeta inteligente típica. La tarjeta inteligente 20 está generalmente definida como que tiene algunas facilidades de procesamiento de datos en combinación con una memoria y una interfase. Como es mostrado en la Figura 4 la tarjeta inteligente 20 incluye una memoria 50, conectada a un procesador de datos 52 a través de una canal de interfase 54. La interfase de comunicaciones 54 es accedida a través de un dispositivo de acceso a la tarjeta inteligente 22 (mostrado en la Figura 2) para leer y escribir datos hacia/desde la memoria 50. Sin embargo, una de las características de las tarjetas inteligentes es que la interfase 54 no tiene acceso directo a la memoria 50. Así solamente el procesador 52 puede acceder a la memoria 50 y luego no todo es accesible a través de la interfase 54. Típicamente una tarjeta inteligente puede incluir datos tal como una clave de codificación KC la cual es pre-almacenada en una memoria 50. La clave de codificación KC no puede ser accedida desde la interfase 54 pero puede ser usada para codificar los datos alimentados a la tarjeta inteligente los cuales pueden ser entonces codificados por el procesador de datos 52 usando la clave pre-almacenada KC. Por lo tanto, generalmente la tarjeta inteligente puede estar caracterizada como que tiene limitaciones de hardware, lo cual restringe el acceso a la memoria 50 proporcionando de esta manera alguna seguridad a los datos almacenados en la tarjeta inteligente. Como será explicado en breve, la tarjeta inteligente proporciona una facilidad para almacenar datos sensibles y descodificar y codificar datos a ser comunicados hacia y desde la red y un programa de aplicaciones.

Un Módulo de Identidad del Abonado (SIM) es un ejemplo de una tarjeta inteligente, siendo otro ejemplo el Módulo de Identidad del Abonado Universal (USIM) los cuales son proporcionados por los proveedores de servicios de red y están únicamente asociados con los usuarios de una red de telecomunicaciones tal como GSM o UMTS. De esta manera cuando es emitida por un proveedor de servicios de red a un usuario, la tarjeta inteligente está únicamente asociada con aquel usuario e incluye la clave de codificación pre-almacenada KC para uso solamente con aquella tarjeta inteligente.

Comunicación Segura entre el Dispositivo de Red y el Dispositivo de Aplicaciones

La Figura 5 proporciona una ilustración de partes del sistema de la Figura 1, el cual incluye el dispositivo de red ND y el dispositivo de aplicaciones AD e ilustra un arreglo para establecer comunicaciones seguras entre la tarjeta inteligente en el dispositivo de red y el programa de aplicaciones en el dispositivo de aplicaciones y para realizar la autenticación mutua. La Figura 5 también muestra al servidor confiable TS de la Figura 1 aunque los otros elementos de la red que aparecen en la Figura 1 no están representados en la Figura 5 para una mayor claridad.

Las realizaciones de la presente invención proporcionan una facilidad para distribuir los datos sensibles a ser usados en un dispositivo de aplicaciones AD utilizando características de seguridad inherentes a las tarjetas inteligentes que pueden ser emitidas a los usuarios por lo proveedores de servicios de red para el uso con los dispositivos de red. Una ventaja proporcionada por las realizaciones de la presente invención es que una facilidad para efectuar comunicaciones seguras entre un dispositivo de aplicaciones y un dispositivo de red es lograda a un costo comparativamente bajo, debido a que la codificación de clave privada puede ser usada en lugar de la codificación de clave pública la cual requiere una capacidad de procesamiento incrementada.

La Figura 5 proporciona una ilustración de un arreglo para efectuar una comunicación segura generando de manera segura una única clave local (KCP). La clave local es generada en el dispositivo de aplicaciones AD por un programa de aplicaciones para ser comunicada al dispositivo de red. Una clave secreta compartida KCP es de esta manera proporcionada para acciones de autenticación y comunicación por el dispositivo de aplicaciones AD y el dispositivo de red ND. Usando la clave local compartida KCP, la codificación de clave privada puede ser utilizada para la comunicación entre el programa de aplicaciones y la tarjeta inteligente.

Correspondientemente, la energía de procesamiento de la tarjeta inteligente puede ser mantenida relativamente baja manteniendo de esta manera reducidos los costos para la tarjeta inteligente con respecto a aquella que sería requerida si fuera usada la codificación de clave pública. La distribución de la clave privada y su generación serán ahora explicadas con referencia a la Figura 4 en combinación con el diagrama de flujo mostrado en la Figura 5.

En la Figura 5 un programa de aplicaciones 60 siendo ejecutado por el procesador de datos 44 en el dispositivo de aplicaciones AD incluye una clave privada KP la cual es única para aquel programa de aplicaciones pero también es conocida por el servidor confiable TS. El programa de aplicaciones 60 está dispuesto para generar de manera aleatoria una clave local compartida KCP para ser compartida en el uso entre el dispositivo de aplicaciones AD y el dispositivo de red ND. El procesador de datos 44 está dispuesto para codificar la clave local KCP con la clave de codificación

de programa KP. La clave local codificada KP(KCP) es entonces comunicada al servidor confiable. La comunicación puede ser efectuada por cualquier medio conveniente tal como copiando la clave local codificada 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 codificada KCP a través del enlace local 42 la cual entonces puede ser comunicada a través de un enlace de red 4 al servidor confiable TS. Sin embargo, como una generalización la comunicación entre el dispositivo de aplicaciones AD y el servidor confiable TS está representada por una flecha de doble cabeza 62.

La clave local codificada KC(KCP) es entonces recibida en el servidor confiable TS y descodificada usando la clave privada KP. El servidor confiable puede entonces comunicar la clave local KCP al dispositivo de red ND, codificando la clave local KCP usando la clave de la tarjeta inteligente KC. Ya que la tarjeta inteligente ha pre-almacenado la clave de la tarjeta inteligente KC entonces la comunicación de la clave local KCP puede ser efectuada a través del enlace de comunicaciones de red 2 a la interfase de comunicaciones 30. La clave local KCP puede entonces ser descodificada en la tarjeta inteligente usando la clave de la tarjeta inteligente KC y almacenada en la memoria de la tarjeta inteligente 50. Por lo tanto, como resultado la clave local KCP es conocida para la tarjeta inteligente en el dispositivo de red ND y el programa de aplicaciones en el dispositivo de aplicaciones AD y además es única para el pareo entre le programa de aplicaciones y la tarjeta inteligente en el dispositivo de red ND. Como resultado, cuando quiera que una comunicación es requerida entre el dispositivo de red ND y el dispositivo de aplicaciones AD la codificación puede ser efectuada usando la clave KCP la cual puede también ser usada para autenticar la tarjeta inteligente así como el programa de aplicaciones 60 en si mismo.

Los pasos del proceso involucrados con la generación de la clave local KCP compartida entre el dispositivo de aplicaciones AD y el dispositivo de red ND son ilustrados en la Figura 6 y se resumen como sigue:

S.1: El programa confiable en el dispositivo de aplicaciones AD genera una única clave aleatoria KCP y codifica la clave aleatoria usando una clave de programa KP el cual ha sido pre-almacenado en el programa confiable.

S.2: La clave local codificada KP(KCP) es comunicada al servidor confiable TS.

S.3: El servidor confiable conoce la clave de codificación KP usada por el programa de aplicaciones confiable y de esta manera puede descodificar la clave local KCP.

S.4: El servidor confiable codifica la clave local KCP con la clave de la tarjeta inteligente KC la cual es almacenada en la tarjeta inteligente y únicamente asociada con el usuario. El servidor confiable TS envía la clave local codificada KC(KCP) al dispositivo de red ND a través del enlace de comunicaciones de red 2.

S.5: La tarjeta inteligente descodifica la clave local KCP usando la clave de la tarjeta inteligente KC pre-almacenada dentro de la tarjeta inteligente 20 y almacena la clave local KCP dentro de la memoria de la tarjeta inteligente.

S.6: La tarjeta inteligente y el programa de aplicaciones pueden entonces intercambiar datos de manera segura usando la única clave local KCP.

Debido a que la clave local KCP ha sido generada de manera aleatoria por el programa de aplicaciones 60, la clave KCP es única para el par de dispositivo de red/aplicaciones. La clave local KCP también puede ser usada para la autenticación de la tarjeta inteligente por el programa de aplicaciones y el programa de aplicaciones por la tarjeta inteligente. El programa de aplicaciones, el cual es una entidad, que puede ser relativamente fácil de copiar, puede estar de esta manera únicamente asociado de manera operativa con una tarjeta inteligente, la cual es una entidad, que no puede ser copiada fácilmente.

Distribución y Actualización de los Datos Sensibles

Las partes del sistema mostrado en la Figura 5 pueden proporcionar una facilidad para comunicar los datos sensibles de manera segura entre el programa de aplicaciones y la tarjeta inteligente para proporcionar un servicio al usuario. Ejemplos de datos sensibles pudieran ser, por ejemplo, una licencia comprada para la reproducción de contenido, información confidencial, detalles de contactos privados o una representación electrónica de datos de un valor monetario. Para el ejemplo de un valor monetario, los valores de las monedas puede ser proporcionados para permitir a un usuario comprar un producto o servicio o conducir alguna transacción electrónica donde un valor monetario es proporcionado a cambio del servicio o producto. Otros ejemplo de datos sensibles son la información privada o información de políticas asociada con, por ejemplo, detalles de contactos que son confidenciales para un usuario. Estos son ejemplos de datos sensibles, que pueden ser cambiados por un programa de aplicaciones después de algún procesamiento de los datos sensibles.

Con referencia nuevamente a la Figura 5 el servidor confiable por ejemplo puede almacenar o generar datos sensibles los cuales van a ser utilizados por el programa de aplicaciones que corre en el dispositivo de aplicaciones AD. Debido a que la tarjeta inteligente incluye la única clave de la tarjeta inteligente KC asociada con el usuario entonces el servidor confiable TS puede codificar los datos sensibles SD y comunicar los datos codificados KC(SD) a la tarjeta inteligente en el dispositivo de red ND usando el enlace de comunicaciones de red 2, como se describió anteriormente. Los datos sensibles codificados KC(SD) son recibidos a través de la tarjeta inteligente usando el dispositivo de

acceso a la tarjeta inteligente 22 y descodificados para recuperar los datos sensibles los cuales pueden entonces ser almacenados en la tarjeta inteligente 20.

Si el programa de aplicaciones en el dispositivo de aplicaciones solicita acceso a los datos sensibles entonces una solicitud de acceso puede ser comunicada a través del enlace local 42 el cual puede ser autenticado usando la clave local KCP la cual puede ser verificada por la tarjeta inteligente 20 en el dispositivo de red. Los datos sensibles pueden entonces ser codificados usando la clave local KCP en la tarjeta inteligente 20 y comunicados al dispositivo de aplicaciones AD donde el programa de aplicaciones puede descodificar los datos sensibles usando la clave local KCP.

El programa de aplicaciones puede también confirmar la presencia de la tarjeta inteligente proporcionando el servicio al usuario de acuerdo con el programa de aplicación. La autenticación y la presencia de la tarjeta inteligente pueden ser confirmadas intercambiando mensajes usando la clave local compartida KCP como ya fue descrito.

Si el programa de aplicaciones cambia los datos sensibles de alguna forma entonces los datos sensibles pueden ser almacenados en la tarjeta inteligente 20 antes de ser actualizados por el servidor confiable. Sin embargo, para 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 la ilustración ejemplo mostrada en las Figuras 1 y 5, la red forma una red de radio móvil y de esta manera el enlace de comunicaciones 2 puede no siempre estar disponible. Por lo tanto el dispositivo de red ND puede no estar siempre en contacto con la red 1. En una situación en la cual el dispositivo de red no pueda comunicarse con la red, la tarjeta inteligente actúa como un almacén local para los datos sensibles. Debido a que la tarjeta inteligente en si misma incluye condiciones de seguridad (explicadas anteriormente), los datos sensibles pueden ser almacenados de manera segura en la tarjeta inteligente, de una forma, que únicamente asocia aquellos datos sensibles con el usuario. Por lo tanto, por ejemplo, si los datos sensibles representan un valor monetario, el cual cambia como resultado de una transacción, entonces los datos sensibles pueden ser actualizados en la tarjeta inteligente para reflejar el cambio en el valor. Los datos sensibles son entonces actualizables a través del enlace de red 2 cuando el enlace de red existe proporcionando de esta manera una operación sustancialmente coherente del servicio del usuario ya que es determinado por el programa de aplicaciones si el dispositivo de red está en comunicación con la red o no. Esto es debido a que cuando la red móvil no está disponible, por ejemplo debido a que carece de cobertura de radio, entonces la tarjeta inteligente actúa como un almacén local para el valor monetario actualizado.

En resumen, la operación de la realización de la invención ilustrada en la Figura 5 es descrita por el diagrama de flujo mostrado en la Figura 7 y la Figura 8. El diagrama de flujo en la Figura 7 ilustra la operación de distribución de los datos sensibles a la tarjeta inteligente, y el acceso a los datos sensibles en la tarjeta inteligente por el programa de aplicaciones. La Figura 8 ilustra la operación del programa de aplicaciones en el dispositivo de aplicaciones cuando se usa la tarjeta inteligente como un servidor local.

El diagrama de flujo mostrado en la Figura 7 se resume como sigue:

S.10: El servidor confiable codifica los datos sensibles SD usando la clave de la tarjeta inteligente KC. El servidor confiable conoce la clave de la tarjeta inteligente KC. La clave de la tarjeta inteligente KC es también pre-almacenada en la tarjeta inteligente.

S.11: El servidor confiable envía los datos sensibles codificados KC(SD) al dispositivo de red.

S.12: El dispositivo de red almacena los datos sensibles codificados KC(SD) en la tarjeta inteligente donde los datos son descodificados usando la clave de la tarjeta inteligente KC.

S.13: La tarjeta inteligente descodifica entonces los datos sensibles, usando la clave de la tarjeta inteligente KC, para recuperar los datos sensibles. La descodificación es realizada en la tarjeta inteligente y los datos sensibles son almacenados en la tarjeta inteligente.

S.14: Cuando el programa de aplicaciones que corre en el dispositivo de aplicaciones solicita el acceso a los datos sensibles para proporcionar un servicio al usuario, el programa de aplicaciones codifica una solicitud de los datos sensibles usando la clave local compartida KCP, la cual ha sido establecida en la tarjeta inteligente.

S.15: Dentro de la tarjeta inteligente, la tarjeta inteligente determina si la solicitud del programa de aplicaciones es auténtica. La autenticación es realizada descodificando la solicitud usando la clave local compartida KCP. Si una solicitud válida es recuperada correctamente (de acuerdo a una forma predeterminada) entonces la solicitud es considerada que es autentica. Si la solicitud es auténtica entonces el procesamiento procede al paso S.19. De otra manera el procesamiento procede al paso S.16.

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

S.17: El programa de aplicaciones determina si la tarjeta inteligente es auténtica. Esto puede ser determinado por ejemplo, haciendo arreglos para que la tarjeta inteligente responda un mensaje de solicitud enviado a ella, generando un mensaje de respuesta de acuerdo a un formato predeterminado y codificando el mensaje usando la clave local compartida KCP. Si después de descodificar la respuesta, un mensaje de respuesta que tiene el formato correcto es

recuperado por el programa de aplicaciones entonces se determina que la tarjeta inteligente es auténtica y el procesamiento procede al paso S.19. De otra manera el procesamiento procede al paso S.18.

S.18: Si la autenticación falla, el procesamiento termina y el servidor confiable es alertado sobre el hecho de que un intento ilegal ha sido realizado para usar una tarjeta inteligente incorrecta.

S.19: Si la tarjeta inteligente y el programa de aplicaciones han realizado la autenticación mutua de manera exitosa, lo que puede ser indicado por un intercambio de mensajes mutuos adicional, entonces la tarjeta inteligente codifica los datos sensibles usando la clave local compartida.

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

Una de las ventajas proporcionada por las realizaciones de la invención es que la tarjeta inteligente puede actuar como un servidor local cuando la red está no disponible para el programa de aplicaciones. Cualquier cambio a los datos sensibles puede ser almacenado en la tarjeta inteligente y actualizado en la red, cuando la red este disponible. La operación del programa de aplicaciones y de la tarjeta inteligente cuando se usa la tarjeta inteligente como un servidor local como es ilustrado en la Figura 8 se resume como sigue:

S.30: La tarjeta inteligente en el dispositivo de red comunica los datos sensibles al programa de aplicaciones cuando estos son solicitados por el programa de aplicaciones que corre en el dispositivo de aplicaciones. El dispositivo de red codifica los datos sensibles usando la clave local compartida KCP antes de ser comunicados a través del enlace local 42.

S.32: Después que el programa de aplicaciones ha procesado los datos sensibles proporcionando un servicio al usuario y posiblemente cambiando los datos sensibles, los datos sensibles son comunicados nuevamente hacia el dispositivo de red por el dispositivo de aplicaciones. El dispositivo de aplicaciones codifica nuevamente los datos sensibles usando la clave local KCP, los cuales son descodificados dentro de la tarjeta inteligente 20 nuevamente usando la clave local compartida KCP. Los datos sensibles actualizados pueden entonces ser mantenidos en la tarjeta inteligente de una manera segura y en una única asociación con el usuario. Así, de esta forma la tarjeta inteligente actúa como lugar de depósito para los datos sensible. Es solamente cuando el dispositivo de red está en contacto con la red que los datos sensibles pueden ser actualizados. Por lo tanto, almacenar los datos sensibles en forma actualizada en la tarjeta inteligente mantiene una representación coherente de los datos sensibles, que pueden ser asegurados en la tarjeta inteligente.

S.34: Si el dispositivo de red se puede conectar a la red, entonces:

S.36: Los datos sensibles SD son actualizados comunicando los datos sensibles actuales desde la tarjeta inteligente al servidor confiable. Los datos sensibles son codificados usando la clave de la tarjeta inteligente KC dentro de la tarjeta inteligente y correspondientemente descodificados en el servidor confiable.

S.38: Si el dispositivo de red no puede ser conectado a la red entonces los datos sensibles son mantenidos solamente en la tarjeta inteligente.

Distribución de Contenido y de los Datos de Administración de Derechos

Otra realización ejemplo de la presente invención será ahora descrita en asociación con proporcionar una facilidad para distribuir contenido al usuario. Como es ilustrado en la Figura 1 el contenido puede ser descargado a un dispositivo de aplicaciones desde un servidor de contenidos donde el contenido está almacenado. Como se mencionó anteriormente, la forma en la cual el contenido puede ser distribuido no está limitado a ser descargado desde un servidor sino que puede ser, por ejemplo, distribuido sobre un medio apropiado tal como un CD ROM o DVD o similar.

La Figura 9 proporciona una ilustración de una realización de la presente invención, la cual está arreglada para distribuir contenido de manera segura y para administrar los derechos de ese contenido. En la Figura 8 un CD ROM 70 es distribuido a un dispositivo de aplicaciones 72. El dispositivo de aplicaciones 72 incluye una pantalla visual 74 para ver el contenido, el cual en la presente aplicación ejemplo incluye material de video. Por lo tanto, como es ilustrado por una flecha 76 el contenido es distribuido del CD ROM a un dispositivo de aplicaciones para su reproducción en el dispositivo de aplicaciones. Sin embargo, para controlar la distribución y el copiado, el contenido es codificado usando una clave de codificación KS referida en la siguiente descripción como la clave de codificación de contenido.

Como ya fue explicado anteriormente, una clave local compartida KCP ha sido ya establecida entre el dispositivo de aplicaciones 72 y el dispositivo de red 80. El dispositivo de red y el dispositivo de aplicaciones mostrado en la Figura 9 se corresponden de manera sustancial con el dispositivo de red y el dispositivo de aplicaciones mostrados en las Figuras 1, 2 y 4 y por lo tanto solamente las diferencias entre estas implementaciones alternativas serán explicadas.

De acuerdo a una realización de la invención, si el usuario desea ver el contenido recibido del CD ROM 70 entonces una licencia para la reproducción y/o permiso para copiar el contenido debe ser obtenida mediante la compra o por el intercambio de condiciones apropiadas. A este fin, un jugador confiable 94, envía una solicitud de la clave de contenido

desde un servidor confiable TS. El jugador confiable 94 representa un ejemplo de un programa de aplicaciones y de está manera se corresponde de manera sustancial con el programa de aplicaciones de la realización ilustrada mostrada en la Figura 5. La solicitud de la clave de contenido pudiera ser enviada desde el dispositivo de red 80, la cual pudiera ser nuevamente codificada usando la clave de la tarjeta inteligente KC. En respuesta a la solicitud para reproducir el contenido, el servidor confiable genera datos de acceso al contenido, los cuales son codificados usando la clave de la tarjeta inteligente KC que es conocida para el servidor confiable. Los datos de acceso al contenido codificados son entonces comunicados a través del enlace de red 2 al dispositivo de red ND.2 y descodificados dentro de la tarjeta inteligente 92 usando la clave de codificación de la tarjeta inteligente KC pre-almacenada.

Para reproducir el contenido, el jugador confiable 94 solicita la clave de contenido KS. Los datos de acceso al contenido incluyen la clave de contenido KS la cual puede ser proporcionada bajo las condiciones para la reproducción y/o el copiado de contenido.

En respuesta a un comando play iniciado por un usuario para solicitar la reproducción de contenido por el jugador confiable, el jugador confiable rescata los datos de acceso al contenido desde la tarjeta inteligente 92 accediendo al dispositivo de red ND.2 a través del enlace de comunicaciones 42. La solicitud es autenticada usando la clave local KCP de manera que en respuesta a la solicitud, el dispositivo de red ND.2 reproduzca los datos de acceso al contenido después que estos han sido codificados dentro de la tarjeta inteligente usando la clave compartida KCP. Los datos de acceso al contenido codificados pueden entonces ser comunicados al jugador confiable 94 y descodificados para recuperar los datos de acceso al contenido. Como se mencionó anteriormente, los datos de acceso al contenido pueden incluir no solamente la clave de codificación del contenido KS que permite que el contenido sea descodificado sino también las condiciones para reproducir el contenido y/o copiar el contenido en la forma referida generalmente como datos de administración de derechos.

Una vez el contenido haya sido descodificado y reproducido, los datos de acceso al contenido pueden ser actualizados y enviados nuevamente al dispositivo de red y almacenados en la tarjeta inteligente. Por lo tanto, la tarjeta inteligente puede ser utilizada como un lugar de depósito para asegurar los datos de acceso al contenido los cuales pueden ser actualizados a lo largo de la red hasta el servidor confiable cuando el dispositivo de red está conectado a la red, como fue explicado con referencia a la anterior realización.

De acuerdo con la realización de la presente invención ilustrada en la Figura 9, una licencia para la reproducción de una pieza de contenido particular puede ser comprada de manera segura usando la naturaleza de seguridad de la tarjeta inteligente. El dispositivo de aplicaciones AD.2 confirma la presencia de la tarjeta inteligente y autentica la tarjeta inteligente antes de que el contenido pueda ser reproducido. Como resultado, un arreglo para la distribución de contenido mejorado es proporcionado el cual reduce la posibilidad de que el contenido pueda ser ilegalmente reproducido y/o copiado de una forma que esté fuera del control del distribuidor.

La operación del dispositivo de aplicaciones y el dispositivo de red para reproducir el contenido codificado son proporcionados en la Figura 10, la cual se resume como sigue:

S.40: El contenido digital, que ha sido codificado, es cargado en el dispositivo de aplicaciones. El contenido ha sido codificado usando una clave de codificación de contenido KS.

S.41: Los datos de acceso al contenido que incluyen datos de administración de derechos que proporcionan los derechos de reproducción y las condiciones para el copiado e incluye la clave KS son codificados por el servidor confiable usando la clave de codificación de la tarjeta inteligente KC. Los datos de acceso al contenido pueden incluir otros tipos de datos e información.

S.42: El servidor confiable comunica los datos de acceso al contenido codificados al dispositivo de red ND.2.

S.43: El dispositivo de red alimenta los datos de acceso al contenido codificados a la tarjeta inteligente donde son descodificados usando la clave de la tarjeta inteligente KC.

S.44: Los datos de acceso al contenido son almacenados en la tarjeta inteligente.

S.45: La tarjeta inteligente codifica los datos de acceso al contenido los cuales incluyen los datos de administración de derechos y la clave de descodificación KS usando la clave local compartida KCP.

S.46: El dispositivo de red envía los datos de acceso al contenido codificados al dispositivo de aplicaciones.

S.47: El jugador confiable en el dispositivo de aplicaciones descodifica los datos de acceso al contenido para recuperar los datos de administración de derechos y la clave de contenido KS.

S.48: El jugador confiable puede entonces descodificar el contenido usando la clave de contenido KS, el cual es reproducido por la pantalla de reproducción 74.

Después que el contenido ha sido reproducido por el dispositivo de aplicaciones los datos de administración de derechos pueden ser solicitados para ser actualizados para reflejar el hecho de que los datos han sido reproducidos.

Correspondientemente, la operación del dispositivo de aplicaciones y el dispositivo de red se resumen en la Figura 11 la cual continúa desde un nodo "A" que aparece en la Figura 10:

S.50: Después de reproducir el contenido el jugador confiable determina si los datos de derechos digitales necesitan ser actualizados.

S.51: Si los datos de administración de derechos si necesitan ser actualizados entonces usando la clave local KCP los datos de administración de derechos actualizados son codificados.

S.52: Los datos de administración de derechos codificados son comunicados a la tarjeta inteligente en el dispositivo de red ND.2.

S.53: El dispositivo de la tarjeta inteligente descodifica los datos de administración de derechos y almacena los datos de administración de derechos en la tarjeta inteligente.

S.54: El dispositivo de red comunica entonces los datos de administración de derechos actualizados al servidor confiable de manera segura codificando los datos de derechos actualizados con la clave de la tarjeta inteligente KC.

En resumen, la distribución de contenido y la administración de derechos en ese contenido es hecho por el servidor confiable en combinación con la tarjeta inteligente la cual está únicamente asociada con un usuario. Usando las características de seguridad inherentes a las tarjetas inteligentes los datos de acceso al contenido pueden ser comunicados de manera segura al usuario en la tarjeta inteligente. Además, haciendo arreglos para que una clave local (KCP) sea generada y compartida entre el jugador confiable (programa de aplicaciones) en el dispositivo de aplicaciones y la tarjeta inteligente en el dispositivo de red los datos de acceso al contenido pueden ser comunicados al jugador confiable y luego actualizados en el dispositivo de red para un almacenaje seguro en la tarjeta inteligente.

Seguridad de Reproducción Mejorada

Para mejorar la seguridad de la reproducción del contenido y la administración y ejecución de los derechos en el contenido condiciones de seguridad mejoradas son proporcionadas. Las condiciones de seguridad mejoradas son proporcionadas haciendo arreglos para que el jugador confiable en el dispositivo de aplicaciones identifique si la tarjeta inteligente está presente dentro del dispositivo de red antes que el contenido sea descodificado y reproducido. En adición, el jugador confiable también puede autenticar la tarjeta inteligente antes de reproducir el contenido o, copiar el contenido, o verdaderamente realizar cualquier otra acción. Un diagrama de flujo que representa un proceso para reproducir el contenido como es ejecutado por el dispositivo de aplicaciones mostrado en la Figura 9 es ilustrado en la Figura 12 y se resume como sigue:

S.60: El usuario activa un modo de reproducción con el efecto de el jugador confiable (programa de aplicaciones) está arreglado para reproducir el contenido, el cual ha sido cargado en el dispositivo de aplicaciones.

S.61: El jugador confiable (programa de aplicaciones) genera entonces un mensaje de solicitud, indicando que el jugador confiable desea reproducir el contenido. El jugador confiable codifica el mensaje de solicitud usando la clave local compartida KCP.

S.62: El jugador confiable comunica entonces la solicitud codificada a la tarjeta inteligente en el dispositivo de red.

S.63: La tarjeta inteligente determina entonces si la solicitud recibida del programa de aplicaciones es auténtica. La autenticidad puede ser determinada descodificando el mensaje de solicitud codificado usando la clave local compartida KCP. Si un mensaje de acuerdo a un formato correcto es recuperado (de acuerdo a un estándar pre-arreglado) entonces el mensaje es autenticado. Si la solicitud es auténtica entonces el procesamiento pasa al paso S.64, de otra manera el procesamiento pasa a través del nodo A al paso S.80.

S.64: La tarjeta inteligente examina entonces los datos de administración de derechos que forman parte de los datos de acceso al contenido para determinar si el programa de aplicaciones tiene el derecho a reproducir o copiar el contenido. Si el programa de aplicaciones no tiene el derecho a reproducir el contenido entonces el procesamiento pasa al paso S.66, de otra manera el procesamiento pasa a través del nodo A al paso S.80.

S.68: En paralelo como parte de una autenticación mutua, el programa de aplicaciones determina si la tarjeta inteligente está presente en el dispositivo de red. Si la tarjeta inteligente está presente entonces el procesamiento pasa al paso S.70, de otra manera el procesamiento pasa a través del nodo A al paso S.80.

S.70: El programa de aplicaciones determina entonces si la tarjeta inteligente, si está presente, es la tarjeta inteligente correcta. Esto puede ser determinado de varias formas. Por ejemplo la tarjeta inteligente puede enviar un mensaje en respuesta al mensaje de solicitud para reproducir el contenido del mensaje. Para algunas realizaciones el mensaje de respuesta pueden ser los datos de acceso al contenido codificados como fue explicado en el paso S.66.

El mensaje de respuesta de la tarjeta inteligente es codificado usando la clave local compartida KCP. Si al descodificar la respuesta recibida de la tarjeta inteligente usando la clave local compartida KCP un mensaje de respuesta

correcto es recuperado, entonces la tarjeta inteligente es determinada como auténtica. Si el programa de aplicaciones determina que la tarjeta inteligente es auténtica, el procesamiento procede al paso S.66, de otra manera el procesamiento pasa a través del nodo A al paso S.80.

S.66: La tarjeta inteligente codifica entonces los datos de acceso al contenido usando la clave local compartida KCP y comunica los datos de acceso al contenido codificados al programa de aplicaciones.

S.72: El programa de aplicaciones descodifica los datos de acceso al contenido y recupera los datos de administración de derechos.

S.76: El programa de aplicaciones determina entonces si los datos de administración de derechos permiten la reproducción y/o el copiado cualquiera que haya sido solicitado. Si los datos de administración de derechos si permiten la reproducción entonces el procesamiento pasa al paso S.78 y el contenido es reproducido, de otra manera el procesamiento pasa al paso S.80.

S.78: El contenido es reproducido y/o copiado de acuerdo con la solicitud.

S.80: En el paso S.80 el contenido no es reproducido y el servidor confiable es alertado del intento de reproducir el contenido de una forma que puede ser contraria a los deseo del distribuidor.

En algunas realizaciones el dispositivo de aplicaciones puede solicitar los datos sensibles desde el servidor confiable de acuerdo con la operación del programa de aplicaciones. Para autenticar la solicitud de los datos sensibles, el programa de aplicaciones puede incluir la clave de programa KP, la cual es conocida para el servidor confiable. Además si la solicitud es comunicada al servidor confiable a través del dispositivo de red, entonces un número de identidad en línea del abonado el cual es pre-almacenado en la tarjeta inteligente (SIM) puede ser comunicado con la solicitud para verificar que la solicitud de los datos sensibles es auténtica.

Varios aspectos y características adicionales de la presente invención son definidos en las reivindicaciones anexadas.

Varias modificaciones pueden ser hechas a las realizaciones aquí antes descritas sin apartarse del alcance de la presente invención. Por ejemplo, aunque las realizaciones descritas conciben al dispositivo de aplicaciones y al dispositivo de red separados conectados a través de un enlace de comunicaciones local, será apreciado que en otras realizaciones los dispositivos de aplicaciones y de red pueden estar combinados en un dispositivo único. Para tal realización no habrá requerimiento de un enlace de comunicaciones local o alternativamente el enlace de comunicaciones local representaría un canal de comunicaciones por cable de hardware entre los 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 software. En este caso en enlace de comunicación 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 proporcionar servicios seguros a un usuario a través de una red de comunicaciones, el sistema comprendiendo

un dispositivo de aplicaciones que incluye un procesador de datos operable para proporcionar un servicio a un usuario de acuerdo con un programa de aplicaciones que solicita datos sensibles, un dispositivo de acceso a la tarjeta inteligente para acceder a una tarjeta inteligente únicamente asociada con el usuario, la tarjeta inteligente incluyendo una primera clave de codificación (KC) pre-almacenada, y el dispositivo de aplicaciones incluye una interfase de comunicaciones para comunicar datos a través de la red de comunicaciones, y

un servidor confiable es operable para comunicar los datos sensibles a la tarjeta inteligente de manera segura a través de la red de comunicaciones codificando los datos sensibles usando la primera clave de codificación (KC), los datos sensibles siendo descodificados y almacenados en la tarjeta inteligente, donde el programa de aplicaciones es operable para acceder a los datos sensibles en la tarjeta inteligente solamente a continuación de una autenticación mutua exitosa entre la tarjeta inteligente y el programa de aplicaciones.

2. Un sistema como el reivindicado en la Reivindicación 1, donde la autenticación mutua incluye un intercambio de mensajes entre el programa de aplicaciones y la tarjeta inteligente, los mensajes siendo codificados usando una segunda clave de codificación local (KCP) compartida entre la tarjeta inteligente y el programa de aplicaciones.

3. Un sistema como el reivindicado en la Reivindicación 2, donde el programa de aplicaciones en el dispositivo de aplicaciones es operable

para generar la segunda clave de codificación local compartida (KCP),

para codificar la segunda clave de codificación local (KCP) usando una tercera clave de codificación de programa (KP) que forma parte del programa de aplicaciones, y

para comunicar la segunda clave de codificación local codificada (KCP) al servidor confiable, y el servidor confiable es operable

para descodificar la segunda clave de codificación local (KCP) usando la tercera clave de codificación de programa (KP) conocida para el servidor confiable,

para codificar la segunda clave de codificación local (KCP) con la primera clave de codificación (KC), y

para comunicar a segunda clave de codificación local codificada (KCP) a la tarjeta inteligente a través de la red de comunicaciones, la tarjeta inteligente siendo operable para descodificar la segunda clave de codificación local (KCP) usando la primera clave de codificación (KC).

4. Un sistema como el reivindicado en la Reivindicación 1, 2, o 3, donde el programa de aplicaciones es operable para actualizar los datos sensibles en la tarjeta inteligente a continuación del procesamiento de los datos sensibles y los datos sensibles son actualizables en el servidor confiable cuando la comunicación está disponible a través de la red de comunicaciones.

5. Un sistema como el reivindicado en cualquiera de las Reivindicaciones precedentes, donde el programa de aplicaciones es operable para confirmar la presencia de la tarjeta inteligente en el dispositivo de acceso a la tarjeta inteligente antes de realizar una acción para proporcionar el servicio al usuario.

6. Un sistema como el reivindicado en la Reivindicación 5, donde el programa de aplicaciones es operable para confirmar la presencia de la tarjeta inteligente intercambiando mensajes codificados usando la segunda clave de codificación local (KCP) con la tarjeta inteligente.

7. Un sistema como el reivindicado en cualquiera de las Reivindicaciones 3 a la 6, que comprende un dispositivo de red para la comunicación a través de la red de comunicaciones, el dispositivo de red incluyendo el dispositivo de acceso a la tarjeta inteligente, la interfase de comunicaciones para comunicar datos de manera segura a través de la red de comunicaciones usando la primera clave de codificación (KC), y una interfase de comunicación local para la comunicación de datos con el dispositivo de aplicaciones, donde el dispositivo de aplicaciones incluye una interfase de comunicación local correspondiente para comunicarse con el dispositivo de red, el dispositivo de red y el dispositivo de aplicaciones siendo operables para efectuar la comunicación segura de los datos sensibles a través de las interfases de comunicación locales usando la segunda clave de codificación local (KCP).

8. Un sistema como el reivindicado en cualquiera de las Reivindicaciones precedentes, donde la red de comunicaciones incluye una red de comunicaciones radio móvil, la interfase de comunicaciones en el dispositivo de red incluyendo un dispositivo de comunicaciones radio móvil para comunicarse a través de la red de radio móvil.

9. Un sistema como el reivindicado en la Reivindicación 8, donde la tarjeta inteligente es un módulo de identidad del abonado, proporcionando la primera clave de codificación (KC) pre-almacenada.

10. Un sistema como el reivindicado en la Reivindicación 8 o 9, donde el programa de aplicaciones es operable para solicitar los datos sensibles desde el servidor confiable, el servidor confiable siendo operable para comunicar los datos sensibles al programa de aplicaciones a continuación de la autenticación de la solicitud del programa de aplicaciones.

11. Un sistema como el reivindicado en la Reivindicación 10, donde la solicitud de los datos sensibles incluye un número de identidad en línea del abonado y la tercera clave de codificación de programa (KP) del programa de aplicaciones, el servidor confiable siendo operable para comunicar los datos sensibles a la tarjeta inteligente si ambos, la tercera clave de codificación de programa (KP) y el número de identidad en línea del abonado, son autenticados.

12. Un método para proporcionar servicios seguros a un usuario a través de una red de comunicaciones, el método comprendiendo

proporcionar un servicio a un usuario de acuerdo con un programa de aplicaciones que solicita los datos sensibles,

acceder a una tarjeta inteligente únicamente asociada con un usuario, la tarjeta inteligente incluyendo una primera clave de codificación (KC) pre-almacenada,

comunicar los datos sensibles a la tarjeta inteligente desde un servidor confiable a través de la red de comunicaciones codificando los datos sensibles usando la primera clave de codificación (KC), los datos sensibles siendo descodificados y almacenados en la tarjeta inteligente, y

realizar una autenticación mutua entre la tarjeta inteligente y el programa de aplicaciones, y

permitir el acceso a los datos sensibles en la tarjeta inteligente por el programa de aplicaciones solamente a continuación de una autenticación mutua exitosa.

13. Un método como el reivindicado en la Reivindicación 12, donde la realización de la autenticación mutua comprende

intercambiar mensajes entre el programa de aplicaciones y la tarjeta inteligente usando una segunda clave de codificación local (KCP) compartida entre la tarjeta inteligente y el programa de aplicaciones.

14. Un método como el reivindicado en la Reivindicación 13, el método comprendiendo

generar la segunda clave de codificación local (KCP) dentro del programa de aplicaciones,

codificar la segunda clave de codificación local (KCP) usando una tercera clave de codificación de programa (KP) que forma parte del programa de aplicaciones, y

comunicar la segunda clave de codificación local (KCP) codificada al servidor confiable,

descodificar la segunda clave de codificación local (KCP) usando la tercera clave de codificación de programa (KP) conocida para el servidor confiable,

codificar la segunda clave de codificación local (KCP) con la primera clave de codificación (KC) en el servidor confiable, y

comunicar la segunda clave de codificación local (KCP) codificada a la tarjeta inteligente a través de la red de comunicaciones, y

descodificar la segunda clave de codificación local (KCP) usando la primera clave de codificación (KC) en la tarjeta inteligente.

15. Un método como el reivindicado en cualquiera de las Reivindicaciones 12, 13, o 14, donde el acceso a los datos sensible en la tarjeta inteligente comprende

procesar los datos sensibles de acuerdo con el programa de aplicaciones,

actualizar los datos sensibles en la tarjeta inteligente, y

actualizar los datos sensibles en el servidor confiable cuando la comunicación esta disponible a través de la red de comunicaciones.

16. Un método como el reivindicado en cualquiera de las Reivindicaciones 12 a 15, que comprende

confirmar la presencia de la tarjeta inteligente en el dispositivo de acceso a la tarjeta inteligente antes de realizar una acción para proporcionar el servicio al usuario de acuerdo con el programa de aplicaciones.

17. Un método como el reivindicado en la Reivindicación 16, donde la confirmación de la presencia de la tarjeta inteligente comprende

intercambiar mensajes codificados usando la segunda clave de codificación local (KCP) con la tarjeta inteligente.

18. Un método como el reivindicado en cualquiera de las Reivindicación 12 a 17, que comprende

comunicar una solicitud de datos sensibles desde el programa de aplicaciones al servidor confiable,

autenticar la solicitud del programa de aplicaciones, y

comunicar los datos sensibles a la tarjeta inteligente a continuación de la autenticación de la solicitud.

19. Un método como el reivindicado en la Reivindicación 18, donde la solicitud de datos sensibles incluye un número de identidad en línea y la tercera clave de codificación de programa (KP), y la autenticación de la solicitud incluye

autenticar el número de identidad en línea del abonado,

autenticar la tercera clave de codificación de programa (KP), y si son auténticos

comunicar los datos sensibles a la tarjeta inteligente si ambos, la tercera clave de codificación de programa y el número de identidad en línea son auténticos.

20. Un dispositivo de aplicaciones para proporcionar un servicio a un usuario, el dispositivo de aplicaciones comprendiendo,

un procesador de datos operable para proporcionar el servicio al usuario de acuerdo con un programa de aplicaciones que solicita datos sensibles,

un dispositivo de acceso a la tarjeta inteligente para acceder a una tarjeta inteligente únicamente asociada con el usuario, la tarjeta inteligente incluyendo una primera clave de codificación (KC) pre-almacenada, y

una interfase de comunicaciones para comunicar los datos de manera segura a través de la red de comunicaciones usando la primera clave de codificación (KC), donde el procesador de datos es operable

para recibir los datos sensibles desde un servidor confiable a través de la red de comunicaciones, los datos sensibles habiendo sido codificados usando la primera clave de codificación (KC), los datos sensibles siendo descodificados y almacenados en la tarjeta inteligente, donde el programa de aplicaciones es operable para acceder a los datos sensibles en la tarjeta inteligente solamente a continuación de una autenticación mutua exitosa entre la tarjeta inteligente y el programa de aplicaciones.

21. Un dispositivo de aplicaciones como el reivindicado en la Reivindicación 20, donde la autenticación mutua es efectuada por un intercambio de mensajes entre el programa de aplicaciones y la tarjeta inteligente, los mensajes siendo codificados usando una segunda clave de codificación local (KCP) compartida entre la tarjeta inteligente y el programa de aplicaciones.

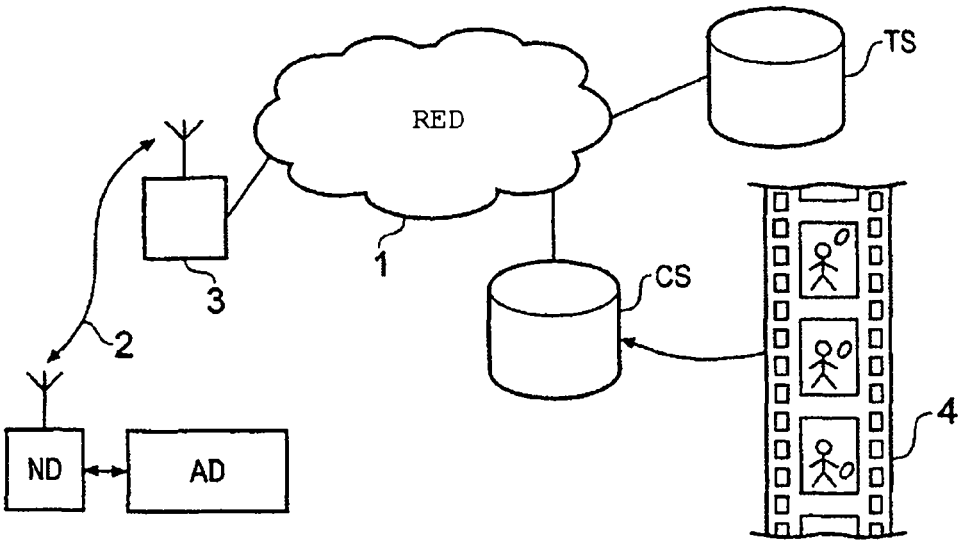

Fig. 1

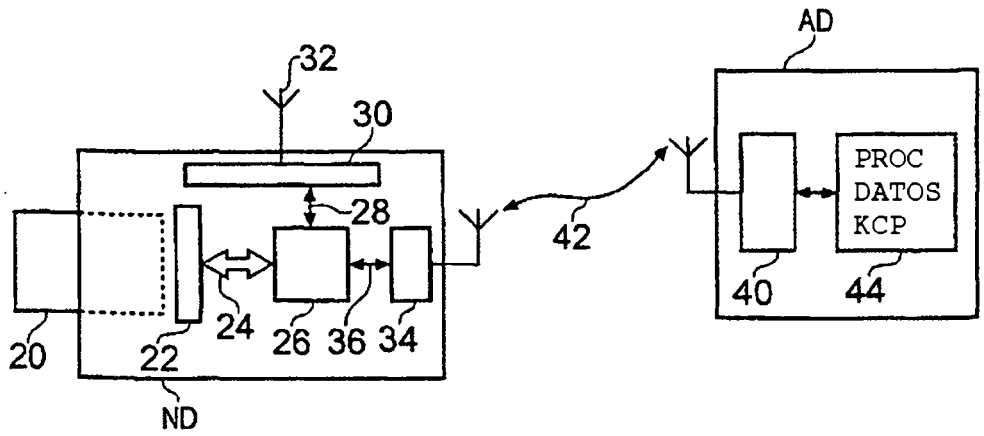

Fig. 2

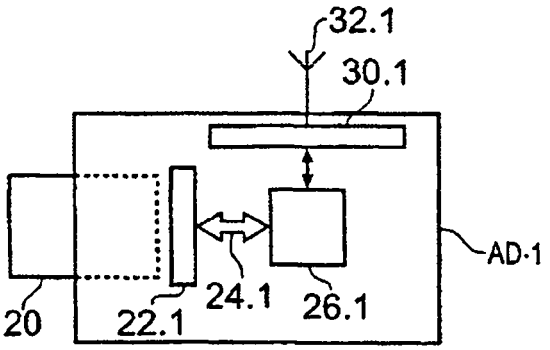

Fig. 3

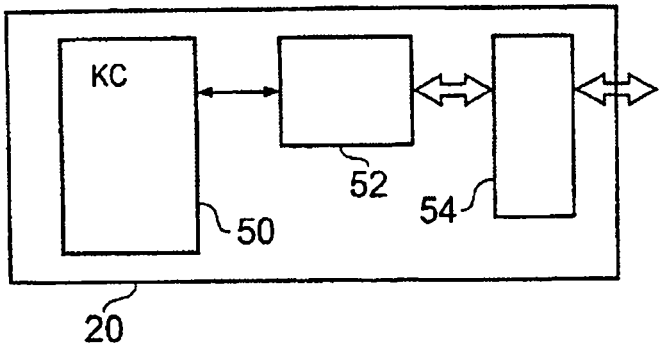
KC
52
54
50
20

Fig. 4

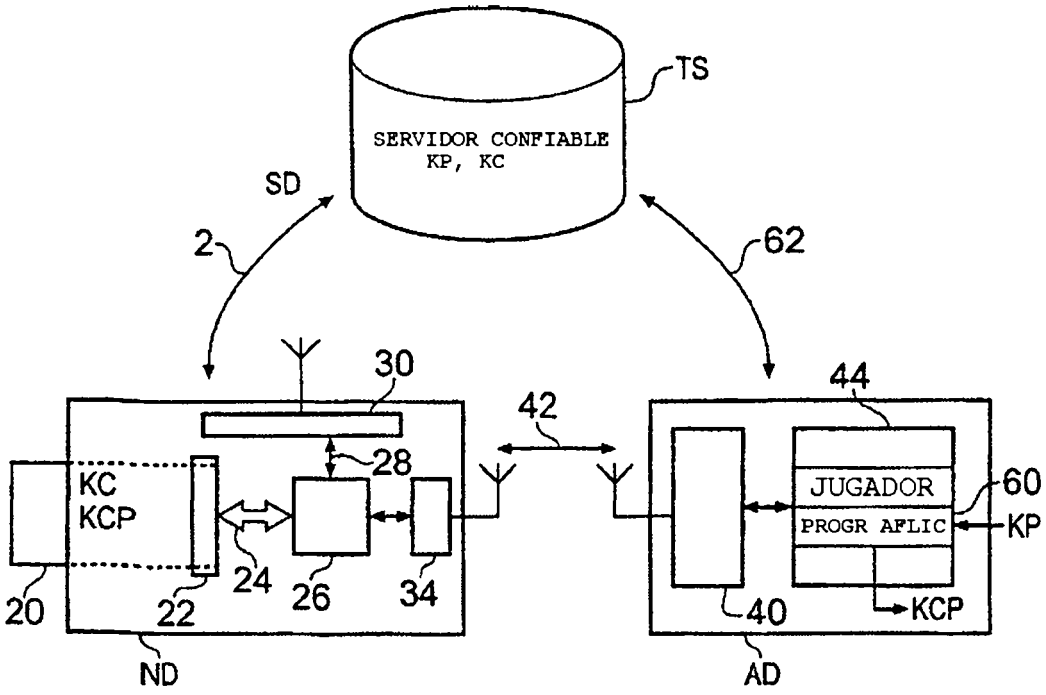
TS
SERVIDOR CONFIABLE
KP, KC
SD
2
62
30
44
42
28
KC
KCP
JUGADOR
PROGR AFLIC
60
KP
24
26
34
20
22
40
KCP
ND
AD

Fig. 5

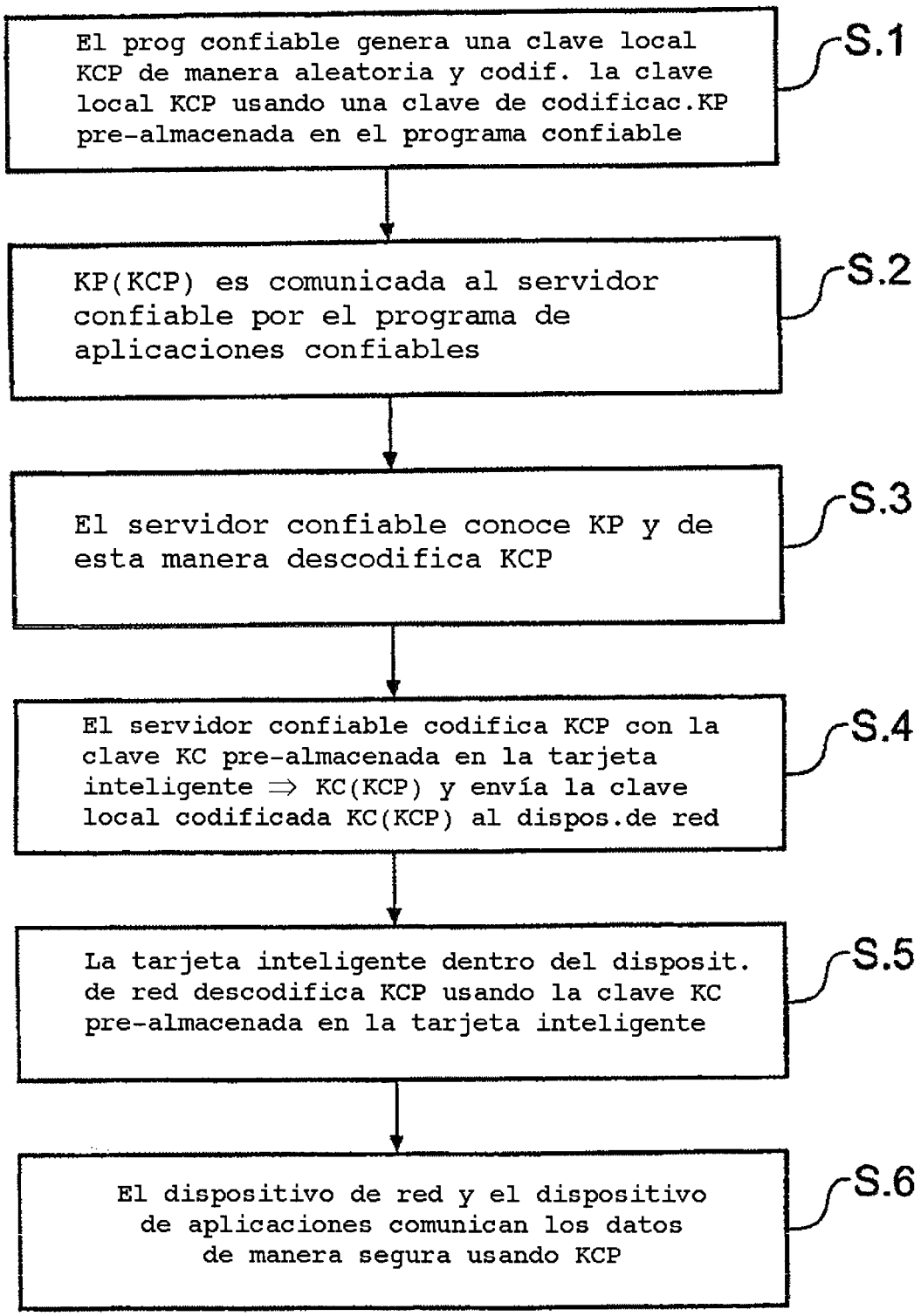
El prog confiable genera una clave local KCP de manera aleatoria y codif. la clave local KCP usando una clave de codificac.KP pre-almacenada en el programa confiable
S.1
KP(KCP) es comunicada al servidor confiable por el programa de aplicaciones confiables
S.2
El servidor confiable conoce KP y de esta manera descodifica KCP
S.3
El servidor confiable codifica KCP con la clave KC pre-almacenada en la tarjeta inteligente ⇒ KC(KCP) y envía la clave local codificada KC(KCP) al dispos.de red
S.4
La tarjeta inteligente dentro del disposit. de red descodifica KCP usando la clave KC pre-almacenada en la tarjeta inteligente
S.5
El dispositivo de red y el dispositivo de aplicaciones comunican los datos de manera segura usando KCP
S.6

Fig. 6

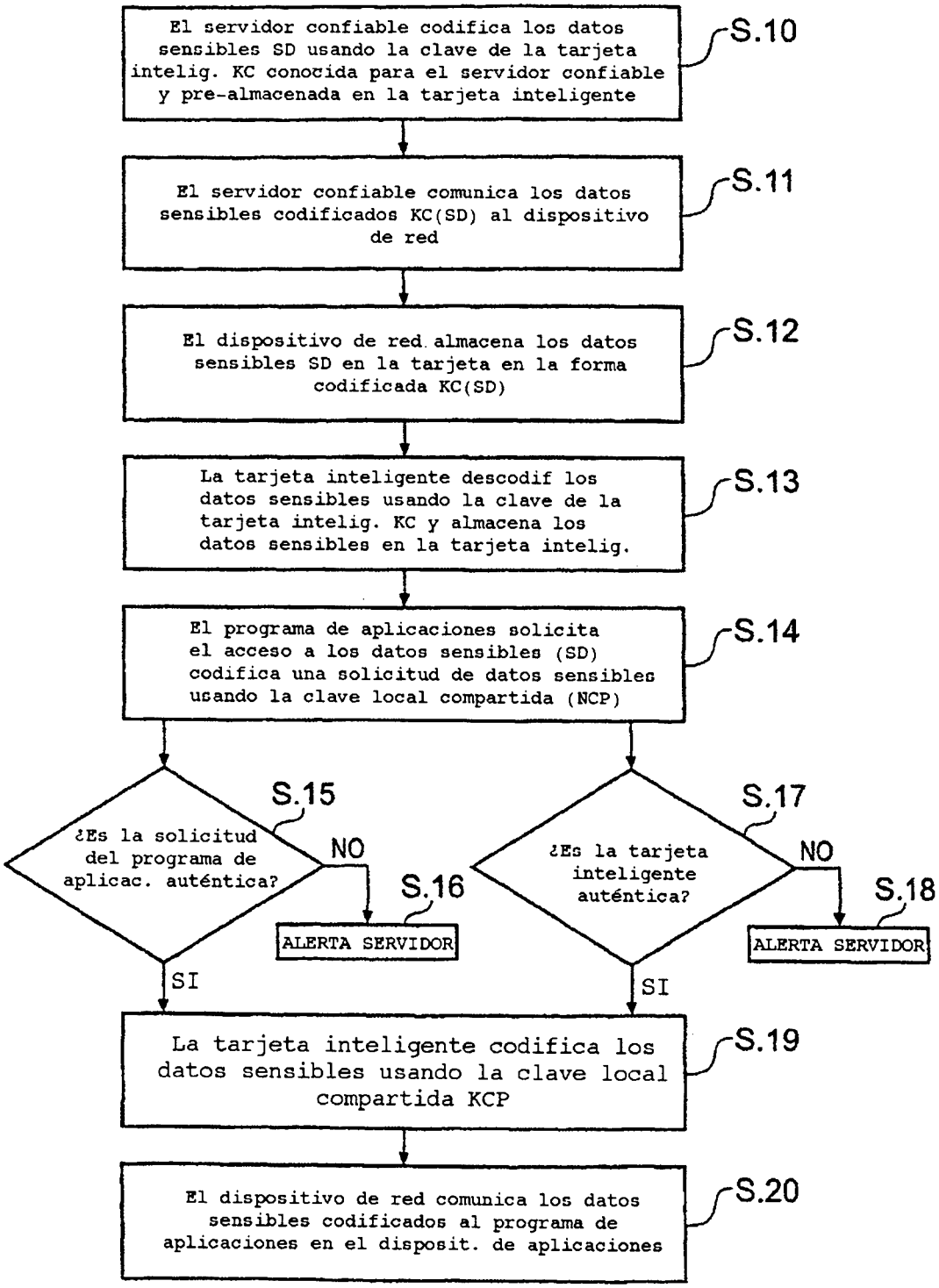
El servidor confiable codifica los datos sensibles SD usando la clave de la tarjeta intelig. KC conocida para el servidor confiable y pre-almacenada en la tarjeta inteligente
S.10
El servidor confiable comunica los datos sensibles codificados KC(SD) al dispositivo de red
S.11
El dispositivo de red almacena los datos sensibles SD en la tarjeta en la forma codificada KC(SD)
S.12
La tarjeta inteligente descodif los datos sensibles usando la clave de la tarjeta intelig. KC y almacena los datos sensibles en la tarjeta intelig.
S.13
El programa de aplicaciones solicita el acceso a los datos sensibles (SD) codifica una solicitud de datos sensibles usando la clave local compartida (NCP)
S.14
S.15
¿Es la solicitud del programa de aplicac. auténtica?
NO
S.16
ALERTA SERVIDOR
SI
S.17
¿Es la tarjeta inteligente auténtica?
NO
S.18
ALERTA SERVIDOR
SI
La tarjeta inteligente codifica los datos sensibles usando la clave local compartida KCP
S.19
El dispositivo de red comunica los datos sensibles codificados al programa de aplicaciones en el disposit. de aplicaciones
S.20

Fig. 7

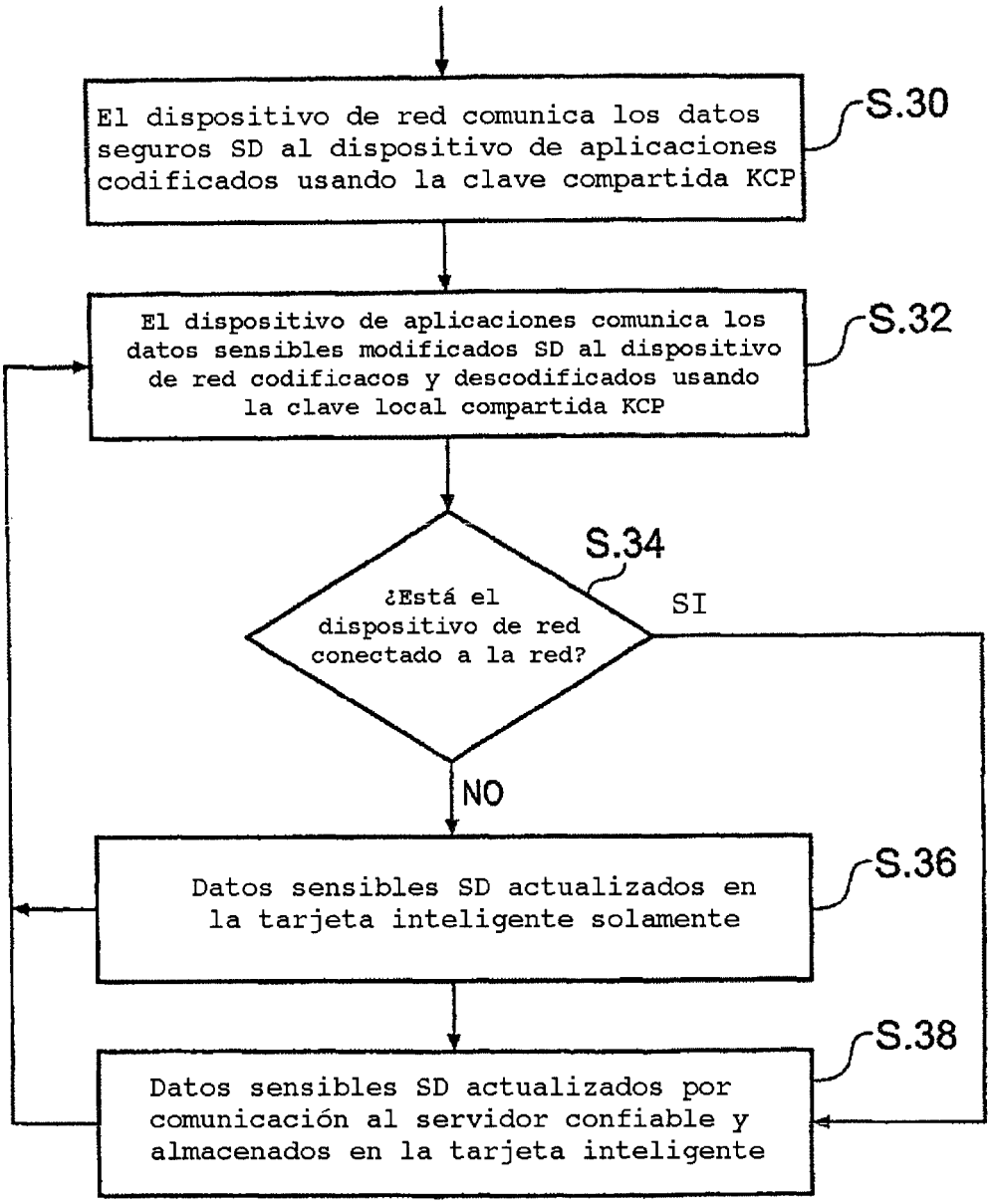
El dispositivo de red comunica los datos seguros SD al dispositivo de aplicaciones codificados usando la clave compartida KCP
S.30
El dispositivo de aplicaciones comunica los datos sensibles modificados SD al dispositivo de red codificacos y descodificados usando la clave local compartida KCP
S.32
S.34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

Fig. 8

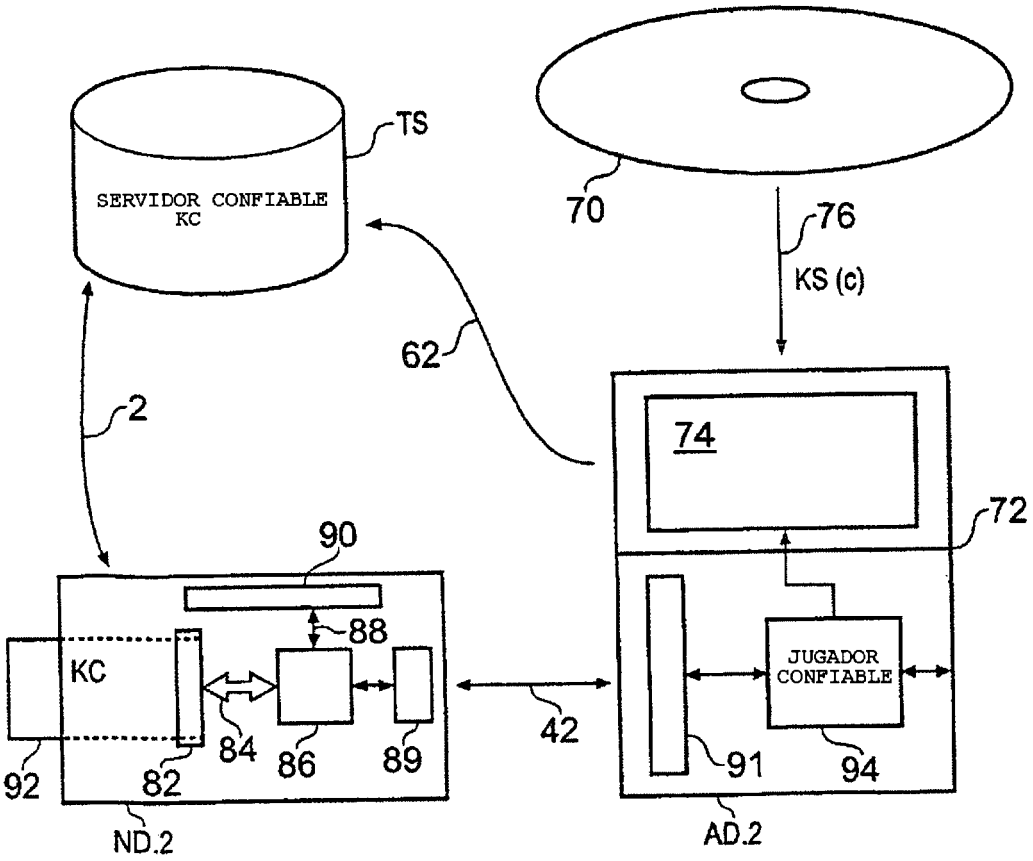
SERVIDOR CONFIABLE
KC
TS
70
76
KS (c)
62
2
74
72
90
88
KC
84
86
89
92
82
42
91
94
JUGADOR
CONFIABLE
ND.2
AD.2

Fig. 9

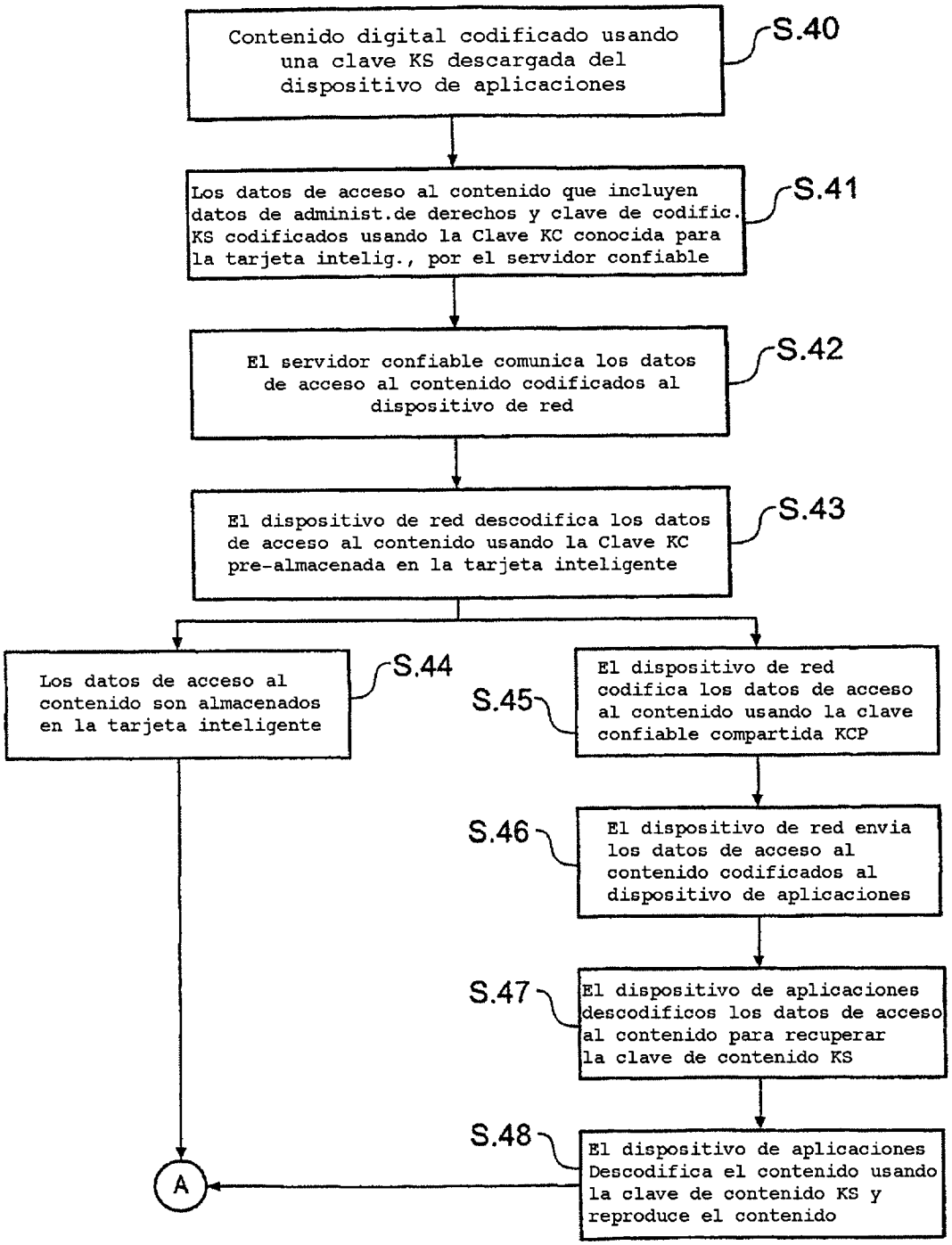
Contenido digital codificado usando una clave KS descargada del dispositivo de aplicaciones
S.40
Los datos de acceso al contenido que incluyen datos de administ.de derechos y clave de codific. KS codificados usando la Clave KC conocida para la tarjeta intelig., por el servidor confiable
S.41
El servidor confiable comunica los datos de acceso al contenido codificados al dispositivo de red
S.42
El dispositivo de red descodifica los datos de acceso al contenido usando la Clave KC pre-almacenada en la tarjeta inteligente
S.43
Los datos de acceso al contenido son almacenados en la tarjeta inteligente
S.44
S.45
El dispositivo de red codifica los datos de acceso al contenido usando la clave confiable compartida KCP
S.46
El dispositivo de red envia los datos de acceso al contenido codificados al dispositivo de aplicaciones
S.47
El dispositivo de aplicaciones descodificos los datos de acceso al contenido para recuperar la clave de contenido KS
S.48
El dispositivo de aplicaciones Descodifica el contenido usando la clave de contenido KS y reproduce el contenido
A

Fig. 10

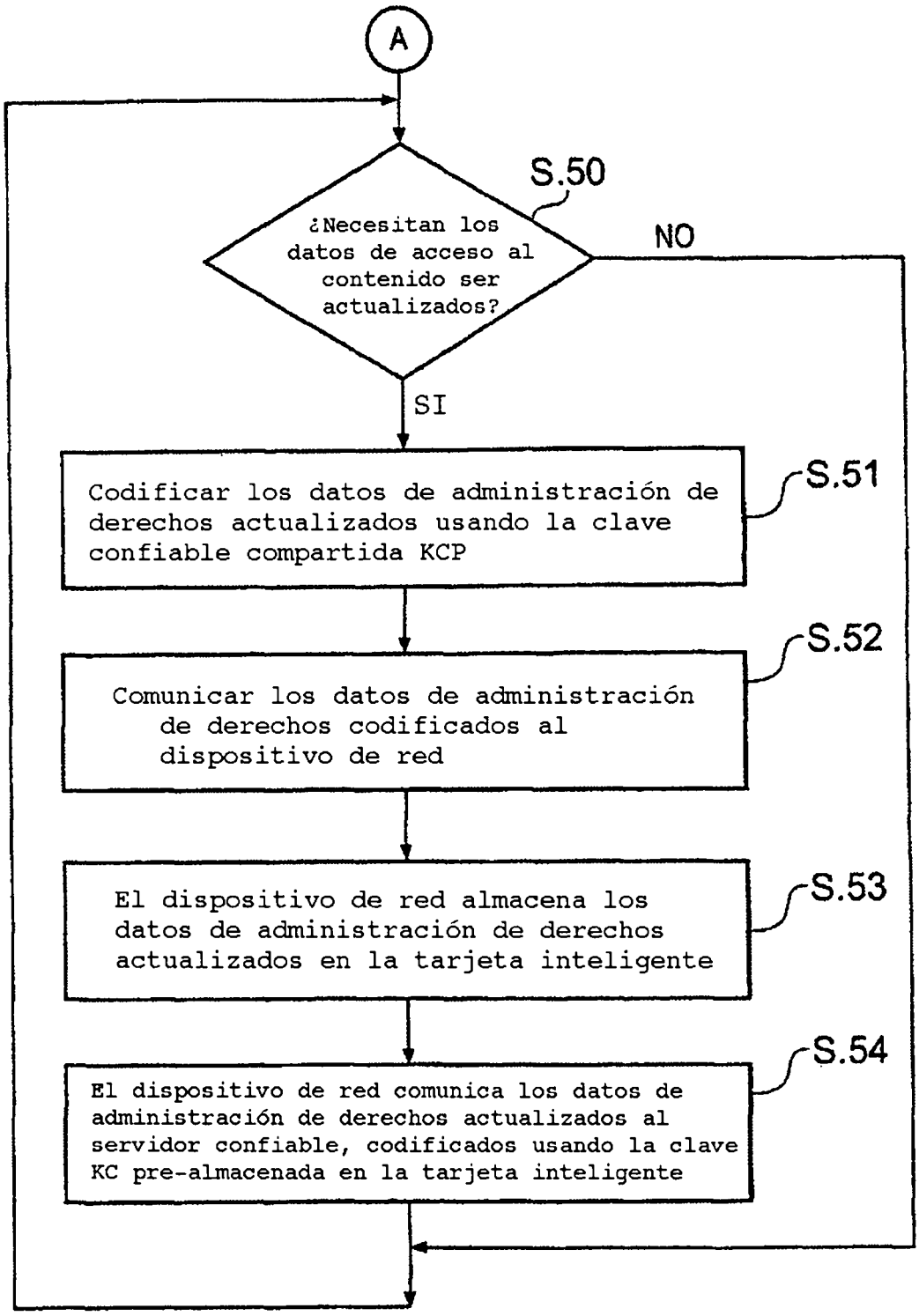
A
S.50
¿Necesitan los datos de acceso al contenido ser actualizados?
NO
SI
Codificar los datos de administración de derechos actualizados usando la clave confiable compartida KCP
S.51
Comunicar los datos de administración de derechos codificados al dispositivo de red
S.52
El dispositivo de red almacena los datos de administración de derechos actualizados en la tarjeta inteligente
S.53
El dispositivo de red comunica los datos de administración de derechos actualizados al servidor confiable, codificados usando la clave KC pre-almacenada en la tarjeta inteligente
S.54

Fig. 11

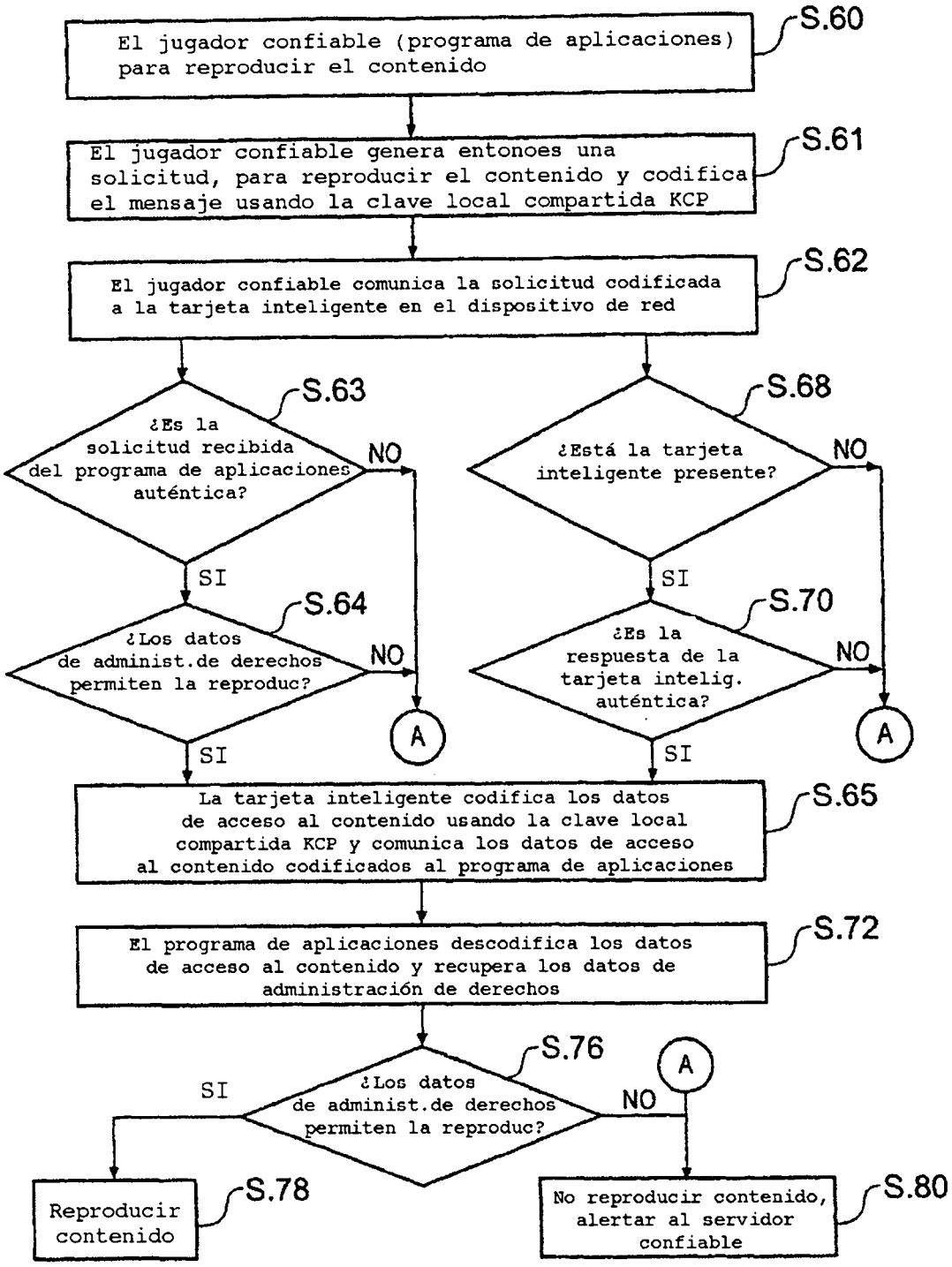
El jugador confiable (programa de aplicaciones) para reproducir el contenido
S.60
El jugador confiable genera entonoes una solicitud, para reproducir el contenido y codifica el mensaje usando la clave local compartida KCP
S.61
El jugador confiable comunica la solicitud codificada a la tarjeta inteligente en el dispositivo de red
S.62
¿Es la solicitud recibida del programa de aplicaciones auténtica?
S.63
NO
SI
¿Los datos de administ.de derechos permiten la reproduc?
S.64
NO
SI
A
¿Está la tarjeta inteligente presente?
S.68
NO
SI
¿Es la respuesta de la tarjeta intelig. auténtica?
S.70
NO
SI
A
La tarjeta inteligente codifica los datos de acceso al contenido usando la clave local compartida KCP y comunica los datos de acceso al contenido codificados al programa de aplicaciones
S.65
El programa de aplicaciones descodifica los datos de acceso al contenido y recupera los datos de administración de derechos
S.72
¿Los datos de administ.de derechos permiten la reproduc?
S.76
SI
NO
A
Reproducir contenido
S.78
No reproducir contenido, alertar al servidor confiable
S.80

Fig. 12